Forderungspapier

Privatsphäre verteidigen: Keine Echtzeit-Überwachung durch KI im öffentlichen Raum

10. Dezember 2024

Hintergrund

Am 1. August 2024 trat mit der „Verordnung über künstliche Intelligenz“[1] oder kurz „KI Verordnung“ das weltweit erste umfassende Gesetz zu Künstlicher Intelligenz in der Europäischen Union in Kraft. Ziel ist es, einen einheitlichen Rechtsrahmen für die Entwicklung und Nutzung von Künstlicher Intelligenz (KI) zu schaffen, der sowohl die Grundrechte schützt als auch Innovation fördert. Die Verordnung gilt unmittelbar in allen Mitgliedstaaten und reguliert KI-Systeme und KI-Modelle entlang ihrer gesamten Wertschöpfungskette, mit besonderem Fokus auf Anbieter und Betreiber solcher Technologien.

Die Verordnung verfolgt einen risikobasierten Ansatz: Je höher das Risiko, das von einem KI-System ausgeht, desto strenger sind die regulatorischen Anforderungen. **KI-Systeme mit einem inakzeptablen Risiko, also Technologien, die grundlegend gegen die Rechte und Freiheiten von Bürger:innen verstoßen, sind verboten**. **Dazu gehören** unter anderem Social Scoring-Systeme, die Menschen anhand ihres Verhaltens oder sozialen Status bewerten, sowie **biometrische Echtzeit-Fernidentifizierungssysteme (Gesichtserkennung) im öffentlichen Raum zu Strafverfolgungszwecken**[2]. Letztere werden als unverhältnismäßige Eingriffe in die Privatsphäre und andere Grundrechte betrachtet und unterliegen daher einem generellen Verbot.

Die Verordnung sieht jedoch eng gefasste Ausnahmen vor, die es Mitgliedstaaten ermöglichen, biometrische Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum zu Strafverfolgungszwecken unter strengen Auflagen zuzulassen. Diese Ausnahmen gelten nur in spezifischen Szenarien, wie der Abwehr einer unmittelbar drohenden terroristischen Bedrohung oder der Suche nach einer Person, die wegen eines schweren Verbrechens gesucht wird. In solchen Fällen müssen Mitgliedstaaten sicherstellen, dass der Einsatz dieser Technologien einer richterlichen oder unabhängigen Genehmigung unterliegt und die Grundsätze der Verhältnismäßigkeit und Notwendigkeit strikt eingehalten werden.

Was sind biometrische Echtzeit-Fernidentifizierungssysteme?

Ein biometrisches Fernidentifizierungssystem ist ein KI-System, das dazu dient, natürliche Personen ohne deren aktive Einbeziehung und in der Regel aus der Ferne zu identifizieren, indem die biometrischen Daten einer Person mit einer Referenzdatenbank abgeglichen werden[3]. Beispiele dafür sind die Erkennung anhand eines Gesichts oder der Bewegungsmuster und Körperkonfiguration einer Person.

1 (EU) 2024/1689, Link:https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689
2 Art 5 (1) d KI Verordnung
3 Art 3 Nr 41 KI Verordnung

Echtzeit-Fernidentifizierungssysteme führen diese Identifizierung ohne erhebliche Verzögerung durch. Dies umfasst sowohl sofortige Identifizierungen als auch solche mit kurzen Verzögerungen, um Umgehungen der Vorschriften zu verhindern[4].

Diese Systeme stellen eine besonders invasive Form der Überwachung dar, da sie eine unmittelbare Erfassung und Verarbeitung biometrischer Daten ermöglichen. Ihre Nutzung in öffentlich zugänglichen Räumen gefährdet die Privatsphäre und die Autonomie der Bürger:innen und kann schwerwiegende Auswirkungen auf Grundrechte wie das Recht auf Datenschutz und die Versammlungsfreiheit haben.

Konflikt mit Grundrechten

Der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum verletzt potenziell das Grundrecht auf Datenschutz gemäß § 1 Datenschutzgesetz (DSG), das den Schutz der Geheimhaltungsinteressen von Personen im Umgang mit ihren personenbezogenen Daten sicherstellt. Zudem kollidiert der Einsatz solcher Systeme mit dem Recht auf Achtung des Privatlebens gemäß Artikel 8 der Europäischen Menschenrechtskonvention (EMRK).

Der Verfassungsgerichtshof (VfGH) hat in mehreren Entscheidungen betont, dass Eingriffe in diese Rechte nur dann zulässig sind, wenn sie verhältnismäßig, notwendig und streng zweckgebunden sind. So hielt der VfGH beispielsweise fest[5], dass die Nutzung von Daten aus Section-Control-Anlagen durch Sicherheitsbehörden eine gravierende Verletzung des Datenschutzrechts darstellen kann. Der Zugriff auf diese Daten betraf eine große Anzahl von Personen unabhängig davon, ob sie ein strafrechtlich relevantes Verhalten zeigten. Dies schuf nicht nur einen unverhältnismäßigen Eingriff in die Geheimhaltungsinteressen gemäß § 1 DSG und Art. 8 EMRK, sondern führte auch zu einem „Gefühl der Überwachung"[6], das die Ausübung anderer Grundrechte wie der Versammlungsfreiheit (Art. 12 Staatsgrundgesetz beeinträchtigen kann. Diese Entscheidung bezog sich auf Überwachung von Autobahnen und Schnellstraßen, wohingegen der Einsatzbereich im dicht besiedelten innerstädtischen Gebiet noch viel heiklere Grundrechtsfragen aufwirft.

