DOI:10.1017/ilm.2025.1

INTRODUCTORY NOTE TO FRAMEWORK CONVENTION ON ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW (COUNCIL EUR.)

BY MARC ROTENBERG*

[September 5, 2024]

Background

While the deployment of artificial intelligence (AI) techniques offers great promise to society, there is growing public concern about AI's impact on human rights, democracy, and the rule of law.[1] As a consequence, many international organizations have developed legal frameworks for AI governance. These began with the Universal Guidelines for AI (2018), the OECD AI Principles (2019), later adopted by the G20 nations, the UNESCO Recommendation on AI Ethics, and most notably, the EU Artificial Act, a comprehensive framework for the regulation of AI.

Alongside these initiatives is the Council of Europe (COE) Framework Convention on AI, Human Rights, and the Rule of Law (AI Treaty). In 2019, the COE Parliamentary Assembly took the lead on the need to create a cross-cutting regulatory framework for AI, and called on the Committee of Ministers to elaborate a legally binding instrument governing AI. The Committee of Ministers established an expert group (the CAHAI) followed by a Committee on AI (the CAI) that presented a formal recommendation. With the adoption of the AI Treaty by the Council of Ministers in September 2024, the AI Treaty is now open for signature and ratification by member states and non-member states.

As of January 2025, there are thirty-seven signatories, with the European Commission representing the twenty-seven EU states. The AI Treaty has also been endorsed by the International Bar Association, leading legal scholars such as Professor Dr. Pascal Pichonnaz, President of the European Law Institute (ELI), and leading AI experts, including Professor Virginia Dignum and Professor Stuart Russell.[2]

Significance

The Council of Europe AI Treaty sets out a legal framework that covers the lifecycle of AI systems and addresses the risks they may pose, while promoting responsible innovation.[3] The Convention adopts a risk-based approach to the design, development, use, and decommissioning of AI systems that also recognizes the need to prohibit certain AI systems.

The Treaty covers the use of AI systems in the public sector—including companies engaged in public administration—and in the private sector. The Treaty offers parties two ways of complying with its principles and obligations when regulating the private sector: (1) parties may opt to be directly obliged by the relevant convention provisions; or (2) they may take other measures to comply with the Treaty's provisions while fully respecting their international obligations regarding human rights, democracy, and the rule of law.

The Convention establishes transparency and oversight requirements for specific contexts and risks, including identifying content generated by AI systems. Parties must adopt measures to identify, assess, prevent, and mitigate possible risks and assess the need for a moratorium, a ban, or other appropriate measures concerning the use of AI systems where their risks may be incompatible with human rights standards.

Parties must also ensure accountability and responsibility for adverse impacts and that AI systems respect equality, including gender equality, the prohibition of discrimination, and privacy rights. Moreover, parties to the Convention must ensure the availability of legal remedies for victims of human rights violations related to the use of AI systems and establish procedural safeguards, including notifying any persons interacting with AI systems that they are interacting with such systems.

With regard to the risks to democracy, the Treaty requires parties to adopt measures to ensure that AI systems are not used to undermine democratic institutions and processes, including the principle of separation of powers, respect for judicial independence, and access to justice.

*Marc Rotenberg is the founder and executive director of the Center for AI and Digital Policy, a global network of AI policy experts and human rights advocates, and adjunct professor at Georgetown Law, United States. He participated in the development and drafting of the Convention as a member of the COE AI Expert Group (the CAHAI) and the COE Committee on AI (CAI). Merve Hickok, Afi Blackshear, and Christabel Randolph contributed to CAIDP's work on the AI Convention.

Parties to the Convention will not be required to apply its provisions to activities related to protecting national security interests but will be obliged to ensure that these activities respect international law and democratic institutions and processes. The Convention will not apply to national defence matters or research and development activities, except when the testing of AI systems may have the potential to interfere with human rights, democracy, or the rule of law.

To ensure effective implementation, the Convention establishes a follow-up mechanism in the form of a Conference of the Parties. The Convention requires that each party establish an independent oversight mechanism to ensure compliance with it. It also raises awareness, stimulates an informed public debate, and carries out consultations on how AI technology should be used.

Context

The Council of Europe was founded in 1949 to safeguard human rights, democracy, and the rule of law. It comprises forty-six member states, twenty-seven of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, an international 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. Observer states that participated in the drafting of the Convention included Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America, and Uruguay.

The Council of Europe AI Treaty builds on similar efforts in the fields of Cybercrime and Data Protection. The COE Convention on Cybercrime, also known as the Budapest Convention, set out a common international policy aimed at the protection of society against cybercrime.[4] There are presently seventy-six parties to the Cybercrime Convention. The original COE *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, also known as Convention 108, was originally open for signature on January 28, 1981, and entered into force in 1985. Convention 108 was ratified by forty-six member states and nine non-member states.[5] In 2018, the Council of Europe adopted the Amending Protocol CETS No. 223 for the modernization of Convention 108.[6]

The Council of Europe has also undertaken a wide range of related projects concerning AI. The subcommittee on AI and Human Rights has published several reports, including *The Need for Democratic Governance of Artificial Intelligence*;[7] *Preventing Discrimination Caused by the Use of Artificial Intelligence*;[8] *Justice by Algorithm—the Role of Artificial Intelligence in Policing and Criminal Justice Systems*;[9] and *The Brain–Computer Interface: New Rights of New Threats to Fundamental Freedoms?*[10] The Council of Europe Congress of Local and Regional Authorities, responsible for strengthening local and regional democracy, published reports on *Smart Cities and Smart Regions: Prospects of a Human Rights-Based Governance Approach* (2022); *Hate Speech and Fake News: The Impact on the Working Conditions of Local and Regional Elected Representatives* (2022); *Beyond Elections: The Use of Deliberative Methods in European Municipalities and Regions* (2022); and *Home Sharing Platforms: Challenges and Opportunities for Municipalities* (2022). The Council Commissioner for Human Rights also raises awareness of the human rights impacts of AI systems in their dialogue with national authorities, national human rights structures, and other relevant stakeholders, including civil society actors. Reports from the Commissioner's office include *Highly Intrusive Spyware Threatens the Essence of Human Rights* (2023); *Unboxing AI: 10 Steps to Protect Human Rights* (2019); and *Safeguarding Human Rights in the Era of Artificial Intelligence* (2018).

Another COE institution participating in the work on AI is the Steering Committee for Human Rights, which is responsible for ensuring AI standard-setting activities are compatible with human rights norms as set out in the European Convention on Human Rights, as interpreted by the European Court of Human Rights. The Committee is tasked with preparing a *Handbook on Artificial Intelligence and Human Rights* by the end of 2025.

Effect

The forward progress of the AI Convention will likely be measured across multiple dimensions. There is first the signature and ratification requirements to give the Convention legal force. The Treaty will enter into force once there are five ratifications, at least three of which must be by member states.[11] At the opening ceremony on September 5, 2024, ten states, including the European Union, representing the EU member states who are also Council member states, signed the Treaty.

Within the context of the Convention, implementation and enforcement of the provisions establishing substantive rights will be the next critical steps, as well as procedures for Public Consultation (Article 19); the Conference of the Parties (Article 23); Reporting Obligations (Article 24); International Cooperation (Article 25); Effective Oversight Mechanisms (Article 26); and possible updates.

There is also the critical question of the interplay between the EU AI Act and the Council of Europe AI Convention. Certain provisions of the Convention seek to obtain alignment between the AI Act and the AI Convention. But the mandate of the Council of Europe is distinct from the European Union, as is the membership. The relationship between the EU legal institutions and the COE legal institutions might best be understood as a binary star system, with each exerting gravitation force on the other even when the EU seeks to direct the motion of the COE.

The United States is likely to play a significant role in the decision of observer states to sign and ratify the Convention, as it did with the Cybercrime Convention. The United States has expressed strong support for the AI Convention. According to the US Department of State, "The Convention defines a baseline in international law for rights-respecting AI activities by governments and provides a powerful affirmation of the relevance of existing human rights obligations to AI activities."[12]

The State Department further explained that the Convention reflects the "enduring commitment to ensuring that AI technologies promote respect for human rights and democratic values" and outlines the alignment of the Convention with existing US policy, such as the requirements for governance, innovation, and risk management of AI systems in the OMB Guidance on AI use by federal agencies, as well as Executive Orders and policy developed by multiple administrations.[13]

Looming over the future of the AI Treaty will be the willingness and ability of states to align AI governance with the mission of the Council of Europe—to safeguard human rights, democracy, and the rule of law.

ENDNOTES

1 The Council of Europe, *Overview of the Council of Europe Activities in the Field of Artificial Intelligence* (March 2023) [hereinafter COE AI Activities], https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6.

2 Center for AI and Digital Policy, *International AI Treaty* (listing endorsements by AI policy experts), https://www.caidp.org/resources/coe-ai-treaty/

3 Press Release, Council of Europe, Council of Europe adopts first international treaty on artificial intelligence (May 17, 2024), https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence.

4 Council of Europe, Convention on Cybercrime, Nov. 11, 2001, E.T.S. No. 185, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

5 Council of Europe, *Chart of Signatures and Ratifications of Treaty 108*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

6 Council of Europe, *Convention 108+: Convention for the protection of individuals with regard to the processing of individual data* (June 2018), https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

7 Resolution 2341 (2020) and Recommendation 2181 (2020).

8 Resolution 2343 (2020) and Recommendation 2183 (2020).

9 Resolution 2342 (2020) and Recommendation 2182 (2020).

10 Resolution 2344 (2020) and Recommendation 2184 (2020).

11 Council of Europe, Treaty Office, *Chart of signatures and ratifications of Treaty 225*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225.

12 U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, *The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (Sept. 5, 2024), https://www.state.gov/the-council-of-europes-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law/.

13 *Id.*

DOI:10.1017/ilm.2025.1

FRAMEWORK CONVENTION ON ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW AND EXPLANATORY REPORT(COUNCIL EUR.)* [September 2024]

Council of Europe Treaty Series - No. 225

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

Vilnius, 5.IX.2024

Preamble

The member States of the Council of Europe and the other signatories hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on the respect for human rights, democracy and the rule of law;

Recognising the value of fostering co-operation between the Parties to this Convention and of extending such co-operation to other States that share the same values;

Conscious of the accelerating developments in science and technology and the profound changes brought about through activities within the lifecycle of artificial intelligence systems, which have the potential to promote human prosperity as well as individual and societal well-being, sustainable development, gender equality and the empowerment of all women and girls, as well as other important goals and interests, by enhancing progress and innovation;

Recognising that activities within the lifecycle of artificial intelligence systems may offer unprecedented opportunities to protect and promote human rights, democracy and the rule of law;

Concerned that certain activities within the lifecycle of artificial intelligence systems may undermine human dignity and individual autonomy, human rights, democracy and the rule of law;

Concerned about the risks of discrimination in digital contexts, particularly those involving artificial intelligence systems, and their potential effect of creating or aggravating inequalities, including those experienced by women and individuals in vulnerable situations, regarding the enjoyment of their human rights and their full, equal and effective participation in economic, social, cultural and political affairs;

Concerned by the misuse of artificial intelligence systems and opposing the use of such systems for repressive purposes in violation of international human rights law, including through arbitrary or unlawful surveillance and censorship practices that erode privacy and individual autonomy;

Conscious of the fact that human rights, democracy and the rule of law are inherently interwoven;

Convinced of the need to establish, as a matter of priority, a globally applicable legal framework setting out common general principles and rules governing the activities within the lifecycle of artificial intelligence

*These texts were reproduced and reformatted from the texts available at the Council of Europe website (visited January 9, 2025), https://rm.coe.int/1680afae3c (Convention text) and https://rm.coe.int/1680afae67 (Explanatory Report).

systems that effectively preserves shared values and harnesses the benefits of artificial intelligence for the promotion of these values in a manner conducive to responsible innovation;

Recognising the need to promote digital literacy, knowledge about, and trust in the design, development, use and decommissioning of artificial intelligence systems;

Recognising the framework character of this Convention, which may be supplemented by further instruments to address specific issues relating to the activities within the lifecycle of artificial intelligence systems;

Underlining that this Convention is intended to address specific challenges which arise throughout the lifecycle of artificial intelligence systems and encourage the consideration of the wider risks and impacts related to these technologies including, but not limited to, human health and the environment, and socio-economic aspects, such as employment and labour;

Noting relevant efforts to advance international understanding and co-operation on artificial intelligence by other international and supranational organisations and fora;

Mindful of applicable international human rights instruments, such as the 1948 Universal Declaration of Human Rights, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), the 1966 International Covenant on Civil and Political Rights, the 1966 International Covenant on Economic, Social and Cultural Rights, the 1961 European Social Charter (ETS No. 35), as well as their respective protocols, and the 1996 European Social Charter (Revised) (ETS No. 163);

Mindful also of the 1989 United Nations Convention on the Rights of the Child and the 2006 United Nations Convention on the Rights of Persons with Disabilities;

Mindful also of the privacy rights of individuals and the protection of personal data, as applicable and conferred, for example, by the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its protocols;

Affirming the commitment of the Parties to protecting human rights, democracy and the rule of law, and fostering trustworthiness of artificial intelligence systems through this Convention,

Have agreed as follows:

Chapter I – General provisions

Article 1 – Object and purpose

1 The provisions of this Convention aim to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.

2 Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used.

3 In order to ensure effective implementation of its provisions by the Parties, this Convention establishes a follow-up mechanism and provides for international co-operation.

Article 2 – Definition of artificial intelligence systems

For the purposes of this Convention, "artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment.

Article 3 – Scope

1 The scope of this Convention covers the activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and the rule of law as follows:

a. Each Party shall apply this Convention to the activities within the lifecycle of artificial intelligence systems undertaken by public authorities, or private actors acting on their behalf.

b. Each Party shall address risks and impacts arising from activities within the lifecycle of artificial intelligence systems by private actors to the extent not covered in subparagraph a in a manner conforming with the object and purpose of this Convention.

Each Party shall specify in a declaration submitted to the Secretary General of the Council of Europe at the time of signature, or when depositing its instrument of ratification, acceptance, approval or accession, how it intends to implement this obligation, either by applying the principles and obligations set forth in Chapters II to VI of this Convention to activities of private actors or by taking other appropriate measures to fulfil the obligation set out in this subparagraph. Parties may, at any time and in the same manner, amend their declarations.

When implementing the obligation under this subparagraph, a Party may not derogate from or limit the application of its international obligations undertaken to protect human rights, democracy and the rule of law.

2 A Party shall not be required to apply this Convention to activities within the lifecycle of artificial intelligence systems related to the protection of its national security interests, with the understanding that such activities are conducted in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes.

3 Without prejudice to Article 13 and Article 25, paragraph 2, this Convention shall not apply to research and development activities regarding artificial intelligence systems not yet made available for use, unless testing or similar activities are undertaken in such a way that they have the potential to interfere with human rights, democracy and the rule of law.

