

Biometrische Fernidentifizierung: Massenüberwachung statt Sicherheit

Die Gesetzesentwürfe zum sogenannten Sicherheitspaket sehen massenhafte biometrische Überwachung und Änderungen im Sicherheitsrecht vor. Die Ampelkoalition droht damit entgegen ihrem Anspruch auf Transparenz, Effektivität und EU-Rechtskonformität zu handeln. Biometrische Erkennung im öffentlichen Raum und im Internet bedeutet Massenüberwachung und gefährdet Grundrechte.

Dieses Factsheet bietet eine faktenbasierte Einordnung der Behauptungen und hilft bei der Bewertung des Sicherheitspakets. Es soll helfen, Populismus, verfassungswidrigen Vorschlägen und technisch nicht umsetzbaren Scheinlösungen entgegenzuwirken.

Für Rückfragen stehen Ihnen D64 (buero@d-64.org, 03057714256) oder das Bündnis Gesichtserkennung Stoppen (mail@digitale-freiheit.jetzt) zur Verfügung.

Biometrische Überwachung erhöht die öffentliche Sicherheit.

Der vermeintliche Sicherheitsgewinn steht in keinem Verhältnis zum massiven Eingriff in die Grundrechte. Biometrische Fernidentifizierungssysteme ermöglichen eine undifferenzierte Massenüberwachung, die mit Grundrechten in Konflikt steht. Sie verletzen das Recht auf Privatsphäre und informationelle Selbstbestimmung.

In der Sachverständigenanhörung im Bundestag warnt [Sarah Lincoln, Gesellschaft für Freiheitsrechte \(GFF\)](#), vor übereilten Maßnahmen, die das Land nicht sicherer machen werden. Denn mehr Sicherheit wird nicht durch populistische Maßnahmen erreicht, sondern durch Bildung, Prävention und psychosoziale Unterstützung. Kostspielige und grundrechtsfeindliche Überwachungstechnologien können von den eigentlichen Problemen ablenken.

[Prof. Dr. Katrin Höffler, Universität Leipzig](#), warnt im Verfassungsblog, dass Gesetzes- und Diskursverschiebungen sogar Radikalisierung verstärken können. In einigen Bereichen besitzen die Regelungen reinen Symbolcharakter und werden die Sicherheitsbehörden mit neuen Aufgaben belasten, die sie davon abhalten, ihren eigentlich wichtigen Tätigkeiten

nachzugehen. Für mehr echte Sicherheit müssen wir auf Maßnahmen setzen, die Grundrechte achten.

Die vorgeschlagenen Maßnahmen sind verhältnismäßig

Der Wunsch nach Maßnahmen zur Steigerung der Sicherheit ist aufgrund der Verunsicherung der Bevölkerung verständlich. Doch gerade dann sind spezifische Regelungen notwendig, die den Grundsatz der Verhältnismäßigkeit wahren. Die Befugnis zum biometrischen Abgleich des gesamten Internets mit Bildern und Stimmen von Tatverdächtigen oder gesuchten Personen greift in die Grundrechte sämtlicher Menschen im öffentlichen Raum unterschiedslos ein, ist daher unverhältnismäßig und beschädigt auch die Demokratie als Ganzes.

Denn Bundeskriminalamt und Bundespolizei sollen diese Befugnis nicht nur zur Bekämpfung von Terrorismus, sondern auch als neues Standardinstrument erhalten. Das Bundesamt für Migration und Flüchtlinge sogar ohne Anfangsverdacht einer Straftat, nur um die Identität von Personen festzustellen.

