BRIEFING

Requested by the JURI AND PETI committees

European Parliament

Biometric Recognition and Behavioural Detection

Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces

Background

Biometric identification together with biometric categorisation, behavioural detection, emotion recognition, brain-computer-interfaces (BCIs), and similar techniques are being used to an increasing extent by public and private bodies. They serve a broad variety of purposes, ranging from healthcare to law enforcement and border control to warfare, and are deployed in public as well as in private spaces.

The term 'biometric techniques' should be understood as including any technology or operation that

- relies on specific technical processing of data relating to physical, physiological or behavioural aspects of the human body (including when in motion);
- for purposes such as authentication or identification of human individuals, categorisation of human individuals according to permanent or long-term characteristics (including with a view to predicting future behaviour), or detection of temporary or permanent conditions of a human individual (such as fear, fatigue, or illness, or a particular intent).

Beyond traditional biometric techniques such as fingerprint or facial recognition, biometric techniques clearly include, e.g., analysis of keystroke or mouse dynamics, gesture dynamics, signature dynamics, as well as voice and gait features. By way of contrast, the term is normally not understood as including behaviour that can be controlled by the human will to a higher extent, such as shopping behaviour, browsing history or the content of communication. As far as such behaviour is analysed to infer conditions of a genetic, physical, physiological, behavioural, psychological or emotional nature characterising a particular individual, it may, however, be justified to include them in the notion of biometric techniques in a broader sense.

Major trends are the increasing use of 'weak' and 'soft' biometrics alongside 'strong' biometrics, focussing on a variety of patterns of a more behavioural kind, and the development towards multimodal biometrics. Together with enhanced sensor and computing capabilities as well as enhanced connectivity, this paves the way for mass roll-out of biometric technologies in a broad variety of sectors and for a broad variety of purposes, far beyond law enforcement and border control, turning biometric technologies into something like universal technologies.

Policy Department for Citizens' Rights and Constitutional Affairs
External authors: Christiane WENDEHORST, Yannic DULLER
Directorate-General for Internal Policies
PE 697.131 - September 2021

EN

Latest technological advances include improved sensors, enabling the capture of entirely new types of bio-signals, such as heart beats and brain waves via EEG or ECG, and the development of brain-computing-interfaces (BCI). BCIs measure neuro activity and translate brain activity into machine-readable input. These new technologies are potentially highly intrusive, allowing for the detection of thoughts or intent and possibly also for influencing operations of the human brain.

The Proposal for an Artificial Intelligence Act (AIA) of 21 April 2021 addresses such techniques in various ways, as do other instruments, both existing and in the pipeline. However, the question arises whether existing and proposed legislation adequately addresses ethical and fundamental rights issues raised.

Key findings

Biometric identification of humans

The main ethical issue raised specifically by biometric identification is related to the enrolment phase, i.e. the creation and storage of a unique template that identifies a particular person. The enrolment phase and the deployment phase may overlap where templates are refined during deployment, e.g. through supervised learning in the field. Creating unique templates means transforming unique physical features of a human being into digital data, leading to a 'datafication' of humans. Since the features that uniquely identify a person are part of a person's body, their collection and use interfere with a human's personal autonomy and dignity. Once this template is created and stored, anyone who comes into possession of it in the future has the power to trace and recognise that individual anywhere in the world and potentially for any purpose. There is no way for the individual to escape it as an individual cannot normally change 'strong' biometric identifiers. Considering also data security concerns, collecting and storing biometric templates has a significant potential for harm.

Apart from this, ethical issues raised by the use of biometric identification methods in public spaces do not so much relate specifically to biometrics, but to large-scale surveillance of individuals as such (i.e., they are similar to issues raised by, for example, large-scale surveillance using mobile device signals), or otherwise to the purposes for which the technology is used, and how it is used. The dimension of ethical issues raised depends, in particular, on

- the concrete purpose of identification;
- the place, manner or dimension of identification;
- the transparency of the identification measures taking place;
- the reactions (e.g. arrest) triggered by a high matching score;
- the evidentiary force ascribed to a high matching score and possibilities of the individual to demonstrate error or identity fraud; and
- any storage and further processing of matching data (e.g. for the creation of mobility profiles).

Issues of discrimination or stigmatisation arise mostly as a result of deficiencies in one or several of the aspects mentioned (e.g. where, despite diminished accuracy of the system with particular ethnic groups, unjustified assumptions are made).

Biometric categorisation of humans

The main ethical issues raised by the biometric categorisation of human individuals (e.g. allocation to risk groups within an airport security system, assessment of job applicants) are related to the development and concrete use of categorisation systems. In particular, ethical issues arise in relation to the definition of categories, the associated assumptions and the conclusions or reactions triggered by the system, leading to risks such as discrimination, stigmatisation, and the drawing of inappropriate inferences. Further risks include manipulation and exploitation of group-specific vulnerabilities. Ethical issues may be related to, in particular,

- the concrete purpose, context and conditions of categorisation;
- the degree of sensitivity of data collected and of inferences drawn;
- the accuracy of the system, the appropriateness of inferences drawn, and any control mechanisms, including human oversight;
- the gravity (including potential irreversibility) of consequences triggered by the system;
- the awareness of the individual of the categorisation and the possibility of the individual to challenge the output; and
- any storage and further processing of data for profiling purposes.

