Guidelines on facial recognition

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data

Convention 108

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Guidelines on facial recognition

Adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)

Council of Europe

French edition:

Lignes directrices sur la reconnaissance faciale

Cover photo: Shutterstock

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Printed at the Council of Europe

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 Automatic 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 shall only be covered by the definition of biometric data when they are processed through a specific technical means 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 may be found to be contrary to the right to respect for private life.[3]

Integrating facial recognition technologies into 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 use of these technologies does not always require the awareness or co-operation of the individuals whose biometric data are processed in this way. This is the case, for instance, with the possibility to access 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 personal 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.

---

1. Consolidated version of modernised Convention 108 available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168076c65bf.
2. Paragraph 59 of the Explanatory Report to Convention 108+, available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.
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.

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

In these guidelines "law enforcement purposes" means 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 more widely as meaning the public prosecution 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+.

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.
5. Law enforcement purposes corresponds to "police purposes" in the "Practical guide on the use of personal data in the police sector" (T-PD(2018)01), by the Consultative Committee of Convention 108, 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 shall be interpreted as excluding or limiting the provisions of the European Convention on Human Rights (ETS No. 5).

Guidelines for legislators and decision makers

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 if 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.

In some legislation,[7] the prohibition of such processing is a rule and its implementation is allowed only by way of exception, in certain specific cases (for example, with the explicit consent of individuals, to protect their vital interests or when the processing is necessary for reasons of overriding public interest), and subject to safeguards that are appropriate to the risks involved.

The necessity for 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 address, for each different use, in particular:

- a detailed explanation of the specific use and the intended 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.

7. See Article 9 of the European Union's General Data Protection Regulation (GDPR, Regulation (EU) 2016/679 of 27 April 2016).
8. The accuracy of the algorithm can be expressed through an assessment of false positive or false negative errors produced by the software.

Strict limitation of certain uses by law

The level of intrusiveness of facial recognition and related infringement of the rights to privacy and data protection will vary according to the particular use and there will be cases where domestic law will strictly limit or even completely prohibit its use where that decision has been reached through the democratic process.

The use of live facial recognition technologies in uncontrolled environments,[9] in light of its intrusiveness on the right to privacy and the dignity of individuals, coupled with the risk of an adverse impact on other human rights and fundamental freedoms,[10] should be subject to a democratic debate and the possibility of a moratorium pending a full 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 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 using facial recognition technologies to arguably detect personality traits, inner feelings, mental health or workers' engagement from facial images. Linking recognition of affect, for instance, to the hiring of staff, or access to insurance or education, may pose risks of great concern, both at individual and societal levels, and should be prohibited.

Legal basis in different contexts

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

- the different phases of the use of facial recognition technologies, including the phases of database creation and deployment;
- the sectors in which these technologies are used;

9. The notion of "uncontrolled environment" covers places freely accessible to individuals, which they can also pass through, including public and quasi-public spaces such as shopping centres, hospitals, or schools.
10. 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.
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 to identify or classify human emotion.

- the intrusiveness of certain types of facial recognition technologies, such as live or non-live facial recognition technologies, while providing clear guidance on their lawfulness.

Integrating digital images into 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 the processing of sensitive data, it is necessary to ensure the possible legal basis considered below, which varies according to the different sectors and uses.

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

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

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

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

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.

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

Law enforcement authorities

Biometric data processing using 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 may provide for different necessity and proportionality tests depending on whether the purpose is verification or identification, taking into account the potential risks to fundamental rights and as long as individuals' images are lawfully collected.

For identification purposes, strict necessity and proportionality shall be observed both in the setting up of the database (watch list) 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 (watch lists) for specific, legitimate and explicit law enforcement purposes (for example, suspicion of severe offences or a 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.

Other public authorities

Legislators and decision makers lay down specific rules for biometric processing using facial recognition technologies for other grounds of substantial public interest by public authorities that are not pursuing law enforcement purposes.

14. The notion of a "controlled environment" covers the cases in which the biometric systems can only be used with the person's participation.

Laws can provide for different necessity and proportionality tests depending on whether the purpose is verification or identification, taking account 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 a legal basis will include the strict necessity and proportionality of their use and will take into consideration the vulnerability of the data subjects and the nature of the environment in which 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 as strictly necessary and proportionate where alternative, less intrusive, mechanisms exist.

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 tasks similar to those of 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 consent by data subjects, the use of facial recognition technologies can only take place in controlled environments for verification, authentication or categorisation[15] purposes.

Depending on the purpose, particular attention must be paid to the quality of the data subject's explicit consent when it forms 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. If the alternative to facial recognition technology seems too long or complicated in comparison, the choice cannot be considered genuine.

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".

If consent is given for a specific purpose, personal data should not be processed in a way that is incompatible with that 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 centres, 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 explicit consent.

Necessary involvement of supervisory authorities

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

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

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

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

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

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 activities.

The idea is to give access to simple concepts that can alert data subjects before they decide to use facial recognition technology, to help them 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 the event of misuse.

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

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.

Quality of data and algorithms

Representativeness of the data used

Like other applicable legal instruments, Article 5 of Convention 108+ provides for a data accuracy requirement. Therefore, developers or manufacturers of facial recognition technologies, as actually also entities using such technologies, shall 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 used, the algorithms will have to be developed using synthetic datasets based on photos of a sufficient diversity of men and women, of different skin colours, different morphology, of all ages and taken 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 that would unavoidably reveal other sensitive data, such as information on a type of illness or physical disability, shall be subject to appropriate additional safeguards.

