

Antrag

der Abgeordneten Donata Vogtschmidt, Clara Bünger, Anne-Mieke Bremer, Katrin Fey, Dr. Gregor Gysi, Luke Hoß, Ferat Koçak, Jan Köstering, Sonja Lemke, Bodo Ramelow, David Schliesing, Aaron Valent, Christin Willnat und der Fraktion Die Linke

Für öffentliche Räume ohne automatisierte biometrische Erkennungssysteme

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Mit der im August 2024 in Kraft getretenen KI-Verordnung (KI-VO, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689) wurde eine umfassende Rechtsgrundlage für den Einsatz von künstlicher Intelligenz (KI) geschaffen. Die Regulierung lässt jedoch Lücken offen, die den Freiheitsrechten und dem Schutz der Menschenwürde entgegenstehen und Voraussetzungen für einen Ausbau der Massenüberwachung im öffentlichen Raum innerhalb der EU schaffen. Insbesondere fehlt ein klares Verbot biometrischer Fernidentifizierung im öffentlichen Raum. Dies betrifft zum Beispiel die automatisierte biometrische Durchkämmung von Daten im Internet oder in Aufzeichnungen von Videokameras.

Zwar besteht grundsätzlich ein Verbot biometrischer Echtzeit-Identifikation im öffentlichen Raum, jedoch wird dieses durch umfangreiche Ausnahmen weitgehend entkräftet. So wird beispielsweise der Einsatz der Erkennung mittels KI in Echtzeit zur Lokalisierung oder Identifizierung einer Person gestattet, die lediglich im bloßen Verdacht steht, eine Straftat begangen zu haben (Artikel 5 Absatz 1 Buchstabe d KI-VO). Für biometrische Fernidentifizierung zur erstmaligen Identifizierung einer tatverdächtigen Person ist laut Artikel 26, Absatz 10 KI-VO nicht einmal nachträglich (ex post) eine behördliche Genehmigung notwendig, sofern die biometrische Identifizierung nicht in Echtzeit, sondern nachträglich (retrograd) durchgeführt wird. Zusätzlicher Spielraum für Massenüberwachung eröffnet sich, weil nicht klar definiert ist, wo die Grenze zwischen „Echtzeit“ und „nachträglich“ verläuft.

Ein von der Nichtregierungsorganisation AlgorithmWatch beauftragtes Gutachten zur Praxistauglichkeit biometrischer Fernidentifizierungssysteme kam im September 2025 zu dem Befund, dass ohne das Anlegen einer Datenbank, es technisch nicht praktikabel sei, einen automatisierten biometrischen Abgleich von Bildern aus dem Internet durchzuführen. Letzteres ist laut Artikel 5, Absatz 1 Buchstabe e KI-VO verboten. Ein Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages vom Januar 2026 (www.die-linke-thueringen.de/fileadmin/DonataVogtschmidt/Dokumente/2026/260-122_WD_Gutachten_Biometrischer_Internetabgleich_KI_Verordnung.pdf) bestätigt die technische Bewertung weitgehend, verweist aber auf einige Szenarien, die das Anlegen von Datenbanken durchaus gestatten könnten. So beschränkt sich das Verbot lediglich auf Gesichtserkennung (zur biometrischen Fernidentifizierung können auch

Stimmen, Bewegungsabläufe, Fingerabdrücke usw. genutzt werden) und das Verbot gilt nicht, sobald die Datenbank im Rahmen einer gezielten Ermittlung oder durch ein nicht-KI-basiertes System erstellt wird, oder wenn die biometrische Fernidentifizierung im Rahmen von Maßnahmen der nationalen Sicherheit (zum Beispiel Terrorabwehr) oder im Kontext von Militär und Verteidigung durchgeführt wird. In diesen Fällen gibt es im Rahmen der KI-VO keinerlei Beschränkungen, weil diese Bereiche von der KI-VO vollständig ausgenommen sind.

