ALLAI.

#Biometric Recognition

31.03.2023

AIA topics

Biometric Recognition

3-pager

This policy brief is the second in a series of short analyses of important, decisive or divisive topics in the legislative process regarding the European Commission proposal for a Regulation for Artificial Intelligence (AIA).

Author:
Catelijne Muller, LL.M

QUICK ANALYSIS

What is the issue?

Biometric recognition, especially the question of to what extent it should be prohibited or allowed has become contentious issue in the ongoing legislative process of the European Artificial Intelligence Act (AIA). The initial proposal of the European Commission contains a rather limited prohibition and multiple MEPs including the EP co-rapporteurs call for expanding the prohibition. Below we give a taxonomy of the various forms of biometric recognition, explain what the proposal actually prohibits and what remains allowed, address a number of contentious elements in the lawmaking process and propose a compromise approach.

The many faces of biometric recognition: a taxonomy

As the AIA appears to be only prohibiting AI-driven biometric recognition aimed at *identifying* a person, which is just one element of biometric *recognition* technologies. It is worthwhile to dive deeper into the various AI-driven biometric techniques and purposes that exist, that go beyond mere identification. Already in 2012 the Article 29 Working Party comprehensively described the different biometric techniques as follows:

- Physical and physiological-based techniques such as fingerprint verification, finger image analysis, iris recognition, retina analysis, face(-expression) recognition, ear shape recognition, body odor detection, voice recognition, heart rate detection, temperature detection, DNA pattern analysis and sweat pore analysis, etc.
- Behavioral-based techniques, which measure the behavior of a person and include hand-written signature verification, keystroke analysis, gait analysis, way of walking or moving, patterns indicating some subconscious thinking like telling a lie, etc.
- Psychological-based techniques that include measuring of response to concrete situations or specific tests to conform to a psychological profile.

The use of these biometric techniques can serve multiple purposes:

1. **Biometric verification/authentication**: the verification of an individual's identity by comparing biometric data of that individual against existing biometric data of that same individual (one-to-one matching)
2. **Biometric identification**: the verification of an individual's identity by comparing biometric data of that individual to a number of biometric templates stored in a database (one-to-many matching)
3. **Biometric categorisation/segregation**: a process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic In this case, it is not important to identify or verify the individual but to assign them automatically to a certain category. For instance an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.
4. **Biometric assessment**: a process of supposedly assessing a person's personal traits, characteristics, behavior, intentions, by assessing their biometric data (often also described as 'emotion recognition' or 'affect recognition'. Also in this case it is not important to identify or verify the individual, but to assign them a specific trait, emotion or intention.

What does the AIA proposal prohibit and what remains allowed?

The AIA prohibits (with exceptions) biometric *identification*, used *for the purpose of law enforcement*, but only if it takes place *in real time*, *remotely* and *in a public space.* Looking at all conditions combined, only a very narrow set of biometric recognition practices for an even narrower group of actors would effectively be banned under the AIA. In fact most biometric recognition practices remain allowed.

What remains allowed in law enforcement:
- Biometric verification/authentication (one-to-one) that takes place via post processing, at close proximity or in a private space
- Biometric identification (one-to-many) that takes place via post processing, at close proximity or in a private space
- Biometric categorization/segregation (no ID necessary)
- Biometric assessment (no ID necessary)

In domains other than law enforcement:
- Biometric authentication
- Biometric identification
- Biometric categorisation/segregation
- Biometric assessment

Impact

Biometric recognition in all its shapes and forms, has a broad and deep impact on our fundamental rights and society as a whole. For starters on the fundamental right to privacy. Privacy discussions around AI currently tend to focus primarily on data privacy and the indiscriminate processing of personal (and non-personal) data, but the impact of biometric recognition on our privacy goes well beyond our data. Biometric recognition creates a situation where we are (constantly) being watched, followed, categorized, assessed or identified. This creates a continuous impact on our (general) privacy and our physical, psychological and moral integrity.

