Примљено: 27. мај 2023.
Прихваћено: 10. септембар 2023.

УДК 57.087.1(497.5)
COBISS.SR-ID 151497993
DOI: 10.5937/ssb2401031P

BIOMETRICS, VIDEO SURVEILLANCE AND FACIAL RECOGNITION TECHNOLOGIES IN REPUBLIC OF CROATIA

Karlo PALJUG, cyber security expert,
UniCredit Group, Croatia

BIOMETRICS, VIDEO SURVEILLANCE AND FACIAL RECOGNITION TECHNOLOGIES IN REPUBLIC OF CROATIA

Summary: *The paper aims to point out some of the key issues of modern society in the context of data protection in the way of ensuring public safety. The use of video surveillance, biometrics and facial recognition technology is placed in the context of the Republic of Croatia, and the largest part of the work is devoted to these issues.*
Keywords: *video surveillance, biometric data, Republic of Croatia.*

Introduction

Privacy is freedom it is democracy. The widespread use of AI facial recognition systems threatens to erode the very essence of our personal freedom. While advocates of facial recognition technology argue that it enhances security and helps law enforcement solve crimes more efficiently, the critics point out that these benefits come at the cost of our individual privacy.

In 2021 The Euroactive reported that Police in several EU countries employ facial recognition technologies for 'ex-post identification' in their criminal investigations and that Croatia will follow it soon.[1] Croatia have bought FRT which enables local police to dramatically speed up the cross-referencing of image and video data and identifying suspects. The software can also analyze and cross-reference video footage taken from surveillance cameras. Journalist speculates that the system could greatly improve the

[1] https://www.euractiv.com/section/data-protection/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says/

surveillance of hooligans at sporting events, or identifying suspects after bank robberies.[2]

Legal framework

Croatian Constitution[3] proclaims in article 36 that the freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable. Also, in the next article the safety and secrecy of personal data is guaranteed for everyone. It states that without consent, personal data may be collected, processed, and used only under the conditions specified by law. Beside that protection of data and oversight of the operations of information systems in the state shall be regulated by law. And very important part states that the use of data contrary to the express purpose of their collection shall be prohibited.

Besides that, Croatia is also signatory to the Convention for the Protection of Human Rights and Fundamental Freedoms, and it should be emphasized that everyone has a right to respect for their private and family life, home and correspondence.

In Croatia the use of video surveillance and biometric data is regulated with few laws:

- General data protection regulation (hereinafter: GDPR)[4],
- Law enforcement directive[5] (hereinafter: LED), i.e. Law on the Protection of Natural Persons in Connection with the Processing and Exchange of Data (hereinafter: LE act)[6],
- Law on the Implementation of the General Regulation on Data Protection[7] (hereinafter: GDPR law),
- By the Law on the Processing of Biometric Data[8] (hereinafter: Biometric law).

---

2 https://www.jutarnji.hr/vijesti/hrvatska/mup-kupuje-napredni-softver-za-prepoznavanje-kontura-lica-nova-ce-tehnologija-pomoci-policiji-ali-i-ugroziti-privatnost-9845785

3 https://www.sabor.hr/en/constitution-republic-croatia-consolidated-text

4 https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679

5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

6 https://www.zakon.hr/z/1061/Zakon-o-za%C5%A1titi-fizi%C4%8Dkih-osoba-u-vezi-s-obradom-i-razmjenom-osobnih-podataka-

7 https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

8 https://www.zakon.hr/z/2431/Zakon-o-obradi-biometrijskih-podataka

Other special regulations that regulate the installation of technical protection, such as, for example, the Law on the Protection of Financial Institutions[9], which stipulates that some entities that are the addressees of that law must implement a video surveillance system for the purpose of protection. This is about banks, slot machine clubs, the post office, Financial agency. Also, Law on police duties and powers[10] address the question of using biometric data for identification, but there are not special stipulations which governs the use of such data for this purpose.