Nach Ansicht der Antragstellenden bestehen demnach umfangreiche Regelungslücken in der KI-VO, die eine massenhafte biometrische Fernidentifizierung im öffentlichen Raum als einen unverhältnismäßigen Eingriff in die Grundrechte ermöglichen und damit auch einen Markt für derartige KI-Werkzeuge eröffnen. Deshalb sollten die Lücken sowohl bei den Verhandlungen zu Änderungen an der KI-VO im Rahmen des Digital-Omnibusses (2025/0360(COD)) als auch durch nationalstaatliche Auslegungsspielräume, etwa durch Erlass von Verwaltungsvorschriften, geschlossen werden. Weiterhin geht eine Gefahr für die Menschenrechte von den bereits verbreiteten KI-Werkzeugen zur biometrischen Fernidentifizierung wie PimEyes aus, hinsichtlich des Rechts auf informationelle Selbstbestimmung beziehungsweise Recht auf den Schutz personenbezogener Daten gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG und Artikel 7 und Artikel 8 GRCh. Ferner wird durch die Verwendung dieser KI-Werkzeuge gegen europäisches Sekundärrecht, konkret die DSGVO (<https://noyb.eu/de/20-mio-eu-geldstrafe-fuer-clearview-ai-italien>) und auch Artikel 5 Absatz 1 Buchstabe e KI-VO verstoßen (<https://netzpolitik.org/2024/sicherheitspaket-eine-biometrische-datenbank-um-alle-zu-finden/>). Die zunehmende Verbreitung derartiger KI-Werkzeuge (<https://netzpolitik.org/2025/behoerden-schauen-zu-ki-suche-fuer-gesichter-breitet-sich-ungehindert-aus/>) offenbart nach Ansicht der Antragstellenden ein schwerwiegendes Versagen der zuständigen Aufsichtsbehörden bei der Durchsetzung geltenden EU-Rechts.

Derzeit ist ein deutsches Umsetzungsgesetz der KI-VO in Arbeit, das nach Kabinettsbeschluss jedoch keinerlei Maßnahmen zur Beschränkung automatisierter biometrischer Fernidentifizierung enthält (<https://bmds.bund.de/aktuelles/pressemitteilungen/detail/kabinetts-beschliesst-schlanke-ki-aufsicht-in-deutschland>). Stattdessen wurde im Sommer 2025 ein Referentenentwurf des Bundesinnenministeriums bekannt, der weitreichende Befugnisse zur automatisierten biometrischen Fernidentifizierung auf Bundesebene eröffnen würde (<https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/>). Weiterhin wurden 2025 Pläne der Innenminister bekannt, die die mögliche Einführung von Gesichtserkennung in Fußballstadien zum Gegenstand hatten (www.tagesschau.de/inland/innenministerkonferenz-142.html). Auf Landesebene gab es bereits diverse Vorstöße (<https://netzpolitik.org/2024/sachsen-polizei-gibt-zu-in-21-verfahren-gesichtserkennung-eingesetzt-zu-haben/>), wobei die erstmalige reguläre Einführung automatisierter biometrischer Fernidentifizierung im Bahnhofsbereich von Frankfurt am Main im Sommer 2025 einen Dammbruch darstellte (<https://netzpolitik.org/2025/als-erstes-bundesland-hessen-setzt-live-gesichtserkennung-ein/>).

Eine erlaubte biometrische Fernidentifizierung im öffentlichen Raum wäre das Ende des Rechts auf Anonymität im öffentlichen Raum. Hierdurch würde das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG verletzt. Die KI-VO beschreibt in Erwägungsgrund 32, welche Gefahren für Freiheitsrechte der Einsatz von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung birgt: Ein „Gefühl der ständigen Überwachung“, die Hinderung an der Ausübung von Grundrechten wie der Versammlungsfreiheit sowie die potenziell diskriminierende Wirkung von KI-Systemen anhand Merkmalen wie das Alter, die ethnische Herkunft, die Rasse, das Geschlecht oder Behinderungen. Auch die biometrischen Daten anderer (unbeteiligter) Personen können erfasst werden. Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss (EDSB und EDSA;