Other fundamental rights can become vulnerable too, such as the freedom of opinion and expression. When the protection of ‘group anonymity’ no longer exists, if everyone in the group could potentially be recognised, this could lead to people no longer freely express themselves or partake in legitimate and peaceful demonstrations.

Moreover, if biometric recognition is only prohibited for public actors (or organizations acting on their behalf) such as law enforcement agencies, this is likely to result in a further concentration of technological expertise, data and power in the hands of the private sector, strengthening their already quite dominant position in our democratic space.

Emotion recognition

Biometric recognition of our micro-expressions, gate, (tone of) voice, heart rate, temperature, etc. is often presented as supposedly being able to determine or predict a person’s character, personality traits, mental state, emotions, behavior, intentions, criminality, intelligence, and even leadership skills, future job performance and so on. These AI practices are commonly known under multiple definitions such as ‘emotion recognition’, ’affect recognition’ and more specifically, ‘deception recognition’, 'behavior analysis' or 'sentiment analysis'. In our taxonomy we categorize them as 'biometric assessment'.

Article 3 (34) AIA defines ‘emotion recognition systems’ as “AI systems that can identify or infer emotions or intentions” and categorizes these systems generally as medium-risk, with the exception of a few areas where they are categorized as high-risk. At this point the European Parliament is finalizing its position on the AIA, including on the topic of emotion recognition and we have heard that several groups in the EP want to prohibit it.

It should be noted up frond that no sound scientific evidence exists corroborating that a person's inner emotions or mental state can be accurately 'read' from a person's face, gate, heart rate, tone of voice or temperature, let alone that future behavior could be predicted by it. In a recent meta-study, a group of scientists concluded that AI-driven emotion recognition could, at the most, recognise how a person subjectively interprets a certain biometric feature of another person[4]. An interpretation does not align with how that person actually feels, and AI is just labelling that interpretation which is highly dependent on context and culture. Far-fetched statements, that AI could for example determine whether someone will be successful in a job based on micro-expressions or tone of voice, are simply without scientific basis. As many others have already argued, broad beneficial use for these kind of systems, is lacking.

Moreover, its intrusiveness and broad impact on multiple fundamental rights merits a prohibition. For exceptional circumstances where the technology could have a scientifically sound benefit, carve outs could be created.

An alternative regulatory approach to biometric recognition

Instead of banning only a narrow set of biometric identification practices and categorizing all others high and medium-risk, we echo the various calls (e.g. by EDPS, EDPR, EESC, IBM, and a majority of MEPs) for a ban on biometric recognition, with carve outs for exceptional uses.

Biometric verification or authentication, i.e. the verification of an individual’s identity by comparing biometric data of that individual against existing biometric data of that same individual (one-to-one matching), could remain allowed. Think of the opening of a device or the door of a lab by using a biometric identifier. Also here, however, it remains crucial to make sure that these uses do not allow for circumvention or create loopholes.

We refer to our paper AIA in-depth #2 | Prohibited AI Practices for text proposals to effectuate the above.

ABOUT ALLAI

ALLAI is an independent organisation that aims to foster, promote and achieve the responsible development, deployment and use of AI.

ALLAI's mission is to take a holistic approach to AI, taking into account all impact domains such as economics, ethics, privacy, laws, safety, labour, education, etc. ALLAI aims to involve all stakeholders in its mission: policy-makers, industry, social partners, consumers, NGOs, educational and care instructions, academics from various disciplines.

ALLAI was founded by the three Dutch members of the High Level Expert Group on AI, Catelijne Muller, LLM, Prof. Virginia Dignum and Associate Prof. Aimee van Wynsberghe. Collectively, the founders have a broad expertise in AI: AI sciences, social impact, national and international policy, legal implications, and ethical impact.

CONTACT

✉ ALLAI
Amsterdam Science Park
LAB42
The Netherlands

www.allai.nl
@ALLAI_EU
welkom@allai.nl

©2023