An die EU-Rechtsgeber*innen: Regulieren Sie Polizeitechnologie!

Die Zivilgesellschaft fordert die EU auf, in der Verordnung über Künstliche Intelligenz Überwachungstechnologie Grenzen zu setzen

KI-Systeme werden zunehmend von Strafverfolgungs-, Migrationskontroll- und nationalen Sicherheitsbehörden eingesetzt. Die Verordnung über künstliche Intelligenz (KI-VO) muss deshalb dringend Menschen vor Rechtsverletzungen schützen und den Behörden für den Einsatz von KI rechtliche Grenzen setzen.

In Europa werden wie auf der ganzen Welt KI-Systeme entwickelt und eingesetzt, die schädliche und diskriminierende Formen der staatlichen Überwachung ermöglichen. In der Strafverfolgung werden KI-Technologien übermäßig dazu genutzt, bereits marginalisierte Gemeinschaften weiter in ihren Rechten zu beschneiden. Indem ihre biometrischen Daten zu ihrer Identifizierung, Erkennung und Kategorisierung verwendet werden und sie zum Objekt von prädiktiven Systemen zur Entscheidungsfindung und Ressourcenzuweisung werden, werden nicht nur ihre Rechts- und Verfahrensrechte untergraben. Zudem wird Massenüberwachung eingeführt.

Wenn KI-Systeme bei der Strafverfolgung, zur Überwachung der Sicherheit und in der Migrationskontrolle eingesetzt werden, wächst das Machtungleichgewicht zwischen den überwachenden Behörden und den Überwachten. Dadurch nimmt auch die Gefahr zu, dass Verstöße gegen die Grundrechte und die Rechtsstaatlichkeit stattfinden.

Durch diese Erklärung fordern wir mit Nachdruck, dass der Einsatz von KI-Systemen durch Strafverfolgungs-, Migrationskontroll- und nationale Sicherheitsbehörden in ganz Europa reguliert werden muss.

Wir weisen besonders auf die Gefahren hin, die der Einsatz solcher Technologien durch Behörden für die Versammlungsfreiheit, generelle Freiheitsrechte, das Recht auf Asyl, die Privatsphäre und den Datenschutz oder auch das Recht auf sozialen Schutz und Nichtdiskriminierung mit sich bringt.

Zivilgesellschaftliche Organisationen fordern eine KI-VO, die eine unkontrollierte diskriminierende und massenhafte Überwachung verhindert. Die KI-VO muss eine Reihe von Voraussetzungen erfüllen, um die Menschenrechte zu schützen und Schäden durch den Einsatz von KI bei der Polizeiarbeit, der Migrationskontrolle und der nationalen Sicherheit zu verhindern:

1. **Das Gesetz muss KI-Anwendungen verbieten, die ein unannehmbares Risiko für die Grundrechte darstellen.** Dazu gehört ein gesetzliches Verbot verschiedener Formen von biometrischer Überwachung, vorausschauender Polizeiarbeit und des schädlichen Gebrauchs von KI bei der Migrationskontrolle.

2. **Der Einsatz „risikoreicher“ KI durch Polizei, Migrationsbehörden und nationale Sicherheitsbehörden muss transparent sein und öffentlich kontrolliert werden.** Eine wesentliche Maßnahme dazu wäre, all diese Behörden dazu zu verpflichten, risikoreiche Anwendungen in der EU-KI-Datenbank zu registrieren.
3. **Die KI-VO muss den Einsatz von KI in den Bereichen Polizei, Migration und nationale Sicherheit hinreichend regeln, wenn dieser Einsatz ein Risiko für die Menschenrechte darstellt.** Dies betrifft insbesondere sämtliche in der Migrationskontrolle eingesetzte KI. Außerdem darf in der KI-VO die nationale Sicherheit nicht vom Anwendungsbereich ausgeschlossen werden.

Warum die KI-VO den Einsatz von KI in den Bereichen Strafverfolgung, Migration und nationale Sicherheit regulieren muss:

- **Die Kontrolle staatlicher und polizeilicher Macht ist für das Funktionieren einer demokratischen, rechtstaatlichen Gesellschaft unerlässlich.** Die KI-VO hat den Zweck, risikoreiche KI-Anwendungen zu identifizieren, sie zu regulieren und sie gegebenenfalls zu verbieten, wenn von ihnen eine zu große Gefahr für die Grundrechte ausgeht. Der Einsatz von KI durch staatliche Behörden in den Bereichen Polizei, Migration und nationale Sicherheit gehört zu den risikoreichsten Anwendungsfällen, da dieser Einsatz Grundrechte wie Versammlungs- und Meinungsfreiheit, das Recht auf ein faires Verfahren, die Unschuldsvermutung, das Diskriminierungsverbot und das Recht auf Asyl am stärksten beeinträchtigt. Die Arbeit der Polizei-, Migrations- und Sicherheitsbehörden regelt den Zugang zu öffentlichen Räumen und wirkt sich entscheidend in den Bereichen Strafjustiz und Migration sowie verschiedenen anderen Lebensbereichen aus, in denen am stärksten die Grundrechte betroffen sind. Der Einsatz von Künstlicher Intelligenz durch diese Behörden erfordert daher ein Höchstmaß an Kontrolle und Transparenz und muss klar gesetzlich geregelt werden, um die grundlegenden demokratischen Prinzipien zu wahren.

