Digital Autonomy Hub
Technik souverän nutzen

POLICY BRIEF #9
JULI 2023

Biometrische Überwachung

Wie biometrische Erkennungssysteme Grundrechte beschneiden können

Digital Autonomy Hub

INHALT

EINLEITUNG

An Bahnhöfen, in Fußballstadien und an ausgewählten öffentlichen Plätzen werden zunehmend technische Systeme eingesetzt, die Menschen anhand ihrer biometrischen Merkmale und mithilfe von Algorithmen erkennen, identifizieren, kategorisieren und damit überwachen können. Der wahrscheinlich schon am längsten genutzte biometrische Marker ist der Fingerabdruck, den Strafverfolgungsbehörden nutzen. Die biometrische Erkennung ist jedoch auch mit mehr Distanz möglich, indem Menschen etwa anhand ihres Gesichts, ihrer Körpergröße, ihrer Stimme oder sogar ihrem Gang erfasst werden. Auch Bewegungsmuster (zum Beispiel „Fallen“ oder „Schlagen“) sollen biometrisch interpretierbar sein.

Die erfassten biometrischen Merkmale können mit Algorithmen analysiert werden, um Menschen zu erkennen. Solche biometrische Erkennung kann zur *Verifizierung* (1-zu-1 Abgleich) und zur *Identifizierung* (Abgleich mit großen Datenmengen) eingesetzt werden.

Wenn eine Person ihr Smartphone durch das Scannen ihres Gesichts entsperrt, handelt es sich dabei um eine Verifizierung, man spricht allgemein von Authentifizierung. Das im Smartphone gespeicherte Bild wird mit dem Gesicht verglichen, das die Kamera des Geräts gerade aufnimmt, und ein Algorithmus wertet aus, wie ähnlich sich die beiden Bilder sind. Ist das Ergebnis ein Treffer, gilt die Person als verifiziert und das Smartphone entsperrt sich. Diese Verifizierung ist in der Regel freiwillig und findet lokal auf einem bestimmten Gerät statt. Wenn das Bild eines Gesichts mit bestehenden Datenbanken von Geschichtsbildern, beispielsweise Sammlungen der Polizei, abgeglichen wird, handelt es sich um eine biometrische Erkennung zum Zweck der Identifizierung. Hier geht es darum, die Identität einer Person festzustellen.

Diese zweite Form der biometrischen Erkennung wird eingesetzt, ohne dass die betroffene Person davon weiß. Der Abgleich mit den Datenbanken kann dabei in Echtzeit oder auch nachträglich mittels gespeicherter Videoaufnahmen vorgenommen werden. Viele moderne Kameras haben eine entsprechende Funktion schon direkt implementiert.

Wenn im öffentlich zugänglichen Raum, zum Beispiel im Supermarkt, am Bahnhof oder auf öffentlichen Plätzen, alle gefilmten Personen – ob in Echtzeit oder nachträglich – mit bestimmten Bildern gesuchter Personen abgeglichen werden, dient die biometrische Erkennung dem Herausfiltern einzelner Personen aus einer großen Menge. Behörden, die solche Systeme einsetzen, wissen dabei zum Beispiel noch nicht, ob

eine bestimmte gesuchte Person tatsächlich vor Ort ist, oder sie möchten herausfinden, an welchen Orten sie sich aufgehalten hat.

Grundsätzlich werden dabei nicht nur die biometrischen Daten einzelner verdächtiger Personen verarbeitet, sondern die Gesichter aller Personen abgeglichen, die vor Ort sind oder waren. Es werden massenhaft biometrische Daten verarbeitet, auch von Personen, die keinerlei Verbindung zu strafrechtlich relevantem Verhalten haben.

Biometrische Auswertungen können auch dazu verwendet werden, Menschen nach bestimmten Merkmalen einzuordnen. Bei dieser sogenannten biometrischen *Kategorisierung* wird versucht, das Geschlecht, das Alter oder sogar die sexuelle Orientierung einer Person festzustellen. Für die Verwendung biometrischer Kategorisierungssysteme gibt es oft kommerzielle Motive. Die Schweizerischen Bundesbahnen (SBB) beabsichtigten beispielsweise, ab Herbst 2023 in über 50 Bahnhöfen die Bewegungen der Reisenden zu erfassen, zu verfolgen und sie dabei auch nach Größe, Alter und Geschlecht zu kategorisieren. Nach den ursprünglichen Ausschreibungsdokumenten verfolgten die SBB dabei vor allem kommerzielle Zwecke. Sie wollten die „Abschöpfung" pro Reisendem erhöhen, etwa durch „gezielte Werbung", „Verbesserung der kommerziellen Performance von Shops" oder der „Optimierung des Mieter-Mix". Die SBB wollten die Möglichkeit schaffen, Reisenden gezielt Werbung anzuzeigen, die zu ihrem Geschlecht oder Alter passt, und das Angebot in den Bahnhofsgeschäften entsprechend auszurichten. Es liegt auf der Hand, dass ein Systemanbieter bei dieser Ausschreibung biometrische Kategorisierungssysteme einsetzen müsste, um solche Auswertungen liefern zu können. Nach einem massiven zivilgesellschaftlichen Aufschrei wurde die Ausschreibung verändert und die Option der biometrischen Kategorisierung gestrichen.[1]

