digitalcourage

Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Tel. +49 521 1639 1639
Fax +49 521 61172
mail@digitalcourage.de

Amtsgericht Bielefeld, VR 2479
USt-ID: DE 187386083

Spendenkonto:
IBAN: DE66 4805 0161 0002 1297 99
Sparkasse Bielefeld
BIC: SPBI DE3B XXX

digitalcourage.de
bigbrotherawards.de

Digitalcourage e.V. • Marktstraße 18 • 33602 Bielefeld

Thüringer Landtag
Ausschuss für Inneres, Kommunales und
Landesentwicklung
Jürgen-Fuchs-Straße 1
99096 Erfurt

Bielefeld, 21.05.2026

**Stellungnahme von Digitalcourage e.V.
im Rahmen des Anhörungsverfahren im Thüringer Landtag zum Zweiten Gesetz zur Änderung des Polizeiaufgabengesetz (Drucksache 8/2478)**

Sehr geehrte Empfänger*innen,

wir bedanken uns für die Möglichkeit, zum Gesetzentwurf für das „Zweite Gesetz zur Änderung des Polizeiaufgabengesetz“ Stellung zu nehmen.

Digitalcourage engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir sind technikaffin, aber wir wenden uns entschieden dagegen, dass politische Probleme mit immer neuer Überwachung beantwortet werden. Freiheit, informationelle Selbstbestimmung und andere Grundrechte sind keine Nebensachen, die man im Namen einer vermeintlich modernen Sicherheitsarchitektur beiseite schieben darf. Sie sind die Grundlage einer demokratischen Gesellschaft.

Wir werden im Folgenden nicht den gesamten Fragenkatalog einzeln abarbeiten. Das ist schon wegen des Umfangs kaum sinnvoll. Wir konzentrieren uns in dieser Stellungnahme stattdessen auf die besonders gefährlichen Teile des Entwurfs: die KI-gestütze Verhaltensanalyse bei Videoaufnahmen im öffentlichen Raum (§ 33a ThürPAG-E), die biometrische Identifizierung über frei zugängliche Internetdaten (§ 43a ThürPAG-E) und die Zusammenführung von Daten aus verschiedenen Quellen zur Palantir-artigen automatisierte Datenanalyse (§ 40a ThürPAG-E). Genau hier bekommen klassische Polizeibefugnisse eine neue Qualität staatlicher Kontrolle in einer Demokratie.

Zur Bewertung dieser ist für uns zentral: Die Gefahr für die Demokratie geht nicht von unüberwachten Bürger*innen aus, sondern vom Erstarken autoritärer und rechtsradikaler Parteien. Gerade in Thüringen, wo die AFD in aktuellen Umfragen auf 39 Prozent kommt, ist es politisch fahrlässig, Überwachungsinstrumente zu schaffen, mit denen das Verhalten von Personen automatisiert bewertet und im öffentlichen Raum verfolgt werden und Datenberge auf

Knopfdruck zusammengeführt werden können. Solche Instrumente greifen tief in die Privatsphäre ein, sind fehleranfällig und entziehen sich wirksamer Kontrolle.

Umso wichtiger ist es deswegen keine Befugnisse zu schaffen, die morgen von einer blau-braunen Regierung missbraucht werden können, etwa um Klimaaktivist*innen elektronische Fußfesseln anzulegen, engagierten Gewerkschafter*innen die Teilnahme an Streiks zu erschweren, bei Demonstrationen mittels Drohnen massenhaft Handydaten auszulesen, statt eines Schlagstocks gleich den Taser zu zücken oder mit KI in Urlaubsfotos auf Instagram Personen zu identifizieren. Der Entwurf schafft Befugnisse und technische Infrastrukturen, die solche Entwicklungen ermöglichen können.

Im Folgenden nehmen wir Stellung zu ausgewählten Teilen des Entwurfs. Vorher aber eine Klarstellung zum Framing der Landesregierung.

Opferschutz ist wichtig – aber keine Tarnkappe für Massenüberwachung.

Die Landesregierung rahmt die Novelle insgesamt ausdrücklich auch mit Opferschutz, insbesondere bei Gewalt gegen Frauen. Genau deshalb muss man sauber trennen: Verhaltensscanner, biometrische Internetsuche und automatisierte Datenanalyse sind keine punktgenauen Instrumente zum Schutz Betroffener häuslicher- oder sexualisierter Gewalt, sondern breite Kontrollwerkzeuge mit allgemeiner Reichweite.

Wer Menschen wirklich schützen will, muss also in Beratung, Frauenhäuser, psychosoziale Hilfe, Prävention, spezialisierte Ansprechstellen, schnelle Unterstützung und gut ausgestattete soziale Infrastruktur investieren. Überwachungstechnik ersetzt das nicht. Sie schafft keine Wohnung für eine bedrohte Frau, keinen freien Platz im Frauenhaus, keine Beratung nach einer Gewalterfahrung und keine verlässliche Begleitung im Verfahren. Stattdessen droht eine Infrastruktur, die alle Menschen im öffentlichen Raum stärker erfassbar, auswertbar und kontrollierbar macht.

