COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

16 June 2020

T-PD(2020)03

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Facial Recognition

Draft Guidelines

Directorate General of Human Rights and Rule of Law

Contents

Facial recognition is a biometric face recognition technology, based on algorithms that learn to recognize the unique features and characteristics of faces in order to identify or authenticate them.
Facial recognition has rapidly evolved from being a technological novelty to an indispensable reality of our daily lives. Facial recognition technologies are advancing rapidly and algorithms are becoming more and more powerful.
For Cicero, the face was the mirror of the soul; he was thus underlining the close link between an image (today in the form of a computer template) and the deepest intimacy of the person. The sensitivity of information of a biometric nature was specifically recognised with the inclusion of data uniquely identifying a person under the special categories of data in Article 6 of the modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (hereinafter "Convention 108+").
The uses of this technology are varied and numerous, some of which may seriously infringe the rights of data subjects. In order to prevent such infringements, the Parties to Convention 108 shall ensure and permit that the development and use of facial recognition respect the right to privacy and the protection of personal data, thereby strengthening human rights and fundamental freedoms.
These guidelines provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and user organisations should apply to ensure that this technology does not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.
Nothing in these guidelines should be interpreted as excluding or limiting the provisions of the European Convention on Human Rights and Convention 108. These guidelines also take into account the new safeguards provided by the modernised Convention 108 (commonly referred to as "Convention 108+").

I. GUIDELINES FOR LEGISLATORS AND DECISION-MAKERS

1. Legal basis

a. Prohibition by law of certain uses

Despite the precautions provided for in the legislation applicable to facial recognition, and in particular Convention 108+, it appears that its use should in some cases be strictly limited or even prohibited by national laws.
For example, facial recognition should never be used to determine a person's skin colour, religion, sex, origin, age or health condition (except, of course, in the context of a medical research project).

Similarly, affect recognition is a sub-category of facial recognition that claims to detect aspects such as personality, inner feelings, mental health and workers' engagement from images or videos of faces. These claims are not supported by sound scientific evidence and may be unethically applied. Linking recognition of affect to hiring of staff, access to insurance, education and policing poses risks of great concern, both at the individual and societal levels, and would be likely to be prohibited.

b. National laws framework

With regard to special categories of data within the meaning of Article 6 of Convention 108+, any processing involving the use of facial recognition shall be authorised only if appropriate

safeguards are provided by law. These safeguards shall be adapted to the risks involved and to the interests, rights and freedoms to be protected, applied alone or cumulatively.

In addition, other texts such as the GDPR prohibit such processing as a principle. They may be implemented, by way of exception, only in certain specific cases (with the express consent of individuals, to protect their vital interests or on the basis of an overarching public interest) and following modalities that are appropriate to those risks.

In any event, it will be necessary to ensure, at the very least, that the use made of such measures is proportionate to the purpose and the impact on the rights of the data subjects.

Without judging the ethical level of different cases of use, they should be categorised, and a legal framework should imperatively be in place in respect of facial recognition that would determine, according to each different use:

- the detailed explanation of the specific use;
- the minimum reliability of the algorithm: minimum reliability percentage;
- the retention duration of the photos used for identification;
- the possibility of auditing these criteria;
- the traceability of the process secured by a "Blockchain" for example.

2. Quality of the consent

Thus, depending on the purpose, particular attention must be paid to the quality of the data subject's explicit consent if it is the legal basis for the processing.

One of the main factors to be taken into account when collecting facial recognition data from a potentially large number of persons is therefore whether and how to obtain their informed consent, especially if these persons are subsequently identified or profiled against other data sets.

Indeed, data subjects may not be able to give or withdraw consent in a meaningful way to the collection of facial recognition data as these systems become more prevalent in private spaces open to the public.