Private Akteure können außerdem ein Interesse daran haben, solche Kategorisierungssysteme für Sicherheitszwecke einzusetzen, etwa um Ladendiebstahl zu verhindern. Weit verbreitet ist heute schon der Einsatz von Überwachungskameras zu diesem Zweck. Ein Supermarkt der Kette Southern Co-op in Großbritannien geht jedoch noch deutlich weiter und nutzt ein System der Firma Facewatch, das von jeder Person, die den Supermarkt betritt, in Echtzeit ein biometrisches Profil erstellt und es den Angestellten ermöglicht, Personen als „verdächtig" zu markieren.[2] Welches Verhalten eine Einstufung als „verdächtig" rechtfertigt, bleibt den Angestellten überlassen, das System von Facewatch macht diesbezüglich keinerlei Vorgaben. Wird dem System eine verdächtige Person gemeldet, wird sie als „Person von Interesse" gelistet und ihr Profil automatisch mit jedem Nutzer des Facewatch-Systems in der weiteren Umgebung, zum Beispiel anderen Ladengeschäften, geteilt. Einer Person könnte also in einem Geschäft im Osten Londons der Zutritt verweigert werden, weil sie in einem Geschäft im Westen Londons, das einem völlig anderen Unternehmen gehört, als verdächtig erfasst wurde. Jeden Monat fügt Facewatch seiner Beobachtungsliste auch „Personen von Interesse" hinzu, die auf den Fahndungs-Websites der Polizei und von Crimestoppers, einer Wohltätigkeitsorganisation zur Verbrechensverhütung, veröffentlicht werden. 2020 rügte die niederländische Datenschutzbehörde einen niederländischen Supermarkt dafür, im Jahr 2019 die Nutzung eines ähnlichen Systems eingesetzt zu haben. Legitime Gründe für den Einsatz eines biometrisches Gesichtserkennungssystems sah die Behörde hier nicht gegeben.[3]

1 Die Digitale Gesellschaft und AlgorithmWatch CH haben sich gegen dieses Vorhaben eingesetzt und konnten die geplante Kategorisierung von Reisenden verhindern, siehe Blogpost AlgorithmWatch CH: https://algorithmwatch.ch/de/erfolg-offener-brief/ [11.07.23].

2 Siehe Frankie Vetch: „UK supermarket uses facial recognition tech to track shoppers", https://www.codastory.com/authoritarian-tech/uk-supermarket-biometric-cameras/ [veröffentlicht am 11.01.23].

3 Siehe Dataguidance.com: „Netherlands: AP issues warning to supermarket for use of facial recognition", https://www.dataguidance.com/news/netherlands-ap-issues-warning-supermarket-use-facial [aktualisierter Beitrag veröffentlicht am 27.01.21].

RISIKEN FÜR DIE GRUNDRECHTE

Auf den ersten Blick scheinen biometrische Erkennungssysteme Instrumente zu sein, die Polizeiarbeit effizienter machen können und für die Gewährleistung von Sicherheit nutzbar sind. Doch mit Blick auf die einführenden Beispiele wird deutlich, dass dieses Bild trügt.

Ist auf öffentlichen Plätzen, in Bahnhöfen, Stadien oder Einkaufszentren eine technische Infrastruktur vorhanden, um Personen jederzeit automatisiert zu identifizieren, berührt das im Kern die demokratische Öffentlichkeit. Durch den Einsatz biometrischer Erkennungssysteme wird die Anonymität im öffentlichen Raum und an Orten, die Menschen nicht meiden können, etwa, weil sie dort Grundbedürfnissen nachgehen, geradezu aufgehoben. Das kann sich fatal auf die Wahrnehmung fundamentaler demokratischer Grundrechte und die Selbstbestimmung auswirken. Menschen, die das Gefühl haben müssen, dass ihre Handlungen an einem öffentlichen Platz überwacht und sie jederzeit ganz persönlich identifiziert werden können, werden möglicherweise davon abgehalten, sich zu versammeln und ihre Meinung zu äußern: Es könnte sie beispielsweise konkret davon abhalten, an einer Demonstration teilzunehmen, eine religiöse Stätte aufzusuchen oder ein Lokal zu besuchen, das besonders bei Menschen einer bestimmten sexuellen Orientierung beliebt ist. Diese Auswirkung, das präventive Anpassen der eigenen Handlungen an eine potenzielle Überwachung, der man ausgesetzt sein könnte, wird als „Chilling Effect“ (Abschreckungseffekt) beschrieben. Dass Menschen ihre Grundrechte wahrnehmen und sich im öffentlichen Raum frei und unerkannt bewegen können, ist jedoch eine Grundvoraussetzung für demokratische Gesellschaften.

Die Tatsache, dass die Erkennung von Gesicht, Stimme oder Gang aus der Ferne erfolgen kann, verstärkt diese Auswirkungen noch: Man weiß nicht, in welchen Momenten tatsächlich eine Überwachung vorgenommen wird, noch kann man ihr ausweichen: Das eigene Gesicht kann man beim Besuch einer Demonstration, Abtreibungsklinik oder Gebetsstätte schlicht nicht zuhause lassen.

Neben diesen Risiken für die demokratische Öffentlichkeit bestehen auch technologisch bedingte, die damit zusammenhängen, dass Gesichtserkennung und andere biometrische Erkennungssysteme teilweise nicht richtig funktionieren, verzerrte Annahmen ihre Entwicklung beeinflussen oder sie auf eine bestimmte Art und Weise eingesetzt werden.