4 Matters relating to national defence do not fall within the scope of this Convention.

Chapter II – General obligations

Article 4 – Protection of human rights

Each Party shall adopt or maintain measures to ensure that the activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights, as enshrined in applicable international law and in its domestic law.

Article 5 – Integrity of democratic processes and respect for the rule of law

1 Each Party shall adopt or maintain measures that seek to ensure that artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice.

2 Each Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as their ability to freely form opinions.

Chapter III – Principles related to activities within the lifecycle of artificial intelligence systems

Article 6 – General approach

This chapter sets forth general common principles that each Party shall implement in regard to artificial intelligence systems in a manner appropriate to its domestic legal system and the other obligations of this Convention.

Article 7 – Human dignity and individual autonomy

Each Party shall adopt or maintain measures to respect human dignity and individual autonomy in relation to activities within the lifecycle of artificial intelligence systems.

Article 8 – Transparency and oversight

Each Party shall adopt or maintain measures to ensure that adequate transparency and oversight requirements tailored to the specific contexts and risks are in place in respect of activities within the lifecycle of artificial intelligence systems, including with regard to the identification of content generated by artificial intelligence systems.

Article 9 – Accountability and responsibility

Each Party shall adopt or maintain measures to ensure accountability and responsibility for adverse impacts on human rights, democracy and the rule of law resulting from activities within the lifecycle of artificial intelligence systems.

Article 10 – Equality and non-discrimination

1 Each Party shall adopt or maintain measures with a view to ensuring that activities within the lifecycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, as provided under applicable international and domestic law.

2 Each Party undertakes to adopt or maintain measures aimed at overcoming inequalities to achieve fair, just and equitable outcomes, in line with its applicable domestic and international human rights obligations, in relation to activities within the lifecycle of artificial intelligence systems.

Article 11 – Privacy and personal data protection

Each Party shall adopt or maintain measures to ensure that, with regard to activities within the lifecycle of artificial intelligence systems:

a. privacy rights of individuals and their personal data are protected, including through applicable domestic and international laws, standards and frameworks; and

b. effective guarantees and safeguards have been put in place for individuals, in accordance with applicable domestic and international legal obligations.

Article 12 – Reliability

Each Party shall take, as appropriate, measures to promote the reliability of artificial intelligence systems and trust in their outputs, which could include requirements related to adequate quality and security throughout the lifecycle of artificial intelligence systems.

Article 13 – Safe innovation

With a view to fostering innovation while avoiding adverse impacts on human rights, democracy and the rule of law, each Party is called upon to enable, as appropriate, the establishment of controlled environments for developing, experimenting and testing artificial intelligence systems under the supervision of its competent authorities.

Chapter IV – Remedies

Article 14 – Remedies

1 Each Party shall, to the extent remedies are required by its international obligations and consistent with its domestic legal system, adopt or maintain measures to ensure the availability of accessible and effective remedies for violations of human rights resulting from the activities within the lifecycle of artificial intelligence systems.

2 With the aim of supporting paragraph 1 above, each Party shall adopt or maintain measures including:

a. measures to ensure that relevant information regarding artificial intelligence systems which have the potential to significantly affect human rights and their relevant usage is documented, provided to bodies authorised to access that information and, where appropriate and applicable, made available or communicated to affected persons;

b. measures to ensure that the information referred to in subparagraph a is sufficient for the affected persons to contest the decision(s) made or substantially informed by the use of the system, and, where relevant and appropriate, the use of the system itself; and

c. an effective possibility for persons concerned to lodge a complaint to competent authorities.

Article 15 – Procedural safeguards

1 Each Party shall ensure that, where an artificial intelligence system significantly impacts upon the enjoyment of human rights, effective procedural guarantees, safeguards and rights, in accordance with the applicable international and domestic law, are available to persons affected thereby.

2 Each Party shall seek to ensure that, as appropriate for the context, persons interacting with artificial intelligence systems are notified that they are interacting with such systems rather than with a human.

Chapter V – Assessment and mitigation of risks and adverse impacts

Article 16 – Risk and impact management framework

1 Each Party shall, taking into account the principles set forth in Chapter III, adopt or maintain measures for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems by considering actual and potential impacts to human rights, democracy and the rule of law.

2 Such measures shall be graduated and differentiated, as appropriate, and:

a. take due account of the context and intended use of artificial intelligence systems, in particular as concerns risks to human rights, democracy, and the rule of law;

b. take due account of the severity and probability of potential impacts;

c. consider, where appropriate, the perspectives of relevant stakeholders, in particular persons whose rights may be impacted;

d. apply iteratively throughout the activities within the lifecycle of the artificial intelligence system;

e. include monitoring for risks and adverse impacts to human rights, democracy, and the rule of law;

f. include documentation of risks, actual and potential impacts, and the risk management approach; and

g. require, where appropriate, testing of artificial intelligence systems before making them available for first use and when they are significantly modified.

3 Each Party shall adopt or maintain measures that seek to ensure that adverse impacts of artificial intelligence systems to human rights, democracy, and the rule of law are adequately addressed. Such adverse impacts and measures to address them should be documented and inform the relevant risk management measures described in paragraph 2.

4 Each Party shall assess the need for a moratorium or ban or other appropriate measures in respect of certain uses of artificial intelligence systems where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law.

Chapter VI – Implementation of the Convention

Article 17 – Non-discrimination

The implementation of the provisions of this Convention by the Parties shall be secured without discrimination on any ground, in accordance with their international human rights obligations.

Article 18 – Rights of persons with disabilities and of children

Each Party shall, in accordance with its domestic law and applicable international obligations, take due account of any specific needs and vulnerabilities in relation to respect for the rights of persons with disabilities and of children.

Article 19 – Public consultation

Each Party shall seek to ensure that important questions raised in relation to artificial intelligence systems are, as appropriate, duly considered through public discussion and multistakeholder consultation in the light of social, economic, legal, ethical, environmental and other relevant implications.

Article 20 – Digital literacy and skills

Each Party shall encourage and promote adequate digital literacy and digital skills for all segments of the population, including specific expert skills for those responsible for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems.

Article 21 – Safeguard for existing human rights

Nothing in this Convention shall be construed as limiting, derogating from or otherwise affecting the human rights or other related legal rights and obligations which may be guaranteed under the relevant laws of a Party or any other relevant international agreement to which it is party.

Article 22 – Wider protection

None of the provisions of this Convention shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant a wider measure of protection than is stipulated in this Convention.

Chapter VII – Follow-up mechanism and co-operation

Article 23 – Conference of the Parties

1 The Conference of the Parties shall be composed of representatives of the Parties to this Convention.

2 The Parties shall consult periodically with a view to:

a. facilitating the effective application and implementation of this Convention, including the identification of any problems and the effects of any reservation made in pursuance of Article 34, paragraph 1, or any declaration made under this Convention;

b. considering the possible supplementation to or amendment of this Convention;

c. considering matters and making specific recommendations concerning the interpretation and application of this Convention;

d. facilitating the exchange of information on significant legal, policy or technological developments of relevance, including in pursuit of the objectives defined in Article 25, for the implementation of this Convention;

e. facilitating, where necessary, the friendly settlement of disputes related to the application of this Convention; and

f. facilitating co-operation with relevant stakeholders concerning pertinent aspects of the implementation of this Convention, including through public hearings where appropriate.

3 The Conference of the Parties shall be convened by the Secretary General of the Council of Europe whenever necessary and, in any case, when a majority of the Parties or the Committee of Ministers requests its convocation.

4 The Conference of the Parties shall adopt its own rules of procedure by consensus within twelve months of the entry into force of this Convention.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

6 The Conference of the Parties may propose to the Committee of Ministers appropriate ways to engage relevant expertise in support of the effective implementation of this Convention.

7 Any Party which is not a member of the Council of Europe shall contribute to the funding of the activities of the Conference of the Parties. The contribution of a non-member of the Council of Europe shall be established jointly by the Committee of Ministers and that non-member.

8 The Conference of the Parties may decide to restrict the participation in its work of a Party that has ceased to be a member of the Council of Europe under Article 8 of the Statute of the Council of Europe (ETS No. 1) for a serious violation of Article 3 of the Statute. Similarly, measures can be taken in respect of any Party that is not a member State of the Council of Europe by a decision of the Committee of Ministers to cease its relations with that State on grounds similar to those mentioned in Article 3 of the Statute.

Article 24 – Reporting obligation

1 Each Party shall provide a report to the Conference of the Parties within the first two years after becoming a Party, and then periodically thereafter with details of the activities undertaken to give effect to Article 3, paragraph 1, sub-paragraphs a and b.

2 The Conference of the Parties shall determine the format and the process for the report in accordance with its rules of procedure.

Article 25 – International co-operation

1 The Parties shall co-operate in the realisation of the purpose of this Convention. Parties are further encouraged, as appropriate, to assist States that are not Parties to this Convention in acting consistently with the terms of this Convention and becoming a Party to it.

2 The Parties shall, as appropriate, exchange relevant and useful information between themselves concerning aspects related to artificial intelligence which may have significant positive or negative effects on the enjoyment of human rights, the functioning of democracy and the observance of the rule of law, including risks and effects that have arisen in research contexts and in relation to the private sector. Parties are encouraged to involve, as appropriate, relevant stakeholders and States that are not Parties to this Convention in such exchanges of information.

3 The Parties are encouraged to strengthen co-operation, including with relevant stakeholders where appropriate, to prevent and mitigate risks and adverse impacts on human rights, democracy and the rule of law in the context of activities within the lifecycle of artificial intelligence systems.

Article 26 – Effective oversight mechanisms

1 Each Party shall establish or designate one or more effective mechanisms to oversee compliance with the obligations in this Convention.

2 Each Party shall ensure that such mechanisms exercise their duties independently and impartially and that they have the necessary powers, expertise and resources to effectively fulfil their tasks of overseeing compliance with the obligations in this Convention, as given effect by the Parties.

3 If a Party has provided for more than one such mechanism, it shall take measures, where practicable, to facilitate effective cooperation among them.

4 If a Party has provided for mechanisms different from existing human rights structures, it shall take measures, where practicable, to promote effective cooperation between the mechanisms referred to in paragraph 1 and those existing domestic human rights structures.

Chapter VIII – Final clauses

Article 27 – Effects of the Convention

1 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention, or have otherwise established relations on such matters, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly, so long as they do so in a manner which is not inconsistent with the object and purpose of this Convention.

2 Parties which are members of the European Union shall, in their mutual relations, apply European Union rules governing the matters within the scope of this Convention without prejudice to the object and purpose of this Convention and without prejudice to its full application with other Parties. The same applies to other Parties to the extent that they are bound by such rules.

Article 28 – Amendments

1 Amendments to this Convention may be proposed by any Party, the Committee of Ministers of the Council of Europe or the Conference of the Parties.

2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Parties.

3 Any amendment proposed by a Party, or the Committee of Ministers, shall be communicated to the Conference of the Parties, which shall submit to the Committee of Ministers its opinion on the proposed amendment.

4 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the Conference of the Parties and may approve the amendment.

5 The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 shall be forwarded to the Parties for acceptance.

6 Any amendment approved in accordance with paragraph 4 shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 29 – Dispute settlement

In the event of a dispute between Parties as to the interpretation or application of this Convention, these Parties shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including through the Conference of the Parties, as provided for in Article 23, paragraph 2, sub-paragraph e.

Article 30 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe, the non-member States which have participated in its elaboration and the European Union.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five signatories, including at least three member States of the Council of Europe, have expressed their consent to be bound by this Convention in accordance with paragraph 2.

4 In respect of any signatory which subsequently expresses its consent to be bound by it, this Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of its instrument of ratification, acceptance or approval.

Article 31 – Accession

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Convention and obtaining their unanimous consent, invite any non-member State of the Council of Europe which has not participated in the elaboration of this Convention to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe, and by unanimous vote of the representatives of the Parties entitled to sit on the Committee of Ministers.

2 In respect of any acceding State, this Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 32 – Territorial application

1 Any State or the European Union may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any Party may, at a later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory, this Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in said declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 33 – Federal clause

1 A federal State may reserve the right to assume obligations under this Convention consistent with its fundamental principles governing the relationship between its central government and constituent states or other similar territorial entities, provided that this Convention shall apply to the central government of the federal State.

2 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent states or other similar territorial entities that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such states of the said provisions with its favourable opinion, and encourage them to take appropriate action to give them effect.

Article 34 – Reservations

1 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation provided for in Article 33, paragraph 1.

2 No other reservation may be made in respect of this Convention.

Article 35 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 36 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention, the European Union, any signatory, any contracting State, any Party and any other State which has been invited to accede to this Convention, of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention, in accordance with Article 30, paragraphs 3 and 4, and Article 31, paragraph 2;

d. any amendment adopted in accordance with Article 28 and the date on which such an amendment enters into force;

e. any declaration made in pursuance of Article 3, paragraph 1, sub-paragraph b;

f. any reservation and withdrawal of a reservation made in pursuance of Article 34;

g. any denunciation made in pursuance of Article 35;

h. any other act, declaration, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done in Vilnius, this 5th day of September 2024, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, to the European Union and to any State invited to accede to this Convention.

DOI:10.1017/ilm.2025.1

Council of Europe Treaty Series - No. 225

Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

Vilnius, 5.IX.2024

I. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, drawn up within the Council of Europe, was adopted by the Committee of Ministers on 17 May 2024 on the occasion of its 133rd Session.

II. The text of the explanatory report submitted to the Committee of Ministers of the Council of Europe does not constitute an instrument providing an authoritative interpretation of the text of the Framework Convention although it may facilitate the understanding of it's provisions.

I. Introduction

1. The Council of Europe, through the work of its various bodies and of the *ad hoc* Committee on Artificial Intelligence (CAHAI), later succeeded by the Committee on Artificial Intelligence (CAI), has long concerned itself with the problems confronting humankind as a result of advances in information and digital technologies, and in particular algorithmic and artificial intelligence (AI) systems.

2. Having taken note of the CAHAI's final paper on the "Possible elements of a legal framework on artificial intelligence, based on Council of Europe's standards on human rights, democracy and the rule of law" adopted in December 2021, the Committee of Ministers of the Council of Europe instructed the CAI to elaborate a Framework Convention on the activities within the lifecycle of artificial intelligence systems, "based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation, which can be composed of a binding legal instrument of a transversal character, including notably general common principles".

3. The Committee of Ministers also decided to allow for the inclusion in the negotiations of the European Union and interested non-European States sharing the values and aims of the Council of Europe – States from around the globe, namely Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America and Uruguay, joined the process of negotiations in the CAI and participated in the elaboration of this Framework Convention as observer States.

