ALGORITHM WATCH

/ Stellungnahme zur öffentlichen Anhörung des Ausschuss für Digitales am 15. Mai 2024

zur nationalen Umsetzung der KI-Verordnung

13. Mai 2024

Ko-Autor*innen: Kilian Vieth-Ditlmann, stv. Teamleiter Policy & Advocacy, AlgorithmWatch, Pia Sombetzki, Policy & Advocacy Managerin, AlgorithmWatch

Unsere Empfehlungen in Kürze

- Die nationale Aufsicht zügig koordinieren und aufbauen sowie unabhängig und schlank aufstellen; dabei vielfältige Expertise einbeziehen, einen KI-Beirat schaffen und ein effektives Beschwerdesystem aufsetzen.
- Verbote für den Einsatz biometrischer Fernidentifikationssysteme im öffentlich zugänglichen Raum ohne Einschränkungen beibehalten und im Durchführungsgesetz konkretisierend ausformulieren.
- Ein nationales KI-Transparenzregister für die öffentliche Hand aufbauen, das die begrenzten Informationen in der EU-Datenbank der Hochrisiko-KI-Systeme umfassend ergänzt.

Kontext

Der Rat der Europäischen Union beschließt die KI-Verordnung (KI-VO) voraussichtlich am 21. Mai 2024.[1] Die Umsetzungsfristen sind knapp, die Anforderungen komplex. Daher bereiten die EU-Mitgliedsstaaten bereits jetzt die Umsetzung der KI-Verordnung ins nationale Recht vor – so auch die deutsche Bundesregierung.

AlgorithmWatch hat die Entstehung der KI-Verordnung von Beginn an aktiv begleitet und zu dem Gesetzgebungsprozess Stellung genommen:

- Positionspapier nach Veröffentlichung des Kommissionsentwurfs (August 2021): https://algorithmwatch.org/en/eu-ai-act-consultation-submission-2021/
- Zivilgesellschaftliches Statement von über 120 Organisationen (November 2021): https://algorithmwatch.org/de/grundrechte-ins-zentrum-der-ki-verordnung/
- Begleitung des Verhandlungsprozesses (April 2022): https://algorithmwatch.org/de/forderungen-artificial-intelligence-act-eu/ &
- Reaktion auf den Entwurfbericht (Mai 2022): https://algorithmwatch.org/de/entwurfsbericht-zum-ai-act/
- Stellungnahme im Auschuss für Digitales des Bundestags (September 2022): https://algorithmwatch.org/de/stellungnahme-digitalausschuss-bundestag-aiact-2022/
- Empfehlungen zur Regulierung von GPAI in der KI-VO (September 2023): https://algorithmwatch.org/de/der-ai-act-und-general-purpose-ai/

Mit der Verabschiedung der KI-VO erkennt die EU an, dass der Einsatz von Künstlicher Intelligenz (KI) unsere Grundrechte, Rechtsstaatlichkeit und demokratische Prozesse gefährden kann. Und dass es Regulierung braucht, um sie zu schützen. Dazu gehört, dass besonders schädliche KI-Systeme, die mit unseren demokratischen Gesellschaften unvereinbar sind, verboten werden müssen.

Viele Aspekte sind am finalen Kompromiss dennoch nicht zufriedenstellend. Vor allem mit Blick auf den wirksamen Schutz von Grundrechten, bestehen eine Reihe von gravierenden Defiziten.[2]

Die kommende Um- und Durchsetzung der KI-VO auf EU-Ebene und in den Mitgliedsstaaten bietet die Chance, einige Lücken und Unklarheiten zu beseitigen und für mehr Grundrechtsschutz zu sorgen. Im Folgenden gehen wir auf die aus unserer Sicht wichtigsten Fragen zur nationalen Ausgestaltung der KI-VO ein.

---

[1] Alle Referenzen zur KI-Verordnung (KI-VO) in dieser Stellungnahme beziehen sich auf die finale Fassung P9_TA(2024)0138, die in Kürze endgültig verabschiedet werden soll.

[2] European Digital Rights (2024), EU's AI Act fails to set gold standard for human rights, https://algorithmwatch.org/en/ai-act-fails-to-set-gold-standard-for-human-rights/, sowie ProtectNotSurveil Coalition (2024), Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move, https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/, und European Center for Not-for-Profit Law (2024), Packed with loopholes: why the AI Act fails to protect civic space and the rule of law https://ecnl.org/news/packed-loopholes-why-ai-act-fails-protect-civic-space-and-rule-law

Fragen 1 und 8 werden zusammengefasst beantwortet:

1 Wie muss die nationale Aufsicht aufgestellt sein, um eine möglichst kohärente, schlanke Governance zu gewährleisten? Wie gelingt uns trotz sektoraler Zuständigkeiten und föderaler Aufteilung der vielzitierte One-Stop-Shop? Welche genauen Aufgaben sollte die Aufsicht übernehmen?

