European Center for
Not-for-Profit Law

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

Call for input for the HRC62 thematic report on "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects"

The European Center for Not-for-Profit Law (ECNL) is pleased to share this submission to contribute to the consultative process for the HRC62 thematic report on "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects".

The exercise of the freedoms of peaceful assembly and association – whether online or offline or a combination thereof – is increasingly shaped and affected by the deployment of digital surveillance technologies, including those based on artificial intelligence.

Below, we are responding to questions addressed to civil society organisations - including social movements, activists, human right defenders and the general public – by providing the evidence we have gathered from various countries across Europe.

1. ***According to your knowledge/experience, how have relevant digital surveillance technologies impacted the exercise of association and assembly rights (online and offline) in your country/countries of work?***

Armenia:

The amended Law on Police in force from August 2025 regulates police access and use of surveillance cameras installed on public buildings, transport and parking areas. The law includes some safeguards to ensure the transparent and accountable use of surveillance systems (e.g., warning signs of equipment in use in public spaces, unless surveillance is conducted for special investigative purposes; pre-defined list of police officers having access to archives; procedure for data processing). However, it also allows municipalities to access police surveillance systems in their communities without clear legal safeguards.

Searches of the premises of CSOs or surveillance of their communications can only be carried out based on a court decision, except for urgent cases when a delay may lead to actions of terrorism or threaten state security. In such cases, the National Security Service (NSS) can carry out surveillance within a 48-hour period before a court decision is secured. However, experts and CSOs are doubtful about the legitimate use of surveillance powers by the NSS and law enforcement bodies as there

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

are no oversight and accountability mechanisms for surveillance activities, or transparent investigations of data leaks.

Given the absence of proper national regulation of artificial intelligence (AI) technologies and public oversight mechanisms, the amended law poses a risk of misuse and infringement to the rights of privacy, freedom of peaceful assembly and non-discrimination principles, guaranteed by Armenia's Constitution and its international human rights obligations. [1]

Belarus:

According to the presidential edict No. 32 of 25 January 2024, video cameras are mandatory in taxis and buses. They are also obliged to record all bookings, both online and in person. Information about bookings will be stored for five years, and law enforcement officials and government agencies will have access to it. Operatives can inspect a computer not only by being directly present on location, but also through remote access.

Measures to fight cybercrime, disinformation, hate speech/incitement to violence and terrorism are widely abused to limit digital rights. Internet use, website commenting, and mobile communication require user identification. Internet providers are obliged to provide intelligence agencies with access to information exchanged by users online. The authorities can demand provision of data about the online activities of any citizens.

Imprisonment for clicking 'like' or 'share' on specific posts on social media continues to be a common practice in 2024 (for instance, links to extremist materials, banned media logos, calls for mass actions, publications on political topics or hate against law enforcement or the ruling political regime, insult to state officials, judges or the president). Many criminal cases of conspiracies, attempted coups, planning of mass riots, acts of terrorism and so on are based on records of intercepted communications or disclosed from confiscated smartphones, as well as from meetings on Zoom or other platforms.[2]

France:

In July 2024, the French National Assembly adopted a law that establishes a digital register of foreign influence activities.[3] All individuals and organisations "acting on behalf of a foreign principal" when conducting activities that aim to influence public decision-making or the conduct of public policies are required to declare their activities and be added to this register. Failure to comply will result in penalties

[1] https://csometer.info/updates/2025-regional-insights-eap-civil-society-environment

[2] https://csometer.info/sites/default/files/2025-05/2024%20CSO%20Meter%20Belarus%20Country%20Report_0.pdf

[3] Law No. 2024-850 of 26 July 2024, https://www.legifrance.gouv.fr/download/pdf?id=z7F5NKvMxLybREePeZx4ZpzKY6oT0Ac8uyatwTORrks=

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

ranging from up to three years in prison, fines up to 45,000 euros for individuals and up to 225,000 euros for legal entities, a ban on receiving public aid, etc. In addition, the law authorises intelligence services - on an experimental basis until 30 June 2028 - to use algorithmic techniques to process online data (including communication over the internet) to gather information likely to reveal foreign interference or threats to national defence. No information is available on whether the government is already conducting this experiment, what algorithmic techniques are being used and what is flagged as "likely to reveal foreign interference". The government must also submit an interim report and a final report evaluating this extension of the algorithmic technique to the online detection of foreign interferences.