In den USA wurden beispielsweise mehrere Menschen irrtümlich verhaftet, weil ein Gesichtserkennungssystem sie fälschlicherweise als Personen identifiziert hatte, die zur Fahndung ausgeschrieben waren. Oft handelte es sich bei den Betroffenen um People of Color. Nicht-weiße Gesichter sind in den Trainingsdaten, mit denen manche Systeme entwickelt wurden, oft unterrepräsentiert – mit der Folge, dass diese Systeme sie weniger gut erkennen. Dasselbe gilt auch für nicht-männliche Gesichter.[4]

Darüber hinaus beruhen viele biometrische Erkennungssysteme, die Aussagen über das Geschlecht, die Emotionen oder andere persönliche Merkmale von Menschen treffen sollen, auf wissenschaftlich fragwürdigen Grundlagen. Die Schlussfolgerungen, die diese Systeme ziehen, sind daher oft ungültig und bedienen teils sogar rassistischer Vorstellungen, die noch aus den Hochzeiten der Eugenik stammen.[5] Von körperlichen Merkmalen wie der Gesichtsform auf andere Persönlichkeitsmerkmale zu schließen, beruht auf rassistischen Annahmen. Nur weil ein

4 Vgl. New York Times, „Wrongfully Accused by an Algorithm“, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [veröffentlicht am 24.06.20].

5 Vgl. New York Times, „The Racist History Behind Facial Recognition“, https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html [veröffentlicht am 10.07.19].

System einen bestimmten Zusammenhang erkennt, heißt das nicht, dass dieser auch einer wissenschaftlichen Überprüfung standhält – und schon gar nicht, dass daraus Rückschlüsse auf eine Einzelperson gezogen werden können. Zur rechtlich umstrittenen Überwachung kommt also nicht selten noch eine Fehlklassifizierung oder Fehlcharakterisierung hinzu – die eine wesentliche Quelle von Ungerechtigkeit darstellen kann.

BIOMETRISCHE GESICHTSERKENNUNG IN DEUTSCHLAND AUF DEM VORMARSCH

Wie zuvor beschrieben, können verschiedene schützenswerte Personendaten von biometrischen Erkennungssystemen erfasst werden. Die folgenden Abschnitte widmen sich vor allem der Technik der Gesichtserkennung und ihrer verschiedenen Einsatzkontexte.

Videoüberwachung in der Polizeiarbeit

Während in den frühen 2010er-Jahren Videoüberwachungssysteme eingesetzt wurden, deren Aufzeichnungen eine nachträgliche Verarbeitung biometrischer Daten für Abgleiche mit Datenbanken ermöglichten, werden heutzutage zunehmend Überwachungssysteme eingesetzt, die diesen Abgleich automatisch und in Echtzeit vollziehen können. Stand der Technik ist, dass die Polizei heute den öffentlichen Raum in Echtzeit überwachen kann.

Allein die Firma Dallmeier hat bis 2021 Videoüberwachungssysteme mit Gesichtserkennungsfunktion an Polizeibehörden in 19 deutschen Städten verkauft.[6] Seit 2018 hatte zum Beispiel die Stadt Köln solche „biometrietauglichen" Kameras in unmittelbarer Nähe zu Arztpraxen, Gebetsstätten und Orten, die vornehmlich von Menschen der LGBTQI-Community besucht werden, installiert. Ein Kölner Bürger klagte gegen diese Polizeipraxis, blieb aber in letzter Instanz erfolglos. Die Polizei musste nach dem Urteil des Oberverwaltungsgerichts Münster lediglich sicherstellen, Bildmaterial von Bewegungen an Hauseingängen und von Innenräumen nicht mit zu erfassen.[7]

Auch die Klage eines Dortmunders gegen die automatisierte polizeiliche Überwachung einer Straße in der Dortmunder Nordstadt wurde im Jahr 2022 unter Berufung auf die Zulässigkeit nach dem Polizeigesetz Nordrhein-Westfalens abgelehnt.[8]

In einem Fall, den die Gesellschaft für Freiheitsrechte gemeinsam mit einem Passauer Bürger vor Gericht brachte, wurde im Juni 2023, vier Jahre nach Erhebung der Klage, in einem Berufungsverfahren vor dem Bayerischen Verwaltungsgerichtshof im Sinne des Klägers entschieden. Die Polizei in Passau hatte trotz rückläufiger Kriminalitätsraten zehn Kameras zur anlasslosen Überwachung auf dem zentral gelegenen Klostergarten-Platz installiert. Das Gericht folgte der Argumentation des Klägers, dass zu keinem Zeitpunkt eine Gefährdungslage im Passauer Klostergarten bestanden habe, die eine Videoüberwachung und die damit verbundenen Grundrechtseinschränkungen gerechtfertigt hätte.[9]

---

6 Vgl. Montag, Luca/Mcleod, Rory/De Mets, Lara/Gauld, Meghan/Rodger, Fraser/Pełka, Mateusz (2021): „The Rise and Rise of Biometric Mass Surveillance in the EU: a legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland", S.16, https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf [11.07.23].

7 Vgl. Openjur.de: „Rechtsprechung OVG Nordrhein-Westfalen, 16.05.2022 - 5 B 264/21", https://openjur.de/u/2397896.html [11.07.23].