It is therefore appropriate to:

- take steps to obtain explicit and affirmative consent, in particular before identifying an anonymous or unidentified person, and of course when such identification is provided to third parties who did not already know their identity outside the context of the relationship with the data subject;

- if this is not possible, commit to collect, use and share facial recognition data in a way that is compatible with the context in which the data were collected, taking into account the likely impact on individuals and the potential for innovative uses of the data to the benefit of individuals;

-in order to ensure that consent is freely given, data subjects should be offered alternative solutions (for example, using a password or an identification badge) but also ensure that the said alternative solution be easy to use as, if it appeared to be too long or complicated compared to the facial recognition technology, the choice would not be a genuine one;

- if consent is given for one purpose, there should be no other use for a second purpose without consent. Similarly, in case of transfer of data to a third party, such transfer should also be subject to specific consent;

- the information provided prior to the collection of the data must of course meet the transparency requirements mentioned above to ensure the quality of consent;

- no unique biometric identifiers should be created and retained over time without appropriate consent;
- finally, withdrawal of consent will have to be taken into account at technical level to ensure its effectiveness.

3. Necessary involvement of supervisory authorities

According to the applicable national or international legislation, the use of facial recognition tools remains prohibited to date with some exceptions.

Several countries now wish to implement experimental facial recognition systems. In this context, it seems desirable to systematically involve the national control authorities and, in particular, to consult them on any draft text adopted with a view to possible experimentation.

These authorities could thus be consulted systematically and in advance on envisaged projects in order to shed light on the protection of the data of data subjects. Similarly, they should have access to the impact assessments carried out and also to all audits, reports and analyses carried out in the context of these experiments.

Finally, the supervisory authorities will be able to propose useful corrective measures and, where appropriate, to support the protection of data subjects upon direct referral.

4. Labelling / Certification

Today, many digital service companies are promoting their artificial intelligence activities and more specifically facial recognition. Moreover, it is still difficult to have a knowledge of all the players in facial recognition, their field of application and intervention, their ethical value about artificial intelligence, etc.

Designers and integrators of facial recognition solutions should be able to communicate, according to their involvement, about:

- The data they use;
- The temporality of these data;
- The diversity of these data;
- Known biases and how to avoid them;
- The publisher solution used;
- Their possible certification;
- Their adherence to an ethical charter;
- Their commitment to the implications of this technology;
- etc.

All of these criteria could be subject to labelling and/or certification demonstrating the ability to master facial recognition technologies, responsibility, ethics and the use of artificial

intelligence in the broadest sense. This process could be based on the same model as pharmacopoeia.

The setting up of independent and qualified certification mechanisms for facial recognition and data protection, as well as data protection labels, to demonstrate full compliance of the processing operations carried out, would be an important element in building user confidence.

Such a labelling could be implemented at various levels depending on the field of application of artificial intelligence: one level to categorise types of structures (algorithm creator, algorithm integrator, etc.), one level to categorise types of algorithms (computer vision, language: sentence understanding and generation, intelligent search, etc.) and one level to categorise uses (critical or non-critical, for example).
The label would cover all the points mentioned in the technical recommendations and would furthermore make it possible to map out these companies and to ascertain the existence of a framework for the use of a technology that is currently much debated.

5. Raising awareness of those concerned

Beyond labelling and/or certification, the issues involved in the proper use of facial recognition must also be accessible to the data subjects.

In this context, it is necessary to raise awareness with and train citizens in a simple and educational way. The idea is to give access to simple concepts that could alert the data subjects before they voluntarily use a facial recognition tool:

- understand what it means to give out one's data;
- understand how facial recognition works;
- alert to potential dangers in case of misuse (identity theft with a photo and a non-infrared camera for example).

This approach must obviously be combined with that of technology developers who must allow real and effective transparency.

II. GUIDELINES FOR DEVELOPERS, MANUFACTURERS AND SERVICE PROVIDERS

1. Data and algorithm quality

a. Representativeness of used data

Like other applicable regulations, including the European Union's General Data Protection Regulation, Article 5 of Convention 108+ provides for a data accuracy requirement. This point is central in the field of facial recognition, since it has been proven on many occasions that errors are frequent and have serious consequences for data subjects.