- Der Einsatz von Künstlicher Intelligenz in den Bereichen Polizei, Sicherheit und Migration verstärkt die strukturelle Diskriminierung bereits marginalisierter und übermäßig überwachter Gemeinschaften, zum Beispiel von Rassismus betroffene Menschen oder Migrant*innen. Es häufen sich Beweise dafür, dass solche KI-Systeme eine unverhältnismäßige Polizeiarbeit, eine übertriebene Überwachung und die Inhaftierung von strukturell diskriminierten Gruppen verstärken. Die Daten, die zum Aufbau und zum Betrieb solcher Systeme verwendet werden, spiegeln eine historische, systemische, institutionelle und gesellschaftliche Diskriminierung wider. Alle im Dienst dieser tief verwurzelten Diskriminierung eingesetzten KI-Systeme tragen dazu bei, dass sie sich weiter in der Gesellschaft festsetzt. Verbote, öffentliche Transparenz und ein Rahmen für eine Rechenschaftspflicht sind notwendig, damit Schäden verhindert werden und die betroffenen Menschen in die Lage versetzt werden, sich dagegen zu wehren.

- **Der Einsatz von KI in den Bereichen Polizei, Sicherheit und Migration lädt den privaten Sektor dazu ein, manche der wichtigsten Funktionen der öffentlichen**

Verwaltung in seinem Sinne zu beeinflussen. Um die Rechte der Bevölkerung zu wahren, sind deshalb eine noch stärkere Aufsicht und rechtliche Grenzen notwendig. Da es sich bei diesen Bereichen um staatliche Aufgaben handelt, muss die KI-VO sicherstellen, dass vom privaten Sektor entwickelte und in diesen Bereichen eingesetzte KI-Systeme öffentlich transparent sind. Ihr Einsatz darf nicht durch die Profitinteressen der Anbieter bestimmt werden und muss vor allem den Standards folgen, die durch das Grundrecht und die Rechtsstaatlichkeit vorgegeben sind. Um diese rechtlichen Grenzen zu schützen, müssen daher geeignete Schutzmaßnahmen und Aufsichtsmechanismen eingeführt werden.

Detaillierte Empfehlungen, wie die KI-VO in den genannten Bereichen geändert werden muss, finden Sie im Anhang zu dieser Erklärung.

Unterzeichnet von:

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

Anhang - Detaillierte Empfehlungen

Um die in der zivilgesellschaftlichen Erklärung „An die EU-Rechtsgeber*innen: Regulieren Sie Polizeitechnologie!“ aufgeführten Forderungen zu erfüllen, muss die KI-VO:

1. **KI-Anwendungen verbieten, die ein unannehmbares Risiko für die Grundrechte darstellen.** Dazu gehört ein gesetzliches Verbot verschiedener Formen von biometrischer Überwachung, vorausschauender Polizeiarbeit und des schädlichen Gebrauchs von KI bei der Migrationskontrolle.
    - Eine ferngesteuerte biometrische Identifizierung in öffentlich zugänglichen Räumen, ob in Echtzeit oder nachträglich, muss vollständig verboten werden (auch in Grenzgebieten und in der Nähe von Abschiebungshaftanstalten), ohne Ausnahme für alle Akteure (Artikel 5, Absatz 1, Buchstabe d).
    - Die Verordnung muss den Begriff „öffentlich zugängliche Räume“ weit gefasst definieren, so dass er Grenzgebiete einschließt (Ablehnung von Erwägungsgrund 9, Mandat des Europäischen Rates).
    - Alle Formen von prädiktiven und profilbildenden Systemen in der Strafverfolgung und der Strafjustiz (einschließlich Systeme, die sich auf Einzelpersonen, Gruppen und Orte oder Gebiete konzentrieren und auf diese abzielen) müssen verboten werden (Artikel 5, Absatz 1, Buchstabe da, Mandat des Europäischen Parlaments).
    - KI im Migrationskontext muss verboten werden, wenn sie dazu eingesetzt wird, individuelle Risikobewertungen durchzuführen und auf der Grundlage personenbezogener und sensibler Daten Profile zu erstellen. Außerdem müssen prädiktive Analysesysteme verboten werden, wenn sie zum Unterbinden, Begrenzen und Verhindern von Migration eingesetzt werden.
    - Zudem muss der Einsatz biometrischer Kategorisierungssysteme verboten werden, also Systeme zur Erstellung von Rassen-, politischen oder Geschlechterprofilen (Artikel 5, Absatz 1, Buchstabe ba, Mandat des EU-

Parlaments), ebenso die Verwendung automatisierter Systeme zur Verhaltenserkennung in öffentlich zugänglichen Räumen.
- Verboten werden muss auch der Einsatz sogenannter „Emotionserkennungssysteme“, die Rückschlüsse auf Gefühle und den Geisteszustand von Menschen ziehen oder diese vorhersagen.
- Der Ausfuhr von Systemen, die in der EU verboten sind, muss unterbunden werden (Artikel 2, Absatz 1, Mandat des EU-Parlaments).

