COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 14 January 2021 CAHAI-PDG(2021)01

AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE (CAHAI)
POLICY DEVELOPMENT GROUP
(CAHAI-PDG)

Draft questionnaire for the multi-stakeholder consultation

www.coe.int/cahai

Background

At its third plenary meeting in December 2020, the CAHAI has agreed[1] to entrust the CAHAI-PDG with a number of tasks in 2021, among which features the following:

"In coordination with the CAHAI-COG and the CAHAI-LFG, and in line with the indications provided by the CAHAI plenary, identify the topics of the feasibility study to be put in the form of questions for multi-stakeholder consultations, and contribute if necessary to the multi-stakeholder consultation (based on available financial resources)"

Objective

The CAHAI-PDG is invited to review the proposed topics and questions with a view to their finalization and use in the framework of the CAHAI multi-stakeholder consultation expected to take place in 2021.

Section 1: Definition of AI Systems

1.1 In a view of a possible legal framework on the design, development and application of AI, based on the standards of the Council of Europe on human rights, rule of law and democracy, what kind of definition should be expected (1 option possible):

- No definition, with a legal instrument focused on the effect of AI systems on human rights, democracy and the rule of law
- Technology neutral and simplified definition, such as "Set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being and to entrust a machine with complex tasks"
- Focusing on machine learning systems
- Other (Please indicate your answer)

Section 2: Opportunities and risks arising from AI systems

2.1 Opportunities arising from AI systems

Please list one to three specific applications of AI that, in your view, contribute to strengthening human rights, democracy and the rule of law?

1.

2.

3.

[1] See the document CAHAI(2020)10 ADD rev2 and the decisions taken by the CAHAI at its 3rd plenary meeting.

2.2 Impact on human rights, democracy and the rule of law

Please list one to three specific applications of AI that, in your view, create a significant risk to human rights, democracy and the rule of law?

1.

2.

3.

Section 3: Potential gaps of existing binding legal instruments applicable to AI

3.1Could you please indicate why existing international, regional or national binding legal instruments are not sufficient to regulate AI systems (tick the box you agree with)?

- They are too many and are difficult to interpret and apply to the AI context
- They provide a basis but fail to provide an effective substantive protection of human rights against the risks posed by AI systems
- They lack specific principles for AI systems' operation
- They do not provide enough guidance to developers and deployers of AI systems
- They are not enough to create trust in AI applications
- Other (please indicate your answer)

Section 4: Elements of a legal framework on AI systems

4.1 Do you consider that the listed key elements are relevant for a future legal framework on the design, development and application of AI systems?

	YES	NO	NO OPINION
1.HUMAN DIGNITY			
Key substantive rights: **1.1.** The right to human dignity, the right to life (Art. 2 ECHR), and the right to physical and mental integrity.			
1.2. The right to be informed of the fact that one is interacting with an AI system rather than with a human being145, in particular when the risk of			

confusion arises and can affect human dignity			
1.3. The right to refuse interaction with an AI system whenever this can adversely impact human dignity.			
Key obligations: **1.4.** Member States should ensure that, where tasks risk violating human dignity if carried out by machines rather than human beings, these tasks are reserved for humans.			
1.5. Member States should require AI deployers to inform human beings of the fact that they are interacting with an AI system rather than with a human being whenever confusion may arise			
2. PREVENTION OF HARM TO HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW			
Key substantive rights: **2.1.**The right to life (Art. 2 ECHR), and the right to physical and mental integrity.			
2.2. The right to the protection of the environment, and the right to sustainability of the community and biosphere.			
Key obligations: **2.3.** Member States should ensure that developers and deployers of AI systems take adequate measures to minimise any physical or mental harm to individuals, society and the environment. -*This could, for instance, be done by ensuring that potentially harmful AI systems operate based on an opt-in instead of an opt-out model. Where this is not possible, clear instructions should be provided on how individuals can opt-out from the system's use and on which alternative non-AI driven methods are available-.*			

