



Chaos Computer Club
Krautspace Jena
Bytespeicher Erfurt
Netz39

Stellungnahme zum Polizeiaufgabengesetz Thüringen

Gesetzentwurf der Landesregierung, Drucksache 8/2478

Constanze Kurz, Jens Kubieziel

24. Mai 2026

Vorbemerkung.....	3
Automatisierte Datenanalyse.....	3
Besondere Gefährlichkeit.....	3
Missachtung grundrechtlicher Vorgaben.....	3
Keine Vorgaben zur tatsächlich eingesetzten Software	5
Verhaltensscanner	6
Detektion ungewünschter Verhaltensmuster.....	7
Abweichende Bewegungsmuster markieren.....	8
Wissenschaftliche Erkenntnisse zur Videoüberwachung.....	8
Biometrische Suche.....	9
Staatstrojaner.....	10
Fazit	11

Vorbemerkung

Im Gesetzentwurf zum Polizeiaufgabengesetz Thüringen sind einige neue polizeiliche Befugnisse geregelt. Diese werfen Fragen zu Grundrechten und zur Zweckbindung, aber auch zur Transparenz, zu effektiver Kontrolle und zu den tatsächlichen technischen Realitäten auf. Diese gemeinsame Stellungnahme widmet sich vor allem rechtlichen und technischen Gesichtspunkten der automatisierten Datenanalyse, der Verhaltensscanner und der biometrischen Suche sowie dem Einsatz von Staatstrojanern. Auch einige Szenarien aus dem Fragenkatalog werden bewertet.

Automatisierte Datenanalyse

Besondere Gefährlichkeit

Mit dem § 40a des Entwurfes soll erstmals die gesetzliche Grundlage für eine automatisiert arbeitende Datenanalyseplattform bei der Polizei Thüringen geschaffen werden. Diese automatisierte Datenanalyse ist ohne Zweifel ein besonders intensiver Eingriff in Grundrechte zahlreicher Menschen. Die Analyseplattform soll Datenbank-, datei- und formatübergreifend vorhandene Daten dauerhaft zusammenführen und aufbereiten.

Das Ergebnis dieser permanenten Zusammenführung, Verknüpfung und Aufbereitung soll genutzt werden, um mit Such- und Analysefunktionen der Plattform möglichst neue Erkenntnisse aus den Daten zu gewinnen. Diese Auswertung massenhafter Datenbestände kann Menschen und ihr Verhalten profilieren und sogar tiefgreifende Persönlichkeitsprofile erzeugen.

Der Grundsatz der Zweckbindung wird durch die dauerhafte Verknüpfung und Analyse der Daten unterminiert. Ein effektiver Rechtsschutz ist wegen der heimlich ablaufenden Analyse kaum möglich.

Die automatisierte Datenanalyse stellt ein drastisches Risiko für die Rechte auf Nicht-Diskriminierung dar. Die Diskriminierungsanfälligkeit dieser Form von Auswertung ergibt sich daraus, dass die zugrundeliegenden Polizeidaten bereits Verzerrungen im Sinne von institutionellen Vorurteilen aufweisen. Wie aber eine Diskriminierung von Menschen bei der Analyse ausgeschlossen werden soll, adressiert der Gesetzentwurf gar nicht.

Missachtung grundrechtlicher Vorgaben

Aufgrund der Fülle der Datenquellen ist unvermeidbar, dass auch zahlreiche Informationen von völlig unbescholtenen Personen in die Analyse einfließen. Insbesondere durch den Einbezug der Vorgangs- und Fallbearbeitungssysteme werden sehr viele Menschen erfasst, die keinerlei Anlass gegeben haben, von Software analysiert zu werden. Es werden also permanent nicht nur Daten von Verdächtigen miteinander verbunden und gerastert, sondern auch von völlig unverdächtigen Menschen, deren Daten aus ganz alltäglichen Gründen in Polizeidatenbanken eingeflossen sind.

Es sind in § 40a Absatz 1 des Entwurfes zur Gefahrenabwehr keine Datenquellen der Polizei vorgesehen, die explizit ausgesondert werden sollen, etwa wegen des weitreichenden Grundrechtseingriffs bei der ursprünglichen Datenerhebung. Selbst Daten aus Wohnraumüberwachungen und Staatstrojanereinsätzen („Online-Durchsuchung“, „Quellen-TKÜ“) dürfen in die automatisierte Analyse einfließen. Diese sind lediglich an höhere Hürden (Vorliegen einer dringenden Gefahr) gebunden. Das bedeutet auch, dass nach Absatz 1 nicht ausgeschlossen werden kann, dass Daten aus dem besonders geschützten Kernbereich der privaten Lebensgestaltung einbezogen werden.

