Responsables politiques de l'UE : réglementez les technologies policières !

La société civile demande à l'UE de fixer des limites aux technologies de surveillance dans la loi sur l'intelligence artificielle.

Alors que les systèmes d'IA sont de plus en plus utilisés par les autorités chargées de l'application de la loi, du contrôle des migrations et de la sécurité nationale, la loi européenne sur l'intelligence artificielle (loi sur l'IA) est une opportunité urgente de prévenir les préjudices et de protéger les personnes contre les violations des droits et de fournir des limites juridiques aux autorités pour qu'elles utilisent l'IA dans les limites de l'État de droit.

De plus en plus, en Europe et dans le monde, des systèmes d'IA sont développés et déployés pour des formes de surveillance étatique préjudiciables et discriminatoires. Qu'il s'agisse de l'utilisation de la biométrie pour l'identification, la reconnaissance et la catégorisation, ou de systèmes prédictifs dans diverses capacités de prise de décision et d'affectation des ressources, l'IA dans l'application de la loi cible de manière disproportionnée des communautés déjà marginalisées, porte atteinte aux droits légaux et procéduraux, et permet une surveillance de masse. Lorsque les systèmes d'IA sont déployés dans des contextes de maintien de l'ordre, de sécurité et de contrôle des migrations (y compris la surveillance de l'ordre sociale), le déséquilibre des pouvoirs entre les autorités et les personnes surveillées est encore plus profond. Cela signifie qu'il existe un risque encore plus grand de préjudice et de violation des droits fondamentaux et de l'État de droit.

Cette déclaration souligne le besoin urgent de réglementer l'utilisation des systèmes d'intelligence artificielle par les autorités chargées de l'application de la loi, du contrôle des migrations et de la sécurité nationale dans toute l'Europe.

Nous soulignons les dangers spécifiques pour la liberté de réunion, la liberté, le droit d'asile, la protection de la vie privée et des données, le droit à la protection sociale et la non-discrimination lorsque ces technologies sont déployées par ces autorités.

Les organisations de la société civile demandent une loi sur l'IA qui empêche les formes incontrôlées de surveillance discriminatoire et de masse. Afin de faire respecter les droits humains et de prévenir les effets néfastes de l'utilisation de l'IA dans les domaines du maintien de l'ordre, du contrôle des migrations et de la sécurité nationale, l'Acte européen sur l'IA doit

1. **Inclure des limites juridiques interdisant l'utilisation de l'IA pour des usages qui présentent un risque inacceptable pour les droits fondamentaux.** Cela inclut une interdiction légale des différentes formes de surveillance biométrique, de la police prédictive et des utilisations préjudiciables de l'IA dans le contexte migratoire.
2. **Assurer la transparence et le contrôle publics lorsque la police, les services d'immigration et les agences de sécurité nationale utilisent l'IA "à haut risque",** en imposant à ces autorités le même devoir d'enregistrer les utilisations à haut risque dans la base de données de l'UE sur l'IA.

3. **Veiller à ce que la loi sur l'IA réglemente correctement les utilisations de l'IA dans les domaines de la police, de l'immigration et de la sécurité nationale qui présentent un risque pour les droits humains,** en particulier la liste complète de l'IA dans le contrôle de l'immigration, et en veillant à ce que la sécurité nationale ne soit pas exclue du champ d'application.

Pourquoi la loi européenne sur l'IA doit-elle réglementer l'utilisation de l'IA dans les domaines de l'application de la loi, des migrations et de la sécurité nationale ?

