Responsables políticos de la UE: ¡regulen la tecnología policial!

La sociedad civil pide a la UE que ponga límites a la vigilancia tecnológica en la Ley de Inteligencia Artificial

Dado que los sistemas de inteligencia artificial son cada vez más utilizados por las autoridades policiales, de control migratorio y de seguridad nacional, la Ley de Inteligencia Artificial de la UE (Ley de Inteligencia Artificial) es una oportunidad urgente para prevenir daños y proteger a las personas de las violaciones de sus derechos, proporcionando límites legales para que las autoridades utilicen la inteligencia artificial dentro del marco del Estado de Derecho.

Cada vez más, en Europa y en todo el mundo, se desarrollan y despliegan sistemas de IA para formas perjudiciales y discriminatorias de vigilancia estatal. Desde el uso de la biometría para la identificación, el reconocimiento y la categorización, hasta los sistemas predictivos en diversas capacidades de toma de decisiones y asignación de recursos, la IA en la aplicación de la ley se dirige de manera desproporcionada a comunidades ya marginadas, socava los derechos legales y procesales y permite la vigilancia masiva de la población. Cuando los sistemas de IA se despliegan en contextos de aplicación de la ley, seguridad y control de la migración (incluida la vigilancia del orden social), el desequilibrio de poder entre las autoridades y los vigilados se hace aún más profundo. Esto significa que existe un riesgo aún mayor de que se produzcan violaciones de los derechos fundamentales, quebrantando así el Estado de Derecho.

Esta declaración subraya la urgente necesidad de regular el uso de los sistemas de IA por parte de las autoridades policiales, de control de la inmigración y de seguridad nacional en toda Europa.

Señalamos los peligros específicos para la libertad de reunión, la libertad, el derecho de asilo, la privacidad y la protección de datos, el derecho a la protección social y la no discriminación cuando esas autoridades despliegan esa tecnología.

Las organizaciones de la sociedad civil piden una Ley de Inteligencia Artificial que impida formas incontroladas de vigilancia discriminatoria y masiva. Para defender los derechos humanos y evitar los perjuicios derivados del uso de la IA en la vigilancia policial, el control de la migración y la seguridad nacional, la Ley de IA de la UE debe:

1. **Incluir límites legales que prohíban la IA para usos que supongan un riesgo inaceptable para los derechos fundamentales.** Esto incluye la prohibición legal de diferentes formas de vigilancia biométrica, la vigilancia policial predictiva y los usos perjudiciales de la IA en el contexto de la migración.
2. **Proporcionar transparencia y supervisión públicas cuando la policía y las agencias de migración y seguridad nacional utilicen IA de "alto riesgo",** manteniendo la misma obligación para estas autoridades de registrar los usos de alto riesgo en la base de datos de IA de la UE**.**

3. **Garantizar que la Ley de IA regula adecuadamente los usos de la IA en el control policial, la migración y la seguridad nacional que suponen un riesgo para los derechos humanos,** en concreto la lista completa de IA en el control de la migración, y garantizar que la seguridad nacional no queda excluida de su ámbito de aplicación.

Por qué es necesario que la Ley de Inteligencia Artificial de la UE regule el uso de la IA en la aplicación de la ley, la migración y la seguridad nacional:

- **El control del poder estatal y policial es esencial para el funcionamiento de una sociedad democrática basada en los derechos**. La Ley de IA pretende reconocer y regular los usos de alto riesgo de la IA y, en caso necesario, prohibirlos cuando la amenaza para los derechos fundamentales sea demasiado grande. Los usos de la IA por parte de las autoridades estatales en los ámbitos policial, de migración y de seguridad nacional se encuentran entre los casos de uso de mayor riesgo, porque afectan de forma más aguda a derechos fundamentales como la libertad de reunión y expresión, el derecho a un juicio justo, la presunción de inocencia, la no discriminación y el derecho a solicitar asilo. La labor de las autoridades policiales, migratorias y de seguridad rige el acceso al espacio público, los resultados en los sectores de la justicia penal y la migración, y otros ámbitos de la vida con mayor repercusión en los derechos fundamentales. Como tal, el uso de la IA por parte de estas autoridades exige el máximo escrutinio y transparencia, y requiere de límites más claros para defender los principios democráticos básicos.

- **El uso de la IA en los ámbitos de la vigilancia policial, la seguridad y la migración profundiza la discriminación estructural contra comunidades ya marginadas y sobrevigiladas,** como las personas racializadas, los migrantes y muchos otros grupos discriminados. Cada vez hay más pruebas que demuestran que estos sistemas de IA refuerzan la sobrevigilancia policial y la vigilancia, detención y encarcelamiento desproporcionados de grupos estructuralmente discriminados. Los datos utilizados para crear y hacer funcionar estos sistemas reflejan una discriminación histórica, sistémica, institucional y social. Esta discriminación es tan fundamental y está tan arraigada que todos estos sistemas refuerzan tales resultados. Son necesarios marcos de prohibición, transparencia pública y rendición de cuentas para prevenir los daños y capacitar a las personas para hacerles frente.

- **El uso de la IA en los ámbitos policial, de seguridad y migratorio invita al sector privado a influir en aspectos fundamentales de la gobernanza pública,** lo que exige una supervisión y unos topes legales aún mayores para garantizar el respeto de los derechos de las personas. Dado que estos ámbitos son funciones gubernamentales, es crucial que la Ley de IA garantice que el desarrollo de la IA por parte del sector privado en estos ámbitos sea públicamente transparente. Los sistemas de IA, cuando se despliegan en ámbitos policiales, migratorios y de seguridad nacional, deben responder ante todo a las normas de derechos fundamentales y al Estado de derecho, y no a motivos lucrativos. Por ello, deben aplicarse salvaguardias, supervisión y límites legales.