2.4. Member States should ensure the existence of adequate (by design) safety, security and robustness requirements and compliance therewith by developers and deployers of AI systems. *These requirements should include, inter alia, resilience to attacks, accuracy and reliability, and the necessity to ensure data quality and integrity. Moreover, AI systems should be duly tested and verified prior to their use as well as throughout the entire life cycle of the AI system including by means of periodical reviews to minimise such risks.*			
2.5. Member States should ensure that AI systems are developed and used in a sustainable manner, with full respect for applicable environmental protection standards			
2.6. Where relevant, member States could foster the use AI systems to avoid and mitigate harm from the actions of human beings and of other technological systems, while safeguarding the standards of human rights, democracy and the rule of law**.**			
2.7. Member states could also consider fostering AI solutions that protect and support human integrity, and that can help to solve environmental challenges.			
3.HUMAN FREEDOM AND HUMAN AUTONOMY			
Key substantive rights: **3.1.** The right to liberty and security (Art. 5 ECHR).			
3.2. The right to human autonomy and self-determination. The right not to be subject to a decision based solely on automated processing when this produces legal effects on or similarly significantly affects individuals			

3.3. The right to effectively contest and challenge decisions informed and/or made by an AI system and demand that such decision be reviewed by a person (right to opt out).			
3.4. The right to decide freely to be excluded from AI-enabled manipulation, individualised profiling and predictions, also in case of non-personal data processing.			
3.5. The right to have the opportunity, when it is not excluded by competing legitimate overriding grounds, to choose to have contact with a human being rather than a robot.			
Key obligations **3.6.** Any AI-enabled manipulation, individualised profiling and predictions involving the processing of personal data must comply with the obligations set out in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Member States should effectively implement the modernised version of the Convention ("Convention 108+") to better address AI-related issue.			
3.7. Member States should require AI developers and deployers to establish human oversight mechanisms that safeguard human autonomy, in a manner that is tailored to the specific risks arising from the context in which the AI system is developed and used: ▪ An adequate level of human involvement should be ensured in the operation of AI systems, based on a contextual risk assessment taking into account the system's impact on human rights, democracy and the rule of law. ▪ Whenever necessary and possible, based on a thorough risk assessment, a qualified human being should be able to			

disable any AI system or change its functionality. ▪ Those developing and operating AI systems should have the adequate competences or qualifications to do so, to ensure appropriate oversight that enables the protection of human rights, democracy and the rule of law. ▪ To protect the physical and mental integrity of human beings, AI deployers should strive to avoid the use of 'attention economy' models that can limit human autonomy.			
3.8. Member States should require AI developers and deployers to duly and timely communicate options for redress.			
4.NON-DISCRIMINATION, GENDER EQUALITY, FAIRNESS AND DIVERSITY			
Key substantive rights: **4.1.** The right to non-discrimination and the right to equal treatment. ▪ The right to non-discrimination (on the basis of the protected grounds set out in Article 14 of the ECHR and Protocol 12 to the ECHR), including intersectional discrimination. ▪ AI systems can also give rise to unjust treatment based on new types of differentiation that are not traditionally protected. ▪ This right must be ensured in relation to the entire lifecycle of an AI system (design, development, implementation and use), as well as to the human choices around the AI system's use, whether used in the public or private sector.			
Key obligations: **4.2.** Member States are obliged to ensure that the AI systems they deploy do not result in unlawful discrimination, harmful stereotypes (including but not limited to gender stereotypes)			

and wider social inequality, and should therefore apply the highest level of scrutiny when using or promoting the use of AI systems in sensitive public policy areas, including but not limited to law enforcement, justice, asylum and migration, health, social security and employment.			
4.3. Member States should include non-discrimination and promotion of equality requirements in public procurement processes for AI systems, and ensure that the systems are independently audited for discriminatory effects prior to deployment. AI systems should be duly tested and verified prior to their use as well as throughout the entire life cycle of the AI system including by means of periodical audits and reviews.			
4.4. Member States should impose requirements to effectively counter the potential discriminatory effects of AI systems deployed by both the public and private sectors and protect individuals from the negative consequences thereof. Such requirements should be proportionate to the risks involved. ▪ These requirements should cover the entire lifecycle of an AI system and should concern, inter alia, filling existing gender data gaps, the representativeness, quality and accuracy of data sets, the design and optimisation function of algorithms, the use of the system, and adequate testing and evaluation processes to verify and mitigate the risk of discrimination. ▪ The transparency and auditability of AI systems must be ensured to enable the detection of discrimination throughout the lifecycle of an AI system			
4.5. Member States should encourage diversity and gender balance in the AI			