8 Welche gesetzlichen und politischen Maßnahmen sind notwendig, um die Zusammenarbeit zwischen den zuständigen Behörden in Deutschland und den Einrichtungen auf EU-Ebene (insbesondere AI Office, AI Board, Advisory Forum und Scientific Panel) schlagkräftig und effizient aufzustellen und wie lässt sich gewährleisten, dass zivilgesellschaftliche und interdisziplinäre wissenschaftliche Expertise bei der Auslegung, Konkretisierung, Umsetzung und Weiterentwicklung des AI Acts substantiell Berücksichtigung finden?

Nach Inkrafttreten der KI-Verordnung hat die Bundesregierung 12 Monate Zeit, die nationale Aufsicht in Deutschland aufzustellen. Es bleibt der Bundesregierung also nicht viel Zeit, diese komplexe Aufgabe zu erfüllen. Die Kommission hat außerdem bereits den Wunsch geäußert, dass die Mitgliedstaaten bis Ende dieses Jahres zuständige Stellen benennen, um die EU-weite Umsetzung der KI-Verordnung zügig und koordiniert voranzubringen. Die geregelten Verbote gelten bereits nach sechs Monaten. Damit beispielsweise Beschwerden bearbeitet werden können, wenn die neuen Regeln nicht eingehalten werden, braucht es daher auch möglichst früh auf nationaler Ebene ein koordiniertes und abgestimmtes Vorgehen.

Die Ressorts und die Behörden, die zentrale und insbesondere koordinierende Aufgaben übernehmen sollen, müssen sich daher dringend abstimmen. Ebenso sollten Vertreter*innen aus zivilgesellschaftlichen Organisationen und Verbraucherschützer*innen bereits jetzt in die aktuellen politischen Erwägungen einbezogen werden, damit konkrete Vorschläge dazu, wie nationale Aufsichtsstrukturen aussehen sollten, nicht erst spät im Prozess Gehör finden und potenziell weniger Wirkung entfalten können, als die von Unternehmen.

Zu den Aufsichtsstrukturen gibt die KI-Verordnung, insbesondere Artikel 70 der KI-Verordnung, lediglich grobe Leitlinien vor. Die Liste der Aufgaben und Befugnisse im Kontext der nationalen Aufsicht ist umfassend. Eine kohärente und klare Governance muss dabei dennoch das Ziel sein. Die zukünftige Aufsicht muss auf den Kompetenzen und Erfahrungen der bestehenden Marktüberwachung aufbauen; es darf keine Doppelstrukturen geben.

Wie bei der nationalen Digitale-Dienste-Koordinierungsstelle, **sollte allerdings sichergestellt werden, dass insbesondere auch Einzelpersonen, die eine Beschwerde einreichen wollen, eine zentrale Kontaktstelle aufsuchen können, die über das gesamte Verfahren ansprechbar bleibt.** Die Anforderungen daran, wie ein solches Verfahren ausgestaltet wird, sollten bereits im Gesetz grundsätzlich geregelt werden. Insbesondere sollten **Kriterien und Indikatoren festgelegt werden, die in Verwaltungsvorschriften näher definieren, woran sich ein effizientes und zugängliches Beschwerdeverfahren messen lässt.** Beispielsweise sollten Bearbeitungs- und Beantwortungsfristen festgelegt werden. Wir empfehlen, dass Beschwerdeführer*innen innerhalb von zehn Tagen über den Verfahrensablauf

umfassend informiert werden, u.a. auch darüber, welche weiteren Behörden in ihr Beschwerdeverfahren einbezogen wurden und von welcher Bearbeitungsdauer sie ausgehen können.[3]

Die KI-Verordnung sieht vor, dass die nationalen Regierungen drei Monate nach Inkrafttreten eine Liste von nationalen Behörden und öffentlichen Stellen veröffentlichen, deren Arbeit darauf zielt, die Grundrechte zu schützen, und diese der Europäischen Kommission mitteilt (Artikel 77 Abs. 1-2 KI-VO). **Bei Beschwerden zu Grundrechts- und Verbraucherschutzfragen muss sichergestellt sein, dass in den Beschwerdeverfahren die Expertise der Stellen einbezogen wird, die für die Beratung in solchen Fällen zuständig sind, wie etwa der Antidiskriminierungsstelle des Bundes.** Grundsätzlich sollte der Begriff der öffentlichen Stellen in Artikel 77 KI-VO weit ausgelegt werden, sodass er z.B. auch Menschenrechts-, Verbraucherschutz- und Umweltschutzorganisationen umfasst. Denn durch den Einsatz von Hochrisiko-KI-Systemen kann eine Vielfalt an Grundrechtsfragen entstehen, wofür wiederum eine Vielfalt an Grundrechts-Expertise aus so vielen Themenfeldern und Betroffenengruppen wie möglich verfügbar sein sollte.

