Legal analysis:
New biometric surveillance laws in Hungary violate the Charter of Fundamental Rights and the AI Act

The Hungarian legal background

On 18 March 2025, the Hungarian Parliament adopted amendments to 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), and Act CLXXXVIII. of 2015. on Facial Image Analysis Register and the Facial Image Analysis System (FRT Act).

These amendments limit the freedom of assembly and freedom of expression by effectively banning LGBTQI+ demonstrations (including Budapest Pride) and qualifying participation in banned demonstrations as infractions. Furthermore, they **create a legal basis for the use of facial recognition technology (FRT) for the purposes of all infraction proceedings**. The Hungarian Parliament adopted the amendments within 24 hours, without any public consultation with relevant stakeholders. The amendments have been **in effect since 15 April 2025**.

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 Charter of Fundamental Rights, the AI Act, as well as the Law Enforcement Directive (LED).

Facial recognition in Hungary

Under the FRT Act, during specific procedures (e.g. criminal procedure, infractions procedure, etc.), authorized bodies, such as the police, may request that the Hungarian Institute for Forensic Sciences (HIFS), a body that is independent from those it provides services for, conduct facial image analysis on images obtained or used in said procedures. Facial analysis is an optional technical assistance that authorized bodies may request from the HIFS.

The facial analysis is conducted against a reference database known as the “Facial Image Analysis Register”. It is composed of **a collection of biometric templates derived from pictures from several official 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.

Based on our analysis, as of 15 April 2025, the police connect to the HIFS's system **directly** and request an automated facial analysis of the sent image in any infraction procedures, including participating in Pride protests. The facial image analysis system analyzes still images individually and **automatically** converts the facial image into a biometric template, and returns the connection codes of the **five closest matches** to the police. The police then determine which match may represent the suspect. Infraction procedures can be initiated on the spot by the police, and during a particular demonstration, to the best of our knowledge, they can 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 have therefore asked 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.

Interaction of Hungarian Laws with the EU Artificial Intelligence Act

The Hungarian FRT Act introduces a broad legal basis for the use of remote biometric identification (RBI) without specifying any technical or procedural safeguards for police operations. This effectively permits a system of remote biometric identification that is prohibited under Article 5(1)(h) of the EU Artificial Intelligence Act (AI Act).

Article 5(1)(h) of the AI Act bans the use of *real-time* RBI systems in publicly accessible spaces for law enforcement purposes, unless certain strict exceptions apply and such use is authorised under national law with appropriate safeguards.

Although courts have not yet interpreted the AI Act, there are compelling reasons to conclude that Hungary's FRT law violates Article 5(1)(h). Assuming it is undisputed that the system constitutes RBI in public spaces, two central questions must be addressed.

1. Does the Hungarian law permit "real-time" use?

Under Article 3(42) of the AI Act, a real-time RBI system is defined as one in which biometric data is captured, compared, and matched without significant delay, including cases with "limited short delays." Recital 17 confirms this includes "near-live" material, while the AI Act Prohibition Guidelines (para. 310) clarify that a use is real-time unless the delay is so significant that the individual has likely already left the scene.

Section 12/A of Hungary's FRT Act enables real-time identification by linking newly recorded material to the HIFS database, allowing police to identify individuals, such as protesters, within moments. This clearly falls under the definition of real-time RBI and is therefore covered by Article 5(1)(h).

Additionally, the Hungarian law undermines the purpose of the AI Act prohibition, as stated in Recital 32, which highlights the chilling effect of such surveillance on public participation and freedom of assembly. A system that allows authorities to identify people at demonstrations in real time significantly deters individuals from exercising their fundamental rights.

2. Is the system used for "law enforcement purposes"?

Article 5(1)(h) of the AI Act applies to uses for "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties." This aligns with Recital 12 of the LED, which includes police activities at demonstrations and maintaining public order.

Hungarian law treats "infraction procedures", such as participation in a banned protest, as criminal procedures. According to Section 3. § 10a of the Hungarian Info Act CXII of 2011, these fall under the LED, not the General Data Protection Regulation (GDPR), and involve punitive sanctions, such as fines. The Court of Justice of the EU (C-439/19) has held that an offence qualifies as criminal based on its classification, nature, and penalty — all of which are met here.