Die in § 40a Absatz 1 des Entwurfes formulierte automatisierte Datenanalyse kann zur Abwehr einer Gefahr nach Maßgabe des § 39 eingesetzt werden. Das Bundesverfassungsgericht gab in seinem Urteil vom 16. Februar 2023¹ vor, dass derartige Eingriffe nur zu rechtfertigen sind, wenn mindestens eine hinreichend konkretisierte Gefahr besteht. Nur für den Bereich der Wohnraumüberwachung und für den Staatstrojaner als „Online-Durchsuchung“ wird das an das Vorliegen einer dringenden Gefahr geknüpft. Insofern bleibt der Entwurf hinter den Vorgaben des Bundesverfassungsgerichts zurück.

Nicht einfließen nach 40a Absatz 2 in die weitergehende Anwendung der automatisierten Datenzusammenführung sollen hingegen DNA-Daten, biometrische Daten in Form von Finger- und Handflächenabdrücken, Audio- und Videodateien sowie Daten aus Wohnraumüberwachungen und von Einsätzen von Staatstrojanern.

Die Datenanalyse soll dabei ohne selbstlernende Systeme und ohne Formen der automatisierten Entscheidungsfindung durchgeführt werden. Möglich ist aber der Einbezug von Daten aus dem Internet, was indirekt und nicht automatisiert geschehen darf. Durch diese Erlaubnis, zusätzlich solche Daten in das System zu importieren, steigt potentiell die Anzahl der von der Datenanalyse betroffenen Menschen nochmals erheblich.

Der Entwurf von § 40a Abs. 2 lehnt sich an das Urteil vom 16. Februar 2023 an, in Rn 176 werden dort Bedingungen für den Einsatz einer automatisierten Datenanalyse formuliert. Der Entwurf erfüllt diese Bedingungen nicht oder nur zum Teil.

Während das Urteil auf besonders schwere Straftaten im Sinne des § 100b Abs. 2 StPO abstellt, fehlt dem Gesetzentwurf der Verweis auf den Katalog. Stattdessen wird im Entwurf von „besonders schweren Straftaten“ gesprochen. Das hat den Nachteil, dass Spielraum für Auslegungen bleibt.

Der Gesetzentwurf verlangt das Vorliegen „tatsächlicher Anhaltspunkte“, das Bundesverfassungsgericht in seinem Urteil jedoch „genügend konkretisierte Tatsachen“. Auch hier wird deutlich von den Vorgaben des Urteils abgewichen.

Schließlich spricht das Urteil in Rn 176 von Straftaten, „die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden“. Diese Qualifizierung fehlt dem Absatz 2 gänzlich.

¹ BVerfGE 165, 363 - 442.

Insgesamt bleibt auch der Absatz 2 des Entwurfes deutlich hinter den Vorgaben des Urteils des Bundesverfassungsgerichts zurück und schwächt somit die Grundrechte der Betroffenen übermäßig.

Keine Vorgaben zur tatsächlich eingesetzten Software

Die Norm zur anlassbezogenen automatisierten Datenanalyse macht keine Vorgaben zur tatsächlich eingesetzten Software. Damit sind alle Varianten denkbar, von einer Eigenentwicklung innerhalb der Polizeibehörden über eine Fremdbeauftragung bis hin zum Kauf einer „fertigen“ Software. Auch lässt der Entwurf offen, ob die Software auf eigenen Systemen und unter vollständiger Kontrolle der Polizei betrieben oder ob eine Software gemietet wird, die dann von Drittanbietern betrieben wird.

Bei der Verarbeitung personenbezogener Daten, die bei automatisierter Datenanalyse einen schwerwiegenden Grundrechtseingriff darstellt, stellen sich Fragen der Nachvollziehbarkeit, der Möglichkeiten zur Aufdeckung von Fehlklassifikationen oder Verzerrungen und der datenschutzrechtlichen Kontrolle der Software. Wenn die Software im eigenen Haus entwickelt wird, besteht die Möglichkeit, sie eng an den Anforderungen und gesetzlichen Erfordernissen zu führen. In diesem Fall ist es jederzeit möglich, anhand von Quellcode, Dokumentation und der im Einsatz befindlichen Softwareversion die Funktionsweise der Software nachzuvollziehen und Kontrollinstanzen Zugang zu gewähren. Dadurch kann ein adäquater Schutz der Grundrechte der betroffenen Personen gewährleistet und Missbrauch oder Fehler aufgedeckt werden.

