BIOMETRIC SURVEILLANCE OF PUBLIC SPACES IN SERBIA

SHARE FOUNDATION'S POSITION AFTER THE PROPOSED DRAFT LAWS

SHARE FOUNDATION

Belgrade, 12.12.2022.

On 08.12.2022, the Ministry of Interior published a new version of the Draft Law on Internal Affairs, the Draft Law on Data Processing and Records in Internal Affairs, as well as a series of drafts of other laws from its jurisdiction. The proposed legislation contains provisions regulating **biometric surveillance in public spaces**. The public discussion on the draft laws is open until **31 December**. SHARE Foundation called all interested parties to take a stand against the legalisation of mass biometric surveillance during the public discussion.

SHARE Foundation categorically **opposes these legal proposals, in accordance with our principled position against any use of biometric surveillance in public spaces**, regardless of whether it is a domestic or international context. Our principled position is expressed, among other things, through our work and membership in EDRi, the most important network for digital rights in Europe, the Reclaim your face movement, which gathers almost a hundred organisations from all over the world that are advocating for the ban of mass biometric surveillance, as well as in the local #hiljadekamera

initiative, a community of individuals and organisations advocating the responsible use of advanced surveillance technologies.

The application of intrusive technology **would have unforeseeable consequences for a democratic society, the rights and freedoms of citizens**, which is why the Office of the United Nations High Commissioner for Human Rights recommended the introduction of a **moratorium** on the use of technology for biometric surveillance in public spaces. Also, the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) called for a **general ban** on the use of advanced technologies for automatic processing of biometric data in public spaces. In addition, it should be noted that the use of biometric surveillance in public spaces is **already prohibited** in a number of cities in the USA. Also, in the process of drafting the Artificial Intelligence Act (AI Act), 177 Members of the European Parliament requested a **ban on mass biometric surveillance** in public spaces.

The adoption of the proposed regulations in practice would mean an indiscriminate intrusion on the right to privacy and protection of personal data of all citizens and anyone who is on the territory of the Republic of Serbia, without previously establishing that such action is proportionate and necessary in a democratic society, which is a standard established by international conventions that are incorporated into the legal system of the Republic of Serbia.

The general position of SHARE Foundation against the legalisation of biometric mass surveillance is based on the following criteria:

Mandatory necessity. Even after almost four years since the announcement of the introduction of advanced surveillance systems, it has not been established that their use is necessary for the performance of the work of competent authorities, which is a condition for data processing to be legal (Article 13 of the Law on Personal Data Protection, Article 5 of Convention 108+ and Article 8 of the European Convention on Human Rights). The Ministry did not prove that modern trends in the execution of criminal offences justify the introduction of this measure, nor that it is the only method that

can effectively reduce the crime rate or find the perpetrators more efficiently. The Criminal Procedure Code, which provides for special evidentiary actions, already has a number of special mechanisms that facilitate proving the commission of specific criminal acts.

Mandatory proportionality. Biometric surveillance and the use of data collected in such a way represent a system that does not meet the criteria of proportionality. Proportionality in relation to the goal is, in addition to necessity, a condition for the legality of processing (Article 14, paragraph 3, Law on Personal Data Protection and Article 5, paragraph 1, Convention 108+). Disproportion always exists when the relationship between the means and the end is disproportionate. In this case, the goal, i.e. the suppression of crime and the more effective finding of perpetrators, is not commensurate with the means - potentially indiscriminate mass surveillance of citizens. We believe that this goal could be achieved with methods that are less intrusive on citizens' privacy.

Mass processing. The Draft Law enables the processing of data that can include an unlimited number of persons when determining identity using software for processing biometric data as prescribed in Article 68. Although this software would be used to determine the identity of persons from three relatively narrowly defined categories, in order to be able to determine the identity of only one person, it is necessary to compare the biometric characteristics (template) of a specific person with the templates of all persons who were in the recorded area, whose biometric characteristics the system extracts and stores for 72 hours. Therefore, mass data processing already exists before the very act of identifying a specific person.