Thus, the use of FRT in these cases qualifies as a law enforcement purpose within the meaning of Article 5(1)(h). Arguing otherwise would allow national authorities to bypass EU law by categorising prohibited uses as infractions — a loophole the AI Act clearly intended to avoid.

No applicable exceptions

Finally, the use of FRT in Hungary does not meet any of the limited exceptions set out in Article 5(1)(h). None of the justifications — such as the search for specific victims, prevention of imminent threats, or prosecution of serious crimes — applies to routine identification at public

gatherings. The stated goal of protecting children does not provide a sufficient legal basis or necessary safeguards.

In conclusion, the Hungarian legislation authorises real-time RBI in ways that directly conflict with the AI Act, and in the next chapter we describe how it is in conflict with the Charter of Fundamental Rights. The law bypasses core EU safeguards and also poses a serious threat to democratic freedoms, particularly the right to peaceful assembly.

Compliance of Hungarian laws with EU Charter of Fundamental Rights

The amendments stand in violation of the EU's AI Act and the rights enshrined in the Charter of Fundamental Rights and in contradiction with the rulings of the Court of Justice of the EU and the European Court of Human Rights (ECtHR). These amendments are discriminatory and limit the right to assembly (Article 12), freedom of expression (Article 11), right to data protection (Article 8) and privacy (Article 7) by effectively banning LGBTQI+ demonstrations, and qualifying participation in banned demonstrations as infractions, and allow the use of facial recognition technology to identify participants.

Privacy and Personal Data – Articles 7 and 8 of the Charter

According to the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement ("the Guidelines"), processing biometric data "under all circumstances constitutes a serious interference in itself" with the rights protected by the Charter of Fundamental Rights (para. 36). According to Article 10 of the Law Enforcement Directive, processing of special categories of data, such as biometric data, shall be allowed only where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject (Guidelines para 66). The Guidelines further state that "[i]n accordance with the settled case-law of the CJEU, the condition of 'strict necessity' is also closely linked to the requirement of objective criteria in order to define the circumstances and conditions under which processing can be undertaken, thus excluding any processing of a general or systematic nature" (para. 73, and see CJEU Case C-623/17, para 78).

Multiple rulings by the Court of Justice of the European Union (CJEU) have confirmed that legislative measures providing a legal basis for personal data processing directly impact the rights under Articles 7 and 8 of the Charter (see, in particular, C-594/12; C-291/12).

In this case, Hungary's use of facial recognition technology to identify individuals committing infractions – regardless of the severity or nature of the offence – limits individuals' right to privacy as outlined in Article 7 of the Charter. In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives.

The ECtHR has explicitly stated that deploying highly intrusive facial recognition technology to identify and arrest peaceful protest participants or to enforce misdemeanor laws breaches Article 8 of the European Convention on Human Rights (*Glukhin v. Russia*). The Court further emphasized that safeguards become even more crucial when live facial recognition is used. Safeguards regarding data protection and privacy are missing from the deployment of FRT in Hungary in relation to protests. The EU Charter of Fundamental Rights must be interpreted in harmony with the European Convention of Human Rights, as required by Article 52(3) of the Charter.

Freedom of Expression, Assembly, and Association – Articles 11 and 12 of the Charter

Hungary's amendments breach Article 11 of the Charter by restricting the right of people to freely express their political views and support for Pride, LGBTQIA+ rights, and other opinions and beliefs peacefully expressed during Pride or at other times when this remote biometric identification system is in operation. Any surveillance system in operation has a severe chilling effect on people participating in civic activities.

Under established ECtHR precedent, there is no doubt that Hungary's Anti-Pride Law violates Articles 10 (freedom of expression) and 11 (freedom of assembly). The ECtHR has consistently held that preventing LGBTQI+ demonstrations or other events infringes Articles 10 and 11 of the ECHR, as well as the prohibition of discrimination based on sexual orientation and gender identity in Article 14 ECHR. In *Baczkowski and others v. Poland*, the ECtHR held that the refusal by Polish authorities to authorise a march and assemblies protesting against discrimination of minority groups – which is, at its core, what Pride is – was a violation of the right of freedom of assembly and the right not to be discriminated against (paragraphs 66-73).