Opferschutz darf nicht als politisches Schutzschild für Befugnisse dienen, die weit über den behaupteten Zweck hinausgehen. Eine Maßnahme, die am Ende alle betrifft, ist kein zielgenauer Schutz, sondern ein Generalverdacht.

KI-gestütze Verhaltensanalyse bei Videoaufnahmen im öffentlichen Raum (33a ThürPAG-E)

Besonders problematisch ist die im Entwurf enthaltene Regelung zur automatisierten Auswertung von Bildaufzeichnungen. Der Vorschlag sieht vor, dass die Polizei Aufzeichnungen bei öffentlichen Veranstaltungen und an besonderen Orten nicht nur anfertigen, sondern auch automatisch auswerten lassen darf. Software soll Verhaltensmuster erkennen, die auf eine Gefahrensituation oder eine Straftat hindeuten können. Wird ein solches Muster erkannt, soll sogar eine automatisierte Nachverfolgung der betroffenen Personen mit weiteren Kameras im öffentlichen Raum möglich sein. Das ist keine kleine technische Ergänzung des bereits Erlaubten. Es ist ein qualitativer Sprung. Die Kamera dokumentiert hier nicht mehr nur, sie produziert Verdacht. Menschen werden hier erstmals im öffentlichen Raum durch eine automatisierte Infrastruktur nicht nur beobachtet, sondern maschinell bewertet, markiert und potenziell weiterverfolgt.

Gegen diese Maßnahme sprechen gleich mehrere Gründe.

Ersten sind solche KI-Systeme technisch alles andere als neutral oder verlässlich. Das National Institute of Standards and Technology (NIST, deutsch: Nationales Institut für Standards und Technologie), eine zentrale US-Großforschungseinrichtung für Standardisierung und Messtechnik vergleichbar mit der deutschen Physikalisch-Technische Bundesanstalt, hat bei der Mehrheit der untersuchten Gesichtserkennungsalgorithmen demografische Unterschiede festgestellt. Die Systeme erkannten Menschen je nach Herkunft, Geschlecht oder Alter unterschiedlich zuverlässig. Besonders asiatische, Schwarze und indigene Personen wurden deutlich häufiger falsch identifiziert als weiße Personen. Die Forschenden betonen, dass solche Fehler insbesondere bei polizeilichen Datenbankabgleichen problematische Folgen haben können.[1]

Solche Systeme sind technisch also nicht verlässlich. Bei der Verhaltensanalyse muss ein Algorithmus nun aber „auffälliges" oder „verdächtiges" Verhalten definieren und von „normalem" Verhalten unterscheiden. Genau daran scheitert die Idee bereits praktisch. Eine Umarmung kann wie ein Angriff aussehen. Ein High-Five kann wie eine Ohrfeige wirken. Eine hektische Bewegung kann eine Gefahr anzeigen – oder schlicht bedeuten, dass jemand einem Bus hinterherrennt. Eine Person, die auf dem Boden sitzt, sich ungewöhnlich bewegt, Pfandflaschen sammelt oder psychisch belastet ist, kann für ein System auffällig erscheinen, ohne dass irgendeine Gefahr besteht. Deshalb reicht es nicht zu sagen, am Ende schaue ja „noch ein Mensch drauf". Die Kamera dokumentiert hier nicht mehr nur, sie produziert Verdächtigungen. Das ist der qualitative Sprung.

Das Problem liegt nicht nur im technischen Fehler. Es liegt in den Folgen. Ein falscher Alarm ist im polizeilichen Kontext nie harmlos. Er kann zu Kontrollen, Einschüchterung, Stigmatisierung und gefährlichen Einsatzsituationen führen. Gerade Menschen, die bereits heute häufiger kontrolliert werden – arme Menschen, obdachlose Menschen, migrantisierte Menschen, Jugendliche, psychisch erkrankte Menschen oder Personen, die aus anderen Gründen nicht in die Norm passen, werden durch solche Systeme, welche mit verzerrten Daten arbeiten, besonders leicht in den Fokus geraten. In den USA gab es mehrfach Fälle, in denen Menschen nach fehlerhaften Treffern kontrolliert oder sogar festgenommen wurden.[2]

Zweitens warnen zahlreiche Fachinstitutionen vor den gesellschaftlichen Folgen biometrischer Gesichtserkennung. Das Deutsche Institut für Menschenrechte verweist in einer umfangreichen Analyse auf „erhebliche rechtliche und ethische Fragen" und hält es für „unerlässlich, diese Technologie nicht vorschnell einzuführen".[3] Neben falschen Verdächtigungen und diskriminierende Algorithmen, wie es auch das NIST feststellte, sehen die Forschenden insbesondere die Gefahr umfassender Profilbildung. Werden Personen über verschiedene Orte und Zeitpunkte hinweg immer wieder erkannt, lassen sich daraus sensible Rückschlüsse auf ihr

