Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
As the OSTP embarks on its review of biometric technologies, we would like to highlight facial recognition as a specific type of biometric technology used for identify verification, identification of individuals and groups, and inference of attributes (including protected status). Given the pervasiveness of facial recognition technology as well as the grave risks posed by its unfettered proliferation and the lack of regulatory frameworks to govern its use and development in the United States, we have conducted a global survey of relevant regulations to inform the OSTP’s request for information. This submission includes an analysis of principles and regulatory frameworks elaborated by the United Nations, the European Commission, and national frameworks in Argentina, Australia, Brazil, India, Japan, México, South Africa, and the UK. The specific details of various legislation and regulation is included as an appendix.

As a scholar-practitioner working at the nexus of media, technology, and human rights for the past two decades, most recently as Director of Advocacy at the Committee to Protect Journalists and now as a Fellow at ITLP, I have seen first-hand the impact that new surveillance technologies can have on a wide range of human and civil rights, often affecting the most vulnerable and marginalized populations as well as those on the frontlines of promoting and protecting these rights, such as journalists and human rights defenders.

Similarly, technologies and legal frameworks developed in the United States have profound implications not just on its citizens, but on populations around the world. Therefore, we urge the OSTP to adopt the guidance provided by international standards and learn from other countries that have already adopted legal frameworks to govern the development and deployment of facial recognition technologies.

At the very core is the State obligation to protect human rights and for States and the private sector to comply with the principles of legality, necessity, and proportionality. Comprehensive human rights due diligence, increase transparency by adequately informing the public and affected individuals, and enabling independent and external auditing of these automated systems.

The international standards promulgated by the United Nations and the European Commission require that the processing of biometric data in facial recognition systems be authorized on an appropriate legal basis that complies with the general principles of legality, necessity and proportionality. To this end, States must address detailed explanations of the specific use and purpose for its deployment that takes into consideration the minimum reliability and accuracy of
the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria and the traceability of the process (among other factors).

Other important aspects to take into consideration in the design and use of this technology involve having data protection systems by default; processors that provide sufficient safeguards and act only on instructions from the data controller; maintenance of a record of processing activities; and a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

<table>
<thead>
<tr>
<th>Country</th>
<th>Key Principles for the U.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Nations</td>
<td>Processing of personal data must be authorized by an appropriate <a href="#">legal basis</a>, complying with the general principles of <a href="#">legality</a>, <a href="#">necessity</a> and <a href="#">proportionality</a>.</td>
</tr>
<tr>
<td>European Union</td>
<td>Processing personal data must meet the <strong>proportionality</strong> and <strong>necessity</strong> principles, the principle of processing personal data on <strong>valid legal basis</strong>.</td>
</tr>
<tr>
<td></td>
<td>In determining proportionality and necessity, the legal framework should address notably: the detailed explanation of the specific use and the purpose; the minimum reliability and accuracy of the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria; the traceability of the process; the safeguards.</td>
</tr>
<tr>
<td></td>
<td>Different tests of necessity and proportionality can be legally addressed “depending on whether the purpose is <a href="#">verification</a> or <a href="#">identification</a>, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected.”</td>
</tr>
<tr>
<td>Argentina</td>
<td>N/A</td>
</tr>
<tr>
<td>Brazil</td>
<td>Processing of personal data on security and public safety purposes “shall be governed by specific legislation, which shall provide proportional and strictly necessary measures for fulfilling the public interest, subject to due legal process”</td>
</tr>
<tr>
<td>Mexico</td>
<td>Any responsible party that intends to process sensitive personal data must carry out an “impact assessment” on the protection of personal data, and submit it for review by the relevant authorities</td>
</tr>
<tr>
<td>South Africa</td>
<td>Personal information must be processed lawfully, and a reasonable manner that does not infringe the privacy of the data subject. Personal information may only be processed if the purpose for processing is adequate, relevant, and not excessive.</td>
</tr>
</tbody>
</table>
Personal information must be **collected directly** from the data subject unless certain exceptions are met.