But this report will focus primarily on the four regulations mentioned above, which represent main legal framework in the Croatia regarding this topic.

Video surveillance

Two main acts which are governing the use of the video surveillance for private and public sector are GDPR and GDPR law, and when we speak about data processing data for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanctions, including protecting against threats to public safety LE act has to be consulted.

We will primarily focus on local laws, so that we can explore more domestic situation.

GDPR law is *lex generalis* in case of video surveillance, as it is specified in article 25. Also, it defines that video surveillance refers to the collection and further processing of personal data, which includes the creation of a recording that forms or is intended to form part of the storage system. What that means that nor GDPR nor GDPR law are applicable in situation where the controller is using fake cameras.[11]

Regarding the purpose of data processing through video surveillance, this can only be carried out for a purpose that is necessary and justified for the protection of persons and property, if the interests of the data subjects do not prevail. Video surveillance may cover rooms, parts of rooms, the external surface of the building, as well as the internal space in public

[9] https://www.zakon.hr/z/784/Zakon-o-za%C5%A1titi-nov%C4%8Darskih-institucija

[10] https://www.zakon.hr/z/173/Zakon-o-policijskim-poslovima-i-ovlastima

[11] For e.g. camera is not connected to the power source or it does not have storage for saving video recording. For more information see the Opinion of Croatia Data Protection Agency https://azop.hr/lazne-kamere/.

transport, the monitoring of which is necessary to achieve the stated purpose.

When we speak about vulnerable data subject's category – employees, the processing of their personal data through the video surveillance system can only be carried out if, in addition to the conditions established by this Act, the conditions established by the regulations governing occupational safety, and if the employees were adequately informed in advance of such a measure, and if the employer informed employees before making a decision on installing a video surveillance system. But, video surveillance of work premises must not include rooms for rest, personal hygiene and changing.

Regarding the monitoring of public areas through video surveillance is permitted only for public authorities, legal entities with public powers and legal entities performing public service, only if it is prescribed by law, if it is necessary for the execution of the tasks and duties of public authorities or for the protection of life and health of people and property. But conducting of Data protection impact assessment[12], which describes a process designed to identify risks arising out of the processing of personal data and to minimize these risks as far and as early as possible, is necessary in case of the systematic monitoring of publicly accessible areas.[13]

In connection with the necessity of implementing the principle of transparency from the article 13 of the GDPR and article 14 of LE act the data controller is obliged to mark that the object or individual room in it and the external surface of the object are under video surveillance, and the mark must be visible at the latest when entering the recording perimeter. This notice should contain all relevant information in accordance with the provisions of stated articles and in particular a simple and easy-to-understand image along with the text providing the data subject with the following information:

- that the space is under video surveillance
- information on the data controller
- contact information through which the data subject can exercise his rights.

It should be noted that the right of access to personal data collected through video surveillance has only responsible person of the data

[12] For more information see Croatia Personal Data Protection Agency's Decision: https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/

[13] Currently, there is no publicly available information to indicate that the DPIA has not been conducted. So *In dubio pro reo* we could conclude that it was.

controller. Also, these recordings must not be used contrary to the purpose established by the GDPR law. Technical and organizational measures have to be introduced to protected data against access by unauthorized persons. That means that devices have to be protected physically from unauthorized access, and also the data should be protected via adequate measures (for. e.g. segregation of data, implementation of the principles "need to know" and "least privilege", strong password, pen-test of the system, vulnerability assessment…). Data controller and his processor are obliged to establish an automated record system for recording access to video surveillance recordings, which will contain the time and place of access, as well as the designation of the persons who accessed the data collected through video surveillance. What that means is that they need to established log system which will gather data about users who have use the system.[14] Also, it should be stressed out, competent state bodies have access to the data from video within the framework of performing tasks within their scope established by law.

When it comes to the implementation of video surveillance and the legal ground, there are few possibilities:

- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

In case of public bodies, the practical basis will always be either the legal obligation of the controller or the performance of a task carried out in the public interest.