workforce and periodic feedback from a diverse range of stakeholders. Awareness of the risk of discrimination, including new types of differentiation, and bias in the context of AI should be fostered.			
4.6. Member States should encourage the deployment of AI systems where they could effectively counter existing discrimination in human and machine-based decision-making.			
5. PRINCIPLE OF TRANSPARENCY AND EXPLAINABILITY OF AI SYSTEMS			
Key substantive rights: **5.1.** The right to be promptly informed that a decision which produces legal effects or similarly significantly impacts an individual's life is informed or made by an AI system.			
5.2. The right to a meaningful explanation of how such AI system functions, what optimisation logic it follows, what type of data it uses, and how it affects one's interests, whenever it generates legal effects or similarly impacts individuals' lives. The explanation must be tailored to the context, and provided in a manner that is useful and comprehensible for an individual, allowing individuals to effectively protect their rights.			
5.3. The right of a user of an AI system to be assisted by a human being when an AI system is used to interact with individuals, in particular in the context of public services**.**			
Key obligations: **5.4.** Member States should require developers and deployers of AI systems to provide adequate communication: ▪ Users should be clearly informed of their right to be assisted by a human being whenever using an AI system that can impact their rights or similarly significantly affect			

them, particularly in the context of public services, and of how to request such assistance.			
5.5. Whenever the use of AI systems risks negatively affecting human rights, democracy and the rule of law, Member States should impose requirements on AI developers and deployers regarding traceability and the provision of information: ▪ Persons with a legitimate interest (e.g. consumers, citizens, supervisory authorities or others) should have easy access to contextually relevant information on AI systems. ▪ This information should be comprehensible and accessible and could, inter alia, include the types of decisions or situations subject to automated processing, criteria relevant to a decision, information on the data used, a description of the method of the data collection. A description of the system's potential legal or other effects should be accessible for review/audit by independent bodies with necessary competences. ▪ Specific attention should be paid if children or other vulnerable groups are subjected to interaction with AI systems.			
5.6. Member States should impose requirements on AI developers and deployers regarding documentation: ▪ AI systems that can have a negative impact on human rights, democracy or the rule of law should be traceable and auditable. The data sets and processes that yield the AI system's decisions, including those of data gathering, data labelling and the algorithms used, should be documented, hence enabling the ex post auditability of the system. ▪ Qualitative and effective documentation procedures should be established.			

5.7. Member States should make public and accessible all relevant information on AI systems (including their functioning, optimisation functioning, underlying logic, type of data used) that are used in the provision of public services, while safeguarding legitimate interests such as public security or intellectual property rights, yet securing the full respect of human rights.			
6. DATA PROTECTION AND THE RIGHT TO PRIVACY			
Key substantive right: **6.1.** The right to respect for private and family life, and the protection of personal data (Art. 8 ECHR).			
6.2. The right to physical, psychological and moral integrity in light of AI-based profiling and affect recognition.			
6.3. All the rights enshrined in Convention 108 and in its modernised version, and in particular with regard to AI-based profiling and location tracking.			
Key obligations: **6.4.** Member States must ensure that the right to privacy and data protection are safeguarded throughout the entire lifecycle of AI systems that they deploy, or that are deployed by private actors. The processing of personal data at any stage, including data sets, of an AI system's lifecycle must be based on the principles set out under the Convention 108+ (including fairness and transparency, proportionality, lawfulness of the processing, quality of data, right not to be subject to purely automated decisions and other rights of the data subject, data security, accountability, impact assessments and privacy by design).			
6.5. Member States should take particular measures to effectively protect individuals from AI driven mass surveillance, for instance			

