Homo
Digitalis

Παράλου 12 & Αχνιάδων 17-19

118 54, Αθήνα | info@homodigitalis.gr

Athens, 14.06.2020

Supporting document to Homo Digitalis response to the European Commission's Consultation on the White Paper on Artificial Intelligence - A European Approach

Contents

Introduction

[Homo Digitalis](#) is a Greek civil society organisation based in Athens that focuses on the promotion and protection of human rights in the digital age. We are also members of the European Digital Rights ([EDRi](#)) network. We welcome European Commission's initiative to launch the public consultation, enabling in this way all European citizens, Member States, civil society, industry and academics to provide their opinion on the White Paper and contribute to the European approach for AI.

A. General Comments and Observations on the AI White Paper and the Consultation

1. The term "Trustworthy AI"

The White Paper presents policy options to enable a "trustworthy" and secure development of AI in Europe. In the same document the European Commission calls for a solid European regulatory framework for trustworthy AI, which will protect all European citizens and will help create a frictionless internal market for the further development and uptake of AI. Moreover, the Commission has established a High-Level Expert Group that published Guidelines on "trustworthy" AI in April 2019.

However, Homo Digitalis would suggest to the European Commission to abstain from using the term "trustworthy" regarding AI applications. As the ethics scholar Thomas Metzinger, who is also part of the AI-HLEG, underlines, the concept of trustworthy AI is in reality market-oriented, while the Trustworthy AI narrative *"is, in reality, about developing future markets and using ethics debates as elegant public decorations for a large-scale investment strategy"*.[1] A technology cannot be trustworthy or untrustworthy. Instead, the applicable legal frameworks, standards, and supervisory mechanisms, which are enhancing the inspection of the related technological applications, are the means that generate trust in the use of any technology.

For example, people do not use elevators because they believe that the various technological means of moving an elevator (such as traction elevators, hydraulic elevators, cable-free elevators using electromagnetic propulsion, or pneumatic elevators) are trustworthy. It is not the technology which makes the elevator operational, the criterion that breeds trust. Instead, the criteria are the elevators' certification schemes that assure the safety, performance and integrity of the elevators, the testing and inspections against specifications, codes and legal requirements arising from EU and national law, the industry standards for the elevators and their components, and the regular elevators' maintenance audits. The same holds true for Artificial Intelligence. It is not the various AI techniques incorporated in a product/service that make this product/service

---

[1] Thomas Metzinger (2019) Ethics washing made in Europe, Available at: https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html

trustworthy. But, the applicable legal frameworks, standards, and supervisory mechanisms which impose obligations and set high standards for the protection of the users.

2. The notion of "high-risk AI applications"

In the AI White Paper, the European Commission notes that an AI application should be considered high-risk where it meets two cumulative criteria: First, the AI application is employed in a sector where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur, and second, the AI application in the sector in question is, in addition, used in such a manner that significant risks are likely to arise. Thus, the Commission takes a risk-assessment approach, in which the assessment of the level of risk of a given use could be based on the impact on the affected parties.

In this regard, Homo Digitalis would like to suggest to the European Commission to take into consideration the latest Recommendation of the Council of Europe on the human rights impacts of algorithmic systems.[2] Based on this Recommendation, the term "high risk" is applied when referring to the use of algorithmic systems in processes or decisions that can produce serious consequences for individuals **or in situations where the lack of alternatives prompts a particularly high probability of infringement of human rights**, **including by introducing or amplifying distributive injustice.** The second criterion provided by the Council of Europe is not reflected in the position of the European Commission, even though it is crucial. Thus, Homo Digitalis maintains that the European Commission should reframe the definition of high-risk AI based applications in order to include such scenarios.

Moreover, Homo Digitalis would like to endorse the positions of Access Now[3] and European Digitalis Rights (EDRi)[4] on mandatory human rights impact assessments for AI applications. As Access Now underlines, where AI systems pose a threat to any of our fundamental rights, the EU must ensure that states uphold their obligation to protect and promote those rights and that companies conduct due diligence according to their responsibility. Moreover, opposed to a binary risk assessment approach, Access Now argues that for all applications in all domains, the burden of proof should be on the entity wanting to develop or deploy the AI system to demonstrate that it does not violate human rights via a human rights impact assessment. In addition, EDRi notes all AI systems meeting the legal criteria must complete mandatory human rights impact assessments

---

[2] Council of Europe (2020) Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies, Available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

[3] Access Now (2020) Submission to the Consultation on the "White Paper on Artificial Intelligence - a European approach to excellence and trust", Available at: https://www.accessnow.org/cms/assets/uploads/2020/05/EU-white-paper-consultation_AccessNow_May2020.pdf

[4] European Digital Rights (2020) Recommendations for a Fundamental Rights-based Artificial Intelligence Regulation Addressing collective harms, democratic oversight and impermissable use, Available at: https://edri.org/wp-content/uploads/2020/06/AI_EDRiRecommendations.pdf

throughout their design, development, and deployment. Such assessment should include an evaluation of the collective, societal, institutional and governance implications the AI systems pose, outlining, at the same time, adequate steps to mitigate these implications.

Additionally, Homo Digitalis would like to endorse the position of the civil society organization AlgorithmWatch.[5] AlgorithmWatch and Access Now jointly call for a mandatory disclosure scheme for AI systems deployed in the public sector. More precisely, legislation shall be enacted in EU level providing for the Member States the obligation to establish public registers of AI systems used by the public sector. Such registers should be used to make public the results of Algorithmic Impact Assessments (AIA)/ Human Rights Impact Assessments (HRIA) undertaken by such public authorities. As the Council of Europe underlines,[6] the HRIAs, including research findings or conclusions from the external review process, must be made available to the public in an easily accessible and machine-readable format, while public authorities should not acquire AI systems from third parties in circumstances where the third party is unwilling to waive restrictions on information (e.g. confidentiality or trade secrets) where such restrictions impede or frustrate the process of carrying out HRIAs and making HRIAs available to the public. Thus, Homo Digitalis calls for the European Commission to adopt the same approach.

Finally, the European Union Agency for Fundamental Rights (FRA) in its latest Fundamental Rights Report 2020,[7] states the opinion that the EU and national legislators should ensure that future and ongoing EU regulatory frameworks and preparatory legislative work address and promote transparent and thorough fundamental rights impact assessments, whenever AI technologies are employed. According to FRA, to complement this, the oversight of independent supervisory bodies is essential to guarantee accountability, trustworthiness and fairness.

---

[5] AlgorithmWatch (2020) Submission on the European Commission's "White Paper on Artificial Intelligence – a European approach to excellence and trust", Available at: https://algorithmwatch.org/wp-content/uploads/2020/06/AlgorithmWatch_Submission_EC-White-Paper-AI_20200612.pdf

[6] Council of Europe (2019) Unboxing Artificial Intelligence: 10 steps to protect Human Rights, Available at: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

[7] European Union Agency for Fundamental Rights – FRA, (2020), Fundamental Rights Report 2020, Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-report-2020_en.pdf

B. AI applications that are very concerning for the promotion and protection of Fundamental Rights

1. Use of AI tools for mass surveillance, such as the use of facial recognition technology for identification purposes

As EDRi underlines in its latest related report,[8] the use of biometric technologies, including facial recognition, for identification purposes in public spaces is fundamentally in conflict with the essence of human dignity and the protection of fundamental rights, such as the rights to privacy, data protection, freedom of expression and freedom of assembly. The risks for increasing authoritarian societal control is too high for any of the alleged "benefits" that the companies developing such systems promise to the law enforcement authorities across Europe. As EDRi rightly mentions "the use of biometric surveillance systems creates a dynamic where the powerful watch and the powerless are watched".

While in a draft version of the AI White Paper leaked in early 2020,[9] the European Commission seemed to take into consideration measures to impose a temporary ban on facial recognition technologies used by both public and private actors, unfortunately, this idea is not reflected in the final version of the AI White Paper. However, biometric mass surveillance systems can exacerbate structural inequalities, accelerate unlawful profiling and put limits on everyone's ability to participate in public and social activities. Thus, Homo Digitalis calls for the European Commission to take into consideration EDRi's position and adopt a ban on all biometric processing in public spaces that could amount to mass surveillance. Finally, all EU bodies who give operational support or advice to EU institutions, including but not limited to Europol, FRONTEX and FRA, shall ensure that Member States cannot use these technologies in a manner enabling fundamental rights abuses.

2. Use of AI tools in predictive policing, such as algorithmic profiling, police stops and crime forecasting

Some existing EU instruments in the field of border management and policing, such as the ETIAS Regulation (Article 33) or the PNR Directive (Article 6) foresee the use of algorithmic tools. However, the deployment of such systems for predictive purposes comes with high risks on human rights violations. Introducing ethical guidelines & standards for the design and

---

[8] European Digital Rights (2020), Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States, Available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

[9] Euractiv (2020), LEAK: Commission considers facial recognition ban in AI 'white paper', Available at: https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/

deployment of these tools is welcome, but not enough. Instead, we need Member States to ensure compliance with the applicable regulatory frameworks such as the EU Charter, the ECHR, the Law Enforcement Directive and the Convention 108. When Member States fail to enforce their legal duties, they shall be held responsible, while clear remedial routes shall be available to the individuals affected.

As FRA notes,[10] in algorithmic profiling the individual is selected "based on connections with others identified by the algorithm, rather than actual behaviour" and "individuals' choices are structured according to information about the group", rather than according to their own personal choices. Moreover, the collection and processing of large data sets raises a number of fundamental rights concerns in relation to discrimination, privacy and data protection. Thus, many challenges are associated with the use of algorithmic profiling in large-scale databases for border management and security purposes. More precisely, FRA underlines the fact that comprehensive data on third country nationals will be used for profiling, including algorithmic profiling, at a scale which was not possible in the past. Thus, their processing comes with risks related to conscious or unconscious bias in the selection of risk indicators, while the design of the algorithms or interpretation of the results could lead to operational actions which could result in discrimination of certain categories of persons.

Finally, while law enforcement authorities spend a high amount of funds in acquiring or developing AI tools for predictive policing applications, they seem not to invest money and time in training their officers in an appropriate manner or in developing internal procedures and organisational guidelines scrutinizing the use of data analytics in policing / border management activities. However, the training of police officers and border guards is a very important tool in minimising the risk of unlawful algorithmic profiling. Thus, Homo Digitalis holds that there shall be clear obligations arising from EU or national law for such trainings to take place, if law enforcement authorities develop or deploy AI systems.

3. Use of AI tools in criminal justice, such as risk assessment tools for offenders' classification

The use of risk assessment tools for offender classification has a long history in the criminal justice system of the United States of America (USA). These tools are used to inform courts' decisions in different stages of the criminal justice system, from pretrial services to proceedings closely related to defendants' freedom. Examples of these stages are assignments of bail amounts to suspects for court appearances after an arrest, parole decisions, rulings related to probation, or even decisions during sentencing proceedings. Risk assessment tools are not used by the judicial

---

[10] European Union for Fundamental Rights -FRA (2018) Preventing unlawful profiling today and in the future: A guide, Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

authorities in the member states of the Council of Europe and the European Union. More precisely, the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ) notes in the adopted European Ethical Charter on the use of artificial intelligence in judicial systems[11] that pilot programs have been carried out in some of the member countries in order to explore the potential use of these applications, but they have not yet been applied on a wider scale. Moreover, some other European countries have established scientific councils examining the use of algorithms in the field of justice.

The use of risk assessment tools that incorporate the processing of special categories of personal data could violate the applicable data protection legal framework such as the Convention 108 and national rules implementing the Law Enforcement Directive. Moreover, challenges arise regarding the principle of data minimization. According to this principle, the data stored shall be adequate, relevant, and not excessive in relation to the purposes for which they are stored. However, risk assessment tools used in the U.S.A., such as COMPAS, are collecting data from various aspects of the defendants' lives ranging from defendants' criminal history, employment, and education to their personal relationships. Such a collection of personal data for the purpose of predicting the risk of recidivism allows very precise conclusions to be drawn concerning the private lives of the defendants.

More precisely, personal data related to every aspect of the life of the defendants are under the microscope, and this personal data do not necessarily have a link with the crimes the defendants are accused to have committed and for which they are standing before the court. Thus, such a collection of a vast amount of personal data is in conflict with the data minimization principle of European data protection law, and it cannot be perceived as adequate, relevant, and not excessive in relation to the purpose of predicting recidivism.

Moreover, this Orwellian collection of personal data interferes with the right to respect for private and family life, provided for in Article 7 of the EU Charter and Article 8 of the ECHR. Of course, interferences that are in accordance with domestic legal provisions, pursue a legitimate aim, are necessary in a democratic society, and at the same time are proportionate to pursue that aim are acceptable interferences (ECHR, art. 8, para. 2, and EU Charter, art. 52, para. 1). However, one could argue that risk assessment tools used in the criminal justice system do not comply with the aforementioned criteria. More precisely, these tools base their assessments on a vast collection of personal data that are non-related to the investigation and prosecution of the crime for which the defendants are accused. Regarding the use of AI tools in the criminal justice sector, Homo Digitalis would suggest to the European Commission to take into consideration the CCBE's Response to the consultation.[12]

---

[11] The European Commission for the Efficiency of Justice – CEPEJ (2019) European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, Available at: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

[12] Council of Bars and Law Societies of Europe – CCBE (2020) CCBE Response to the consultation on the European

C. Upgrading the Horizon Europe Programme towards the enhancement of fundamental rights promotion and protection

Many research projects in the field of smart policing and border management are funded by the European Commission under the Horizon 2020 scheme "Secure societies - Protecting freedom and security of Europe and its citizens". It is true that research projects lie at the heart of innovation and make a critical contribution to the development of Europe's societies and cultures. Nevertheless, a number of Horizon2020 research projects deployed in Greece raises important challenges for the future of our societies and the protection of human rights.

As described in the latest report of EDRi "Ban Biometric Mass Surveillance" the EU Horizon 2020-funded SPIRIT project reinforces the lack of fundamental rights compliance, transparency and accountability. Five law enforcement-related stakeholders participate in this research project: the Hellenic Police (GR), West Midlands Police (UK), Police and Crime Commissioner for Thames Valley (UK), Serbian Ministry of Interior (RS), and Police Academy in Szcytno (PL). The information available on the project's website is very limited, even though the project has been up and running since August 2018. Nevertheless, it is evident from the website's content that the project aims to use tools such as face extraction and matching and to correlate information from social media data which constitutes a form of mass surveillance. Based on a successful access to information request filed by Homo Digitalis, the Hellenic Police (Border Unit) is being involved in trials runs between January and August 2020.

In the field of border management, another research project that has attracted attention over the past years is iBorderCtrl, which came to an end in August 2019. The project claimed to enable faster and more thorough border control for third country nationals crossing the land borders of EU Member States. It included software and hardware technologies ranging from portable readers and scanners related to biometric verification, automated deception detection, document authentication, and risk assessment, while pilot runs of the project were implemented on the Hungarian, Greek, and Latvian borders. Based on a successful access to information request filed by Homo Digitalis, no real travelers participated in the Greek pilots. As EDRi notes, the technologies developed in this project, and particular the automated deception detection, could be considered part of the state mass surveillance apparatus because they rely on technologies of watching, with an unequal power dynamic and a use that is generally targeted against marginalised individuals.

Lastly, another interesting research project in the field of border management is the H2020 project ROBORDER. The aim of ROBORDER is to deliver a fully-functional, autonomous border surveillance system composed of unmanned mobile robots including aerial, water surface,

---

Commission's White Paper on Artificial Intelligence, Available at:
https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20200605_CCBE-Response-to-the-consultation-regarding-the-European-Commission-s-White-Paper-on-AI.pdf

underwater and ground vehicles. The Hellenic Ministry of Defense is one of the Greek stakeholders involved in this research project. One could argue that the expertise and technical knowledge acquired by ROBORDER, will in turn feed into the development and deployment of similar tools by the Hellenic Army in the near future

For more information and/or clarifications regarding this input, please contact info@homodigitalis.gr and/or Eleftherios Chelioudakis at e.chelioudakis@homodigitalis.gr

D. Replies of Homo Digitalis to the questionnaire of the AI White Paper Consultation

Consultation on the White Paper on Artificial Intelligence - A European Approach

Fields marked with * are mandatory.

Introduction

Artificial intelligence (AI) is a strategic technology that offers many benefits for citizens and the economy. It will change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans and the protection of workers, and in many other ways that we can only begin to imagine.

At the same time, AI entails a number of potential risks, such as risks to safety, gender-based or other kinds of discrimination, opaque decision-making, or intrusion in our private lives.

The European approach for AI aims to promote Europe's innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU. According to this approach, AI should work for people and be a force for good in society.

For Europe to seize fully the opportunities that AI offers, it must develop and reinforce the necessary industrial and technological capacities. As set out in the accompanying European strategy for data, this also requires measures that will enable the EU to become a global hub for data.

The current public consultation comes along with the **White Paper on Artificial Intelligence - A European Approach** aimed to foster a European ecosystem of excellence and trust in AI and a Report on the safety and liability aspects of AI. The White Paper proposes:

- Measures that will streamline research, foster collaboration between Member States and increase investment into AI development and deployment;
- Policy options for a future EU regulatory framework that would determine the types of legal requirements that would apply to relevant actors, with a particular focus on high-risk applications.

This consultation enables all European citizens, Member States and relevant stakeholders (including civil society, industry and academics) to provide their opinion on the White Paper and contribute to a European approach for AI. To this end, the following questionnaire is divided in three sections:

- **Section 1** refers to the specific actions, proposed in the White Paper's Chapter 4 for the building of an ecosystem of excellence that can support the development and uptake of AI across the EU economy and public administration;
- **Section 2** refers to a series of options for a regulatory framework for AI, set up in the White Paper's Chapter 5;
- **Section 3** refers to the Report on the safety and liability aspects of AI.

Respondents can provide their opinion by choosing the most appropriate answer among the ones suggested for each question or suggesting their own ideas in dedicated text boxes.

Feedback can be provided in one of the following languages:
BG | CS | DE | DA | EL | EN | ES | ET | FI | FR | HR | HU | IT | LT | LV | MT | NL | PL | PT | RO | SK | SL | SV

Written feedback provided in other document formats, can be uploaded through the button made available at the end of the questionnaire.

The survey will remain open until 14 June 2020.

About you

* Language of my contribution
- ○ Bulgarian
- ○ Croatian
- ○ Czech
- ○ Danish
- ○ Dutch
- ● English
- ○ Estonian
- ○ Finnish
- ○ French
- ○ Gaelic
- ○ German
- ○ Greek
- ○ Hungarian
- ○ Italian
- ○ Latvian
- ○ Lithuanian
- ○ Maltese
- ○ Polish
- ○ Portuguese
- ○ Romanian
- ○ Slovak
- ○ Slovenian
- ○ Spanish
- ○ Swedish

* I am giving my contribution as

- ○ Academic/research institution
- ○ Business association
- ○ Company/business organisation
- ○ Consumer organisation
- ○ EU citizen
- ○ Environmental organisation
- ○ Non-EU citizen
- ● Non-governmental organisation (NGO)
- ○ Public authority
- ○ Trade union
- ○ Other

* First name

Eleftherios

* Surname

Chelioudakis

* Email (this won't be published)

e.chelioudakis@homodigitalis.gr

* Organisation name

255 character(s) maximum

Homo Digitalis

* Organisation size

- ● Micro (1 to 9 employees)
- ○ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ○ Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](). It's a voluntary database for organisations seeking to influence EU decision-making.

611935634267-89

* Country of origin

Please add your country of origin, or that of your organisation.

○ Afghanistan	○ Djibouti	○ Libya	○ Saint Martin
○ Åland Islands	○ Dominica	○ Liechtenstein	○

3

			Saint Pierre and Miquelon
○ Albania	○ Dominican Republic	○ Lithuania	○ Saint Vincent and the Grenadines
○ Algeria	○ Ecuador	○ Luxembourg	○ Samoa
○ American Samoa	○ Egypt	○ Macau	○ San Marino
○ Andorra	○ El Salvador	○ Madagascar	○ São Tomé and Príncipe
○ Angola	○ Equatorial Guinea	○ Malawi	○ Saudi Arabia
○ Anguilla	○ Eritrea	○ Malaysia	○ Senegal
○ Antarctica	○ Estonia	○ Maldives	○ Serbia
○ Antigua and Barbuda	○ Eswatini	○ Mali	○ Seychelles
○ Argentina	○ Ethiopia	○ Malta	○ Sierra Leone
○ Armenia	○ Falkland Islands	○ Marshall Islands	○ Singapore
○ Aruba	○ Faroe Islands	○ Martinique	○ Sint Maarten
○ Australia	○ Fiji	○ Mauritania	○ Slovakia
○ Austria	○ Finland	○ Mauritius	○ Slovenia
○ Azerbaijan	○ France	○ Mayotte	○ Solomon Islands
○ Bahamas	○ French Guiana	○ Mexico	○ Somalia
○ Bahrain	○ French Polynesia	○ Micronesia	○ South Africa
○ Bangladesh	○ French Southern and Antarctic Lands	○ Moldova	○ South Georgia and the South Sandwich Islands
○ Barbados	○ Gabon	○ Monaco	○ South Korea
○ Belarus	○ Georgia	○ Mongolia	○ South Sudan
○ Belgium	○ Germany	○ Montenegro	○ Spain
○ Belize	○ Ghana	○ Montserrat	○ Sri Lanka
○ Benin	○ Gibraltar	○ Morocco	○ Sudan
○ Bermuda	● Greece	○ Mozambique	○ Suriname
○ Bhutan	○ Greenland	○ Myanmar /Burma	○ Svalbard and Jan Mayen
○ Bolivia	○ Grenada	○ Namibia	○ Sweden
○ Bonaire Saint Eustatius and Saba	○ Guadeloupe	○ Nauru	○ Switzerland
○ Bosnia and Herzegovina	○ Guam	○ Nepal	○ Syria
○ Botswana	○ Guatemala	○ Netherlands	○ Taiwan
○ Bouvet Island	○ Guernsey	○ New Caledonia	○ Tajikistan
○ Brazil	○ Guinea	○ New Zealand	○ Tanzania

◎ British Indian Ocean Territory	◎ Guinea-Bissau	◎ Nicaragua	◎ Thailand
◎ British Virgin Islands	◎ Guyana	◎ Niger	◎ The Gambia
◎ Brunei	◎ Haiti	◎ Nigeria	◎ Timor-Leste
◎ Bulgaria	◎ Heard Island and McDonald Islands	◎ Niue	◎ Togo
◎ Burkina Faso	◎ Honduras	◎ Norfolk Island	◎ Tokelau
◎ Burundi	◎ Hong Kong	◎ Northern Mariana Islands	◎ Tonga
◎ Cambodia	◎ Hungary	◎ North Korea	◎ Trinidad and Tobago
◎ Cameroon	◎ Iceland	◎ North Macedonia	◎ Tunisia
◎ Canada	◎ India	◎ Norway	◎ Turkey
◎ Cape Verde	◎ Indonesia	◎ Oman	◎ Turkmenistan
◎ Cayman Islands	◎ Iran	◎ Pakistan	◎ Turks and Caicos Islands
◎ Central African Republic	◎ Iraq	◎ Palau	◎ Tuvalu
◎ Chad	◎ Ireland	◎ Palestine	◎ Uganda
◎ Chile	◎ Isle of Man	◎ Panama	◎ Ukraine
◎ China	◎ Israel	◎ Papua New Guinea	◎ United Arab Emirates
◎ Christmas Island	◎ Italy	◎ Paraguay	◎ United Kingdom
◎ Clipperton	◎ Jamaica	◎ Peru	◎ United States
◎ Cocos (Keeling) Islands	◎ Japan	◎ Philippines	◎ United States Minor Outlying Islands
◎ Colombia	◎ Jersey	◎ Pitcairn Islands	◎ Uruguay
◎ Comoros	◎ Jordan	◎ Poland	◎ US Virgin Islands
◎ Congo	◎ Kazakhstan	◎ Portugal	◎ Uzbekistan
◎ Cook Islands	◎ Kenya	◎ Puerto Rico	◎ Vanuatu
◎ Costa Rica	◎ Kiribati	◎ Qatar	◎ Vatican City
◎ Côte d'Ivoire	◎ Kosovo	◎ Réunion	◎ Venezuela
◎ Croatia	◎ Kuwait	◎ Romania	◎ Vietnam
◎ Cuba	◎ Kyrgyzstan	◎ Russia	◎ Wallis and Futuna
◎ Curaçao	◎ Laos	◎ Rwanda	◎ Western Sahara
◎ Cyprus	◎ Latvia	◎ Saint Barthélemy	◎ Yemen
◎ Czechia	◎ Lebanon	◎	◎ Zambia

○ Democratic Republic of the Congo	○ Lesotho	Saint Helena Ascension and Tristan da Cunha ○ Saint Kitts and Nevis	○ Zimbabwe
○ Denmark	○ Liberia	○ Saint Lucia	

○ **Anonymous**
Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

◉ **Public**
Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the [personal data protection provisions]

Section 1 - An ecosystem of excellence

To build an ecosystem of excellence that can support the development and uptake of AI across the EU economy, the White Paper proposes a series of actions.

In your opinion, how important are the six actions proposed in section 4 of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Working with Member states	○	○	○	○	◉	○
Focussing the efforts of the research and innovation community	○	○	○	○	◉	○
Skills	○	○	○	○	◉	○
Focus on SMEs	○	○	○	◉	○	○
Partnership with the private sector	◉	○	○	○	○	○
Promoting the adoption of AI by the public sector	◉	○	○	○	○	○

Are there other actions that should be considered?

500 character(s) maximum

-Strong collaboration with the civil society community, which focuses on the interplay between the protection of human rights and the design/deployment/development of new technologies within the EU.
-Meaningful consultation with users and or groups of people affected by the development of AI tools via interactive online channels and community meetings in EU and national level

Revising the Coordinated Plan on AI (Action 1)

The Commission, taking into account the results of the public consultation on the White Paper, will propose to Member States a revision of the Coordinated Plan to be adopted by end 2020.

In your opinion, how important is it in each of these areas to align policies and strengthen coordination as described in section 4.A of the White Paper (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Strengthen excellence in research	○	○	○	○	●	○
Establish world-reference testing facilities for AI	○	○	●	○	○	○
Promote the uptake of AI by business and the public sector	●	○	○	○	○	○
Increase the financing for start-ups innovating in AI	○	○	●	○	○	○
Develop skills for AI and adapt existing training programmes	○	○	○	○	●	○
Build up the European data space	○	○	○	●	○	○

Are there other areas that that should be considered?

500 character(s) maximum

The development and deployment of AI systems must respect human rights. Therefore, the European Commission shall ensure that the policies will be built on existing values enshrined in the Treaties, the EU Charter of Fundamental Rights and the ECHR. When EU bodies or the Member States fail to enforce their legal duties, they shall be held responsible, while clear remedial routes shall be available to the individuals affected

A united and strengthened research and innovation community striving for excellence

Joining forces at all levels, from basic research to deployment, will be key to overcome fragmentation and create synergies between the existing networks of excellence.

In your opinion how important are the three actions proposed in sections 4.B, 4.C and 4.E of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Support the establishment of a lighthouse research centre that is world class and able to attract the best minds	○	○	○	●	○	○
Network of existing AI research excellence centres	○	○	○	●	○	○
Set up a public-private partnership for industrial research	○	○	○	○	○	●

Are there any other actions to strengthen the research and innovation community that should be given a priority?

500 character(s) maximum

-Break "data silos" and stimulate sharing, re-using and trading of non-personal data assets
-Involve human rights organization in the activities of the research and innovation community related to the design and development of AI tools.
-Provide for the supervisory mechanisms ensuring that the research and innovation community will effectively respect the applicable regulatory frameworks of data protection, when datasets of personal data are used

Focusing on Small and Medium Enterprises (SMEs)

The Commission will work with Member States to ensure that at least one digital innovation hub per Member State has a high degree of specialisation on AI.

In your opinion, how important are each of these tasks of the specialised Digital Innovation Hubs mentioned in section 4.D of the White Paper in relation to SMEs (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Help to raise SME's awareness about potential benefits of AI	○	○	●	○	○	○
Provide access to testing and reference facilities	○	○	○	●	○	○
Promote knowledge transfer and support the development of AI expertise for SMEs	○	○	●	○	○	○
Support partnerships between SMEs, larger enterprises and academia around AI projects	○	○	○	○	○	●
Provide information about equity financing for AI startups	○	○	○	○	○	●

Are there any other tasks that you consider important for specialised Digital Innovations Hubs?
500 character(s) maximum

-Any innovation hub could develop AI tools that lack conformity with the applicable legal human rights framework. Thus, there should not be in place lower standards aiming at innovation, such as sandboxing, without ensuring at the same time the protection of human rights via specific supervisory procedures and processes.
When EU money are funding a project, the EC should ensure a scheme where fruits of the research are part of the public domain and the funding is reverted in this way to EU

Section 2 - An ecosystem of trust

Chapter 5 of the White Paper sets out options for a regulatory framework for AI.

In your opinion, how important are the following concerns about AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
AI may endanger safety	○	○	○	○	●	○
AI may breach fundamental rights (such as human dignity, privacy, data protection, freedom of expression, workers' rights etc.)	○	○	○	○	●	○
The use of AI may lead to discriminatory outcomes	○	○	○	○	●	○
AI may take actions for which the rationale cannot be explained	○	○	○	○	●	○
AI may make it more difficult for persons having suffered harm to obtain compensation	○	○	○	○	●	○
AI is not always accurate	○	○	○	●	○	○

Do you have any other concerns about AI that are not mentioned above? Please specify:

500 character(s) maximum

> Policies should provide for Inclusion of human rights organizations in the design and development of AI intended for use in public services. Such inclusion creates transparency and boosts trust, since when civil society orgs can actively participate, pose questions, express opinions, and receive clarifications, they would have more confidence in the decisions agreed upon.
> -EU bodies when give operational support or advice to EU institutions shall follow a human rights-based approach.

Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

○ Current legislation is fully sufficient
○ Current legislation may have some gaps
○ There is a need for a new legislation
● Other
○ No opinion

Other, please specify

500 character(s) maximum

> Existing EU instruments such as the ETIAS Regulation or the PNR Directive foresee the use of algorithmic tools. However, the deployment of such systems for predictive purposes comes with high risks on human rights violations. Introducing ethical guidelines for the design and deployment of these tools is welcome, but

not enough. Instead, we need MSs and the EC to ensure compliance with the applicable regulatory frameworks such as the EU Charter, the ECHR, the GDPR, the LED and Conv.108

If you think that new rules are necessary for AI system, do you agree that the introduction of new compulsory requirements should be limited to high-risk applications (where the possible harm caused by the AI system is particularly high)?

○ Yes
● No
○ Other
○ No opinion

Additional Comments

500 character(s) maximum

The use of AI systems for high-risk applications (based on a human rights impact assessment) shall be banned. New legislation, if introduced, shall focus on providing clear remedial routes in national level for the individuals affected by low-risk or medium risk AI applications. The legislation shall take into consideration the EU wide, cross-border use of some commercial applications, as well.

If you wish, please indicate the AI application or use that is most concerning ("high-risk") from your perspective:

500 character(s) maximum

-Use of AI tools for mass surveillance, such as the use of facial recognition technology for identification and categorization purposes.
-Use of AI tools in predictive policing, such as algorithmic profiling and/or police stops, crime forecasting etc.
-Use of AI tools in criminal justice, such as risk assessment tools for offenders' classification.
Such uses are fundamentally in conflict with the essence of human dignity and the protection of fundamental rights and freedoms.

In your opinion, how important are the following mandatory requirements of a possible future regulatory framework for AI (as section 5.D of the White Paper) (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
The quality of training data sets	○	○	○	○	●	○
The keeping of records and data	○	○	○	○	○	●
Information on the purpose and the nature of AI systems	○	○	○	○	●	○
Robustness and accuracy of AI systems	○	○	○	●	○	○

Human oversight	○	○	○	○	●	○
Clear liability and safety rules	○	○	○	○	●	○

In addition to the existing EU legislation, in particular the data protection framework, including the General Data Protection Regulation and the Law Enforcement Directive, or, where relevant, the new possibly mandatory requirements foreseen above (see question above), do you think that the use of remote biometric identification systems (e.g. face recognition) and other technologies which may be used in public spaces need to be subject to further EU-level guidelines or regulation:

- ○ No further guidelines or regulations are needed
- ○ Biometric identification systems should be allowed in publicly accessible spaces only in certain cases or if certain conditions are fulfilled (please specify)
- ○ Other special requirements in addition to those mentioned in the question above should be imposed (please specify)
- ○ Use of Biometric identification systems in publicly accessible spaces, by way of exception to the current general prohibition, should not take place until a specific guideline or legislation at EU level is in place.
- ● Biometric identification systems should never be allowed in publicly accessible spaces
- ○ No opinion

Please specify your answer:

> The use of facial recognition for identification and categorization purposes in public spaces is fundamentally in conflict with the essence of human dignity and the protection of fundamental rights and freedoms in public spaces, such as the rights to privacy, data protection, freedom of expression and freedom of assembly. The risks for increasing authoritarian societal control is too high for any alleged "benefits" that AI developers /companies promise to LEAs from the use of these technologies. We call the European Commission and the MSs to follow EDRi's approach published in May 2020 on this matter and to ban any use of remote biometric identification systems.

Do you believe that a voluntary labelling system (Section 5.G of the White Paper) would be useful for AI systems that are not considered high-risk in addition to existing legislation?

- ○ Very much
- ○ Much
- ○ Rather not
- ● Not at all
- ○ No opinion

Do you have any further suggestion on a voluntary labelling system?
500 character(s) maximum

> The voluntary labelling system for no-high risk AI applications presented in the AI White Paper is unfortunately inefficient for the users of these AI services and products. The idea is interesting, but without

structural changes in the labelling scheme, the latter would unfortunately be nothing other than a publicity /marketing stunt for the AI developers. A good approach would be for the developers to provide precise information regarding the AI techniques incorporated in a product.

What is the best way to ensure that AI is trustworthy, secure and in respect of European values and rules?

- ☐ Compliance of high-risk applications with the identified requirements should be self-assessed ex-ante (prior to putting the system on the market)
- ☐ Compliance of high-risk applications should be assessed ex-ante by means of an external conformity assessment procedure
- ☐ Ex-post market surveillance after the AI-enabled high-risk product or service has been put on the market and, where needed, enforcement by relevant competent authorities
- ☑ A combination of ex-ante compliance and ex-post enforcement mechanisms
- ☐ Other enforcement system
- ☐ No opinion

Do you have any further suggestion on the assessment of compliance?

500 character(s) maximum

We do not agree with the term "trustworthy AI" used. Nevertheless, possibly, some new legal frameworks - sector oriented - could be established to codify new requirements, obligations, rights, oversight bodies, regular reviews, and remedial routes. Lastly, maybe is some cases new legal frameworks are not necessary. Instead, revising the existing frameworks and complementing them with provisions on the use of AI tools could be a more efficient option.

Section 3 – Safety and liability implications of AI, IoT and robotics

The overall objective of the safety and liability legal frameworks is to ensure that all products and services, including those integrating emerging digital technologies, operate safely, reliably and consistently and that damage having occurred is remedied efficiently.

The current product safety legislation already supports an extended concept of safety protecting against all kind of risks arising from the product according to its use. However, which particular risks stemming from the use of artificial intelligence do you think should be further spelled out to provide more legal certainty?

- ☑ Cyber risks
- ☑ Personal security risks
- ☑ Risks related to the loss of connectivity
- ☑ Mental health risks

In your opinion, are there any further risks to be expanded on to provide more legal certainty?

500 character(s) maximum

-Risks related to discrimination

-Risks related to intellectual isolation and radicalization arising from filter bubbles created by algorithmic targeted advertising, personalized searches and personalized news-feed

- AI designers/developers shall take into consideration individuals with special needs or disabilities or those at risk of exclusion

-Issues related to access to the available AI tools arising from financial criteria or technological illiteracy that could create inequality

Do you think that the safety legislative framework should consider new risk assessment procedures for products subject to important changes during their lifetime?

- ● Yes
- ○ No
- ○ No opinion

Do you have any further considerations regarding risk assessment procedures?

500 character(s) maximum

> The European Commission and MSs shall ensure that the relevant supervisory/ oversight bodies in EU and national level are equipped with the necessary resources (human and financial) and authority to investigate, oversee and co-ordinate compliance with their relevant legislative and regulatory framework.

Do you think that the current EU legislative framework for liability (Product Liability Directive) should be amended to better cover the risks engendered by certain AI applications?

- ● Yes
- ○ No
- ○ No opinion

Do you have any further considerations regarding the question above?

500 character(s) maximum

> A key aspect of future AI policy framework is the choice of the liability regime for damages caused by AI. As CEPS underlines, there are 3 main aspects on this issue. The first is related to the scope of the liability, the second to the type of remedy, and hence the type of liability rule to adopt, and the third revolves around problems of attribution or appointment of liability. Finally, the future EU liability regime will also have to be designed with a suitable insurance framework.

Do you think that the current national liability rules should be adapted for the operation of AI to better ensure proper compensation for damage and a fair allocation of liability?

- ○ Yes, for all AI applications
- ● Yes, for specific AI applications
- ○ No
- ○ No opinion

Please specify the AI applications:

In general, AI tools must be adapted to the existing legal systems, rather than the other way around. Nevertheless, some of the existing legal systems have to be revised in order to contemplate new, AI-enabled, ways of providing goods and services, organizing production, and channeling social interaction.

Do you have any further considerations regarding the question above?

500 character(s) maximum

Issues related to data ownership: The rapid expansion of the data economy in the field of AI raises questions about who has the ownership on data generated by AI products and services, as well as what such data "ownership" entails in terms of exclusive rights. The concept of data ownership raises important questions about how to strike a balance between the rights of the AI developers and the society's interest in accessing and reusing these data as part of the public domain.

Thank you for your contribution to this questionnaire. In case you want to share further ideas on these topics, you can upload a document below.

You can upload a document here:

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Contact

CNECT-AI-CONSULT@ec.europa.eu