Violation of the right to privacy. Remote biometric facial recognition dramatically increases the ability of state authorities to systematically identify and track individuals in public spaces, threatening the right of a person to privacy, i.e. to freely lead their lives and the right to their image, which is the essence of the right to privacy that the state has the obligation to provide to its citizens, as provided for in Article 8 of the European Convention on Human Rights. Namely, by the very fact that they are walking through public spaces that are

under video surveillance, citizens' privacy is threatened (and their personal data, i.e. their image, is processed) because it is possible to determine where they moved based on the video materials. The possibility that they can be tracked in real time (which is enabled by the data processing system introduced by the Draft Law) based on their unique and unchangeable biometric characteristics, the risk to privacy more than significantly increases. It is obvious that an omission was made during the preparation of the Draft Law, which is reflected in the lack of balance between two conflicting rights - the right to safety and security and the right to privacy. It is unclear whether these measures will increase the safety of citizens, and it is obvious that their privacy will be significantly threatened.

Violation of other rights. In addition to the right to privacy, the mass processing of biometric data through facial recognition technologies in public places causes serious and somewhat irreversible risks for a whole range of other rights and freedoms of citizens. Since the processing in question can have an irreversible and harmful impact on the reasonable expectations of citizens to be anonymous in public spaces, it can cause citizens to have a justified fear of constant monitoring and surveillance by the state, resulting in a direct deterrent on the exercise of freedom of expression, assembly, association, as well as freedom of movement.

History of abuse and mistrust. The handling of modern technologies in the work of public authorities in Serbia is burdened with numerous irregularities and abuses to the detriment of the constitutional rights of citizens, especially the right to privacy and protection of personal data. Irregularities are not eliminated and responsibility is not established for abuses. For example, our research on data retention practices in electronic communications points to several years of massive abuses with hundreds of thousands of instances of access to citizens' data, which are carried out by the Ministry of Interior and other public authorities without a court order. The incident from June 2020, when a video of a traffic accident in front of the Government of Serbia was leaked to the public, revealed the absence of even elementary physical protection measures: an unknown person used a mobile phone to record the screen of the competent authorities

on which the video of the accident was shown and shared it without authorisation.

WHAT DO THE DRAFT LAWS PROPOSE

The current legal framework of the Republic of Serbia provides the possibility for video surveillance used by the Ministry. What is new is that the proposed regulation introduces the possibility of biometric surveillance.

Specifically, **Article 44 of the Draft Law on Internal Affairs** defines a system of audio and video surveillance that consists of a set of fixed and mobile cameras and software-hardware solutions with analytical tools. Parts of this system are used to process biometric data.

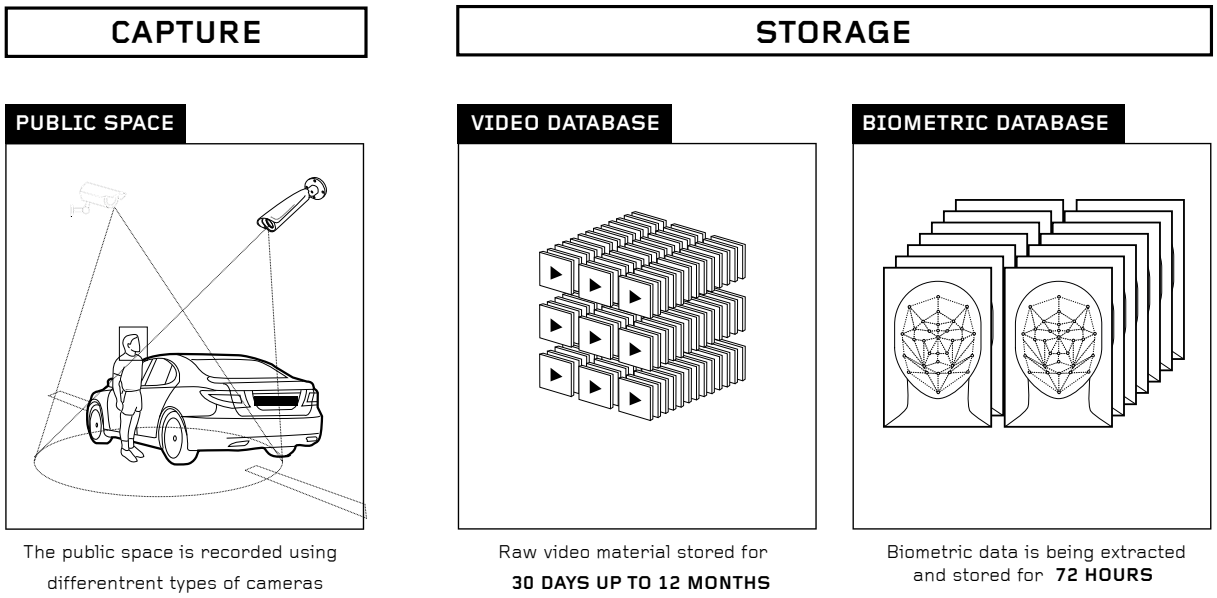
In a practical sense, this represents the legalisation of the system for biometric surveillance in public spaces, for which the infrastructure is provided by the acquisition of smart cameras and analytical tools from the Chinese company Huawei. It also provides a basis for the acquisition of software and infrastructure for processing and storing biometric data and video materials, which the Ministry has claimed to not have until now.

