EVENT DESCRIPTION SHEET

(To be filled in and uploaded as deliverable in the Portal Grant Management System, at the due date foreseen in the system.

⚠ *Please provide one sheet per event (one event = one workpackage = one lump sum).)*

PROJECT	
Participant:	5 - ARSASAG A SZABADSAGJOGOKERT - TASZ
PIC number:	938599064
Project name and acronym:	Democratic Digital Commons—DDC

EVENT DESCRIPTION	
Event number:	7
Event name:	Budapest assembly – LGBTQI and AI Surveillance
Type:	citizens' assembly
In situ/online:	in-situ
Location:	Hungary, Budapest
Date(s):	September 2. 2026
Website(s) (if any):	https://euroalter.com/events/ddc-assembly-3-no-pride-in-surveillance/
Participants	
Female:	23
Male:	26
Non-binary:	2
Hungary	32
Spain	2
Germany	5
France	2
Netherlands	1
Slovakia	1
Poland	3
Bulgaria	1
Romania	4

Total number of participants:	51	From total number of countries:	9

Description

Provide a short description of the event and its activities.

The Budapest Citizens' Assembly, organised by TASZ within the Democratic Digital Commons (DDC) project, focused on the use of AI-based facial recognition technologies in the context of the Hungarian government's efforts under Viktor Orbán to introduce legal measures enabling AI-based surveillance to restrict Pride events and the right to assembly. The discussions examined how such measures could affect the LGBTQI+ community in particular, while also exploring the wider implications of AI-powered surveillance for other groups in society, fundamental rights and democratic freedoms. Participants considered how surveillance technologies could be used to restrict civic participation, and what safeguards would be necessary to protect citizens against misuse. Bringing together people from across Europe and beyond, the participants assisted by experts had the opportunity to shape their positions on the democratic boundaries of state surveillance.

One of the most pressing questions of our time is what justifies the use of facial recognition technologies and how we can prevent abuse. What is more, in an authoritarian regime, AI-powered facial recognition is not merely prone to abuse, but serves as a systematic weapon for total state surveillance, chilling political dissent and erasing any remaining space for civil liberties. So far, the use of technology has been assessed almost exclusively by governments, authorities, tech companies, and lawyers. Since facial recognition, surveillance, and analysis technologies can impact the exercise of fundamental rights, such as whether citizens feel safe participating in a demonstration or organizing for their interests, we wanted to hear the opinion of those being impacted – citizens.

Throughout the day, European experts gave presentations, and group work and joint discussions also took place. Participants shared their fears and also came up with possible safeguards that would limit the use of these technologies.

Where?

The event took place in Budapest, in MagNet Community House. The place provides a platform for programs, presentations, and discussions centered on community and social initiatives, sustainability, self-discovery, and culture.

When?

The assembly was held on 2nd of September 2026 from 9am until 6pm.

Who?

We recruited participants by open calls, social media campaigns, posters through the city, so the group became a very diverse one: members of the LGBTQI+ community, municipal workers, human rights professionals, citizens, students, artists, IT specialists, activists, educators, journalists, pensioners, members of civil society organizations, from different ages and backgrounds. They all had a different understanding of the topic so the discussion was not only shaped by facts and knowledge but their own personal feelings about the technologies.

The presence of the LGBTQI+ community was particularly important given the event's focus on the potential use of surveillance to restrict Pride events and freedom of assembly.

We invited three speakers to contribute with their expertise:

- Máté Szabó (HCLU Director of Programs) - Summary of AI-based facial recognition
- Pete Fussey (Professor at the University of Southampton) - How does facial recognition technology operate?
- Karolina Iwanska (Legal Officer at the European Center for Not-for-Profit Law) - European Union regulation (AI act)

In order to have everyone's voice and opinions being heard, we organized the participants into smaller groups that later reported back to the plenary discussion.

