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

Athens, Greece 4.9.2020

Submission to the Council of Europe (CoE) Data Protection Committee on draft Guidelines on Facial Recognition, dated 16 June 2020

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. Moreover, we serve as an observer organisation at the Ad hoc Committee on Artificial Intelligence (CAHAI) of the Council of Europe.

We welcome Council of Europe (CoE) Data Protection Committee's initiative to publish its draft Guidelines on Facial Recognition, enabling in this way Homo Digitalis and other civil society organisations to provide their feedback and comments. With our submission, we would like to underline some key elements regarding the text of the draft Guidelines, **as well as to officially endorse the submissions of two partner organisations of ours, i.e. Access Now and European Digital Rights (EDRi)**.

Comments

To begin with, we would like to state that as a member of the EDRi network, Homo Digitalis' position is that the use of all forms of biometric technologies in public or publicly accessible spaces, including online, whether by private or public actors (such as law enforcement) is an important challenge which creates a serious interference with a number of human rights. As such, the primary focus should always be on ensuring that human rights are protected, upheld and promoted.

The use of facial recognition by law enforcement authorities in Europe is in fundamental conflict with the essence of human dignity and the protection of human rights and freedoms in public spaces, such as the rights to privacy, data protection,

freedom of expression, and freedom of assembly. The risk of increased authoritarian societal control outweighs any alleged "benefits" that the use of these technologies promise. As EDRi rightly states in its latest related report "**Ban Biometric Mass Surveillance**", the use of biometric surveillance systems creates a dynamic where the powerful watch and the powerless are watched.

Datasets and related challenges

The text of the draft Guidelines rightly makes specific references to the necessary limitations that should exist when it comes to access to relevant databases when entities are using facial recognition technology (Section "Limitations on use – Proportionality"), while also underlines that strong security measures, both at technical and organisational level, should be in place in order to protect datasets against loss and unauthorised access or use (Section "Data security").

We could suggest to the Data Protection Committee to further reflect on the important challenges that arise regarding the use of datasets in the design, development, ongoing deployment and procurement of facial recognition systems. As the CoE Committee of Ministers rightly points out in the Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems, States should carefully assess what human rights could be affected as a result of the quality of data that are being put into and extracted from an algorithmic system. The provenance and possible shortcomings of the dataset, the possibility of its inappropriate or decontextualised use, the negative externalities resulting from these shortcomings and inappropriate uses as well as the environments within which the dataset will be or could possibly be used, should also be assessed carefully. Lastly, attention should be paid to the generation of new, inferred, potentially sensitive data and forms of categorisation through automated means.

Impact analysis and risk assessment

As the text of the draft Guidelines rightly mentions, where a public authority has not yet acquired or developed a facial recognition system, a risk assessment of the potential impact of the processing on fundamental rights and freedoms should be carried out prior to the acquisition and/or development of the tool and should be made public. We would like to mention that since such processing activities are using new technologies and are very likely to result in a high risk to the rights and freedoms of the data subjects, based on EU law, and specifically the Articles 27-28 of the Directive 2016/680, law enforcement authorities in EU are legally obliged to carry out, prior to the processing, a data protection impact assessment and to consult their national supervisory auhtority on this matter.

It is important to underline the importance of these provisions, since we can already see in practice that this obligation is not respected. For example, Homo Digitalis has already a pending case against the Hellenic Police before the Hellenic Data Protection Authority, while the latter has officially launched a formal investigation regarding a smart policing contract. According to the technical specifications of this contract, in early 2021, the vendor will develop and deliver to the Hellenic Police smart devices

with integrated software enabling facial recognition and automated fingerprint identification, among other functionalities. The devices will be the size of a smartphone, and police officers will be able to use them during police stops and patrols in order to take a close-up photograph of an individual's face and collect her/his fingerprints. Then, the fingerprints and the photographs collected will immediately be compared with data already stored in central databases for identification purposes. However, it appears that the Hellenic Police has not proceeded to the necessary risk assessment, and it remains to be seen whether a violation of EU data protection law has taken place. Thus, it is understood that this Section of the draft Guidelines is of outmost importance for the protection of the rights and freedoms of individuals in Europe.

The necessity and proportionality principles

We could suggest that the final text of the Guidelines would further reflect on the necessity and proportionality principles as regards the use of facial recognition systems. Undoubtedly, any interference that is in accordance with domestic legal provisions, pursues a legitimate aim, is necessary in a democratic society, and is proportionate to pursue that aim, is considered to be acceptable.[1] However, as a means to establish whether a particular infringement upon the right to privacy or any other right is "necessary in a democratic society" there is the need to balance on the one hand the State's interests to incorporate facial recognition tools in public spaces and on the other hand the individual's right to privacy and/or any other affected rights as mentioned above.

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 interference with the right to privacy. 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.[2] Nevertheless, this 'pressing social need' requirement mentioned above 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'.[3]

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 with their measures interfere with the right to privacy of individuals shall achieve a fair balance between the purpose of this interreference and the means

---

[1] *ECHR* , art 8[2]; *EU Charter,* art 52[1].

[2] European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights', (Online Report, 2020) https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

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

used to achieve it. Otherwise stated, the added value of the interreference should not outweigh its potential negative impact to the individual concerned.[4]

Thus, one could argue that European States that are interested in incorporating facial recognition tools, would firstly need to identify the pressing social need that these tools aim to address, and secondly to demonstrate that the adoption of these tools will substantially contribute to addressing this particular pressing need. However, as far as Homo Digitalis is concerned, European countries neither have justified the pressing social need that would demand the adoption of facial recognition tools, nor have proved that these tools will substantially contribute to addressing such pressing social need.

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