Wird hingegen Software von Fremdanbietern eingesetzt, entweder gekauft und auf eigenen IT-Systemen betrieben oder als Mietmodell, muss entsprechender Aufwand betrieben werden, um ein ähnliches Schutzniveau zu gewährleisten. Zu fordern ist dann:

- ♦ Der Quellcode der Software muss vorliegen und von unabhängiger fachkundiger Stelle geprüft werden.
- ♦ Es muss sichergestellt sein, dass der vorliegende und geprüfte Quellcode korrekt in ausführbaren Programmcode überführt wurde. Durch diesen Schritt kann ausgeschlossen werden, dass unbemerkt Zusatzcode hinzugefügt oder entfernt wurde.
- ♦ Schließlich ist sicherzustellen, dass auch genau der zuvor geprüfte ausführbare Code zum Einsatz kommt.

Diese Schritte sind vor jeder Aktualisierung oder wesentlichen Änderung der Software erneut auszuführen. Dadurch wäre es möglich, die Funktionsweise der Software nachzuvollziehen und bei Kontrollen entscheiden zu können, ob sie den Anforderungen des Grundrechtsschutzes und der gesetzlichen Schranken genügt.

Im Leitsatz 5b des Urteils des Bundesverfassungsgerichts vom 16. Februar 2023 wird die Festlegung, Dokumentation und Veröffentlichung abstrakt-genereller Vorgaben gefordert. Diese sollen dann durch andere Instanzen, insbesondere durch Datenschutzbeauftragte geprüft werden können. Eine solche Kontrolle kann nur erfolgen, wenn die Software dies ermöglicht, also mindestens die oben aufgeführten Forderungen erfüllt.

Der § 40a Abs. 5 lit. 2 des Entwurfes verbietet den Einsatz selbstlernender oder „lernfähiger“ Systeme. Damit ist Software ausgeschlossen, deren innere Mechanismen sich fortlaufend und damit nur schwer kontrollierbar ändern. Die verbleibende „deterministische“ Software garantiert technisch Wiederholbarkeit. Allerdings hat dies wenig Einfluss auf die Nachvollziehbarkeit, denn Software mit komplexen Funktionen und Mustererkennung bleibt schwer nachvollziehbar.

Im Allgemeinen ist eine Kontrolle nur möglich, wenn der Anbieter Quellcode, Konfiguration und weitere Parameter zur Verfügung stellt. Ohne diese Angaben ist eine wirksame Kontrolle de facto ausgeschlossen. Wie oben angemerkt, ist aber auch unter Zurverfügungstellung dieser Daten eine Kontrolle anspruchsvoll.

Die Beispiele aus Hessen („HessenDATA“) und Bayern („VeRA“) zeigen, dass bisher eine Kontrolle nur aus einer Jahre zurückliegenden einmaligen Sichtung des Quellcodes des Software-Anbieters besteht,² dass sie aber nicht dauerhaft durchgeführt wird und dass die Systeme der automatisierten Datenanalyse auch nach Updates mit signifikanten Änderungen ohne neuerliche Sichtung weiter betrieben werden.

Verhaltensscanner

Die Befugnisse zur Auswertung der Videoüberwachung sollen um automatisch arbeitende Verhaltensscanner mit Live-Beobachtung erweitert werden. Dabei sollen mit Hilfe von Software Verhaltensmuster erkannt werden, die „auf die Entstehung einer Gefahrensituation oder die Begehung einer Straftat hindeuten“. Zu denken ist etwa an die Erkennung von Einbrüchen, Diebstählen, Vandalismus, Unfällen oder Angriffen gegen Menschen. Der Gesetzentwurf enthält keine konkreten Anhaltspunkte, welche ungewöhnlichen Verhaltensmuster damit gemeint oder gerade nicht gemeint sind oder was als Anomalie definiert ist.

