cdt EUROPE

CDT Facial recognition briefing Paper
February 2023

The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act

In April 2021, the European Commission unveiled its proposal for an Artificial Intelligence Act, which lays down harmonised rules on artificial intelligence that aim to ensure that Europeans can benefit from new technologies that are in compliance with fundamental rights. CDT Europe welcomed that step taken to protect society against risks related to the use of AI systems but also raised concerns about the lack of a rights-based approach in the draft Regulation, and the broad derogations to the prohibition on the use of remote biometric surveillance in publicly accessible spaces by law enforcement, which include untargeted facial recognition systems.

The EU AI Act, currently being negotiated in the European Parliament and the Council of the European Union, classifies uses of AI systems on a scale going from limited to high-risk, and prohibits the most dangerous applications. In doing so, the draft Regulation differentiates between remote real-time biometric identification techniques, such as voice recognition, retina and fingerprint scanning, and facial recognition systems, and *ex post* use of these techniques. Under the proposal, remote real-time use in publicly accessible places is prohibited, with, so many exceptions that they effectively swallow the rule. CDT previously explained that law enforcement's use of facial recognition AI systems can pose a particularly high threat to human rights, given the risks of the improper deprivations of liberty that may result from such use, including racial profiling and indiscriminate surveillance . These risks are particularly acute when facial recognition is used in an untargeted manner—scanning a crowd looking for faces that match those in a database—as opposed to a targeted scan, such as where the face of a select individual is run through facial recognition in order to identify that person by matching them to a face in the database. As a result, CDT has generally called for a ban on law enforcement use of untargeted facial recognition and for moratoriums on law enforcement use of targeted use of facial recognition systems, until robust safeguards and effective limitations are in place.

This briefing paper aims to analyse how the EU AI Act addresses risks raised by the use of facial recognition systems by law enforcement and immigration authorities.

Untargeted and Targeted Scanning for Facial Recognition: State of Play in the EU AI Act

Under the EU AI Act, the prohibition of 'real time' remote biometric identification (RBI) systems in 'publicly accessible spaces' for the purpose of law enforcement (Article 5), contains very broad exemptions, such as the search of specific potential victims of crime or the prevention of terrorism attacks. The proposal, moreover, does not prohibit the use, by law enforcement, of facial recognition systems in 'real time' in places that are private in nature such as homes and offices, nor of '*ex post*' facial recognition.

The distinction between real-time and *ex post* use of the technology is arbitrary. Law enforcement could simply stock-pile images of faces obtained through untargeted scanning and seek to identify any individuals in their databases after the images have been recorded. Such use would undermine human rights just as much as real-time scanning: in both cases, for example, law enforcement could seek to identify attendees at a public political protest absent any suspicion or evidence that the protestors had broken any laws. The distinction between public and private spaces also seems to be ambiguous and again provides no valid basis to differentiate when rights are violated. The EU AI Act should rather focus on the concrete human rights risks associated with facial recognition technologies in the context in which they are used and the manner in which they are deployed.

EU law prohibits mass surveillance; to be deemed lawful, any use of facial recognition technology needs to demonstrate that it was subject to robust safeguards and procedures that do not go beyond what is necessary to achieve a given objective. In this regard, a distinction must be made between untargeted and targeted uses of facial recognition systems. Untargeted scanning seeks to run a check on all faces that appear within a video feed and identify any individuals that match a watchlist, database, or some other collection of facial images. These may occur in real-time to support immediate identification of individuals designated as alleged security threats, but could also occur *ex post,* such as by scanning and seeking to identify all individuals passing by a security camera on a previous day. Targeted scanning aims to identify a single, discrete individual in an image. The defining feature of targeted scans is that they attempt to identify a specific person by matching that person's face to a face in a permitted database, rather than scanning all the faces in a crowd in order to find matches in the database. Targeted scanning could involve identifying an official suspect when there are strong reasons that they have committed a crime or pose a high security threat. However, absent strong limits, targeted scanning could also be used in a nefarious manner, such as to target and identify an individual leading a protest. Conducting a targeted facial recognition scan in real-time is not technically possible because it involves a human making the decision to identify a select person, and inputting their image into a facial recognition system. However, it is possible to conduct targeted facial recognition in a near real-time manner: this is the case when a law enforcement officer in the field takes a photo of a suspected person, and shares it, which allows them to conduct a facial recognition scan almost concurrently.

The use of untargeted scanning by law enforcement carries an unacceptably high risk to human rights and should therefore be prohibited within the AI Act. Such use of AI tech would lead to draconian surveillance, such as effortlessly stockpiling the identities of everyone at a protest, cataloguing each person that attends service at a mosque, or scanning for undocumented individuals outside hospitals and schools. However, targeted scanning also carries human rights risks which should be accounted for in the AI Act and which could be mitigated by the adoption of strong legal safeguards, in particular in a law enforcement and migration context.