In the new Impact Assessment draft made by the Ministry of Interior in November 2022, it is stated that the collection of biometric data is carried out by detecting faces during recording, by creating a photo of the face/image of the face from the video and extracting biometric data from the photo as a template/digital code.

Articles 12 and 13 of the *Draft Law on Data Processing and Records in Internal Affairs* define the storage time of collected data. The video materials are stored on a central data storage system. Photos with biometric features of the face (templates) are stored on the central data storage system, separately from the video recordings, for a maximum of 72 hours from the moment of their creation.

These processes are defined in a way that they take place within the jurisdiction of the police, and biometric data are indiscriminately

collected and stored without applying the procedure prescribed for special evidentiary actions, i.e. without approval of the competent court.



Article 68 of the Draft Law on Internal Affairs stipulates that an authorised officer may determine the identity of a person by using software for processing biometric data in order to:

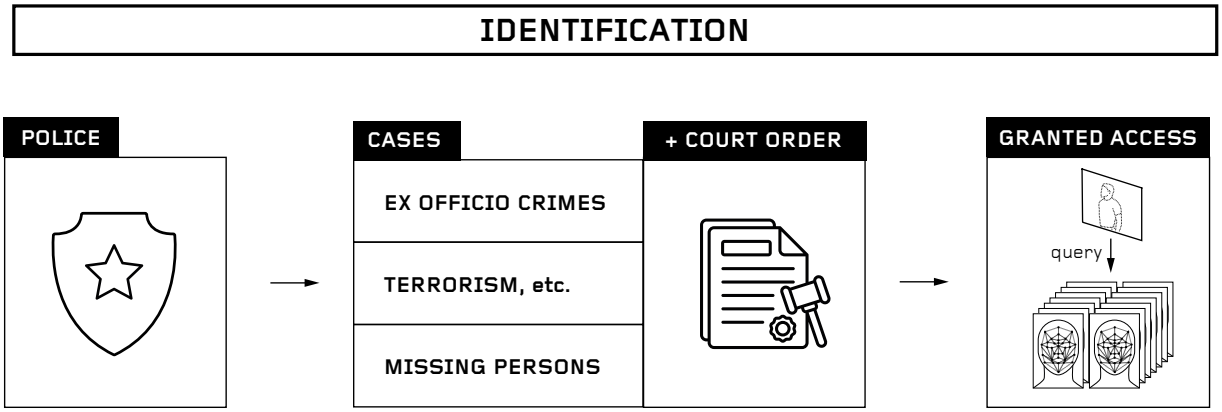
1) find the perpetrator of a criminal act for which prosecution is undertaken ex officio;

2) find persons who are reasonably suspected of preparing the commission of the criminal act of terrorism and related criminal acts, as well as other criminal acts for which preparatory actions are punishable by law;

3) finding a missing person who is reasonably suspected of being the victim of a criminal act for which prosecution is undertaken ex officio.

Determining the identity of a person in this way must be carried out according to the procedure for the application of special evidentiary actions prescribed by the law governing criminal proceedings, although it is not entirely clear which procedure for the application of special evidentiary actions would be applied, considering that for each of these evidentiary actions different conditions are prescribed.

These provisions essentially define the conditions for processing biometric data of specific categories of persons in terms of their identification.



Article 13 of the *Draft Law on Data Processing and Records in Internal Affairs* foresees two types of biometric data searches:

1) semi-automated and

2) automated, limited to:

a) specific locations - can be applied only in accordance with a security problem profile and only lasting for a specific time period;

b) faces - based on a previously made profile of a person of security interest.

It is particularly problematic that the proposed legal provisions do not define the difference between semi-automated and automated processing. Rather than in the law, this difference is described in the current working version of the Impact Assessment.

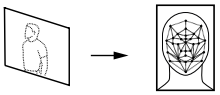
Semi-automated biometric data search is a retroactive biometric data search. It is used in situations where a person from a certain video needs to be identified, and the biometric data stored in the system is used to search other databases in possession of the Ministry. This is done by extracting a template about a specific person from a video, and using it as an input, i.e. an input value for a query in other biometric databases. The result of this search is identification, i.e. data about the identified person.