En el anexo de esta declaración figuran recomendaciones detalladas sobre cómo debe modificarse la Ley de AI de la UE en estos ámbitos.

Firmado,

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

Anexo - Recomendaciones detalladas

Para lograr los objetivos expuestos en la declaración de la sociedad civil "Responsables políticos de la UE: ¡regulen la tecnología policial!

1. Incluir límites legales que prohíban la IA para usos que supongan un riesgo inaceptable para los derechos fundamentales. Esto incluye la prohibición legal de diferentes formas de vigilancia biométrica, la vigilancia policial predictiva y los usos perjudiciales de la IA en el contexto de la migración.

- Prohibición total de la identificación biométrica en tiempo real y a distancia en espacios de acceso público (incluidas las zonas fronterizas y los alrededores de los centros de detención de inmigrantes), por parte de todos los actores, sin excepción (artículo 5, apartado 1, letra d));
- Una definición amplia de los espacios de acceso público, que incluya las zonas fronterizas (rechazar el considerando 9 del mandato del Consejo);
- Prohibición de todas las formas de sistemas de predicción y elaboración de perfiles en la aplicación de la ley y la justicia penal (incluidos los sistemas que se centran en personas, grupos y lugares o zonas y se dirigen a ellos) (Artículo 5(1)(da) del mandato del PE);
- Prohibición de la IA en contextos migratorios para realizar evaluaciones y perfiles de riesgo individuales basados en datos personales y sensibles, y sistemas analíticos predictivos cuando se utilicen para interceptar, restringir e impedir la migración;
- Prohibición del uso de sistemas de categorización biométrica, como los sistemas de elaboración de perfiles raciales, políticos o de género (artículo 5.1 (ba) del mandato del PE) ; y del uso de sistemas automatizados de detección de comportamientos en espacios de acceso público;
- Prohibición del uso de los llamados sistemas de "reconocimiento de emociones" para inferir o predecir las emociones y estados mentales de las personas.
- Prohibir la exportación de sistemas prohibidos en la UE (artículo 2(1) del mandato del Parlamento Europeo).

2. Proporcionar transparencia y supervisión públicas cuando la policía y las agencias de migración y seguridad nacional utilicen IA de "alto riesgo", manteniendo la misma obligación para estas autoridades de registrar los usos de alto riesgo en la base de datos de IA de la UE.

- Mantener la obligación de registrarse a sí mismos y de registrar el uso que hacen de los sistemas de IA de alto riesgo en la base de datos pública (Rechazar la exención prevista en los artículos 29 (5) y 51 (2);
- Exigir la misma transparencia a los proveedores de sistemas de alto riesgo desplegados en los ámbitos policial y de migración para que registren sus productos en la base de datos pública (Rechazar la exención prevista en el artículo 51, apartado 1, del mandato del Consejo);

- Garantizar que la notificación de las pruebas de los sistemas de IA en entornos aislados sea transparente y que no se establezca una exención general para el tratamiento de "datos operativos sensibles", que es un término vago y amplio (rechazar las exenciones previstas en el artículo 53, apartado 5, y en el artículo 54, apartado 1, letra j));
- Garantizar la obligación de registrar los ensayos en condiciones reales en la base de datos de la UE (rechazar las exenciones previstas en los artículos 54 bis, apartado 4, letra c), y 54 bis, apartado 4, letra j), del mandato del Consejo);
- Garantizar la aplicación coherente en toda la Ley de medidas estrictas de supervisión humana, especialmente para los sistemas de IA de alto riesgo utilizados por estas autoridades (Rechazar las exenciones previstas en el artículo 14, apartado 5, y en el artículo 29, apartado 4).

4. **Garantizar que la Ley de IA regula adecuadamente los usos de la IA en el ámbito policial, migratorio y de seguridad nacional que suponen un riesgo para los derechos humanos, en concreto una lista exhaustiva de la IA en el control migratorio, y garantizar que la seguridad nacional no queda excluida de su ámbito de aplicación.**

- Rechazar la adición por parte del Consejo de una exención general de la Ley de IA para los sistemas de IA desarrollados o utilizados con fines de seguridad nacional (artículo 2, apartado 3, del mandato del Consejo);
- Rechazar la exención general para los sistemas de alto riesgo que forman parte de bases de datos de migración (por ejemplo, EURODAC, VIS, SIS) enumerados en el anexo IX (según el artículo 83, apartado 1, del mandato del PE);
- Garantizar que la lista de sistemas de alto riesgo del anexo III incluya todos los sistemas de IA potencialmente peligrosos:
    - Sistemas de identificación biométrica, como escáneres manuales de imagen facial, de huellas dactilares o de la palma de la mano, tecnología de identificación por voz o iris, cuyo uso puede conducir a la discriminación, la vigilancia y la coacción de la persona sometida (anexo III, punto 1, mandato del PE).
    - Sistemas de IA utilizados para actividades de gestión de fronteras, como drones no tripulados o cámaras térmicas, que pueden dar lugar a la interceptación violenta de solicitantes de asilo y a su rechazo (Anexo III, Punto 7 (d a) Mandato del PE);
    - Sistemas de IA para prever los movimientos migratorios y el cruce de fronteras, cuyo uso puede informar las políticas punitivas (Anexo III, Punto 7 (d b) Mandato del PE).