Hungary:

In March 2025, Hungary's parliament amended domestic laws to ban LGBT-related events, citing the Child Protection Act and expanded police powers to use Remote Biometric Surveillance (RBI) via facial recognition technology (FRT). FRT has been in operation since 2016 within the state's so-called Still Image Facial Recognition System under the Hungarian Institute for Forensic Sciences (HIFS) but was previously limited to detect infractions punishable by a custodial sentence, whereas now it can be deployed for all proceedings related to all sorts of infractions, including participation in prohibited assemblies. The amendments were introduced and adopted without public consultation.[4]

Georgia:

Although Georgian law provides nominal guarantees against unauthorised interference or attacks on privacy, there are significant gaps in enforcement and judicial oversight. Agencies such as the State Security Service and its Operative–Technical Agency are granted broad surveillance powers that are often executed without adequate judicial scrutiny. The approval rate for covert surveillance requests by courts exceeds 91.7%, and these approvals are rarely accompanied by public justification, raising concerns about the impartiality and transparency of the process.[5]

In December 2024, the "Georgian Dream"-led single-party Parliament significantly tightened the penalties provided for in the Administrative Offences Code for blocking roadways during protests. In October 2025, Georgia enacted new amendments to the Code on Administrative Offenses and the Criminal Code related to violations under the Law on Assemblies and Manifestations. The new package further restricts freedom of peaceful assembly by replacing previous fines with

[4] https://www.researchgate.net/publication/345438022_Still_Image_Face_Recognition_in_Hungary

[5] https://csometer.info/sites/default/files/2025-05/CSO%20Meter%202024%20Country%20Report%20Georgia%20ENG.pdf

administrative detention and introducing criminal liability for repeated administrative offenses.[6]

Moldova

In Moldova, surveillance is legally possible as part of a criminal investigation, but only upon authorisation of the investigative judge at the prosecutor's request. However, it is not clear to what extent the legal mechanisms to protect against surveillance-related abuses, illegal or disproportionate collection, processing and storage of personal information work in practice, except in cases brought to public attention by media investigations.

The Moldovan Security and Intelligence Service (SIS)'s surveillance powers extend beyond the scope of a criminal investigation and include the right to monitor a person's home, to install audio, video or photo surveillance devices in the home as well as to visually monitor and intercept communications, even without the consent of a judge. The Council of Europe's Venice Commission pointed out that the SIS is granted very extensive and undefined powers, including an apparent enforcement role, without providing clear legal remedies and without explanations concerning the legal consequences or sanctions.[7]

Public institutions use several technologies, such as FRT systems at border control, road traffic monitoring systems (including drones). There is only informal evidence regarding the integration of AI in public institutions and the availability of more advanced technologies in monitoring and surveillance. Still, there is no oversight mechanism for seeking remedies against violations of digital rights and any suspicions of violation may only be subject to traditional legal mechanisms.[8]

The Netherlands:

The draft "Online Public Order Disruption Act" is currently under consultation. If adopted, this law grant municipality mayors the power to issue a removal order to those who post online messages that "*disturb public order or that give rise to serious fears of a public order disturbance*."[9]

Concerns have also been raised in the country regarding police tactics and surveillance practices against protesters, particularly during environmental protests and protests expressing solidarity with Palestine:

1) The Royal Netherlands Marechaussee (military police) used FRT to identify participants in an "Extinction Rebellion" protest at Schiphol Airport in November 2022. Pictures taken on the spot were compared to pictures available

[6] https://matsne.gov.ge/ka/document/view/31678?publication=22

[7] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282023%29041-e, para 16

[8] Draft CSO Meter County report 2025 (not published yet).

[9] https://www.internetconsultatie.nl/oaoov/b1

through public sources (particularly social media profile pictures). In July 2023, 176 people received a letter from the Public Prosecutor that they had been identified. While they were not prosecuted, the letter warned against future participation in climate protests, saying next time the Prosecutor would press charges. Furthermore, 7 persons were wrongfully identified.[10] In response to questions asked in Parliament, the Minister of Justice said "*Given the aforementioned circumstances, not least the attitude of the demonstrators themselves, with such a large number of arrests within a short period of time – and, of course, within the limits of legal powers – a certain margin of error in the identification process must be accepted. We regret this, but unfortunately it can never be completely ruled out in such situations. This makes it all the more important for the authorities to follow up adequately when this occurs.*"[11] The National Ombudsman launched an investigation into police's home visits to protesters, warning of privacy concerns and a chilling effect on civic participation.[12]