---

1 National Institute of Standards and Technology: NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19.12.2019, aktualisiert am 03.02.2025, online abrufbar unter: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

2 Innocence Project: *When Artificial Intelligence Gets It Wrong*, online abrufbar unter: https://innocenceproject.org/news/when-artificial-intelligence-gets-it-wrong/

3 Eric Töpfer/Steven Kleemann: *Polizeiliche Gesichtserkennung. Menschenrechtliche Herausforderungen einer Risikotechnologie*, Deutsches Institut für Menschenrechte, Analyse, August 2025, online abrufbar unter: https://www.institut-fuer-menschenrechte.de/publikationen/detail/polizeiliche-gesichtserkennung,

Leben ziehen – etwa mit wem jemand regelmäßig demonstriert, welche religiösen Veranstaltungen besucht werden oder ob jemand häufig eine psychiatrische Klinik aufsucht.

Drittens ist der behauptete Sicherheitsgewinn schlecht belegt. Überblicksstudien zu klassischer Videoüberwachung zeigen insgesamt nur begrenzte Effekte; die deutlichsten und konsistentesten Wirkungen finden sich bei Parkplätzen und Eigentumsdelikten, nicht als allgemeines Wundermittel gegen Gewalt im öffentlichen Raum.[4] Die Vorstellung, KI-gestützte Videoüberwachung könne nun zuverlässig Straftaten verhindern oder Gefahren erkennen, ist deshalb Sicherheitstheater: technisch aufwendig, grundrechtlich teuer und hinsichtlich des tatsächlichen Nutzens hoch spekulativ. Kameras sind seit langem ein politisch dankbares Mittel, um Handlungsfähigkeit zu demonstrieren. Gekoppelt mit KI wird daraus eine noch eingriffsintensivere Variante einer Law-and-Order-Politik, deren Nutzen weit weniger belegt ist als ihr Grundrechtseingriff.

Spontane Gewalttaten werden durch Überwachung nicht vereitelt. Jedes Video, das Gewalt zeigt, belegt das. Täter, die impulsiv handeln, lassen sich davon nicht abschrecken. Die Praxisbeispiele, mit denen solche Systeme in Deutschland beworben werden, geben gerade keinen Anlass zu Technikoptimismus. Nach Recherchen von netzpolitik.org wird ein Verhaltensscanner in Mannheim seit 2018 trainiert; einen benennbaren Fall, in dem das System eine Ermittlung unterstützt hätte, konnte die Polizei dort dem Bericht zufolge nicht nennen. Gleichzeitig läuft in Hamburg bereits ein Folgeprojekt im Wirkbetrieb: Dort sollen „ungewöhnliche Bewegungsmuster“ erkannt, an Beamt*innen gemeldet und die Detektionsqualität weiter erhöht werden. Genau darin zeigt sich das Problem: Erst wird die Infrastruktur geschaffen, dann wird ihr Nutzen nachträglich behauptet. Ist die Technik einmal da, sinkt erfahrungsgemäß die politische Schwelle für deren Ausweitung.[5]

Viertens verschärft automatisierte Videoauswertung bestehende Ungleichheiten im öffentlichen Raum. Orte, die als Kriminalitätsschwerpunkte gelten, sind häufig Orte, an denen sich arme, junge oder migrantisierte Menschen aufhalten. Dort wird mehr kontrolliert, dort werden mehr Verstöße festgestellt, und genau diese Zahlen dienen später als Begründung für noch mehr Kontrolle. So entsteht eine selbsterfüllende Prophezeiung. Wer viel sucht, findet viel. Und wo viel gefunden wird, wird noch mehr gesucht.

Das gilt besonders, wenn polizeiliche Technik an sogenannte besondere oder gefährliche Orte geknüpft wird. Die Einstufung solcher Orte ist nie neutral. Sie ist Ergebnis politischer, polizeilicher und sozialer Zuschreibungen. Ein öffentlicher Platz wird nicht dadurch gefährlich, dass dort arme Menschen sitzen, Jugendliche sich treffen oder Menschen ohne Konsumabsicht verweilen. Wenn aber gerade solche Orte mit immer neuer Technik überzogen werden, verschiebt sich der öffentliche Raum: Wer konsumiert, sitzt geschützt in der Außengastronomie. Wer daneben auf einer Bank sitzt, wird zum Objekt polizeilicher Beobachtung.

---

4 Eric L. Piza/Brandon C. Welsh/David P. Farrington/Amanda L. Thomas: *CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis*, in: *Criminology & Public Policy*, Vol. 18, Issue 1, 2019, S. 135–159, online abrufbar unter: https://www.ojp.gov/library/publications/cctv-surveillance-crime-prevention-40-year-systematic-review-meta-analysis

5 Martin Schwarzbeck: *Polizeigesetz-Novelle: Auch Thüringen will Verhaltensscanner*, netzpolitik.org, 05.02.2026, online abrufbar unter: https://netzpolitik.org/2026/polizeigesetz-novelle-auch-thueringen-will-verhaltensscanner/

Fünftens verändert schon die bloße Tatsache permanenter algorithmischer Beobachtung das Verhalten von Menschen. Bereits das Wissen, dass Behörden Kameras mit Gesichtserkennung einsetzen, kann Menschen einschüchtern und sogenannte „Chilling Effects" auslösen, also Situationen, in denen Menschen aus Angst vor Überwachung oder möglichen Konsequenzen auf die Ausübung ihrer Grundrechte verzichten – etwa an Demonstrationen teilzunehmen oder politische Veranstaltungen zu besuchen.