Biometrische Echtzeit-Fernidentifizierungssysteme bergen ähnliche Risiken. Trotz der Einschränkung ihres Einsatzes auf besonders schwere Straftaten gemäß der EU-KI-Verordnung bleibt die Gefahr eines unverhältnismäßigen Eingriffs bestehen. **Die potenziell flächendeckende Überwachung betrifft alle Personen in einem öffentlichen Raum, unabhängig davon, ob sie ein Verhalten zeigen, das Anlass zur Überwachung gibt.** Derartige Maßnahmen schaffen ein Klima der ständigen Kontrolle, das die freie Ausübung demokratischer Rechte, wie das Recht auf friedliche Versammlung oder Meinungsfreiheit, massiv einschränken kann.

Österreich wollte strengere Regeln zu biometrischer Überwachung im Rat

Wohl auch aus den im vorherigen Abschnitt dargestellten grundrechtlichen Bedenken **hat Österreich im Rahmen der Verhandlungen zur EU-KI-Verordnung eine kritische Position zu biometrischen Echtzeit-Fernidentifizierungssystemen eingenommen**[7]. In einem offiziellen Positionspapier an den Rat der Europäischen Union wurde hervorgehoben, dass die in Artikel 5(1)(d) vorgesehenen Ausnahmen

4 Artikel 3 Nr. 42 KI Verordnung
5 G 72-74/2019
6 Seite 4 G 72-74/2019, https://www.vfgh.gv.at/downloads/VfGH_Verkuendung_11.12.2019_G_72_2019.pdf
7 https://data.consilium.europa.eu/doc/document/ST-9645-2024-ADD-1-REV-2/en/pdf

„zu weitreichend und nicht mit dem österreichischen Verständnis von verhältnismäßigen Eingriffen in die Grundrechte vereinbar“[8] seien.

Österreich betonte, dass diese Technologien erhebliche Eingriffe in die Privatsphäre darstellen und auch in Ausnahmefällen nur unter strengsten Bedingungen erlaubt werden dürften. Diese Position unterstreicht das Bewusstsein für die Risiken, die biometrische Überwachungstechnologien für Datenschutz und Grundrechte mit sich bringen.

Technische Gefahren und Fehleranfälligkeit

Zusätzlich zu den rechtlichen und ethischen Fragen kommt die technische Fehleranfälligkeit biometrischer Technologien hinzu. Ein Vorfall in Österreich im Zusammenhang mit der nachträglichen biometrischen Identifizierung zeigt die potenziell gravierenden Folgen solcher Fehler auf[9]. **Im Jahr 2019 wurde eine Person aufgrund eines Fehlers der Gesichtserkennungssoftware zu Unrecht mit einer Straftat in Verbindung gebracht**. Dieser Vorfall führte zu langwierigen rechtlichen Auseinandersetzungen und erheblichem Schaden für die betroffene Person. Solche Fehler verdeutlichen, dass selbst bei begrenztem Einsatz biometrischer Technologien erhebliche Risiken bestehen, die die Lebensrealität unschuldiger Menschen dramatisch beeinflussen können.

Forderung

Der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme ist gemäß der KI Verordnung grundsätzlich untersagt und nur in klar definierten Ausnahmefällen zulässig, wenn diese durch spezifische nationale gesetzliche Regelungen präzise ausgestaltet werden. In Österreich gibt es derzeit keine derartigen gesetzlichen Regelungen.

Angesichts der erheblichen grundrechtlichen Bedenken, insbesondere der potenziellen Eingriffe in das Grundrecht auf Datenschutz und das Recht auf Achtung des Privatlebens, sollte Österreich keine gesetzlichen Grundlagen schaffen, die solche Technologien zulassen könnten. Der Schutz der Privatsphäre und der Versammlungsfreiheit darf nicht durch invasive Überwachungsmaßnahmen gefährdet werden.

Darüber hinaus ist die nach wie vor hohe Fehleranfälligkeit solcher Technologien ein weiterer entscheidender Grund, von ihrer Einführung abzusehen. Fälle fehlerhafter Identifizierungen verdeutlichen, wie dramatisch die Folgen für Betroffene sein können und wie das Vertrauen in staatliche Institutionen erodiert.

Stattdessen sollte Österreich konsequent auf einen bewährten und grundrechtskonformen Ansatz setzen, der den Schutz vor Überwachungstechnologien sicherstellt und die Wahrung von Freiheitsrechten stärkt.

8 Ebd
9 https://www.derstandard.at/story/3000000215580/kampf-um-entschaedigung-nach-fehler-der-gesichtserkennung