28 January 2021 T-PD(2020)03rev4

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

CONVENTION 108

Guidelines on Facial Recognition

Directorate General of Human Rights and Rule of Law

Contents

Facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates.

The sensitivity of information of a biometric nature was recognised explicitly 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[1] (hereinafter "Convention 108+").

The context of the processing of images is relevant to the determination of the sensitive nature of the data as not all processing of images involves the processing of sensitive data. Images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual[2].

These Guidelines cover uses of facial recognition technologies, including live facial recognition technologies. The uses of this technology are many and varied, some of which may seriously infringe the rights of data subjects. Legislation authorising vast surveillance of individuals can be found contrary to the right to respect for private life[3].

Integrating facial recognition technologies to existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data as well as to other fundamental rights since the uses of these technologies do not always require the awareness or cooperation of the individuals whose biometric data is processed, considering for instance the possibility of accessing digital images of individuals on the Internet.

In order to prevent such infringements, the Parties to Convention 108+ shall ensure that the development and use of facial recognition respect the rights to privacy and to data protection, thereby strengthening human rights and fundamental freedoms by implementing the principles enshrined in the Convention in the specific context of facial recognition technologies.

These guidelines[4] provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.

The guidelines have a general scope and cover uses of facial recognition technologies in the private and public sectors. They do not exclude that further protective measures be required in the applicable legal framework depending on the case of use. They assess various uses of these technologies in different sectors by taking into account the purposes of these uses and their potential impact on the right to data protection and other fundamental rights.

---

[1] Amending Protocol CETS No. 223 to Convention 108.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[2] Paragraph 59 of the Explanatory Report to Convention 108+.

[3] Declaration of the Committee of Ministers of the Council of Europe on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, adopted on 11 June 2013, available at
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d.

[4] These Guidelines build upon a 2019 report by Sandra Azria and Frédéric Wickert "Facial recognition: current situation and challenges", available at https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1.

Law enforcement purposes mean in these guidelines the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties. This includes the maintenance of public order by the police (hereinafter referred to as "law enforcement purposes")[5]. The term “law enforcement authorities” is understood as meaning more widely the public prosecutor services and/or other public and/or private bodies authorised by law to process personal data for the same purposes (hereinafter “law enforcement authorities”).

Nothing in these guidelines should be interpreted as excluding or limiting the provisions of Convention 108[6]. These guidelines also take into account the new safeguards provided by Convention 108+.

I. GUIDELINES FOR LEGISLATORS AND DECISION-MAKERS

1. Lawfulness

As provided for by Article 6 of Convention 108+, the processing of special categories of data, such as biometric data, shall only be authorised if such processing relies on an appropriate legal basis, and complementary and appropriate safeguards are enshrined in domestic law. These safeguards shall be adapted to the risks involved and to the interests, rights and freedoms to be protected.

Some laws[7] have enacted the prohibition of such processing as a rule and only allow its implementation by way of exception, in certain specific cases (*e.g*. with the explicit consent of individuals, to protect their vital interests or when the processing is necessary for the reasons of an overarching public interest) and subject to safeguards that are appropriate to those risks.

The necessity of the use of facial recognition technologies has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects.

The different cases of use should be categorised, and a legal framework applicable to the processing of biometric data through facial recognition should be in place. This legal framework should, according to each different use, address notably:

- the detailed explanation of the specific use and the purpose;
- the minimum reliability and accuracy[8] of the algorithm used;
- the retention duration of the photos used;
- the possibility of auditing these criteria;
- the traceability of the process;
- the safeguards.

[5] Law enforcement purposes corresponds to ‘police purposes’ in the Practical guide on the use of personal data in the police sector, see Committee of Convention 108, Practical guide on the use of personal data in the police sector (T-PD(2018)01) available at https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

[6] Obviously, for Parties to the Convention which are Council of Europe member states, nothing in the guidelines can furthermore be interpreted as excluding or limiting the provisions of the European Convention on Human Rights.

[7] See Article 9 of the European Union’s General Data Protection Regulation (GDPR).

[8] The accuracy of the algorithm can be expressed through an assessment of false positive or false negative errors produced by the software.

1.1. Strict Limitation by Law of Certain Uses

The level of intrusiveness of facial recognition, and related infringement on the rights to privacy and data protection will vary according to the particular situation of their uses and there will be cases where domestic law will strictly limit it, or even completely prohibit it where the democratic process will have led to that decision.

