EUROSMART
The Voice of the Digital Security Industry

AI act

Eurosmart's comments on provisions regarding 'biometric identification system'

Eurosmart is fully engaged in promoting the development of reliable and trusted AI solutions and has repeatedly made clear its position throughout the legislative process: we support the necessary adoption of standards and rules regulating AI in Europe, and in particular to govern the use of biometric identification systems, such as those put forward by the European Commission in its initial proposal for the AI Act.

The Digital security industry welcomes the work achieved by the European Parliament providing key legal definitions for such a complex matter. However, the European Parliament proposes to considerably restrain the development, deployment, and use of biometric identification systems, without proper evaluation of their potential impact on internal security and on Europe's global industrial leadership in this field.

The European identity technologies industry, as represented by Eurosmart, are global leaders, committed in providing reliable, unique, and safe solutions and would like to express concerns with some key provisions aimed at tackling the issue of the development, deployment, use and export of biometric identification systems.

Exclusion of remote biometric identification systems

> *Amendment 41 – recital 18*
> *Amendment 220, 221, 222,223 and 229 to 231 – article 5*
>
> ***Eurosmart's proposal:*** *revert to the European Commission's proposal.*

These amendments would lead to a complete ban of any 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement in Europe. Eurosmart considers that the approach proposed by the European Commission in its proposal remains the right and balanced approach as it prohibits in principle the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, except for three well identified objectives.

Eurosmart recommends reverting to the European Commission's proposal which drastically limits the risks of mass surveillance and violations of personal freedoms while still allowing to benefit from these systems in certain well-identified situations (article 5(1)d). Moreover, the initial proposal considers the

"hierarchy of norms" within the European law ensuring the primacy of fundamental rights: accountability for public authority and strong counter powers exist and independent justice allows citizen to contest decisions if they are not lawful.

Beyond biometric identification systems, other kinds of technological tools may be diverted to carry out mass surveillance and violations of personal freedoms. However, these tools have been used for years in Europe in full compliance with fundamental rights and data protection requirements and it has not raised debates such as:

- Search engines which log the IP address and research of each individual;
- Mobile phone manufacturer or mobile app developer that can geolocate an individual;
- Personal electronic devices (including mobile phones) manufacturer that can potentially identify user thanks to their behavior (habits, way to type, location...).

In addition, from a philosophical perspective, banning technologies is very disturbing, as this may constitute a very dangerous precedent. From a legal aspect the EU legislative corpus should focus on functional, and security needs to respect the technology neutrality principle. There should not be favoritism nor discrimination against any technology. Forbidding a technology because of what it could be used for is contradictory to this principle. It would substantially hinder long-term research, development, and emergence of new technologies in the European Union.

Banning a particular technology for the very reason that it may be a threat to democracy could actually reach opposite results and weaken the grounds of democracy in the long-term. Innovation strongly contributes to democracy, as democracy only exists where there is wealth to share. Without prosperity and wealth, and thus without innovation and new technologies, democracy is also at risk.

Definition of remote biometric identification systems

> *Amendment 24 – recital 8*
> *Amendment 193 - Article 3 – paragraph 1 – point 36*
>
> ***Eurosmart's proposal:*** *revert to the European Commission's proposal and include a definition of 'verification system'.*

Amendment 24

Eurosmart very much welcomes this amendment which explicitly states that verification systems which merely compare the biometric data of an individual to their previously provided biometric data are not remote biometric identification systems.

However, the use of *"one-to-one"* creates confusion in the clarification. Many verification systems and corresponding use cases do not rely on a "one-to-one" comparison, but rather on a "one-to-several" comparison. For instance, this is the case for secure access to restricted area, or passenger facilitation at an airport, where the biometric data of the person is compared to several biometric reference data, which are those of all the users that have subscribed to the service.

The following sentences, and especially the wording *"Individual consent"* and "*is not de facto annulled by pre-enrolment*" also bring confusion. These provisions cover 'verification use-cases' (individual consent and pre-enrolment explicitly hint to verification systems). Therefore, this last sentence appears as contradictory to the provisions of the amendment 193 that exclude "verification system" from the definition of 'remote biometric identification system'.

