POSITION IN RELATION TO THE POST-TRIALOGUE VERSION OF THE EU AI ACT AND ITS IMPLICATIONS FOR SERBIA

(POLICY BRIEF)
DEC, 2023

SHARE FOUNDATION

EU Context

The unprecedented development and use of AI prompted the EU lawmakers to fast-forward the groundbreaking legislative step in shaping the future of artificial intelligence by achieving a political agreement on the text of the **AI Act in December 2023**, a comprehensive legislative framework designed to regulate the development and deployment of AI technologies across its member states.

Building upon earlier initiatives, the EU AI Act represents a pivotal response to the ethical, social, and legal challenges posed by the rapid advancement of artificial intelligence. The Act seeks to strike a delicate balance between fostering innovation and safeguarding fundamental rights.

This legislation comes at a time when the transformative potential of AI is accompanied by concerns regarding privacy, bias, and the ethical implications of automated decision-making. By setting clear guidelines and standards, the EU AI Act positions the European Union as a global leader in responsible AI governance, creating an environment that encourages innovation while ensuring that AI systems adhere to ethical principles and respect fundamental human rights.

Essentially, the **AI Act introduces a risk-based approach, distinguishing between minimal, limited, high, and unacceptable risks**, each requiring a corresponding level of regulatory scrutiny. Moreover, it places a strong emphasis on the prohibition of certain AI practices deemed unacceptable, reinforcing the commitment to ethical AI development.

The EU's AI Act leaves a very limited, narrow possibility for its **restrictive application with a robust oversight**. EU Member States must adhere to transparency obligations, conduct thorough risk assessments, implement quality management systems, and ensure human oversight.

Importantly, high-risk AI systems, such as those used in biometric mass surveillance, are subject to stringent requirements. Despite the ***push by the European Parliament to ban the use of real-time remote biometric identification in public spaces*** altogether, which would affect both private and public entities, the compromise AI Act text allows for a very limited number of use of BSM.

While **biometric identification systems will be *banned in principle***, an agreement has been reached on **narrow exceptions** for the use of such systems in publicly accessible spaces for **law enforcement purposes**. Accordingly, they may only be used after prior judicial authorization and for the prosecution of a strictly defined list of crimes. Moreover, national data protection authorities will need to be notified when biometric identification systems are being used. **Post-remote biometric identification systems** shall be deployed solely for the "targeted search of a person convicted or suspected of having committed a serious crime". As for **real-time biometric**

identification systems,[1] they will need to comply with a set of strict conditions and their use will be limited in time and location, for the purposes like targeted searches of victims (abduction, trafficking, sexual exploitation) or prevention of a specific and present terrorist threat.

In essence, governments can only use real-time biometric surveillance in public spaces for law enforcement purposes, subject to prior judicial authorization and for strictly defined lists of crimes, prevention of genuine, present, or foreseeable threats, such as terrorist attacks, and searches for people suspected of the most serious crimes.

Furthermore, its use must be aligned with the E**U General Data Protection Regulation (GDPR) principles**, emphasizing the importance of data protection, privacy, and user consent. It grants individuals the right to know when they are interacting with AI systems and provides mechanisms for challenging decisions made by AI. However, biometric data does not always constitute special-category data under the GDPR. GDPR Article 9(1) considers biometric data to be special-category data only when it is used for the purpose of uniquely identifying a natural person.

Application of BMS and AI high-risk systems in Serbia

As an EU Candidate Country which negotiates membership since 2014, Serbia is expected and has committed to gradually align with EU standards and harmonize its legislation with EU law (*acquis*).

This basically means that each and every piece of legislation that is adopted in Serbia as of January 2014 needs to be assessed and aligned with the EU's standards in the given area, in particular with the aim that rule of law, fundamental rights and freedoms standards are met and upheld.

Against this backdrop, the **EU's AI Act serves as a benchmark**, encouraging Serbia to adopt a similar set of rules to ensure a consistent and compatible legal framework.