Therefore, developers or manufacturers of facial recognition tools but also user organisations will have to take steps to ensure that facial recognition data are accurate, in particular to avoid mislabelling, by sufficiently testing their systems and identifying and eliminating significant disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination.

Furthermore, in order to ensure both the quality of the data and the efficiency of the algorithms, the algorithms will have to be developed using properly labelled photos, but also that dataset are representative of the whole population, i.e. based on a quantity of diverse photos of men and women, of different skin colours, different morphology, of all ages and from different camera angles.

On another level, the questions asked by people with disabilities and those whose physical characteristics do not correspond to the technical standards of the tool used must be answered. Back-up procedures should be provided for in case of system failure if the physical characteristics do not correspond to the technical standards.
On the other hand, the collection of personal data for automated processing poses an additional problem if these biometric data unnecessarily but unavoidably reveal other sensitive data such as information on a type of illness or physical disability.

b. Data life duration

A facial recognition tool requires periodic renewal of data (the photos of faces to be recognised) in order to train and improve the algorithm used.

It seems difficult at the current stage of technology development to define a fixed renewal period.

On the other hand, each algorithm has a percentage of recognition reliability during its development and use. It seems therefore important to date and record this percentage in order to monitor its evolution. Should its reliability deteriorate, it will be necessary to renew the training photos and therefore ask users again to provide photos. This will also enable to protect from the consequences of changes in the shape of faces (due to ageing, to accessories (piercing or other), to accident modifying part of the face, etc.).

That would also enable data subject to renew or not to renew their consent to the use of their photos for facial recognition.

These reliability percentage records (global for the algorithm and specific for the user) should be easily available to users in the form of a dashboard for example.

2. Reliability of the tools used

It should be recalled that artificial intelligence algorithms are at random.
It would be useful to consider a minimum required reliability percentage, that could vary according to the nature of the purpose. A facial recognition system for customers in a shop does not necessarily need the same level of reliability as for cash dispensers or for detecting persons wanted in criminal investigations.

Similarly, where facial recognition is carried out using a camera, the level of sophistication of the tool will need to be adapted to the purpose. Thus, in the context of identity management, it would be harmful if the system allowed identification by means of a photo that was simply placed in front of the camera, making identity theft very easy. For such a purpose where facial recognition is used as both an account and a password, the camera should be equipped with infra-red sensors.

3. Awareness and traceability

Companies developing and selling facial recognition technology software should endeavour to take reasonable steps - such as making recommendations and providing advice - to help organisations or companies using their facial recognition technology to apply transparency and respect for privacy.

For example:

. by setting reasonable using limits in the wording of the contract;
. by providing companies with a sample language for signage of physical locations or mention in their privacy policies;
. by recommending clear, easy-to-understand signage that states whether facial recognition technology is deployed in public space;
. by advising other reasonable efforts to promote the provision of clear and complete information to data subjects.

Moreover, in addition to this information on the use of this technology, it is useful to also provide for information to ensure that the data subject is fully informed, while of course respecting business secrecy. That information could thus concern:

. the reliability level of the algorithm and the record of this reliability;
. the records of the successive versions of the algorithm;
. the process and reasoning of the algorithm;
. the type of data used as input, etc...

This information will of course have to be worded in a clear and understandable for all language. Such a pedagogical documentation could have the form of articles, images, videos, FAQs.

Beyond the primary usefulness of information for data subjects, such an endeavour will also make it possible to raise their level of digital awareness by enabling them to understand the impact of a publication on social networks or a click on an advertisement.

This pedagogical vocation could be adapted to the type of data subjects and thus reach a maximum number of people (schools, businesses, retirement homes, etc.).

4. Privacy by design

Businesses or organisations can implement the principle of privacy by design in a variety of ways, including:

- by anticipating and preventing events that infringe on human rights and privacy before they occur;

- by integrating privacy protection into the design and architecture of facial recognition products and services, as well as into internal IT systems and the use of dedicated tools;

- by implementing an internal review process designed to identify and mitigate potential privacy risks in products and services that use facial recognition technology before they are made available or deployed;

- by integrating such an approach into their organisational practices, including for example, assigning dedicated staff, providing privacy training to employees, and conducting privacy analyses upon the development or modification of facial recognition products and services.