4. It was also important for the Council of Europe to closely involve relevant non-State actors in these negotiations. A total of 68 civil society and industry representatives were involved in the CAI as observers, participating in the negotiations together with States and representatives of other international organisations, such as the Organisation for Security and Co-operation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the United Nations Educational, Scientific and Cultural Organisation (UNESCO) and relevant Council of Europe bodies and committees. The European Union also participated in the negotiations represented by the European Commission, including in its delegation also representatives

from the European Union Agency for Fundamental Rights (FRA) and the European Data Protection Supervisor (EDPS).

5. This Framework Convention focuses on the protection and furtherance of human rights [1], democracy and the rule of law, and does not expressly regulate the economic and market aspects of artificial intelligence systems. Taken as a whole, it provides a common legal framework at the global level in order to apply the existing international and domestic legal obligations that are applicable to each Party in the sphere of human rights, democracy and the rule of law of each Party and aims to ensure that the activities within the lifecycle of artificial intelligence systems by both public and private actors comply with these obligations, standards and commitments.

II. Commentary on the Preamble and the provisions of the Framework Convention

Preamble

6. The Preamble reaffirms the commitment of the Parties to protecting human rights, democracy and the rule of law and recalls international legal instruments and treaties of the Council of Europe and the United Nations which directly deal with topics within the scope of this Framework Convention.

7. During the negotiation and subsequent adoption of this Framework Convention, the following international legal and policy instruments on artificial intelligence, in particular those prepared by the Council of Europe and other international organisations and processes, were taken into account:

   (a) Declaration of the Committee of Ministers of the Council of Europe on the manipulative capabilities of algorithmic processes, adopted on 13 February 2019 - Decl(13/02/2019)1;

   (b) Recommendation on Artificial Intelligence adopted by the OECD Council on 22 May 2019 (the "OECD AI Principles");

   (c) Recommendation of the Committee of Ministers of the Council of Europe to member States on the human rights impacts of algorithmic systems, adopted on 8 April 2020 - CM/Rec(2020)1;

   (d) Resolutions and Recommendations of the Parliamentary Assembly of the Council of Europe, examining the opportunities and risks of artificial intelligence for human rights, democracy, and the rule of law and endorsing a set of core ethical principles that should be applied to AI systems; [2]

   (e) UNESCO Recommendation on the Ethics of Artificial Intelligence adopted on 23 November 2021;

   (f) G7 Hiroshima Process International Guiding Principles for Organisations Developing Advanced AI Systems and Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (adopted on 30 October 2023); and

   (g) EU Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) adopted on 13 March 2024.

8. Furthermore, the negotiations were inspired by elements of the following political declarations:

   (a) Declaration by Heads of State and Government made at the 4th Council of Europe Summit in Reykjavík on 16-17 May 2023;

   (b) G7 Leaders' Statement on the Hiroshima AI Process of 30 October and 6 December 2023; and

   (c) The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023.

9. The Preamble sets out the basic aim of the Framework Convention – to ensure that the potential of artificial intelligence technologies to promote human prosperity, individual and societal wellbeing and to make our world more productive, innovative and secure, is harnessed in a responsible manner that respects, protects and fulfils the shared values of the Parties and is respectful of human rights, democracy and the rule of law.

10. The Drafters wished to emphasise that artificial intelligence systems offer unprecedented opportunities to protect and promote human rights, democracy and the rule of law. At the same time, they also wished to acknowledge that there are serious risks and perils arising from certain activities within the lifecycle of artificial intelligence such as, for instance, discrimination in a variety of contexts, gender inequality, the undermining of democratic processes, impairing human dignity or individual autonomy, or the misuses of artificial intelligence systems by some States for repressive purposes, in violation of international human rights law. The Drafters also wanted to draw attention to human dignity and individual autonomy as foundational values and principles that are essential for the full realisation of human rights, democracy and the rule of law and that can also be adversely impacted by certain activities within the lifecycle of artificial intelligence systems. The Drafters wished to emphasise that when referring to individuals that can be affected by artificial intelligence systems creating or aggravating inequalities, these include individuals discriminated based on their "race" [3] or ethnicity, including indigenous individuals. They also wished to emphasise the need to avoid discrimination on grounds of sex, bias or other systemic harms, in accordance with international obligations and in line with relevant United Nations declarations. Furthermore, trustworthy artificial intelligence systems will embody principles such as those set out in Chapter III of the Framework Convention that should apply to activities within the lifecycle of artificial intelligence systems. Finally, the Drafters were fully aware that the increasing use of artificial intelligence systems, due to their transformative nature for societies, brings new challenges for human rights, democracy and the rule of law which are not yet foreseeable at the time of drafting.

11. Consequently, the Preamble sets the scene for a variety of legally binding obligations contained in the Framework Convention that aim to ensure that the activities within the lifecycle of artificial intelligence systems that have the potential to interfere with the respect for human rights, the functioning of democracy, or the observance of rule of law in both the public and private sectors are in full compliance with this Framework Convention.

Chapter I: General provisions

Article 1 – Object and purpose

On the object and purpose of the Framework Convention and its relationship with the existing human rights protection regimes and mechanisms

12. Paragraphs 1 and 2 set out the object and purpose of the Framework Convention, which is to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law. At the same time, it is important to underline that the Framework Convention does not intend to regulate all aspects of the activities within the lifecycle of artificial intelligence systems, nor artificial intelligence technologies as such. Both its object and purpose are confined to questions pertaining to the mandate of the Council of Europe with a focus on artificial intelligence systems which have the potential to interfere with human rights, democracy and the rule of law.

13. The Framework Convention ensures that each Party's existing applicable obligations on human rights, democracy and the rule of law are also applied to activities within the lifecycle of artificial intelligence systems. In this sense, the Framework Convention is aligned with the applicable human rights protection systems and mechanisms of each Party, including their international law obligations and other international commitments and their applicable domestic law. As such, no provision of this Framework Convention is intended to create new human rights or human rights obligations or undermine the scope and content of the existing applicable protections, but rather, by setting out various legally binding obligations contained in its Chapters II to VI, to facilitate the effective implementation of the applicable human rights obligations of each Party in the context of the new challenges raised by artificial intelligence. At the same time, the Framework Convention reinforces the role of international human rights law and relevant aspects of domestic legal frameworks in relation to activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and rule of law.

Regarding activities within the lifecycle of artificial intelligence systems

14. Throughout its text the Framework Convention creates various obligations in relation to the activities within the lifecycle of artificial intelligence systems. This reference to the lifecycle ensures a comprehensive approach towards addressing AI-related risks and adverse impacts on human rights, democracy and the rule of law by capturing all stages of activities relevant to artificial intelligence systems. Applying these obligations to the entirety of the lifecycle ensures that the Convention can cover not only current but future risks, which is one of the ways in which the Drafters sought to make the Framework Convention future proof in view of rapid and often unpredictable technological developments. It is important to clarify that, throughout the Framework Convention, "within" is not used as a technical term and is not meant to have a limiting effect on the concept of the lifecycle.

15. With that in mind, and without giving an exhaustive list of activities within the lifecycle which are specific to artificial intelligence systems, the Drafters aim to cover any and all activities from the design of an artificial intelligence system to its retirement, no matter which actor is involved in them. It is the intentional choice of the Drafters not to specify them explicitly as they may depend on the type of technology and other contextual elements and change over time, but drawing inspiration from the latest work of OECD, at the time of the drafting, the Drafters give as examples of relevant activities: (1) planning and design, (2) data collection and processing, (3) development of artificial intelligence systems, including model building and/or fine-tuning existing models for specific tasks, (4) testing, verification and validation, (5) supply/making the systems available for use, (6) deployment, (7) operation and monitoring, and (8) retirement. These activities often take place in an iterative manner and are not necessarily sequential. They may also start all over again when there are substantial changes in the system or its intended use. The decision to retire an artificial intelligence system from operation may occur at any point during the operation and monitoring phase.

Regarding the implementation of the Framework Convention

16. Paragraph 2 of Article 1 sets out the approach to implementation agreed upon by the States which negotiated the Framework Convention. This provision requires Parties to give effect to the provisions of this Framework Convention, but also provides that they enjoy a certain margin of flexibility as to how exactly to give effect to the provisions of the Framework Convention, in view of the underlying diversity of legal systems, traditions and practices among the Parties and the extremely wide variety of contexts of use of artificial intelligence systems in both public and private sectors.

17. In order to account for existing rules and mechanisms in the domestic legal system of each Party, paragraph 2 of Article 1 and many of the obligations require Parties to "adopt or maintain" certain measures to address the risks of artificial intelligence. In using "adopt or maintain", the Drafters wished to provide flexibility for Parties to fulfil their obligations by adopting new measures or by applying existing measures such as legislation and mechanisms that existed prior to the entry into force of the Framework Convention. Use of both of these terms acknowledges that, for the purpose of domestic implementation, either of these approaches may be equally sufficient. Paragraph 2 of Article 1 further provides that such measures should be "graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law". This provision conveys that measures pursuant to the Framework Convention need to be tailored to the level of risk posed by an artificial intelligence system within specific spheres, activities and contexts, as appropriate, and that this task falls on Parties to the Framework Convention to decide how to balance the relevant competing interests in each sphere, taking into account specificities of activities in the private sector, their domestic regulatory framework and national agenda for artificial intelligence while ensuring the protection and promotion of human rights, democracy and the rule of law. The Parties may also take into account specificities of public sector activities such as law enforcement, migration, border control, asylum and the judiciary.

18. It is crucial that in accordance with Article 1, paragraph 2, the consideration of the mentioned issues should start with an assessment by each Party of risks and potential impacts on human rights, democracy and the rule of law in a given context and consideration of maintaining or establishing appropriate measures to address

those impacts. In reaching an understanding of such potential impacts of activities within the lifecycle of artificial intelligence systems, Parties should consider the broader context, including power asymmetries that could further widen existing inequalities and societal impacts. Given the wide range of sectors and use cases in which artificial intelligence systems are used and could be deployed in the future, such as the distribution of social welfare benefits, decisions on the creditworthiness of potential clients, staff recruitment and retention processes, criminal justice procedures, immigration, asylum procedures and border control, policing, and targeted advertising and algorithmic content selection, some adverse impacts could translate into human rights violations throughout the whole society. They could also potentially impact social justice, alter the relationship and affect the trust between citizens and government, and affect the integrity of democratic processes.

19. After careful consideration of the respective risks and other relevant factors, each Party will need to decide whether it will fulfil its obligations by applying existing measures or updating its domestic regulatory framework and, if so, how. It must be borne in mind that by virtue of the respective international human rights obligations and commitments, each Party already has in place various human rights protection and conflict adjudication mechanisms as well as specific manner(s) of administering the relevant rules and regulations.

20. Parties could therefore, for example, decide to keep making use of existing regulation, simplify, clarify or improve it, or they could work on improving its enforcement or supporting the making available of existing remedies more accessible or more available (see the commentary regarding Articles 14–15 in paragraphs 95–104 below). Parties could also consider the adoption of new or additional measures, which could take the shape of rule- based, principle-based or goal-based legislation, policy or regulation; the establishment of compliance mechanisms and standards; co-regulation and industry agreements to facilitate self-regulation; or resort to various combinations of the above. Measures to be adopted or maintained pursuant to the Framework Convention may also consist of administrative and non-legally binding measures, interpretative guidance, circulars, internal mechanisms and processes, or judicial case-law, as each Party deems appropriate in line with the "graduated and differentiated approach" described in Article 1, paragraph 2. Any mention of adopting or maintaining "measures" in this Framework Convention may also be satisfied by appropriate administrative measures.

21. Furthermore, to implement the principles and obligations set forth in the Framework Convention a Party may adopt AI-specific measures or maintain and update so-called "horizontal" measures that are applicable irrespective of the type of technology used, such as for example non-discrimination, data protection and other legislation that could be relied upon to implement specific principles and obligations of this Framework Convention.

Regarding the follow-up mechanism

22. Paragraph 3 notes that, to ensure effective implementation of the Framework Convention, the Framework Convention establishes a follow-up mechanism, which is set out in Chapter VII, see the commentary in paragraphs 129–135, and provides for international co-operation, see the commentary to Article 25 in paragraphs 137–140.

Article 2 – Artificial intelligence systems

23. The definition of an artificial intelligence system prescribed in this article is drawn from the latest revised definition adopted by the OECD on 8 November 2023. The choice of the Drafters to use this particular text is significant not only because of the high quality of the work carried out by the OECD and its experts, but also in view of the need to enhance international co- operation on the topic of artificial intelligence and facilitate efforts aimed at harmonising governance of artificial intelligence at a global level, including by harmonising the relevant terminology, which also allows for the coherent implementation of different instruments relating to artificial intelligence within the domestic legal systems of the Parties.

24. The definition reflects a broad understanding of what artificial intelligence systems are, specifically as opposed to other types of simpler traditional software systems based on the rules defined solely by

natural persons to automatically execute operations. It is meant to ensure legal precision and certainty, while also remaining sufficiently abstract and flexible to stay valid despite future technological developments. The definition was drafted for the purposes of the Framework Convention and is not meant to give universal meaning to the relevant term. The Drafters took note of the Explanatory Memorandum accompanying the updated definition of an artificial intelligence system in the OECD Recommendation on Artificial Intelligence (OECD/LEGAL/0449, 2019, amended 2023) for a more detailed explanation of the various elements in the definition. While this definition provides a common understanding between the Parties as to what artificial intelligence systems are, Parties can further specify it in their domestic legal systems for further legal certainty and precision, without limiting its scope.

25. This definition must be read in light of other relevant provisions of the Framework Convention, which refer to (1) the systems with potential to interfere with human rights, democracy, or the rule of law and (2) the graduated and differentiated approach in Article 1 and contextual elements in the Framework Convention's individual provisions (Articles 4 and 5, see the respective commentaries in paragraphs 37-41, 42-48 below).

Article 3 – Scope

26. This Framework Convention has a broad scope to encompass the activities within the lifecycle of article intelligence systems that have the potential to interference with human rights, democracy and rule of law.

27. Consistent with Recommendation No. R (84) 15 of the Committee of Ministers to member States Relating to Public Liability of 18 September 1984, the Drafters' shared understanding is that the term "public authority" means any entity of public law of any kind or any level (including supranational, State, regional, provincial, municipal, and independent public entity) and any private person when exercising prerogatives of official authority.

28. Subparagraph 1 (a) obliges the Parties to ensure that such activities within the lifecycle of artificial intelligence systems comply with the provisions of this Framework Convention when undertaken by public authorities as well as private actors acting on their behalf. This would include an obligation to comply with the provisions of this Framework Convention in regard to activities for which public authorities delegate their responsibilities to private actors or direct them to act, such as activities by private actors operating pursuant to a contract with a public authority or other private provision of public services, as well as public procurement and contracting.