[14] In this sense, Croatian Personal Data Protection Agency has fined dana processor for violating rights of dana subject, i.e. the employees of processor have published video recording on the Internet which shoves data subject and his habits. More information on: https://www.bug.hr/dogadjaji/zastitarska-tvrtka-iz-zagreba-kaznjena-po-gdpr-u-zbog-curenja-videa-nadzorne-18955

Biometrics

Regarding this topic, it will focus primarily in the situations when it is used for identification of data subject by public authorities.[15]

GDPR act is stressing out that in public authorities, the processing of biometric data can only be carried out if it is determined by law and if it is necessary for the protection of persons, property, classified data or business secrets. Also, the mentioned law is stipulating that the processing of biometric data will be considered to be in accordance with the law if it is necessary for the fulfillment of obligations from international agreements regarding the identification of an individual when crossing a state border.

Mentioned law is applicable to subjects in the Republic of Croatia if the processing is carried out by:

- a data controller with a place of business in the Republic of Croatia or who provides services in the Republic of Croatia
- public authority body.
- Also, the DPIA is necessary.

But what we need to have in mind that the provisions of this law, when it comes to the processing of biometric data, do not apply to the area of defense, national security and the security-intelligence system.

LE act states in article 11, biometric data processing is permitted if:

- processing of personal data necessary for the purpose of exercising the rights and obligations of the data controller based on this Act or special regulations

[15] Regarding the private sector and the use of biometric data, the GDPR acts states:
Article 22.
(1) The processing of biometric data in the private sector can only be carried out if it is prescribed by law or if it is necessary for the protection of persons, property, classified data, business secrets or for the individual and secure identification of service users, taking into account that the interests of the respondents do not prevail are in conflict with the processing of biometric data from this article.
(2) The legal basis for processing the biometric data of the respondent for the purpose of securely identifying the service user is the express consent of such data subject given in accordance with the provisions of the General Regulation on Data Protection.
Article 23.
The processing of biometric data of employees for the purpose of recording working hours and for entering and leaving official premises is allowed, if it is prescribed by law or if such processing is carried out as an alternative to another solution for recording working hours or entering and leaving official premises, provided that the employee has given express consent for such processing of biometric data in accordance with the provisions of the General Data Protection Regulation.

- processing of personal data necessary to protect the life or physical integrity of the respondent or another person
- the respondent has published personal data.

In connection to the processing biometric data, the LE act prescribes provisions regarding automated decision making. To be specific, a decision that produces a legal effect for the data subject cannot be based solely on automated processing. But there is exception to this rule, which allows it but adequate protection of the rights of data subjects. And these decisions can be based for e.g. on biometric data but only if appropriate measures have been established. The law does not allow, in any circumstances, creation of profiles that leads to discrimination of data subject based on special categories of data i.e. on biometric data.

The LE act demands that technical and organizational measures are implemented. In other words, the controller and processor have to implement appropriate technical and organizational measures to ensure an appropriate level security with regard to risk, especially with regard to the processing of special categories (for e.g. deny unauthorized persons access to processing equipment used for processing; prevent unauthorized reading, copying, modification or removal of the data carrier; prevent unauthorized entry of personal data and unauthorized viewing, modification or deletion of stored personal data…).[16]

Biometric law applies on competent authorities when they act in accordance with their duties and obligation. It stipulates that those authorities process biometric data:

- during the process of issuing personal identification documents (purpose – preventing of identity abuse);
- during criminal investigations (purpose – discovering of perpetrator of criminal offence);
- from prisoners and convicts (purpose – discovering of perpetrator of criminal offence);
- from the wanted criminals (purpose – discovering of perpetrator of criminal offence);
- from missing persons who are being searched for (purpose – finding of missing person);
- from persons who do not have personal identification documents (purpose – establishing of identity);
- from unidentified remains (purpose – establishing of identity);

[16] For more information see article 30 of the LE act.