The use of live facial recognition technologies in uncontrolled environments[9], in light of the intrusiveness it bares upon the right to privacy and the dignity of individuals, coupled with a risk of adverse impact on other human rights and fundamental freedoms[10], should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis.

The use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination[11].

Similarly, affect recognition[12] can also be carried out with facial recognition technologies to arguably detect personality traits, inner feelings, mental health or workers' engagement from face images. Linking recognition of affect, for instance, to hiring of staff, access to insurance, education may pose risks of great concern, both at the individual and societal levels and should be prohibited.

1.2. Legal Basis in Different Contexts

The legal framework applicable to the processing of biometric data through facial recognition should, in complement to elements mentioned in Section 1, consider and address:

- the different phases of the use of facial recognition technologies, including the creation of databases and deployment phases;
- the sectors in which these technologies are used;
- the intrusiveness of types of facial recognition technologies such as live or non-live facial recognition technologies, while providing clear guidance on the lawfulness.

1.2.1. Integrating Digital Images to the Facial Recognition Technologies

Legislators and decision-makers shall ensure that images available in a digital format cannot be processed to extract biometric templates[13] or to integrate them into biometric systems without a specific legal basis for the new processing, when those images were initially captured for other purposes (from social media for instance).

As extracting biometric templates from digital images involves sensitive data processing, the possible legal basis considered below, varying for different sectors and uses must be secured.

---

[9] The notion of “uncontrolled environment” covers places freely accessible to individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools.

[10] See the Guidelines on Artificial intelligence and data protection: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

[11] It could for example be authorised for a medical research project, subject to appropriate safeguards enshrined in law.

[12] Affect recognition is the use of technology to attempt identifying or classifying human emotion.

[13] A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and is stored in a biometric database.

Specifically, using digital images that were uploaded on the Internet, including social media or online photo management websites or were captured passing through the lens of video surveillance cameras cannot be considered lawful on the sole basis that the personal data were made manifestly available by data subjects.

Legislators and decision-makers should ensure that existing databases of digital image initially used for other purposes can only be used to extract biometric templates and integrate them into biometric systems when it is for overriding legitimate purposes and it is provided by law and strictly necessary and proportionate for these purposes (for instance law enforcement or medical purposes).

1.2.2. Use of Facial Recognition Technologies in the Public Sector

Consent should not, as a rule, be the legal ground used for facial recognition performed by public authorities considering the imbalance of powers between data subjects and public authorities. For the same reason, as a rule, it should not be the legal ground used for facial recognition performed by private entities authorised to carry out similar tasks as public authorities.

The lawfulness of the use of facial recognition technologies shall be based on the purposes of the biometric processing provided by law and necessary safeguards complementing the Convention 108+.

Legislators and decision-makers have to lay down specific rules for biometric processing by facial recognition technologies for law enforcement purposes. These laws will ensure that such uses must be strictly necessary and proportionate for these purposes and prescribe the necessary safeguards to be provided.

Law enforcement authorities

Biometric data processing by facial recognition technologies for identification purposes in a controlled[14] or uncontrolled environment should be restricted, in general, to law enforcement purposes. It should be carried out solely by the competent authorities in the area of security.

Laws can provide different necessity and proportionality tests depending on whether the purpose is verification or identification, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected.

For identification purposes, the strict necessity and proportionality must be observed both in the setting-up of the database (watchlist) and deployment of (live) facial recognition technologies in an uncontrolled environment.

Laws should provide clear parameters and criteria that law enforcement authorities should adhere to, when creating databases (watchlists) for specific, legitimate and explicit law enforcement purposes (for example suspicion of severe offences or risk to public security).

Considering the intrusiveness of these technologies, in the deployment phase of the live facial recognition technologies in uncontrolled environments, the law shall ensure that law enforcement authorities demonstrate that a variety of factors, including the place and timing of deployment of these technologies, justify the strict necessity and proportionality of the uses.

[14] The notion of “controlled environment” covers the cases in which the biometric systems can only be used with the person’s participation.

Other public authorities

Legislators and decision-makers will lay down specific rules for biometric processing by facial recognition technologies for other substantial public interests by public authorities that are not pursuing law enforcement purposes.