29. Subparagraph 1 (b) obliges all Parties to address risks and impacts to human rights, democracy and the rule of law in the private sector also for private actors to the extent these are not already covered under subparagraph 1 (a). Further, references to object and purpose have the effect of importing all of the concepts of Article 1, i.e. addressing risks is not merely acknowledging those risks, but requires the adoption or maintaining of appropriate legislative, administrative or other measures to give effect to this provision as well as co-operation between the Parties as in the provisions on the follow-up mechanism and international co-operation. However, the obligation does not necessarily require additional legislation and Parties may make use of other appropriate measures, including administrative and voluntary measures. So while the obligation is binding and all Parties should comply with it, the nature of the measures taken by the Parties could vary. In any case, when implementing the obligation under paragraph 1, subparagraph (b), a Party may not derogate from or limit the application of its international obligations undertaken to protect human rights, democracy and rule of law.

30. To ensure legal certainty and transparency, each Party is obliged to set out in a declaration how it intends to meet the obligation set out in this paragraph, either by applying the principles and obligations set forth in Chapters II to VI of the Framework Convention to activities of private actors or by taking other appropriate measures to fulfil the obligation set out in this paragraph. For Parties that have chosen not to apply the principles and the obligations of the Framework Convention in relation to activities of other private actors, the Drafters expect the approaches of those Parties to develop over time as their approaches to regulate the private sector evolve.

31. All Parties should submit their declarations to the Secretary General of the Council of Europe at the time of signature, or when depositing an instrument of ratification, acceptance, approval or accession. Since it is important for Parties to the Framework Convention to know what declarations have been formulated, the Secretary General of the Council of Europe will immediately share the declarations received with the other Parties. Parties may, at any time and in the same manner, amend their declarations.

32. While maintaining a broad scope of the Framework Convention, paragraph 2 envisages that a Party is not required to apply this Framework Convention to the activities within the lifecycle of artificial intelligence systems related to the protection of its national security interests, regardless of the type of entities carrying out the corresponding activities. Such activities must nevertheless be conducted in a manner consistent with the applicable international law obligations, since national security is included in the scope of many international human rights treaties, such as but not limited to the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, ECHR), the American Convention on Human Rights (Pact of San José), the United Nations (UN) International Covenant on Civil and Political Rights (ICCPR) and the UN International Covenant on Economic, Social and Cultural Rights (ICESCR). Activities to protect national security interests that interfere with human rights must be provided for by law, respect the essence of the human rights and, as applicable within the scope of the aforementioned obligations, constitute a necessary and proportionate measure in a democratic society. These activities must also be conducted with respect for the Parties' democratic processes and institutions, as provided for in their domestic legislation in compliance with applicable international law. This exception from the scope of the Framework Convention applies only if and insofar the activities relate to the protection of national security interests. This maintains in the scope of the Framework Convention activities regarding 'dual use' artificial intelligence systems insofar as these are intended to be used for other purposes not related to the protection of the Parties' national security interests and are within the Party's obligations under Article 3. All regular law enforcement activities for the prevention, detection, investigation, and prosecution of crimes, including threats to public security, also remain within the scope of the Framework Convention if and insofar as the national security interests of the Parties are not at stake.

33. As regards paragraph 3, the wording reflects the intent of the Drafters to exempt research and development activities from the scope of the Framework Convention under certain conditions, namely that the artificial intelligence systems in question have not been made available for use, and that the testing and other similar activities do not pose a potential for interference with human rights, democracy and the rule of law. Such activities excluded from the scope of the Framework Convention should in any case be carried out in accordance with applicable human rights and domestic law as well as recognised ethical and professional standards for scientific research.

34. It is also the intent of the Drafters to consider that artificial intelligence systems that are made available for use as a result of such research and development activities would need in principle to comply with the Framework Convention, including in regard to their design and development.

35. The exemption for research and development activities contained in paragraph 3 should be implemented without prejudice to the principle of "safe innovation", see Article 13, and the exchange between Parties on information about risks, as well as significant positive or negative effects on human right, democracy and the rule of law, arising in research contexts, see Article 25, paragraph 2, on "international co-operation".

36. For the exemption of "matters relating to national defence" from the scope of the Framework Convention, the Drafters decided to use language taken from Article 1, d, of the Statute of the Council of Europe (ETS No. 1) which states that "[m]atters relating to national defence do not fall within the scope of the Council of Europe". This exemption does not imply that activities within the lifecycle of artificial intelligence systems relating to national defence are not covered by international law.

Chapter II: General obligations

Article 4 – Protection of human rights

37. This provision refers to the obligations of each Party in the sphere of human rights protection, as enshrined in applicable international and domestic law, with respect to activities within the lifecycle of artificial intelligence systems.

38. Under international law, the Parties have the duty to ensure that their domestic law is in conformity with their international legal obligations, which includes obligations under international treaties which are binding on them. International human rights law establishes the obligation for each Party to respect, protect, and fulfil human rights. Each Party has an obligation to ensure that its domestic law is in conformity with its applicable international human rights obligations. At the same time, Parties are free to choose the ways and means of implementing their international legal obligations, provided that the result is in conformity with those obligations. This is an obligation of result and not an obligation of means. In this respect, the principle of subsidiarity is essential, putting upon the Parties the primary responsibility to ensure respect for human rights and to provide redress for violations of human rights.

39. Below is a list of the main global and regional international human rights instruments and treaties to which various States that negotiated the Framework Convention may be Parties to (in chronological order):

United Nations instruments:

1. The 1965 United Nations International Convention on the Elimination of All Forms of Racial Discrimination (ICERD);
2. The 1966 United Nations International Covenant on Civil and Political Rights and its Optional Protocols (ICCPR);
3. The 1966 United Nations International Covenant on Economic, Social and Cultural Rights (ICESCR) and its Optional Protocol;
4. The 1979 United Nations Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and its Optional Protocol;
5. The 1984 United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment and its Optional Protocol;
6. The 1989 United Nations Convention on the Rights of the Child (UNCRC) and its Optional Protocols;
7. The 2006 United Nations Convention for the Protection of All Persons from Enforced Disappearance; and
8. The 2006 United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) and its Optional Protocol.

Council of Europe and EU instruments:

1. The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, ECHR) and its Protocols;
2. The 1961 European Social Charter (ETS No. 35, ESC) and its protocols and the 1996 Revised European Charter (ETS No. 163);
3. The 1981 Convention for the Protection of Individuals with Regard to Automatic Processing Personal Data, as amended (ETS No.108, CETS No 223) and its Protocols;
4. The 1987 European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (ETS No. 126) and its Protocols;

5. The 1997 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164, the Oviedo Convention) and its Protocols;
6. The 1998 Framework Convention for the Protection of National Minorities (ETS No. 157);
7. The 2000 Charter of Fundamental Rights of the European Union (CFR, recognised with the same legal value as the Treaties pursuant to Article 6 (1) of the Treaty on EU);
8. The 2005 Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197);
9. The 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, the Lanzarote Convention); and
10. The 2011 Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (CETS No. 210, the Istanbul Convention);

Other regional instruments:

1. The 1969 American Convention on Human Rights (Pact of San José) and its first additional Protocols;
2. The 1985 Inter-American Convention to Prevent and Punish Torture;
3. The 1994 Inter-American Convention on the Forced Disappearance of Persons;
4. The 1994 Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women;
5. The 1999 Inter-American Convention on the Elimination of All Forms of Discrimination against Persons with Disabilities;
6. The 2013 Inter-American Convention against Racism, Racial Discrimination, and Related Forms of Intolerance; and
7. The 2015 Inter-American Convention on Protecting the Human Rights of Older Persons.

40. In addition to the legal obligations resulting from international human rights law, Article 4 of the Framework Convention also refers to the protection of human rights in each Party's domestic law. These typically include constitutional and other subordinate norms and rules, as well as mechanisms for supervision and enforcement of their implementation, which aim to protect human rights. The Drafters wished to clarify that reference to domestic law in this provision and elsewhere is not intended to serve as providing for an exemption from the obligations of the Parties to comply with their international law obligations.

41. Against the above background, the general obligation in Article 4 of the Framework Convention requires Parties to take stock of their existing human rights obligations, frameworks and mechanisms in their domestic legal system and, in line with the approach described in Article 1, paragraph 2, ensure that the existing frameworks, rules and mechanisms continue to protect and promote human rights, consistent with international human rights obligations, and are sufficient and effective to respond to the evolving artificial intelligence landscape.

Article 5 – Integrity of democratic processes and respect for the rule of law

42. Artificial intelligence technologies possess significant potential to enhance democratic values, institutions, and processes. Potential impacts include the development of a deeper comprehension of politics among citizens, enabling increased participation in democratic debate or improving the integrity of information in online civic space. Similarly, political representatives, candidates, public officials or public representatives can establish closer connections with individuals, ultimately enhancing the ability of political representatives, public officials or public representatives to represent the public more effectively. This alignment

between political representatives, public officials or public representatives and citizens has the potential to transform electoral campaigns and significantly enhance the policymaking process, fostering greater inclusiveness, transparency and efficiency.

43. Concerns regarding the use of artificial intelligence in politics have long been present, but those specifically associated with democracies and the electoral process have intensified with recent technological advancements. The recently introduced applications of this emerging technology could pose numerous threats to democracy and human rights, serving as a potent tool for fragmenting the public sphere and undermining civic participation and trust in democracy. Such tools could enable users, including malicious actors, to disseminate disinformation and misinformation that could undermine information integrity (including through the use of AI-generated content or AI-enabled manipulation of authentic content) and, where applicable, the right of access to information; make prejudiced decisions about individuals, potentially resulting in discriminatory practices; influence court rulings, with potential implications for the integrity of the justice system; and undertake illegal or arbitrary surveillance, leading to restrictions on the freedom of assembly or freedom of expression, and privacy.

44. The use of artificial intelligence technology in the above-described manner could escalate tensions or undermine public trust which is a main element of an effective democratic government. Artificial intelligence has the capability to generate false information or lead to the exclusion of individuals or those who may be underrepresented or in a vulnerable situation from the democratic processes. It could also exacerbate manipulative content curation. Despite its advantageous aspects, artificial intelligence carries the significant risk to negatively impact the democratic process and the exercise of relevant human rights. However, with the implementation of appropriate safeguards, these technologies may prove beneficial to democracy.

45. In Article 5, the Drafters wished to point towards specific sensitive contexts (paragraph 1 covering mainly the relevant institutional aspects and paragraph 2 covering principally the relevant democratic processes) where a potential use of artificial intelligence should be preceded by a careful consideration of risks to democracy and the rule of law and accompanied with appropriate rules and safeguards. Despite the lack of a commonly agreed upon definition of the term "democratic institutions and processes", the reference is being made to all systems of government with certain basic features and institutions which are common to all democratic countries.

46. In implementing its obligations to protect democratic institutions and processes under Article 5, Parties may wish to focus, for example, on the risks of artificial intelligence systems to:

(a) the principle of separation of powers (in executive, legislative and judicial branches);

(b) an effective system of checks and balances between the three branches of government, including effective oversight of the executive branch;

(c) where applicable, a balanced distribution of powers between different levels of government (so-called vertical separation of powers);

(d) political pluralism (ensured in large part by the protection of human rights the respect of which is essential for a thriving democracy, such as freedom of expression, freedom of association and freedom of peaceful assembly; and existence of pluralist and independent media and a range of political parties representing different interests and views) and fair access to and participation in public debate;

(e) participation in democratic processes through free and fair elections, and a plurality of forms of meaningful civil and political participation;

(f) political majority rule coupled with respect of the rights of political minority(ies);

(g) respect for the rule of law (generally encompassing the principles of legality, legal certainty and non-arbitrariness) and the principle of access to justice and its proper administration; and

(h) respect for the principle of judicial independence.

47. Furthermore, the integrity of democracy and its processes is based on two important assumptions referred to in Article 7, namely that individuals have agency (capacity to form an opinion and act on it) as well as influence (capacity to affect decisions made on their behalf). Artificial intelligence technologies can strengthen these abilities but, conversely, can also threaten or undermine them. It is for this reason that paragraph 2 of the provision refers to the need to adopt or maintain measures that seek to protect "the ability [of individuals] to freely form opinions". With respect to public sector uses of artificial intelligence, this could refer to, for example, general cybersecurity measures against malicious foreign interference in the electoral process or measures to address the spreading of misinformation and disinformation.

48. At the same time, this provision is not intended to create, reduce, extend or otherwise modify the existing applicable standards regarding any human rights, including freedom of expression (such as for instance regarding political advertising), freedom of association and freedom of assembly, as provided for in each Party's applicable international obligations and domestic human rights law.

Chapter III: Principles related to activities within the lifecycle of artificial intelligence systems

Article 6 – General approach

49. This provision makes clear that the principles contained in this Chapter should be incorporated into the Parties' domestic approaches to the regulation of artificial intelligence systems. As such, they are purposefully drafted at a high level of generality, with the intention that they should be overarching requirements that can be applied flexibly in a variety of rapidly changing contexts. They are also purposive, expressing the reason behind the rule and have very broad application to a diverse range of circumstances.

50. The Drafters wished to make it clear that the implementation of this Chapter, in line with the obligations set out in Articles 4 and 5, should be carried out by each Party in line with the approach described in Article 1, paragraph 2, in a manner appropriate to its domestic legal system, and also taking into account the other obligations contained in this Framework Convention.

51. This point is particularly important insofar as, as already mentioned earlier, by virtue of their respective international human rights obligations each Party already has a detailed legal regime of human rights protection with its own set of rules, principles and practices regarding the scope, content of rights and possible restrictions, derogations or exceptions to these rights as well as the functioning of the applicable supervision and enforcement mechanisms.

52. Furthermore, nothing in this Framework Convention is intended to impact existing human rights obligations whenever they overlap with the principles in Chapter III.

Article 7 – Human dignity and individual autonomy

53. This provision emphasises the importance of human dignity and individual autonomy as part of human-centric regulation and governance of the activities within the lifecycle of artificial intelligence systems that fall in the scope of the Framework Convention. Activities within the lifecycle of artificial intelligence systems should not lead to the dehumanization of individuals, undermine their agency or reduce them to mere data points, or anthropomorphise artificial intelligence systems in a way which interferes with human dignity. Human dignity requires acknowledging the complexity and richness of human identity, experience, values, and emotions.

54. Upholding human dignity implies respecting the inherent value and worth of each individual, regardless of their background, characteristics, or circumstances and refers in particular to the manner in which all human beings should be treated. Since the dignity of the human person is universally agreed as constituting the basis of human rights [4], the reference to it as the first principle of Chapter III highlights the global character of the Framework Convention since all Parties recognise the inherent dignity of the human person as an underlying basis of human rights, democratic participation and the rule of law.

55. Individual autonomy is one important aspect of human dignity and refers to the capacity of individuals for self-determination; that is, their ability to make choices and decisions, including without coercion, and live their lives freely. In the context of artificial intelligence, individual autonomy requires that individuals have control over the use and impact of artificial intelligence technologies in their lives, and that their agency and autonomy are not thereby diminished. Human-centric regulation acknowledges the significance of allowing individuals to shape their experiences with artificial intelligence, ensuring that these technologies enhance rather than infringe upon their autonomy. The Drafters considered that referring to this concept in this Framework Convention is particularly appropriate in view of the capacity of artificial intelligence systems for imitation and manipulation.