<table>
<thead>
<tr>
<th>Country</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>N/A</td>
</tr>
<tr>
<td>India</td>
<td>The Supreme Court of India has clarified that any law that encroached upon the right to privacy would be subject to constitutional scrutiny and would have to meet the three-fold requirement for: <strong>Legality</strong>, <strong>Necessity</strong>, and <strong>Proportionality</strong>.</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>N/A</td>
</tr>
<tr>
<td>Australia</td>
<td>Collecting sensitive information about an individual must receive <strong>consent</strong> and the information is <strong>reasonably necessary</strong></td>
</tr>
</tbody>
</table>
APPENDIX: LEGAL ANALYSIS OF

FACIAL RECOGNITION TECHNOLOGY GOVERNANCE GLOBALLY

1. Facial recognition under United Nations standards

The right to privacy is stipulated in Article 12 of the Universal Declaration of Human Rights\(^1\) and in Article 17 of International Covenant on Civil and Political Rights\(^2\). On the report *The right to privacy in digital age*\(^3\), the OHCHR highlights that advances in the field of biometric recognition technology have led to its increasing use by law enforcement and national security agencies. What raises serious concerns is that these processes are deployed by authorities across the globe and increasingly carried out in real time and remotely.\(^4\) “Some of these concerns reflect the problems associated with predictive tools, including the possibility of erroneous identification of individuals and disproportionate impacts on members of certain groups. Moreover, facial recognition technology can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics.”

Furthermore, remote biometric recognition directly impacts on the right to privacy, as it reveals unique characteristics and key attributes of personality. This function has led many States authority to “systematically identity and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement.”\(^5\)

Also, this type of artificial intelligence has served a security purpose to decide whether people’s emotional and mental state from their facial expressions and other “predictive biometrics” deduced from the system constitute a security threat.\(^6\) In this sense, “facial emotional recognition

\(^1\) Article 12 states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.” [https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx](https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx)

\(^2\) Article 17 states that “(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.” [https://www.un.org/en/about-us/universal-declaration-of-human-rights](https://www.un.org/en/about-us/universal-declaration-of-human-rights)


\(^4\) Paragraph 25 of the Report “The right to privacy in the digital age”.

\(^5\) Paragraph 27 of the Report “The right to privacy in the digital age”.

\(^6\) Paragraph 28 of the Report “The right to privacy in the digital age”.
systems operate on the premise that it is possible to automatically and systematically infer the emotional state of human beings from their facial expressions, which lacks a solid scientific basis.”

In the report, the High Commissioner recommends States to impose a moratorium on the use of biometric technologies in public spaces, at least until authorities can demonstrate that there are no significant issues with accuracy or discriminatory impacts and that these AI systems comply with robust privacy and data protection standards.7

The Special Rapporteur on freedom of opinion and expression stated that when these technologies are used for surveillance purposes, they can directly impact on human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation.8 In this regard, the Special Rapporteur urged States to adopt national measures that are consistent with international human rights standards and that serve to protect individuals from unlawful surveillance. In particular, he urged “development of public mechanisms for approval and oversight of surveillance technologies; strengthening of export controls; and assurance of legal tools of redress.”9

The Special Rapporteur on freedom of opinion also expressed that the use of these technologies is marketed and supported by private companies, who appear to be operating without constraint.10 Therefore, “it is critical that companies themselves adhere to their human rights responsibilities, including by disclosing their transfers, conducting rigorous human rights impact assessments, and avoiding transfers to States unable to guarantee their compliance with their human rights obligations.”