Der European Data Protection Board und der European Data Protection Supervisor warnen ausdrücklich, dass biometrische Identifizierung in öffentlich zugänglichen Räumen die berechtigte Erwartung beschädigt, sich dort anonym bewegen zu können, und dass dies Meinungsfreiheit, Versammlungsfreiheit, Vereinigungsfreiheit und Bewegungsfreiheit direkt beeinträchtigt. [6] Auch der Europäische Gerichtshof für Menschenrechte hat im Einsatz von Gesichtserkennungssoftware einen Eingriff in das Recht auf Privatsphäre gesehen und vor einer abschreckenden Wirkung auf die Meinungs- und Versammlungsfreiheit gewarnt.[7] Auch das Bundesverfassungsgericht kennt solche „Chilling Effects" seit Jahrzehnten und berief sich schon mehrfach auf diesen Effekt, der einer freien Gesellschaft diametral entgegensteht. Bereits im Volkszählungsurteil von 1983 warnte das Gericht davor, dass Menschen ihr Verhalten verändern, wenn sie nicht mehr wissen können, wer was wann über sie speichert.[8]

Genau das ist der Punkt: Menschen verhalten sich anders, wenn sie wissen, dass Kameras nicht nur aufzeichnen, sondern analysieren. Wer nicht in die Norm passt, wer laut ist, arm ist, krank ist, politisch sichtbar ist oder einfach nur auffällt, wird vorsichtiger, stiller, angepasster. Aus Angst, als potentielle ‚Gefährder' abgestempelt zu werden. Wollen wir wirklich in einer Zukunft leben, in der jede spontane Geste, jede kleine Abweichung und jeder geringfügige Verstoß technisch erfasst, bewertet und potenziell gegen Menschen verwendet werden kann? Ab wann hört moderne Polizeiarbeit auf und beginnt eine Überwachungslogik, die wir sonst mit autoritären Staaten verbinden?

Digitalcourage lehnt § 33a ThürPAG-E in dieser Form ab. Eine demokratische Gesellschaft darf ihren Alltag nicht zum Einsatzfeld für automatisierte Verdächtigungen verwandeln. Eine KI-gestützte Verhaltensanalyse im öffentlichen Raum darf unter anderem aus den angeführten Gründen nicht eingeführt werden.

---

6 European Data Protection Board/European Data Protection Supervisor: Joint Opinion 5/2021 on the proposal for a Regulation laying down harmonised rules on artificial intelligence, 18.06.2021, , Rn. 30, S. 12., online abrufbar unter: https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

7 Europäischer Gerichtshof für Menschenrechte: *Glukhin v. Russia*, Nr. 11519/20, Urteil vom 04.07.2023, online abrufbar unter: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}

8 Bundesverfassungsgericht: Urteil vom 15.12.1983 – 1 BvR 209/83 u. a. –, BVerfGE 65, 1 (*Volkszählungsurteil*), online abrufbar unter: http://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf,

Biometrische Identifizierung über frei zugängliche Internetdaten (§ 43a ThürPAG-E)

Genauso entschieden lehnen wir die KI-gestützte Gesichtserkennung und den Stimmabgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet ab. Diese Maßnahme bedeutet in der Praxis, dass unzählige Fotos, Videos und Sprachaufnahmen von Unbeteiligten durchsucht werden, obwohl sie keinerlei Anlass gegeben haben.

Öffentlich im Internet bedeutet nicht frei zur biometrischen Polizeidurchsuchung. Wer ein Urlaubsfoto hochlädt, auf einem Gruppenbild erscheint, auf einer Demonstration gefilmt wird, in einem Livestream auftaucht oder auf einer Vereinsseite zu sehen ist, stellt sich damit nicht für eine staatliche Datenbank bereit. Es macht einen Unterschied, ob ein Bild von Menschen betrachtet werden kann oder ob es automatisiert vermessen, indexiert und polizeilich durchsuchbar gemacht wird.

Diese Unterscheidung ist zentral. Der öffentliche Raum und das Internet leben davon, dass Menschen sichtbar sein können, ohne dadurch vollständig identifizierbar, verfolgbar und auswertbar zu werden. § 43a droht genau diese Grenze einzureißen. Aus Kommunikation, politischer Teilhabe, privaten Erinnerungen und Alltagsbildern würde ein biometrisches Fahndungsfeld.