Laws can provide different necessity and proportionality tests depending on whether the purpose is verification or identification, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected.

Considering the potential intrusiveness of these technologies, legislators and decision-makers have to ensure that an explicit and precise legal basis provides the necessary safeguards for the processing of biometric data. Such legal basis will include the strict necessity and proportionality of these uses and will take into consideration the vulnerability of the data subjects and the nature of the environment where these technologies are used for verification purposes.

For example, ensuring security in controlled or uncontrolled environments, including schools or other public buildings, should not, as a rule, be considered strictly necessary and proportionate where less intrusive alternative mechanisms exist.

1.2.3. Use of Facial Recognition Technologies in the Private Sector

The use of facial recognition technologies by private entities, except for private entities authorised to carry out similar tasks as public authorities, requires according to Article 5 of Convention 108+ the explicit, specific, free and informed consent of data subjects whose biometric data is processed.

Considering the requirement for such a consent of data subjects, the use of facial recognition technologies can only take place in controlled environments for verification or for authentication or for categorisation[15] purposes.

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

In order to ensure that consent is freely given, data subjects should be offered alternative solutions to the use of facial recognition technologies (for example, using a password or an identification badge) that are 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 a specific purpose, personal data should not be processed in a way that is incompatible with this purpose. Similarly, in case of disclosure of data to a third party, such disclosure should also be subject to specific consent.

Private entities shall not deploy facial recognition technologies in uncontrolled environments such as shopping malls, especially to identify persons of interest, for marketing purposes or for private security purposes.

Passing through an environment where facial recognition technologies are used cannot be considered as an explicit consent.

[15] Biometric categorisation means the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action.

2. Necessary Involvement of Supervisory Authorities

In compliance with Article 15(3) of Convention 108+, supervisory authorities are to be consulted on proposals for any legislative or administrative measures implying the processing of personal data by facial recognition technologies. It is necessary to systematically involve the supervisory authorities and, in particular, to consult them on any possible experimentation or foreseen deployment.

These authorities shall thus be consulted systematically and prior to envisaged projects. Similarly, they should have access to the impact assessments carried out as well as to all audits, reports and analyses carried out in the context of such experiments or projects.

Legislators and decision-makers should ensure effective cooperation between various supervisory authorities competent for the oversight of different aspects of these data processing where different authorities are responsible for the control of the compliance of such processing activities with the law.

3. Certification

Legislators and decision-makers should use different mechanisms to ensure the accountability of the developers, manufacturers, service providers or entities using these technologies.

The setting up of independent and qualified certification mechanism for facial recognition and data protection to demonstrate full compliance of the processing operations carried out would be an essential element in building users' confidence.

Such a certification could be implemented according to the application of artificial intelligence used by the facial recognition technology: one type of certification to categorise structures (design of algorithm, integration of algorithm, etc) and another to categorise algorithms (computer recognition, intelligent search, etc.).

4. Raising Awareness

The awareness of data subjects and the understanding by the general public of facial recognition technologies and of their impact on fundamental rights should be actively supported through accessible and educational actions.

The idea is to give access to simple concepts that could alert the data subjects before they decide to use a facial recognition technology, to understand what it means to use sensitive data such as biometric data, how facial recognition works, and to alert them to potential dangers, notably in case of misuse.

Legislators and decision-makers should facilitate public engagement in the development and use of these technologies and in the provision of adequate safeguards to protect fundamental rights at stake while using facial recognition.

II. GUIDELINES FOR DEVELOPERS, MANUFACTURERS AND SERVICE PROVIDERS

This section of the guidelines specifically covers issues related to the development and manufacturing phases of facial recognition technologies. Where developers, manufacturers and service providers process biometric data for their own purposes in the development phase, they will furthermore be concerned by section III of the guidelines on entities using such technology.

1. Data and Algorithms Quality

1.1. Representativeness of the Data Used

Like other applicable legal instruments, Convention 108+ in its Article 5 provides for a data accuracy requirement. Therefore, developers or manufacturers of facial recognition technologies, as actually also entities using facial recognition technologies, will have to take steps to ensure that facial recognition data are accurate. In particular, they will have to avoid mislabelling, thereby sufficiently testing their systems and identifying and eliminating 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 synthetic datasets based on sufficiently diverse photos of men and women, of different skin colours, different morphology, of all ages and from different camera angles. Back-up procedures should be provided for in case of system failure if the physical characteristics do not correspond to the technical standards.