Article 8 – Transparency and oversight

56. Due to certain features that distinguish artificial intelligence systems from traditional computing systems, which may include complexity, opacity, adaptability, and varying degrees of autonomy, activities within the lifecycle of artificial intelligence systems falling within the scope of the Framework Convention require appropriate safeguards in the form of transparency and oversight mechanisms.

57. The principle of transparency in Article 8 refers to openness and clarity in the governance of activities within the lifecycle of artificial intelligence systems and means that the decision-making processes and general operation of artificial intelligence systems should be understandable and accessible to appropriate artificial intelligence actors and, where necessary and appropriate, relevant stakeholders. In certain cases, this could also refer to providing additional information, including, for example, on the algorithms used, subject to security, commercial and intellectual property and other considerations, as detailed in paragraph 62 below. The means of ensuring transparency would depend on many different factors such as, for instance, the type of artificial intelligence system, the context of its use or its role, and the background of the relevant actor or affected stakeholder. Moreover, relevant measures include, as appropriate, recording key considerations such as data provenance, training methodologies, validity of data sources, documentation and transparency on training, testing and validation data used, risk mitigation efforts, and processes and decisions implemented, in order to aid a comprehensive understanding of how the artificial intelligence system's outputs are derived and impact human rights, democracy and the rule of law. This will in particular help to ensure accountability and enable persons concerned to contest the use or outcomes of artificial intelligence system, where and as applicable (see the commentary to Article 14, in paragraphs 95-102).

58. Providing transparency about an artificial intelligence system could thus require communicating appropriate information about the system (such as, for instance, purpose(s), known limitations, assumptions and engineering choices made during design, features, details of the underlying models or algorithms, training methods and quality assurance processes). The term 'algorithmic transparency' is often used to describe openness about the purpose, structure and underlying actions of an algorithm-driven system. Additionally, transparency may involve, as appropriate, informing persons concerned or the wider public about the details of data used to create, train and operate the system and the protection of personal data along with the purpose of the system and how it was designed, tested and deployed. Transparency should also include informing persons concerned about the processing of information and the types and level of automation used to make consequential decisions, and the risks associated with the use of the artificial intelligence system. Providing transparency could in addition facilitate the possibility for parties with legitimate interests, including copyright holders, to exercise and enforce their intellectual property rights.

59. The provision also provides for measures with regards to the identification of AI-generated content in order to avoid the risk of deception and enable distinction between authentic, human-generated content and AI-generated content as it becomes increasingly hard for people to identify. Such measures could include techniques such as labelling and watermarking – which usually involves embedding a recognisable signature into the output of artificial intelligence system – subject to the availability of these technologies and their proven effectiveness, the generally acknowledged state of the art, and specificities of different types of content.

Promoting the use of technical standards, open-source licences and the collaboration of researchers and developers supports the development of more transparent artificial intelligence systems in the long run.

60. It is important to underline two important aspects of the principle of transparency, notably explainability and interpretability. The term "explainability" refers to the capacity to provide, subject to technical feasibility and taking into account the generally acknowledged state of the art, sufficiently understandable explanations about why an artificial intelligence system provides information, produces predictions, content, recommendations or decisions, which is particularly crucial in sensitive domains such as healthcare, finance, immigration, border services and criminal justice, where understanding the reasoning behind decisions produced or assisted by an artificial intelligence system is essential. In such cases transparency could, for instance, take the form of a list of factors which the artificial intelligence system takes into consideration when informing or making a decision.

61. Another important aspect of transparency is interpretability, which refers to the ability to understand how an artificial intelligence system makes its predictions or decisions or, in other words, the extent to which the outputs of artificial intelligence systems can be made accessible and understandable to experts and non-experts alike. It involves making the internal workings, logic, and decision-making processes of artificial intelligence systems understandable and accessible to human users, including developers, stakeholders, and end-users, and persons affected. Both aspects are also crucial in meeting the requirements mentioned in Articles 12, 13 and 14 in.general and paragraph (b) in particular, and in Article 16. Additionally, the Drafters wished to underline that transparency in the context of artificial intelligence systems is subject to technological limitations – often the precise pathway to a particular outcome of an artificial intelligence system is not readily accessible even to those who design or deploy it. The realisation of the principle of transparency in such circumstances is a question of degree, the state of the art, circumstances and context.

62. Since the disclosure of some of this information in pursuit of transparency may run counter to privacy, confidentiality (including, for instance, trade secrets), national security, protection of the rights of third parties, public order, judicial independence as well as other considerations and legal requirements, in implementing this principle Parties are required to strike a proper balance between various competing interests and make the necessary adjustments in the relevant frameworks without altering or modifying the underlying regime of the applicable human rights law.

63. As regards the second principle referred to in this provision, oversight in the context of artificial intelligence systems refers to various mechanisms, processes, and frameworks designed to monitor, evaluate, and guide activities within the lifecycle of artificial intelligence systems. These can potentially consist of legal, policy and regulatory frameworks, recommendations, ethical guidelines, codes of practice, audit and certification programmes, bias detection and mitigation tools. They could also include oversight bodies and committees, competent authorities such as sectoral supervisory authorities, data protection authorities, equality and human rights bodies, National Human Rights Institutions (NHRIs) or consumer protection agencies, continuous monitoring of current developing capabilities and auditing, public consultations and engagement, risk and impact management frameworks and human rights impact assessment frameworks, technical standards, as well as education and awareness programmes.

64. One option, in some cases, could be to provide for some form of protection from retaliation for internal whistleblowers who report misconduct and the veracity of public statements by artificial intelligence actors. In this regard, the Drafters wished to make particular reference to Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers.

65. Given the complexity of artificial intelligence systems and difficulty of overseeing them, Parties are encouraged to implement measures ensuring that these systems are designed, developed and used in such a way that there are effective and reliable oversight mechanisms, including human oversight [5], within the lifecycle of artificial intelligence systems. The principle of oversight is more general and thus different from the specific substantive obligation set out in Article 26 of the Framework Convention, which requires Parties to establish or designate effective mechanisms to oversee compliance with the obligations in the Framework Convention,

as given effect by the Parties in their domestic legal system (see the commentary to Article 26 in paragraphs 141-144 below).

Article 9 – Accountability and responsibility

66. The principle of accountability and responsibility in this provision refers to the need to provide mechanisms in order for individuals, organisations, or entities responsible for the activities within the lifecycle of artificial intelligence systems to be answerable for the adverse impacts on human rights, democracy or the rule of law resulting from the activities within the lifecycle of those systems. Namely, the provision requires Parties to establish new frameworks and mechanisms, or to maintain existing frameworks and mechanisms as may then be applied to activities within the lifecycle of artificial intelligence systems to give effect to that requirement. This also may include judicial and administrative measures, civil, criminal and other liability regimes and, in the public sector, administrative and other procedures so that decisions can be contested, or the placement of specific responsibilities and obligations on operators.

67. In line with the approach described in the commentary to Article 4 in paragraphs 37-41 and the commentary to Article 6 in paragraphs 50-51 above, the terms "adverse impacts on human rights, democracy and the rule of law" used in this provision refer principally to the human rights obligations and commitments applicable to each Party's existing frameworks on human rights, democracy and the rule of law. These standards, insofar as applicable, include the notion of a "violation of human rights" contained in Article 2 of the ICCPR, Articles 13, 34, 41 and 46 of the ECHR and Articles 25 and 63 of the Pact of San José. As regards democracy and the rule of law, see in particular the contexts mentioned in the commentary to Article 5 (paragraphs 45 and 46 above) and the relevant applicable existing domestic frameworks regarding the protection of the integrity of democratic processes and institutions.

68. This principle emphasises the need for clear lines of responsibility and the ability to trace actions and decisions back to specific individuals or entities in a way that recognises the diversity of the relevant actors and their roles and responsibilities. This is important to ensure that, for example, in case the use of an artificial intelligence system results in an adverse impact on human rights, democracy or the rule of law, there is a mechanism to identify such outcomes and attribute responsibility in an appropriate manner. In other words, all actors responsible for the activities within the lifecycle of artificial intelligence systems, irrespective of whether they are public or private organisations, must be subject to each Party's existing framework of rules, legal norms and other appropriate mechanisms so as to enable effective attribution of responsibility applied to the context of artificial intelligence systems.

69. The principle of accountability and responsibility is inseparable from the principle of transparency and oversight, since the mechanisms of transparency and oversight enable accountability and responsibility by making clearer how artificial intelligence systems function and produce outputs. When the relevant stakeholders understand the underlying processes and algorithms, it becomes easier to trace and assign responsibility in the event of adverse impacts on human rights, democracy or the rule of law, including violations of human rights.

70. Finally, due to the previously described features of an artificial intelligence lifecycle, the principle of accountability and responsibility also includes the requirement for States to adopt or maintain measures aimed at ensuring that those responsible for artificial intelligence systems consider the potential risks to human rights, democracy and the rule of law resulting from the activities within the lifecycle of artificial intelligence systems. This includes proactive action in preventing and mitigating both the risks and adverse impacts to human rights, democracy or the rule of law (see the commentary to Article 16 in paragraphs 105-112).

Article 10 – Equality and non-discrimination

71. In formulating Article 10, paragraph 1, which mentions "equality, including gender equality and the prohibition of discrimination, as provided under applicable international and domestic law", the Drafters' intention was to refer specifically to the body of the existing human rights law consisting of international (at both global and regional levels) and domestic legal instruments applicable to each Party, which together provide a

solid legal basis and guidance for each Party to consider what measures to adopt or maintain, with a view to ensuring equality and prohibition of discrimination in respect of the issues in the relevant spheres in the context of activities within the lifecycle of artificial intelligence systems.

72. At the global level, frameworks relevant to each Party may include the following provisions:

(a) Article 2, 24 and 26 of the ICCPR;

(b) Articles 2, 3 and Article 7 of the ICESCR; and

(c) Specialised legal instruments such as the ICERD, the CEDAW, the UNCRC and the UNCRPD.

73. At the regional level, frameworks relevant to each Party may include:

(a) Article 14 of the ECHR and its Protocol No. 12;

(b) Paragraphs 20 and 27 of Part I, Article 20 of Part II and Article E of Part V of the ESC;

(c) Specialised legal instruments of the Council of Europe such as Article 4 of the Framework Convention for the Protection of National Minorities and Article 4 of the Istanbul Convention;

(d) Title III of the EU Charter of Fundamental Rights, EU Treaties (e.g., Article 2 of the Treaty on the European Union, Article 10 of the Treaty on the Functioning of the European Union), EU secondary legislation [6] and the relevant case-law of the Court of Justice of the European Union;

(e) Article 24 of the Pact of San José; and

(f) Specialised legal instruments, such as the 1999 Inter-American Convention on the Elimination of All Forms of Discrimination against Persons with Disabilities; the 2013 Inter-American Convention against Racism, Racial Discrimination, and Related Forms of Intolerance and the 2015 Inter-American Convention on Protecting the Human Rights of Older Persons.

74. Parties should consider relevant elements of their domestic law, which could include constitutional law, statutes, and jurisprudence.

75. The Drafters also reflected on the real and well-documented risk of bias that can constitute unlawful discrimination arising from the activities within the lifecycle of artificial intelligence systems. The Framework Convention requires the Parties to consider appropriate regulatory, governance, technical or other solutions to address the different ways through which bias can intentionally or inadvertently be incorporated into artificial intelligence systems at various stages throughout their lifecycle. The following issues have been well-documented with regard to some artificial intelligence systems:

(a) potential bias of the algorithm's developers (e.g. due to the conscious or unconscious stereotypes or biases of developers);

(b) potential bias built into the model upon which the systems are built;

(c) potential biases inherent in the training data sets used (e.g. when the data-set is accurate or not sufficiently representative), or in the aggregation or evaluation of data (e.g. where groups are inappropriately combined, or if benchmark data used to compare the model to other models does not adequately represent the population that the model would serve);

(d) biases introduced when such systems are implemented in real world settings (e.g. exposure to a biased environment once it is being used, or due to a biased use of the artificial intelligence system, malicious use or attacks that intentionally introduce bias by manipulating the artificial intelligence system) or as artificial intelligence evolves by self-learning due to errors and deficiencies in determining the working and learning parameters of the algorithm, or

(e) automation or confirmation biases, whereby humans may place unjustified trust in machines and technological artefacts or situations where they select information that supports their own views, in both cases ignoring their own potentially contradictory judgment and validating algorithmic outputs without questioning them.

76. The issues of equality in the specific artificial intelligence context include relatively new categories of problems such as 'technical bias', which occurs from problems in applying machine learning that results in additional biases that are not present in the data used to train the system or make decisions; and 'social bias', i.e. failures to properly account for historical or current inequalities in society in the activities within the lifecycle of artificial intelligence systems such as designing and training models. These inequalities include, for example, historical and structural barriers to gender equality and to fair and just treatment for persons belonging to groups that have been or are still partly underserved, discriminated against, or otherwise subject to persistent inequality. These issues also include the recognition that various individuals experience different impacts based on factors which are linked to their personal characteristics, circumstances or membership of a group, including those covered by the relevant and applicable instruments included in paragraphs 72 and 73 of the Explanatory Report as interpreted by the relevant jurisprudence and practices of international human rights treaty bodies.

77. The provision makes clear that the required approach under this article should not stop at simply requiring that a person not be treated less favourably "without objective and reasonable justification" based on one or more protected characteristics that they possess in relevant matters of a protected sector. Parties undertake to adopt new or maintain existing measures aimed at overcoming structural and historical inequalities, to the extent permitted by its domestic and international human rights obligations, and moreover these processes should be, where appropriate, informed by the views of those impacted.

78. Mindful of conceptual, doctrinal, legal and technical differences between the ways these issues are addressed in the domestic legal systems of various Parties and in order to provide the Parties with the necessary flexibility in this regard, the Drafters inserted a formulation which enables each Party to comply with the obligation set out in paragraph 2 of Article 10 in line with its own applicable domestic and international human rights obligations and commitments by applying the applicable existing frameworks to the context of activities within the lifecycle of artificial intelligence systems.

Article 11 – Privacy and personal data protection

79. The protection of privacy rights and personal data protection is a common principle required for effectively realising many other principles in this Framework Convention. Personal data collection is already ubiquitous not only as the basis of business models across many industries, but also as one of the key activities of government agencies, including law enforcement authorities, which use a variety of technologies and automated systems that collect, process and generate personal data in decision-making processes that directly impact people's lives. With artificial intelligence systems being principally data-driven, in the absence of appropriate safeguards the activities falling within the lifecycle of such systems could pose serious risks to the privacy of individuals.