8 Siehe ovg.nrw.de: „Polizeiliche Videoüberwachung in der Dortmunder Nordstadt darf fortgeführt werden", https://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2022/51_220923/index.php [veröffentlicht am 22.09.22].

9 Siehe freiheitsrechte.org: „Videoüberwachung im Klostergarten Passau", https://freiheitsrechte.org/themen/freiheit-im-digitalen/passau [11.07.23].

Derweil experimentieren Polizeibehörden in Deutschland weiter mit neuen Anwendungsmöglichkeiten für die algorithmische oder automatisierte Überwachung mithilfe von Videoüberwachungssystemen. Zuletzt wurde ein Fall aus Hamburg bekannt, wo in der Nähe des Hauptbahnhofs ein auf Künstlicher Intelligenz (KI) basierendes Überwachungssystem „verdächtige Bewegungen erkennen und Alarm auslösen" soll.[10] Bereits seit 2019 sind am Hamburger Hansaplatz nahe dem Hauptbahnhof 16 Kameras in Betrieb, nun soll die zusätzlich installierte Technologie die Bewegungsmuster Schlagen, Treten und Hinfallen erkennen und Beamt·innen über potenzielle Gefahrensituationen informieren. Entwickelt und getestet wurde das System zuvor in Mannheim. Laut Antwort des Hamburger Senats auf die Anfrage eines Abgeordneten[11] startete die Planungsphase der „intelligenten Videobeobachtung" Anfang März 2023. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit war zum Zeitpunkt, als erstmals über das System am Hansaplatz berichtet wurde, noch nicht darüber in Kenntnis gesetzt. Die Erklärung des Senats: Zunächst wurden polizeiintern datenschutzrechtliche Aspekte geprüft. Im Herbst 2023, wenn die sechsmonatige Erprobungsphase in Hamburg abgeschlossen sein wird und eine Evaluation vorliegt, soll darüber entschieden werden, ob eine dauerhafte Implementierung sinnvoll ist.

Auch wenn die Entscheidung über die Weiternutzung des KI-Videoüberwachungssystems in Hamburg noch aussteht, wird das Potenzial der technologischen Erweiterung bestehender Infrastrukturen für die polizeiliche Überwachung deutlich. Die Möglichkeit der automatischen, KI-gestützten Analyse von Videomaterial auf mögliche Gefahrensituationen hin wird bei Polizeibehörden den Wunsch wecken, eher noch mehr Kameras zu installieren, da mit der neuen Technik riesige Datenmengen ausgewertet werden können, ohne dafür mehr Personal einsetzen zu müssen.

Videoüberwachung bei der Bahn

Auch die Deutsche Bahn (DB) plant für die Zukunft mehr Überwachung. Laut Medienberichterstattung betrieb die DB im März 2023 etwa 9.000 Videokameras auf Bahnhöfen, bis 2024 sollen es 11.000 werden.[12] In den Wagen von fast drei Viertel aller Nahverkehrs- und S-Bahnzüge sind fast 50.000 Kameras installiert. Aufgrund der Häufung von tätlichen Angriffen testet DB seit Februar 2023 zusätzlich einen Teil des Zugpersonals mit

10 Siehe Nur Maulawy: „Hamburgs Polizei setzt auf KI", https://taz.de/Ueberwachung-von-Drogenszene/!5933508/ [veröffentlicht am 23.05.23].

11 Siehe Drucksache 22/12180 der Bürgerschaft der Freien und Hansestadt Hamburg: „Schriftliche Kleine Anfrage des Abgeordneten Deniz Celik (DIE LINKE) vom 08.06.23 und Antwort des Senats", https://www.buergerschaft-hh.de/parldok/dokument/84096/einsatz_von_kuenstlicher_intelligenz_bei_der_ueberwachung_des_hansaplatzes.pdf [11.07.23].

12 Vgl. tagesschau.de: „Bahn will Personal mit Bodycams ausstatten", https://www.tagesschau.de/inland/innenpolitik/deutsch-bahn-bodycams-personal-uebergriffe-101.html [veröffentlicht am 04.03.23].

Bodycams auszustatten. Ob die Videosysteme der DB technisch in der Lage sind, biometrische Merkmale auszuwerten, geht aus der Berichterstattung nicht hervor. Gerade bei der Neuinstallation von Anlagen wäre dies allerdings zu erwarten.