Biometric data unavoidably revealing other sensitive data such as information on a type of illness or physical disability would have to be subject to complementary appropriate safeguards.

1.2. Data Life Duration

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

Each algorithm has a percentage of recognition reliability, both during its development and use. It therefore seems important to date and record this percentage to monitor its evolution. Should its reliability deteriorate, it will be necessary to renew the training photos and therefore ask more recent photos to be provided. This will also enable to protect from the consequences of changes in the shape of faces (due to ageing, to accessories - piercing or other - or to other modifications).

These reliability percentage records could be made easily available to individuals or interested customers or entities using facial recognition technologies, in the form of a dashboard for example, to facilitate their choice of acquisition and deployment of a specific technology.

2. Reliability of the Tools Used

The reliability of the tools used depends on the effectiveness of the algorithm. This effectiveness relies on different factors, among others: false positives, false negatives, performance in different lights, reliability when faces are turned from the camera, impact of face coverings.

The highest possible level of reliability should be ensured, considering that the use of a facial recognition system might result in very significant adverse consequences for the individual.

3. Awareness

Companies developing and selling facial recognition technologies should take reasonable steps - such as making recommendations and providing advice - to help the entities using them to apply transparency and respect for privacy (by providing them with a sample language for their privacy policies or by recommending clear, easy-to-understand signage that indicates that a facial recognition technology is deployed in a specific space).

4. Accountability

Companies developing and selling facial recognition technologies should adopt specific measures to ensure the compliance with data protection principles, such as:

- integrate data protection into the design and architecture of facial recognition products and services, as well as into internal IT systems and integrate the use of dedicated tools including the automatic deletion of raw data after extracting biometric templates;
- offer a certain level of flexibility in the design of these technologies to adjust the technical safeguards according to the principles of purpose limitation, data minimisation and limitation of the duration of storage of data;
- implement an internal review process designed to identify and mitigate the potential impact on the rights and fundamental freedoms before facial recognition technologies are made available;
- integrate a data protection approach into their organisational practices, including assigning dedicated staff, providing privacy training to employees, and conducting data protection impact assessments upon the development or modification of facial recognition products and services.

III. GUIDELINES FOR ENTITIES USING FACIAL RECOGNITION TECHNOLOGIES

Entities[16] have to comply with all the applicable data protection principles and provisions while processing biometric data in their use of facial recognition technologies. Entities using facial recognition technologies have to be able to demonstrate that this use is strictly necessary, and proportionate, in the specific context of their use and that it does not interfere with the rights of the data subjects.

Entities can rely on the exceptions provided in the applicable legislation complying with Article 11 of Convention 108+ (provided for by law, pursuing a specific legitimate aim, respecting the essence of the fundamental rights and freedoms and constituting a necessary and proportionate measure in a democratic society).

Entities using facial recognition technologies have to assure that the voluntary use of the technology will not have an impact on individuals who happen to unintentionally come into contact with it.

[16] In this section of the Guidelines, the term “entities” covers data controllers, and where applicable processors, in both the public and private sectors.

1. Legitimacy of Data Processing and Quality of Data

Entities will rely on different legal basis according to their sectors and to the purposes of the use of facial recognition technologies mentioned in section I.

Transparency and Fairness

As the facial recognition technologies can be used without any intention of or cooperation with data subjects, the transparency and fairness of the processing is of utmost importance and will have to be duly considered by entities using them.

The entities will have to provide all the necessary information about the processing as detailed in Article 8 of Convention 108+.

The factors that will determine whether transparency is ensured include, for example, that the information is 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 or instead, of an integral part of the service itself. They should also be informed on how the collection, use or sharing of facial recognition data is likely to affect them, especially when they concern persons in vulnerable situations. The information provided also has to state which rights and legal remedies the data subjects are entitled to.

Privacy policies on facial recognition or the informational material regarding the technologies should include, in addition to the information provided for in Article 8 of Convention 108+, the following information[17]:

- whether and to which extent facial recognition data can be transmitted to third parties (and where such is the case, information on the identity of the third-party contractual partners receiving the data in the course of providing the product or service);
- the retention, deletion or de-identification of facial recognition data;
- contact points available for individuals to ask questions about the collection, use and sharing of facial recognition data;
- when the collection, use and sharing practices change significantly, entities should update their privacy policy or publicise these changes in light of the context of the change and its impact on individuals.