Offenbar soll „unverzüglich“ nach einer automatischen Detektion einer Situation, die auf eine Gefahr oder eine Straftat „hindeutet“, ein Polizeibediensteter prüfen, ob tatsächlich eine Gefahr bevorsteht. Nach dem Gesetzentwurf ist ein sofortiges Reagieren auf Anomalie-Meldungen der Verhaltenserkennungssoftware vorgesehen. Welchen Fehlerquoten dabei als realistisch angenommen werden, bleibt offen.

Fällt dann die Bewertung des Polizeibediensteten in Bezug auf ein Risiko oder die Wahrscheinlichkeit einer Straftatbegehung „in absehbarer Zeit“ positiv aus, soll neben der stetig auswertenden Video-Beobachtung noch ein weiterer automatisierter Prozess starten: Die detektierten involvierten Personen sollen in der Software gekennzeichnet und nachverfolgt werden.

Das in Frage 44 des Fragenkatalogs beschriebene Szenario erscheint durchaus im Bereich des Möglichen. Es kommt bei Systemen zur Verhaltenserkennung zu zahlreichen Fehldetektionen. Der § 33 Abs. 4 verlangt in Satz 2 nur, dass das System ein Muster „erkennt“, was auf die „Entstehung einer Gefahrensituation

² Vgl. die Prüfung der bayerischen Software-Variante durch das Fraunhofer-Institut SIT 2023, Drs 19/7043 des Bayerischen Landtags, https://www.bayern.landtag.de/www/ElanTextAblage_WP19/Drucksachen/Schriftliche%20Anfragen/19_0007043.pdf vom 7. Juni 2025, abgerufen am 18. Mai 2026.

oder die Begehung einer Straftat hindeutet“. Satz 4 legt dann die Verantwortung in die Hände des betrauten Beamten. Dieser muss prüfen, ob „in absehbarer Zeit mit hinreichender Wahrscheinlichkeit“ mit der Begehung von Straftaten gerechnet werden muss.

In der Praxis ist zu beobachten, dass sich Menschen auf Entscheidungen eines Computers verlassen und diese „durchwinken“ (sog. Automation Bias). Gerade bei der öffentlich geführten Diskussion um die sogenannte Künstliche Intelligenz ist zu erwarten, dass die Entscheidungen des Auswertungssystems als gegeben akzeptiert werden.

Selbst wenn der beobachtende Beamte die Entscheidungen kritisch bewerten sollte, enthält das Gesetz keine Beschränkungen, wie etwa eine Prüfung durch einen Vorgesetzten oder Richter. Damit obliegt die Entscheidung allein dem Polizeibediensteten. Nun erlaubt der Satz 5 die automatisierte Nachverfolgung bis hin zum Fahrzeug der Person. Insgesamt ist das beschriebene Szenario der Frage 44 des Fragenkatalogs im Rahmen des Gesetzentwurfs denkbar.

Der Gesetzentwurf geht nicht auf die gesetzlichen Regelungen im Artificial Intelligence Act der Europäischen Union (KI-Verordnung) ein, die jedoch Einschränkungen für die Nutzung von Verhaltensscannern vorschreiben.

Detektion unerwünschter Verhaltensmuster

Verhaltenserkennung gründet technisch typischerweise auf einer komplexen räumlichen Echtzeit-Analyse der Bewegungsmuster von Objekten und Personen, ihren Körperteilen und Interaktionen zwischen diesen Objekten und Personen sowie gleichzeitiger Gestenerkennung. Dazu werden oft synthetische Datensätze oder Video-Sequenzen von tatsächlichen Interaktionen zwischen Menschen herangezogen und analysiert, um „unauffällige“ von unerwünschten oder illegalen Verhaltensmustern zu trennen. Solche Analysen werden technisch seit einigen Jahren auch als kommerzielle Produkte angeboten.

Die Fehleranfälligkeit der Verhaltenserkennung ist hoch, die sichere korrekte Erkennung unerwünschter Verhaltensmuster oft nicht nachgewiesen.³ Die technischen Herausforderungen bestehen vor allem darin, die komplexen Bewegungsmuster von Menschen korrekt zu bewerten und mit gegenseitigen und teilweise starken Verdeckungen in gefüllten oder überfüllten städtischen Räumen und mit wechselnden Belichtungen dieser Räume umzugehen.

Insgesamt sind nicht nur die technischen Erkennungsaspekte herausfordernd, es mangelt auch an handfesten Belegen zu den tatsächlichen Erkennungsleistungen. Der Bereich ist wissenschaftlich wenig erforscht und geprägt von Marketing-Versprechen kommerzieller Anbieter.