This issue has already been partly addressed by the Big Data Guidelines , which propose to give priority to by-design solutions to "avoid potential hidden bias and the risk of discrimination or negative impact on the fundamental rights and freedoms of data subjects, both during collection and analysis".

However, this approach cannot of course be carried out only by solution providers on a technical level. Other professionals should be involved in the implementation, including committees of experts from different areas (social sciences, law, ethics, etc.), which may provide the best framework to engage in debate and address the issues of the impact on the individual and on society, thus compensating for developers' limited perspective.

III. GUIDELINES FOR USER ORGANISATIONS

1. Limitations on use - Proportionality

Entities using facial recognition technology should consider how this use will impact both those who voluntarily use facial recognition technology and those who accidentally come into contact with facial recognition products or services or who cannot reasonably avoid a company's use of facial recognition technology.

For example, when facial recognition data are used to match a person's facial print to a set of registered user credentials, the company should attempt to remove all data from the facial recognition template as soon as possible in the event of a non-compatible result.

In addition, the choice of a verification or identification function dependent very much on the intended purpose of the facial recognition system and on the circumstances in which it will be used. The instrument must thus serve the purpose for which the data were collected and not be unnecessarily oversized. Therefore, when a verification system also appears possible, the choice of an identification system will require a specific justification.

Finally, the particularity of biometric data for facial recognition is that they often contain more information than is necessary for the verification or identification of persons. Excessive data processing can be avoided by limiting the storage and use of data. The system must therefore be designed in such a way that the data obtained reveal only the information necessary for its purpose. In particular, it must avoid any possible link with other data of a sensitive nature (e.g. illness).

Of course, personal data must not be further processed in a way that the data subject might find unexpected, inappropriate, or objectionable.

Moreover, in case of transfer of data to third parties or public dissemination of data (e.g. on social networks), technical and/or legal means should be identified to avoid other uses than those initially intended. Such measures may include technical degradation of individual images, limitation of automated access to relevant databases and the creation of contractual obligations for partners to respect the legal framework.

2. Data security

Any failure in data security may have particularly serious consequences for data subjects, as unauthorised disclosure cannot be corrected, for example by changing a password.

Strong security measures, both at technical and organisational level, should therefore be implemented to protect facial recognition data and image sets against loss and unauthorised access or use during collection, transmission and storage. Reasonable security should include data encryption and a combination of virus protection, access controls, employee training and other high standards security practices.

Any breach of this obligation should be notified to the supervisory authority and, where appropriate, to the data subjects.

Security measures should evolve over time and in response to changing threats and identified vulnerabilities and should also be proportionate to the sensitivity of the data, to the context in which facial recognition technology is used and its purposes, to the likelihood of harm to individuals and other relevant factors.

Strict retention and disposal practices for facial recognition data, with the shortest possible retention periods should also be defined and applied.

3. Transparency

One of the greatest risks raised by the use of facial recognition is that, contrary to the use of biometric data, it can be carried out with the data subject's completely ignoring it.

It is therefore essential to hold such use to a real and effective transparency (Article 8 Convention 108+).

Thus, the factors that will determine whether a use is compatible with such a principle of transparency include, for example, the information given to individuals, the context of the collection, reasonable expectations as to how the data will be used, whether facial recognition is merely a feature of a product or service and not an integral part of the service itself, and how the collection, use or sharing of facial recognition data is likely to affect individuals, especially when used with persons in vulnerable situations.

A privacy policy on facial recognition or informational material could include, in addition to the information provided for in Article 8 of Convention 108+, the following information:

. whether facial recognition data can be shared (see below about full identification of third party contractual partners who receive the data in the course of providing the product or service);
. the retention, deletion or de-identification of facial recognition data;
. the choices of the persons at their disposal regarding their facial recognition data;
. contact points available for individuals to ask questions about the collection, use and sharing of facial recognition data;
. full identification of the third-party contractual partners who receive the data in the course of providing the product or service;
. when collection, use and sharing practices change significantly, companies should update their privacy policy or publicise these changes in light of the context of the change and its impact on individuals.