Das verletzt informationelle Selbstbestimmung nicht am Rand, sondern im Kern. Besonders schwer wiegt die abschreckende Wirkung auf politische Teilhabe: Gehe ich noch auf eine Demonstration, wenn ich im Nachhinein biometrisch identifiziert werden kann? Rede ich noch offen, wenn meine Stimme als Suchmerkmal taugt? Solche Systeme verschieben die Schwelle des Sag- und Machbaren in der Demokratie.

Das Deutsches Institut für Menschenrechte beschreibt Gesichtserkennung zutreffend als Kontrolltechnologie mit erheblichen Risiken für Grund- und Menschenrechte: In überwachten Räumen bedeutet sie das Ende der Anonymität, erzeugt Abschreckungseffekte und kann Menschen davon abhalten, ihre Meinungs- und Versammlungsfreiheit wahrzunehmen.[9] Der European Court of Human Rights hat im Fall Fall Glukhin v. Russia gerade die Kombination aus Internetfotos, Videoüberwachung und Gesichtserkennung gegen einen friedlichen Demonstranten als besonders eingriffsintensiv bewertet und als nicht notwendig in einer demokratischen Gesellschaft beanstandet.[10] Die Botschaft ist klar: Biometrische Identifizierung politisch aktiver Menschen ist in einer demokratischen Gesellschaft besonders gefährlich.

Hinzu kommt die Fehleranfälligkeit solcher Systeme. Das National Institute of Standards and Technology hat bei der Mehrheit der untersuchten Gesichtserkennungsalgorithmen demografische Unterschiede festgestellt. Je nach Algorithmus traten insbesondere bei

---

9 Eric Töpfer/Steven Kleemann: *Polizeiliche Gesichtserkennung. Menschenrechtliche Herausforderungen einer Risikotechnologie*, Deutsches Institut für Menschenrechte, Analyse, August 2025, online abrufbar unter: https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Analyse_Studie/Analyse_Polizeiliche_Gesichtserkennung_01.pdf

10 Europäischer Gerichtshof für Menschenrechte: *Glukhin v. Russia*, Nr. 11519/20, Urteil vom 04.07.2023, online abrufbar unter: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}

bestimmten Gruppen deutlich höhere Fehlerraten auf.[11] Auch wenn technische Systeme besser werden, bleibt das Grundproblem bestehen: Ein falscher Treffer im polizeilichen Kontext kann für Betroffene massive Folgen haben. Er kann Kontrollen, Ermittlungen, Stigmatisierung oder Freiheitsentziehung auslösen. Die Behauptung technischer Objektivität ist deshalb gefährlich. Sie verschleiert, dass Systeme mit Daten, Annahmen und gesellschaftlichen Ungleichheiten arbeiten.

Europarechtlich ist die Richtung ebenfalls klar: Die europäische Regulierung bewegt sich nicht auf eine Ausweitung solcher Praktiken zu, sondern auf ihre Begrenzung. Die KI-Verordnung der EU, der AI Act, stellt in Artikel 5 unmissverständlich klar, dass bestimmte AI-Praktiken in der EU verboten sind. Darunter fallen bestimmter KI-Systeme für manipulative, ausbeuterische, soziale Kontroll- oder Überwachungspraktiken, die ihrem Wesen nach gegen die Grundrechte und die Werte der Union verstoßen. Darunter fallen beispielsweise KI zur Vorhersage kriminellen Verhaltens, Emotionserkennung an Arbeitsplätzen und in Bildungseinrichtungen aber auch Überwachungskameras der Polizei, die mit KI-basierten Gesichtserkennungstechnologien ausgestattet sind, um gesuchte Personen zu identifizieren.[12] Verboten ist insbesondere, „Datenbanken für die Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder aus Videoüberwachungsaufnahmen [zu] erstellen oder [zu] erweitern".

Ein von AlgorithmWatch beauftragtes technisches Gutachten von Professor Dirk Lewandowski von der Hochschule für Angewandte Wissenschaften Hamburg kommt zudem zu dem Schluss, dass ein praktikabler biometrischer Abgleich mit Bildern aus dem Internet nicht ohne Datenbanklogik funktioniert.[13] Bilder müssten gesammelt, vorverarbeitet, indexiert und für spätere Suchen strukturiert werden. Der Wissenschaftliche Dienst des Deutschen Bundestages hat ebenfalls festgehalten, dass ein sinnvoller, praktikabler automatisierter Abgleich mit öffentlich zugänglichen Internetbildern ohne entsprechende Datenbanken nicht umsetzbar ist.[14] Es ist also technisch nicht umsetzbar, frei verfügbare Bilder aus dem Internet für einen Abgleich praktikabel durchsuchbar zu machen, ohne eine Datenbank zu erstellen.

Damit steht § 43a im Konflikt mit europäischem KI-Recht. Soweit ein biometrischer Internetabgleich praktisch auf den Aufbau, die Nutzung oder die Erweiterung durchsuchbarer biometrischer Datenbestände hinausläuft, steuert er genau in die Logik hinein, die der AI Act verbietet. Das ist kein Zufall, sondern Ausdruck der Einsicht, dass bestimmte KI-Praktiken schon ihrer Natur nach Grundrechte gefährden. Das sollte der Thüringer Gesetzgeber nicht ignorieren.