Ab April 2020 testete die DB außerdem ein System, um den Passagierfluss zu kontrollieren und sicherzustellen, dass Fahrgäste in den Nahverkehrszügen zur Vermeidung von Corona-Infektionen Abstand halten. Das KI-System der Berliner Firma brighter AI nutzte die Videoaufnahmen bereits installierter Überwachungskameras und ersetzte die Gesichter der aufgenommenen Personen durch künstliche Nachbildungen, um die Möglichkeit der Identifizierung einzelner Fahrgäste auszuschließen. Gleichzeitig sollten jedoch Informationen wie Geschlecht oder Alter erhalten bleiben.[13] Bei Erfolg des Pilotprojekts, wollte die DB die Anwendung bundesweit einsetzen. Im Februar 2023 meldete das Berliner Unternehmen brighter AI, als einziges Unternehmen im letzten Jahr einen Zuschlag von DB Digital Ventures für die Finanzierung ihrer fortschrittlichen Technologie erhalten zu haben.[14] Es kann also davon ausgegangen werden, dass die Anwendung der Video-Anonymisierungssoftware in der Zwischenzeit als erfolgreich eingestuft wurde. Das Unternehmen wirbt ausdrücklich damit, die Aufnahmen von Gesichtern so zu verzerren, dass Gesichtszüge nicht erkennbar bleiben, damit datenschutzrechtliche Bestimmungen leichter erfüllt werden können. Erkennbar bleiben jedoch weiterhin andere Eigenschaften wie beispielsweise Hautfarbe und Größe, auch können anhand des Bildmaterials weiterhin Annahmen über Alter und Geschlecht gemacht werden. Es ist also auch beim Einsatz dieser Software nicht ausgeschlossen, dass Fahrgäste im Zuge einer Kategorisierung unterschieden und gruppiert werden. Die oben beschriebenen Pläne für ein Kategorisierungssystem der Schweizerischen Bundesbahnen haben den kommerziellen Nutzen eines solchen Vorgehens herausgestellt. Grundsätzlich gilt jedoch, dass Maßnahmen auf technischer Ebene alleine keinen zuverlässigen Schutz vor der Identifikation von Personen bieten, denn für Betroffene ist schwer erkennbar, welche dieser Maßnahmen aktiv sind und welche nicht. Die Entscheidung darüber liegt meist gänzlich beim Betreiber oder dem entwickelnden Unternehmen.

Biometrische Bilderkennung im Netz und bei der Polizei

Nebst diesen Anwendungsfällen, die in den Bereich der KI-basierten oder -unterstützten Videoüberwachung fallen, nutzen Polizeibehörden biometrische Erkennungssysteme auch zur Identifikation von Personen. In den letzten Jahren ist bekannt geworden, dass in einer Reihe von Ländern Polizeibehörden Gesichtserkennungssoftwares von Firmen wie Clearview AI

13 Siehe Kim Rixecker: „Mit KI und Kamera: Bahn will Passagierfluss digital auswerten“, https://t3n.de/news/ki-kamera-bahn-passagierfluss-1274035/ [veröffentlicht am 30.04.20].

14 Siehe Blogpost brighter AI „brighter AI erhält Investment von der Deutschen Bahn“, https://brighter.ai/de/resources/brighter-ai-erhaelt-investment-von-der-deutschen-bahn/ [veröffentlicht am 07.02.23].

und PimEyes nutzen. Im Kern bauen diese Unternehmen Gesichtsbildersuchmaschinen für den Abgleich mit Bilddatenbanken, deren Inhalte von Plattformen wie Facebook oder Twitter übernommen wurden – in der Regel ohne die Einwilligung der Nutzenden. In den Datenbanken liegen biometrische Daten der erfassten Personen, verknüpft mit den ursprünglichen Webadressen der Bilder. Lädt jemand in den Apps von Clearview oder PimEyes ein neues Foto hoch, erfasst die Suchmaschine die biometrischen Daten der Person und gleicht sie mit der Datenbank ab. So können Nutzende dieser Softwares unbekannte Personen identifizieren: Basierend auf der Wiedererkennung biometrischer Daten werden passende Webadressen angezeigt, beispielsweise zu den Social-Media-Profilen der gesuchten Person. Diese können wiederum Rückschlüsse auf weitere persönliche Informationen ermöglichen, etwa über den Arbeitgeber oder die Social-Media-Kontakte.

Bürgerrechtsorganisationen in den USA und Datenschutzbehörden in verschiedenen europäischen Ländern gingen in der Vergangenheit bereits gegen Suchmaschinen wie PimEyes und Clearview AI vor, weil diese ohne Einwilligung der betroffenen Personen persönliche Bilder in Datenbanken einspeisen und Profile bilden. Die Datensammelpraxis bei PimEyes, Clearview AI und anderen läuft allerdings scheinbar ungebremst weiter und die Dienste werden vorschriftswidrig genutzt.[15] Die schwedische Datenschutzbehörde hat beispielsweise 2021 festgestellt, dass die schwedische Polizei Clearview AI mehrfach bei Ermittlungen eingesetzt hatte, ohne eine Genehmigung dafür einzuholen. Eine administrative Strafe in Höhe von rund 250.000€ wurde verhängt.[16]

Auf europäischer Ebene wollen sich Polizeibehörden zukünftig gegenseitig mit Informationen zum Vorliegen biometrischer Fotos aushelfen.[17] Der Plan der Europäischen Kommission ist es, biometrische Fotos allen Polizeibehörden im Schengen-Raum zugänglich zu machen.[18] Das deutsche Bundeskriminalamt beteiligt sich aktiv an der Ausweitung des sogenannten Prüm-Systems[19] und die Abfrage von Gesichtsbildern bei der europäischen Datenbank soll im Kern wie beim deutschen Bundeskriminalamt funktionieren: Zunächst werden Nutzer·innen der Software informiert, ob ein Treffer vorliegt oder nicht. Bei einem positiven Ergebnis können dann weitere Informationen bei der jeweiligen Stelle, die sie vorliegen hat, angefragt werden. In einigen EU-Staaten, die noch keine Gesichtserkennungssysteme in ihrer Polizeiarbeit einsetzen, dürfte die zweite Ausbaustufe des Systems (Prüm II) den Grundstein dafür legen.[20]

Die Autor·innen der Studie „The Rise and Rise of Biometric Mass Surveillance in the EU“ (2021) attestieren Deutschland eine schleichende, sich über mindestens 20 Jahre entwickelnde Manifestierung einer weitreichenden Überwachungsinfrastruktur. Fragen nach der Verhältnismäßigkeit werden in vielen Fällen gestellt, denn sowohl das Grundrecht auf informationelle Selbstbestimmung als auch Datenschutzbestimmungen sehen Grenzen vor. Biometrische Daten werden in der europäischen Datenschutzgrundverordnung als besonders schützenswert beschrieben.