Darüber hinaus haben diese Stellen konkrete Auskunftsrechte gegenüber KI-Entwickler*innen und KI-Anbietern. **Auch wenn die Mandate unterschiedlich ausfallen: Koordinierungsstelle, Marktüberwachungsbehörden und die Behörden, die für die Einhaltung der Grundrechte zuständig sind, müssen wirksam zusammenarbeiten, um wichtige Informationen zu bekommen.**

Um zu überprüfen, ob dieses komplexe Zusammenspiel zwischen Koordinierungsstelle, verschiedenen Behörden und Stellen angemessen funktioniert und die Koordinierungsstelle unabhängig agiert, sollte in einem Durchführungsgesetz festgeschrieben werden, dass **eine regelmäßige Evaluierung erfolgt**. **Es sollte außerdem evaluiert werden, wie teuer und wirksam eine Koordinierungsstelle im Vergleich mit einer zentralen Aufsichtsbehörde wäre. Mittelfristig empfehlen wir, die Kompetenzen in einer Digitalagentur zusammenzuführen.**

Zudem sollte ein KI-Beirat eingerichtet werden. Er würde dafür sorgen, dass zivilgesellschaftliche und interdisziplinäre wissenschaftliche Expertise sowie die Perspektive Betroffener in die Arbeit der Koordinierungsstelle einfließt, um die KI-Verordnung auszulegen, zu präzisieren und weiterzuentwickeln.

Solch ein KI-Beirat sollte die Koordinierungsstelle bei grundsätzlichen Fragen der Anwendung und Durchsetzung der KI-Verordnung beraten, allgemeine Empfehlungen zur effektiven und einheitlichen Durchführung der Verordnung vorschlagen und wissenschaftliche, technische und gesellschaftspolitische Fragestellungen an die Koordinierungsstelle herantragen.

Mitglieder eines KI-Beirats sollten das Recht haben, Fragen an die Koordinierungsstelle und zuständige Behörden zu stellen. Nur dann kann der Beirat gut informierte Einschätzungen abgeben. Darüber hinaus sollte die Unabhängigkeit des Beirats sichergestellt werden. Er muss sich eine eigene Geschäftsordnung geben können, die

[3] Vorschlag: zehn Tage s. Seite 7: https://www.baymevbm.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Sozialpolitik/2024/Downloads/Verfahrensleitfaden_NKS_FINAL-DEU.pdf

keiner Zustimmung eines Ministeriums oder einer Behörde bedarf. Er sollte darüber hinaus eigenständig Studien und Gutachten erstellen und beauftragen können. Die Arbeit des Beirats sollte auch finanziell unterstützt werden: Es bräuchte eine angemessen ausgestattete Geschäftsstelle sowie Aufwandsentschädigungen für Beirats-Mitglieder, die im Haushalt eingeplant werden. Die Sitzungen eines solchen Beirats sollten grundsätzlich öffentlich stattfinden und offen sein für die Einbeziehung weiterer zivilgesellschaftlicher Akteure und Verbraucherschützer, die nicht selbst als Mitglieder im Beirat vertreten sind.

Wie beim Digitale-Dienste-Gesetz sollte ein Forschungsetat eingeführt werden, der unabhängige Forschung durch Wissenschaft und Zivilgesellschaft unterstützt. Damit ein solcher Forschungsetat seine beabsichtigte Wirkung entfalten könnte, müsste er angemessen hoch ausfallen.

Fragen 3 und 17 werden zusammengefasst beantwortet:

3 Bei der biometrischen Fernidentifizierung im öffentlichen Raum eröffnet der AI Act die Möglichkeit des Nachschärfens der EU-weiten Mindeststandards. Sowohl für Echtzeit-Fernidentifizierungssysteme als auch für nachträgliche biometrische Fernidentifizierung im öffentlichen Raum können die Mitgliedstaaten in nationalen Rechtsgrundlagen auch strengere Regeln erlassen. Wie lässt sich diese Möglichkeit für einen umfassenderen Grundrechtsschutz nutzen, wo könnten entsprechende Vorschriften im nationalen Recht verankert werden und wie sollten diese – etwa im Hinblick auf ein ausnahmsloses Verbot – inhaltlich ausgestaltet sein?

17 Welche konkrete Regelung empfehlen Sie für die nationale Umsetzung des AI-Acts, um die im Koalitionsvertrag enthaltene Position eines Verbots biometrischer Fernidentifikationssysteme im öffentlichen Raum umzusetzen für die Sicherung der Grundrechte auf Privatsphäre sowie Datenschutz, auf Nichtdiskriminierung, Meinungs- und Informationsfreiheit, auf Versammlungs- und Vereinigungsfreiheit sowie auf Rechtsstaatlichkeit und inwiefern ergibt es mit Blick auf die genannten Grundrechte Sinn, dabei hinsichtlich Echtzeit und retrograder Fernidentifikation zu unterscheiden, insbesondere da die Unterscheidung zwischen Echtzeit und retrograd unklar ist?

Notwendigkeit eines Verbots biometrischer Fernidentifizierungssysteme

Die automatisierte Fernidentifizierung von Personen anhand von biometrischen Daten wie dem Gesicht, dem Gang oder der Stimme im öffentlich zugänglichen Raum ermöglicht eine **biometrische Massenüberwachung**. Sie steht im Kern mit Grundrechten wie der Privatsphäre, der informationellen Selbstbestimmung und der Versammlungsfreiheit sowie grundlegenden rechtsstaatlichen Prinzipien in Konflikt.