80. Despite some differences in the legal traditions, specific rules and protection mechanisms, the States which negotiated the Framework Convention share a strong commitment to the protection of privacy, for example, as enshrined at the global level in Article 17 of the ICCPR and regionally in Article 8 of the ECHR, Article 8 of the EU Charter and Article 11 of the Pact of San José.

81. At its core, privacy rights of individuals entail partially overlapping elements with varying degrees of legal recognition and protection across jurisdictions, such as: (1) protected interest in limiting access to an individual's life experiences and engagements (2) protected interest in secrecy of certain personal matters (3) degree of control over personal information and data (4) protection of personhood (individuality or identity, dignity, individual autonomy) and (5) protection of intimacy and physical, psychological or moral integrity. The provision underlines these various approaches by pointing at some of the key commonalities

in this sphere, even though it is not intended to endorse or require any particular regulatory measures in any given jurisdiction.

82. In view of the key role that the protection of personal data plays in safeguarding privacy rights and other human rights in the digital world, the Drafters made a specific mention in the text of the provision of the domestic and international laws, standards and frameworks in the sphere of personal data protection. In order to underline their importance in ensuring effective protection in the artificial intelligence context, Article 11, subparagraph (b) also explicitly refers to other "guarantees and safeguards" that individuals (also called "data subjects" in some jurisdictions) usually enjoy by virtue of such laws, standards and frameworks. The Drafters consider this obligation to require Parties to take measures to protect privacy.

83. One such instrument is the Council of Europe's Convention 108+, which covers both the public and private sectors and it is open to accession by States at a global level. At the EU level, the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") is a comprehensive data protection law that applies to natural or legal persons that process personal data belonging to natural persons in the European Union regardless of whether the processing takes place in the European Union or not. At the domestic level, most of the States which negotiated the Framework Convention have dedicated personal data or privacy protection laws and often specialised authorities responsible for the proper supervision of the relevant rules and regulations.

Article 12 – Reliability

84. This provision points to the potential role to be played by standards, technical specifications, assurance techniques and compliance schemes in evaluating and verifying the trustworthiness of artificial intelligence systems and for transparently documenting and communicating evidence for this process. Standards, in particular, could provide a reliable basis to share common expectations about certain aspects of a product, process, system or service with a view to building justified confidence in the trustworthiness of an artificial intelligence system if its development and use are compliant with these standards.

85. This provision highlights the importance of establishing measures that seek to assure the reliability of artificial intelligence systems through measures addressing key aspects of functioning such as robustness, safety, security, accuracy and performance as well as functional prerequisites such as data quality and accuracy, data integrity, data security, and cybersecurity. Relevant standards, requirements, assurance and compliance schemes may cover these elements as a precondition for successfully building justified public trust in artificial intelligence technologies.

86. Technical standards can help deliver mutually understood and scalable artificial intelligence assurance and compliance, while it must be ensured that they are developed in a transparent and inclusive process that encourages consistency with applicable international and domestic human rights instruments.

87. In addition, measures to be adopted or maintained under this provision should aim at ensuring that, like any other software system, artificial intelligence systems are "secure and safe by design", which means that the relevant artificial intelligence actors should consider the security and safety as core requirements, not just technical features. They should prioritise security and safety throughout the entire lifecycle of the artificial intelligence system.

88. In some cases, it may not be enough to set out standards and rules about the activities within the lifecycle of artificial intelligence systems. Measures to promote reliability may therefore include, depending on the context, providing relevant stakeholders with clear and reliable information about whether artificial intelligence actors have been following those requirements in practice. This means ensuring, as appropriate, end-to-end accountability through process transparency and documentation protocols. There is a clear connection between this principle and the principle of transparency and oversight in Article 8 and the principle of accountability and responsibility in Article 9.

89. Assurance and compliance schemes are important both for securing compliance with rules and regulations, and also for facilitating the assessment of more open-ended risks where rules and regulations alone do not

provide sufficient guidance to ensure that a system is trustworthy. There is an important role for consensus based, technical standards in this context to fill gaps and also to provide guidance on mitigating risks from a technical standpoint (see also the commentary to Article 16 in paragraphs 105 and 112 below).

Article 13 – Safe innovation

90. This provision points at an important theme which lies at the heart of the approach of the Framework Convention: Parties should seek to promote and foster innovation in line with human rights, democracy and the rule of law. One suitable way to stimulate responsible innovation with regard to artificial intelligence is by enabling the authorities in the relevant sector of activity to set up "controlled environments" or "frameworks" to allow development, training, live experimentation and testing of innovations under the competent authorities' direct supervision, in particular to encourage the incorporation of quality, privacy and other human rights concerns, as well as security and safety concerns in the early stages. This is especially important as certain risks associated with artificial intelligence systems can only be effectively addressed at the design stage.

91. It is also important to recognise that some artificial intelligence developers, including those with a public interest mission, cannot proceed with their innovation unless they can be reasonably sure that it will not have harmful implications and incorporate appropriate safeguards to mitigate risks in a controlled environment. Given that innovation is essentially collaborative and path dependent, with new systems building on what has taken place before, there is a risk that this innovation may be impeded because it cannot equally use or build on existing innovations that are not sufficiently secure. This provision is not meant to stifle innovation but recognises that innovation may be shaped as much by regulation as by the absence of it. Failure to create an environment in which responsible innovation can flourish risks stifling such innovation and leaving the playing field open to more reckless approaches.

92. In view of the diversity and underlying complexity of legal systems and regulatory traditions in the States which negotiated the Framework Convention, the provision leaves the specific details of the relevant arrangements up to the Parties provided that the regimes set up under this provision comply with the requirement to "avoid adverse impacts on human rights, democracy and the rule of law". One approach to achieve these goals is, for instance, "regulatory sandboxes" that aim to foster innovation, provide legal certainty and enable regulatory learning. Other approaches include special regulatory guidance or no-action letters to clarify how regulators will approach the design, development, or use of artificial intelligence systems in novel contexts.

93. The approaches pointed at by this provision offer many advantages particularly suitable in the case of artificial intelligence systems, the fast pace of their development and the ubiquitous character of their use:

    (1) By allowing controlled development and testing, validating and verifying of artificial intelligence systems, such approaches may help identify potential risks and issues associated with artificial intelligence systems early in the development process. This proactive approach may enable developers to address concerns before widespread deployment. Sandboxes or the issuance of informal regulatory guidance, for example, provide an environment that simulates real-world conditions, allowing for development and rather realistic testing of artificial intelligence applications. This may help uncover challenges that might not be apparent in isolated testing environments and enables co-operation with the competent authorities in earlier states of the innovation lifecycle.

    (2) Such approaches facilitate knowledge-sharing among private entities, regulators, and other stakeholders. These collaborative environments may foster a better understanding of artificial intelligence technologies, their implications, and potential governance approaches and provide legal certainty to innovators and support them in their compliance journey.

    (3) Artificial intelligence technologies evolve rapidly, and traditional regulatory frameworks may struggle to keep pace. Such approaches make it possible to learn about the opportunities and risks of an innovation at an early stage and provide evidence for regulatory learning purposes and may provide

flexibility for regulations and technologies to be tested to check their adaptability to the changing landscape of artificial intelligence. Based on the result obtained, the framework can be interpreted to take into account these novel challenges and specific contexts, implemented more effectively or, where needed, adjusted.

(4) Such environments may allow regulators to experiment with different regulatory approaches and evaluate their effectiveness in ensuring respect for human rights, democracy and the rule of law, as well as the prevention and mitigation of adverse impact on them. This iterative process may help regulators develop informed policies which strike a balance between fostering innovation and protecting the public interest.

(5) The existence of such approaches can boost public and industry confidence by demonstrating that regulators are actively engaged in understanding and overseeing artificial intelligence technologies to ensure respect for human rights, democracy and the rule of law. This transparency contributes to building trust in the responsible development and deployment of artificial intelligence.

(6) Such approaches allow organisations developing and deploying artificial intelligence systems, which could also include other stakeholders, as appropriate, to work closely with regulators to understand and meet compliance requirements. This collaborative approach helps streamline the regulatory process and compliance that is particularly helpful for smaller companies who lack the necessary resources.

Chapter IV: Remedies

94. Since the obligations in this Chapter are intended to complement each Party's applicable international and domestic legal regime of human rights protection, which includes not only specific rules and procedures but also diverse institutions and supervisory and enforcement mechanisms, the implementation of the obligations in this Chapter should be carried out by each Party applying their existing frameworks to the context of artificial intelligence systems. In doing so, Parties should have in mind the object and purpose of the Framework Convention, which is to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.

Article 14 – Remedies

95. As already mentioned, each Party already has in place existing frameworks in relation to human rights, democracy and the rule of law. The Framework Convention requires Parties to apply those existing frameworks to the context of activities within the lifecycle of artificial intelligence systems.

96. Due to certain unique characteristics of artificial intelligence systems, such as their technical complexity, their data-driven character and the relative opaqueness of the operations of some such systems, human interactions with artificial intelligence systems have been affected by the problem of opaqueness of artificial intelligence systems and information asymmetry, i.e. a significant imbalance in the access to, understanding of, or control over information between different parties involved in the activities within the lifecycle of artificial intelligence systems.

97. This problem is particularly acute in situations where human rights are adversely impacted by the activities within the lifecycle of artificial intelligence systems, as the affected or potentially affected persons may not become aware of such impacts or have the necessary information to exercise their rights in this connection or avail themselves of relevant procedures and safeguards.

98. That is why this provision recalls the principle that a remedy needs to be both effective and accessible. In order to be effective, the remedy must be capable of directly remedying the impugned situations, and in order to be accessible, it has to be available with sufficient procedural safeguards in place to make the remedy meaningful for the person concerned. In order to underline the link and ensure complementarity with the applicable international and domestic human rights protection mechanisms, the provision uses

the legal terminology referenced in Article 2 of the ICCPR, Article 13 of the ECHR and Article 25 of the Pact of San José. The term of "violations of human rights" used in the first paragraph of this provision refers to the well-established notions contained in Article 2 of the ICCPR, Articles 13, 34, 41 and 46 of the ECHR and Articles 25 and 63 of the Pact of San José, if and as applicable to respective future Parties of this Framework Convention (see the commentary in paragraph 67 above).

99. Consistent with the principles in Articles 8 (Principle of transparency and oversight) and 9 (Principle of accountability and responsibility), Article 14 of the Framework Convention requires Parties to adopt or maintain specific measures to document and make available certain information to the affected persons in order to support the aim of making available, accessible and effective remedies for violations of human rights in the context of activities in the lifecycle of an artificial intelligence system. The relevant content in the information-related measures should be context-appropriate, sufficiently clear and meaningful, and critically, provide a person concerned with an effective ability to use the information in question to exercise their rights in the proceedings in respect of the relevant decisions affecting their human rights. It is also important to recall that exceptions, limitations or derogations from such transparency obligations are possible in the interest of public order, security and other important public interests as provided for by applicable international human rights instruments and, where necessary, to meet these objectives.

100. For violations of human rights resulting from the activities within the lifecycle of artificial intelligence systems, it is also important to provide the persons concerned with an effective possibility to lodge a complaint to competent authorities, as specified in Article 14, paragraph 2, subparagraph (c) of the Framework Convention. This may include the oversight mechanism(s) referred to in Article 25. In some situations, effective redress may include complaints by public interest organisations, in accordance with a Party's domestic legal system.

101. The Drafters wished to underline that the expressions "significantly affect human rights" in subparagraph (a) of paragraph 2 of Article 14 and "significantly impact(s) upon the enjoyment of human rights" in paragraph 1 of Article 15 both introduce a threshold requirement, which means that (1) the relevant requirements of Articles 14 and 15 do not apply automatically to all artificial intelligence systems falling within the scope of Article 3 of the Framework Convention; (2) that the artificial intelligence systems which have no significant effect or impact on human rights do not fall within the scope of the specific new obligations in this Article; and (3) it is up to the Parties of the Framework Convention to examine whether, in view of their existing international and domestic human rights law and the context and other relevant circumstances in relation to a given artificial intelligence system, such system can be said to have "significant effect" or "significant impact" on human rights.

102. Likewise, the expression "substantially informed by the use of the [artificial intelligence] system" in subparagraph (b) of Article 14 is meant to introduce a threshold requirement which underlines that not every use of an artificial system in decision-making triggers the application of subparagraph (b), and these measures should apply only in cases where the decision has been at least "substantially informed" by the use of the system. It is at the discretion of the Parties to the Framework Convention to define the meaning of this expression, consistent with its applicable international and domestic human rights law.

Article 15 – Procedural safeguards

103. Paragraph 1 of Article 15 sets out a separate obligation for the Parties to ensure that the existing procedural guarantees, safeguards and rights prescribed in the applicable international and domestic human rights law remain available and effective in the artificial intelligence context. Where an artificial intelligence system substantially informs or takes decisions impacting on human rights, effective procedural guarantees should, for instance, include human oversight, including ex ante or ex post review of the decision by humans. Where appropriate, such human oversight measures should guarantee that the artificial intelligence system is subject to built-in operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.

104. Paragraph 2 of Article 15 deals specifically with situations of direct human interaction with an artificial intelligence system. In such cases and where appropriate taking into account the circumstances and context of use, and with a view in particular to avoiding the risk of manipulation and deception, persons interacting with an artificial intelligence system should be duly notified that they are interacting with an artificial intelligence system rather than with a human. For example, interactions with AI-enabled chatbots on government websites would likely trigger the notification obligation under this provision. At the same time, this obligation is not intended, for instance, to cover situations where the very purpose of the use of the system would be counteracted by the notification (law enforcement scenarios) or where the use of the system is obvious from the context, which renders notification unnecessary.

Chapter V: Assessment and mitigation of risks and adverse impacts

Article 16 – Risk and impact management framework

105. In order to take into account the iterative character of the activities within the lifecycle of artificial intelligence systems and also to ensure the effectiveness of the measures undertaken by the Parties, the Framework Convention contains a dedicated provision prescribing the need to identity, assess, prevent and mitigate ex ante and, as appropriate, iteratively throughout the lifecycle of the artificial intelligence system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments. These obligations are one of the key tools for enabling the implementation of the requirements of the Framework Convention and Chapters II and III in particular and should be implemented by the Parties in light of all relevant principles, including the principles of transparency and oversight as well as the principle of accountability and responsibility.

106. The purpose of this provision is to ensure a uniform approach towards the identification, analysis, and evaluation of these risks and the assessment of impacts of such systems. At the same time, it is based on the assumption that the Parties are best placed to make relevant regulatory choices, taking into account their specific legal, political, economic, social, cultural, and technological contexts, and that they should accordingly enjoy a certain flexibility when it comes to the actual governance and regulation which accompany the processes.

