Legal analysis:

New biometric surveillance laws in Hungary violate the prohibition of real-time remote biometric identification under the AI Act

1. The Hungarian legal background

Relevant legislation:

- Act CXII of 2011 on Informational Self-determination and Freedom of Information (Info Act)
- Ministerial Decree 78/2015. (XII. 23.) BM of the Minister of Interior (Ministerial Decree)
- Government Decree 350/2016. (XI. 18.) Korm. on the Hungarian Institute for Forensic Sciences
- Order 11/2016. (IV. 29.) ORFK of the National Police on the tasks related to the use of the facial image analysis register and the facial image analysis system
- Act XXXI. of 1997. on the Protection of Children (Act on the Protection of Children)

On 18 March 2025, the Hungarian Parliament adopted amendments to the following acts:

- Act LV. of 2018. on the Right of Assembly (Assembly Act)
- Act II. of 2012 on Infractions, Infraction Procedure and the Infraction Records System (Infraction Act)
- Act CLXXXVIII. of 2015. on Facial Image Analysis Register and the Facial Image Analysis System (FRT Act)

These amendments limit the right to protest and freedom of expression by effectively banning LGBTQI+ demonstrations (including Budapest Pride) and designating participation in banned demonstrations as infractions and **create a legal basis for the use of facial recognition technology (FRT) for the purposes of all infraction proceedings**. The Hungarian Parliament adopted them within 24 hours, without any public debate. The amendments are **in effect from 15 April 2025**.

The amendments to the Assembly Act ban assemblies that infringe, among others, the prohibition on 'depicting or promoting homosexuality' according to the Act on the Protection of Children. Organising or participating in such assemblies is an infraction punishable by fines (Infraction Act, Section 189 (1) b).

The amendments to the Infractions Act (Section 56/A (5)) create the possibility of using facial recognition technology in all infraction proceedings, including any investigation against people participating in peaceful LGBTQI+ protests: *"in order to establish the identity of a person suspected of having committed an infraction, if the offender is unknown, the court, the infraction authority, the body conducting the preparatory procedure may use the facial*

analysis activity of the body conducting the facial analysis activity, as defined in the Act on the Facial Image Analysis Register and the Facial Image Analysis System."

So far, the use of facial recognition has only been permissible in the case of infractions punishable by a custodial sentence. The recently adopted changes therefore **widen the scope of use of facial recognition technologies (FRT) to all infractions**. According to Section 3 (3) of the FRT Act, one of the objectives of maintaining the facial profile register is to *"prevent, deter, detect and disrupt infractions, and bring offenders to justice".* Consequently, the new law, in order to assist with the identification of persons suspected of having attended banned protests, grants authorities access to FRT technology. The new legislation is strikingly disproportionate as it covers all infractions, regardless of their gravity.

It is important to note that Section 3 10a) of the Info Act defines data '*processing for law enforcement purposes'* as *"processing by an organ or person which is, within its or his functions and powers laid down by law, engaged in an activity aimed at preventing or eliminating threats to public order or public safety, preventing and detecting criminal offences, carrying out, or contributing to, criminal proceedings and preventing and detecting infractions, as well as carrying out, or contributing to, infraction proceedings, and enforcing the legal consequences imposed in criminal proceedings or infraction proceedings"*. This means that **under Hungarian law data processing for law enforcement purposes also encompasses data processing related to infractions**.

We argue that the broadened application of FRT to track individuals attending banned Pride events and committing even minor infractions (such as jaywalking) violates the AI Act, as well as the Law Enforcement Directive (LED) and the Charter of Fundamental Rights.

2. Facial recognition in Hungary

According to the FRT Act, still-image facial analysis is conducted:

- for the purposes set out in Section 3(3),
- upon request from designated bodies specified in the Act ("eligible bodies"), listed in Sections 9-9/A,
- during the course of the eligible bodies' own procedures that are governed by specific rules (e.g. during a criminal procedure, regulated by the Code on Criminal Procedure),
- by the Hungarian Institute for Forensic Sciences (HIFS), which is independent of the bodies it provides services for.