- **Le contrôle des pouvoirs de l'État et de la police est essentiel au fonctionnement d'une société démocratique fondée sur les droits.** La loi sur l'IA vise à reconnaître et à réglementer les utilisations à haut risque de l'IA et, le cas échéant, à les interdire lorsque la menace pour les droits fondamentaux est trop importante. Les utilisations de l'IA par les autorités publiques dans les domaines du maintien de l'ordre, de l'immigration et de la sécurité nationale figurent parmi les cas d'utilisation les plus risqués, parce qu'elles ont un impact très important sur les droits fondamentaux, notamment la liberté de réunion et d'expression, le droit à un procès équitable, la présomption d'innocence, la non-discrimination et le droit de demander l'asile. Le travail des autorités de police, d'immigration et de sécurité régit l'accès à l'espace public, les résultats dans les secteurs de la justice pénale et de l'immigration, ainsi que divers autres domaines de la vie qui ont le plus d'impact sur les droits fondamentaux. En tant que telle, l'utilisation de l'IA par ces autorités exige la plus grande surveillance et la plus grande transparence, ainsi que les limites les plus claires afin de respecter les principes démocratiques fondamentaux.

- **L'utilisation de l'IA dans les domaines de la police, de la sécurité et de l'immigration amplifie la discrimination structurelle à l'encontre de communautés déjà marginalisées et sur-surveillées, telles que les personnes racialisées, les migrants et de nombreux autres groupes discriminés.** Des preuves de plus en plus nombreuses démontrent que ces systèmes d'IA renforcent la vigilance policière abusive et la surveillance, la détention et l'emprisonnement disproportionnés de groupes structurellement discriminés. Les données utilisées pour créer et faire fonctionner ces systèmes reflètent la discrimination historique, systémique, institutionnelle et sociétale. Cette discrimination est tellement fondamentale et enracinée que tous ces systèmes renforceront ces résultats. Les interdictions, la transparence publique et les cadres de responsabilité sont nécessaires pour prévenir les préjudices et donner aux gens les moyens de les contester.

- **L'utilisation de l'IA dans les domaines de la police, de la sécurité et de la migration invite le secteur privé à s'immiscer dans des aspects essentiels de la gouvernance publique,** ce qui nécessite une surveillance et des limites juridiques encore plus strictes afin de garantir le respect des droits des citoyens. Étant donné que ces domaines relèvent de la compétence des pouvoirs publics, il est essentiel que la loi sur l'IA garantisse que le développement de l'IA par le secteur privé dans ces domaines fasse l'objet d'une transparence publique. Les systèmes d'IA, lorsqu'ils sont déployés dans les domaines du maintien de l'ordre, de l'immigration et de la sécurité nationale, doivent avant tout

répondre des normes en matière de droits fondamentaux et de l'État de droit, plutôt que d'être motivés par le profit. À ce titre, des garanties, une surveillance et des limites juridiques doivent être appliquées.

Des recommandations détaillées sur la manière dont la loi européenne sur l'IA doit être modifiée dans ces domaines figurent en annexe de la présente déclaration.

Signé,

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

Annexe - Recommandations détaillées

Afin de répondre aux demandes formulées dans la déclaration de la société civile "Responsables politiques de l'UE - réglementez les technologies policières", la loi européenne sur l'IA doit

1. Inclure des limites juridiques interdisant l'utilisation de l'IA pour des usages qui présentent un risque inacceptable pour les droits fondamentaux. Cela inclut une interdiction légale des différentes formes de surveillance biométrique, de la police prédictive et des utilisations préjudiciables de l'IA dans le contexte migratoire.

- Une interdiction totale de l'identification biométrique en temps réel et à distance dans les espaces accessibles au public (y compris les zones frontalières et autour des centres de détention de migrants), par tous les acteurs, sans exception (article 5, paragraphe 1, point d)) ;
- Une définition large des espaces accessibles au public, qui inclut les zones frontalières (rejeter le considérant 9, mandat du Conseil) ;
- L'interdiction de toutes les formes de systèmes de prédiction et de profilage dans le cadre de l'application de la loi et de la justice pénale (y compris les systèmes qui se concentrent sur des individus, des groupes, des lieux ou des zones et les ciblent) (article 5, paragraphe 1, point d), du mandat du Parlement européen) ;
- Interdiction de l'utilisation de l'IA dans les contextes migratoires pour évaluer les risques individuels et établir des profils sur la base de données personnelles et sensibles, et des systèmes d'analyse prédictive lorsqu'ils sont utilisés pour interdire, freiner et prévenir les migrations ;
- L'interdiction d'utiliser des systèmes de catégorisation biométrique, tels que les systèmes de profilage racial, politique ou de genre (article 5, paragraphe 1, point b bis), du mandat du Parlement européen) ; et l'interdiction d'utiliser des systèmes de détection comportementale automatisés dans les espaces accessibles au public ;
- L'interdiction d'utiliser des systèmes dits de "reconnaissance des émotions" pour déduire ou prédire les émotions et les états mentaux des personnes.Prohibit export of systems which are banned in the EU (article 2(1) of the European Parliament mandate).