AGENDA – Budapest Assembly

8:30-9:00 Registration

9:00- 9:25 Introductions

9:25- 10:45 Presentations and table work

- Máté Szabó and Pete Fussey

after each presentation the groups collected their questions about the presentations

10:45- 11:00 Break

11:00- 13:00 Presentations, table work and Q&A

after the presentation the groups collected their questions, and then from 12-13h, the experts answered the questions plenary

13:00- 13:40 Lunch

13:40- 15:10 Deliberation

joint exploration of the topic, collection of opinions, brainstorming

15:10- 15:30 Break

15:30- 17:10 Deliberation

joint exploration of the topic, collection of opinions, brainstorming

17:10- 17:20 Break

17:20 - 17:40 Voting

17:40- 18:00 Closing

Preparation Phase

Preparation for the assembly included:

- Research on the legal status of AI surveillance in Hungary
- Pre-interviews with members of the LGBTQ+ community that were affected by Orbans attempted ban of the pride.
- A mapping of relevant european-wide stakeholders in the protection of rights against AI surveillance, including CSOs, legal groups, advocacy groups, activists, researchers, and technologists.
- A european-wide communications campaign across the identified stakeholders, plus through the channels of the consortium partners (newsletters, social media posts).

Narrative report & outcomes

The diversity of the participants resulted in a broad range of perspectives. Participants included people with professional experience in the AI surveillance industry and international diplomacy, students and people with little previous exposure to the topic, as well as human rights activists. This diversity sometimes led to strong disagreements and required active facilitation, particularly to ensure that more vocal participants did not dominate the discussions. At the same time, the discussions remained largely respectful and constructive. Facilitators observed that even when participants strongly disagreed, they were generally willing to engage with each other's arguments and reconsider their own positions.

The educational part of the assembly generated a wide range of questions concerning both the technical and societal dimensions of facial recognition. Recurring themes included the ownership and protection of biometric data, the possibility of opting out of facial recognition, the accuracy and reliability of the technology, accountability in cases of false identification, transparency around surveillance, the role of human decision-makers, and the ability of legislation and democratic institutions to keep pace with technological development. Participants also questioned what constitutes a legitimate national security interest, who is responsible for overseeing its use, and how citizens can know when and how they are being monitored.

A particularly important outcome of the educational phase was that participants did not approach facial recognition solely as a technological issue. Their questions increasingly focused on the wider social and institutional consequences of its use: who has access to the technology and the resulting data, who can be held accountable for decisions based on automated systems, what safeguards exist against abuse, and what possibilities citizens have to exercise meaningful control over their biometric data.

The deliberative part showed that participants' positions were not simply divided into support for or opposition to facial recognition. Instead, the discussions led to a more nuanced examination of possible exceptional uses and the conditions that would have to be fulfilled for such uses to be considered acceptable. Across the groups, participants were particularly cautious about the use of facial recognition for general crime prevention, indiscriminate surveillance, and broad monitoring by state authorities. They repeatedly questioned whether less intrusive alternatives could achieve the same public-safety objectives.

Several participants considered narrowly defined uses potentially acceptable, including the identification of missing persons or children, certain security procedures at airports, and specific

banking-related authentication processes. Where such uses were considered acceptable, participants emphasised strict limitations, such as the use of narrowly defined databases, data minimisation, short retention periods, meaningful alternatives or opt-out possibilities, and restrictions on the sharing of biometric data.

The groups also identified a number of safeguards that they considered important if facial recognition were to be used at all. These included independent oversight with broad supervisory powers; independent auditing of technologies, including from a human-rights perspective; judicial authorisation in specific cases; transparency regarding the effectiveness and error rates of systems; restrictions on the linking and sharing of biometric databases; limitations on private-sector use; and notification of individuals where their image has been specifically used in an investigation. Participants also discussed the evidentiary value of facial recognition and stressed that an automated match should not, on its own, be sufficient grounds for a criminal conviction.

A recurring concern throughout the day was the distribution of power between citizens, public authorities and technology companies. Participants expressed particular concern about situations in which individuals have little knowledge of whether they are being monitored, what happens to their biometric data, or how automated systems influence decisions concerning them. This contributed to a broader discussion about democratic accountability and the need for meaningful checks and balances around surveillance technologies.

Overall, the deliberative process demonstrated that participants' views evolved through discussion. Rather than simply maintaining their initial positions, participants engaged with competing arguments and explored the conditions under which different uses might or might not be justified. In several groups, the key question became whether a particular public-safety objective could be achieved through a less intrusive means. This shift from a general discussion of the technology towards concrete use cases, safeguards and alternatives was one of the main outcomes of the deliberative process.