4. Impact analysis and risk assessment

A risk assessment of the potential impact of the processing on fundamental rights and freedoms is necessary to balance the protection of these rights with the different interests involved in the use of facial recognition.

Both public authorities and private companies or other bodies should adopt a precautionary approach based on appropriate prevention and risk mitigation measures, and be required to carry out systematic assessment of existing facial recognition tools, measuring their potential impact on human rights, taking into account the nature, context, scope and purpose of the system. Such analyses should not, of course, be limited to identifying risks, but offer effective significant mitigation solutions.

Where a public authority has not yet acquired or developed a facial recognition system, this assessment should be carried out prior to the acquisition and/or development of the tool and should be made public. In addition, public authorities should require any potential tool provider to lift any restrictions on the exchange of information if this has a limiting effect on the impact assessment.

The impact assessment could be carried out either by an independent monitoring body or by an auditor having relevant expertise to help find out, measure or map out impacts and risks over time.

Such impact assessments should of course be carried out at regular intervals.

If a risk is identified, the bodies concerned should be able to refer to any existing ethics committees, and of course first and foremost to the competent supervisory authorities to examine the human rights risks.

Finally, for the implementation of any new project, this approach should be combined with a "privacy by design" approach, as provided for in point II

5. Accountability

Accountability and vigilance are central to ensure that practices comply with the legal framework:

- user organisations will be required to implement transparent policies, procedures and practices to ensure that the principles to protect the rights of the data subjects underlie their use of facial recognition technologies;

- this includes implementing training programmes and audit procedures for those in charge of processing facial recognition data;

- it would also be useful to consider setting up internal review committees to assess and approve any processing involving facial recognition data;

- these principles should be contractually extended to third party service providers, business partners or companies using facial recognition technology and thus deny access to third parties that would not comply with them;

- the use of facial recognition by public authorities in particular could be subject to minimum levels of performance in terms of accuracy, especially where public security purposes are concerned;

- similarly, with regard to the public sector, which is already heavily involved in the use of facial recognition, it would be useful to provide for specific transparency and prior evaluation constraints in public procurement procedures with suppliers of facial recognition tools.

6. Ethical framework

To follow the logic as exposed above, giving an ethical framework to the use of this technology seems to be a crucial issue. Indeed, regulation is essential, but companies also "need an internal accountability structure that goes beyond ethical guidelines." This could take the form of external ethics advisory boards that could carry out audits and publish the results of their research.

Furthermore, in order to avoid human rights abuses, conventions of experts from different fields of expertise would be likely to define the most potentially dangerous cases when using facial recognition technology.

On this topic, whistleblowers have also an important role to play and employees of companies or organisations developing or using these solutions should be able to benefit from an appropriate protection status, as provided for in particular in Recommendation (2014)7 on the protection of whistleblowers.

IV. THE RIGHTS OF DATA SUBJECTS

As facial recognition is based on the processing of sensitive data, all the rights provided for by Article 9 of Convention 108+ are guaranteed to the data subjects, such as the right to information, the right to object, the right to rectification, the right not to be subject to a fully automated decision, etc.

The Explanatory Report to Convention 108+ rightly emphasises that "human dignity requires the establishment of safeguards when processing personal data, so that individuals are not treated as mere objects. »

Indeed, where the use of facial recognition technology is intended to enable a decision to be taken exclusively on the basis of automated processing which would significantly affect the data subject, the latter must in particular have the right not to have such processing carried out without his or her views being taken into account.

Data subjects also have the right to know the reasoning underlying the processing operations on data concerning them, which should include the consequences of that reasoning.

Data subjects shall have the right to object at any time, on grounds relating to their situation, to facial recognition processing unless the controller demonstrates legitimate grounds for processing which override their interests, rights and fundamental freedoms.