[Dr. Stephan Schindler, Universität Kassel](#), betont, dass potenziell alle Internetnutzer:innen betroffen seien, die hierfür mehrheitlich keinen Anlass gegeben hätten. Auch [Sarah Lincoln, GFF](#), meint, dass „überwiegend Grundrechte von Millionen, wenn nicht Milliarden von unbeteiligten Personen betroffen wären, die keinen Anlass für polizeiliche Überwachung gegeben haben.“

Der Einsatz ist mit Grundrechten vereinbar

Der Einsatz dieser Systeme im öffentlichen Raum kann nicht auf grundrechtskonforme Weise geschehen, sondern ist inhärent inkompatibel mit zentralen demokratisch garantierten Freiheiten. [Prof. Dr. Dennis-Kenji Kipker \(Universität Bremen\)](#) warnt vor einem „sicherheitsbehördlichen Daten-Supergau“ und der Annäherung an den „gläsernen Bürger“.

Solche Maßnahmen können „zu Einschüchterungseffekten führen“ ([Schindler, Universität Kassel](#)), die Menschen vom Wahrnehmen ihrer Grundrechte wie der Meinungsäußerungs- oder Versammlungsfreiheit abhalten. Denn auch nachträgliche biometrische Fernidentifikation ermöglicht zum Beispiel die Bildung umfassender Personenprofile.

Nunmehr hat das [Bundesverfassungsgericht entschieden](#), dass das BKA-Gesetz in Teilen verfassungswidrig ist, da die Speicherung von Daten nicht klar geregelt und in der bisherigen Form teilweise unverhältnismäßig ist. Die geplanten Maßnahmen würden weit über die bisherigen Regelungen hinausgehen. Anstatt nun sehenden Auges ein verfassungs- und europarechtswidriges Gesetzespaket in aller Eile durch das Parlament zu drücken, kann die Regierungskoalition die Frist des Bundesverfassungsgerichts zur Korrektur des BKA-Gesetz nutzen und zeigen, dass Sicherheitspolitik nicht aktionistisch und von rechten Scharfmacher*innen getrieben sein muss, sondern auch besonnen und innerhalb der Grenzen des verfassungsmäßig Möglichen betrieben werden kann.

Wir müssen jetzt Handlungsfähigkeit zeigen

Die Aushandlung von Freiheit und Sicherheit ist zu wichtig für Schnellschüsse. Es ist verständlich, dass man angesichts der Wahlerfolge von rechtsextremer Parteien handlungsfähig erscheinen möchte. Doch anstatt sich von der AfD jagen zu lassen, gilt es besonnen zu handeln. Gute Politik braucht Zeit für Beratung mit Expert:innen und politische Aushandlungsprozesse.

Es gibt keinen Grund, warum Grundrechte im Hauruckverfahren eingeschränkt werden müssen. In den Worten der [BfDI Louisa Specht-Riemenschneider](#): „Es hilft niemandem, wenn Sie heute ein Gesetz machen, was morgen in Karlsruhe kassiert wird.“ Auch [Prof. Dr. Clemens Arzt, Hochschule für Wirtschaft und Recht Berlin](#), spricht von „Ignoranz in einem ohnehin schon überstürzten Gesetzgebungsverfahren“.

Missbrauch kann verhindert werden

Selbst gut gemeinte Gesetze können Missbrauch nicht verhindern. Die Geschichte zeigt, dass einmal geschaffene Überwachungsinfrastrukturen oft zweckentfremdet werden, besonders in Krisenzeiten.

Denn wenn Menschen im öffentlichen Raum jederzeit identifiziert und überwacht werden können, kann nachvollzogen werden, wer sich wann, wo und mit wem bewegt. Biometrische Fernidentifizierungssysteme schaffen daher ein gefährliches Instrument, das von zukünftigen, ggf. extremistischen Kräften zur gezielten Verfolgung kritischer Stimmen genutzt werden kann. [Louisa Specht-Riemenschneider, BfDI](#), mahnt, dass alle

vorgesehenen Eingriffsnormen zur Gesichtserkennung zu unscharfe Tatbestandsmerkmale aufweisen.