In case databases are created by law enforcement authorities for identification or verification purposes, the transparency obligation may be proportionally restricted to not prejudice the law enforcement purposes, in accordance with Article 11 of Convention 108+ and subject to its requirements.

When live facial recognition technologies are deployed in an uncontrolled environment, law enforcement authorities can take a layered approach to providing the necessary information to data subjects passing through the uncontrolled environment.

[17] On this point, see the recommendations by the Future Privacy Forum "Privacy Principles for Facial Recognition Technology in Commercial Applications" https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/.

The first layer of the provision of the information will contain readable and intelligible information about the purpose of the processing, the authority using the technology, duration of the processing and perimeter concerned, and will be affixed in the appropriate vicinity of the place where these technologies are deployed.

The second layer of the provision of information will contain all necessary information required according to Article 8 of Convention 108+, to be displayed at the entry points of the place of deployment.

Covert use of live facial recognition technologies by law enforcement authorities could at most be possible if it is strictly necessary and proportionate to prevent imminent and a substantial risk to public security, which should be documented before the covert use.

Purpose Limitation, Data Minimisation and Limited duration of storage

Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes according to Article 5(4) of Convention 108+.

Furthermore, before any subsequent processing, entities will have to consider whether the purposes of the new processing are compatible with the purposes initially defined. Otherwise, the new processing will require a distinct legal basis.

Entities have to comply with the data minimisation principle, which requires that only the required information be processed, and not all information available to the entities.

Entities also have to set a retention period, which cannot be longer than what is necessary for the specific purpose of the processing, and ensure the deletion of biometric templates upon completion of that purpose. While determining the retention period, the biometric nature of the personal data must be taken into account.

In the deployment of live facial recognition technologies, entities furthermore have to ensure that different storage limitation periods apply to the different phases of the processing:

- if there is no match of the biometric templates, the biometric template of individuals passing through an uncontrolled environment cannot be retained and have to be automatically deleted;

- if there is a match, the biometric templates can be retained for a strictly limited time provided by law with necessary safeguards and match reports including personal data can also be retained for a limited time;

- and in any case, the watchlist and biometric templates have to be deleted upon completion of the purpose for which live facial recognition technologies were deployed.

Accuracy

Entities have to ensure that the biometric templates and digital images are accurate and updated. For instance, the quality of images and biometric templates inserted in watchlists must be checked to prevent potential false matches since low quality images can cause an increase in the number of errors. This is directly linked to the sources of the images compiled in the watchlist, which require strict respect of the data protection principles such as the principle of purpose limitation.

In case of false matches, the entities will take all reasonable steps to correct future occurrences and ensure the accuracy of digital images and biometric templates.

2. Data Security

Any failure in data security may have particularly severe consequences for data subjects, as unauthorised disclosure of such sensitive data cannot be corrected.

Strong security measures, both at the technical and organisational levels, should therefore be implemented to protect facial recognition data and image sets against the loss and unauthorised access or use of the data during all the processing stages, be it the collection, transmission and storage.

Entities will take measures to prevent technology-specific attacks, including presentation attacks and morphing attacks.

Any breach of the security of the data which may seriously interfere with the rights and fundamental freedoms of data subjects has to 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. They should also be proportionate to the sensitivity of the data, to the context in which a specific facial recognition technology is used and its purposes, to the likelihood of harm to individuals and other relevant factors.

Strict retention and disposal practices - through safe procedures - for facial recognition data, with the shortest possible retention periods, also contribute to reducing security exposures.

3. Accountability

Entities will take all appropriate measures to comply with their obligations and to be able to demonstrate that the data processing under their control complies with those, as foreseen in Article 10 of Convention 108+.

The following organisational measures have to be taken into account by entities using facial recognition technologies:

- implementation of transparent policies, procedures and practices to ensure that the protection of the rights of data subjects underlie their use of facial recognition technologies;

- publishing transparency reports about the concrete use of facial recognition technologies;

- setting up and delivery of training programmes and audit procedures for those in charge of processing facial recognition data;

- setting up of internal review committees to assess and approve any processing involving facial recognition data;

- contractual extension to third-party service providers, business partners or other entities using facial recognition technology of the applicable requirements (and denial of the access to third parties that would not comply with them);

- in the public sector: prior evaluation constraints in public procurement procedures involving suppliers of facial recognition tools, assessment of minimum levels of performance in terms of accuracy, especially where law enforcement purposes are concerned.