www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf), der ehemalige UN-Hochkommissar für Menschenrechte (www.ohchr.org/en/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469), der Wissenschaftliche Dienst des Europäischen Parlaments (EPRS) sowie über 200 Nichtregierungsorganisationen in Europa und weltweit (www.accessnow.org/campaign/ban-biometric-surveillance/) warnen in ihren Stellungnahmen vor den Folgen, die der Einsatz der biometrischen Fernidentifizierung für die Grundrechte haben kann.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. von den in Artikel 5 Absatz 5 und Artikel 26 Absatz 10 der KI-Verordnung vorgesehenen Klauseln Gebrauch zu machen und einen Gesetzentwurf vorzulegen, der ein konsequentes Verbot des Einsatzes automatisierter biometrischer Fernidentifikations- und Kategorisierungssysteme sowie algorithmengesteuerter Emotionserkennungssysteme im öffentlichen Raum umfasst;
2. sich bei den Verhandlungen zur Änderung der KI-Verordnung im Rahmen des Digital-Omnibusses (2025/0360(COD)) für ein EU-weites Moratorium für den Einsatz von KI-Systemen zur automatisierten Erkennung biometrischer Merkmale (in Echtzeit sowie retrograd) in öffentlich zugänglichen Räumen einzusetzen;
3. zu prüfen, welche Maßnahmen ergriffen werden können, damit die Inverkehrbringung und der Gebrauch von Werkzeugen wie PimEyes, ClearviewAI, ProFaceFinder, TrustPics oder FaceCheck.ID zur biometrischen Identifizierung konsequent geahndet und unterbunden werden kann.

Berlin, den 17. März 2026

Heidi Reichinnek, Sören Pellmann und Fraktion

Begründung

Den Antragstellenden ist bewusst, dass der öffentliche Raum den Behörden im Rahmen ihrer Tätigkeit grundsätzlich zugänglich sein muss. Dafür gibt es bereits weitreichende Befugnisse, und auch die Digitalisierung der Polizeiarbeit und Verknüpfung von Datenbeständen, kann eine sinnvolle Maßnahme sein, um die behördliche Arbeit zu verbessern. Voraussetzung hierfür ist allerdings, dass dadurch nicht gegen geltendes Recht, insbesondere die Grundrechte Betroffener verstoßen wird. Eine Automatisierung der biometrischen Analyse des öffentlichen Raums, aufgezeichnet durch Videokameras oder im Internet, potenziert jedoch die Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung enorm, sodass keine Verhältnismäßigkeit zwischen diesem Eingriff und dem Rechtfertigungsgrund hierfür (Wahrung der öffentlichen Sicherheit und Ordnung) besteht. Letztlich entsteht hierdurch das Potential für eine totale Überwachung des öffentlichen Raumes, was im Gefühl resultiert, ständig beobachtet zu werden. Hierdurch werden Menschen davon abgehalten, Grundrechte wie jenes der Versammlungsfreiheit wahrzunehmen, opportunistisches Verhalten wird aufgezwungen und es entstehen Hemmungen, sich überhaupt in der Öffentlichkeit zu zeigen oder zu äußern (Chilling Effect).

Hinzu kommt, dass zunächst auch alle unbeteiligten Personen von Scans betroffen sind beziehungsweise beobachtet werden. Davon abgesehen, dass sich daraus ein großes Missbrauchspotential ergibt, können sich aufgrund der großen Anzahl Unbeteiligter falschpositive Treffer auch bei geringen Fehlerraten schnell summieren und mit möglichen Ermittlungserfolgen ins Missverhältnis geraten, wie dies die testweise Überwachung am Bahnhof Südkreuz im Jahr 2017 zeigte (www.sueddeutsche.de/projekte/artikel/digital/falsch-positive-machen-prognose-