Sections 8–10 of the 350/2016 Government Decree set out that "eligible bodies" have to enter into a cooperation agreement with the HIFS to be eligible for requesting facial analysis. After entering into a cooperation agreement, the eligible bodies request unique identifiers to "authorised personnel". Facial analysis may only be requested by a member of the authorised personnel.

In a nutshell, during specific procedures (e.g. criminal procedure, infractions procedure, etc.), eligible bodies may request that the HIFS conduct facial image analysis on images obtained or

used in said procedures. Facial analysis is an optional technical assistance that eligible bodies may request from the HIFS.

What is the reference database?

The reference database for the facial analysis is known as the "Facial Image Analysis Register" and is composed of **a collection of biometric templates derived from pictures from several government databases**, such as images of IDs, passports and driver's licenses (stored in the "address registry"), as well as criminal or asylum records, if applicable.

What kind of data is processed?

- Facial Image Analysis Register: the controllers of government databases send facial images and corresponding connection codes to the HIFS; the HIFS converts facial images into biometric templates and deletes the original pictures. Only the biometric templates and the connection codes are stored.

- Eligible bodies (e.g. the police): they control the facial images according to their specific statutes; they send the images to HIFS, which, if there is a match, only sends them the connection codes.

- HIFS: controls the facial images sent by the eligible bodies and produces a biometric template, which is checked against the Facial Image Analysis Register. If there is a match, it requests the corresponding facial images from the relevant government database through the connection codes. After facial analysis is completed, the connection code of the matching image is sent to the requesting eligible body, and the images are deleted.

How is facial analysis performed?

Below we detail two procedures available to the police for conducting facial analysis within the amended legal framework. Understanding the details of and the differences between these two procedures is crucial for the analysis of the interplay with Article 5 of the AI Act.

- ***Facial image analysis - the standard procedure regulated in Section 12 of the FRT Act***

1. The eligible body sends an image and a request to HIFS.
2. Experts at HIFS convert the image into a biometric template.
3. The biometric template is checked against the Facial Image Analysis Register.
4. The experts may ask for the original images from the given government database through the connection code.
5. An image is considered a match if two experts label it as such independently of each other.
6. If there is a match, the connection codes are sent to the eligible body so they can access the image from the given government database.

- ***Automatic comparison - applicable to infraction procedures and regulated in Section 12/A of the FRT Act***

1. Requested in **infraction procedures** and for police ID checks.
2. The police connect to the HIFS's system **directly** and request an automated facial analysis of the sent image.
3. The facial image analysis system operates by analysing still images individually.
4. The system **automatically** converts the facial image into a biometric template and returns the connection codes of the **five closest matches** to the police.
5. The police determine which match may represent the suspect.
6. The police request the facial images corresponding to the connection codes from the government databases.

> Conclusion:
>
> **Based on our analysis, as of 15 April 2025, the police rely on "automatic comparison" in any infraction procedures, including participating in Pride protests. To the best of our knowledge, infraction procedures can be initiated on the spot by the police, and during a particular demonstration, they can already have a direct connection to the HIFS's system (as opposed to having to request connection after the fact). We also understand that in the case of assemblies, the images are derived from video footage recorded by the police, as recording assemblies is a common practice. To confirm these assumptions grounded in our analysis of Hungarian legislation we have filed a freedom of information request with the police in Hungary. However, considering the government's lack of transparency and the rule of law crisis in Hungary, we might not receive a satisfactory response.** We therefore ask the AI Office to request relevant information from the Hungarian authorities regarding the conditions of use of FRT, as well as the technical details, in particular the process and timeline for obtaining direct connection to the HIFS's system and the involvement of the HIFS experts in the process.

3. Interaction of the Hungarian laws with the EU Artificial Intelligence Act

The AI Act aims to harmonize national legislation, among others, to protect citizens and society against the adverse effects of AI. Its main legal basis is Article 114 of TFEU, while the use of AI-enabled biometric data processing by law enforcement is based on Article 16 TFEU, which provides a legal basis to rely on data protection.