Die dem Gesetzentwurf zugrundeliegende Vorstellung, was eine automatisierte Verhaltenserkennung technisch leisten kann, ist übertrieben und nicht mit der Realität in Einklang zu bringen. Entsprechend ist in hohem Maße zweifelhaft, ob

³ Vgl. M. Liu, H. Liu, et. al.: 3D Skeleton-Based Action Recognition: A Review, <https://arxiv.org/pdf/2506.00915> vom 1. Juni 2025, abgerufen am 18. Mai 2026.

das Ziel der Gefahrenabwehr und der Verbesserung der Effizienz polizeilicher Maßnahmen mit Verhaltensscannern erreicht werden kann.⁴

Abweichende Bewegungsmuster markieren

Software, die auf typische Bewegungen von Menschen trainiert wird, soll und muss zwangsläufig abweichende Bewegungsmuster markieren. Es kann als „auffällig“ oder „verdächtig“ markiert werden, wenn Menschen etwa bestimmte Posen einnehmen oder eine Geste wie High five oder Winken ausführen.

Das Fokussieren auf untypisches Verhalten bedeutet zugleich, dass Menschen, die vom vermeintlich normalen Verhalten in ihren Bewegungsmustern abweichen, von der Software häufiger als auffällig gekennzeichnet werden. Praktisch ist an Menschen zu denken, die ungleichgewichtig, stockend oder schwankend gehen oder die Gehhilfen oder Rollstühle nutzen.

Entsprechend führt die Verhaltenserkennung zu Diskriminierung. Zugleich ist die Bewertung realer Anwendungen kaum wissenschaftlich untersucht.

Wissenschaftliche Erkenntnisse zur Videoüberwachung

Zur Frage nach wissenschaftlichen Erkenntnissen über Videoüberwachung ist die internationale Vergleichsstudie von Piza, Welsh, Farrington und Thomas maßgeblich.⁵ Dort wurden 80 Studien aus den letzten vierzig Jahren analysiert. Hierbei wurde festgestellt, dass eine alleinige Videoüberwachung zu keinem Rückgang von Straftaten führt. Erst in Verbindung mit begleitenden Maßnahmen wie besserer Beleuchtung oder Notrufsystemen waren Effekte zu beobachten. Diese Effekte spielten aber insbesondere bei Parkplätzen eine große Rolle. Gerade im Bereich von Innenstädten und Wohnhäusern war kein Effekt zu beobachten. Auf Gewaltkriminalität hatte Videoüberwachung keinen Einfluss.⁶

Den Befund bestätigt auch eine vom nordrhein-westfälischen Innenministerium beauftragte Studie: Das Kriminologische Forschungsinstitut Niedersachsen kam dort zu dem Ergebnis, dass ein allgemein kriminalitätsreduzierender Effekt der polizeilichen Videoüberwachung nicht nachgewiesen werden konnte.⁷

Im Allgemeinen leistet die Videoüberwachung allein keinen wissenschaftlich nachgewiesenen Effekt auf die Gefahrenabwehr. Wie die obige internationale

⁴ Siehe auch die praktischen Beispiele des Videoüberwachungssystems am Hansaplatz im Hamburger Stadtteil St. Georg oder den Prototyp, der seit 2018 in Mannheim getestet wird, vgl. Chaos Computer Club: Automatisierte Verhaltensüberwachung, <https://www.ccc.de/de/updates/2026/verhaltenueberwachung> vom 6. März 2026, abgerufen am 18. Mai 2026.

⁵ E. Piza, B. Welsh, D. Farrington, A. Thomas: CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis, https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1275&context=jj_pubs von 2019, abgerufen am 18. Mai 2026.

⁶ Vgl. auch Metastudie: Videoüberwachung schützt kaum vor Straftaten, <https://www.datenspeicherung.de/index.php/metastudie-videoueberwachung-schuetzt-kaum-vor-straftaten/> vom 18. April 2021, abgerufen am 18. Mai 2026.

⁷ Vgl. Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gemäß § 15a PolG NRW, https://kfn.de/wp-content/uploads/Forschungsberichte/FB_143.pdf von 2018, abgerufen am 18. Mai 2026.

Vergleichsstudie zeigt, können Einzeleffekte nur nachgewiesen werden, wenn die Videoüberwachung in ein größeres Konzept eingebettet wird.

