EU Trilogues: The AI Act must protect people's rights

A civil society statement on fundamental rights in the EU Artificial Intelligence Act

As European Union institutions[1] begin trilogue negotiations, civil society calls on EU institutions to ensure the Regulation puts people and fundamental rights first in the Artificial Intelligence Act (AI Act).

In Europe and around the world, AI systems are used to monitor and control us in public spaces, predict our likelihood of future criminality, facilitate violations of the right to claim asylum, predict our emotions and categorise us, and to make crucial decisions that determine our access to public services, welfare, education and employment.

---

1   European Parliament, the Council of the European Union and European Commission engage in inter-institutional negotiations, 'trilogues', to reach a provisional agreement on a legislative proposal that is acceptable to both the Parliament and the Council.

Without strong regulation, companies and governments will continue to use AI systems that exacerbate mass surveillance, structural discrimination, centralised power of large technology companies, unaccountable public decision-making and environmental damage.

We call on EU institutions to ensure that AI development and use is accountable, publicly transparent, and that people are empowered to challenge harms:

1. Empower affected people with a framework of accountability, transparency, accessibility and redress

It is crucial that the EU AI Act empowers people and public interest actors to understand, identify, challenge and seek redress when the use of AI systems exacerbate harms and violates fundamental rights. To do this, it is crucial that the AI Act develops a framework of accountability, transparency, accessibility and redress. This must include:

- An obligation on all public and private 'users' (deployers) to conduct and publish a fundamental rights impact assessment before each deployment of a high-risk AI system and meaningfully engage civil society and affected people in this process;

- Require all users of high-risk AI systems, and users of all systems in the public sphere, to register their use in the publicly viewable EU database before deployment;

- Ensure that EU-based AI providers whose systems impact people outside of the EU are subject to the same requirements as those inside the EU.

- Ensure horizontal and mainstreamed accessibility requirements for all AI systems;

- Ensure people affected by AI systems are notified and have the right to seek information when affected by AI-assisted decisions and outcomes;

- Include a right for people affected to lodge a complaint with a national authority if their rights have been violated by the use of an AI system;

- Include a right to representation of natural persons and the right for public interest organisations to lodge standalone complaints with a national supervisory authority;

- Include a right to effective remedies for the infringement of rights.

2. Draw limits on harmful and discriminatory surveillance by national security, law enforcement and migration authorities

Increasingly AI systems are developed and deployed for harmful and discriminatory forms of state surveillance. Such systems disproportionately target already marginalised communities, undermine legal and procedural rights, as well as contributing to mass surveillance. When AI systems are deployed in the context of law enforcement, security and migration control, there is an even greater risk of harm, and violations of fundamental rights and the rule of law. To maintain public oversight and prevent harm, the EU AI Act must include:

- A full ban on [real-time and post remote biometric identification](#) in publicly accessible spaces, by all actors, without exception;

- A prohibition of all forms of [predictive and profiling systems](#) in law enforcement and criminal justice (including systems which focus on and target individuals, groups and locations or areas);

- Prohibitions on [AI in migration contexts](#) to make individual risk assessments and profiles based on personal and sensitive data, and predictive analytic systems when used to interdict, curtail and prevent migration;

- A prohibition on [biometric categorisation systems](#) that categorise natural persons according to sensitive or protected attributes as well as the use of any biometric categorisation and automated behavioural detection systems in publicly accessible spaces;

- A ban on the use of [emotion recognition systems](#) to infer people's emotions and mental states;

- Reject the Council's addition of a blanket exemption from the AI Act of AI systems developed or used for national security purposes;

- Remove exceptions and loopholes for law enforcement and migration control introduced by the Council;

- Ensuring public transparency as to what, when and how public actors deploy high-risk AI in areas of law enforcement and migration control, avoiding any exemption to the obligation to register high-risk uses into the EU AI database.

3. Push back on Big Tech lobbying: remove loopholes that undermine the regulation

The EU AI Act must set clear and legally-certain standards of application if the legislation is to be effectively enforced. The legislation must uphold an objective process to determine which systems are high-risk, and remove any 'additional layer' added to the high-risk classification process. Such a layer would allow AI developers, without accountability or oversight, to decide whether or not their systems pose a 'significant' enough risk to warrant legal scrutiny under the Regulation. A discretionary risk classification process risks undermining the entire AI Act, shifting to self-regulation, posing insurmountable challenges for enforcement and harmonisation, and incentivising larger companies to under-classify their own AI systems.