15 Siehe Markus Reuter: „Datenschutz-Verfahren gegen PimEyes und Clearview“, https://netzpolitik.org/2021/gesichtserkennung-datenschutz-verfahren-gegen-pimeyes-und-clearview/ [veröffentlicht am 27.05.21].

16 Siehe European Data Protection Board: „Swedish DPA: Police unlawfully used facial recognition app“, https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en [veröffentlicht am 12.02.21].

17 Siehe Matthias Monroy: „Polizei-Behörden erhalten europaweit mehr Datenzugriff“, https://www.golem.de/news/gesichtsbilder-polizei-behoerden-erhalten-europaweit-mehr-datenzugriff-2201-162674.html [veröffentlicht am 27.01.22].

18 Siehe Europäische Kommission: „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit („Prüm II“)“, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0784 [veröffentlicht am 08.12.21].

19 Der Name bezieht sich auf ein zwischenstaatliches Abkommen, das am 27.05.2005 in Prüm geschlossen wurde und die Verbesserung des grenzüberschreitenden polizeilichen Informationsaustausches zum Ziel hatte. Kernelemente des Übereinkommens wurden in den Beschluss 2008/615/JI des Rates der EU vom 23.06.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, übernommen. Siehe EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Ajl0005 [11.07.23].

20 Siehe Matthias Monroy: „EU-Ausschuss kritisiert geplante Verpflichtung zur Gesichtserkennung“, https://netzpolitik.org/2022/pruem-ii-verordnung-zu-datenaustausch-eu-ausschuss-kritisiert-geplante-verpflichtung-zur-gesichtserkennung/ [veröffentlicht am 30.05.22].

Dennoch müssen Betroffene von Überwachungsmaßnahmen ihre Rechte oft mühsam einklagen, obwohl die Risiken biometrischer Überwachung – sowohl für Einzelpersonen als auch für die Gesellschaft insgesamt – bekannt sind.

REGULIERUNG BIOMETRISCHER ERKENNUNGSSYSTEME AUF EUROPÄISCHER EBENE

Die EU verhandelt derzeit eine Verordnung („KI-Verordnung“)[21], die unter anderem Regeln für den Einsatz biometrischer Erkennungssysteme EU-weit und sektorübergreifend einführen wird. Im Kommissionsentwurf vorgesehen ist ein Verbot biometrischer Fernidentifizierung im öffentlichen Raum, allerdings ergänzt um eine Reihe an Ausnahmen. Das Verbot bezieht sich in erster Linie auf die Nutzung biometrischer Fernidentifizierung im öffentlichen Raum durch Strafverfolgungsbehörden und lässt andere Behörden oder private Akteure außen vor. Zusätzlich werden drei Ausnahmen für den Einsatz definiert: (1) Die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern, (2) das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags und (3) das Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat, der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.[22] Der Kommissionsentwurf unterscheidet außerdem zwischen „Echtzeit-“ und „nachträglicher Verwendung“ biometrischer Fernidentifizierung. Auf diese Weise schafft der Gesetzentwurf ein weiteres Schlupfloch, denn es erlaubt den Strafverfolgungsbehörden, biometrische Identifizierung nachträglich auf Videoaufzeichnungen oder Fotos anzuwenden.

Mittlerweile haben auch Rat und Parlament Stellung genommen und Änderungsvorschläge eingebracht, die bis zum voraussichtlichen Abschluss der Verhandlungen Ende 2023 diskutiert werden. Die Ratsposition vom Dezember 2022 ist, dass nur in Echtzeit eingesetzte Fernidentifizierung verboten werden soll. Außerdem sollen nur Strafverfolgungsbehörden und ihre Auftragnehmer diesen Einschränkungen unterliegen. Von dem Verbot wären demnach sowohl privatwirtschaftliche Unternehmen als auch andere Behörden ausgenommen. Darüber hinaus ist die biometrische Identifizierung erlaubt, wenn die Systeme auf gespeicherte Daten zugreifen, statt in Echtzeit gewonnene Daten zu verarbeiten. Für Strafverfolgungsbehörden gelten zudem etliche Ausnahmen vom Verbot, etwa wenn biometrische Fernidentifizierung zur Abwehr von Terrorangriffen, von Gefahren für die Gesundheit oder die körperliche Unversehrtheit oder bei bestimmten Arten von Straftaten zur Identifizierung mutmaßlicher Täter·innen eingesetzt wird. Zu guter Letzt sieht der Ratsentwurf noch vor, dass alle aufgeführten Verbote nicht in Situationen gelten sollen, in denen sich Mitgliedstaaten auf ihre „nationale Sicherheit“ berufen.[23]

Das Europäische Parlament stimmte im Juni 2023 über die gemeinsame Position ab. Die Abgeordneten verschärften bestehende Verbote für die Nutzung biometrische Fernidentifizierung im öffentlichen Raum und ergänzten weitere: Verboten werden sollen (1)