Für bereits benachteiligte Gruppen, Minderheiten und politische Dissidenten zeigen sich die negativen Auswirkungen typischerweise in verstärkter Form. Es ist daher hochproblematisch, dass, wie [Prof. Dr.-Ing. Christoph Sorge, Universität des Saarlandes](#), kritisiert, „eine auch nur ansatzweise konkretisierte technische Konzeption“ fehlt und daher, besonders im Bereich der Biometrie, die Vorschläge kaum im Detail zu überprüfen seien. Es sind also sehr weitreichende Eingriffe vorgesehen, ohne dass die Bürger wissen, worauf sie sich einstellen müssten.

Biometrische Systeme sind objektiv

Studien zeigen, dass Gesichtserkennungssysteme diskriminierend wirken können. Sie erkennen beispielsweise Menschen [dunkler Hautfarbe oder Frauen weniger gut](#), was zu einer höheren Anzahl an falsch positiven Treffern bei diesen Gruppen führt. Grund dafür ist, dass die Daten, mit denen die Systeme trainiert wurden, nicht repräsentativ sind bzw. überproportional Daten von Menschen weißer Hautfarbe und Männern enthalten. Dies kann im Strafverfolgungskontext erhebliche Auswirkungen auf Individuen haben.

Umso problematischer, dass diskriminierende Algorithmen nicht durch klare Vorgaben eingeschränkt werden, wie [Prof. Dr. jur. Dennis-Kenji Kipker, Universität Bremen](#), feststellt. Doch das Problem ist nicht nur Diskriminierung durch Bias in den Trainingsdaten. Auch wenn die Systeme auf technischer Ebene akkurat funktionieren würden und der Bias „beseitigt“ werden könnte, können sie im öffentlichen Raum nicht in grundrechtskompatibler Weise benutzt werden.

Die geplanten Maßnahmen sind mit EU-Recht vereinbar.

Die geplante Überwachungsstruktur ist technisch nur möglich, wenn riesige, unterschiedslose Gesichtsdatenbanken angelegt werden. Sei es, um den eingesetzten Algorithmus zu testen oder um später damit Abgleiche durchzuführen.

Diese Regelungen sind auch nach Artikel 5 der KI-Verordnung „nicht mit der KI-Verordnung in Einklang zu bringen“, ([Specht-Riemenschneider, BfDI](#)). [Art. 5 Abs. 1\(e\) KI-VO](#) verbietet explizit ausnahmslos „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen

Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern“.

Anders als mithilfe einer solchen Datenbank lässt sich die Erfassung der riesigen Datenmengen im Internet jedoch technisch nicht sinnvoll bewerkstelligen. Diese Datenbanken verstärken ferner das Gefühl der Massenüberwachung und stellen massiven Einschränkungen von Grundrechten dar, insbesondere des Rechts auf Privatsphäre, führen. Prof. Dr. [Christoph Sorge, Universität des Saarlandes](#), konstatiert daher ebenfalls: „Die Normen werden daher sehr wahrscheinlich die Anforderungen des Unionsrechts nicht erfüllen“.

Literaturliste

- Die schriftlichen und mündlichen Stellungnahmen von Kipker, Lincoln, Schindler, Sorge, Specht-Riemenschneider sowie eine Zusammenfassung und das Video der Anhörung im Innenausschuss finden Sie hier:
<https://www.bundestag.de/dokumente/textarchiv/2024/kw39-pa-inneres-sicherheit-asyl-1019032>
- AG Migration, SPD (September 2023): „Rechtswidrigkeit des Gesetzesentwurfs zur Verbesserung der inneren Sicherheit und des Asylsystems“,
https://cdn.netzpolitik.org/wp-upload/2024/09/Factsheet_AG_Migration_SPD.pdf
- Arzt, Clemens (17.09.2024): „Die Woche der Sicherheitspakete“,
<https://verfassungsblog.de/die-woche-der-sicherheitspakete>
- Höffler, Katrin (20.09.2024): „Solingen 93/24: Menschenrechte als bestes Präventionskonzept“, <https://verfassungsblog.de/solingen-93-24/>
- Hill, Kashmir (03.08.2020), New York Times „Wrongfully Accused by an Algorithm“,
<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>