

# Serbian government is implementing unlawful video surveillance with face recognition in Belgrade

- Policy brief -

The Impact assessment of video surveillance on human rights, conducted by the Ministry of Interior did not meet the legal requirements; also, the installation of the system lacks basic transparency. Hence, the process should be suspended immediately and the authorities should engage in an inclusive public debate on the necessity, implications and conditionality of such a system.

## Introduction

The installation of smart video surveillance in Belgrade, with thousands of cameras and face recognition software, has raised public concern. Hundreds of people have submitted FOI requests asking the Ministry of Interior (Mol) about said cameras, while public officials made contradictory statements and withheld crucial information. Consequently, civil society has sought to assess the introduction of new forms of video surveillance in public spaces.

Three civil society organisations (CSOs) – SHARE Foundation, Partners for Democratic Change Serbia (Partners Serbia) and Belgrade Centre for Security Policy (BCSP) – published a detailed analysis of the Mol's Data Protection Impact Assessment (DPIA) on the use of smart video surveillance and have reached a conclusion that the document does not meet the formal or material conditions required by the Law on Personal Data Protection in Serbia.<sup>1</sup>

The Commissioner on Personal Data Protection in Serbia published his opinion on the DPIA, confirming the findings of the aforementioned organisations. According to the Commissioner, the DPIA was not conducted in line with the requirements of the Personal Data Protection Law; it is not clear which surveillance system it refers to and what are the legal grounds thereof; it does not include a risk assessment regarding the rights and freedoms of data subjects, nor a comprehensive description of data protection measures.<sup>2</sup>

## Chronology

At the beginning of 2019, the Minister of Interior and the Director of Police announced the placement of 1,000 cameras on 800 locations in Belgrade. The public was informed that these surveillance cameras will have facial and license plate recognition software.

Thereafter, CSOs requested the Mol information on:

1. Public procurement of the cameras,

---

<sup>1</sup> See (Serbian): <https://tinyurl.com/urjx9t4>

<sup>2</sup> See (Serbian): <https://tinyurl.com/up7l6tw>

2. Impact assessment on personal data protection that must be developed under the Personal Data Protection Law,
3. Camera locations and
4. Crime risk assessment based on which camera locations were determined.

The Mol answered that all documents for the public procurement of video equipment are confidential, while the information on locations and crime rate analysis is not contained in any document that the Ministry possesses, which is a legal precondition for accessing information of public importance in Serbia.<sup>3</sup>

The Mol added that the impact assessment of data processing on the protection of personal data has not completed because the implementation of the new Personal Data Protection Law had not yet begun.<sup>4</sup> However, the Mol's responses contain some information on cooperation with the Chinese company Huawei on improving the information and telecommunication system through the "Safe City" project<sup>5</sup>.

The Mol entered into a Strategic Partnership Agreement with Huawei in 2017, aiming to introduce eLTE technologies. The Serbian government provided consent for this agreement in 2016.

At the same time, Huawei published significantly more information on cooperation with the Mol. Huawei stated

that it offered Mol smart video surveillance and intelligent transport systems, advanced 4G network, unified data centres and related command centres. Furthermore, nine test cameras were originally installed at five locations, which successfully performed, according to Huawei. This information was unknown to the Serbian public.

Huawei removed the content on cooperation with the Mol from the official website shortly after the SHARE Foundation released a report,<sup>6</sup> which contained information that Huawei already published online. The archived version is still available.<sup>7</sup> In the meantime, the Minister of Interior said that 2,000 cameras will be installed instead of 1,000.

Finally, in September the Mol drafted and delivered the DPIA to the Commissioner for an opinion. For civil society, this was a commendable reaction of the authorities, especially given that the new Personal Data Protection Law entered into force at the end of August and the DPIA was completed in September 2019.

## Findings

The opportunity to address all issues of public interest through the Mol's DPIA was missed, as well as the obligation to fulfil both formal and material terms required by the Personal Data Protection Law.

The DPIA does not meet the minimum legal requirements, especially in relation to smart video surveillance, which is a

---

<sup>3</sup> See (Serbian): <https://tinyurl.com/wamepfw>

<sup>4</sup> See (Serbian): <https://tinyurl.com/sq7arrp>

<sup>5</sup> See: <https://tinyurl.com/y5y7ag5p>

<sup>6</sup> See: <https://tinyurl.com/t3e6oxa>

<sup>7</sup> See: <https://archive.li/pZ9HO>

source of most interest and concern of the domestic and foreign public. The methodology and structure of the DPIA do not comply with the requirements of the Personal Data Protection Law because:

- There is no comprehensive description of the intended actions on processing personal data in the case of smart video surveillance;
- There is no risk assessment regarding the rights and freedoms of the data subjects;
- The measures that are to be taken in relation to the existence of risk are not described;
- The technical, organizational and personnel measures for data protection are only partially described
- The legal basis for the mass use of smart video surveillance systems is disputable.

The positive effects on crime reduction as described in the DPIA are overestimated,

## Conclusion

The MoI should suspend further introduction of smart video surveillance systems. In addition, the MoI and the Commissioner should initiate an inclusive public debate on video surveillance legislation and practice that will be in line with a charter on the democratic application of video surveillance in the European Union.<sup>8</sup>

due to the fact that relevant research and comparative practices have been used selectively.

It has not been established that the use of smart video surveillance is necessary for the sake of public safety, or that the use of such invasive technology is proportionate, considering the risks to citizens' rights and freedoms.

The DPIA contains examples from countries that rely heavily on video surveillance and facial recognition technology and neglects the growing trend of banning or restricting such systems in the world, due to the identified risks to citizens' rights and freedoms.

There are numerous concerns and inconsistencies about the use of smart video surveillance comparing the DPIA and statements made by MoI officials in the media.



<sup>8</sup> See: <https://tinyurl.com/uz4npyh>