---

11 National Institute of Standards and Technology: *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, 19.12.2019, aktualisiert am 03.02.2025, online abrufbar unter: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

12 Verordnung (EU) 2024/1689 über künstliche Intelligenz (AI Act), Art. 5; siehe ergänzend: Europäische Kommission: *AI Act Service Desk – Article 5: Prohibited AI practices*, online abrufbar unter: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-5

13 AlgorithmWatch: *Braucht die Polizei eine Datenbank zum biometrischen Abgleich?*, Gutachten von Prof. Dr. Dirk Lewandowski, 15.10.2025, online abrufbar unter: https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/

14 Wissenschaftliche Dienste des Deutschen Bundestages: *Biometrischer Abgleich mit Bildern aus dem Internet*, WD 5 – 105/25 / EU 6 – 074/25, 22.01.2026, online abrufbar unter: https://www.bundestag.de/resource/blob/1149732/EU-6-074-25-WD-5-105-25.pdf

Digitalcourage fordert deshalb: Kein biometrischer Abgleich mit öffentlich zugänglichen Internetdaten. Keine Gesichtersuchmaschine. Kein Stimmabgleich mit Internetmaterial. Keine polizeiliche Infrastruktur, die aus öffentlicher Sichtbarkeit biometrische Verfolgbarkeit macht.

Zusammenführung von Daten aus verschiedenen Quellen zur Palantir-artigen automatisierten Datenanalyse (§ 40a ThürPAG-E)

Besonders alarmierend ist außerdem die vorgesehene anlassbezogene automatisierte Datenanalyse, also eine Palantir-artige Verknüpfung und Auswertung großer Datenbestände. Das Problem ist nicht der Name Palantir. Das Problem ist das Konzept: Daten aus verschiedenen Quellen werden zusammengeführt, verknüpft, analysiert und in polizeiliche Handlungsmöglichkeiten übersetzt.

Das Bundesverfassungsgericht hat 2023 die Regelungen in Hessen und Hamburg zur automatisierten Datenanalyse durch die Polizei für verfassungswidrig erklärt beziehungsweise aufgehoben.[15] Es hat zugleich klargestellt, dass automatisierte Datenanalyse einen eigenständigen Grundrechtseingriff darstellt. Die Botschaft war klar: Solche Systeme sind nur unter sehr strengen und engen Grenzen überhaupt denkbar.

Dabei reicht es nicht, nur auf Einzelfälle zu schauen. Schon der Effizienzgewinn solcher Systeme verändert das Machtverhältnis zwischen Bürger*innen und Staat. Was früher aufwendig, langsam oder praktisch unmöglich war, kann plötzlich automatisiert, schnell und in großem Umfang geschehen. Genau dadurch entsteht die neue Eingriffsqualität.

Der frühere Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beschreibt für VeRA und ähnliche Systeme, dass unterschiedliche polizeiliche und externe Datenbanken angebunden, zusammengeführt, verknüpft und ausgewertet werden können.[16] Betroffen sind dabei keineswegs nur Beschuldigte. Polizeiliche Datenbestände enthalten auch Daten von Opfern, Zeug*innen, Hinweisgeber*innen, Anzeigeerstatter*innen und anderen unbeteiligten Dritten. Wer also von „Polizeidaten“ spricht, spricht nicht von einer sauberen Liste tatsächlich gefährlicher Personen. Er spricht von Datenbeständen, die aus Verdächtigungen, Kontakten, Hinweisen, früheren Kontrollen, Zeugenaussagen und Zufallsfunden bestehen.

Gerade darin liegt die demokratische Gefahr. Polizeidaten sind keine neutrale Abbildung von Kriminalität. Sie spiegeln auch bisherige Kontrollpraxis wider. Wenn bestimmte Viertel stärker kontrolliert werden, entstehen dort mehr polizeiliche Daten. Wenn bestimmte Gruppen häufiger

---

15 Bundesverfassungsgericht: Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 – zur automatisierten Datenanalyse durch die Polizei, online abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

16 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: *Stellungnahme bezüglich der polizeilichen Analyse-Software Bundes-VeRA*, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.04.2024, 16.04.2024, online abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN-polizeiliche-Analysesoftware.html

überprüft werden, tauchen sie häufiger in Datenbanken auf. Wenn diese Daten dann automatisiert analysiert werden, reproduziert und verstärkt das System bestehende Selektionsmuster. Die Technik gibt ihnen nur einen scheinbar objektiven Anstrich.

So entsteht eine selbsterfüllende Prophezeiung: Wo die Datenanalyse Gefahren vermutet, wird stärker kontrolliert. Wo stärker kontrolliert wird, werden mehr Verstöße gefunden. Diese Funde bestätigen anschließend die vermeintliche Prognose. Am Ende wirkt die Maschine treffsicher, obwohl sie bestehende Ungleichheiten nur verstärkt.