Data life duration

A facial recognition system requires the 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 its use. It is therefore important to date and record this percentage to monitor its evolution. Should its reliability deteriorate, it will be necessary to renew the photos used to train the system and therefore to obtain more recent ones. This will also protect from the consequences of changes in the shape of the face (due to ageing, accessories – piercing or other – or other modifications).

These percentage reliability 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 in the acquisition and deployment of a specific technology.

Reliability of the tools used

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

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

Awareness

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

Accountability

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

- integrating data protection into the design and architecture of facial recognition products and services, as well as into internal information technology systems, and integrating the use of dedicated tools including the automatic deletion of raw data after extracting biometric templates;
- offering 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 data storage;
- implementing an internal review process designed to identify and mitigate the potential impact on rights and fundamental freedoms before facial recognition technologies are made available;
- integrating a data protection approach into their organisational practices, including assigning dedicated staff, providing training to employees on respect for privacy, and conducting data protection impact assessments during the development or modification of facial recognition products and services.

Guidelines for entities using facial recognition technologies

Entities[16] shall 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+ (which states that any exception shall be provided for by law, pursue a specific legitimate aim, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society).

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

Legitimacy of data processing and quality of data

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

Transparency and fairness

As facial recognition technologies can be used without the co-operation of data subjects or their intent, the transparency and fairness of the processing are of the utmost importance and will have to be duly considered by entities using such technologies.

16. In this section of the guidelines, the term "entities" covers data controllers and, where applicable, data processors, in both the public and private sectors.

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, the information given to individuals, the context of the collection, reasonable expectations as to how the data will be used, and whether facial recognition is merely a feature of a product or service or rather an integral part of the service itself. Individuals should also be informed of how the collection, use or sharing of facial recognition data is likely to affect them, especially when the data concern persons in vulnerable situations. The information provided shall also state which rights and legal remedies the data subjects are entitled to.

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

- whether and to what 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;
- the 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 the light of the context of the change and its impact on individuals.

In the event that databases are created by law enforcement authorities for identification or verification purposes, the transparency obligation may be proportionally restricted so as not to 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 may 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 of Privacy Forum "Privacy principles for facial recognition technology in commercial applications", available at 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, the duration of the processing and perimeter concerned, and will be affixed in the 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 in order to prevent an imminent and substantial risk to public safety 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 paragraph 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. If this is not the case, the new processing will require a distinct legal basis.

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

Entities also have to set a retention period, which cannot exceed what is necessary for the specific purpose of the processing and ensure the deletion of biometric templates once that purpose has been reached. When determining the retention period, the biometric nature of the personal data shall be taken into account.

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

- if there is no match with 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 may be retained for a strictly limited time provided by law, with necessary safeguards; match reports including personal data may also be retained for a limited time;
- in all case, the watch list and biometric templates have to be deleted once the purpose for which live facial recognition technologies were deployed has been reached.

Accuracy

Entities have to ensure that the biometric templates and digital images are accurate and kept up to date. For instance, the quality of images and biometric templates inserted in watch lists shall 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 watch list, which require strict respect of the data protection principles such as the principle of purpose limitation.

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

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 or storage.

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

Any breach of the security of 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 to its purposes, to the likelihood of harm to individuals and other relevant factors.

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

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 obligations, 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 underpin their use of facial recognition technologies;
- publication of transparency reports about the specific use of facial recognition technologies;
- the setting up and delivery of training programmes and audit procedures for those in charge of processing facial recognition data;
- the setting up of internal review committees to assess and approve any processing involving facial recognition data;
- the contractual extension to third-party service providers, business partners or other entities using facial recognition technology, of the applicable requirements (and denial of 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 in which they are used.

Entities using facial recognition technologies should ensure that human operators continue to play a decisive role in the actions taken on the basis of 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.

Data protection impact assessment

Entities using facial recognition technologies have to carry out impact assessments prior to the processing, as the use of these technologies involves the processing of biometric data and presents high risks for 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 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 various fundamental rights, including the rights to data protection, privacy, freedom of expression, freedom of assembly and freedom of movement, or the prohibition of discrimination, depending on the potential uses in different locations.

The impact assessment may be carried out either by entities themselves, by an independent monitoring body or by an auditor with relevant expertise to help discover, 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 committee and to the competent supervisory authorities to examine the potential risks.

After completion, the assessment should be published in order to obtain the views of the public on the potential deployment of facial recognition technologies.

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 limitation of the duration of storage, and integrate all other necessary safeguards into the technologies.

When defining the technical features of these technologies, entities shall incorporate these principles into their design in order to ensure that their deployment will uphold the right to data protection.

Ethical framework

In addition to respecting legal obligations, it is also crucial to give an ethical framework to the use of this technology, in particular with regard to the higher risks inherent in the use 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 deployment of the technology, 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 technologies should be able to benefit from an appropriate protective status, as provided for in particular in Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistle-blowers.

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.

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, in particular, the right to information, the right of access, the right to obtain knowledge of the underlying reasoning, the right to object and the right to rectification.

These rights may 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 their general right to remedy.

In the case of false matches, data subjects may request rectification to avoid further false matches.

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 shall, 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 act solely on the basis of the results provided by these technologies, this can be considered as solely automated decision making that could significantly affect the data subject due to the consequences of possible false matches. The data subject can thus request, according to Article 9 paragraph 1.*a*, of Convention 108+, that his or her views be taken into account.

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. Their uses are varied and numerous, and some may seriously infringe the rights of data subjects, notably as facial recognition is a biometric technology. To prevent such infringements, the Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data shall ensure 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 systems 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, including the right to protection of personal data, of any person.

PREMS 020221

www.coe.int/dataprotection

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE