Homo Digitalis
Παράλου 12 & Αχνιάδων 17-19
118 54, Αθήνα | info@homodigitalis.gr

Athens, Greece 27.9.2020

Submission of Homo Digitalis' input - Chapter 7 of the draft feasibility study

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. Moreover, we serve as a member organisation at the European Digital Rights (EDRi) network. Please, find below our comments and suggestions on chapter 7 of the draft feasibility study. We would like also to state that we officially endorse the related submissions of the Conference INGOs and Access Now.

Comments & Suggestions

To begin with, we endorse the suggested structure of Chapter 7 as communicated on 25/9 by the leading coordinators/drafters. We would like to submit the following thoughts:

-As regards Section "I.a Fundamental Principles":

- **Sub-section "i. Human Autonomy":** The interaction of AI systems with the autonomy of end-users is an ethical issue of utmost importance, while it is interrelated with the ECHR since it has strong connections with human integrity and dignity. However, the use of the term 'human autonomy' might also seem inaccurate under this human rights law section. The reason is that the term human autonomy is not used in any Article of the ECHR, while it also encompasses broader conceptual variations that go beyond human rights law. The concept of autonomy functions differently in a variety of contexts, and it plays various roles in the theoretical accounts of persons, conceptions of moral obligation and responsibility, justification of social policies and in numerous aspects of political theory. Thus, does not seem to be fit for purpose and could create confusion for the reader.[1]
- **Sub-section "v. Data protection and privacy":** Homo Digitalis suggests the final text to thoroughly reflect on the necessity and proportionality principles. As a means to establish whether a particular infringement upon the right to privacy is "necessary in a democratic society" there is the need to balance on the one hand the State's interests to incorporate AI tools and on the other hand the individual's right to privacy. In line with established case-law of the ECtHR, the term "necessary" is not a synonym for 'useful', 'reasonable', or 'desirable', but instead implies the existence of a 'pressing social need' for the

[1] A detailed description of our positions on human autonomy, as well as in the suggested structure of Chapter 7, which is similar to the structure used by the European Commission AI HLEG, can be found at the publication "Centre for European Policy Studies, Task Force Evaluation of the HLEG Trustworthy AI Assessment List (Pilot Version), 2020, available at https://www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity/ " in which Homo Digitalis had an active drafting role

interference with the right to privacy.[2] It is for the State to make the primary assessment of the pressing social need in a case by case basis. However, its assessment remains subject to review by the ECtHR.[3] Thus, we would like the text to reflect on the established case-law which is flexible enough to cover different technologies used. Moreover, this 'pressing social need' requirement appears to be related to the significance of the 'pursuit of a legitimate aim'. Thus, based on the high standards set by European human rights law, it is not sufficient that the interests served by a limitation on the right to privacy are legitimate, but additionally they should be 'pressing'.[4] Finally, with regard to the proportionality assessment, it is evident from the ECtHR's case law that of utmost importance are the legislative choices underlying it. Thus, any authorities that via the use of AI tools interfere with the right to privacy of individuals shall achieve a fair balance between the purpose of this interreference and the means used to achieve it. Otherwise stated, the added value of the interreference should not outweigh its potential negative impact to the individual concerned.[5]

-As regards Section "I.b. Key Requirements":

- **Sub-section "iv. Measures to ensure transparency":** It is important to underline the fact that oversight bodies at national level shall have the powers to audit and assess the functioning of algorithmic systems, if needed. Such oversight powers could complement the existing obligations arising from European data protection law (accountability principle, impact assessment, prior consultation with supervisory authorities, etc) in an attempt to increase transparency. The auditing procedure itself could be strictly confidential in order to respect trade secrets or other conflicting commercial rights, as well as minimize security threats.[6] However, the results/outcome of such auditing procedures shall always be made publicly available or be freely available following access to information requests. Of course, different approaches can be appropriate, based on the algorithmic system used. Nevertheless, it would be important for CAHAI to promote more agile and flexible processes incentivising the use of documentation models while at the same time guaranteeing flexible processes, formats and tools. In addition, Homo Digitalis would like to stress that key information on AI systems - using non-expert language – shall be made available to end-users of AI tools, giving the opportunity to the latter to understand the risks involved in using such a tool for personal or commercial use.

[2] See for example, Handyside v. UK, Dudgeon v. UK, Z. v. Finland etc.

[3] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights', 2020, Available at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

[4] Janneke Gerards, 'How to improve the necessity test of the European Court of Human Rights', 2013 11(2) International Journal of Constitutional Law 466

[5] European Union Agency for Fundamental Rights (FRA), European Data Protection Supervisor, Council of Europe, Handbook on European Data Protection Law', 2018

[6] Marcus Comiter, Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019

-As regards Section "III Liability for damage caused by artificial intelligence":

Homo Digitalis would like to draw attention to a detailed study recently published by the European Parliamentary Research Service.[7] Based on the conclusions shared by the authors, a clear and coherent system of a civil liability regime for AI has the potential to reduce risks and increase safety, decrease legal uncertainty and related legal and litigation costs, and enhance consumer rights and trust. Thus, timely action at European level would reduce regulatory fragmentation and costs for producers of AI, while also helping to ensure a high level of protection for human rights.

**For more information about this submission please contact Eleftherios Chelioudakis at e[dot]chelioudakis[at]homodigitalis[dot]gr*

[7] European Parliamentary Research Service, Civil liability regime for artificial intelligence: European added value assessment, 2020, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU(2020)654178_EN.pdf