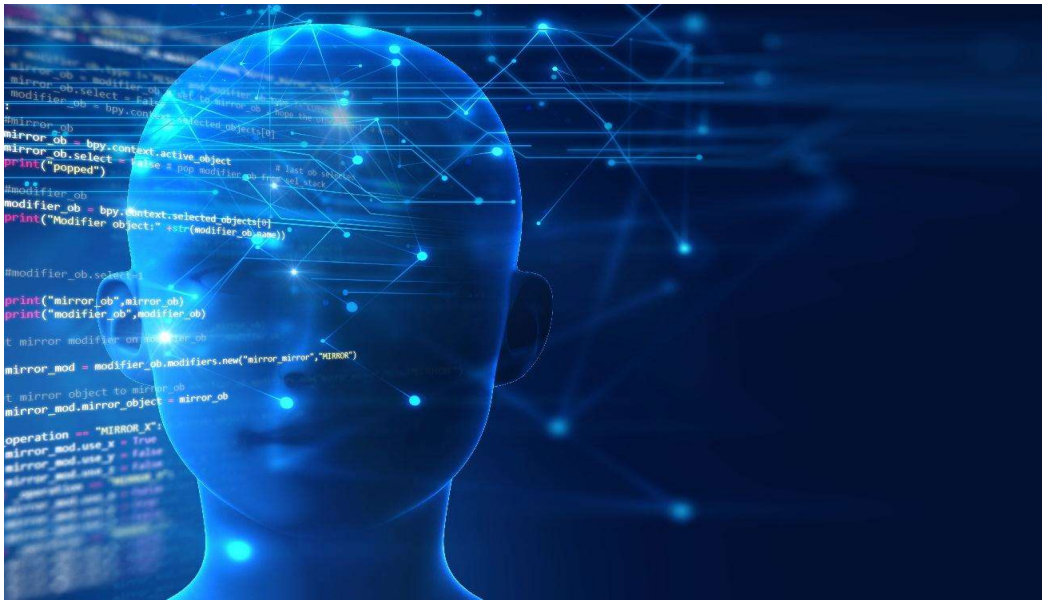
Feedback regarding
Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement



Herta Security, S.L.

May 2022

1) Protection of all fundamental rights vs ban on FR.

Most of the approaches regarding facial recognition ("FR") are based in the same mistake: what a fundamental right is and how must be protected.

The whereas 4 of the Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR") defines the privacy as a fundamental right whose scope is limited, shaped by all other freedoms and rights colluding with it:

"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

Unfortunately, the Guidelines we are referring to suffers from the same illness. There is none reference to the freedoms and fundamental rights that FR protects and that will be hindered if the total ban you request for FR in publicly accessible spaces or to infer emotions in natural persons is approved.

Perhaps the best way to understand such a mistake is to use as an example a fundamental right not involved, prima facie, in FR apps, such as the freedom of expression. Let's put and answer some questions regarding this right:

a) Is the freedom of expression absolute, unlimited?

   No, it's not. There are other fundamental rights at stake, such as the right to privacy and family life, the right to a truthful information and of course the freedom of expression of others, which may be impaired in case we protect unlimitedly the freedom of a sole person.

b) Being the freedom of expression limited, shaped by other fundamental rights deserving the same amount of care, how does the law protect it?

   In the same way than all other rights and freedoms. All of them are protected within the foggy boundaries marked by all other rights acting at the same time and at the same place. As it is said in article 29.2 of the Universal Declaration of Human Rights:

   "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others."

Coming back to FR apps, the previous reflections show that a legal and ethical approach must balance all rights at stake, not only the right to privacy or to personal data. So that, FR shall take into account the protection of, at least, the following fundamental rights:

- **The right to the protection of personal data**. Known as informational self-determination, it is included in the broader category of privacy, honour and reputation rights. It is protected in the article 8.2 of the Charter of Fundamental Rights of the European Union (the "Charter"), according to which the personal data *"must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law"*.