2) In October 2024, a report published by Amnesty International denounced that Dutch police use video surveillance cars and drone from a fixed location, relying on "*broad and generic powers from Article 3 of the Dutch Police Act to decide on surveillance measures.*"[13] Responding to the report's findings, the Minister of Justice argued that he did not see a need to create an additional legal basis for the use of technical surveillance instruments and believed Article 3 of the Police Act (which is very broad and vaguely formulated) was actually sufficient. However, the Minister expressed his intention to discuss the use of surveillance cameras on the basis of this article with the police to ensure such use was done only in case there is a specific reason and for a short term. That said, the Minister added that he did not support a full ban on development and deployment of FRT for identification purposes and did not support a mandatory fundamental rights impact assessment for the introduction of digital technologies, as there are already various requirements in place (e.g., data protection impact assessment and Dutch "FRAIA").[14]

Ukraine:

The use of video surveillance systems and covert investigative tools is becoming increasingly widespread, applied not only in cases of serious crimes but also in proceedings of moderate severity. The Territorial Center for Recruitment and Social

[10] https://www.bitsoffreedom.nl/2023/09/06/monthly-update-on-human-rights-tech-august-2023/

[11] Antwoorden Kamervragen over de waarschuwingsbrieven van het Openbaar Ministerie", October 9, 2023:https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/09/antwoorden-kamervragen-over-de-waarschuwingsbrieven-van-het-openbaar-ministerie

[12] https://civicspacewatch.eu/the-netherlands-legislative-proposals-risk-stigmatising-csos-expanding-censorship-and-granting-more-powers-to-authorities/

[13] Amnesty International, "Recording Dissent: camera surveillance at peaceful protests in the Netherlands": https://www.amnesty.org/en/documents/eur35/8469/2024/en/

[14] https://open.overheid.nl/documenten/dpc-8ebdd946b7b523ae4cd87ded04a59922393c2637/pdf

Support can access personal data without a court order, including phone checks, superficial inspections and even restrictions on personal freedom.[15]

2. ***What have been the consequences of the use of digital surveillance (targeted or mass surveillance, online or offline) on the exercise of the rights to freedom of peaceful assembly and association?***

Belarus:

CSOs in the country are concerned that recordings from the cameras mandatorily installed in cars or buses will go to a certain server in the 'Kipod' video surveillance and FRT system and will potentially be misused to further crackdown on activists. Existing video surveillance systems on the streets are used to detain persons subject to movement restrictions due to political activism or to arrest activists returning from abroad who are accused of disseminating extremist information. Employment checks using these databases could lead to reprisals due to past participation in protests or independent CSOs.

Experts note that in Belarus, various databases and registers are created for all sorts of occasions: e.g., the Ministry of Internal Affairs runs a unified database of participants in unauthorised demonstrations (known as the Besporiadki database, in use since late 2020) aimed at bringing them to administrative and criminal justice. There are also unofficial lists of individuals who signed in support of the nomination of opposition candidates for president in 2020, the registry of Belarusian citizens holding foreign residence permits and database mobile billing, etc.

Furthermore, national security, border control or counter-terrorism laws authorise opaque and unaccountable government requests for data, where users have no knowledge of these requests and no right to challenge them.[16]

Georgia:

Following the legislative reforms adopted in 2024 and 2025 restricting freedom of peaceful assembly, the Patrol Police Department of the Ministry of Internal Affairs (MIA), in coordination with the "Public Safety Command Center 112" (LEPL), started massively drawing up offence reports and fine participants in protests and demonstrations on the basis of state-wide video surveillance systems.[17]

In December 2024 and January 2025, the MIA upgraded the video surveillance system in the area surrounding the Parliament building, substantially increasing the number of video cameras as well as their technical capabilities. Analysis of state

[15] Ukraine Country CSO Meter report draft 2025 (not published yet)

[16] https://csometer.info/sites/default/files/2025-05/2024%20CSO%20Meter%20Belarus%20Country%20Report_0.pdf