Another scenario of the use of semi-automated search is applied in a situation where, for an already identified person, it is necessary to determine their movement or location at a certain moment. In that case, biometric data in the form of a template is extracted from an existing photo or video (which can be taken from the Ministry's system or a third-party system) or an automatically generated template (for the previous 72 hours) is used. That template is then used for a query in the database, and the results of that search are all the locations and times in which that person was recorded in a public space.

Automated search of biometric data means a search that is carried out in real time. This means that according to the proposed solution, in the form of a special evidentiary action, a specific person or persons would be searched for in real time at a predetermined location. The input for this type of search is a photo or biometric template of a certain person, and it is additionally possible to define alarms that would give a notification if the wanted person or vehicle appears at a certain location.

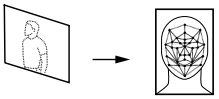
TYPES OF ACCESS

SEMI AUTOMATED SEARCH

INPUT	OUTPUT
 IMAGE BIOMETRICS	 MATCH A PERSON IN LOCATION

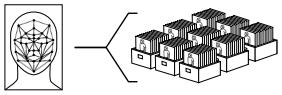
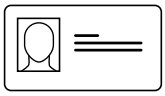
This is used when a known person needs to be located or traced over the previous 72 hours.

AUTOMATED SEARCH

INPUT	OUTPUT
 IMAGE BIOMETRICS	 MATCH IDENTITY AND LOCATION OF A PERSON IN REAL TIME

This is used when a specific person needs to be monitored in real time

SEMI AUTOMATED SEARCH

INPUT	OUTPUT
 BIOMETRICS OTHER DATABASES	 IDENTITY OF A PERSON

This is used when a person of interest is recorded and needs to be identified.

TIMELINE

In early 2019, the **then Minister of Interior** announced that Belgrade will be covered with biometric surveillance cameras, which will have the possibility of pairing with facial and licence plate recognition software. This advanced and insufficiently tested surveillance system was **procured from Chinese company Huawei.** After the announcement, SHARE Foundation filed freedom of information requests to the Ministry in relation to the procurement and technical specifications of the equipment. Multiple SHARE Foundation requests were left without an official response, while some of them are still in the appeal procedure.

The public concern because of the procurement and use of intrusive biometric surveillance was also reflected in the fact that in November 2020, **more than 17.000 citizens** signed a petition for the ban of this technology.

In accordance with the Law on Personal Data Protection, the Commissioner for Information of Public Importance and Personal Data Protection asked the Ministry to conduct an **Impact Assessment of the new surveillance system on citizens' rights.** The Ministry issued the first Impact Assessment in 2019, and when it was deemed as inadequate, the Ministry presented a new version of the assessment in mid 2020. The second version of the assessment also did not fulfil the conditions in the law, nor the accepted international standards.

In late summer of 2021, the Ministry of Interior published the Draft Law on Internal Affairs and opened a public discussion. SHARE Foundation, as well as a major part of the expert and general public, deemed the proposed solution as an attempt to legalise the Chinese mass biometric video surveillance system. **The international community** also reacted: a network of digital rights organisations European Digital Rights - EDRi sent an official letter to the Government of Serbia and Ministries of Interior and Justice, warning that the proposed provisions are incompatible with the European Convention on Human Rights guarantees.

Previously, in April 2021, a group of Members of the European Parliament sent a letter to the then Minister of Interior regarding the procurement of biometric surveillance equipment in Serbia, which still has not received a response. The European Commission spokesperson Ana Pisonero stated in July 2021 that Serbia suspended biometric data processing until the relevant legislation is aligned with the Law on Personal Data Protection. European Commission progress reports for Serbia from 2021 and 2022 state that the proportionality and necessity of such surveillance will need to be assessed, under the provisions of the personal data protection law, before its possible deployment.

The Draft Law was quickly pulled from the procedure, after which the Ministry invited civil society organisations, as well as expert and academic communities to participate in **7 consultative meetings** held from September 2021 to November 2022, where they discussed technical and legal aspects of personal data processing in the biometric video surveillance system. At the meeting held in May 2022, the Ministry presented a new draft version of the Impact Assessment, to which SHARE Foundation sent comments. Although the Ministry accepted some of SHARE's comments and implemented them in the new version of the document from November 2022, the key problems with biometric surveillance **were not addressed**, to which we pointed out in the new round of comments on the working document.