12th January 2021

Dear Executive Vice-President Vestager,
Dear Vice President Jourová,
Dear Commissioner Breton,
Dear Commissioner Dalli,
Dear Commissioner Reynders,
Dear Commissioner Johansson,

cc: Lucilla Sioli,
cc: Juha Heikkilä,

Re: Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence

We, the undersigned, write to restate the vital importance of clear regulatory red lines to prevent uses of artificial intelligence which violate fundamental rights. As we await the Commission's legislative proposal on artificial intelligence, expected from Directorate-General CONNECT during Q1 of 2021, we emphasise that regulatory limitations form a necessary part of a fundamental rights-based artificial intelligence regulation.

EU Member States and EU institutions have an obligation under the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights to ensure that each person's rights to privacy, data protection, free expression and assembly, non-discrimination, dignity and other fundamental rights are not unduly restricted by the use of new and emerging technologies. Without appropriate limitations on the use of AI-based technologies, we face the risk of violations of our rights and freedoms by governments and companies alike.

The development of AI offers great potential to benefit people and society. However, socially-beneficial innovation can only be achieved when we guarantee that uses are safe, legal, and do not discriminate. The European Union now has the opportunity and the responsibility to ensure democratic oversight and clear regulation before technologies are deployed. Europe's industries - from AI developers to car manufacturing companies - will also benefit greatly from the regulatory certainty that comes from clear legal limits and an even playing field for fair competition.

We, the undersigned, **call for regulatory limits on deployments of artificial intelligence that unduly restrict human rights.** In addition to strong enforcement of the General Data Protection Regulation (GDPR) and safeguards such as human rights impacts assessments, software transparency and the availability of datasets for public scrutiny, **it is vital that the upcoming regulatory proposal establishes in law clear limitations as to what can be considered lawful uses of AI**, to unequivocally address the following issues:

- the enabling of biometric mass surveillance and monitoring of public spaces;
- the exacerbation of structural discrimination, exclusion and collective harms;
- the restriction of and discriminatory access to vital services such as health-care and social security;
- the surveillance of workers and infringement of workers' fundamental rights;
- the impeding of fair access to justice and procedural rights;
- the use of systems which make inferences and predictions about our most sensitive characteristics, behaviours and thoughts;

- and, crucially, the manipulation or control of human behaviour and associated threats to human dignity, agency, and collective democracy.

In particular, we call attention to specific (but non-exhaustive) examples of uses that are incompatible with a democratic society and must be prohibited or legally restricted in the AI legislation:

1. **Biometric mass surveillance**:
   Uses of biometric surveillance technologies to process the indiscriminately or arbitrarily-collected data of people in publicly-accessible spaces (for example, remote facial recognition) enables mass surveillance and creates a 'chilling effect' on people's fundamental rights and freedoms. Any deployment of biometric surveillance in public or publicly-accessible spaces amounts to, per definition, the mass indiscriminate processing of biometric data. Such use of biometric mass surveillance intrudes the psychological integrity and well-being of individuals, in addition to the violation of a vast range of fundamental rights. As emphasised in EU data protection legislation and case law, such uses are neither necessary nor proportionate to the aim sought, and **must therefore be clearly prohibited in the AI legislation through an explicit ban on the indiscriminate or arbitrarily-targeted use of biometrics which can lead to mass surveillance.** This will ensure that law enforcement, national authorities and private entities cannot abuse the current wide margin of exception and discretion currently possible under the existing general legal principles of a prohibition on biometric processing.

2. **Uses of AI at the border and in migration control:**
   The increasing examples of AI deployment in the field of migration control pose a growing threat to the fundamental rights of migrants, to EU law, and to human dignity. Among other worrying use cases, AI has been tested to purportedly detect lies for the purposes of immigration applications at European borders and to monitor deception in English language tests through voice analysis, all of which lack credible scientific basis. In addition, EU migration policies are increasingly underpinned by AI systems, such as facial recognition, algorithmic profiling and prediction tools for use within migration management processes, including for forced deportation. These use cases may infringe on data protection rights, the right to privacy, the right to non-discrimination, and several principles of international migration law, including the right to seek asylum. Given those concerns and the significant power imbalance that such deployments exacerbate and exploit, **there should be a ban or moratorium on the use of automated technologies in border and migration control until they are independently assessed to determine compliance with international human rights standards.**

3. **Social scoring and AI systems determining access to social rights and benefits**
   AI systems have been deployed in various contexts in a manner that threatens the allocation of social and economic rights and benefits. For example, in the areas of welfare resource allocation, eligibility assessment and fraud detection, the deployment of AI systems to predict risk, verify people's identity and calculate their benefits greatly impacts people's access to vital public services and has a potentially grave impact on the fundamental right to social security and social assistance. This is due to the likelihood of discriminatory profiling, mistaken results and the inherent fundamental rights risks associated with the processing of sensitive biometric data. A number of examples demonstrate how automated decision-making systems are negatively impacting and targeting poor, migrant and working class people, including the

deployment of SyRI in the Netherlands and the use of data-driven systems in Poland to profile unemployed people, with severe implications for data protection and non-discrimination rights. Further, uses in the context of employment and education have highlighted highly-intrusive worker and student surveillance, including social scoring systems, intensive monitoring for performance targets, and other measures which limit work autonomy, diminish well-being and limit workers' and students' privacy and fundamental rights. There are have also been cases of discriminatory use of AI technologies against persons with disabilities by state and private entities in the allocation of social benefits and access to education. **The upcoming legislative proposal must legally restrict uses and deployments of AI which unduly infringe upon access to social rights and benefits.**