In this regard, the High Commissioner expressed that both States and businesses “should ensure that comprehensive human rights due diligence is conducted when AI systems are acquired, developed, deployed and operated, as well as before big data held about individuals are shared or used. As well as resourcing and leading such processes, States may also require or otherwise incentivize companies to conduct comprehensive human rights due diligence.”11

The report of the High Commissioner also recommends States to dramatically increase the transparency of their use of AI, including by adequately informing the public and affected individuals and enabling independent and external auditing of automated systems. The more likely

---

9 Id. Supra.
11 Paragraph 48 of the Report “The right to privacy in the digital age”. 
and serious the potential or actual human rights impacts linked to the use of AI are, the more transparency is needed.\textsuperscript{12}

With respect to the use of facial recognition and surveillance technologies to track and control specific demographic groups, the Committee on the Elimination of Racial Discrimination raises concern when profiling people based on race, color, national or ethnic origin or gender, since it has been demonstrated that the accuracy of facial recognition technology may differ depending on the color, ethnicity or gender of the persons assessed, which may lead to discrimination.\textsuperscript{13}

Therefore, States should carefully assess the potential human rights impact prior to employing facial recognition technology, which can lead to misidentification owing to a lack of representation in data collection. “Before national deployment, States should consider a pilot period under the supervision of an independent oversight body that is inclusive of individuals who reflect the diverse composition of the population, to mitigate against any potential instances of misidentification and profiling based on skin color.”

2. Facial recognition under European Commission standards

The European Commission is based on the rule of law.\textsuperscript{14} This means that every action taken by the EU is founded on treaties that are binding for EU member countries. Under these treaties, EU institutions can adopt legislation, which the member countries then implement.\textsuperscript{15} The European Commission is the EU’s politically independent executive arm. It is alone responsible for drawing up proposals for new European legislation.\textsuperscript{16} The Council of Europe is the continent's leading human rights organization. It includes 47 member states, 28 of which are members of the European Union.\textsuperscript{17} In relation to the conventions adopted by the Council of Europe, their legal existence is owed by the consent of those member States that sign and ratify them.

- **Convention for the protection of individuals with regard to the processing of personal data - Convention 108 +**

The Convention for the protection of individuals with regard to the processing of personal data (Convention 108+)\textsuperscript{18} is the only legal binding multilateral instrument which protects individuals with regard to the processing of their personal data, thereby contributing

---

\textsuperscript{12} Paragraph 55 of the Report “The right to privacy in the digital age”.

\textsuperscript{13} Committee on the Elimination of Racial Discrimination. *General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials.* December 17, 2020.  

\textsuperscript{14} https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

\textsuperscript{15} https://european-union.europa.eu/principles-countries-history/principles-and-values/founding-agreements_en


\textsuperscript{17} https://www.coe.int/en/web/yerevan/the-coe/about-coe

to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy. “Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.”

This Convention stipulates core protection principles when processing personal data, related to the legitimacy of data processing, “such as the proportionality and necessity, the principle of processing personal data on valid legal basis, for explicit, specified legitimate purposes and to the quality of data (Article 5), special categories of data (Article 6), data security (Article 7), transparency (Article 8), accountability measures such as privacy by design, data protection impact assessments (Article 10), and new generation of data subject’s rights such as the right not to be subject to a decision based solely on automated processing, right to know the reasoning of the processing, right to object (Article 9).”

Regarding special categories of data, Article 6 of the Convention states that biometric data uniquely identifying a person “shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention”, and that “such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.”

Under this provision, processing of biometric data is also considered sensitive when it is precisely used to uniquely identify the data subject, and therefore has the potential to adversely affect data subjects’ rights when it is processed for specific information it reveals.

In order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes needs to be accompanied by “appropriate safeguards”, such as “a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted”.  