Amendment 193

This provision should include the definition of "verification system" to ensure legal clarity. Based on the elements provided in recital 8 and recital 8a (through amendment 25), the definition could be as follows:

'Verification system' is defined as an AI system using biometric identification means in close proximity whose sole purpose is to confirm whether or not a specific natural person presenting themselves for identification is permitted, such as in order to gain access to a service, a device, or premises, through the comparison of a person's biometric data with biometric data contained in a reference database, and with prior knowledge whether the targeted person will be present and can be identified.

Export ban

> *Amendment 29 – recital 10*
>
> *Amendment 147 - Article 2 – paragraph 1 – point c a (new)*
>
> ***Eurosmart's proposal:** remove these amendments.*

The proposal to prohibit the export of both 'real time' and 'post' remote biometric identification systems will de facto leave the global market to third country providers typically subject to less stringent measures aimed at protecting personal data, privacy, and other fundamental rights, than those existing in Europe. The sole EU market (customer demands & supplier sides) of remote biometric identification is not strong enough to force other areas to align on the same principles. The risk is to rely on third countries' solution whose development does not follow the EU principles, despite the rules enacted by the future AI act.

Simultaneously, this ban will be highly detrimental to the European research and development in the field of Artificial Intelligence and thus hamper the capacity of the EU to be at the forefront of the Artificial Intelligence revolution. The geopolitical repercussions of such a measure should not be underestimated and are likely to be at odds with the EU's Open Strategic Autonomy.

Moreover, Eurosmart considers that the legal basis for such provision is incorrect: the basis of the text is the TFEU Article 114 (establishment and functioning of the internal market), but the export ban shall rather be based on the EU common commercial policy (TFEU Article 207);

Finally, legislative instruments are already in place to cover this aspect. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 sets up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.. Likewise,, this item falls under the category of cyber surveillance item defined as follows:

- Cyber-surveillance items' means dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting, or analysing data from information and telecommunication systems (article 2(20));
- In order to address the risk that certain non-listed cyber-surveillance items exported from the customs territory of the Union might be misused by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law, it is appropriate to place the export of such items under control. Associated risks relate to cases where cyber-surveillance items are specially designed to enable intrusion or deep packet inspection into information and telecommunications systems to conduct covert surveillance of natural persons by monitoring, extracting, collecting, or analysing data - including biometrics data - from those systems. Items used for purely commercial

applications such as billing, marketing, quality services, user satisfaction or network security are generally considered not to entail such risks (recital 8).

Such a text already provides for governance, process, criteria, and in addition a much more graduated approach based on risk assessment.

Exclusion of access control use cases from remote biometric identification systems

> *Amendment 25 - Recital 8 a (new)*
>
> ***Eurosmart supports this amendment.***

This amendment providing a definition is the right approach. To enhance the legal effect, such a provision could be translated into a paragraph within the definition section (article 3).

Clarification of the concept of bias

> *Amendment 78 – recital 44*
>
> ***Eurosmart supports this amendment.***

This amendment provides elements to mitigate possible bias of datasets. It also provides a definition for negative bias.

No restrictions on the use of 'post' remote biometric identification systems

> *Amendment 41 – recital 18*
> *Amendment 227 - Article 5 – paragraph 1 – point d d (new)*
> ***Eurosmart proposal: remove these amendments.***

Post remote biometric identification systems have proven to be useful to solve criminal cases and investigations. 1500 terrorists, criminals, fugitives, persons of interest or missing persons have been identified since the launch of INTERPOL's facial recognition system at the end of 2016.Also, for the success of any investigation, it is key to start examining the evidence as soon as possible, as time is a critical factor and of the essence.This principle is enacted for example by the British police:

- Golden hour principle - His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (justiceinspectorates.gov.uk);
- Investigation process | College of Policing ("Fast-track actions").

Therefore, the use of such solutions should not be further restricted and slowed down by requiring "pre-judicial authorization in accordance with Union law" for "specific serious criminal offense as defined in Article 83(1) of TFEU".

In addition, Eurosmart observes that the concept of "specific serious criminal offense as defined in Article 83(1) of TFEU" seems undefined. Therefore, it will be up to the Member States to further define this concept, which may lead to diverging national interpretations and thus fragmentation across EU when implementing the AI.