Das anlasslose, unterschiedslose oder stichprobenartige Beobachten, Verfolgen und Analysieren von Menschen anhand ihrer biometrischen Merkmale, insbesondere dem Gesicht, mit automatisierter Gesichtserkennung, schafft Überwachungsmöglichkeiten, die sonst zwar theoretisch, nicht aber praktisch realisierbar waren. Der Eingriff in

Grundrechte bekommt eine neue Qualität und ist mit einer herkömmlichen Videoüberwachung nicht zu vergleichen.[4] Video- und Fotoaufnahmen können automatisiert mit Bilddatenbanken abgeglichen, Personen über mehrere Videokameras hinweg automatisiert verfolgt und Verhaltens- und Bewegungsprofile erstellt werden.[5] Wo bisher einzelne Personenkontrollen möglich sind, können mit KI zehntausende oder hunderttausende Menschen erfasst werden.

Von einer automatisierten Gesichtserkennung werden wir alle wie wandelnde QR-Codes behandelt, können erkannt, gespeichert und abgeglichen werden, ohne es zu merken oder einen Einfluss darauf zu haben. **Die Anonymität im öffentlichen Raum wird dadurch ausgehebelt.** Die Erwartung, sich unerkannt zu bewegen, ist aber ein wichtiges Vorfeld-Grundrecht, ähnlich dem Datenschutz, um viele andere Grundrechte ausüben zu können. Wenn Menschen im öffentlichen Raum jederzeit identifiziert und überwacht werden können, verletzt dies nicht nur ihr Recht auf Privatsphäre, sondern hat auch eine abschreckende Wirkung (sog. „chilling effect"). Die Angst, erkannt und gespeichert zu werden, hält sie vom Wahrnehmen anderer Grundrechte wie der Meinungsäußerungs- oder Versammlungsfreiheit ab, zum Beispiel auf dem Weg zu einer gewerkschaftlichen Kundgebung oder einer Demonstration, zu Lokalen, die Hinweise auf ihre Religion, politische Gesinnung oder sexuelle Orientierung geben könnten oder zu einem Gespräch mit einer Journalist*in. All diese Grundrechte sind somit auch für die freie Meinungsbildung in einer demokratischen Gesellschaft zentral.

Biometrische Überwachung betrifft auch das Recht auf Gleichbehandlung. Grundsätzlich gilt zwar: Je besser die biometrische Fernidentifizierung funktioniert, desto gefährlicher wird sie. Dennoch besteht auch eine Gefahr der Diskriminierung in der bestehenden hohen Fehleranfälligkeit der Erkennungssysteme, insbesondere bei Personengruppen mit bestimmten Eigenschaften, die in Datensätzen unterrepräsentiert sind. Hinzu kommt die Gefahr der gezielten Diskriminierung, die genau den Zweck verfolgt, bestimmte Personen oder Gruppen anhand biometrischer Merkmale herauszufiltern. Für bereits benachteiligte oder von Diskriminierung betroffene Personen und Gruppen sowie für politische Aktivist*innen zeigen sich die Auswirkungen von biometrischer Massenüberwachung oft in verstärkter Form.

<u>Verbot biometrischer Echtzeit-Fernidentifizierung für Strafverfolgung und Polizei</u>

Angesichts des enormen Schädigungspotenzials für Grundrechte und Demokratie verbietet die KI-Verordnung die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen durch Polizei und Strafverfolgungsbehörden grundsätzlich. Artikel 5 Absatz 1 Buchstabe h untersagt „die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken" (vgl. auch Erwägungsgrund 32f). Die KI-VO stellt also klar:

[4] Martini (2022), Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, NVwZ – Extra 1-2/2022, S. 7ff: https://rsw.beck.de/docs/librariesprovider176/default-document-library/aufs%C3%A4tze-online/nvwz-extra-1-2-2022.pdf?sfvrsn=ea8c3b34_1

[5] Videoüberwachung ist in der Bundesrepublik weit verbreitet, sei es im ÖPNV, in Supermärkten oder in Innenstädten. „Schätzungen gehen von mehreren hunderttausend Überwachungskameras in Deutschland aus." – Hornung & Schindler (2017), Das biometrische Auge der Polizei, ZD 5/2017, S. 203: https://www.uni-kassel.de/fb07/index.php?eID=dumpFile&t=f&f=601&token=b3bed1274d80c7bfcd1def6b4464e72c636f3dc9

Ohne explizite gesetzliche Grundlage im nationalen Recht liegt keine Erlaubnis für den Einsatz biometrischer Erkennungssysteme im öffentlichen Raum für Zwecke der Strafverfolgung und Gefahrenabwehr vor.

Wenn nun über strengere Regeln oder Einschränkungen diskutiert wird, KI-basierte Gesichtserkennungssystem im öffentlichen Raum einzusetzen, impliziert das, dass sie grundsätzlich für Zwecke der Strafverfolgung und Gefahrenabwehr eingesetzt werden sollen. Das sollte auf Grund der ausgeführten Gefahren für Grundrechte und Rechtsstaatlichkeit aber ausnahmslos verhindert werden. Denn die Technologie ist in einer demokratischen Gesellschaft weder erforderlich noch verhältnismäßig. Daran ändern auch Öffnungsklauseln nichts. **Allein das Vorhandensein einer entsprechenden Infrastruktur im öffentlichen Raum bringt die erwähnten Chilling Effects mit sich**, da Betroffene nie wissen können, ob und wann die biometrische Überwachung stattfindet. Das spricht gegen ein Verbot mit Ausnahmen, denn es ermöglicht die grundlegende Infrastruktur und diese Ausnahmen, ob und wann biometrische Fernidentifizierung eingesetzt wird, sind für Menschen nicht nachvollziehbar.

