BIOMETRIE: KÖRPER ALS UNIVERSAL-AUSWEIS?

IN KÜRZE

- Biometrie verbreitet sich immer stärker im Alltag von Konsument*innen und soll zu mehr Sicherheit führen.
- Biometrische Verfahren digitalisieren Körpermerkmale und können auch unbemerkt zum Einsatz kommen.
- Die Verarbeitung biometrischer Daten ist in vielen Fällen intransparent und schwer kontrollierbar.
- Biometrie birgt daher auch Risiken für Privatsphäre, Sicherheit und Grundrechte.
- Regulierungsmaßnahmen können dazu beitragen, einige Risiken zu reduzieren.

WORUM GEHT ES?

Biometrie bezeichnet die automatisierte Erkennung von Individuen anhand biologischer Merkmale oder Verhaltensmuster. Biometrische Daten werden u.a. aus Fingerabdruck, Gesicht, Iris, Sprache oder Bewegungsmustern generiert. In Lichtbildausweisen sind sie schon lang in Verwendung. Biometrie dient i.d.R. dazu, die Identität einer Person anhand bestimmter, für sie charakteristischer Merkmale festzustellen oder die Echtheit (Authentizität) zu bestätigen. Das Anwendungsspektrum von Biometrie nimmt generell zu. Die Technologie wird nicht mehr nur im Sicherheitsbereich, sondern auch im kommerziellen Bereich verwendet. Im Alltag von Konsument*innen hat Biometrie vor allem als „Bequemlichkeitstechnologie“ Einzug gefunden. Verfahren wie Fingerabdruckscan oder Gesichtserkennung sind immer häufiger in digitalen Endgeräten wie Smartphones und Computern integriert. Im Vergleich zu einem PIN oder Passwort sollen biometrische Verfahren hier regelmäßig die Anmeldung bzw. Entsperrung der Geräte beschleunigen. Zudem setzen Banken und Finanzdienstleister auch immer mehr auf biometrische Verfahren. Konsument*innen werden somit an Biometrie im Alltag gewöhnt. Darüber hinaus ermöglichen neue Auswertungsverfahren, biometrische Daten auch bei großen Datenbeständen automatisiert zu verarbeiten. Beispiele hierfür sind u.a. der Abgleich von Fingerabdrücken, Stimm- oder Gesichtserkennung. Vorgänge, die also vor einigen Jahren noch auf spezialisierte Systeme u.a. von Sicherheitsbehörden beschränkt waren, sind heute auch im kommerziellen Bereich im Einsatz – und bestimmen unseren Alltag mit.

Fingerabdrücke als Synonym biometrischer Merkmale

Ein kritischer Aspekt dabei: Daten befinden sich häufig völlig ungeschützt im Internet. Die Personen, von denen die Daten ursprünglich stammen, haben oft keine Möglichkeit, diese biometrische Auswertung zu erkennen oder darauf Einfluss zu nehmen. Der Körper wird damit quasi unbewusst zum Universalausweis, der regelmäßig auch ohne Wissen oder Unterstützung der erfassten Person erfasst oder kontrolliert werden kann. Biometrie hat daher eine Reihe erheblicher gesellschaftlicher Auswirkungen, wie z.B. unbemerkte Identifikation im öffentlichen Raum oder Identitätsdiebstahl. Das verschärft die komplexe Problematik der Überwachung und bringt erhebliche Herausforderungen für Sicherheit, Datenschutz und Demokratie.

ECKDATEN

Projekttitel:	Der Körper als Schlüssel?
Projektteam:	Schaber, F.; Strauß, S.; Peissl W.
Laufzeit:	04/2020 – 11/2020
Auftraggeber:	Bundesarbeitskammer

GEFAHRENPOTENZIAL

Biometrie hat vor allem Bequemlichkeitsvorteile und verspricht mehr Sicherheit. Mit steigender Verbreitung entstehen allerdings auch neue Sicherheitsrisiken. Biometrische Merkmale sind unweigerlich an den Körper gebunden, und daher nicht veränderbar. Sie können damit auch Gefahren wie Identitätsdiebstahl erhöhen. Auch biometrische Daten sind nicht fälschungssicher und können mit einfachen Mitteln kopiert werden (z.B. Klebestreifen bei Fingerabdruck oder digitales Gesichtsbild) um Sicherheitssysteme auszutricksen.