algorithmen-zum-problem-e716375/). Weiterhin wurde von Fachleuten vielfach darauf hingewiesen, dass Gesichtserkennung bestimmte Personengruppen diskriminiert. Zum Beispiel werden Frauen und Menschen mit dunkler Hautfarbe schlechter als andere Menschen bei biometrischen Analysen ihres Gesichts erkannt, was die Wahrscheinlichkeit von Falschpositiven hierbei vergrößern kann. Zudem kann Diskriminierung durch die Kontextualisierung mit einem prekären Umfeld entstehen, zum Beispiel bei Asylsuchenden, wenn sie sich den Video- oder Internetbildern zufolge in einem bestimmten Stadtteil aufhalten. Weiterhin deutet eine aktuelle Studie darauf hin, dass mit Gesichtserkennung durch KI bereits ohne weitere Informationen Persönlichkeitsmerkmale prognostiziert werden können (www.heise.de/news/Gesichtserkennung-Wie-KI-darueber-entscheiden-koennte-wer-eingestellt-wird-11074078.html).

Der Ausbau biometrischer Fernidentifizierung im öffentlichen Raum entspricht dem Gegenteil dessen, was ein gesundes, menschwürdiges gesellschaftliches Leben und eine Demokratie ausmacht. Die Einwanderungsbehörde ICE in den USA demonstriert aktuell eindrucksvoll, wie schädlich sich die Anwendung automatisierter biometrischer Fernidentifizierung auf das gesellschaftliche Klima und die Freiheitsrechte auswirkt. Die Behörde setzt zur biometrischen Fernidentifizierung mit Bildern aus dem Internet das KI-Werkzeug ClearviewAI ein und treibt die Überwachung durch Verknüpfung mit behördlichen Datenbanken durch die mobile App „Mobile Fortify“ und Software von Palantir (ImmigrationOS) auf die Spitze (www.derstandard.de/story/3000000294353/us-einwanderungsbehoerde-ice-benutzt-gesichtserkennung-auf-offener-strasse; www.finanzen.net/nachricht/aktien/ice-debatte-kontroverse-um-palantir-aktie-ceo-karp-verteidigt-ice-zusammenarbeit-und-us-behoerdenprojekte-00-15465069). Im Fokus stehen dabei nicht nur Migrant*innen, sondern auch bereits Protestierende.

Auch außerhalb behördlicher Anwendung biometrischer Fernidentifizierung muss gesetzlich konsequent gehandelt werden, um die Verbreitung von KI-Werkzeugen zu stoppen, die bereits nach geltender Gesetzeslage rechtswidrig sind. Erst im vergangenen Jahr wurde demonstriert, wie leicht sich smarte Brillen des Meta-Konzerns mit Werkzeugen wie PimEyes kombinieren lassen (www.br.de/nachrichten/netzwelt/metas-neue-ki-brille-ueberwachung-in-cool,UxocLSn). Umso dringender sind klare gesetzliche Stoppschilder, die eine derartige Entgleisung technologischer Entwicklung und deren Markteintritt verhindern.

Im Übrigen teilen die Antragstellenden, die in der Protokollerklärung der österreichischen Bundesregierung zur KI-VO geäußerte Kritik, dass die vorhandenen Regelungen über die Zulässigkeit und Hürden von Überwachungsmaßnahmen nicht in ein Marktregulierungsinstrument wie der KI-VO gehören. Denn in mehreren Artikeln verweist die KI-VO auf ein komplexes nationalstaatliches Regel-Ausnahmegeflecht und nationalstaatliche Kompetenzen der Mitgliedstaaten. Dies führt dazu, dass es absehbar keine EU-weit harmonisierte Rechtslage geben wird. Da der Grundrechtsschutz und insbesondere der Schutz der Menschenwürde jedoch in Deutschland höchsten Rang haben sollten, erscheint eine nationalstaatliche Zusatzregelung im beschriebenen Sinne unabdingbar.