Diese Gefahren hat die aktuelle Bundesregierung bereits anerkannt und in ihrem Koalitionsvertrag festgelegt, dass biometrische Erkennung im öffentlichen Raum europarechtlich auszuschließen und der Einsatz von biometrischer Erfassung zu Überwachungszwecken abzulehnen ist.[6] **Die in der KI-Verordnung formulierten Verbote sollten daher absolut ausgelegt werden und keine gesetzlichen Grundlagen geschaffen werden, die selbst mit Einschränkungen leicht dazu führen könnten, eine geschaffene Infrastruktur schleichend auszuweiten.**

Gegenwärtig existiert im deutschen Recht keine Gesetzesgrundlage für den Einsatz biometrischer Fernidentifizierungssysteme durch Strafverfolgungsbehörden. Es lässt sich derzeit allerdings beobachten, wie bestehende Befugnisse zweckentfremdet und als Legitimation für solche Einsätze herangezogen werden.

Dazu gehört unter anderem die Rasterfahndung (§ 98a Strafprozessordnung), die gegenwärtig zumindest von einigen Strafverfolgungsbehörden als rechtliche Grundlage für den Einsatz biometrischer Überwachungssysteme herangezogen wird.[7]

Rasterfahndung wurde auf Bundesebene 1992 gesetzlich geregelt. Die Rasterfahndung konnte biometrische Gesichtserkennungssysteme noch gar nicht umfasst haben, da die KI-basierte Gesichtserkennungstechnik zum Zeitpunkt der Einführung der Rechtsgrundlage noch gar nicht in der heutigen Funktionsweise existierte. Die Menge an biometrischen Daten, die heute durch KI-Systeme automatisiert verarbeitet werden, hätte sich der Gesetzgeber damals nicht träumen lassen. Auch der

[6] Koalitionsvertrag 2021- 2025 zwischen SPD, BÜNDNIS 90 / DIE GRÜNEN und FDP, S. 15 und 86f, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf

[7] Monroy (2024), Heimliche Polizeiaktion: Gesichtserkennung aus parkendem Fahrzeug, 17.04.2024, nd, https://www.nd-aktuell.de/artikel/1181467.ueberwachungstechnik-heimliche-polizeiaktion-gesichtserkennung-aus-parkendem-fahrzeug.html; siehe auch: Schriftliche Anfrage, Abgeordnetenhaus Berlin, Drucksache 19 / 18 461, S. 3f, https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-18461.pdf

verfassungsrechtliche Wesentlichkeitsvorbehalt verbietet eine Auslegung bestehender Gesetzesgrundlagen für derart grundrechtsinvasive und gefährliche Befugnisse.[8]

Eine bestehende gesetzliche Grundlage für ein bestimmtes Ermittlungsinstrument kann demnach nicht für neue biometrische Überwachungssysteme herangezogen bzw. umgedeutet werden. Erst recht nicht, wenn neuere Datenverarbeitungsmethoden viel tiefer in unsere Grundrechte eingreifen und das Potenzial haben, unsere demokratische Gesellschaft als Ganzes zu verändern. Das Bundesverfassungsgericht hat bereits für die großflächige, automatisierte Verarbeitung von Kfz-Kennzeichen durch Polizei und Strafverfolgungsbehörden hohe verfassungsrechtliche Anforderungen aufgestellt.[9] Und dort ging es nicht um besonders sensible biometrische Daten wie Gesichter, sondern um Kfz-Kennzeichen. Die automatisierte Erhebung und Auswertung von öffentlich zugänglichen personenbezogenen Daten stellt nach Rechtsprechung des Bundesverfassungsgerichts immer einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.[10]

Auch ein jüngeres Verfassungsurteil über die automatisierte Datenanalyse für die vorbeugende Bekämpfung von Straftaten stellt mit Verweis auf das Grundrecht auf informationelle Selbstbestimmung klar, dass automatische Abgleiche biometrischer Daten besonders voraussetzungsvoll sind.[11] Die Mindestanforderungen für biometrische Fernidentifizierung, wie sie in der KI-VO beschrieben werden, sind demnach zu unspezifisch. Die Einsatzzwecke und die Abgrenzung zwischen Echtzeit-Verarbeitung und nachträglicher Verarbeitung sind zu unbestimmt. Und weder die Referenzdatenbanken gesuchter Personen, noch die zu durchsuchenden Bild- oder Videodaten (etwa hinsichtlich zeitlicher und räumlicher Beschränkung) sind hinreichend konkretisiert.

