The European Commission's Proposed Regulatory Scheme for 'AI'

Extracts of Passages Relevant to Surveillance

27 September 2021

EC (2021) 'Proposal for a Regulation on a European approach for Artificial Intelligence' European Commission, 21 April 2021, at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788

Note: No attempt is made here to search out passages relevant to surveillance in any of the many relevant aspects of EU law external to the Proposal itself, such as the statutes referenced in Annex II: List of Union harmonisation legislation.

Art.3 Definitions ...

(33) **'biometric data' means** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(34) **'emotion recognition system' means** an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(35) **'biometric categorisation system' means** an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

(36) **'remote biometric identification system' means** an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

(37) **''real-time' remote biometric identification system' means** a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.

(38) **''post' remote biometric identification system' means** a remote biometric identification system other than a 'real-time' remote biometric identification system;

(39**)** **'publicly accessible space' means** any physical place accessible to the public, regardless of whether certain conditions for access may apply;

(40) **'law enforcement authority' means**:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including **the safeguarding against and the prevention of threats to public security**; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(41) **'law enforcement' means** activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including **the safeguarding against and the prevention of threats to public security**;

(44) **'serious incident' means** any incident that directly or indirectly leads, might have led or might lead to any of the following:

(a) the death of a person or serious damage to a person's health, to property or the environment,

(b) a serious and irreversible disruption of the management and operation of critical infrastructure.

Article 5 Prohibited Artificial Intelligence Practices

1. The following artificial intelligence practices shall be prohibited: ...

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for **the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to** either or both of the following:

(i) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) **the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives**:

(i) the **targeted search for specific potential victims of crime**, including missing children;

(ii) the **prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack**;

(iii) **the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence** referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[62] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least **three years**, as determined by the law of that Member State.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a **prior authorisation granted by a judicial authority or by an independent administrative authority** of the Member State in which the use is to take place, **issued upon a reasoned request and in accordance with the detailed rules of national law** referred to in paragraph 4. **However**, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and **the authorisation may be requested only during or after the use**.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for **the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed** in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in

point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

Article 40 Harmonised Standards

Article 41 Common Specifications

[This Article **absolves** high-risk AI systems referred to in point 1 of Annex III (**'Biometric identification and categorisation')** from needing to undergo **conformity assessment**.]

Article 42 Presumption of conformity with certain requirements

1. Taking into account their intended purpose, high-risk AI systems that have been trained and tested on data concerning the specific geographical, behavioural and functional setting within which they are intended to be used shall be **presumed to be in compliance** with the requirement set out in Article 10(4).

[This Article provides **relief** for all High-Risk Systems from one of the requirements of **data governance**.]

Article 43 Conformity Assessment

1. ... **when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies**, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

2. For **high-risk AI systems referred to in points 2 to 8 of Annex III**, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body.

[This **voids the obligation of almost all 'High-Risk AI Systems' from all regulatory provisions relating to conformity assessment**, substituting a weak requirement for self-regulation. Article 43(3) does, however, save provisions in existing Union harmonisation legislation.]

Article 47 Derogation from conformity assessment procedure

1. By way of **derogation from Article 43**, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional **reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets**. That authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay.

[This enabled even such conformity assessment regulation as may exist to be got around for an interim period, and perhaps even for the life of the application.]

Article 52 Transparency obligations for certain AI systems

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are **informed that they are interacting with an AI system**, unless this is obvious from the circumstances and the context of use. This obligation **shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences**, unless those systems are available for the public to report a criminal offence.

2. Users of an emotion recognition system or a biometric categorisation system **shall inform** of the operation of the system the natural persons exposed thereto. This obligation **shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences**.

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (‘deep fake’), **shall disclose** that the content has been artificially generated or manipulated.

However, the first subparagraph shall not apply where the use is **authorised by law to detect, prevent, investigate and prosecute criminal offences** or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the

Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.

Article 54 Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

1. In the AI regulatory sandbox **personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing** certain innovative AI systems in the sandbox under the following conditions:

(a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

(i) **the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security**, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

(ii) **public safety and public health, including disease prevention, control and treatment**;

(iii) **a high level of protection and improvement of the quality of the environment**;

[This appears to authorise what would otherwise be a breach of the GDPR.]

Annex III: High-Risk AI Systems Referred to in Article 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. **Biometric identification and categorisation of natural persons**:

(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;

2. **Management and operation of critical infrastructure**:

(a) AI systems intended to be used as safety components in the management and operation of **road traffic and the supply of water, gas, heating and electricity**.