The Hungarian FRT law effectively **creates a broad legal base for the use of remote biometric identification (RBI)** while offering no details about technical or procedural safeguards that the police must follow. The Hungarian law is also unclear whether the police are allowed to record every demonstration and if so, for what purposes. As a result, individuals attending demonstrations and expressing their political opinions have to take into account that they can be subject to biometric surveillance and face potential repercussions. This creates a **chilling effect on exercising their fundamental rights**.

Below we argue why the amendments *de facto* authorise a remote biometric identification system which is prohibited under Article 5 (1)(h) of the EU Artificial Intelligence Act.

Violation of the prohibition of real-time remote biometric identification

Article 5(1)(h) of the EU AI Act prohibits "*the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement*" unless it falls under one of the three exceptions in points (i) - (iii) and is authorised in the Member State's national law with the accompanying safeguards.

Although the AI Act has not yet been subject to interpretation by courts due to its novelty, there are compelling reasons to conclude that **the Hungarian FRT Act would contravene Article 5(1)(h)** of the AI Act. Below, we consider two key determining questions (with the assumption that it is indisputable that the system amounts to RBI in publicly accessible spaces):

1) ***Does the FRT Act permit the "real-time" use of remote biometric identification systems, thereby coming under the scope of Article 5, or only high-risk "post" use?***

Several parts of the AI Act and the European Commission's AI Act Prohibition Guidelines are relevant to determining what exactly constitutes a real-time use. In particular (bold for emphasis):

- Article 3(42) of the AI Act defines real-time remote biometric identification system' as a *"remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur **without a significant delay**, comprising not only instant identification, but **also limited short delays in order to avoid circumvention;**"*
- Recital (17) of the AI Act further confirms that "***'near-live' material***" is also considered within the scope of the ban described in Article 5(1)(h). To the contrary, post (retrospective) use "*involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, **which has been generated before the use of the system in respect of the natural persons concerned**;*"
- Paragraph (310) of the Guidelines on Prohibitions in the AI Act also clarifies that whether or not a use is real-time "*will have to be **assessed on a case-by-case basis***", but that "*a delay is significant* [and therefore not subject to the prohibition] ***at least***

when the person is likely to have left the place where the biometric data was taken."

An RBI system does not exist just at the point of the creation of a biometric template, but is a broader system of inputs, analyses and outputs. As explained in Part 2 above, the automated facial comparison system outlined in Section 12/A of the FRT Act is clearly designed with **the ability to take newly-generated or recently-generated material** (usually from CCTV footage, and police recordings during demonstrations, but conceivably also from a phone or other hand-held recording device) a**nd to automatically identify people in the material** through direct connection to the HIFS system.

The law has thus been designed to facilitate the use of systems having **the capability to seamlessly go from a person attending a demonstration, to that person being identified, in a very short amount of time, which would not amount to a "significant delay"**. For all intents and purposes, the system is capable of the same use case and same outcome as a system which captures, analyses and identifies a person in one fell swoop (a 'traditional' real-time system). It thus meets the criteria laid down in the AI Act for a "real-time" system, and is distinct from a "post" system where the input material is generated independently from the use.

Regardless of the technical design of a particular system that might currently be at the disposal of the HIFS, Section 12/A of the FRT Act is formulated in a way which **does not explicitly preclude real-time facial image analysis**, e.g. by clarifying that the request for analysis can only be sent to HIFS after the demonstration and not on the spot or without a significant delay. Therefore, **this law evidently opens the door to developing and deploying a system with clear real-time identification capabilities**.

Finally, the amendments clearly contravene the purpose of the Article 5(1)(h) prohibition explained in Recital (32), by creating a significant chilling effect from attending a demonstration:

- Recital 32: "*The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons,* ***to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights***."

> Conclusion:
>
> **Considering that the AI Act recognises the need for a case-by-case assessment of whether or not a system is "real-time" - and that the rules should not be circumvented by arbitrary technical or procedural elements - it is important for a Charter-compliant interpretation of the Act that the use of systems which manifestly reach this threshold are**

> **considered to fall within scope. Based on these arguments, we conclude that for all intents and purposes,** the Hungarian FRT Act permits the use of RBI systems against people suspected of committing an infraction, including participants of banned demonstrations, in ways that should be considered "real-time"**. This means that the FRT Act, and any use of a system on the basis of the FRT Act, would be manifestly non-compliant with the rules and safeguards laid down in the AI Act.**

2) Would the use of real-time RBI be considered "for the purposes of law enforcement"?