In Bezug auf die geplante polizeiliche Videoüberwachung am Erfurter Anger fehlt ein solches Konzept. Nach dem Text der Frage 43 des Fragenkatalogs findet bereits ein signifikanter Anteil der dort verübten Gesamtstraftaten in jetzt schon videoüberwachten Bereichen statt. Gerade im Lichte der wissenschaftlichen Forschungsergebnisse ist nicht zu erwarten, dass eine zusätzliche, verstärkte Videoüberwachung nun einen positiven Effekt hätte. Somit ist das Mittel weder geeignet noch erforderlich.

Biometrische Suche

Der Gesetzentwurf soll die Nutzung einer biometrischen Gesichtserkennung ermöglichen, die Daten aus dem Internet einbezieht. Auch andere biometrische Daten dürfen abgeglichen werden: Vorgesehen ist explizit die Nutzung von Stimmen. Dazu sollen automatisiert solche öffentlich frei zugänglichen Bild-, Audio- oder Videodateien aus dem Internet durchforstet werden, die für jedermann ohne spezielle Registrierung sichtbar sind.

Die öffentlichen personenbezogenen Daten sollen für den biometrischen Abgleich zuvor technisch umgewandelt werden. Ohne diese Verarbeitung wäre eine Nutzung unmöglich, da sich laut Begründung „öffentlich zugängliche Daten in Format und Struktur von den in den polizeilichen Informationssystemen gespeicherten Daten unterscheiden“. Das bedeutet, dass sämtliche für den Abgleich herangezogenen Daten auch zuvor verarbeitet werden müssten.

Der Gesetzentwurf enthält keine Eingangsschwellen für den Einsatz des biometrischen Abgleichs. Es wird allgemein von einer „Gefahr“ gesprochen und diese nicht weiter qualifiziert. Im Weiteren ist von Leib, Leben und Freiheit als Eingangsschwelle die Rede. Auch diese wird nicht weiter qualifiziert. Damit wäre bereits bei einfachen Delikten die Eingriffsschwelle erreicht. Gerade bei Maßnahmen mit einem derart erheblichen Grundrechtseingriff muss es angemessene und spezifische Regelungen zum Schutz der Grundrechte geben.

In § 43a Abs. 1 des Entwurfes wird die Erhebung öffentlich frei zugänglicher personenbezogener biometrischer Daten sowie der nachträgliche Abgleich mit bereits bekannten biometrischen Daten erlaubt. Eine Begrenzung der zu erhebenden biometrischen Daten ist mit Ausnahme der Vorgaben des Abs. 3 nicht zu erkennen. Damit liegt die Grenze bei den technisch vorhandenen oder beschaffbaren Speichermöglichkeiten.

Biometrische Daten sind durch Art. 9 DSGVO bzw. Art. 10 JI-Richtlinie besonders geschützt.⁸ Der Art. 10 der JI-Richtlinie verlangt für die Verarbeitung von biometrischen Daten für Zwecke der Strafverfolgung und der Gefahrenabwehr eine unbedingte Erforderlichkeit sowie weitere Garantien. Dem Gesetzentwurf scheint dieser Schutzgedanke fern. Stattdessen wird auch eine massenhafte Erhebung dieser Daten erlaubt.

⁸ Vgl. auch Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg zu PimEyes, <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/> vom 21. Dezember 2022, abgerufen am 18. Mai 2026.

Neben den beiden obigen EU-Regelungen geht der Art. 5 Abs. 1 lit. e der KI-Verordnung auf Datenbanken zu Gesichtserkennung mittels ungezieltem Auslesen aus dem Internet ein und verbietet explizit diese Praktiken. Im vorliegenden Gesetzentwurf ist unklar, ob diese Regelungen überhaupt in die Betrachtungen eingeflossen sind. Je nach technischer Umsetzung droht ein Verstoß gegen die KI-Verordnung.

Neben den oben aufgeführten Punkten ist zu befürchten, dass Menschen wegen der weiträumigen Foto- und Videoaufnahmen von Polizeien ihre Grundrechte weniger wahrnehmen. Eine biometrische Gesichtserkennung kann Menschen einschüchtern und diesen Effekt verstärken.