Yet, **implementing the AI Act in Serbia may pose challenges**, given the need for infrastructure development, regulatory capacity building, and public awareness. Essentially, there are *two wider problems with the proper transposition of AI Act's provisions into the Serbian positive law*: (1) general legal safeguards pertaining to the protection of fundamental and human rights, and (2) use of BMS by the Ministry of Interior which is widely deployed through the surveillance cameras in Belgrade and other major cities.

Firstly, **Serbia lacks constitutional and legal framework, as well as the solid institutional**

[1] real-time biometric identification systems, they will need to comply with a set of strict conditions and their use will "be limited in time and location, for the purposes of:

- targeted searches of victims (abduction, trafficking, sexual exploitation);
- prevention of a specific and present terrorist threat; or
- the localisation or identification of a person suspected of having committed one of the specific crimes mentioned in the regulation (e.g. terrorism, trafficking, sexual exploitation, murder, kidnapping, rape, armed robbery, participation in a criminal organisation, environmental crime)".16
- Second, certain AI systems with "significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law" will be classified as **high-risk**, including:
- "certain critical infrastructures for instance in the fields of water, gas and electricity";
- "medical devices";
- "systems to determine access to educational institutions or for recruiting people";
- "certain systems used in the fields of law enforcement, border control, administration of justice and democratic processes"; and
- "biometric identification, categorisation and emotion recognition systems"

set-up whereby the main concern represents the lack of an independent body that will oversee the implementation and execution of AI Act provisions as stipulated, to underpin the proper rule of law functionality. Despite efforts towards EU accession and legal harmonization, deficiencies persist. Notable concern lies in the judiciary, where the independence of the legal system has faced scrutiny, as well as the instances of political influence, delayed court proceedings, and insufficient protection for judges against external pressures have raised doubts about the effectiveness of the judiciary in upholding the rule of law. Furthermore, Serbia's legal framework lacks adequate protection of fundamental rights, including issues related to media freedom, freedom of expression, and the right to peaceful assembly. Reports of limitations on media pluralism, self-censorship, and occasional intimidation of journalists have highlighted challenges to freedom of the press. Overall, addressing these deficiencies is crucial for Serbia's progress toward meeting AI Act requirements and ensuring robust adherence to the *numerus clausus* list of exemptions for the limited use of high-risk AI systems.

Secondly, the ***clarification on the use of BMS throughout Serbia***, including in Belgrade where the deployment of thousands of Huawei cameras equipped with the BMS tools poses a fundamental threat to a number of human and fundamental rights. The use of BMS in public spaces has raised ethical and human rights concerns globally. There are no guarantees who,[2] when and how it uses, processes, stores and operates the data collected through these systems, as well as whether they are used for targeting political opponents. This is particularly worrisome, as seen on the example of communications metadata retention in Serbia, which only has formal abuse prevention and oversight mechanisms when it comes to access to this data by the police and security services. Data obtained from the Commissioner for Information of Public Importance and Personal Data Protection has shown that the authorities had been accessing retained metadata directly in the operators' systems rather than going through the formal process of submitting requests to the telecom operators.[3]

Way Forward

Both of these challenges represent a major obstacle that the area of "real-time" BMS and its use with strict conditions while limited in time and location will be in place in Serbia.

While the AI Act offers the strict conditionality and exceptions under which the limited use is possible, the lack of Fundamentals implies that the use of BSM in real-time in Serbia will likely remain out of scope. Furthermore, EU citizens will have a right to launch complaints about AI systems and receive explanations about decisions based on high-risk AI systems that impact their rights.

All of this implies that the only solution, especially in the light of the new Draft of Interior Affairs Law, is the **uphold of ban on use of BMS in Serbia as long as the Fundamentals are not set in place** sufficiently to guarantee the just, proportionate and limited use of AI high-risk systems.

[2] Similar case regarding the evidence of data retention, as demonstrated in SHARE's study, proves the lack of oversight independent mechanism with the view to implement the Law on Electronic Communication. As practice has shown, everything has been reduced to a mere form, instead of there being information about direct access to the databases of the retained data, which is achieved by the police and security services. The whole study is accessible here: https://www.sharefoundation.info/wp-content/uploads/Zadrzani-podaci-2020_izvestaj.pdf

[3] SHARE Foundation research on this topic is available here: https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/