21 Siehe Kommissionsvorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung Harmonisierter Vorschriften Für Künstliche Intelligenz (“KI-Verordnung”), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0206 [veröffentlicht am 21.04.2021]

22 Ebd., S.51

23 Siehe Allgemeine Ausrichtung des Rats zur Verordnung des Europäischen Parlaments und des Rates zur Festlegung Harmonisierter Vorschriften Für Künstliche Intelligenz, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf, S.82 [veröffentlicht am 06.12.22]

biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen; (2) biometrische Fernidentifizierung, die nachträglich eingesetzt werden kann, mit der einzigen Ausnahme von Strafverfolgungsbehörden zur Verfolgung von schweren Straftaten und nur nach richterlicher Genehmigung; (3) biometrische Kategorisierungssysteme, die sensible Merkmale verwenden (z. B. Geschlecht, Rasse, ethnische Zugehörigkeit, Staatsangehörigkeit, Religion, politische Orientierung); (4) Systeme zur Erkennung von Emotionen in der Strafverfolgung, im Grenzschutz, am Arbeitsplatz und in Bildungseinrichtungen; und (5) wahlloses Auslesen biometrischer Daten aus sozialen Medien oder Videoaufnahmen zur Erstellung von Gesichtserkennungsdatenbanken.[24] Die deutsche Bundesregierung hatte bereits in ihrem Koalitionsvertrag festgehalten, dass biometrische Erkennung im öffentlichen Raum mithilfe von KI europarechtlich auszuschließen sei.[25]

POLITISCHE HANDLUNGS-EMPFEHLUNGEN

Dieser Policy Brief hat dargestellt, welche Risiken für die Grundrechte mit der Verwendung biometrischer Erkennungssysteme im öffentlichen Raum einhergehen. Menschen sind zunehmend Überwachungsinfrastrukturen ausgesetzt und werden mit der Fortentwicklung technologischer Möglichkeiten immer stärker in ihren Grundrechten beschnitten.

Erkennbar ist tendenziell eine Ausweitung von Überwachungsmöglichkeiten in Polizeigesetzen. Damit Menschen ihre Rechte wahrnehmen können, braucht es dringend klare Grenzen für den Einsatz biometrischer Erkennungssysteme im öffentlichen Raum. Datenschutzbestimmungen und das Recht auf informationelle Selbstbestimmung bieten in Deutschland zwar bereits einen gewissen Schutz vor unverhältnismäßigen Überwachungsmaßnahmen, doch die Praxis zeigt, dass Rechte und Regeln in vielen Einzelfällen nicht beachtet werden und der Schutz immer wieder aktiv eingefordert werden muss. Fälle, in denen Menschen erfolglos gegen den Einsatz von Videoüberwachung geklagt haben, machen die Grenzen dieses Schutzes sichtbar. Die unterschiedlichen Polizeigesetze im In- und Ausland lassen teils weite Spielräume zu und verstärken den Eindruck, dass der Grundrechtsschutz so manches Mal hinter den Interessen der Polizeibehörden anstehen muss.

Zudem zeigen die Beispiele, dass Menschen an öffentlichen Orten wie Bahnhöfen, Flughäfen und Supermärkten nicht nur immer stärker biometrischer Überwachung ausgesetzt sind, sondern Unternehmen biometrische Erkennungssysteme auch schon für kommerzielle Zwecke einsetzen. Diese Ausweitung von Überwachungskontexten hat das Potenzial, dass Menschen sich anpassen und ihre fundamentalen demokratischen Grundrechte wie Meinungsäußerung und Versammlungsfreiheit im öffentlichen Raum nicht mehr wahrnehmen.

Der Policy Brief zeigt außerdem auf, dass Menschen hinsichtlich des verbreiteten ungefragten Sammelns und der ungeklärten Nutzung biometrischen Bildmaterials besseren Schutz benötigen. Einzelne Datenschutzbehörden in der EU haben zwar teils hohe Geldstrafen verhängt, doch Gesichtsbildersuchmaschinen

24 Siehe Parlamentsposition zur Verordnung des Europäischen Parlaments und des Rates zur Festlegung Harmonisierter Vorschriften Für Künstliche Intelligenz, https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf, S. 129 ff., [veröffentlicht am 11.05.23]

25 Vgl. Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), https://www.bundesregierung.de/resource/blob/974430/1990812/1f422c60505b6a88f8f3b3b5b8720bd4/2021-12-10-koav2021-data.pdf?download=1, S. 18 [12.07.23].

wie PimEyes oder Clearview AI sind weiterhin weitgehend uneingeschränkt nutzbar.

Wir empfehlen den nationalen und überstaatlichen Gesetzgeber·innen unter anderem die folgenden Maßnahmen und Schritte:

— Die biometrische Identifizierung an öffentlich zugänglichen Orten stellt einen schweren Eingriff in die Grund- und Menschenrechte dar. Ein Verbot sollte daher auf deutscher und europäischer Ebene erlassen werden. Die Bundesregierung sollte sich in den derzeitigen Verhandlungen zur europäischen KI-Verordnung für ein weitreichendes Verbot, das die biometrische Echtzeit- und nachträgliche Fernidentifikation im öffentlichen Raum untersagt, einsetzen.[26]

— Darüber hinaus sollte sich die Bundesregierung für ein Verbot biometrischer Kategorisierungssysteme, die natürliche Personen anhand von sensiblen oder geschützten Merkmalen Gruppen zuordnen, sowie der Nutzung jeglicher biometrischer Kategorisierungs- und automatischer Verhaltenserkennungssysteme in öffentlich zugänglichen Räumen einsetzen.