As appropriate safeguards, necessity has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects. This legal framework should, according to each different use, address notably: the detailed explanation of the specific use and the purpose;

---


20 Submission by the Data Protection Unit of the Council of Europe to the OHCHR for the preparation of the thematic report on "the right to privacy in the digital age"

21 Explanatory Report on Convention 108+
the minimum reliability and accuracy of the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria; the traceability of the process; the safeguards.\(^{22}\)

**Guidelines for facial recognition technologies**

In January 2021, the Council of Europe’s Committee of Convention 108 drafted guidelines for facial recognition technologies.\(^{23}\) The guidance was drawn up for government and private entities, as well as facial recognition developers, manufacturers and service providers. The Guidelines call for strict rules to avoid the significant risks to privacy and data protection posed by the increasing use of facial recognition technologies.\(^{24}\)

**Principal guidelines for legislators and decision makers:**

1. **Strict Limitation by Law of Certain Uses**

   According to the Guidelines, the use of live facial recognition technologies in uncontrolled environments – as places freely accessible to individuals – 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, 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 color, 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.

   Similarly, affect recognition (attempted to identify or classify human emotions) 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, or education may pose risks of great concern, both at the individual and societal levels and should be prohibited.

1.1. **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 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).

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. Use of Facial Recognition Technologies in the Public Sector

Different tests of necessity and proportionality can be legally addressed “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.”

Biometric data processed by facial recognition technologies for identification purposes in a controlled or uncontrolled environment should be generally restricted to law enforcement purposes, and it should be carried out solely by the competent authorities in the security domain.

For these purposes, a strict test of both necessity and proportionality must be observed in the design, deployment, and use of facial recognition technologies in an uncontrolled environment. In this sense, clear parameters should be followed by law enforcement authorities when creating databases for specific, legitimate, and explicit law enforcement purposes.

Furthermore, given the intrusive nature of these technologies, in the deployment phase of live facial recognition technologies, laws should ensure that enforcement authorities demonstrate that factors such as location and timing justify the strict necessity and proportionality for its use.

In cases other than law enforcement, legislators and decision-makers must consider an explicit and precise legal basis for safeguards in the processing of biometric data. For verification purposes, the necessity and proportionality test should take into account the vulnerability of data subjects and the nature of the environment in which these technologies are being deployed.

1.3. Use of Facial Recognition Technologies in the Private Sector

The use of facial recognition technologies by private entities, except for private entities authorized 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 categorization purposes. Private entities shall not deploy facial recognition technologies in uncontrolled environments, especially to identify persons of interest, for marketing purposes or for private security purposes.

- **GDPR and Facial Recognition Technology**

  Under the GDPR, data collected by FRT is classified as biometric data, which is prohibited to be processed for identification purposes. However, according to Article 9(2), there are some exceptions:

  1. The data subject has given explicit consent to the personal data processing; or
  2. The data processing is necessary for reasons of significant public interest. Article 9(2)(g).

  The provision implies that the use of FRT is only possible when legal consent is obtained in accordance with the GDPR. Companies looking to use FRT should establish definitive legal grounds prior to the technology implementation.

  Also, to establish the necessity for processing biometric data to identify a person, the GDPR requires “a systematic description of the envisaged processing operations and the purposes of the processing” and “an assessment of the necessity and proportionality of the processing operations in relation to the purposes.” *See* Article 35.

  Furthermore, before data processing, one has to collect the data. According to the Article 5(1)(a) of the GDPR, “it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.”

  Finally, in processing the data, one has to abide by the “principle of data security.” That is, the data must be processed in a manner that ensures appropriate security for personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (Article 5(1)(f) GDPR). Further, the principle can also be found in Article 32 of the GDPR which prescribes that the controller and processor should implement proportionate technical and organizational measures to prevent that personal data is disclosed to, or accessed by, unauthorized persons or organs.²⁵

- **The AI Act (a draft law currently being negotiated in the European Union)**

---

The European Commission presented the Artificial Intelligence Act, which seeks to establish high standards for the regulation of the use of AI in Europe. It sets out core horizontal rules for the development, trade and use of AI driven products, services and systems within the EU, and it applies to all industries (the legislation is not sectoral in nature).

The Act introduces a sophisticated product safety regime that is constructed around a set of 4 risk categories. It stipulates that a mandatory CE-marking procedure is a prerequisite for market entrance and certification of High-Risk AI systems. It combines a risk-based approach (based on the pyramid of criticality) with a layered enforcement mechanism. The strictness of the rules is directly proportional to the nature of the risk. And it stipulates that there must be a ban on applications that have unacceptable risk. Fines for violating the rules can be up to 6 percent of the global turnover for companies.

Objectives:

1. ensure that AI systems are safe and respect existing law on fundamental rights and Union values;
2. ensure legal certainty to facilitate investment and innovation in AI;
3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation

Unacceptable Risk AI systems are any AI systems that are considered a clear threat to the safety, livelihoods and rights of people. This includes AI applications that manipulate human behavior to circumvent users’ free will and systems that allow ‘social scoring’ by governments.

High risk AI systems are AI applications used in: a) critical infrastructure (transport), b) essential private and public services, c) law enforcement, d) migration asylum and border control management, e) administration of justice and democratic processes, (among other designated High Risk AI uses)

The AI Act imposes strong obligations on these High Risk AI systems prior to market deployment:

a) Adequate risk assessment and mitigation systems
b) High Quality of datasets
c) Logging of activity to ensure traceability of results
d) Detailed documentation (both of information and purpose) to authorities for compliance
e) Appropriate human oversight to minimize risk
f) High level of robustness, security, and accuracy

All remote biometric identification systems are considered high risk and subject to strict requirements. And the Act does stipulate a prohibition in principle of the live use of such identification systems (AFR) in publicly accessible spaces for law enforcement purposes. There are however, limited exceptions such as in the case of a missing child, or to prevent a specific
and imminent terrorist threat, or to identify or prosecute a perpetrator or suspect of a serious criminal offence. It is required however, that a judicial or other independent body authorize these searches, and set appropriate limits in time, geographical search and the databases searched.

- **The European Parliament's Resolution (that strongly recommended bans on multiple use cases of AFR technology, specially in the context of law enforcement and judicial use. 2020/2016(INI))**

The European Parliament called for a ban on the police use of facial recognition technology in public places, and on predictive policing. In an EU resolution on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters, the Parliament adopted by 377 votes to 248 (with 62 abstentions). It outlined the important considerations that stand to be violated as a result of using AI for law enforcement use. The voting record on this non-binding resolution is useful as it’s a useful way to predict the nature of the negotiations that are liable to (Salient points among the 36 operative sections of the Resolution are given below):

1) **Respect for Fundamental Rights:** The EU Legal Framework on data protection and privacy must be fully respected and should form a basis for any future regulation of AI for law enforcement and judicial use, and when AI solutions stand to be incompatible with fundamental rights, they ought to be prohibited. (AI solutions need to respect the principles of human dignity, non-discrimination, freedom of movement, the presumption of innocence, and the right of defense, and other salient rights in accordance with the Charter and the European Convention on Human Rights)

2) **Risk of discrimination:** The EU Parliament called for algorithmic explainability, transparency, traceability, and verification as a necessary part of the oversight mechanism, to ensure that the development, deployment and use of AI systems for the judiciary and law enforcement comply with fundamental rights, and are trusted by citizens, as well as in order to ensure that results generated by AI algorithms can be rendered intelligible to users and to those subject to these systems, and that there is transparency on the source data and how the system arrived at a certain conclusion

3) **Mandatory Impact Assessments:** Calls for a compulsory fundamental rights impact assessment to be conducted prior to the implementation or deployment of any AI systems for law enforcement or the judiciary, in order to assess any potential risks to fundamental rights; recalls that the prior data protection impact assessment is mandatory for any type of processing, in particular, using new technologies, that is likely to result in a high risk to the rights and freedoms of natural persons and is of the opinion that this is the case for most AI technologies in the area of law enforcement and judiciary

