EU policymakers: regulate police technology!

Civil society calls on the EU to draw limits on surveillance technology in the Artificial Intelligence Act

As AI systems are increasingly used by law enforcement, migration control and national security authorities, the EU Artificial Intelligence Act (AI Act) is an urgent opportunity to prevent harm, protect people from rights violations and provide legal boundaries for authorities to use AI within the confines of the rule of law.

Increasingly, in Europe and around the world, AI systems are developed and deployed for harmful and discriminatory forms of state surveillance. From the use of biometrics for identification, recognition and categorisation, to predictive systems in various decision-making and resource allocation capacities, AI in law enforcement disproportionately targets already marginalised communities, undermines legal and procedural rights, and enables mass surveillance.

When AI systems are deployed in contexts of law enforcement, security and migration control (including the policing of social security), the power imbalance between the authorities and the surveilled is even more profound. This means that there is an even greater risk of harm, and violations of fundamental rights and the rule of law.

This statement outlines the urgent need to regulate the use of AI systems by law enforcement, migration control and national security authorities throughout Europe.

We point to the specific dangers to freedom of assembly, liberty, the right to asylum, privacy and data protection, the right to social protection, and non-discrimination when such technology is deployed by those authorities.

Civil society organisations are calling for an AI Act that prevents unchecked forms of discriminatory and mass surveillance. In order to uphold human rights and prevent harm from the use of AI in policing, migration control and national security, the EU AI Act must:

1. **Include legal limits prohibiting AI for uses that pose an unacceptable risk for fundamental rights.** This includes a legal prohibition on different forms of biometric surveillance, predictive policing, and harmful uses of AI in the migration context.

2. **Provide public transparency and oversight when police, migration and national security agencies use 'high-risk' AI,** by upholding an equal duty of these authorities to register high risk uses in the EU AI database.

3. **Ensure that the AI Act properly regulates the uses of AI in policing, migration and national security that pose risk to human rights,** specifically the full list of AI in migration control, and ensuring that national security is not excluded from scope.

Why the EU AI Act needs to regulate the use of AI in law enforcement, migration and national security:

- **Checks on state and police power are essential to the functioning of a democratic rights-based society**. The AI Act is intended to recognise and regulate high-risk uses of AI and, where necessary, prohibit them where the threat to fundamental rights is too great. Uses of AI by state authorities in fields of policing, migration and national security are amongst the most high risk use cases, because they most acutely impact fundamental rights including freedom of assembly and expression, the right to a fair trial, the presumption of innocence, non-discrimination, and the right to claim asylum. The work of police, migration and security authorities governs access to the public space, outcomes in the criminal justice and migration sectors, and various other areas of life with the highest impact on fundamental rights. As such, the use of AI by these authorities calls for the greatest scrutiny and transparency, and requires the clearest boundaries to uphold basic democratic principles.
- **The use of AI in the fields of policing, security and migration amplifies structural discrimination against already marginalised and over-surveilled communities**, such as racialised people, migrants, and many other discriminated groups. Mounting evidence demonstrates that such AI systems reinforce the over-policing, disproportionate surveillance, detention and imprisonment of structurally discriminated against groups. The data used to create and operate such systems reflects historical, systemic, institutional and societal discrimination. This discrimination is so fundamental and ingrained that all such systems will reinforce such outcomes. Prohibitions, public transparency and accountability frameworks are necessary so that harms are prevented and people are empowered to challenge harms.
- **The use of AI in field of policing, security and migration invites private sector influence into core aspects of public governance,** requiring even stronger oversight and legal limits in order to ensure peoples' rights are upheld. As these fields are government functions, it is crucial the AI Act ensures that private sector's development of AI in these fields is publicly transparent. AI systems, when deployed in areas of policing, migration and national security must be accountable first and foremost to fundamental rights standards and the rule of law, rather than

profit motives. As such safeguards, oversight and legal limits must be applied.

Detailed recommendations on how the EU AI Act must be amended in these areas are provided in annex to this statement.