- from citizens of third countries or stateless persons who reside illegally in the State and do not have an identity document or there is doubt about their identity, and from citizens of a third country in the process of forced removal (purpose – checking of previous registration);
- from citizens of third countries or stateless persons who have expressed their intention to apply for international protection (purpose – checking of previous registration);
- from citizens of third countries or stateless persons who apply for a visa (purpose – checking of previous registration);
- from citizens of third countries or stateless persons who cross the state border when registering data on entry and exit (purpose – registration of entry and exit);
- when the entry to the State is denied (purpose – registration of entry and exit).

The collected biometric data is processed by an automated process and compared with those already in the database. In all procedures, the establishment of technical and organizational measures is legally imposed for the purpose of preventing access, deletion, modification and copying by unauthorized persons. It is also necessary to establish data segregation according to the principle of "the least privilege" or RBA. Any such system must have an established log database in order to be able to determine who and when entered the database and measures to ensure secure data transfer. Equally, a data recovery plan must be established so that in the event of an interruption there is the possibility of re-establishment.

Face recognition technology (FRT)

The Croatia does not have special law on face recognition technology, so applicable laws are those mentioned before. Also, there are no publicly available information which can confirm that this kind of technology is deployed in publicly accessible areas.

We must have in mind that provisions of Biometric law, when it comes to the processing of biometric data, do not apply to the area of defense, national security and the security-intelligence system.

But, with previously said within the applicable regulations, we can conclude that videos depicting individuals cannot in themselves be

considered biometric data in accordance with Article 10 LED if they are not specifically technically processed to contribute to the identification of data subject. In order for processing to be considered processing of special categories of personal data, biometric data must be processed "for the purpose of unique identification of an individual".

In other words, if the unique identification of a person is "thrown out", data obtained through a certain type of surveillance is not considered biometric data within the meaning of the GDPR and LED. For example, if only the gender of the persons appearing in the video is determined, such processing will not be considered processing of biometric data.

Also, that using this kind of technology will be legal in cases when the competent authorities needs to protect lives and property as part of their duties and obligations.

What needs to be raised is that FRT is built on the processing of biometric data, therefore, it encompasses the processing of special categories of personal data. Often, FRT uses components of artificial intelligence (AI) or machine learning (ML). While this enables large scale data processing, it also induces the risk of discrimination and false results. FRT may be used in controlled 1:1 situations, but also on huge crowds and important transport hubs.[17]

It should be noted, the EDPB recalls its and the EDPS' joint call for a ban of certain kinds of processing in relation to (1) remote biometric identification of individuals in publicly accessible spaces, (2) AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation or other grounds for discrimination (3) use of facial recognition or similar technologies, to infer emotions of a natural person and (4) processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online.[18]

So, the future EU AI act[19] and other relevant regulations will provide guidelines and steps which should be taken into account that the use of this kind of technology in legal way compatible with democratic achievements.

---

[17] https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

[18] https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (p. 7.)

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

But as we are waiting for the legislation, changes on the market are bringing new risks which, if not addressed appropriately, could damage our way of life. So, it is essential, to have in mind that this kind of risk needs to be taken into account even before relevant regulation is adopted.

БИОМЕТРИЈА, ВИДЕО НАДЗОР И ТЕХНОЛОГИЈЕ ПРЕПОЗНАВАЊА ЛИЦА У РЕПУБЛИЦИ ХРВАТСКОЈ

Karlo PALJUG, cyber security expert,
UniCredit Group, Croatia

Сажетак

Рад има за циљ да укаже на нека од кључних питања савременог друштва у контексту заштите података у начину обезбеђивања јавне безбедности. Употреба видео-надзора, биометрије и технологије препознавања лица стављена је у контекст Републике Хрватске, а овим питањима посвећен је највећи део рада.

Кључне речи: *видео надзор, биометријски подаци, Република Хрватска.*