Photo: Alex Iby / Unsplash

Datensicherheit und sichere Übertragung biometrischer Daten ist daher essentiell. Kommen die Daten abhanden, können sie nicht wie PIN oder Passwort einfach geändert werden, denn sie sind untrennbar mit der erfassten Person verbunden. Dritte könnten diese Daten missbrauchen, Personen unbemerkt identifizieren oder in Systeme eindringen. In der Praxis ist das Schutzniveau bei biometrischen Verfahren häufig unzureichend. Angriffe auf biometrische Systeme nehmen daher zu. Ein weiteres Problem sind teils hohe Fehlerraten biometrischer Verfahren. Das gilt insbesondere für Gesichtserkennung. Das Risiko der Falscherkennung ist besonders groß, wenn einige wenige Personen aus einer großen Anzahl an Personen erkannt werden sollen. Die Folge können falsche Verdächtigungen, Diskriminierung oder Rassismus sein. Zahlreiche Studien zeigen Bias in Gesichtserkennung. So sind etwa Menschen mit nicht-weißer Hautfarbe bei bestimmten Algorithmen bis zu 100 Mal häufiger von Falscherkennungen betroffen als Weiße. Ein großes Risiko geht auch von der nachträglichen Auswertung bestehender Daten aus. So können z. B. im Internet veröffentlichte Gesichtsbilder auch lange nach Erstveröffentlichung biometrisch ausgewertet werden. Dadurch wird eine allgegenwärtige, unbemerkte Überwachung möglich. Hier gibt es rechtliche Grauebereiche und unzureichende Schutzstandards. Somit besteht ein dauerhaftes Risiko für die Privatsphäre und die Problematik der unbemerkten Identifizierung und Überwachung nimmt auf globaler Ebene erheblich zu. Um die Gefahren zu verringern, sind daher besondere Regelungen für biometrische Daten notwendig.

WAS TUN?

Die Gefahren biometrischen Anwendungen erzeugen erhöhten Schutz- und Steuerungsbedarf:

- Ein klares Verbot biometrischer Methoden im öffentlichen Raum und insbesondere von Echtzeitüberwachung auf Basis von Biometrie und Gesichtserkennung sollte angedacht werden. Das sollte auch indirekte Überwachung etwa durch Verknüpfen privater und öffentlicher biometrischer Datenbestände umfassen.
- Es sollte mehr Rechtssicherheit und klare Trennung zwischen Authentifizierung und Identifizierung geschaffen werden. Biometrie verwischt hier die Grenzen. Es ist daher nötig, den Einsatz von Biometrie enger zu regulieren, um einer ausufernden Kommerzialisierung biometrischer Daten entgegenzuwirken.
- Gesichtsbilder und Sprachaufnahmen sollten grundsätzlich als biometrische Daten eingestuft und entsprechend geschützt werden, um Missbrauchsrisiken einzudämmen.
- Datenschutz- und Sicherheitsstandards sollten erhöht werden, um die Risiken biometrischer Verfahren einzugrenzen. Es braucht höhere und verbindliche Mindeststandards für Datensicherheit und Transparenz biometrischer Verfahren auf nationaler, europäischer und internationaler Ebene.
- Die komplexe globale Problematik erfordert es, in der EU und in weiterer Folge auch international eine harmonisierte Regulierung anzustreben.

ZUM WEITERLESEN

Schaber, F.; Strauß, S; Peissl, W. (2020) Der Körper als Schlüssel – Biometrische Methoden für Konsument*innen; Endbericht, Nr. ITA-2020-03, Wien: Institut für Technikfolgen-Abschätzung (ITA) in Kooperation mit der Bundesarbeitskammer
epub.oeaw.ac.at/ita/ita-projektberichte/2020-03.pdf

KONTAKT

Stefan Strauß
E-Mail: *tamail@oeaw.ac.at*
Telefon: +43 1 51581-6582

IMPRESSUM: Medieninhaber: Österreichische Akademie der Wissenschaften; Juristische Person öffentlichen Rechts (BGBl. 569/1921 i.d.F. BGBl. I 31/2018); Dr. Ignaz Seipel-Platz 2, A-1010 Wien; Herausgeber: Institut für Technikfolgen-Abschätzung (ITA); Apostelgasse 23, A-1030 Wien; *www.oeaw.ac.at/ita* | Erscheinungsweise: Die ITA-Dossiers erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des ITA. Die Dossiers werden in kleiner Auflage gedruckt und open access über das Portal „epub.oeaw" zur Verfügung gestellt: *epub.oeaw.ac.at/ita/ita-dossiers* | ISSN: 2306-1960

ITA-Dossier Nr. 53, Februar 2021, *epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier055.pdf* | Koautoren: Schaber, F., Peissl, W.