[17] https://idfi.ge/public/upload/0IDFI/Human%20Rights%20Crisis%20In%20Georgia%20ENG.pdf

procurements reveals that the perimeter is mainly equipped with Chinese-made (Dahua) cameras. Following the end of a demonstration, Patrol Police and/or Tbilisi Police Departments of the MIA request video records from the LEPL, without indicating any legal basis for the request, "due to official necessity".[18]

Although the use of automated FRT systems is not mentioned in any of the reports, the LEPS offence reports point to the tracking of individuals via use of biometric data. However, Article 9 of the Law of Georgia "On Personal Data Protection" does not allow the use of biometric data for the purposes of a response to administrative offenses.[19]

Despite numerous documented incidents of unlawful surveillance over the years, in 2024, state authorities still have not faced any repercussions and investigations rarely lead to prosecutions. Individuals associated with CSOs or those critical of the government are particularly vulnerable to privacy infringements, largely due to the extensive use of covert surveillance measures. [20]

Hungary:

As a result of the 2025 legislative reform, the 2025 Budapest Pride Parade was banned by the police and FRT was allowed to be used to detect participants. The presence of cameras during the unauthorised parade was indeed documented.[21] However, so far there have been no reports of individuals being identified or fined in relation to the Pride march nor with regards to the aforementioned surveillance FRT, likely because of the international attention and publicity.

There has also been no record of dissolutions of associations tied to the usage of the relevant surveillance tools. However, the EU Fundamental Rights Agency warned that the 2025 measures enabling the police to use facial image analysis around assemblies risk violating the right to freedom of assembly/association and privacy, which can violate rights to civic participation.[22]

---

[18] https://idfi.ge/en/massive-surveillance-of-protesters-and-inadequate-response-of-the-personal-data-protection-service

[19] https://idfi.ge/en/massive-surveillance-of-protesters-and-inadequate-response-of-the-personal-data-protection-service

[20] https://csometer.info/sites/default/files/2025-05/CSO%20Meter%202024%20Country%20Report%20Georgia%20ENG.pdf

[21] https://apnews.com/article/budapest-pride-march-defies-ban-orban-hungary-6919758b70c812bfe95dddb589e44132 para. 1

[22] https://www.researchgate.net/publication/345438022_Still_Image_Face_Recognition_in_Hungary

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

3. ***What has been the impact of digital surveillance on targeted activists, human rights defenders, civil society, social movements or protests considering intersectional vulnerabilities?***

Armenia:

In recent years, civil society representatives and journalists have been targeted by spyware, phishing campaigns, and DDoS attacks, aiming to steal sensitive information, disrupt operations, and exploit limited cybersecurity capacities. Hacker groups affiliated with Russia are increasingly involved in targeting Armenia's digital infrastructure. For example, in April 2025, dozens of CSOs received a spear-phishing message via Signal messenger, appearing to come from the head of the EU Delegation to Armenia and containing a malicious link disguised as a Microsoft Teams meeting link. the IP addresses were traced to a cloud provider located in Russia. Another phishing attack followed in May 2025, using a PDF attachment disguised as an official document and redirecting to malicious page. Also, several instances of the use of spyware both by government and out-of-country actors have been reported, and several civil society representatives and journalists have been targeted by two kinds of advanced spyware: Predator and Pegasus.[23]

Hungary:

The EU Fundamental Rights Agency states that the recent measures associated with surveillance in Hungary restrict civic space and risk chilling participation by targeted groups (including LGBTQ+ communities). This created a chilling effect beyond the LGBTQ+ community exclusively, with wider implications for the expression of assembly rights.[24] Another chilling effect for CSOs documented by the Hungarian-Helsinki is the potential deterrence from engagement.[25] This further undermines the ability of CSOs to operate and constrains their impact on freedom of association.

Moldova:

The number of citizens approaching the National Center for Personal Data Protection of the Republic of Moldova (CNPDCP) regarding violations related to the processing of personal data has continuously increased in recent years. In 2024, the CNPDCP received 1,160 petitions, most of which reported the processing of personal data through video/audio surveillance systems (435 cases), without the subject's consent (346 cases), through disclosure on social media (179 cases), and regarding the exercise of individuals' rights (access, information, intervention, objection) (134 cases). The CNPDCP initiated inspections in 312 cases, resulting in 173 confirmed violations, of which 143 were classified as administrative offences. In 2025, courts

[23] https://csometer.info/sites/default/files/2025-01/ENG%20Armenia%202024%20CSO%20Meter%20Country%20Report.pdf