Es lässt sich zusammenfassen: Selbst wenn der Gesetzgeber eine Rechtsgrundlage für den Einsatz biometrischer Fernidentifizierungssysteme in Echtzeit im öffentlich zugänglichen Raum zu Strafverfolgungszwecken schaffen wollte, entsprächen die Verfahrensanforderungen nach KI-Verordnung nicht den in Deutschland geltenden verfassungsrechtlichen Mindeststandards.

Eine explizites Verbot, biometrische Fernidentifizierungssysteme im öffentlichen Raum einzusetzen, würde die gegenwärtigen Rechtsunklarheiten beseitigen.

<u>Verbot nachträglicher biometrischer Fernidentifizierung</u>

Der Einsatz sämtlicher nicht ausdrücklich verbotener biometrischer Fernidentifizierungssysteme, unabhängig davon wer sie verwendet, fällt nach KI-VO unter die Hochrisiko-Anwendungen (Art. 26 Abs. 10 in Verbindung mit Anhang III, Absatz

[8] Rückert (2021), Mit künstlicher Intelligenz auf Verbrecherjagd, 22.01.2021, Verfassungsblog, https://verfassungsblog.de/ki-verbrecherjagd/
[9] BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, https://www.bverfg.de/e/rs20080311_1bvr207405.html
[10] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, https://www.bverfg.de/e/rs20181218_1bvr014215.html
[11] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, Rn. 87, https://www.bverfg.de/e/rs20230216_1bvr154719.html

1, Buchstabe a KI-VO). Das schließt auch solche Systeme mit ein, die nicht in Echtzeit, sondern nachträglich Gesichter in Videodaten oder Fotomaterial identifizieren.

Eine Unterscheidung zwischen Echtzeit-Systemen und Systemen zur nachträglichen Fernidentifizierung ist jedoch mit Blick auf die Grundrechtsauswirkungen unlogisch. Erstens ist im Gesetzestext nicht klar definiert, ab welchem Zeitversatz Echtzeit-Identifizierung zu nachträglicher Identifizierung wird. Zweitens bergen beide Formen der biometrischen Erkennung dasselbe Missbrauchspotenzial, dieselben Abschreckungseffekte, und dasselbe Risiko für diskriminierende Überwachung (siehe oben). Warum allein wegen einer Zeitverzögerung von einem geringeren Eingriff in Grundrechte ausgegangen werden sollte, bleibt unklar.

Im Gegenteil schafft die nachträgliche Fernidentifizierung zusätzliche Gefahren: Die Zeitverzögerung ermöglicht komplexere und damit tiefergehende Auswertungen und eröffnet das Risiko, dass Daten für neue Zwecke ausgewertet werden, die ursprünglich noch gar nicht der Erhebungsgrund waren. Es entsteht ggf. ein Anreiz, Videoaufnahmen lange zu speichern. Das schafft zusätzliche Einschüchterungseffekte, wenn wir nicht wissen, ob und wann Videoaufnahmen oder anderes Datenmaterial in Zukunft mit KI-Systemen ausgewertet werden können. Die KI-basierte Analyse von biometrischen Daten ist ein elaboriertes technisches Verarbeitungsverfahren und keine technische Arbeitshilfe für ein manuelles Verfahren.[12]

Ein umfassendes nationales Verbot biometrischer Fernidentifizierung im öffentlich zugänglichen Raum für Strafverfolgungszwecke muss daher im Sinne eines wirksamen Grundrechtsschutzes sämtliche biometrischen Erkennungssysteme unabhängig vom Zeitpunkt der Verwendung umschließen. Diese Möglichkeit bietet die KI-VO ausdrücklich (Artikel 26, Absatz 10, Unterabsatz 7 KI-VO). Erwägungsgrund 95 KI-VO betont zudem, dass nachträgliche Gesichtserkennung keinesfalls das Verbot von Echtzeit-Fernidentifizierung unterlaufen darf. Gemäß Artikel 10 der Richtlinie über Datenschutz in der Strafverfolgung (EU Richtlinie 2016/680) können alle EU Mitgliedstaaten weiterführende Regelungen bei der Verarbeitung biometrischer Daten durch Polizei und Strafverfolgung erlassen.

Es gilt aber auch hier die gleiche rechtliche Ausgangslage: Jede Form der biometrischen Fernidentifizierung bedarf einer eindeutigen gesetzlichen Grundlage. Solange diese nicht geschaffen wird, herrscht keine Erlaubnis. Bestehende Rechtsgrundlagen für automatisierte Gesichtserkennung heranzuziehen ist unzulässig und missachtet das Bestimmtheitsgebot (siehe oben). Polizei und Strafverfolgung benötigen für ein solch eingriffsintensives Instruments immer einer hinreichend bestimmten gesetzlichen Regelung. Sie kann nicht auf bereits vorhandenen, allgemeineren Normen basieren.[13]

[12] Vgl. die datenschutzrechtliche Einordnung und Beanstandung der Gesichtserkennungssoftware „Videmo 360“ in Hamburg: Tätigkeitsbericht Datenschutz 2018 des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, S.86f: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Taetigkeitsberichte_Datenschutz/Taetigkeitsberichte_PDF/27._Taetigkeitsbericht_Datenschutz_2018.pdf