through remote biometric recognition technology or other AI-enabled tracking technology, as this is not compatible with the Council of Europe's standards on human rights, democracy and the rule of law. In this regard, as mentioned in Chapter 3, where necessary and appropriate to protect human rights, states should consider the introduction of additional regulatory measures or other restrictions for the exceptional and controlled use of the application and, where essential, a ban or moratorium.			
6.6. When procuring or implementing AI systems, member States should assess and mitigate any negative impact thereof on the right to privacy and data protection as well as on the broader right to respect for private and family life, by particularly considering the proportionality of the system's invasiveness in light of the legitimate aim it should fulfil, as well as its necessity to achieve it.			
6.7. Member states should consider the development and use of AI applications that can harness the beneficial use of (personal) data where it can contribute to the promotion and protection of human rights, such as the right to life (for instance in the context of AI-driven evidence-based medicine). In doing so, they must ensure the fulfilment of all human rights, and in particular the right to privacy and data protection by ensuring full compliance with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and effectively implementing the modernised version of the Convention ("Convention 108+").			
6.8. Given the importance of data in the context of AI, Member states should put in			

place appropriate safeguards for transborder data flows to ensure that data protection rules are not circumvented, in accordance with Convention 108 and its modernised version.			
7. ACCOUNTABILITY AND RESPONSIBILITY			
Key substantive rights: **7.1.** The right to an effective remedy (Art. 13 ECHR).			
7.2. This should also include the right to effective and accessible remedies whenever the development or use of AI systems by private or public entities causes unjust harm or breaches an individual's legally protected rights**.**			
Key obligations: **7.3.** Member States must ensure that effective remedies are available under respective national jurisdictions, including for civil and criminal responsibility, and that accessible redress mechanisms are put in place for individuals whose rights are negatively impacted by the development or use of AI applications.			
7.4. In this regard, they could also consider the introduction of class actions in the context of harm caused by the use of AI systems and ensure that the general rules about the sharing and reversal of the burden of proof in antidiscrimination legislation are applied**.**			
7.5. Member States should establish public oversight mechanisms for AI systems that may breach legal norms in the sphere of human rights, democracy or the rule of law			
7.6. Member States should ensure that developers and deployers of AI systems: ▪ identify, document and report on potential negative impacts of AI systems on human rights, democracy and the rule of law; ▪ put in place adequate mitigation measures to ensure			

responsibility and accountability for any caused harm.			
7.7. Member States should put in place measures to ensure that public authorities are always able to audit AI systems used by private actors167, so as to assess their compliance with existing legislation and to hold private actors accountable.			
8. DEMOCRACY			
Key substantive rights: **8.1.** The right to freedom of expression, freedom of assembly and association (Art. 10 and 11 ECHR).			
8.2. The right to vote and to be elected, the right to free and fair elections, and in particular universal, equal and free suffrage, including equality of opportunities and the freedom of voters to form an opinion. In this regard, individuals should not to be subjected to any deception or manipulation.			
8.3. The right to (diverse) information, free discourse and access to plurality of ideas and perspectives.			
8.4. The right to good governance			
Key obligations: **8.5.** Member States should take adequate measures to counter the use or misuse of AI systems for unlawful interference in electoral processes, for personalised political targeting without adequate transparency, responsibility and accountability mechanisms, or more generally for shaping voters' political behaviours or to manipulate public opinion in a manner that can breach legal norms safeguarding human rights, democracy and the rule of law.			
8.6. Member States should adopt strategies and put in place measures for fighting disinformation and identifying online hate speech to ensure fair informational plurality.			

8.7. Member States should subject the public procurement of AI systems to adequate oversight mechanisms: ▪ Member States should subject their public procurement processes to legally binding requirements that ensure the responsible use of AI in the public sector by safeguarding compliance with the above-mentioned principles, including transparency, fairness, responsibility and accountability.			
8.8. Member States should subject the use of AI systems in the public sector to adequate oversight mechanisms: ▪ This can also include providing redress to ombudspersons and the courts. ▪ Member states should also secure oversight over how AI systems are being used in individual public sector organisations and intervene and coordinate where appropriate to safeguard their alignment with human rights, democracy and the rule of law. ▪ Member States should ensure that, when the public sector is utilising AI systems, this happens with the involvement of people with appropriate competences from a wide range of fields, including also public administration and political science, to ensure that there is a thorough understanding of the potential implications for the governance of the administrative state and the citizen-state relationship.			
8.9. Member States should make public and accessible all relevant information on AI systems (including their functioning, optimisation functioning, underlying logic, type of data used) that are used in the provision of public services, while safeguarding legitimate interests such as public security.			