Signed,

1. European Digital Rights (EDRi)
2. Access Now
3. AlgoRace
4. Algorights
5. AlgorithmWatch
6. All Out
7. Àltera
8. AMERA International
9. Amnesty International
10. Angela Daly - Professor of Law, University of Dundee, Scotland, UK
11. Anita Okoro
12. ApTI - Asociația pentru Tehnologie și Internet
13. Asia Indigenous Peoples Pact
14. Aspiration
15. Association for Legal Studies on Immigration (ASGI)
16. Association Konekt
17. Association of citizens for promotion and protection of cultural and spiritual values Legis Skopje
18. ASTI asbl - Association de soutien aux travailleurs immigrés
19. AsyLex
20. Bits of Freedom
21. Bridget Anderson - University of Bristol
22. Bulgarian center for Not-for-Profit Law (BCNL)
23. Centre for Information Technology and Development (CITAD)
24. Centre for Peace Studies

25. Chaos Computer Club e.V.

26. Chiara De Capitani (PhD, Università degli Studi di Napoli "L'Orientale")

27. Civil Liberties Union for Europe

28. Comisión General de Justicia y Paz de España

29. Controle Alt Delete

30. Corporate Europe Observatory (CEO)

31. D64 - Zentrum für Digitalen Fortschritt e. V.

32. Danes je nov dan, Inštitut za druga vprašanja

33. Democracy Development Foundation

34. Digital Ethics Center / Skaitmenines etikos centras

35. Digitalcourage

36. Digitale Gesellschaft

37. Digitale Gesellschaft

38. Dr Derya Ozkul

39. Ekō

40. Electronic Frontier Finland

41. Elektronisk Forpost Norge (EFN)

42. Elisa Elhadj

43. epicenter.works

44. Equipo Decenio Afrodescendiente

45. Ermioni Xanthopoulou

46. Eticas

47. EuroMed Rights

48. European Anti-Poverty Network (EAPN)

49. European Center for Not-for-Profit Law

50. European Civic Forum

51. European Movement Italy

52. European Sex Workers' Rights Alliance (ESWA)

53. Exploring Womanhood Foundation

54. Fair Trials

55. Fair Vote UK

56. Francesca Palmiotto Hertie School

57. Fundación Cepaim

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

59. Gernot Klantschnig, University of Bristol

60. Glitch

61. Greek Forum of Migrants

62. Homo Digitalis

63. Human Rights Association (İHD)

64. I Have Rights

65. IDAY Liberia Coalition Inc

66. Instituto de Asuntos Culturales

67. International Commission of Jurists

68. International Women* Space e.V

69. Irish Council for Civil Liberties (ICCL)

70. King's College London

71. KISA - Equality, Support, Antiracism

72. La Quadrature du Net

73. Legal Center for the Protection of Human Rights and the Environment (PIC)

74. Legal Centre Lesvos

75. Liberty

76. Ligue algérienne pour la défense des droits de l'homme

77. Ligue des droits de l'Homme (France)

78. Ligue des droits humains (Belgium)

79. LOAD e.V.

80. Lorenzo Vianelli (University of Bologna)

81. Mallika Balakrishnan, Migrants Organise

82. Migrant Tales

83. Mirjam Twigt

84. Moje Państwo Foundation

85. Mujeres Supervivientes

86. Novact

87. Open Knowledge Foundation Germany

88. Organisation International Federation of ACAT (FIACAT)

89. Panoptykon Foundation

90. Partners Albania for Change and Development

91. Platform for International Cooperation on Undocumented Migrants (PICUM)

92. Politiscope

93. Privacy First

94. Privacy International

95. Privacy Network

96. Prof. Dr. Lorenz Boellinger, University of Bremen

97. Prof. Jan Tobias Muehlberg (Universite Libre de Bruxelles)

98. Promo-LEX Association

99. Prostitution information center

100. REFUGEE LEGAL SUPPORT

101. REPONGAC Réseau des Plateformes Nationales d'ONG d'Afrique Centrale

102. Ryan Lutz, University of Bristol

103. Sea-Watch

104. SOLIDAR & SOLIDAR Foundation

105. Statewatch

106. Stichting Landelijk Ongedocumenteerden Steunpunt

107. SUDS - Associació Internacional de Solidaritat i Cooperació

108. Superbloom (previously known as Simply Secure)

109. SUPERRR Lab

110. Symbiosis - Council of Europe School for Political Studies in Greece

111. Taraaz

112. Michael Ellison, University of Bristol

113. Vicki Squire, University of Warwick

114. Victoria Canning - University of Bristol

115. Volonteurope

Annex - Detailed recommendations

In order to achieve the calls outlined in the civil society statement 'EU policymakers – regulate police technology!', the EU AI Act must:

1. Include legal limits prohibiting AI for uses that pose an unacceptable risk for fundamental rights. This includes a legal prohibition on different forms of biometric surveillance, predictive policing, and harmful uses of AI in the migration context.

- A full ban on real-time and post remote biometric identification in publicly accessible spaces (including border areas and around migration detention facilities), by all actors, without exception (Article 5(1)(d));
- A broad definition of of public-accessible spaces, which includes border areas (Reject Recital 9, Council Mandate);
- 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) (Article 5(1)(da) EP mandate);
- 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 ban on the use of biometric categorisation systems, such as racial, political or gender profiling systems (Article 5(1) (ba) EP mandate) ;[1] and the use of automated behavioural detection systems in publicly accessible spaces; [2]
- A ban on the use of so called 'emotion recognition' systems to infer or predict people's emotions and mental states[3]
- Prohibit export of systems which are banned in the EU (article 2(1) of the European Parliament mandate).

2. Provide public transparency and oversight when police, migration and national security agencies use 'high-risk' AI, by upholding an equal duty of these authorities to register high risk uses in the EU AI database.

- Uphold the obligation to register themselves and their use of AI high-risk systems in the public database (Reject exemption foreseen in Articles 29 (5) and 51 (2);

[1] EP mandate: Article 5.1.(ba) – ban on biometric categorisation, but limited to characteristics defined in recital XX.

[2] EP: ban on automated behavioural detection received strong support in Plenary but did not make the final text.

[3] EP mandate: Art. 5.1.(d)(dc) – ban on emotion recognition in specific sectors: law enforcement….

- Require equal transparency for providers of high-risk systems deployed in the areas of law enforcement and migration to register their products on the public database (Reject exemption foreseen in Article 51 (1) Council mandate);
- Ensure the reporting of the testing of AI systems in sandboxes is transparent and no blanket exemption is made for processing of 'sensitive operational data' , which is a vague and broad term (Reject exemptions foreseen in Articles Article 53 (5), Article 54 (1) (j));
- Ensure the obligation to register the testing in real-world conditions in the EU database (Reject exemptions foreseen in Articles Article 54a (4) (c) and 54a (4) (j) Council mandate);
- Ensure strong human oversight measures apply consistently throughout the Act, especially for AI high-risk systems used by these authorities (Reject exemptions foreseen in Articles 14(5) and Article 29 (4)).

3. Ensure that the AI Act properly regulates the uses of AI in policing, migration and national security that pose risk to human rights, specifically a comprehensive list of AI in migration control, and ensuring that national security is not excluded from scope.

- Reject the Council's addition of a blanket exemption from the AI Act of AI systems developed or used for national security purposes (Article 2(3) Council mandate);

  Reject the blanket exemption for high-risk systems that are part of migration databases (e.g. EURODAC, VIS, SIS) listed in Annex IX (as per Article 83(1) EP Mandate);
- Ensure the list of high-risk systems in Annex III includes all potential dangerous AI systems:
  - BIometric identification systems, such as hand-held facial image, fingerprint or palm scanners, voice or iris identification technology, whose use can lead to discrimination, surveillance and coercion of the person subjected (Annex III, Point 1 EP Mandate)
  - AI systems used for border management activities, such as unmanned drones or thermal cameras, which can lead to the violent interception of asylum seekers and their push-back (Annex III, Point 7 (d a) EP Mandate);
  - AI systems to forecast migration movements and border crossings whose use can inform punitive policies (Annex III, Point 7 (d b) EP Mandate).