4. **Predictive policing:**
   Uses of predictive modelling to forecast where, and by whom, certain types of crimes are likely to be committed repeatedly score poor, working class, racialised and migrant communities with a higher likelihood of presumed future criminality. As highlighted by the European Parliament, deployment of such predictive policing can result in "grave misuse". The use of apparently "neutral" factors, such as postal code, in practice serve as a proxy for race and other protected characteristics, reflecting histories of over-policing of certain communities, exacerbating racial biases and affording false objectivity to patterns of racial profiling. A number of predictive policing systems have been demonstrated to disproportionately include racialised people, in complete disaccord with actual crime rates. Predictive policing systems undermine the presumption of innocence and other due process rights by treating people as individually suspicious based on inferences about a wider group. **The European Commission must legally prohibit deployments of predictive policing systems in order to protect fundamental rights.**

5. **Use of risk assessment tools in the criminal justice system and pre-trial context**
   The use of algorithms in criminal justice matters to profile individuals within legal decision-making processes presents severe threats to fundamental rights. Such tools base their assessments on a vast collection of personal data unrelated to the defendants' alleged misconduct. This collection of personal data for the purpose of predicting the risk of recidivism cannot be perceived as necessary nor proportionate to the perceived purpose, in particular considering the implications for the right to respect for private life, and the presumption of innocence. In addition, substantial evidence has shown that the introduction of such systems in criminal justice systems in Europe and elsewhere has resulted in unjust and discriminatory outcomes. Beyond this, it may be impossible for legal professionals to understand the reasoning behind the outcomes of the system. **We argue that legal limits must be imposed on AI risk assessment systems in the criminal justice context.**

These examples illustrate the need for an ambitious artificial intelligence proposal in 2021 which foregrounds people's rights and freedoms. The signatories of this letter call for the legislative proposal on artificial intelligence to include:

1. An explicit ban on the indiscriminate or arbitrarily-targeted use of biometrics in public or publicly-accessible spaces which can lead to mass surveillance;
2. Legal restrictions or legislative red-lines on the uses which contravene fundamental rights, including, but not limited to, uses of AI at the border, predictive policing, systems which restrict access to social rights and benefits, and risk-assessment tools in the criminal justice context;

3. The explicit inclusion of marginalised and affected communities in the development of EU AI legislation and policy moving forward.

We look forward to a legislation which puts people first, and await your response about how the upcoming artificial intelligence proposal will address the concerns outlined in this letter.

Yours sincerely,

European Digital Rights (EDRi), including:

Access Now
Bits of Freedom
Chaos Computer Club
D3 - Defesa dos Direitos Digitais
Electronic Privacy Information Center (EPIC)
Fitug
Hermes Center
Homo Digitalis
IT-Pol Denmark
Iuridicum Remedium
Metamorphosis Foundation
Panoptykon Foundation
Privacy International
Statewatch

Other signatories:

AI Now Institute, NYU
Algorithm Watch
Amnesty International
App Drivers and Couriers Union (ADCU)
Associazione Certi Diritti
Associazione Luca Coscioni
Associazione per gli Studi Giuridici sull'Immigrazione
Big Brother Watch
Center for Intersectional Justice (CIJ)
Democratic Society
Digitale Freiheit
Dutch Section - International Commission of Jurists (NJCM)
Each One Teach One (EOTO) e.V.
Eumans
European Disability Forum
European Evangelical Alliance (EEA)
European Network Against Racism (ENAR)
European Network On Religion and Belief (ENORB)
European Roma Grassroots Organizations (ERGO) Network
European Youth Forum
Fair Trials
Federation of Humanitarian Technologists
Fundación Secretariado Gitano
Ghett'up
Greek Forum of Migrants

Human Rights Watch
ILGA-Europe
info.nodes
International Committee on the Rights of Sex Workers in Europe (ICRSE)
International Federation for Human Rights (FIDH)
International Decade for People of African Descent, Spain
Kif Kif
Liberty
Ligue des Droits Humains
Minderhedenforum
Montreal AI Ethics Institute
Open Society European Policy Institute
Platform for International Cooperation on Undocumented Migrants (PICUM)
Privacy Network
Ranking Digital Rights
Refugee Law Lab, York University
Save Space e.V.
Simply Secure
Stop Ethnic Profiling Platform Belgium
StraLi - for Strategic Litigation
UNI europa – European Services Workers Union
University College Dublin Centre for Digital Policy