[13] Vgl. dazu Schindler (2021), Im Auge der Polizei – Polizeiliche Gesichtserkennung im öffentlichen Raum, Verfassungsblog.de: https://verfassungsblog.de/os3-auge-polizei/

Verbot für Private

Die KI-VO erkennt die Nutzung von biometrischen Fernidentifikationsystemen durch private Akteure in öffentlich zugänglichen Räumen, sei es in Echtzeit oder nachträglich, laut Erwägungsgrund 39 als unzulässig an. Die KI-VO beinhaltet allerdings kein ausdrückliches Verbot von automatisierter Fernidentifizierung in öffentlich zugänglichen Räumen durch private Stellen (z.B. Betreiber von Einkaufszentren oder Sportanlagen) und öffentliche Stellen außerhalb der Polizei (z.B. kommunale Behörden, Schulen oder Universitäten), sei es in Echtzeit oder nachträglich, da die EU Datenschutzgrundverordnung 2016/679 dies schon untersagt.

Eine informierte Einwilligung oder ein berechtigtes Interesse kann bei biometrischer Fernidentifizierung durch Private im öffentlichen Raum nicht gegeben sein. Und es kann strukturell aufgrund der Vielzahl an potenziell betroffenen Personen bei biometrischer Fernidentifizierung nie angenommen werden. Keine private Stelle kann aus der Anwesenheit in einem öffentlichen Raum ein Einverständnis in die Datenerhebung herleiten.

Zusammenfassend lässt sich Folgendes festhalten:

- ➔ Gemäß der EU KI-Verordnung, insbesondere Erwägungsgrund 37, ist die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Zwecken der Strafverfolgung und der Gefahrenabwehr verboten.

- ➔ Im Einklang mit Artikel 10 der Richtlinie über Datenschutz in der Strafverfolgung (EU Richtlinie 2016/680) ist der Einsatz von Systemen zur nachträglichen biometrischen Fernidentifizierung in öffentlich zugänglichen Räumen durch Polizei und Strafverfolgung verboten.

- ➔ Basierend auf Artikel 9 der Datenschutz-Grundverordnung ist der Einsatz von biometrischen Fernidentifizierungssystemen in öffentlich zugänglichen Räumen, sowohl in Echtzeit als auch nachträglich, durch private und öffentliche Stellen verboten.

Dennoch bestehen Rechtsunklarheiten und Umsetzungsdefizite in der Praxis. Ein Durchführungsgesetz sollte diese ausräumen, indem darin die geltenden Verbote noch einmal konkretisierend ausformuliert werden.

9 Wie muss die Umsetzung des AI Acts in Deutschland gestaltet werden, um einerseits die Sicherheit und Bürgerrechte zu wahren und andererseits ein innovationsfreundliches Umfeld zu schaffen, das Innovationskraft und privatwirtschaftlichen Wettbewerb auf dem deutschen Markt ideal unterstützt?

Sicherheit und Bürgerrechte stehen nicht im Widerspruch zu einem innovationsfreundlichen Umfeld, sondern sind seine Grundlage. Entwicklungen, die unserer Sicherheit und unseren Bürgerrechten entgegenstehen, sind keine

Innovationen, sondern Gefahren. Die Frage, die sich stellt, ist: Wie kann es Unternehmen so leicht wie möglich gemacht werden, die Auflagen aus der KI-Verordnung einzuhalten?

Die Antwort sind klare und verständliche Vorgaben, eine effiziente Aufsichtsstruktur und Beratungsangebote durch die Koordinierungsstelle.

Auch Unternehmen sollten, ebenso wie Individuen, klare Ansprechpartner*innen haben und nicht mit einem Zuständigkeitswirrwarr konfrontiert sein. Das schafft Rechtssicherheit, was wiederum dazu führt, dass Unternehmen schneller Entscheidungen darüber treffen können, welche Produkte sie entwickeln und anbieten möchten, und minimiert ihre Kosten.

Klare und verständliche Vorgaben, die auch eingehalten werden können, führen zu einem „level playing field" der Unternehmen untereinander und belohnen nicht die „bad actors".

Zudem sollte die Aufsichtsbehörde eine Beratung für Unternehmen anbieten, die es ihnen erleichtert, gesetzeskonforme Produkte zu entwickeln und anzubieten.

18) Wie sollte und könnte ein nationales KI-Transparenzregister über den Bereich der Hoch Risiko Systeme hinausgehen, um wirksame Transparenz im Sinne des Verbraucherschutzes (Nachvollziehbarkeit, Beschwerdebasis etc.) herzustellen und insbesondere beim Einsatz von KI-Systemen durch die öffentliche Hand dem erhöhten Anspruch an Grundrechtsschutz und bestehende Abhängigkeiten gerecht zu werden und wie sollte generell ein solches Transparenzregister organisiert sein, hinsichtlich:

- **wer sollte es aufbauen und wen dabei einbeziehen**
- **wie sollte es aufgebaut werden**
- **wer sollte es verwalten**
- **welche Informationen sollte es enthalten?**