107. This is the principal reason why the provision mentions graduated and differentiated measures which should take due account of "the context and intended use of artificial intelligence systems" that allows flexibility to the Parties in the approaches and methodologies they choose to carry out this assessment. In particular, the Parties may choose to implement this assessment at the different levels, such as at regulatory level by prescribing different categories of risk classification and/or at operational level by relevant actors assigned with responsibilities for the activities within the lifecycle of artificial intelligence systems. Parties may also choose to focus at the operational level only on certain pre-defined categories of artificial intelligence systems in line with the graduated and differentiated approach to keep the burden and obligations proportionate to the risks (Article 16, paragraph 2, subparagraph (a)). Parties could also consider the capacity of various categories of private sector actors to respond to these requirements, in particular those regarding documentation and communication with relevant authorities and stakeholders, and where possible and appropriate, adjust them accordingly.

108. The Drafters also wished to clarify that along with the risks to human rights, democracy and the rule of law, the assessments can, where appropriate, take due account of the need to preserve a healthy and sustainable environment, as well as projected benefits for society as a whole and positive impacts on human rights, democracy and the rule of law. Such factors as "severity", "probability", duration and reversibility of risks and impacts are also very important in the artificial intelligence context and should be taken into account in the risk management framework (Article 16, paragraph 2, subparagraph (b)), specifically when identifying and assessing risks and potential impacts. Moreover, it is important to specify that the requirement to take into account the perspective of persons whose rights may be impacted, depending

on context, to the extent practicable and where appropriate, entails considering the perspective of a variety of relevant stakeholders, such as outside technical experts and civil society (Article 16, paragraph 2, subparagraph (c)).

109. The provision is also based on the understanding that carrying out risk assessment at the beginning of the artificial intelligence system lifecycle is only a first, albeit critical, step in a much longer, end-to-end process of responsible evaluation and re-assessment (Article 16, paragraph 2, subparagraph (d)). In the risk and impact assessment process, attention should be paid both to the dynamic and changing character of activities within the lifecycle of artificial intelligence systems and to the shifting conditions of the real-world environments in which systems are intended to be deployed. The provision further introduces requirements regarding not only the documenting of the relevant information during the risk management processes, but also the application of sufficient preventive and mitigating measures in respect of the risks and impacts identified. It is important for the requirement of proper documentation of the risk and impact management processes in Article 16, paragraph 2, subparagraph (f) to play its role in the identification, assessment, prevention and mitigation of risks or adverse impacts to human rights, democracy or the rule of law arising throughout the lifecycle of artificial intelligence systems. Both technical documentation and documentation of risks and adverse impacts should be properly drawn up and regularly updated. Where appropriate, the documentation may include public reporting of adverse impacts. Testing (Article 16, paragraph 2, subparagraph (g)) may include providing independent auditors with access to aspects of artificial intelligence systems.

110. Paragraph 3 of Article 16 also prescribes the application of measures in respect of the risks and impacts identified, in order to adequately address the adverse impacts of artificial intelligence systems to human rights, democracy and the rule of law.

111. Paragraph 4 of Article 16 states that Parties to the Framework Convention shall assess the need for moratoria, bans, or other appropriate measures regarding uses of artificial intelligence systems that they consider "incompatible" with the respect of human rights, democracy, and the rule of law. The determination of what is "incompatible" in this context is made by each Party, as is the assessment of whether such a scenario would require a moratorium or ban, on the one hand, or another appropriate measure, on the other. Without measures prohibiting, limiting or otherwise regulating the use of artificial intelligence systems in these circumstances, such uses could pose excessive risks to human rights, democracy, and the rule of law.

112. While this provision leaves the details of how to address moratoria, bans or other appropriate measures to each Party, given their gravity, measures like moratoria or bans should only be considered in circumstances where a Party assesses that a particular use of an artificial intelligence system poses an unacceptable risk to human rights, democracy or the rule of law. Further consideration may include, for example, careful examination of whether there are any measures available for mitigating that risk. These measures should also be accompanied with appropriately organised review procedures in order to enable their update, including possible reversal (for example, once relevant risks have been sufficiently reduced or appropriate mitigation measures have become available, or new unacceptable practices have been identified). The Drafters also note the importance of public consultations when discussing measures set out under this provision.

Chapter VI: Implementation of the Convention

Article 17 – Non-discrimination

113. This article prohibits discrimination in the Parties' implementation of the Framework Convention. The meaning of discrimination in Article 17 is identical to that laid out in the applicable international law, such as, inter alia, Article 26 of the ICCPR, Article 2 of the ICESCR, Article 14 of the ECHR and its Protocol No. 12, Article 24 of the Pact of San José, and Article E of the ESC, if and as applicable to Parties to the Framework Convention.

114. Taken together, these provisions cover a broad range of non-discrimination grounds which are linked to individuals' personal characteristics, circumstances or membership of a group, including those covered

by the relevant and applicable instruments included in paragraphs 72 and 73 of the Explanatory Report as interpreted by the relevant jurisprudence and practices of international human rights treaty bodies.

115. Not all of these grounds are explicitly stated or identically formulated in the human rights treaties by which the Parties to the present Framework Convention may be bound. Those treaties usually contain open-ended lists of such grounds, as interpreted by the jurisprudence of competent international courts such as the European and the Inter-American Courts of Human Rights and in the relevant practice of competent international bodies, such as the United Nations Human Rights Committee. There may thus be variations between the various international human rights regimes applicable to different Parties. As with other human rights conventions and treaties, here too the approach of the Framework Convention is not to create new human rights obligations or to reduce, extend or otherwise modify the scope or content of the international human rights obligations applicable to a Party (see the comment to Article 1, in paragraph 13 above).

Article 18 – Rights of persons with disabilities and of children

116. This provision sets out an obligation for the Parties, in the context of the activities within the lifecycle of artificial intelligence systems, to take due account of "specific needs and vulnerabilities in relation to respect of the rights of persons with disabilities and of children" and in this regard it correlates directly with the provisions and the legal regime of the UNCRPD and the UNCRC as well as the applicable domestic law of each Party on the rights of persons with disabilities and the rights of the child. Explicit reference to the applicable domestic law on the rights of the child and the rights of persons with disabilities has been inserted, in particular, with a view to take into consideration the situation of any Party to the Framework Convention which did not ratify the UNCRC or the UNCRPD, but nevertheless has domestic legislation securing the enjoyment of such rights.

117. The reference to domestic law in this provision is meant solely to point at provisions of domestic law which provide the level of protection in the relevant context similar or supplementary to the UNCRPD or the UNCRC, and such reference cannot be invoked by a Party as justification for its failure to perform this treaty obligation. The objective is thus to guarantee the highest possible level of consideration for any specific needs and vulnerabilities in relation to respect of the rights of persons with disabilities and of children, including training on digital literacy, as explained in relation to Article 20 in.the Explanatory Report.

118. In view of the serious risk that artificial intelligence technologies could be used to facilitate sexual exploitation and sexual abuse of children, and the specific risks that it poses to children, in the context of the implementation of this provision the Drafters considered the obligations set forth in the Lanzarote Convention, the Optional Protocol to the UN Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and General Comment No. 25 to the UNCRC on children's rights in relation to the digital environment.

Article 19 – Public consultation

119. The purpose of this article is to prompt the Parties, insofar as appropriate, to foster civic engagement, empower individuals and experts to partake in public discussion on issues of broad social and political importance, and create greater public awareness of the fundamental and emerging questions, including issues applicable to the early stages of design, raised by the activities within the lifecycle of artificial intelligence systems. Views of society and various perspectives should be ascertained and taken into due consideration as far as possible with regard to the relevant problems, which could include, for example, risks as well as positive and adverse impacts. To this end, meaningful "public discussion and multi-stakeholder consultation" are recommended.

120. Engagement should involve engaging a diverse range of stakeholders, including the general public, industry experts, academics, National Human Rights Institutions (NHRIs), and civil society. For the Drafters of the Framework Convention, these discussions and consultations play a crucial role in ensuring that artificial intelligence systems align with universal human rights and address relevant concerns regarding human

rights, democracy and the rule of law, by reflecting a broad range of perspectives and thus informing the relevant policy-making and regulatory initiatives.

121. The expression "as appropriate" leaves it to the Parties to determine the topics, frequency and other modalities of such consultations in the light of social, economic, legal, ethical, environmental and other relevant implications. For example, States may organise surveys and questionnaires, public workshops, focus groups, citizen juries and deliberative polling, expert panels and consultative committees, public hearings, national and international conferences, or combinations of the above. Final assessment and incorporation of the outcomes of such discussions and consultations into the relevant policy initiatives could also be adequately and appropriately communicated to the relevant stakeholders.

Article 20 – Digital literacy and skills

122. The provision draws the attention of the Parties to the fact that promotion of digital literacy and digital skills for all segments of the population is critically important in today's technology-driven world. The two terms refer to the ability to use, understand, and engage with digital, including artificial intelligence and other data-based technologies effectively and thus contribute to promoting broad awareness and understanding in the general population and to preventing and mitigating risks or adverse impacts on human rights, democracy or the rule of law, as well as other societal harms such as malicious or criminal use of such technologies. The Drafters also wished to mention particularly beneficial effects of such programmes for individuals from diverse backgrounds and those who may be underrepresented or in vulnerable situations, which may include, for example, women, girls, indigenous peoples, elderly people and children, with due respect for safeguards regarding the use of artificial intelligence systems for people in situations of vulnerability.

123. Owing to the object and purpose of the Framework Convention, the specific training programmes regarding artificial intelligence technologies referred to under Article 20 could include enhancing awareness of and the ability to manage the potential risks and adverse impacts of artificial intelligence systems in the context of human rights, democracy or the rule of law and, depending on context, could cover such topics as:

a. the concept of artificial intelligence;

b. the purpose of particular artificial intelligence systems;

c. capabilities and limitations of different types of artificial intelligence models and the assumptions underlying them;

d. socio-cultural factors associated with the design, development, and use of artificial intelligence systems, including in relation to data used to train them;

e. human factors relevant to the use of artificial intelligence systems, such as how end users may interpret and use outputs;

f. domain expertise relevant to the context in which artificial intelligence systems are used;

g. legal and policy considerations;

h. perspectives of individuals or communities that disproportionately experience adverse impacts of artificial intelligence systems.

124. In view of how essential training is to those responsible for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence, the provision refers additionally to this specific group of addressees (such actors include, for instance, judiciary, national supervisory authorities, data protection authorities, equality and human rights bodies, ombuds, consumer protection authorities, artificial intelligence providers and artificial intelligence users), in particular with reference to the application of the methodology set out in Article 16.

Article 21 – Safeguard for existing human rights

125. Consistent with the 1969 Vienna Convention on the Law of Treaties, this article seeks to ensure that the Framework Convention harmoniously coexists with other international human rights treaties and instruments, such as those listed in paragraph 39 above.

126. This provision reinforces that the overall aim of this Framework Convention is to ensure the highest level of protection of human rights, democracy and the rule of law in the context of the activities within the lifecycle of artificial intelligence systems. In this context, all references to domestic law in this Framework Convention should be read as limited to cases where domestic law provides for a higher standard of human rights protection than applicable international law.

Article 22 – Wider protection

127. This provision safeguards those provisions of domestic law and existing and future binding international instruments, which provide supplementary protection in respect of activities within the lifecycle of artificial intelligence systems in sensitive contexts from the point of view of human rights, democracy and the rule of law, going beyond the level secured by this Framework Convention; this Framework Convention shall not be interpreted so as to restrict such protection. The phrase "wider measure of protection" can be interpreted as providing the possibility of putting a person, for example, in a more favourable position than provided for under the Framework Convention.

Chapter VII: Follow-up mechanism and co-operation

128. Chapter VII of the Framework Convention contains provisions which aim at ensuring the effective implementation of the Framework Convention by the Parties through a follow-up mechanism and co-operation. This is the mechanism announced in Article 1 paragraph 3.

Article 23 – Conference of the Parties

129. This article provides for the setting-up of a body under the Framework Convention, the Conference of the Parties, composed of representatives of the Parties.

130. The establishment of this body will ensure equal participation of all Parties in the decision- making process and in the Framework Convention follow-up procedure and will also strengthen co-operation between the Parties to ensure proper and effective implementation of the Framework Convention.

131. The flexibility of the follow-up mechanism established by this Framework Convention is reflected by the fact that there is no temporal requirement for its convocation. It will be convened by the Secretary General of the Council of Europe (paragraph 3) as appropriate and periodically (paragraph 2). However, it can only be convened at the request of the majority of the Parties or at the request of the Committee of Ministers of the Council of Europe (paragraph 3).

132. With respect to this Framework Convention, the Conference of the Parties has the traditional follow-up competencies and plays a role in respect of:

(a) the effective implementation of the Framework Convention, by making proposals to facilitate or improve the effective use and implementation of this Framework Convention, including the identification of any problems therein, and the effects of significant legal, policy or technological developments pertaining to the activities within the lifecycle of artificial intelligence systems, as well as the effects of any declaration or reservation made under this Framework Convention;

(b) the amendment of the Framework Convention, by making proposals for amendment in accordance with Article 28, paragraph 1 and formulating its opinion on any proposal for amendment of this Framework Convention which is referred to it in accordance with Article 28, paragraph 3;

(c) a general advisory role in respect of the Framework Convention by expressing specific recommendations on any question concerning its interpretation or application, including, for instance,

suggesting interpretations of legal terms contained in the Framework Convention. Although not legally binding in nature, these recommendations may be seen as a joint expression of opinion by the Parties on a given subject which should be taken into account in good faith by the Parties in their application of the Framework Convention.

(d) serving as a forum for facilitating the exchange of information on significant legal, societal, policy or technological developments in relation to the application of the provisions of the Framework Convention, including in relation to the international co-operation activities described in Article 25;

(e) in accordance with Article 29 of the Framework Convention, facilitating, where necessary, the friendly settlement of disputes related to the application of its provisions, in a non-binding, consultative capacity;

(f) facilitating co-operation with stakeholders, including non-governmental organisations and other bodies which can improve the effectiveness of the follow-up mechanism. In view of the highly technical subject matter of the Framework Convention, paragraph 6 of Article 23 expressly points at the possibility for the Conference of the Parties to seek, where appropriate, relevant expert advice.

133. The Conference of the Parties must adopt rules of procedure establishing the way in which the follow-up system of the Framework Convention operates, on the understanding that its rules of procedure must be drafted in such a way that such follow-up is effectively ensured. The rules of procedure shall be adopted by consensus, namely a decision taken in the absence of sustained objection and without a formal vote. Article 23, paragraph 4 further stipulates that the Conference of the Parties shall adopt such rules within twelve months of the entry into force of the Framework Convention.