4) **Stresses that only robust European AI governance with independent evaluation can enable the necessary operationalization of fundamental rights principles; calls for periodic mandatory auditing of all AI systems used by law enforcement and the judiciary where there is the potential**
to significantly affect the lives of individuals, by an independent authority, to test and evaluate algorithmic systems, their context, purpose, accuracy, performance and scale, and, once they are in operation, in order to detect, investigate, diagnose and rectify any unwanted and adverse effects and to ensure the AI systems are performing as intended

5) Supports the recommendations of the **Commission’s High-Level Expert Group on AI** that advocated for a ban on AI-enabled mass scale scoring of individuals

6) The resolution also expressed great concern over the use of private facial recognition databases by law enforcement actors and intelligence services such as Clearview AI. It additionally called on Member States to oblige law enforcement actors to disclose whether they are using Clearview technology or other equivalent technologies from other providers. It referenced another opinion of the **European Data Protection Board** that the use of services such as Clearview by law enforcement authorities would likely be inconsistent with the EU data protection regime.

- **Legal Provisions within the broader context of the EU’s multi-level framework** (specifically, the Charter of fundamental rights, and the Law Enforcement Directive)

The use of FRT implies the processing of data for the purpose of identification. It’s use by public authorities will entail an infringement of Art. 8 (Charter of fundamental rights of the European Union) as it violates the right to data protection (the use of the technology will have to comply with Art. 8(2)). It also has the capacity to interfere with the right to private life under article 7 CFR.

The **Law Enforcement Directive** is a piece of EU Legislation that is parallel to GDPR, and it deals with the processing of personal data by data controllers for ‘law enforcement purposes’ - which typically falls outside the scope of GDPR. It effectively provides rules on the protection of natural persons (w.r.t. processing of personal data by competent authorities) for the specific purpose of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the protection against threats to public security and its prevention. Several obligations under the Law Enforcement Directive are identical to those under GDPR.

Some of the important obligations include:

1) Implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive (Art. 19)
2) Implement data protection by design and by default (Art. 20)
3) Use processors that provide sufficient guarantees and act only on instructions from the data controller (Art. 22)
4) Maintain a record of processing activities (Art. 24)
5) Implement logging measures (Art. 25)
6) Cooperate with the supervisory authority in performance of its tasks on request (Art. 26)
7) Carry out a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Art. 27)

8) The requirement to notify a supervisory authority of a personal data breach without delay (where feasible no later than 72 hours after having become aware) (Art. 30)

9) Communicate the personal data breach to the data subject without undue delay (where the breach is liable to result in a high risk to their rights and freedoms) (Art. 31)

10) To make a clear distinction between personal data of different categories of data subjects, e.g., a) persons convicted of a criminal offence, b) victims of a criminal offence, c) other parties to a criminal offence (Art. 6)

11) Processing of the data must be lawful, i.e., necessary for the performance of a task carried out by a competent authority (Art. 8)

12) Processing of special categories of data is allowed only when strictly necessary Art. 10

3. Argentina

The National Constitution enshrines the right to privacy as a fundamental right in Articles 18 and 19 and boasts a robust — although outdated — data protection regime, through Article 43 of the Constitution and National Law Nº 25.326 on the protection of personal data. It is also a signatory to Convention 108+ 183 and the European Commission recognized Argentina as having an adequate level of data protection in 2003, through decision 2003/490 EC.

Unfortunately, these laws have proven to be insufficient to protect citizens from state surveillance. “Governments use the exceptions in these laws as legal bases for the deployment of surveillance programs for the normal exercise of state functions, service improvement, and public safety.”

In Argentina, there is no federal law regulating government use of face surveillance technology. However, deployment of facial recognition technology for public safety purposes is currently underway in the following provinces and municipalities:

1. Ciudad Autónoma de Buenos Aires: is the only district where the legislative branch passed an amendment to the Law No. 5688 on Integral Public Security System. In September 2020, the Legislature issued Law No. 6339, that incorporated the Fugitive Facial Recognition System (the "Recognition System") on the Public Security System. The objective of the Recognition System is to recognize the faces of people sought by the authorities as a result of a court order that have been registered in the Databases of the

---