8.10. Member States should put in place measures to increase digital literacy and skills in all segments of the population. Their educational curricula should adjust to promote a culture of responsible innovations that respects human rights, democracy and the rule of law.			
8.11. Member States should foster the use of AI solutions and other tools that can: ▪ strengthen the informational autonomy of citizens, improve the way they collect information about political processes and help them participate therein; ▪ help fight corruption and economic crime, and that enhance the legitimacy and functioning of democratic institutions. This can contribute to the positive impact of AI systems within the democratic sphere and enhance trust; ▪ help in the provision of public services. ▪ In doing so, they should always safeguard respect for human rights, democracy and the rule of law.			
9. RULE OF LAW			
Key substantive rights: **9.1.** The right to a fair trial and due process (Art. 6 ECHR). This should also include the possibility to get insight into and challenge an AI-informed decision in the context of law enforcement or justice, including the right to review of such decision by a human.			
9.2. The right to judicial independence and impartiality, and the right to legal assistance.			
9.3. The right to an effective remedy (Art. 13 ECHR), also in case of unlawful harm or breach an individual's human rights in the context of AI systems.			
Key obligations: **9.4.** Member States must ensure that AI systems used in			

the field of justice and law enforcement are in line with the essential requirements of the right to a fair trial. To this end, they should pay due regard to the need to ensure the quality and security of judicial decisions and data, as well as the transparency, impartiality and fairness of data processing methods. Safeguards for the accessibility and explainability of data processing methods, including the possibility of external audits, should be introduced to this end**.**			
9.5. Member States must ensure that effective remedies are available and that accessible redress mechanisms are put in place for individuals whose rights are violated through the development or use of AI systems in contexts relevant to the rule of law.			
9.6. Member States should provide meaningful information to individuals on the use of AI systems in the public sector whenever this can significantly impact individuals' lives. Such information must especially be provided when AI systems are used in the field of justice and law enforcement, both as concerns the role of AI systems within the process, and the right to challenge the decisions informed or made thereby.			
9.7. Member States should ensure that use of AI systems does not interfere with the decision-making power of judges or judicial independence and that any judicial decision is submitted to human oversight.			

4.2 What key principles/substantive principles or obligations could be missing in the list above?

4.3 Do you consider that this future legal framework should consider regulating a new regime of liability?

- Yes
- No

4.4 If yes, what aspects should be covered?

Section 5: Policies and measures to be developed

5.1 Please evaluate the relevance of the listed compliance mechanisms to mitigate the risks arising from the application of AI?

	Relevant	Not so relevant
Human rights impact assessments		
Certification and quality labelling		
Audits		
Regulatory sandboxes		
Continuous automated monitoring		

5.2 Do you think that Council of Europe could play a role in compliance policies on AI?

- Yes
- No

5.3 If yes, what kind of role do you support?

	Provider	Participation in the definition of standards	Observer to provide advice
Human rights impact assessments			
Certification and quality labelling			
Audits			
Other			

5.4 Do you think that a follow-up mechanism could be useful after CAHAI completes its mandate??

- Yes
- No

5.5 If yes, please designate what mechanisms seem preferable?

	Preferable	Not Preferable
Monitoring of AI legislations and policies in member States (and at international/regional level?)		
Capacity building on CoE instruments, including legislative assistance to ensure ratification of and implementation of relevant CoE instruments		
Clearing house to share good practices and exchange information on legal, policy and technological developments related to AI systems		
Center of expertise on AI and human rights		
Other kind of mechanism		

5.6 If you mentioned other kind of mechanism, please specify/elaborate below your proposals