[24] https://revdem.ceu.edu/2025/06/03/pride-hungary-orbans-culture-war-escalates-ahead-of-2026-election

[25] https://helsinki.hu/en/pride2025/

registered 7 cases concerning violations of Article 177 (Violation of Personal Life). By comparison, in 2024 there were 10 cases, in 2023 – 8 cases, and in 2022 – 3 cases.[26]

4. ***Chilling effects: how has the use of digital surveillance (targeted or indiscriminate/mass surveillance) impacted the way activists, civil society, social movements or protests continue their activities, and pursue their mission and objectives?***

Armenia:

Though the new Law on Police prohibits using personal technical means by police officers, during protests some police officers were reported to be filming the demonstrators with their mobile phones, which raises concerns about further possible unlawful processing of data and relevant accountability measures.[27]

Hungary:

The EU and UN bodies have highlighted the foreseeable chilling effects of the Hungarian law reforms on the people's right to participation, expression, peaceful assembly and privacy, especially in LGBTIQ+ assemblies considering this specific context. [28] The EU Fundamental Rights Agency also described the recent developments as possibly restricting the "operating environment" for CSOs.[29]

Civil society in Hungary exhibited preparedness and resilience despite these challenges: e.g., multiple NGOs published information to inform participants of the legal circumstances and anticipated questions about the Pride Parade.[30] The Hungarian Helsinki Committee indicated as well that a user manual would be made available in the future for anyone who was fined or faced prosecution. Budapest Pride 2025 was a historically large LGBTQ+ advocacy event: despite the police ban and the real threat of the usage of remote biometric surveillance, it was reported to have gathered at least 100,000 participants.[31] However, this is primarily due to international attention and presence of journalists and EU politicians.

---

[26] Draft CSO Meter County report 2025 (not published yet).

[27] Armenia Draft CSO Meter Country report 2025 (to be published later this year or early 2026)

[28] https://www.ohchr.org/sites/default/files/2024-03/Toolkit-law-enforcement-Component-on-Digital-Technologies.pdf page 8

[29] https://docs.un.org/en/A/HRC/44/24 page 7

[30] https://helsinki.hu/en/pride2025 para. 16

[31] https://apnews.com/article/budapest-pride-march-defies-ban-orban-hungary-6919758b70c812bfe95dddb589e44132 para. 1

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

5. ***What has been the broader impact of digital surveillance on the wider public to safely and freely exercise their rights to freedom of peaceful assembly and of association, and to engage in political and democratic debates in online and offline spaces?***

Belarus:

The government's track record of suppressing dissent suggests a significant risk that AI could be further employed to enhance state surveillance capabilities, thereby infringing on citizens' freedoms and privacy. In Belarus there is currently no space for independent CSOs to freely participate in discussions about responsible AI on an equal basis with the state. On the international stage, Belarus' isolation, exacerbated by the fallout from the 2020 election protests and later by Belarus' engagement in the war in Ukraine, limits its participation in international AI governance dialogues. Sanctions and diplomatic tensions also hinder Belarusian entities from engaging effectively in international forums. The government's tight control over the academic and research sectors, compounded by a broader suppression of dissent and independent initiatives, creates a challenging environment for independent AI researchers to freely collaborate on state-led projects. While there may be some level of engagement, especially in fields deemed strategically important by the state, such as the military, these collaborations are often closely monitored and subject to strict regulations, limiting the scope and openness.[32]

Georgia:

Georgia's current extremely restrictive and volatile environment and the practice of impunity exacerbate the already existing challenges faced by CSOs, leading to self-censorship and a diminished capacity to act as watchdogs of government activities. CSOs and protesters lack adequate protection against the illegitimate collection, processing, and storage of their data, whether conducted online or offline.[33]

Two key institutions—the Ministry of Internal Affairs (MIA) and the State Security Service (SSS)—form the backbone of this repressive machinery. Though the SSS is nominally independent from the executive, both agencies are staffed by loyalists and operate with no meaningful oversight. The SSS in particular has evolved into a sprawling surveillance and enforcement body, encompassing a mass electronic surveillance programme, supervision of the civil service—including the public education system—and the orchestration of election manipulation efforts. Specialised SSS units also monitor and exert influence over the Georgian Orthodox Church, other religious organizations, opposition political parties, and civil society groups, consolidating the regime's grip on all facets of public life to their roles in