— Des Weiteren sollte sich die Bundesregierung für ein Verbot von Systemen einsetzen, die vorgeben, Emotionen und mentale Zustände von Personen zu erkennen.

— Gesichter-Suchmaschinen, die von privaten Unternehmen als Software angeboten werden, gilt es zu verbieten. Die Bundesregierung sollte daher den Vorstoß des Europäischen Parlaments, das wahllose Auslesen biometrischer Daten aus sozialen Medien oder Videoaufnahmen zur Erstellung von Gesichtserkennungsdatenbanken zu verbieten, im Zuge der Verhandlungen über die KI-Verordnung unterstützen.

— Die Bundesregierung sollte sich auf EU-Ebene gegen die Ausweitung biometrischer Überwachungsinfrastrukturen für die polizeiliche Zusammenarbeit einsetzen, wie sie im „Prüm II“-Vorschlag vorgesehen ist.

Mehrere Städte und Kommunen weltweit haben bereits die Verwendung von biometrischen Erkennungssystemen im öffentlichen Raum verboten, darunter San Francisco, weitere US-Städte[27] und drei Städte in der Schweiz[28], wo die Sensibilisierungsmaßnahmen verschiedener zivilgesellschaftlicher Organisationen Wirkung zeigten. Auf europäischer Ebene fordert die Kampagne „Reclaim Your Face“[29] ein Verbot von Gesichtserkennungs- und biometrischen Fernidentifizierungssystemen, die Massenüberwachung und diskriminierende gezielte Überwachung von Individuen ermöglichen. Dahinter steht ein breites Bündnis an zivilgesellschaftlichen Organisationen aus ganz Europa, die ein entschlossenes Handeln der Politik fordern. Von der deutschen Bundesregierung wird insbesondere mit Blick auf die Verhandlungen zur KI-Verordnung erwartet, sich für strikte Verbote in der EU einzusetzen – schon um das eigene gesteckte Ziel aus dem Koalitionsvertrag zu erreichen.

26 Siehe dazu den offenen Brief, in dem AlgorithmWatch und 26 weiteren zivilgesellschaftliche Organisationen die Bundesregierung zu einem strikten Verbot für biometrische Überwachung aufrufen: https://algorithmwatorg/de/offener-brief-biometrische-ueberwachung-in-der-ki-verordnung-umsetzen/ [veröffentlicht am 08.11.22].

27 Siehe Rachel Metz: „Beyond San Francisco, more cities are saying no to facial recognition”, https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html [veröffentlicht am 17.07.19].

28 Dazu zählen die Städte Zürich, St. Gallen, Lausanne. Siehe Estelle Pannatier: „Erfolg: Lausanne verbietet Gesichtserkennung im öffentlichen Raum!“, https://algorithmwatch.ch/de/lausanne-verbietet-gesichtserkennung-offentlichen-raum/ [veröffentlicht am 31.03.23].

29 Vgl. https://reclaimyourface.eu/ [12.07.23].

Digital Autonomy Hub
Technik souverän nutzen

Der *Digital Autonomy Hub – Technik souverän nutzen* ist ein Kompetenzzentrum, das ein interdisziplinäres Netzwerk von 43 Instituten und Organisationen koordiniert. Der Hub macht sichtbar, woran die Partner forschen und welche Ideen sie entwickeln, um die individuelle digitale Souveränität zu stärken. Ziel dieses Wissenstransfers ist es, allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten, Geräten und Anwendungen zu ermöglichen. Das Kompetenzzentrum bereitet aktuelle Forschungsergebnisse für Zivilgesellschaft, Politik, Wissenschaft und Wirtschaft auf und berät die verschiedenen Akteure zu ethischen, rechtlichen und sozialen Aspekten der Datennutzung.

Der *Digital Autonomy Hub* wird vom Bundesministerium für Bildung und Forschung im Rahmen des Forschungsprogramms „Technik zum Menschen bringen" gefördert und von AlgorithmWatch und Gesellschaft für Informatik e.V. (GI) umgesetzt.

Mehr Informationen unter: www.digitalautonomy.net

Biometrische Überwachung: Wie biometrische Erkennungssysteme Grundrechte beschneiden können

Policy Brief #9
des Digital Autonomy Hubs

Juli 2023

Autorin:
Pia Sombetzki
(Policy & Advocacy Managerin, AlgorithmWatch)

Lektorat:
Karola Klatt

Bilder:
Julian21 / Unsplash (Titel),
cottonbro studio / Pexels (S. 3),
Atypeek Dgnv/ Pexels (S. 7),
cottonbro studio / Pexels (S. 8)
Sora Shimazaki / Pexels (S. 11)

Layout:
Beate Autering

Veröffentlicht von
AW AlgorithmWatch gGmbH
Linienstr. 13, 10178 Berlin

Gesellschaft für Informatik e.V. (GI)
Spreepalais am Dom
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Kontakt:
info@digitalautonomy.net

Der Digital Autonomy Hub wird gefördert vom

Bundesministerium für Bildung und Forschung

im Rahmen des Forschungsprogramms „Technik zum Menschen bringen"