- **The right to liberty and security**. It is protected in the article 6 of the Charter, which says simply that *"everyone has the right to liberty and security of person"*.

- **The rights to life and to health**:
  The right to life is protected in article 2 and 3, which refers to the respect for physical and mental integrity.
  With regards to the right to health it is protected in article 34, guaranteeing the right to Social Security, and in article 35, according to which *"everyone has the right of access to preventive health care and the right to benefit from medical treatment"*.

- **The right to an effective remedy and to a fair trial**. Protected in article 47 of the Charter, according to which *"everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal"*. This includes the right to obtain evidences and to use them in a fair trial. Such evidences obtention will surely affect the rights and freedoms of other persons, but as long as the legal paths are followed, such right to an effective remedy shall prevail.

For instance, a security FR application within an airport or a train station may protect the

liberty and security of the commuters or even their rights to life and to health in situations of terrorist attack threat or health risk (because of a pandemic or for other medical reasons). Meanwhile, forensic uses of FR, that is to say the application of FR techniques to already recorded footage within the limited time and space where a crime has been committed, will provide substantial evidences (the face and perhaps the identity of the perpetrator), thus protecting the right to an effective remedy and to a fair trial of the victims.

2) No EU legal precedent supporting the proposed ban.

Taking into account the previous approach, with regards to the protection of fundamental rights, all EU laws and law proposals about personal data have tried to limit the processing of personal data, to require technical guarantees for such processing, but never to totally prohibit FR. In other words, the ban you propose in the Guidelines 05/2022 has no precedent in EU law.

On the contrary, the Directive (EU) 2016/680 (Law Enforcement Directive – "LED"), the GDPR and the recent proposal by the European Commission of an Artificial Intelligence Regulation (AI Act), instead of banning FR in public spaces permit it in a *numerus clausus* of cases:

1) Article 10 of LED. The processing of biometric data *"shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:*

   (a) where authorised by Union or Member State law;

   (b)to protect the vital interests of the data subject or of another natural person; or

   (c) where such processing relates to data which are manifestly made public by the data subject."

2) Article 9.2 of GDPR balances all rights above described and set a series of cases where FR can be used, at least the following:

   a. Substantial public interest, article 9.2.g of GDPR, *"on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"*

      The expression *"substantial public interest"* is not defined in the GDPR. Up to now, no data protection agency has interpreted this concept (not even the European Data Protection Board to whom this feedback is aimed). In spite of this lack of references there is no hint about a total prohibition, no EU or national law has introduced a ban or a moratorium in base of this article, because no prohibition is suggested, no ban can be deducted from it.

      Moreover, we can infer that, because of the addition of the word *"substantial"*, there should be serious reasons of public interest, in order to justify the installation of a FR system. In other words, from a point of view of security, of public security, this kind of systems must be available at least for the most threatened infrastructures and facilities.

      Of course, this mean real-time FR in publicly accessible spaces for law

enforcement purposes, because there is no other way to implement a useful FR system in this kind of scenarios.

b. Reasons of public interest in the area of public health, article 9.2.i of GDPR, *", such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy"*.

As abovementioned with regard to the right to life and health care, the article 9.2.i of GDPR is tailor made for a pandemic. According to it, it is permitted to process the so called special categories of personal data (not only biometric data but, especially in this case, health or even genetic data) in order to fight against *"serious cross-border threats to health"* or to ensure high standards of quality and safety of health care and of medicinal products or medical devices.

Again, no recommendation to prohibit FR in publicly accessible spaces and no law banning the technology as you suggest.

c. Establishment, exercise or defence of legal claims, article 9.2.f of GDPR, *"or whenever courts are acting in their judicial capacity"*.

The aforesaid right to an effective remedy and to a fair trial may prevail over the right to the protection of personal data, where the processing of biometric data (using FR for instance) is proportional and necessary to prepare, issue or defend against any kind of legal claims *"whether in court proceedings or in an administrative or out-of-court procedure"*, as stated in Whereas 52 of GDPR.