Recommendations and Next Steps

The overall attitude of the participants towards the use of facial recognition technologies was highly critical. A majority of participants expressed strong opposition to their use and argued that facial recognition should not be used at all. At the same time, the deliberations showed that participants recognised that such technologies are already in use and that some specific use cases may be difficult to address without them. Against this background, the safeguards discussed during the deliberations can be understood as conditions intended to minimise the risks in cases where the use of facial recognition is nevertheless permitted, rather than as an endorsement of the technology itself.

The deliberations resulted in a number of recommendations concerning the conditions and safeguards that should apply to the use of facial recognition technologies.

Participants identified the following key safeguards and limitations:

- Independent oversight: An independent organisation with broad powers should continuously monitor institutions using facial recognition technologies.
- Independent audits: Technologies should be audited by independent civil society organisations, including with regard to compliance with human rights requirements and the extent of power they give to their users.
- Strictly limited use: The use of facial recognition should be restricted to clearly defined and exceptional circumstances. Participants discussed serious violent crime and the search for wanted or missing persons as possible cases where its use could be justified.
- Judicial authorisation: Where facial recognition is used in relation to a crime, participants proposed that court authorisation should be required as an additional safeguard.
- Restrictions on the use of results: A facial recognition result could be admissible as evidence, but should not be sufficient on its own to lead to a conviction.
- Transparency and notification: Authorities should make publicly available information about the effectiveness and false-positive rates of the systems they use. Participants also proposed that individuals should be notified retrospectively where their image has been specifically used in an investigation.
- Protection of biometric data: Databases containing information about individuals should not be freely linked or shared between different actors, and companies should not be allowed to trade in such data.
- Limits on private-sector use: Participants expressed strong reservations about the use of facial recognition by companies and argued that companies should have only a very limited scope to use such technologies.

- Data minimisation: Where facial recognition is permitted, participants emphasised that data should not be stored, or should only be stored for a very limited period. They also distinguished between checking an individual's identity against a specific document or database and using data from the general population.
- Less intrusive alternatives: Participants repeatedly returned to the question of whether the same objective could be achieved through a less intrusive means. In particular, they argued that facial recognition should not be used for generic crime prevention where other approaches, such as social services, education, stronger communities or improved street lighting, could be used instead.

The discussions also identified several areas for further consideration. While the role of states and public authorities received the most attention, one participant repeatedly raised the responsibility and influence of the companies developing facial recognition software and the pressure they can exert on government systems. The regulation of AI companies and the responsibilities of technology providers therefore emerged as an area that could be explored further in future discussions.

Participants also raised broader questions about how legislation can keep pace with rapidly changing technologies, how citizens can know when they are being monitored, what possibilities they have to refuse facial recognition, and what forms of training or authorisation should be required for people operating these systems. These issues can provide a basis for further discussion within the DDC project.

The outcomes of the event will provide the HCLU with an evidence-based foundation for its future advocacy efforts aimed at narrowing the currently overly broad scope of facial recognition technology use. Advocacy may be conducted in partnership with other NGOs, such as Amnesty International Hungary, the Hungarian Helsinki Committee and Háttér Society.

The citizens' assembly generated valuable insights to inform an advocacy paper that the HCLU plans to develop under a grant from the AI Collaborative.

Communication and dissemination

EU visibility

Publicity of the EU CERV programme's support was integrated across event materials, including videos, posters, the in-person presentation and online platforms.

Event page & photos/graphics:

https://www.facebook.com/events/1359845148995231

https://tasz.hu/en/who-watches-us-a-citizens-assembly-on-the-limits-of-ai-powered-surveillance/

https://drive.google.com/drive/folders/1nfD6xT4YUi_WVE2d_VIg3J7RGtGGmq4Y?usp=sharing

Media reach

https://www.instagram.com/reel/Dc1MwOxsxFq/

https://qubit.hu/2026/09/04/a-tisza-kormany-feladata-lenne-az-arcfelismero-rendszerekrol-szolo-torveny-eltorlese-de-egyelore-nem-tettek-erte-semmit

https://infostart.hu/belfold/2026/09/05/arcefelismero-ai-a-bunuldozesben-a-tasz-szerint-sok-meg-a-hiba-a-nyilvanosag-sokat-segitene#



Funded by the European Union

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	01.04.2022	Initial version (new MFF).