The European Commission's proposal is not clear on whether or not the prohibition on real time RBI systems in publicly accessible spaces differentiates between untargeted and targeted use of facial recognition AI systems. However, the General Approach agreed on 6 December 2022 by EU Member States would tend to confirm that the prohibition in the Regulation is on untargeted use of such systems; paragraph 8 of the Recital defines remote biometric identification systems as "*typically used to perceive (scan) multiple persons or their behaviour simultaneously in order to significantly facilitate the identification of a number of persons without their active involvement. Such a definition excludes verification/authentication systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises*."

It is crucial that such distinction between targeted and untargeted use of biometric identification AI systems is clearly stated in the EU AI Act. As risks associated with each of these uses differs depending on the context, we need such clarity to ensure forcibility of legal provisions in the Act. The law should clearly state this distinction so that the human rights risks can be appropriately mitigated. For this to work in practice of course, it will be vital that the General Approach by the Council does not dilute the prohibition of untargeted use of facial recognition to a point that it becomes the exception.

Member States' Positions on the EU AI Act

Given the previously outlined high risks to human rights protection, it should follow that law enforcement's untargeted uses of facial recognition should be categorised as 'unacceptable risks'. Unfortunately, despite clarifying that untargeted use is prohibited, EU Member States have chosen to extend when untargeted biometric identification AI systems can be used by law enforcement and migration authorities. They agreed on 6 December 2022 in their General Approach, which outlines their mandate for negotiating the text with the European Parliament, to:

1. Massively expand the cases in which real-time remote untargeted biometric identification AI technologies, including facial recognition technologies, could be used by law enforcement authorities (art. 5 (1)(d)) by adding further exceptions to the banning of real-time remote facial recognition for law enforcement uses:
    a. The European Commission had initially already proposed exceptions to the prohibition in the case of missing victims of crimes, the prevention of terrorist attacks and for a defined list of crimes. The European Council concluded that those exceptions were not enough and proposed to allow the use of such systems in order to prevent not only terrorist attacks, but also a broad range of other situations such as threats to critical infrastructure, life, or the health or physical safety of natural persons.
    b. EU Member States seek to authorise the use of real time remote untargeted facial recognition systems to investigate and prosecute all offences carrying a sentence of at least 5 years in EU Member States. This broad extension of the authorised use of these systems has not only the potential to create disparities between EU countries with different criminal laws but also to open the door to more widespread use of these systems.

2. Seek to explicitly exclude border control areas from their new definition of 'publicly accessible spaces' in Recital 9, which in turn amounts to authorising the use of remote biometric surveillance tools such as facial recognition systems in these areas.
3. Introduce many new exemptions on obligations for law enforcement, border control, immigration and asylum authorities uses of high-risk AI systems, such as a complete waiver to the registering of their high-risk AI systems in the public EU database before placing them on the market or putting them into service (Article 51).

Such proposals would preclude some of the very most at-risk and vulnerable groups from the protections that the AI Act should offer and would allow for broad untargeted use of facial recognition AI systems throughout the EU.

Why does Law Enforcement & Immigration Authorities Use of Facial Recognition Technology Pose A Particular Threat?

The use of facial recognition by law enforcement and immigration authorities poses a particular threat to human rights because it can result in unjustified deprivations of liberty. The risk of racial profiling and the lack of accuracy in facial recognition applications amplifies this risk.

A 2021 EU Fundamental Rights Agency's study on racial profiling found that, in some EU countries, police stopped almost 50% of people from certain minorities, most often men, young people, ethnic minorities, Muslims or people who do not identify as heterosexual. In 2017, the use of facial recognition at the Notting Hill Carnival by the UK Police led to the mistaken arrest of an individual attending the event and also threw up many false positives. This echoes other studies where it has been found that some algorithms are 100 times more likely to misidentify Asian and Black individuals than white men. And even if algorithmic bias issues in facial recognition are addressed, surveillance technologies will perpetuate existing disparities in policing. There is therefore a real risk that the use of AI technologies can deeply exacerbate this existing problem of racial profiling and over-policing of historically and currently marginalised groups.

Amplifying this concern are questions of system settings and procedures for use. There is no standard on this across the EU, and no transparency regarding how much law enforcement relies on matches, whether human review is required before adverse actions are taken, and how much ability suspects or defendants would have to review such systems. People arriving at Europe's borders are often fleeing conflict, poverty or persecution. The migratory route to Europe is one of the deadliest in the world, which gives an insight to what difficult a situation people are in before putting their families in a boat to risk the journey. Depending on where they arrive, people are at risk of detention and violence at the borders. They are also already at a high risk for racism, xenophobia and discrimination. In understanding the way in which AI facial recognition will play a role in the human rights risk, we cannot ignore the political context of migration which increases the risks to the individual concerned more generally.

Privacy rights are an essential gateway to many other human rights for irregular migrants. EU member states have, for instance, a general duty under international human rights law to ensure the right to health, without any discrimination based on nationality or residence status. However, they can often be denied access to, or be too afraid to access, essential healthcare services simply based on their migratory status. Only some EU member states put this into practice, in others it would be all too easy for databases linked to facial recognition to become weaponised in denying access to essential healthcare and other services to irregular migrants.

What Prohibitions & Safeguards Would Be Necessary to Bring the AI Act Back in Line with Human Rights Standards?