As in the previous cases, no data protection agency has interpreted article 9.2.f of GDPR, and no law has prohibited FR in publicly accessible spaces, because such solution has been never suggested by GDPR. On the contrary, the forensic use of FR, that is to say the application of FR tools to already filmed footage, for instance to recover evidence in a criminal or civil case, can be deemed proportional and necessary, due to the limited amount of biometric data that will be processed.

3) Article 5.1.d of the AI Act permits *"the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement"* in the next cases:

a. the targeted search for specific potential victims of crime, including missing children;

b. the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

c. the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

In addition, articles 5.2 and 5.3 add further requirements for the use of the facial recognition in real time in public spaces for law enforcement purposes, which can be summarised in the next points:

a) Evaluation of proportionality.
b) Balance of risks avoided and of threats to the rights and freedoms of the concerned persons.
c) Safeguards and conditions of use, especially regarding temporal, geographic and personal limitations.
d) Prior authorisation of a judicial or administrative authority for *"each individual use"*, which can be issued *a posteriori* in situations of urgency.

Finally, number 4 of article 5, states that the Member States can further develop by means of national legislation the use of facial recognition in public spaces, according to the requirements above defined.

3) Conclusions.

As it is shown in the previous point, in order to allow FR, LED and GDPR require a legal framework of the Member States or the EU, providing *"suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"*. Indeed, the AI Act represents the first effort, at EU level, to take into effect such legal framework.

Instead of this solution, you propose to ban the use of FR in publicly accessible spaces or to infer emotions in natural persons. This approach implies at least four undesirable consequences:

1) Hindering the rights to liberty and security, the rights to life and to health and the right to an effective remedy and to a fair trial, which will be protected by means of the FR whose prohibition you are requesting.

2) Holding up the development of AI European industry, which is a key objective for the EU, according to the White Paper on AI published on 19 February 2020 by the Commission. A key objective that the Commission is trying to implement by means of the AI ACT.

3) Contradicting the EU privacy laws. Because neither the GDPR nor the LED has never praised the total prohibition of FR or other kind of biometric data processing, but a strict regulation, the stricter in the world, which will not only protect the right to privacy but all other rights at stack.

4) Providing a negative message to law makers, judicial and administrative authorities and even to the industry. Because banning is an easy path or at least an easier path than creating standards of quality, technical measures, judicial authorisations, risk evaluation measures and all the overwhelming requirements that the AI Act tries to impose in order to authorise the use of FR in public spaces for law enforcement purposes.

But, in addition to all these reasons, there is a more powerful one for rejecting the ban you propose: FR in public spaces is not the same the mass surveillance system you wrongly describe in you Guidelines.

Of course, you do not define what massive surveillance is. At a first glance any video surveillance in public spaces fits perfectly in the definition. Nevertheless, you deem it acceptable, surely because it is absolutely legal since decades ago. Because of that, we suppose that it is not only a question of recording the movements of a lot of people, but something more you do not say but suggest: the surveillance of all or most of the people all or most of the time.

This kind of surveillance will, of course, vulnerate the privacy and other freedoms and fundamental rights, but what is proposed in the AI Act, respecting the guidelines of GDPR and LED, is nothing similar to this frightening threat. At least because of the following reasons:

1) The system will operate only in critical facilities and spaces. Not everywhere.

2) The system will operate only when there is a need for it (terrorist threat, searching for the perpetrator of a serious crime, etc.). Not every time.

3) The system will operate only with judicial authorisation. Not without legal control.

4) The system will operate always as a tool under the human supervision of law enforcement officers. Not automatically.

In other words, FR in public spaces will be just a tool improving the mass surveillance that it is already been taken into effect by law enforcement forces. A tool that, indeed, will improve the searching abilities of the law officers, reducing the error rates, avoiding to disturb the citizens with wrong identifications.

Probably because of that and because of the increase of crime rates, a lot of the cities and states in the US that followed the wrong path of banning you are suggesting, are right now backing off such prohibition of FR: https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/