KI-03-125 Künstliche Intelligenz mit dem Menschen im Mittelpunkt

Antragsteller*in: BAG Digitales und Medien, BAG Kultur, BAG Demokratie und Recht
Beschlussdatum: 03.10.2026

Änderungsantrag zu KI-03

Von Zeile 124 bis 125 einfügen:
Grund verbietet der EU AI Act Anwendungen, die mit erheblichen Risiken verbunden sind.

Der Einsatz von KI in der öffentlichen Verwaltung, der Justiz und insbesondere in den Sicherheitsbehörden berührt das Fundament unserer Bürger*innenrechte und der rechtsstaatlichen Gewaltenteilung. Ein KI-gestützter Überwachungsstaat widerspricht unseren Grundwerten tiefgreifend.

Keine automatisierten Grundrechtseingriffe: Algorithmen dürfen weder Ermittlungsentscheidungen treffen noch automatisierte Verwaltungs- oder Gerichtsakte ausführen. Die letztgültige Verantwortung und Entscheidung muss stets unvertretbar beim Menschen liegen.

Verbot diskriminierender KI-Systeme: Intransparente Datensammlung birgt das Risiko, bestehende Diskriminierung zu verstärken, etwa bei Einstellungen für berufliche Positionen, Beförderungen, Kreditvergaben und in der Justiz.

Verbot der verhaltensbasierten Überwachung in Betrieben, sofern nicht zur Sicherheit (z.B. in Hochrisikobereichen) zwingend erforderlich: Das Erfassung von Leistungsdaten oder biometrischen Informationen birgt das Risiko der totalen Überwachung. Grundrechte wie das Recht auf informationelle Selbstbestimmnung dürfen nicht verletzt werden. Beschäftigte haben ein Recht auf Transparenz zur Erhebung von Daten und zum Recht auf Widerspruch.

Verbot von Massenüberwachung und biometrischer Erkennung: Wir lehnen die flächendeckende biometrische Gesichtserkennung im öffentlichen Raum, automatisierte Gefühlserkennung sowie Systeme zur vorausschauenden Polizeiarbeit (Predictive Policing) und zur verdachtslosen Rasterfahndung strikt ab. Sie führen zu Generalverdacht und Diskriminierung.

Keine Palantir-Software in Sicherheitsbehörden: Wir fordern die umgehende Kündigung bestehender Verträge und das Verbot des Einsatzes von Software-Lösungen des US-Konzerns Palantir (wie Gotham oder Foundry) sowie vergleichbarer Anwendungssoftware bei Polizei- und Sicherheitsbehörden von Bund und Ländern. Geschäftsmodelle, die auf Datenmonopolen, intransparenten Algorithmen und der Auswertung sensibelster Bürger*innendaten durch US-Tech-Oligarchen beruhen, sind mit den europäischen Datenschutzstandards und dem Rechtsstaat unvereinbar.

Heimische und europäische IT-Lösungen für die Strafverfolgung: Software zur digitalen Datenanalyse in der Strafverfolgung muss zwingend aus Deutschland oder der Europäischen Union stammen. Sie muss quelloffen (Open Source), unabhängig auditiert, datensparsam und strikt an die Grundrechte und die europäische Datenschutz Grundverordnung (DSGVO) gebunden sein.