It follows that the fundamental rights risks to be addressed in this context are primarily associated with standardised profiling and/or scoring as a means to achieve a given end in a given social context. The fact that categorisation includes biometrics (e.g. that a person's age is inferred from wrinkles in their face rather than from their shopping history) adds some ethical relevance, as an individual cannot easily change most biometric traits (e.g. wrinkles), but it is hardly ever the decisive factor (as compared, e.g., with age-specific targeting that might follow categorisation). Biometric inferences, i.e. inferences drawn with regard to permanent or long-term physical, physiological or behavioural characteristics, may in general be ethically even more relevant than the use of biometric techniques as such.

Biometric detection of human conditions

The main ethical issues raised by the biometric detection of human conditions (e.g. intention to commit a crime, fear, fatigue or illness) follow from its potentially intrusive nature, often analysing very intimate traits, some of them beyond the individual's consciousness. In addition, previously unknown conditions, when revealed to the individual, may cause stress or anxiety.

Most ethical issues raised by the use of biometric detection do not relate specifically to the fact that biometric data are used for inferring a condition, but to detection of that condition as such (i.e., they are largely identical to issues raised by, for example, detection on the basis of a shopping or browsing history), and to the way the information about this condition is used (e.g. for manipulation and exploitation of detected vulnerabilities). Again, the fact that an individual has little control over their physical, physiological or behavioural signals, many of which will be subconscious, may give their use to detect conditions a special ethical dimension.

Fundamental rights risks posed by biometric detection techniques are very similar to those posed by biometric categorisation. However, within the field of biometric detection systems, it is systems detecting human emotions, thoughts and intentions that deserve particular attention from an ethical and regulatory

perspective, potentially calling for a new set of 'neuro-rights' (such as the right to mental privacy and mental integrity).

Key recommendations

The recent Proposal for an AIA goes in the right direction but still fails to address ethical concerns in a consistent manner, in particular due to various restrictions in the scope of provisions. The study proposes to include in the Proposal a new Title IIa that is devoted to restricted AI practices, including biometric techniques and inferences, ensuring responsible use of these techniques without stifling innovation and growth.

The Study suggests that, in particular, the amendments to the Proposal as listed below should be considered by the European Parliament.

The definitions in Article 3 should be amended:

- The definitions of 'emotion recognition system' and 'biometric categorisation system' should be detached from the concept of 'biometric data' as defined in the GDPR and rather based on a new definition of 'biometrics-based data';
- The definitions of 'remote' and 'real-time' with regard to biometric identification should be slightly modified.
- An additional definition for 'biometric inferences' should be introduced;

Title II on prohibited AI practices should be amended:

- The current Article 5(1)(d) and (2) to (4) on real-time remote biometric identification should be removed from Article 5 and transferred to a new Title IIa on 'restricted AI practices';
- The list of prohibited AI practices in Article 5(1) should be enriched, at least, by a prohibition of total or comprehensive surveillance of natural persons in their private or work life and of infringements of mental privacy and integrity (further extensions being beyond the scope of this Study);
- The Commission should have the possibility to adapt the list of prohibited AI practices periodically, potentially under the supervision of the European Parliament;
- There should be a clarification that prohibitions following from other laws (such as data protection or consumer protection law) remain unaffected.

A new Title IIa on 'restricted AI applications' should be inserted:

- The new Title IIa should deal with 'real-time' remote biometric identification (or even with other forms of real-time remote identification) in a more comprehensive way, without limitation to law enforcement purposes;
- It should also include a provision on other biometric identification systems, emotion recognition systems and biometric categorisation systems, limiting the admissibility of such systems and integrating the transparency obligation which is currently in Article 52(2);
- Title IIa should likewise include a new provision on decisions based on biometric techniques;
- Title IIa might possibly also include provisions that put substantive limits to the drawing of biometric inferences and provide for automated consent management.

Annex III point 1 should be extended so as to cover emotion recognition systems in (at least) the same way as biometric categorisation systems.

Administrator responsible: Mariusz MACIEJEWSKI Editorial assistant: Christina KATSARA
Contact: Poldep-citizens@ep.europa.eu

This document is available on the internet at: www.europarl.europa.eu/supporting-analyses
I
Print ISBN 978-92-846-8468-7 | doi:10.2861/677284 | QA-08-21-250-EN-C
PDF ISBN 978-92-846-8647-0 | doi:10.2861/|488838/ QA-08-21-250-EN-N