Auch hier gilt: Eine menschliche Nachkontrolle löst das Problem nicht automatisch. In der Praxis genießen technische Systeme oft einen Vertrauensvorschuss. Was die Software ausgibt, wirkt objektiv, präzise und neutral. Gerade deshalb besteht die Gefahr, dass maschinelle Treffer nicht kritisch hinterfragt, sondern als Ausgangspunkt weiterer Maßnahmen genutzt werden. Die Verantwortung verschiebt sich: vom konkreten Verdacht zur statistischen Wahrscheinlichkeit, von überprüfbaren Tatsachen zu intransparenten Mustern.

Wer glaubt, das sei nur eine theoretische Zukunftsfrage, verharmlost den Ist-Zustand. Software des Unternehmens Palantir Technologies wird im polizeilichen Bereich bereits in mehreren Bundesländern genutzt, etwa als HessenData, DAR und VeRA. Gleichzeitig gehört zu den verbotenen Praktiken des AI Act, dass KI-Systeme untersagt sind, die das Risiko einer Straftat allein auf Grundlage von Profiling oder Persönlichkeitsmerkmalen bewerten oder vorhersagen. Genau dort liegt aber die politische Versuchung solcher Plattformen: aus Daten scheinbar objektive Vorhersagen zu machen und Menschen rein statistisch zu verdächtigen. Was technisch nach Mustererkennung klingt, ist demokratisch eine Machtverschiebung – weg von nachvollziehbaren Tatsachen, hin zu rein statistischen Verdächtigungen. Auch hier steht die geplante Regelung im Konflikt mit EU-Recht.

International lässt sich beobachten, wohin solche Infrastrukturen führen können, wenn sie mit repressiver Politik verbunden werden. Bei Razzien und Abschiebungsoperationen der US-Einwanderungsbehörde ICE kommt zunehmend Software von Palantir zum Einsatz. Recherchen von „WIRED“ und dem „Guardian“ zeigen, dass ICE mithilfe von Palantir-Systemen große Datenmengen aus unterschiedlichen Behördenquellen zusammenführt, um Zielpersonen zu identifizieren, Aufenthaltsorte zu bestimmen und Razzien zu koordinieren.[17][18] Besonders umstritten ist dabei das System „ImmigrationOS“ beziehungsweise das Tool „ELITE“. Dabei handelt es sich um Analyseplattformen, die Daten aus Polizeidatenbanken, Visa- und Grenzbehörden, Telefonnummern, Fahrzeugregistern oder Social-Media-Bezügen zusammenführen und grafisch verknüpfen können. So lassen sich Bewegungsprofile, soziale Kontakte oder mögliche Aufenthaltsorte einzelner Personen automatisiert darstellen und für operative Einsätze nutzbar machen. Ein Bericht des Office of the United Nations High Commissioner for Human Rights dokumentiert für den Iran den Einsatz von ähnlichen

17 Caroline Haskins/Makena Kelly: *ICE Is Using Palantir's AI Tools to Sort Through Tips*, WIRED, 28.01.2026, aktualisiert am 29.01.2026, online abrufbar unter: https://www.wired.com/story/ice-is-using-palantirs-ai-tools-to-sort-through-tips/

18 The Guardian: *Documents offer rare insight on ICE's close relationship with Palantir*, 22.09.2025, online abrufbar unter: https://www.theguardian.com/us-news/ng-interactive/2025/sep/22/ice-palantir-data

Überwachungsinstrumenten zur Kontrolle von Frauen im öffentlichen Raum.[19]

Das heißt nicht, Thüringen mit dem Iran und den USA gleichzusetzen. Aber demokratische Grenzüberschreitungen werden nicht erst dann problematisch, wenn der Endzustand erreicht ist: Freiheitsfeindliche Systeme fallen nicht plötzlich vom Himmel. Sie werden schrittweise eingeführt, jeweils mit einem guten Zweck legitimiert und stehen später bereit, wenn politische Mehrheiten kippen oder der Anwendungsbereich still ausgeweitet wird. Wer meint, das seien überzogene Bedenken, sollte sich vergegenwärtigen, wohin biometrische und digitale Überwachung in autoritären Kontexten führen kann. Ob die Software dann Palantir heißt oder eine deutsche oder europäische Anwendung ist, die als „digital-souverän" vermarktet wird, ändert nichts an der autoritären Logik dahinter.

Besonders gefährlich ist die Gewöhnung. Ist eine solche Software einmal beschafft und organisatorisch eingebunden, sinkt die Schwelle ihres Einsatzes. Aus der Ausnahme wird ein praktisches Werkzeug. Aus dem schweren Grundrechtseingriff wird ein Mausklick im Polizeialltag. Aus der begrenzten Analyse wird der Wunsch nach mehr Daten, mehr Schnittstellen, mehr Trefferquote. Genau diese Dynamik muss der Gesetzgeber verhindern, bevor sie entsteht.