Staatstrojaner

Nach 34a ist bisher der Einsatz von Staatstrojanern zur Gefahrenabwehr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen bereits erlaubt. Hinzugefügt werden sollen nun Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen, bei denen nun ebenfalls Hacking-Methoden zur laufenden Telekommunikationsüberwachung eingesetzt werden dürfen.

Die im Entwurf genannten „sonstigen Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ lassen enormen Spielraum für die Auslegung. Denn es sind sehr viele Arten von Anlagen mit einer unmittelbaren Bedeutung für das Gemeinwesen denkbar. So kämen öffentliche Straßen, Verwaltungsgebäude, technische Anlagen und vieles mehr in Betracht.

Damit wird der Rahmen für mögliche Einsätze der Staatstrojaner enorm ausgeweitet, ohne dass eine zusätzliche Kontrolle oder Evaluation der Maßnahme vorgesehen ist. Eine sachliche Begründung der Ausweitung fehlt.

Wegen der besonderen Gefahren, die von einem Einsatz eines Staatstrojaners ausgehen, müssen nach Abschluss jeder „Quellen-TKÜ“ die Betroffenen des infiltrierten Systems nicht nur über Beeinträchtigungen der Vertraulichkeit ihrer Telekommunikation, sondern auch über die Beeinträchtigung der Integrität ihres informationstechnischen Systems explizit unterrichtet werden.

Staatstrojaner sind als Werkzeuge nicht sofort einsetzbar und daher in der konkreten Gefahrenabwehr wenig sinnvoll. Denn bevor die Schadsoftware auf einem abzuhörenden informationstechnischen System installiert werden kann, müssen über dieses System Informationen zur passenden Konfiguration des Trojaners gesammelt werden. Jeder Trojaner muss speziell für den jeweiligen Einsatz zusammengebaut werden,

Diese zwingend notwendige Vorlaufzeit dient nicht nur der Anpassung an das Zielsystem, sondern auch der Gewinnung von Erkenntnissen darüber, ob das Hacking beim konkreten System überhaupt erfolgversprechend ist. Auch da dies keineswegs immer der Fall ist, ist die „Quellen-TKÜ“ kein gut geeignetes Mittel zur Gefahrenabwehr.

Der Einsatz staatlicher Schadsoftware hat neben den Folgen für den einzelnen Verdächtigen auch gesellschaftliche Auswirkungen, die sich aus der Ausnutzung

der Sicherheitslücken unvermeidbar ergeben. Behörden bekannt gewordene Sicherheitslücken sollten zum Schutz von Privatpersonen, der Wirtschaft und auch der eigenen Behördeninfrastruktur schnellstmöglich behoben werden.

Fazit

Die im Entwurf vorgesehene automatisierte Datenanalyse und damit dauerhafte Zusammenführung zahlreicher Datenbestände stellt einen besonders intensiven Grundrechtseingriff dar, der weit über bisherige polizeiliche Möglichkeiten der Datennutzung hinausgeht. Die einfließenden Daten sind in Art und Umfang kaum begrenzt. Ein solches daten- und methodenoffen definiertes System, das zu systematischen Fehlern und Diskriminierung von Menschen neigt, ist wegen der Streubreite nicht mit dem Grundrechtsschutz der vielen Betroffenen in Einklang zu bringen, da der Entwurf den Vorgaben des Bundesverfassungsgerichts nicht ausreichend Rechnung trägt.

Die im Entwurf vorgesehene Verhaltensüberwachung ist unter technischen Gesichtspunkten als kaum realistisches Wunschdenken zu klassifizieren. Videoüberwachung und insbesondere die geplanten Verhaltensscanner sind zur Gefahrenabwehr ungeeignet.

Massenhaft Fotos von Menschen aus dem Netz zusammenzuklauben und biometrisch auszuwerten, ist ebenfalls mit einer erheblichen Eingriffstiefe und zahlreichen Betroffenen verbunden. Die biometrische Suche mit automatisierter Massenauswertung ist abzulehnen.

Der Gesetzentwurf erlaubt eine ganze Reihe neuer technischer Methoden der Überwachung, die teilweise noch zu wenig wissenschaftlich erforscht sind, sowie die starke Ausweitung des verdeckten Zugriffs auf informationstechnische Systeme mit Staatstrojanern. Die vom Bundesverfassungsgericht angeregte Gesamtüberwachungsrechnung wäre schon wegen der teilweise heimlich und massenhaft erfolgenden und wegen der dauerhaften Überwachungsmethoden hier angezeigt.