In the Hungarian laws, the new amendments criminalize both the organizers of the Pride march and the participants. In *Alekseyev v. Russia*, the Court found that imposing a ban on a Pride march and penalising participants for violating the ban violated Article 11 ECHR and Article 14 ECHR (paragraphs 88, 110).

The law also constitutes a violation of Article 12 of the Charter, which protects the freedoms of assembly and of association. Article 13/A of the amended Assembly Act, with a reference to Article 6/A of the Act on the Protection of Children (Act XXXI of 1997), makes it mandatory for the police to ban the organization of any assembly that "makes pornographic content available to minors, as well as content that depicts sexuality for its own sake, or promotes or displays deviation from the biological sex, gender reassignment, or homosexuality." As clearly indicated by the legislators' aim and recent experiences, this provision effectively prohibits Pride, which is a direct violation of the right to assembly. Furthermore, it is constructive to consider the connection between the exercise of this right and the existence of democracy itself, which has been recognized by the long-standing case law of the ECtHR. Recently, in *Kudrevičius and Others v. Lithuania*, the court held that "the right to freedom of assembly is a fundamental right in a democratic society and, like the right to freedom of expression, is one of the foundations of such a society. Thus, it should not be interpreted restrictively."

Discrimination – Article 21(1) of the Charter

In one of the aforementioned cases, *Baczkowski and others v. Poland*, the ECtHR held that merely refusing to sanction a public demonstration against discrimination against minority groups was a violation of Article 14 (discrimination), in conjunction with Article 11 (assembly and association), of the Convention on Human Rights. In parallel, this interpretation should extend to Article 21(1) of the Charter (non-discrimination) – and if the act of refusing to allow such a demonstration is in violation of said rights, surely Hungary's ban of such activity is also such a violation.

Proportionality and legality

According to Article 52 (1), any restriction on Charter rights must be: 1. provided for by law and respect the essence of the right, 2. pursue an objective of general interest (legitimate aim), and 3. necessary and proportionate to that aim. This has been reaffirmed in the case law of the CJEU (see, in particular, joined Cases C-293/12 and C-594/12 and Case C-362/14).

Under the case law of the ECtHR, in *Kudrevičius and Others v. Lithuania*, *Alekseyev v. Russia*, the ECtHR has held that the suppression of LGBTQI+ expression and information is not reasonably connected to any legitimate objective, even when the alleged justification is the "protection" of children.

In light of this jurisprudence, the Hungarian amendments fail to pursue a legitimate aim, as their stated objective, according to the law's reasoning, is to ensure that "only such assemblies may be held in Hungary which respect the right of children to proper physical, mental, and moral development". Our analysis is in line with the Advocate General's Opinion Case C-769/22 in which she argues that Hungary's Child Protection Act does not fulfill an acceptable, legitimate general interest which could justify its interference with fundamental rights protected by the Charter. And if that is the case, then it is unnecessary to apply subsequent steps of proportionality review as no justification is possible. (115.)

Furthermore, the legislation constitutes a manifest breach of fundamental rights and is incompatible with the core values enshrined in the EU Treaties, particularly the principle of respect for human dignity, freedom, and equality under Article 2 TEU, which sets out the fundamental values on which the European Union is founded.

Even if we assume that the legislative amendments have a legitimate aim, these provisions fail the proportionality test. Regarding law enforcement uses of remote biometric identification, the EDPB Guidelines conclude that such practices are disproportionate if police controls with FRT occur, even restricted to designated areas, capturing the general public as they pass by surveillance cameras. These systems create biometric templates from facial images and compare them to a database, treating everyone as a potential suspect, revealing sensitive personal information, and potentially influencing democratic participation by deterring individuals from attending protests.

Eva Simon
eva.simon@liberties.eu

Karolina Iwańska
Karolina@ecnl.org

Ella Jakubowska
ella.jakubowska@edri.org

Adam Remport
Remport.adam@tasz.hu