[32] https://csometer.info/sites/default/files/2025-05/2024%20CSO%20Meter%20Belarus%20Country%20Report_0.pdf

[33] https://csometer.info/sites/default/files/2025-05/2024%20CSO%20Meter%20Regional%20Report_0_0.pdf

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

violent crackdowns marked by gross human rights violations. The MIA, through its Department of Special Tasks, has led violent crackdowns on protesters. [34]

Hungary:

The 2025 reforms have created legal uncertainty for the wider public exercise of assembly/association rights, thereby having potentially had a significant chilling effect on civic participation.[35] UN experts urged authorities to avoid using FRT to identify attendees.[36]

A panopticon effect describes how the awareness or perception of constant observation leads people to potentially self-censor and/or alter behaviour.[37] Further to the Budapest Pride 2025, the prospect of being observable and identifiable in public space can plausibly deter some possible participants from exercising assembly/association rights, consistent with this effect's predicted conceivable chilling on autonomy and expression.[38]

6. ***How has digital surveillance affected the rights of association and assembly of people belonging to groups in vulnerable and marginalised situations (such as women, children and youth, indigenous people, afro-descendant communities, LGBTQI+ persons, historically marginalised groups and minorities, etc)***

Belarus:

Covert surveillance accompanies broader crackdown practices, such as forced public outing of LGBTQ+ individuals used as a means of harassment, blackmail, inducement to cooperate with intelligence services, as well as a punishment during imprisonment.[39]

Hungary

Hungary's 2025 changes targeted assemblies linked to LGBTQ+ expression by tying the right of assembly to the 2021 "child protection" rules and empowering police to ban Pride-related events and use the Facial Image Analysis Register to fine

[34] https://www.law.nyu.edu/sites/default/files/2025-09/Georgia%20Report_EN_FINAL_SEPT%202.pdf

[35] https://algorithmwatch.org/en/pridewithpride/

[36] https://www.ohchr.org/en/press-releases/2025/03/concern-hungarys-new-anti-lgbtiq-law

[37] https://aiethicslab.rutgers.edu/e-floating-buttons/panopticon para. 1

[38] https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf page 6

[39] https://csometer.info/sites/default/files/2025-05/2024%20CSO%20Meter%20Belarus%20Country%20Report_0.pdf

participants.[40] A 2025 constitutional amendment further reinforced the framework connected to the "child protection" law. Therefore, while the permission to potentially employ FRT is not explicitly exclusive to the LGBTQ+ community, at the time it was framed and applied around Pride-related assemblies, creating disproportionate impact on LGBTQ+ peoples' ability to freely assemble. [41]

7. ***Recommendations: What specific safeguards should be put in place through the lifecycle of deployment of digital surveillance technology to prevent unlawful and arbitrary surveillance, and to mitigate chilling effects on the exercise of the rights to freedom of peaceful assembly and association (online and offline):***

States should:

1. Refrain from using – or stop using or exporting – new and emerging technologies, including AI systems, whose deployment is incompatible with international human rights law or poses undue risks to the enjoyment of human rights, unless and until the adequate safeguards to protect human rights and fundamental freedoms are in place.[42] Examples include technologies allowing indiscriminate and/or untargeted surveillance of individuals or on the basis of group affiliation, spyware or other forms of equipment interference targeting the digital devices of participants in peaceful protests.[43]

2. Publish details on which public authorities – or private bodies acting on their behalf - deploy surveillance systems, including AI-based systems; what procedures are followed to authorise surveillance, sharing, storage, and destruction of data acquired through AI systems; and key information about the use of AI systems, such as the number/type of investigations in which they were used in and the outcomes of those investigations.[44]

---

[40] https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775839/EPRS_BRI%282025%297758 39_EN.pdf

[41] https://revdem.ceu.edu/2025/06/03/pride-hungary-orbans-culture-war-escalates-ahead-of-2026-election

[42] See UN HRC/RES/58/23, para 9 (b): https://docs.un.org/en/A/HRC/RES/58/23

[43] See OHCHR, Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, Component 2: A principled-based guidance for the human-rights compliant use of digital technologies in the context of peaceful protests: https://www.ohchr.org/sites/default/files/2024-03/Toolkit-law-enforcement-Component-on-Digital-Technologies.pdf