2. Assurer la transparence et le contrôle publics lorsque la police, les services d'immigration et les agences de sécurité nationale utilisent l'IA "à haut risque", en imposant à ces autorités le même devoir d'enregistrer les utilisations à haut risque dans la base de données de l'UE sur l'IA.

- Maintenir l'obligation de s'enregistrer et d'enregistrer leur utilisation des systèmes d'IA à haut risque dans la base de données publique (rejeter l'exemption prévue à l'article 29, paragraphe 5, et à l'article 51, paragraphe 2) ;
- Exiger une transparence égale pour les fournisseurs de systèmes à haut risque déployés dans les domaines du maintien de l'ordre et de la migration, afin qu'ils enregistrent leurs produits dans la base de données publique (rejeter l'exemption prévue à l'article 51, paragraphe 1, du mandat du Conseil) ;

- Veiller à ce que la notification des essais de systèmes d'IA dans des bacs à sable soit transparente et à ce qu'il n'y ait pas d'exemption générale pour le traitement de "données opérationnelles sensibles", qui est un terme vague et large (rejeter les exemptions prévues à l'article 53, paragraphe 5, et à l'article 54, paragraphe 1, point j)) ;
- Garantir l'obligation d'enregistrer les essais en conditions réelles dans la base de données de l'UE (rejeter les exemptions prévues à l'article 54 bis, paragraphe 4, point c), et à l'article 54 bis, paragraphe 4, point j), du mandat du Conseil) ;
- Veiller à ce que des mesures de surveillance humaine rigoureuses soient appliquées de manière cohérente dans l'ensemble de la loi, en particulier pour les systèmes d'IA à haut risque utilisés par ces autorités (rejeter les exemptions prévues à l'article 14, paragraphe 5, et à l'article 29, paragraphe 4).

3. Veiller à ce que la loi sur l'IA réglemente correctement les utilisations de l'IA dans les domaines de la police, de l'immigration et de la sécurité nationale qui présentent un risque pour les droits de l'homme, notamment en dressant une liste exhaustive de l'IA dans le contrôle de l'immigration et en veillant à ce que la sécurité nationale ne soit pas exclue du champ d'application de la loi.

- Rejeter l'ajout par le Conseil d'une exemption générale de la loi sur l'IA pour les systèmes d'IA développés ou utilisés à des fins de sécurité nationale (article 2, paragraphe 3, du mandat du Conseil) ;
- Rejeter l'exemption générale pour les systèmes à haut risque qui font partie des bases de données sur les migrations (par exemple EURODAC, VIS, SIS) énumérées à l'annexe IX (conformément à l'article 83, paragraphe 1, du mandat du PE) ;
- Veiller à ce que la liste des systèmes à haut risque figurant à l'annexe III comprenne tous les systèmes d'IA potentiellement dangereux :
    - ◦ les systèmes d'identification biométrique, tels que les scanners portables d'images faciales, d'empreintes digitales ou de paume, la technologie d'identification vocale ou de l'iris, dont l'utilisation peut conduire à la discrimination, à la surveillance et à la coercition de la personne soumise (annexe III, point 1 du mandat du PE).
    - ◦ Les systèmes d'IA utilisés pour les activités de gestion des frontières, tels que les drones ou les caméras thermiques, qui peuvent conduire à l'interception violente des demandeurs d'asile et à leur refoulement (annexe III, point 7 (d a) du mandat du PE) ;
    - ◦ les systèmes d'IA permettant de prévoir les mouvements migratoires et les franchissements de frontières, dont l'utilisation peut éclairer les politiques punitives (annexe III, point 7 (d b) du mandat du PE).