For determining whether the Hungarian RBI system will be used for the purposes of law enforcement, and therefore fall within the scope of the prohibition in Article 5(1)(h) of the AI Act, we should consider the interplay between the AI Act, the Law Enforcement Directive, relevant Court of Justice jurisprudence and national Hungarian law.

Article 5(1)(h) forbids the use of biometric identification systems in public places for "*the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*". We note that this should be interpreted in light of the definition of law enforcement activities outlined in Recital (12) of the LED:

- "*focused mainly on the prevention, investigation, detection or prosecution of criminal offences";*
- *"such activities can also include the exercise of authority by taking* ***coercive measures such as police activities at demonstrations****";*
- *"they also include* ***maintaining law and order as a task conferred on the police or other law-enforcement authorities*** *where necessary to safeguard against and prevent threats to public security and* ***to fundamental interests of the society protected by law which may lead to a criminal offence***."

These provisions are also reconfirmed in the AI Act Prohibition Guidelines (Paragraph (321)).

Further, the definition of a "*criminal offence"* has been clarified by the Court of Justice of the European Union. The three determining criteria include: 1) the classification of the offence under national law 2) the nature of the offence 3) the nature of the penalty.

We argue that in this case these conditions are clearly met:

- As discussed above, Section 3 § 10a of the Info Act considers "infraction procedures", such as attending a banned demonstration, to be a "criminal procedure" and consequently, the applicable data protection rules are included in the Law Enforcement Directive, and not the GDPR. This means that the Hungarian national law considers infractions to be treated in the same way as criminal offences and as such should be covered by the scope of Article 5(1)(h) and **within the bounds of law enforcement purposes**.

- Furthermore, these offenses carry a punitive sanction and can lead to financial penalties.
- Finally, the jurisprudence of theEuropean Court of Human Rights - mirrored by the CJEU in the above mentioned case - has confirmed that minor offences, as well as a**dministrative offences related to holding a public assembly, constitute and should be treated as criminal offences.**

We also note that Section 217/C of Act C of 2012 on the Hungarian Criminal Code provides that organising or promoting a banned assembly is, in fact, a criminal offence: *"a person who organises a prohibited assembly or announces such an assembly within the meaning of the Act on the right of assembly is guilty of a misdemeanour and shall be punished by imprisonment for up to one year, unless another criminal offence is established"*. It is therefore evident that the use of RBI during demonstrations to identify those who organise or promote them (while necessarily capturing faces of all participants) will fall within the scope of law enforcement activities and, consequently, within the scope of the Article 5 prohibition. Accepting the argument that the AI Act prohibition does not apply to infraction procedures, even when the same system can be used for identifying regular participants and organisers at the same time, **would create an easy way for Hungarian authorities to circumvent the AI Act, which is contrary to the EU legislator's intent.**

Last but not least, the stated purpose of the new Hungarian laws is for police to protect the fundamental interests of society - allegedly, the rights of children, which is a law enforcement activity based on the LED and therefore should be interpreted as law enforcement also for the purposes of enforcing the AI Act prohibition.

> *Conclusion:*
>
> **Based on established CJEU jurisprudence and the teleological interpretation of the AI Act, we believe that the use of RBI as envisioned by the FRT Act** will constitute law enforcement activities and will therefore fall within the scope of both the LED and the prohibition in Article 5(1)(h) of the AI Act. **Argument to the contrary would lead to an absurd situation where people's fundamental rights would enjoy significantly weaker protection in less serious offences, which certainly was not the intention of the EU legislator.**

3) Exceptions to the prohibition

For the avoidance of doubt, the use of FRT for all infractions **does not fall within the scope of any of the limited exceptions** in Article 5(1)(h), all the more when it is destined to unduly restrict citizens' freedom of assembly. The introduction of the legal basis for conducting real-time RBI in Hungary is therefore in glaring contradiction with the prohibition included in Art. 5(1)(h).