[44] See ECNL, Taking Action Against Biometric Surveillance Civil society tactics and strategies https://ecnl.org/sites/default/files/2024-11/ECNL%20Biometrics%20Surveillance%20Strategies%202024_v%2030.09.24_0.pdf

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

3. Adopt AI governance frameworks that are not shaped solely by commercial priorities but are firmly rooted in human rights law and developed responsibly through inclusive, meaningful multistakeholder processes. Special attention must be paid to specific rights of individuals and communities who are most at risk of AI-related harms, including women, children, LGBTQIA+ persons, persons belonging to national, ethic, religious and linguistic minorities as well as persons with disabilities. [45]

4. Require AI developers and deployers to carry out human rights due diligence and impact assessments across the full lifecycle of AI systems, including risk identification, stakeholder consultation, mitigation planning, and ongoing monitoring.[46]

5. Require that private surveillance companies disclose products and services offered and sold, which clients are involved and when products are developed for national security and/or counter-terrorism purposes.[47]

6. Ensure that biometric identification and recognition technologies, including FRT, are used only when consistent with international human rights law and the principles of legality, necessity and proportionality.[48] In particular:
   a. ensure that restrictions to fundamental rights – including freedom of peaceful assembly – are narrowly defined by law,strictly necessary and proportionate;
   b. ensure that are not such technologies are *not* used by public and private actors for mass surveillance;
   c. avoid sweeping exemptions for law enforcement, criminal investigation, border control, counter-terrorism, and national security;
   d. ban the use of FRT to identify those peacefully participating in a protest or other assemblies;[49]

---

[45] See Freedom Online Coalition (FOC) Joint Statement on Artificial Intelligence and Human Rights (2025): https://freedomonlinecoalition.com/joint-statement-on-ai-and-human-rights-2025/

[46] See Freedom Online Coalition (FOC) Joint Statement on Artificial Intelligence and Human Rights (2025): https://freedomonlinecoalition.com/joint-statement-on-ai-and-human-rights-2025/

[47] See ECNL, Taking Action Against Biometric Surveillance Civil society tactics and strategies https://ecnl.org/sites/default/files/2024-11/ECNL%20Biometrics%20Surveillance%20Strategies%202024_v%2030.09.24_0.pdf

[48] UN HRC/RES/58/23, para 9 (n): https://docs.un.org/en/A/HRC/RES/58/23

[49] See Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, A/HRC/44/24, para 53 (h): https://docs.un.org/en/A/HRC/44/24

info@ecnl.org
0031 639029805
www.ecnl.org
Linkedin | Bluesky | Mastodon

e. restrict government authorities from expanding surveillance beyond its initial scope, capabilities, and purposes and from sharing biometric data between agencies;

f. prohibit government agencies, especially law enforcement agencies, from using and accessing data and information derived from use of these technologies by private companies and other private actors.[50]

7. Ensure effective access to remedies for human rights violations and abuses arising from biometric identification and recognition technologies.[51]

Private actors (technology/AI providers) should:

8. Incorporate transparency and human rights-by-design principles into tech/AI design and governance models in order to identify, mitigate and prevent adverse human rights impacts linked to their activities.

9. Conduct human rights due diligence across the full lifecycle of AI systems (design, development, promotion, deployment, sale, licensing, and use) – including by assessing the human right impacts that their products may have – with the meaningful engagement of affected groups and publish the results of their human rights impact assessments.[52]

10. Adopt and implement export controls and moratoriums on sales to law enforcement with poor human rights records.[53]

Tech/AI standards development organisations should:

11. Collaborate with human rights experts and civil society expertise to promote the development and adoption of interoperable AI standards that uphold human rights.

---

[50] See Ban biometric surveillance: Statement (English version). https:// www.accessnow.org/wp-content/uploads/2022/08/BanBS-Statement-English.pdf

[51] UN HRC/RES/58/23, para 9 (n): https://docs.un.org/en/A/HRC/RES/58/23

[52]See ECNL, Taking Action Against Biometric Surveillance Civil society tactics and strategies https://ecnl.org/sites/default/files/2024-11/ECNL%20Biometrics%20Surveillance%20Strategies%202024_v%2030.09.24_0.pdf

[53]See ECNL, Taking Action Against Biometric Surveillance Civil society tactics and strategies https://ecnl.org/sites/default/files/2024-11/ECNL%20Biometrics%20Surveillance%20Strategies%202024_v%2030.09.24_0.pdf