As previously outlined, at this point in the negotiations, the EU AI Act does not provide a framework which offers sufficiently robust safeguards and effective limitations on the use of facial recognition technology. As CDT and its civil society partners have been clear about, untargeted face recognition is the most frightening use of this technology. Yet, under the Regulation, court or administrative authorities *could* authorise these uses in real-time if it is 'necessary and proportionate' in the situation. More worryingly, as it stands, the Regulation allows for the use of untargeted scanning without a judge or administration order "in duly justified situation of urgency" (art. 5 (3)) and doesn't specify nor define what those situations of urgency would be. This is not sufficient; untargeted face recognition in public spaces needs to be outrightly banned by the AI Act, without the broad exemptions contained for law enforcement.

The EU AI Act is silent on the use of non-remote biometric identification such as targeted facial recognition systems by law enforcement, but the text seems to imply that these systems would be classified as high-risk. The AI Act authorises the use of high-risk AI systems only if they comply with certain obligations: they need to undergo a self assessment or, in the case of biometric identification and categorisation of natural persons, a third party conformity assessment by a 'notified body'[1], to enter the EU market, and later comply with a risk management system and transparency obligations. These requirements mainly rest on providers (developers) of AI systems, with very minimal obligations placed on users (deployers) of high-risk AI systems, and few-to-no meaningful fundamental rights assessment measures. It is doubtful that these safeguards will be sufficient to counter risks related to uses of facial recognition by law enforcement authorities that are not prohibited by the Regulation. The third party assessment, in particular, will be developed on the basis of new industry standards that the Commission has mandated the CEN and CENELEC to develop, and access to standard setting fora is known to be difficult for public interest and human rights voices.

However, strong safeguards are needed to counter human rights risks raised by the use of targeted scanning. In particular, it **should be subject to a court authorisation prior to use** - this is a critical protection against untargeted use, massive surveillance and from law enforcement using these systems to stockpile identities of individuals going to protests, spaces of worship, hospitals, etc.

In addition, when assessing whether or not the use of targeted scanning is necessary and proportionate in the situation, the judge should fully respect the right to the presumption of innocence and, before authorising this use, **assess whether law enforcement authorities have shown good reasons to believe** that the person has committed a serious crime listed in

[1] The authority, designated in each EU Member State, responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring under the AI Act.

the Regulation. Unfortunately however, neither the proposed Regulation nor the European Council General Approach require a judge or administration to ensure the police provide evidence that the technology will be used to identify someone suspected of a crime. The link between the potential threat or crime to be prevented or investigated and the person must be established if we want to protect the presumption of innocence, as established in international human rights law and article 48 of the EU Charter of Fundamental Rights.

Identification via these AI systems **should never be the sole basis for arrest.** All of the above mentioned safeguards should clearly be stated in the Regulation to ensure that the use of targeted biometric identification AI technologies is governed by a strong fundamental rights framework.

The Regulation should also require that suspects and accused are **informed about the use of targeted biometric identification AI systems** in the investigation against them. This positive provision should go further and also include access to all information about what type of algorithm was used, what system settings were, what reference photo was scanned, what (if any) alterations were made to the reference photo, what other matches were returned by the system and whether they were investigated. The use of these systems should in any case appear along with any other evidence brought by the Prosecution and the police, communicated to the Defence, to allow challenges to the legal use of the AI system that affected the defendant.

The obligations imposed on providers and users of high-risk AI systems described previously do not contain these obligations. Therefore, in addition to banning real-time remote biometric identification such as untargeted facial recognition systems and ensuring the exceptions for law enforcement are removed, we must conclude that at present, and especially in view of the Council's General Approach which considerably extends the situations under which law enforcement and immigration authorities can use facial recognition, the EU AI Act does not provide any of the safeguards necessary to ensure that the proposal protects against human rights violations.

Recommendations

- **The EU AI Act should define 'remote' to clarify that the prohibition on remote biometric identification applies to AI systems that conduct generalised scanning such as untargeted facial recognition systems. The use of targeted scanning systems by law enforcement authorities should comply with the Rule of Law, existing EU legislation such as GDPR, and criminal procedural requirements as outlined above. Requirements for high-risk systems need to be strengthened and aligned with these standards.**

- **Recent proposals from EU Member States to extend the list of exceptions to the prohibition on law enforcement uses of real-time remote biometric identification such as untargeted facial recognition scanning must be strongly opposed by members of the European Parliament, who currently have an opportunity to support amendments deleting these exceptions in Article 5 of the Regulation.**

Without this push back, law enforcement uses of facial recognition AI systems will effectively become the rule and not the exception in the EU. MEPs should also strongly advocate for a ban on untargeted uses of real-time remote biometric identification in publicly accessible spaces.

- **Members of the European Parliament should go to the negotiating table with EU Member States with the strongest mandate to protect human rights, in particular of those of the vulnerable and at-risk groups such as migrants, asylum-seekers and refugees by rejecting all proposed derogations in the Act that would impact such groups, such as derogations for EU border surveillance technologies and databases.**