# 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.

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.

---

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.

**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. Hermes Center
11. Irish Council for Civil Liberties (ICCL)
12. Panoptykon Foundation
13. Platform for International Cooperation on the Rights of Undocumented Migrants (PICUM)

Signed:

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

39. Civil Society Advocates
40. Coalizione Italiana Libertà e Diritti civili
41. Comisión General Justicia y Paz de España
42. Commission Justice et Paix Luxembourg
43. Controle Alt Delete
44. Corporate Europe Observatory (CEO)
45. D64 - Zentrum für digitalen Fortschritt
46. D64 - Zentrum für Digitalen Fortschritt e. V.
47. DanChurchAid (DCA)
48. Danes je nov dan, Inštitut za druga vprašanja
49. Data Privacy Brasil
50. Data Privacy Brasil Research Association
51. Defend Democracy
52. Democracy Development Foundation
53. Digital Security Lab Ukraine
54. Digital Society, Switzerland
55. Digitalcourage
56. Digitale Gesellschaft
57. Digitalfems
58. Diotima Centre for Gender Rights & Equality
59. Donestech
60. epicenter.works - for digital rights
61. Equinox Initiative for Racial Justice
62. Estonian Human Rights Centre
63. Eticas
64. EuroMed Rights
65. European Anti-Poverty Network (EAPN)
66. European Center for Human Rights
67. European Center for Not-for-Profit Law
68. European Civic Forum
69. European Movement Italy
70. European Network Against Racism (ENAR)
71. European Network on Statelessness
72. European Sex Workers Rights Alliance (ESWA)
73. Fair Vote
74. FEANTSA, European Federation of National Organisations Working with the Homeless
75. Free Press Unlimited
76. Fundación Secretariado Gitano
77. Gong
78. Greek Forum of Migrants
79. Greek Forum of Refugees
80. Health Action International
81. Hiperderecho
82. Homo Digitalis
83. horizontl Collaborative
84. Human Rights Watch
85. I Have Rights
86. IDAY-Liberia Coalition Inc.
87. ILGA-Europe (the European region of the International Lesbian, Gay, Bisexual, Trans and Intersex Association)
88. info.nodes
89. Initiative Center to Support Social Action "Ednannia"
90. Institute for Strategic Dialogue (ISD)
91. International Commission of Jurists
92. International Rehabilitation Council for Torture victims
93. IT-Pol
94. Ivorian Community of Greece
95. Kif Kif vzw
96. KOK - German NGO Network against Trafficking in Human Beings
97. KontraS
98. Kosovar Civil Society Foundation (KCSF)
99. La Strada International
100. Lafede.cat
101. LDH (Ligue des droits de l'Homme)

102. Legal Centre Lesvos

103. Liberty

104. Ligali / IDPAD (Hackney)

105. Ligue des droits humains, Belgium

106. LOAD e.V.

107. Maison de l'Europe de Paris

108. Metamorphosis Foundation

109. Migrant Tales

110. Migration Tech Monitor

111. Mnemonic

112. Mobile Info Team

113. Moje Państwo Foundation

114. Moomken organization for Awareness and Media

115. National Campaign for Sustainable Development Nepal

116. National Network for Civil Society (BBE)

117. National old folks of Liberia.com

118. Novact

119. Observatorio Trabajo, Algoritmo y Sociedad

120. Open Knowledge Foundation Germany

121. Partners Albania for Change and Development

122. Politiscope

123. Privacy First

124. Privacy International

125. Privacy Network

126. Promo-LEX Association

127. Prostitution Information Center (PIC)

128. Protection International

129. Public Institution Roma Community Centre

130. Racism and Technology Center

131. Red en Defensa de los Derechos Digitales

132. Red Española de Inmigración y Ayuda al Refugiado

133. Refugee Law Lab, York University

134. REPONGAC

135. SHARE Foundation

136. SOLIDAR & SOLIDAR Foundation

137. Statewatch

138. Stichting LOS

139. Superbloom (previously known as Simply Secure)

140. SUPERRR Lab

141. SwitchMED - Maghweb

142. Symbiosis

143. TAMPEP European Network for the Promotion of Rights and Health among Migrant Sex Workers.

144. TEDIC - Paraguay

145. The Border Violence Monitoring Network

146. The Good Lobby

147. Transparency International

148. Volonteurope

149. WeMove Europe

150. Xnet