134. Paragraph 7 concerns the contribution of Parties which are not member States of the Council of Europe to the financing of the activities of the Conference of the Parties. The contributions of member States to these activities are covered collectively by the ordinary budget of the Council of Europe, whereas non-member States contribute individually, in a fair manner. The Framework Convention does not stipulate the form in which the contributions, including the amounts and modalities, of Parties which are not members of the Council of Europe shall be established. The legal basis for the contribution of such Parties will be the Framework Convention itself and the act(s) establishing that contribution. The Framework Convention does not affect domestic laws and regulations of Parties governing budgetary competencies and procedures for budgetary appropriations. Without prejudice to the agreement referred to above, one of the ways for a Party which is not a member of the Council of Europe to make its payment of contribution is to pay within the limit of budget approved by the legislative branch.

135. Paragraph 8 of this provision gives the Conference of the Parties the authority to deliberate on the limitation of involvement in its proceedings by any Party that has been disqualified from membership of the Council of Europe pursuant to Article 8 of the Statute of the Council of Europe for a serious violation of Article 3 of the Statute. Similar action can be undertaken regarding any Party that is a non-member of the Council of Europe by a decision of the Committee of Ministers of the Council of Europe.

Article 24 – Reporting obligation

136. To enable co-operation and regularly update on the implementation of the Framework Convention, each Party should provide a report to the Conference of the Parties within the first two years after becoming a Party and then periodically thereafter, with details of the activities undertaken to give effect to Article 3, paragraph 1, subparagraphs (a) and (b). The Conference of the Parties will determine the format and the process for the report in accordance with its rules of procedure. The Drafters strongly encourage the Parties to invite signatories not yet Parties to the Framework Convention to share information on the steps and measures taken to address risks to human rights, democracy and the rule of law and to facilitate exchanges.

Article 25 – International co-operation

137. This article sets out the provisions on international co-operation between Parties to the Framework Convention. It starts by mentioning the obligation applicable among Parties to afford one another the greatest measure of assistance in connection with the realisation of the purpose of this Framework Convention, which is to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.

138. This general obligation is supplemented by an important point regarding the need for the Parties to offer support, as deemed suitable, to States that have not yet become Parties to this Framework Convention. This assistance should be aimed at guiding these States in aligning their actions with the principles outlined in this Framework Convention and ultimately encouraging their accession to it. This collaborative effort should seek to promote a collective commitment to the goals and provisions of the Framework Convention, fostering a broader and more inclusive adherence to its terms among States globally. Such support and guidance do not necessarily imply financial assistance.

139. Furthermore, the co-operation setup by the Framework Convention should include facilitation of the sharing of pertinent information regarding various aspects of artificial intelligence between the Parties, including measures adopted to prevent or mitigate risks and impacts on human rights, democracy and the rule of law. This information exchange should encompass elements that could exert substantial positive or adverse impacts on the enjoyment of human rights, the functioning of democratic processes, and the respect of the rule of law, including risks and effects that have arisen in research contexts and in relation to the private sector. This sharing also extends to risks and effects that have surfaced within the contexts of research on artificial intelligence, promoting a comprehensive understanding of the multifaceted implications of these technologies across these critical domains. In this regard, the provision also points at the need for the Parties to include relevant non-State actors, such as academics, industry representatives, and civil society organisations, with a view to ensure multi-stakeholder view of the relevant topics.

140. Lastly, the provision directly specifies that, for the follow-up of the application of the Framework Convention to be truly effective, the Parties' efforts in co-operation should aim specifically at the prevention and mitigation of risks and adverse impacts resulting from the activities within the lifecycle of artificial intelligence systems and that such co-operation should moreover include a possibility of involving representatives of non-governmental organisations and other relevant bodies.

Article 26 – Effective oversight mechanisms

141. This provision requires Parties to adopt or maintain effective mechanisms to oversee compliance with the obligations in the Framework Convention. In view of the ubiquitous character of the use of artificial intelligence systems and the fact all Parties already have various regulations and supervising mechanisms in place for the protection of human rights in various sectors, the provision emphasises the need for the Parties to review the already existing mechanisms to apply to the context of activities within the lifecycle of artificial intelligence systems. Parties may also choose to expand, reallocate, adapt, or redefine their functions or, if appropriate, set up entirely new structures or mechanisms. The provisions under this article leave these decisions expressly to the Parties' discretion, subject to the conditions in paragraphs 2 and 3, with an understanding that the relevant bodies should be vested with the sufficient powers to effectively pursue their oversight activities.

142. Whether established, newly setup or designated, such bodies should satisfy the criteria set out in paragraph 2 of the provision insofar as they should be functionally independent from the relevant actors within the executive and legislative branches. The reference to "independently and impartially" in paragraph 2 denotes a sufficient degree of distance from relevant actors within both executive and legislative branches, subject to oversight enabling the relevant body(ies) to carry out their functions effectively. This term accommodates a variety of types of functional independence that could be implemented in different

legal systems. For example, this may include oversight functions embedded within particular government bodies that assess or supervise the development and use of artificial intelligence systems.

143. A number of further elements mentioned in the provision contribute to safeguarding the required level of functional independence: the bodies should have the necessary powers, expertise, including in human rights, technical knowledge and proficiency, as well as other resources to fulfil their tasks effectively.

144. Given the shared subject matter and a real possibility that the oversight of the activities within the lifecycle of artificial intelligence systems is shared by multiple authorities across a range of sectors (this is particularly true for Parties with existing specialised human rights mechanisms, such as for example data protection, equality bodies, or National Human Rights Institutions (NHRIs), acting in a given sector or across sectors), the provision requires the Parties to promote effective communication and co-operation between them.

Chapter VIII: Final clauses

145. With some exceptions, the provisions in Article 27 to 36 are essentially based on the Model Final Clauses for Conventions, Additional Protocols and Amending Protocols concluded within the Council of Europe adopted by the Committee of Ministers at its 1291st meeting of the Ministers' Deputies, on 5 July 2017.

Article 27 – Effects of the Convention

146. Paragraph 1 of Article 27 provides that Parties are free to apply agreements or treaties concluded prior to this Framework Convention, including international trade agreements, that regulate activities within the lifecycle of artificial intelligence systems falling within the scope of this Framework Convention. However, Parties must respect the object and purpose of the Framework Convention when doing so and therefore cannot have obligations that would defeat its object and purpose.

147. Paragraph 2 of this article also acknowledges the increased integration of the European Union, particularly as regards regulation of artificial intelligence systems. This paragraph, therefore, permits European Union member States to apply European Union law that governs matters dealt with in this Framework Convention between themselves. The Drafters intended European Union law to include measures, principles and procedures provided for in the European Union legal order, in particular laws, regulations or administrative provisions as well as other requirements, including court decisions. Paragraph 2 is intended, therefore, to cover the internal relations between European Union member States and between European Union member States and institutions, bodies, offices and agencies of the European Union. The same clause should also apply to other Parties that apply European Union rules to the extent they are bound by these rules in view of their participation in the European Union internal market or being subject to internal market treatment.

148. This provision does not affect the full application of this Framework Convention between the European Union or Parties that are members of the European Union, and other Parties. This provision similarly does not affect the full application of this Framework Convention between Parties that are not members of the European Union to the extent they are also bound by the same rules and other Parties to the Framework Convention.

Article 28 – Amendments

149. This article provides for a possibility of amending the Framework Convention and establishes the mechanism for such process. This amendment procedure is primarily intended to be for relatively minor changes of a procedural and technical character. The Drafters considered that major changes to the Framework Convention could be made in the form of amending protocols.

150. Amendments to the provisions of the Framework Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Conference of the Parties. These amendments shall then be communicated to the Parties to the Framework Convention.

151. On any amendment proposed by a Party or the Committee of Ministers, the Conference of the Parties shall submit to the Committee of Ministers its opinion on the proposed amendment.

152. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Conference of the Parties and may approve the amendment.

153. In accordance with paragraphs 5 and 6, any amendment approved by the Committee of Ministers would come into force only when all Parties have informed the Secretary General of the Council of Europe of their acceptance. This requirement seeks to ensure equal participation in the decision-making process for all Parties and that the Framework Convention will evolve in a uniform manner.

Article 29 – Dispute settlement

154. The Drafters considered it important to include in the text of the Framework Convention an article on dispute settlement, which imposes an obligation on the Parties to seek a peaceful settlement of any dispute concerning the application or the interpretation of the Framework Convention through negotiation or any other peaceful means of their choice.

155. In addition to negotiation as specifically mentioned in the first paragraph of this article, Parties may have recourse to any other peaceful means of their choice, as referred to in Article 33 of the Charter of the United Nations. As provided in Article 23, they may also, by mutual consent, turn to the Conference of the Parties at any stage. The provision does not speak further about any specific procedures to be adopted in the context of a potential disputes. Any procedure for solving disputes shall be agreed upon by the Parties concerned.

Article 30 – Signature and entry into force

156. Paragraph 1 states that the Framework Convention is open for signature by Council of Europe member States, non-member States that participated in its elaboration (Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States and Uruguay) and the European Union. Once the Framework Convention enters into force, in accordance with paragraph 3, other non-member States not covered by this provision may be invited to accede to the Framework Convention in accordance with Article 31, paragraph 1.

157. Paragraph 2 states that the Secretary General of the Council of Europe is the depositary of the instruments of ratification, acceptance or approval of this Framework Convention.

158. Paragraph 3 sets the number of ratifications, acceptances or approvals required for the Framework Convention's entry into force at five. At least three of these must be made by Council of Europe members, in accordance with the treaty-making practice of the Organisation.

Article 31 – Accession

159. After the entry into force of this Framework Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Framework Convention and obtaining their unanimous consent, invite any non-member State of the Council of Europe which has not participated in the elaboration of the Framework Convention to accede to it. This decision requires the two-third majority provided for in Article 20.d of the Statute of the Council of Europe, and the unanimous vote of the representatives of the Parties entitled to sit on the Committee of Ministers.

Article 32 – Territorial application

160. Paragraph 1 is a clause on territorial application such as those often used in international treaty practice, including in the conventions elaborated within the Council of Europe. Any Party may specify the territory or territories to which the Framework Convention applies. It is well understood that it would be incompatible with the object and purpose of the Framework Convention for any Party to exclude parts of its territory from application of the Framework Convention without valid reason (such as the existence of different legal status or different legal systems applying in matters dealt with in the Framework Convention).

161. Paragraph 2 is concerned with the extension of application of the Framework Convention to territories for whose international relations the Parties are responsible or on whose behalf they are authorised to give undertakings.

Article 33 – Federal clause

162. Consistent with the goal of enabling the largest possible number of States to become Parties to the Framework Convention, Article 33 allows for a reservation which is intended to accommodate the difficulties federal States may face as a result of their characteristic distribution of power between central and regional authorities and the fact that in some systems federal governments of the particular country may not be constitutionally competent to fulfil the treaty obligations. Precedents exist for federal declarations or reservations to other international agreements [7], including, within the framework of the Convention on Cybercrime (ETS No.185) on enhanced co-operation and disclosure of electronic evidence of 23 November 2001 (Article 41).

163. Article 33 recognises that some variations in coverage may occur as a result of well-established domestic law and practice of a Party which is a federal State. Such variations must be based on its Constitution or other fundamental principles and practices concerning the division of powers in relation to the matters covered by the Framework Convention between the central government and the constituent States or territorial entities of a federal State.

164. Some articles of the Framework Convention contain requirements to adopt or maintain legislative, administrative or other measures that a federal State may be unable to require its constituent States or other similar territorial entities to adopt or maintain.

165. In addition, paragraph 2 of Article 33 provides that, in respect of provisions the implementation of which falls within the legislative jurisdiction of the constituent States or other similar territorial entities, the federal government shall refer the provisions to the authorities of these entities with a favourable endorsement, encouraging them to take appropriate action to give them effect.

Article 34 – Reservations

166. Article 34 specifies that a State may make use of the reservation provided for in Article 33, paragraph 1, either at the moment of signing or upon depositing its instrument of ratification, acceptance, approval, or accession.

167. Paragraph 2 specifies that no reservation may be made in relation to any provision of this Framework Convention, with the exceptions provided for in paragraph 1 of this article.

Article 35 – Denunciation

168. In accordance with the United Nations Vienna Convention on the Law of Treaties, Article 35 allows any Party to denounce the Framework Convention at any time. The sole requirement is that the denunciation be notified to the Secretary General of the Council of Europe who shall act as depository of the Framework Convention.

169. This denunciation takes effect three months after it has been received by the Secretary General.

Article 36 – Notification

170. Article 36 lists the notifications that, as the depositary of the Framework Convention, the Secretary General of the Council of Europe is required to make, and also designates the recipients of these notifications (States and the European Union).

ENDNOTES

1 The term "human rights" used in this Framework Convention is intended to include "fundamental freedoms" in jurisdictions which draw a distinction between the two terms.

2 The reference is being made, in particular, to Resolution 2341 (2020) and Recommendation 2181 (2020) - the need for democratic governance of artificial intelligence; Resolution 2343 (2020) and Recommendation 2183 (2020) - preventing discrimination caused by the use of artificial intelligence; Resolution 2342 (2020) and Recommendation 2182 (2020) - justice by algorithm – the role of artificial intelligence in policing and criminal justice systems; Recommendation 2185 (2020) - artificial intelligence in health care: medical, legal and ethical challenges ahead; Resolution 2345 (2020) and Recommendation 2186 (2020) - artificial intelligence and labour markets: friend or foe?; Resolution 2346 (2020) and Recommendation 2187 (2020) - legal aspects of "autonomous" vehicles; Resolution 2344 (2020) and Recommendation 2184 (2020) - The brain-computer interface: new rights or new threats to fundamental freedoms?

3 Since all human beings belong to the same species, theories based on the existence of different "races" are rejected. However, the term "race" is used in order to ensure that those persons who are generally and erroneously perceived as "belonging to another race" are not excluded from the protection provided by this Framework Convention.

4 See, as the most prominent examples, the preambles of the Universal Declaration of Human Rights, the United Nations International Covenant on Civil and Political Rights and the United Nations International Covenant on Economic, Social and Cultural Rights; Articles 5, 6 and 11 of the American Convention on Human Rights; Protocol No. 13 to the European Convention on Human Rights; Article 1 of the Charter of Fundamental Rights of the European Union.

5 The Drafters noted the important link between this concept and that of human determination and human agency.

6 The reference is being made in particular to the EU Equality Directives, such as EU Directive 2000/43/EC ('Racial Equality Directive'), Directive 2000/78/EC ('Employment Equality Directive'), Directive 2004/113/EC ('Gender Equality Directive in goods and services'), Directive 2006/54/EC ('Gender Equality Directive in employment'), Directive 2010/41/EU6 ('Gender Equality Directive in self-employment'), Directive 79/7/EEC ('Gender Equality Directive in social security').

7 See, as examples, the 1951 UN Convention Relating to the Status of Refugees of 28 July 1951, Article 41; The 1954 UN Convention Relating to the Status of Stateless Persons, Article 37; The 1958 UN Convention on the Recognition and Enforcement of Foreign Arbitral Awards, Article 11; The 1972 UN Convention for the Protection of World Cultural and Natural Heritage, Article 34.