Entities will take the necessary technical measures to ensure the quality of biometric data by following internationally agreed technical standards, depending on the context of their uses.

Entities using facial recognition technologies should ensure that human operators continue to play a decisive role in the actions taken upon the results of these technologies. Entities using these technologies should take organisational measures to oversee the human operators taking decisions which can have a significant impact on individuals.

3.1. Data Protection Impact Assessment

Entities using facial recognition technologies have to carry out impact assessments before the processing as the use of these technologies involves biometric data processing and presents high risks to the fundamental rights of data subjects.

During the preparation of the impact assessment, the entities will not only recognise the risks arising from the potential processing but also consider the necessary mitigating measures to tackle these risks by taking the necessary technical and organisational measures. In this assessment, they will explain, among other things:

- the lawfulness of the use of these technologies;
- which fundamental rights are at stake in the biometric processing;
- the vulnerability of data subjects;
- how these risks can be effectively mitigated.

Specifically, while considering the deployment of facial recognition technologies in uncontrolled environments, law enforcement authorities will have to:

- assess and explain in their assessment the strict necessity and proportionality of the deployment of these technologies;
- address the risk to different fundamental rights, including data protection, privacy freedom of expression, freedom of assembly, freedom of movement or anti-discrimination, depending on the potential uses in different places.

The impact assessment could be carried out either by entities themselves or 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.

During the preparation of the impact assessment, entities have to engage with stakeholders, including affected individuals, to assess the potential impact from their perspective.

Such impact assessments have to be carried out at regular intervals.

If a risk is identified, the entities concerned should be able to refer to any existing ethics committees, and to the competent supervisory authorities to examine the potential risks.

After completion of this assessment, entities should publish it to receive views from the public on the potential deployment of facial recognition technologies.

3.2. Data Protection by Design

Data protection by design covers the whole value chain of processing by facial recognition technologies. Entities using these technologies for identification or verification purposes have to ensure that the products or services they are using are designed to process biometric data in compliance with the principles of purpose limitation, data minimisation and limited duration of the storage, and integrate all other necessary safeguards in the technologies.

When entities set the technical features of these technologies, they implement these principles into their design, to ensure that their deployment will uphold the right to data protection.

4. Ethical Framework

In addition to the respect of legal obligations, giving an ethical framework to the use of this technology is also crucial, in particular with regard to higher risks inherent to the uses of facial recognition technologies in certain sectors. This could take the form of independent ethics advisory boards that could be consulted before and during lengthier deployments, carry out audits and publish the results of their research to complement or endorse an entity's accountability. Expressly ethical considerations may help strike an appropriate balance between competing interests in a demonstrably fair way.[18]

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

On this topic, whistle-blowers also have an important role to play, and employees of entities using these solutions should be able to benefit from an appropriate protection status, as provided for in particular in Recommendation (2014)7 of the Committee of Ministers on the protection of whistle-blowers.

IV. RIGHTS OF DATA SUBJECTS

As facial recognition is based on the processing of personal data, all the rights provided for in Article 9 of Convention 108+ are guaranteed to the data subjects, such as notably the right of information, the right of access, the right to obtain knowledge of the reasoning, the right to object, the right to rectification.

These rights can be restricted but only when such restriction is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for specific legitimate purposes (such as law enforcement purposes), according to Article 11 of Convention 108+.

In the case of limitation of the rights of data subjects, law enforcement authorities have to inform data subjects *inter alia* about their right to lodge a complaint with supervisory authorities, and about their general right to remedy.

In the case of false matches, data subjects can request rectification to avoid further/repetitive false matches.

[18] See the Guidelines on Artificial intelligence and data protection, available at https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

Where the use of facial recognition technologies is intended to enable a decision to be taken solely based on automated processing which would significantly affect the data subject, the latter must, in particular, be entitled not to have such processing carried out without his or her views being taken into account.

In the deployment of live facial recognition technologies, if human operators solely act upon results of these technologies, it can be considered as solely automated decision making which would significantly affect the data subject due to the consequences of possible false matches. The data subject can thus request, according to Article 9(1)(a) of Convention 108+, that his or her views be taken into account.