Transparenz und Nachvollziehbarkeit ist nicht nur im Hochrisikobereich gemäß KI-VO von Nutzen, sondern sollte für alle automatisierten Entscheidungssysteme von öffentlichen Stellen gelten. Die geplante EU-Datenbank (Art. 71 KI-VO), in der die Nutzung von Hochrisiko-KI-Systemen von öffentlichen Stellen gelistet werden sollen, wird nur wenige der insgesamt eingesetzten Systeme aufführen. Auf nationaler Ebene sollte daher nachgebessert und ein nationales KI-Transparenzregister für die gesamte öffentliche Hand eingeführt werden. Da die KI-VO ein generelles KI-Register nicht regelt, kann sie in diesem Bereich auch keine harmonisierende Wirkung haben. Die Niederlande haben bereits ein nationales KI-Register für die öffentliche Verwaltung eingeführt.[14]

[14] Siehe z.B. https://algoritmes.overheid.nl/en

Ein nationales KI-Transparenzregister sollte zentral koordiniert und standardisiert sein. Um eine Doppelstruktur zu vermeiden, sollte es über eine Schnittstelle zur EU Datenbank der Hochrisiko-Systeme verfügen. Damit steht es nicht im Konflikt mit der EU-Datenbank, sondern **ergänzt und vervollständigt den Überblick über staatliche KI-Einsätze.**

Ein nationales KI-Register für die öffentliche Verwaltung kann nicht nur Transparenz für Betroffene herstellen und Verantwortlichkeit erzeugen, sondern auch positive Anreize für Behörden schaffen: vorhandene Anwendungen werden sichtbar und auffindbar, ineffizienten Parallelentwicklungen lassen sich viel leichter vermeiden. Aktuell wird bereits durch das Beratungszentrum für Künstliche Intelligenz (BeKI) des BMI ein „Marktplatz der KI-Möglichkeiten“[15] entwickelt. Er soll Ministerien und Behörden die Potenziale von KI-Anwendungen aufzeigen und „Transparenz über die KI-Anwendungslandschaft und Erfahrungswerte in den Ressorts“[16] liefern.

Wichtig ist, dass die Angaben über KI-Anwendungen in Behörden über den in der KI-VO geforderten Datenkranz (vgl. Anhang VIII der KI-VO) hinausgehen. Denn wirksame Transparenz wird durch die dort geforderten spärlichen Informationen noch nicht hinreichend sichergestellt. Ziel sollte sein, Nachvollziehbarkeit für alle Menschen und eine effektive Grundlage für Nachfragen und Beschwerden sicherzustellen.

Ein **umfassender Transparenzbericht** sollte alle ethisch relevante Auswirkungen und die ergriffenen Gegenmaßnahmen detailliert aufführen. Dazu zählt u.a.:

- Definition des Problems, das das KI-System lösen soll
- Konkrete Zieldefinition (z.B. Effizienz- oder Leistungsverbesserungen, Entscheidungsunterstützung, Automatisierung von Aufgaben, Kostensenkung usw.)
- Ethische und rechtliche Anforderungen an das System (Datenschutz, IT-Sicherheit, Fairness, Erklärbarkeit, etc.)
- Transparenz über sämtliche Grundrechtsauswirkungen
- Transparenz über die Umweltverträglichkeit (Energieverbrauch, Treibhausgasemissionen, indirekter Ressourcenverbrauch, etc.)
- Benennung der Verantwortlichen für Konzeption und Implementierung.

Die Listung von KI-Anwendungen in einem nationalen KI-Transparenzregister sollte zudem **verpflichtend** sein. So wird Verbindlichkeit bezüglich der einzutragenden Daten geschaffen. Freiwillige Einträge in das Register werden zwangsläufig lückenhaft bleiben. Damit wäre das Ziel, Synergien zu nutzen und vertrauensbildende Transparenz für Betroffene zu gewährleisten, verfehlt.

[15] Bundesministerium des Innern (Pressemitteilung November 2023), Künstliche Intelligenz in der Verwaltung, https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/datenpolitik/daten-und-ki/daten-und-ki-node.html
[16] Ebenda.

Alle Ressorts sollten in die Entwicklung und Umsetzung des KI-Transparenzregisters einbezogen werden. Bei der Entwicklung ist ein strukturierter Stakeholderdialog, der frühzeitig alle relevanten Interessengruppen einbezieht, von großem Nutzen.

AlgorithmWatch ist eine Menschenrechtsorganisation mit Sitz in Berlin und Zürich, die sich mit den gesellschaftlichen Auswirkungen von algorithmischen Entscheidungssystemen (ADM) und Künstlicher Intelligenz (KI) befasst. Wir setzen uns dafür ein, dass solche Technologien Menschenrechte, Demokratie und Nachhaltigkeit stärken, statt sie zu schwächen. Dazu tragen wir mit politischen Kampagnen, Lobbyarbeit, journalistischen Recherchen, Forschung und Technikentwicklung bei.

Unsere Webseite: https://algorithmwatch.org/

Kontakt zu den Autor*innen:

Kilian Vieth-Ditlmann, [redacted]@algorithmwatch.org

Pia Sombetzki, [redacted]@algorithmwatch.org