2. **Transparenz für den Einsatz „risikoreicher“ KI durch Polizei, Migrationsbehörden und nationale Sicherheitsbehörden herstellen und eine öffentliche Kontrolle festlegen.** Eine Maßnahme dazu wäre, all diese Behörden dazu zu verpflichten, risikoreiche Anwendungen in der EU-KI-Datenbank zu registrieren.

   - Die Verpflichtung, eigenständig den Einsatz von KI-Hochrisikosystemen in der öffentlichen Datenbank zu registrieren, muss aufrechterhalten werden (Ablehnung der in Artikel 29, Absatz 5, und Artikel 51, Absatz 2 vorgesehenen Ausnahmen).
   - Es müssen für alle Anbieter von Hochrisikosystemen, die in den Bereichen Strafverfolgung und Migration eingesetzt werden, die gleichen Transparenzverpflichtungen gelten. Im Zuge dessen müssen sie ihre Produkte in der öffentlichen Datenbank registrieren (Ablehnung der in Artikel 51, Absatz 1, Mandat des EU-Rats vorgesehenen Ausnahme).
   - Es muss sichergestellt werden, dass die Berichterstattung über die Erprobung von KI-Systemen in Reallaboren transparent ist und keine pauschale Ausnahme für die Verarbeitung von „sensiblen operativen Daten“ vorsieht, was ein zu vager und weit gefasster Begriff ist (Ablehnung der in Artikel 53, Absatz 5, und Artikel 54, Absatz 1, Buchstabe j vorgesehenen Ausnahmen).
   - Es muss die Verpflichtung gelten, Tests unter realen Bedingungen in der EU-Datenbank zu registrieren (Ablehnung der in Artikel 54a, Absatz 4, Buchstabe c, und Artikel 54a, Absatz 4, Buchstabe j, Mandat des EU-Rats vorgesehenen Ausnahmen).
   - Es muss sichergestellt werden, dass im gesamten Rechtsakt durchgängig strenge menschliche Aufsichtsmaßnahmen durchgeführt werden, insbesondere für KI-Hochrisikosysteme, die von den genannten Behörden verwendet werden (Ablehnung der in Artikel 14, Absatz 5, und Artikel 29, Absatz 4 vorgesehenen Ausnahmen).

3. **Den Einsatz von KI in den Bereichen Polizei, Migration und nationale Sicherheit hinreichend regeln, wenn dieser Einsatz ein Risiko für die Menschenrechte darstellt.** Dies betrifft insbesondere sämtliche in der Migrationskontrolle eingesetzte KI. Außerdem darf in der KI-VO die nationale Sicherheit nicht vom Anwendungsbereich ausgeschlossen werden.

   - Die vom Rat in die KI-VO eingefügte pauschale Ausnahme von KI-Systemen, die für Zwecke der nationalen Sicherheit entwickelt oder verwendet werden, ist abzulehnen (Artikel 2, Absatz 3, Mandat des EU-Rats).

Ebenso abzulehnen ist die pauschale Ausnahme für Hochrisikosysteme, die Teil von Migrationsdatenbanken (z.B. EURODAC, VIS, SIS) und in Anhang IX aufgeführt sind (gemäß Artikel 83, Absatz 1, Mandat des EU-Parlaments).

- Es muss sichergestellt werden, dass die Liste der Hochrisikosysteme in Anhang III alle potenziell gefährlichen KI-Systeme enthält:
    - Biometrische Identifizierungssysteme wie tragbare Gesichts-, Fingerabdruck- oder Handflächenscanner, Stimm- oder Iris-Identifizierungstechnologien, deren Verwendung zu Diskriminierung, Überwachung und Nötigung der unterworfenen Person führen kann (Anhang III, Punkt 1, Mandat des EU-Parlaments)
    - KI-Systeme, die für Grenzschutzmaßnahmen eingesetzt werden, wie unbemannte Drohnen oder Wärmebildkameras, die zum gewaltsamen Abfangen von Asylbewerbern und deren Zurückdrängung führen können (Anhang III, Nummer 7, Buchstabe d a, Mandat des EU-Parlaments)
    - KI-Systeme zur Vorhersage von Migrationsbewegungen und Grenzübertritten, deren Einsatz als Grundlage für Strafmaßnahmen dienen kann (Anhang III, Punkt 7 (d b), Mandat des EU-Parlaments)