Negotiators of the AI Act must not give in to lobbying efforts of large tech companies seeking to circumvent regulation for financial interest. The EU AI Act must:

- Remove the additional layer added to the risk classification process in Article 6 restore the clear, objective risk-classification process outlined in the original position of the European Commission;

- Ensure that providers of general purpose AI systems are subject to a clear set of obligations under the AI Act, avoiding that smaller providers and users bear the brunt of obligations better suited to original developers.

Drafted by:

1. European Digital Rights (EDRi)
2. Access Now
3. Algorithm Watch
4. Amnesty International
5. Bits of Freedom
6. Electronic Frontier Norway (EFN)
7. European Center for Not-for-Profit Law, (ECNL)
8. European Disability Forum (EDF)
9. Fair Trials
10. Homo Digitalis
11. Irish Council for Civil Liberties (ICCL)
12. Panoptykon Foundation

13. Platform for International Cooperation on the Rights of Undocumented Migrants (PICUM)

Signed:

14. 7amleh-The Arab Center for the Advancement of Social Media
15. Academia Cidadã - Citizenship Academy
16. Africa Solidarity Centre Ireland
17. AlgoRace
18. Algorights
19. All Faiths and None
20. All Out
21. Anna Henga
22. Anticorruption Center
23. ARSIS - Association of the Social Support of Youth
24. ARTICLE 19
25. Asia Indigenous Peoples Pact
26. Asociación Por Ti Mujer
27. Aspiration
28. Association for Juridical Studies on Immigration (ASGI)
29. Association Konekt
30. ASTI asbl - Luxembourg
31. AsyLex
32. Austria human rights League
33. Avaaz
34. Balkan Civil Society Development Network
35. Bulgarian center for Not-for-Profit Law (BCNL)
36. Bürgerrechte & Polizei/CILIP, Germany
37. Canadian Civil Liberties Association

38. Chaos Computer Club
39. Charity & Security Network
40. Citizen D / Državljan D
41. Civil Liberties Union for Europe
42. Civil Society Advocates
43. Coalizione Italiana Libertà e Diritti civili
44. Comisión General Justicia y Paz de España
45. Comisión Legal Sol
46. Commission Justice et Paix Luxembourg
47. Controle Alt Delete
48. Corporate Europe Observatory (CEO)
49. D64 - Zentrum für digitalen Fortschritt
50. DanChurchAid (DCA)
51. Danes je nov dan, Inštitut za druga vprašanja
52. Data Privacy Brasil
53. Defend Democracy
54. Democracy Development Foundation
55. Digital Security Lab Ukraine
56. Digital Society, Switzerland
57. Digitalcourage
58. Digitale Gesellschaft
59. Digitalfems
60. Diotima Centre for Gender Rights & Equality
61. Donestech

62. epicenter.works - for digital rights

63. Equinox Initiative for Racial Justice

64. Estonian Human Rights Centre

65. Eticas

66. EuroMed Rights

67. European Anti-Poverty Network (EAPN)

68. European Center for Human Rights

69. European Civic Forum

70. European Movement Italy

71. European Network Against Racism (ENAR)

72. European Network on Statelessness

73. European Sex Workers Rights Alliance (ESWA)

74. Fair Vote

75. FEANTSA, European Federation of National Organisations Working with the Homeless

76. Free Press Unlimited

77. Fundación Secretariado Gitano

78. Gong

79. Greek Forum of Migrants

80. Greek Forum of Refugees

81. Health Action International

82. Hiperderecho

83. Homo Digitalis

84. horizontl Collaborative

85. Human Rights Watch

86. I Have Rights

87. IDAY-Liberia Coalition Inc.

88. ILGA-Europe (the European region of the International Lesbian, Gay, Bisexual, Trans and Intersex Association)

89. info.nodes

90. Initiative Center to Support Social Action "Ednannia"

91. Institute for Strategic Dialogue (ISD)

92. International Commission of Jurists

93. International Rehabilitation Council for Torture victims

94. IT-Pol

95. Ivorian Community of Greece

96. Kif Kif vzw

97. KOK - German NGO Network against Trafficking in Human Beings

98. KontraS

99. Kosovar Civil Society Foundation (KCSF)

100. La Strada International

101. Lafede.cat

102. LDH (Ligue des droits de l'Homme)

103. Legal Centre Lesvos

104. Liberty

105. Ligali / IDPAD (Hackney)

106. Ligue des droits humains, Belgium

107. LOAD e.V.

108. Maison de l'Europe de Paris

109. Metamorphosis Foundation

110. Migrant Tales

111. Migration Tech Monitor

112. Mnemonic

113. Mobile Info Team

114. Moje Państwo Foundation

115. Moomken organization for Awareness and Media