§ 40a darf nicht zur Hintertür für digitale Rasterfahndung werden. Digitalcourage lehnt die vorgesehene automatisierte Datenanalyse in dieser Form ab. Eine demokratische Polizei darf nicht auf undurchsichtige maschinelle Mustererkennung vertrauen.

Fazit

Der falsche Weg beginnt nicht erst mit einer offen autoritären Regierung. Er beginnt früher: Wenn Überwachung normalisiert, automatisiert und politisch verharmlost wird. Genau darum geht es hier. Nicht um eine einzelne Kamera, nicht um ein einzelnes Analysewerkzeug, nicht um ein isoliertes Softwareprodukt. Es geht um die Frage, welche Art von Gesellschaft wir sein wollen.

Wollen wir in einer Demokratie leben, in der Menschen sich im öffentlichen Raum bewegen können, ohne permanent bewertet zu werden? In der ein gepostetes Foto nicht in einer staatlichen Datenbank landet? In der Polizeiarbeit an konkrete Tatsachen gebunden bleibt – statt an maschinell erzeugte Verdächtigungen? Oder wollen wir sehenden Auges eine Infrastruktur schaffen, die aus Freiheit und Unangepasstheit einen Risikofaktor macht?

Digitalcourage empfiehlt dem Thüringer Landtag, die Regelungen zu § 33a, § 43a und § 40a aus dem Entwurf zu streichen. Aus unserer Sicht braucht es keine Ausweitung, sondern klare rote Linien:

Keine KI-gestützte Verhaltensanalyse im öffentlichen Raum. Keine biometrische Identifizierung über öffentlich zugängliche Internetdaten. Keine Palantir-artige Massenverknüpfung polizeilicher Datenbestände. Keine biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum. Keine Schleppnetzlogik gegen Hunderttausende Unbeteiligte.

---

19 Office of the United Nations High Commissioner for Human Rights: *Report of the independent international fact-finding mission on the Islamic Republic of Iran*, UN Human Rights Council, A/HRC/58/63, 2025, online abrufbar unter: https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session58/advance-version/a-hrc-58-63-auv.docx

Diese roten Linien sind kein technikfeindlicher Sonderweg. Sie stehen im Einklang mit der verfassungsgerichtlichen Rechtsprechung zur automatisierten Datenanalyse und mit der europäischen Regulierung besonders gefährlicher KI-Praktiken. Der Rechtsstaat muss nicht alles technisch Machbare erlauben. Im Gegenteil: Seine Aufgabe ist es, Macht zu begrenzen.

Schon die bestehende Überwachungsgesamtrechnung ist eine deutliche Mahnung gegen weitere Überwachungspläne: Bereits heute ist das Netz staatlicher Überwachungsbefugnisse so dicht und komplex, dass seine Gesamtwirkung kaum noch demokratisch überschaubar ist.[20] Die vom Max-Planck-Institut 2025 vorgelegte Pilotstudie hat mehr als 3.200 gesetzliche Überwachungsbefugnisse ausgewertet und kommt zu dem Befund, dass die sicherheitsrechtlichen Befugnisnormen insgesamt hoch komplex sind.. Wer unter diesen Bedingungen neue Befugnisse schafft, darf nicht so tun, als gehe es um isolierte Einzelmaßnahmen. Jede neue Kameraanalyse, jede neue Datenverknüpfung, jede neue biometrische Identifizierung kommt zu einem bereits bestehenden Überwachungsgefüge hinzu. KI-gestützte Verhaltensscanner, Palantir-artige Datenanalysen und biometrische Identifizierung verschärfen dieses Problem noch einmal erheblich: Sie machen Überwachung nicht nur umfassender, sondern auch undurchschaubarer. Denn solche Systeme beobachten nicht bloß, sie bewerten, verknüpfen, sortieren und erzeugen Verdachtsmomente, oft auf eine Weise, die für Betroffene, Öffentlichkeit, Parlamente und Gerichte kaum noch nachvollziehbar ist. Welche Auswirkungen das bereits jetzt auf unsere Demokratie hat, ist kaum mehr durchschaubar. Genau deshalb braucht es keine weitere Aufrüstung, sondern Grenzen, Kontrolle und Rückbau.

Sicherheit entsteht nicht durch immer tiefere Eingriffe in Freiheitsrechte. Sicherheit entsteht auch nicht dadurch, dass man technische Aufrüstung mit politischer Handlungsfähigkeit verwechselt. Wirksamer Schutz braucht Opferschutz, Prävention, soziale Infrastruktur, Beratung, Personal, rechtsstaatliche Kontrolle und eine Polizei, die an Grundrechte gebunden bleibt.

Grundrechte sind nicht das Hindernis einer demokratischen Sicherheitsordnung. Sie sind ihre Voraussetzung. Was wir brauchen, ist eine Politik, die Grundrechte nicht als Hindernis betrachtet, sondern als Maßstab.

---

20 Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, *Überwachungsgesamtrechnung für Deutschland. Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden. Band 1: Bericht*, Freiburg 2025, abrufbar unter: https://pure.mpg.de/rest/items/item_3649030/component/file_3649042/conten