...

5. **Access to and enjoyment of essential private services and public services and benefits**:

(a) AI systems intended to be used by public authorities or on behalf of public authorities **to evaluate the eligibility of natural persons for public assistance benefits and services**, as well as to grant, reduce, revoke, or reclaim such benefits and services;

(b) AI systems intended to be used **to evaluate the creditworthiness of natural persons** or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

6. **Law enforcement**:

(a) AI systems intended to be used by law enforcement authorities **for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences**;

(b) AI systems intended to be used by law enforcement authorities as **polygraphs and similar tools or to detect the emotional state of a natural person**;

...

(e) AI systems intended to be used by **law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling** of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 **or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups**;

(f) AI systems intended to be used by law enforcement authorities **for profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 **in the course of detection, investigation or prosecution of criminal offences**;

(g) AI systems intended to be used **for crime analytics regarding natural persons**, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. **Migration, asylum and border control management**:

(a) AI systems intended to be used by competent public authorities as **polygraphs and similar tools or to detect the emotional state of a natural person**;

(b) AI systems intended to be used by competent public authorities **to assess a risk**, including a security risk, a risk of irregular immigration, or a health risk, **posed by a natural person** who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities **for the verification of the authenticity of travel documents and supporting documentation of natural persons** and detect non-authentic documents by checking their security features;

(d) AI systems intended to assist competent public authorities **for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons** applying for a status.

Explanatory Memorandum

...

(7) **The notion of biometric data** used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council35, Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council36 and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council37.

(8) **The notion of remote biometric identification system** as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used. Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

(9) For the purposes of this Regulation **the notion of publicly accessible space** should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. **Online spaces are not covered** either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as **streets, relevant parts of government buildings and most transport infrastructure**, spaces such as **cinemas, theatres, shops and shopping centres** are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

...

*(18) The use of AI systems for **'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement** is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.*

(19) The use of those systems for the purpose of law enforcement should therefore be **prohibited, except in three exhaustively listed and narrowly defined situations**, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve **the search for potential victims of crime**, including missing children; certain **threats to the life or physical safety of natural persons** or of a terrorist attack; and the **detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences** referred to in Council Framework Decision 2002/584/JHA38 if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least **three years** and as they are defined in the law of that

Member State. Such threshold for the custodial sentence or detention order in accordance with national law contributes to ensure that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, of the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA, some are in practice likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification will foreseeably be necessary and proportionate to highly varying degrees for the practical pursuit of the detection, localisation, identification or prosecution of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences.

(20) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to appropriate limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.

(21) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation **should <u>in principle</u> be obtained prior to the use**, except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier.

(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation.

(23) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as lex specialis in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should only be possible in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In this context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive 2016/680. However, **the use of 'real-time' remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement**, including by competent authorities, **should <u>not</u> be covered by** the specific framework regarding such use for the purpose of law enforcement set **by this Regulation**. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to it.

(24) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, including where those systems are used by competent authorities in publicly

accessible spaces for other purposes than law enforcement, should continue to comply with all requirements resulting from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680, as applicable.

...

(33) Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to **biased results and** entail **discriminatory effects**. This is **particularly** relevant when it comes to **age, ethnicity, sex or disabilities**. Therefore, 'real-time' and 'post' remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be **subject to specific requirements on logging capabilities and human oversight**.

...

(38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of **power imbalance and** may lead to **surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights** guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular **AI systems intended to be used by law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person**, to detect 'deep fakes', for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or **assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences**, as well as for **crime analytics regarding natural persons**. AI systems specifically intended to be used for **administrative proceedings by tax and customs authorities should <u>not</u> be considered high-risk AI systems** used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

(39) AI systems used in **migration, asylum and border control management** affect people who are often in **particularly vulnerable position** and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control management as **polygraphs and similar tools or to detect the emotional state of a natural person**; for **assessing certain risks posed by natural persons entering the territory** of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council49, the Regulation (EC) No 810/2009 of the European Parliament and of the Council50 and other relevant legislation.

...

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial

phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, **the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility**, with the only **exception** of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(65) In order to carry out third-party conformity assessment for AI systems intended to be used **for the remote biometric identification of persons**, notified bodies should be designated under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.

...

(70) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, **natural persons should be notified when they are exposed to** an emotion recognition system or **a biometric categorisation system**. Such information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin.