TAB
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Neue Anwendungsfelder biometrischer Identifikationsverfahren

Themenkurzprofil Nr. 29 | Stephan Richter • Tobias Jetzke | Mai 2019

In vielen staatlichen und unternehmerischen Bereichen ist die Fähigkeit, Menschen zuverlässig und gegebenenfalls in Echtzeit mit technischen Mitteln identifizieren zu können, zu einem wichtigen Werkzeug geworden – hierzu gehören beispielsweise der Grenzübertritt, die Forensik oder die Zugangskontrolle in Gebäuden. Die hierfür entwickelten biometrischen Verfahren nutzen verschiedene messbare, individuelle verhaltensbedingte Merkmale (wie Stimme, Schreibverhalten, Lippenbewegung) oder Körpercharakteristika (wie Fingerabdruck, Gesicht oder Muster der Iris), um eine Person automatisiert zu erkennen.

Über öffentliche Anwendungen hinaus halten biometrische Identifikationsverfahren immer mehr Einzug in unseren privaten Alltag. Typische Beispiele sind der Zugangsschutz für IKT-Endgeräte (Smartphones, Tablets, PC) oder die Freigabe von Onlinezahlungen durch den Abgleich des Fingerabdrucks oder von Gesichtsmerkmalen. Vor allem mobile biometrische Verfahren erleben durch die zunehmende technologische Reife aktuell einen regelrechten Hype. Es wird davon ausgegangen, dass ab 2020 alle neu auf den Markt gebrachten Smartphones, Wearables und Tablets biometriefähig sein werden.

Nach einer Umfrage von IBM aus dem Jahr 2018 ist die Akzeptanz für die private Nutzung von (mobilen) biometrischen Identifikationsverfahren in der Bevölkerung hoch (Tendenz steigend). Auch wenn im Vergleich zur Jahrtausendwende die Technologiereife gestiegen ist und sich Sicherheitsmerkmale verbessert haben, bestehen weiterhin Bedenken, zum Beispiel in Bezug auf das Manipulationspotenzial. So könnten etwa mittels künstlicher Intelligenz (KI) entwickelte Fingerabdrücke als eine Art Generalschlüssel eingesetzt werden. Auch Fragen hinsichtlich des Datenschutzes sind mit Blick auf einen rechtskonformen Einsatz biometrischer Verfahren noch nicht abschließend beantwortet.

Hintergrund und Entwicklung

Biometrische Identifikationsverfahren sind Systeme, die auf Basis biometrischer Merkmale Personen erkennen und eindeutig identifizieren können (Corcoran/Costache 2016; Unar et al. 2014). Zu den individuellen biometrischen Merkmalen des Menschen zählen verhaltensspezifische Eigenschaften (wie Tippverhalten, Stimme, Schrift oder Gangart) oder Körpereigenschaften, etwa der Hand (z.B. Fingerabdruck), des Gesichts (z.B. Gesichtszüge und -proportionen) oder der Augen (z.B. Muster der Iris) sowie Charakteristika der Physiologie und Biochemie (z.B. DNA oder Körpergeruch) (Abb. 1).

Die Nutzung biometrischer Merkmale hat eine lange Historie

Biometrische Merkmale wurden schon vor mehreren hundert Jahren genutzt. Bereits im 14. Jahrhundert wurden in China Fingerabdrücke verwendet, um die Identität von Kaufleuten festzustellen (Kalyani 2017). Seit Ende des 19. Jahrhunderts werden biometrische Merkmale für die Strafverfolgung genutzt (Jain et al. 2016). Es ist überliefert, dass die argentinische Polizei erstmals im Jahr 1892 Fingerabdrücke als Beweismittel in einem Mordfall einsetzte. 1901 begann Scotland Yard in Großbritannien, Fingerabdrücke in der Strafverfolgung zu nutzen, die 1905 erstmals in einem Strafverfahren als Beweismittel akzeptiert worden sind. In Deutschland wurde 1903 ein System des Fingerabdrucks offiziell eingeführt (BSI o.J.a). In den USA wurde das Justizministerium im Jahr 1924 durch den Kongress ermächtigt, Fingerabdrücke von verhafteten Personen zu erheben. Dies war ein wichtiger Grundstein für die Etablierung der sogenannten „ten print cards“ durch das

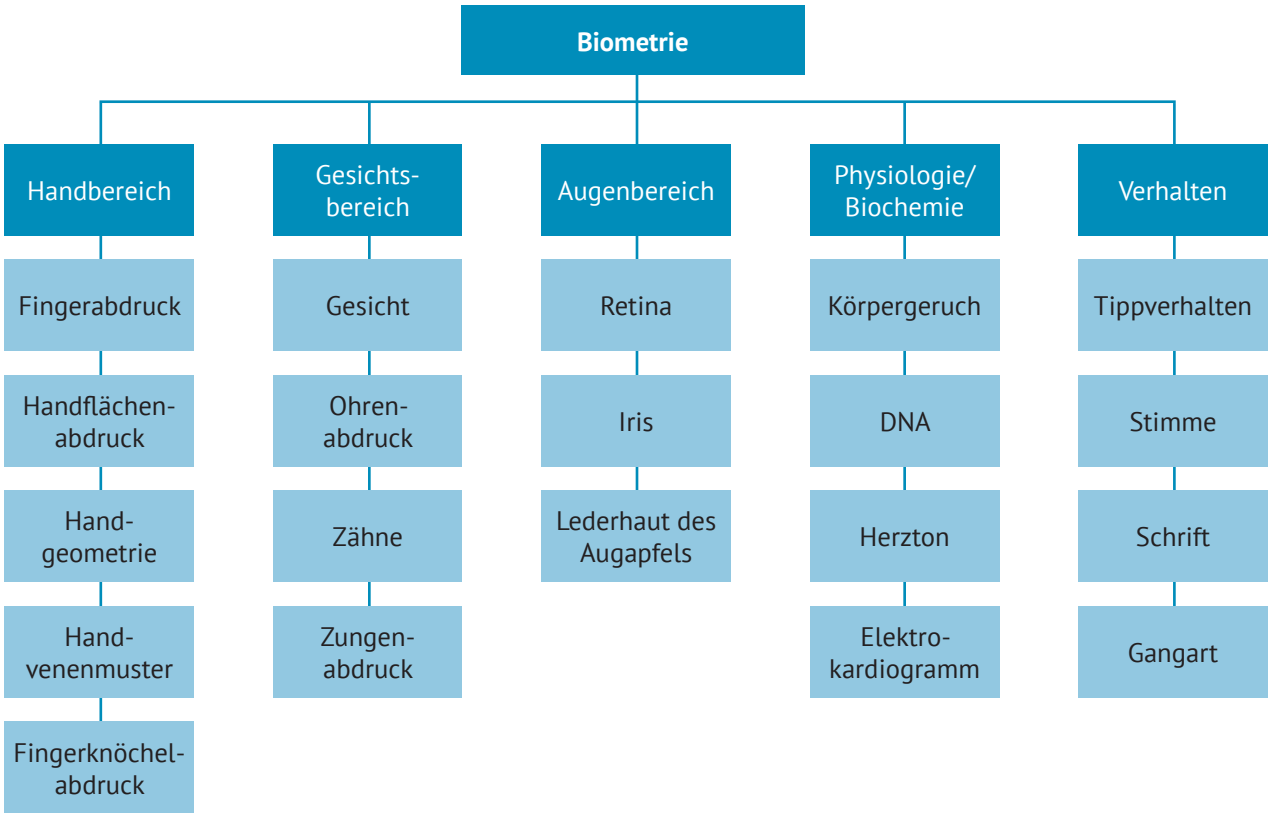


Abbildung 1: Biometrische Merkmale; angepasst nach Unar et al. (2014).

FBI, also Karten, auf denen die Abdrücke aller zehn Finger festgehalten werden.

Nachdem man Fingerabdrücke zunächst ausschließlich manuell analysierte, wurden in den 1960er Jahren erstmals automatisierte Verfahren für diese Aufgabe entwickelt (Trauring 1963). Zur gleichen Zeit begann die Entwicklung weiterer Identifikationsverfahren, die auf anderen biometrischen Merkmalen wie beispielsweise Gesicht, Stimme oder Unterschrift basierten (Jain et al. 2016).

Funktionsweise biometrischer Identifikationserfahren

Um biometrische Identifikationsverfahren betreiben zu können, müssen diejenigen Personen, die später vom System erkannt werden sollen, zunächst registriert werden (Jain et al. 2016). Hierfür werden die biometrischen Merkmale einer Person mithilfe eines spezifischen Sensors vermessen. Aus den aufgenommenen Daten wird mittels eines Algorithmus ein individueller Biometriedatensatz extrahiert, der zusammen mit der Identität der jeweiligen Person in einer Referenzdatenbank gespeichert wird.

Während des Betriebs biometrischer Identifikationsverfahren werden die hinterlegten Registrierungsdaten mit den biometrischen Merkmalen der zu überprüfenden Person auf Übereinstimmung geprüft. Hierbei lassen sich zwei Betriebsarten unterscheiden:

1. Bei der Verifikation (auch: Authentifikation) wird die Identität einer Person bestätigt. Es wird überprüft, ob es sich bei einer Person um diejenige handelt, die sie vorgibt zu sein. Dazu werden die biometrischen Daten der Person erfasst und mit den von dieser Person im Vorfeld erfassten biometrischen Referenzdaten verglichen (1:1-Vergleich) (Corcoran/Costache 2016; Unar et al. 2014). Zu den typischen Anwendungsfeldern solcher Systeme zählen Zugangskontrollen, die Benutzerauthentifizierung auf mobilen Geräten und Computern, am Geldautomaten oder bei E-Commerce-Anwendungen (Unar et al. 2014). Hier stellt der Nutzer seine biometrischen Daten in der Regel freiwillig zur Verfügung, um Zugang zu Geräten, Gebäuden oder Dienstleistungen zu erhalten.
2. Bei der Identifikation geht es um die Feststellung der Identität einer Person im Vergleich zu einer Vielzahl an zuvor registrierten Personen. Der biometrische Datensatz der zu identifizierenden Person wird dazu mit allen in der Datenbank vorhandenen Referenzdatensätzen auf Übereinstimmung geprüft (1:n-Vergleich) (Corcoran/Costache 2016; Unar et al. 2014). Anwendungsfelder solcher Systeme sind bislang überwiegend in staatlichen Kontexten zu finden. Im Bereich der Strafverfolgung werden diese genutzt, um Personen anhand ihrer Fingerabdrücke oder Gesichter über den Abgleich mit entsprechenden Datensätzen in polizeilichen (Fahndungs-)Datenbanken zu identifizieren. Ein aktuelles Beispiel in diesem Zusammenhang ist der zwischen 2017 und 2018 durchgeführte Pilotversuch zur automatisierten Gesichtserkennung am Bahnhof Berlin Südkreuz, in dessen Rahmen die technische Eignung derzeit verfüg-

barer biometrischer Gesichtserkennungssysteme für die Personenfahndung in Echtzeit getestet wurde (Bundespolizeipräsidium Potsdam 2018). Solche Anwendungsfelder werden nachfolgend nicht weiter vertieft, weil das Kurzprofil auf private Nutzungsformen biometrischer Identifikationsverfahren fokussiert.

Die Zuverlässigkeit hängt von verschiedenen Faktoren ab

Entscheidend für den Einsatz biometrischer Verfahren ist deren Zuverlässigkeit, die zuvor in der Referenzdatenbank erfassten Personen richtig zu erkennen. Die Messergebnisse eines biometrischen Merkmals einer Person werden allerdings durch unterschiedliche Faktoren beeinflusst, beispielsweise durch Sensorrauschen, veränderte Umgebungsbedingungen während des Messvorgangs (Beleuchtung, Temperatur, Luftfeuchtigkeit etc.) oder durch im Zeitverlauf variierende Körpercharakteristika oder Verhaltensänderungen des Nutzers, etwa Verletzungen wie Schnitte und Prellungen am Finger, Alterserscheinungen, Krankheiten oder Operationen (Jain et al. 2004).

In der Praxis führt dies dazu, dass Personen vom System nicht immer korrekt erkannt werden können. Dabei ist grundsätzlich zwischen zwei Arten von Erkennungsfehlern zu unterscheiden (Jain et al. 2004): der Zulassungsrate Unberechtigter (Falschakzeptanzrate [FAR]), also der Quote fälschlicherweise zugelassener Nutzer, sowie der Abweisungsrate Berechtigter (Falschrückweisungsrate [FRR]), also der Quote fälschlicherweise nicht zugelassener Nutzer.

Biometrische Identifikationsverfahren werden zunehmend privat genutzt

Wurden biometrische Identifikationsverfahren ursprünglich vor allem in staatlichen Kontexten, insbesondere im Bereich der Strafverfolgung, entwickelt und eingesetzt, werden sie seit einigen Jahren vermehrt auch im unternehmerischen Umfeld (hier insbesondere für Zugangskontrollen) und in stark wachsendem Umfang im Privatbereich genutzt.

Aktuelle Marktstudien bestätigen die zunehmende Verbreitung biometrischer Identifikationsverfahren im Privatbereich. Während beispielsweise 2010 der Technologieeinsatz im Sicherheitssektor bei 58 %, im industriellen Bereich bei 40 % und nur zu 2 % im Konsumgüterbereich lag, hat sich dieses Verhältnis im Jahr 2016 deutlich zugunsten des Konsumgüterbereichs verschoben: Beinahe zwei Drittel des Umsatzes mit biometrischen Technologien entfielen 2016 auf den Konsumgüterbereich (Statista 2018).

Für die erfolgreiche Einführung biometrischer Identifikationsverfahren im privaten Bereich spielte deren technische Integration in mobile Endgeräte, vor allem Smartphones, Wearables und Tablets, eine maßgebliche Rolle. Diese begann bereits in den frühen 2000er Jahren, zum Beispiel in Form von Fingerabdrucksensoren in persönlichen digitalen Assistenten (PDAs). Auf breiter Front konnte sich die Technologie aber erst mehr als 10 Jahre später durchsetzen (Corcoran/Costache 2016). Mit der Einführung des Fingerabdrucksensors Touch IDTM wurden biometrische Identifikationsverfahren ab dem Jahr 2013 zu einer Standardtechnologie für mobile Endgeräte. Aktuell etabliert sich immer mehr auch die Authentifizierung via Gesichtsmerkmale oder Stimmerkennung im privaten Bereich. Zusätzlich zum Fingerabdruck können die biometrischen Merkmale der Hand und der Augen oder auch das Tippverhalten für eine mobile Authentifizierung genutzt werden (Alzubaidi/Kalita 2016; Corcoran/Costache 2016; Spolaor et al. 2016; Wojciechowska et al. 2017).

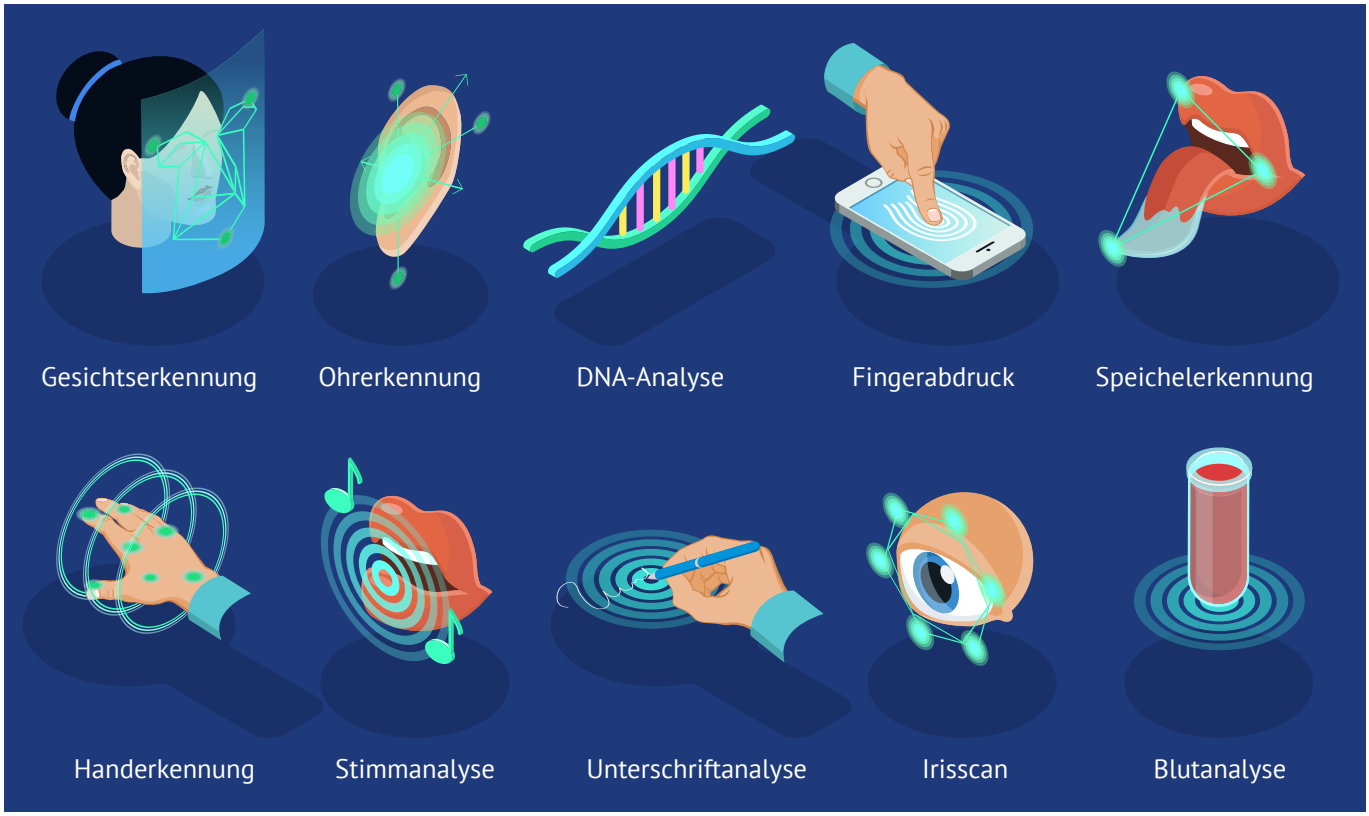
Die zunehmende Verbreitung biometrischer Identifikationsverfahren in Smartphones, Wearables und Tablets – bereits im Jahr 2020 sollen alle neu auf den Markt gebrachten Geräte über ebensolche Technologien verfügen (Statista 2017) – ist ein Indikator dafür, dass zukünftig weitere Anwendungsfelder für biometrische Identifikationsverfahren im Privatbereich erschlossen werden könnten, beispielsweise bei der Authentifizierung für das Onlinebanking oder im Kontext von E-Commerce.

Die Akzeptanz biometrischer Identifikationsverfahren scheint hoch zu sein. So ziehen laut einer Umfrage von IBM weltweit 87 % der Menschen eine zukünftige Nutzung biometrischer Identifikationsverfahren zur Authentifizierung in Erwägung (Kessem 2018). In Deutschland zeichnet sich ein ähnliches Bild ab: 60 % der Menschen gaben 2016 an, dass sie sich vorstellen könnten, sich beim bargeldlosen Bezahlen mit Fingerabdruck oder Irisscan zu identifizieren (Bitkom 2016). Zukünftig kann also eine vermehrte Nutzung biometrischer Identifikationsverfahren im Privatbereich erwartet werden.

Gesellschaftliche und politische Relevanz

Biometrische Identifikationsverfahren sind bequem für Nutzer, bergen aber auch Risiken

Aus gesellschaftlicher Sicht bieten private Nutzungsformen biometrischer Identifikationsverfahren Chancen vor allem in Bezug auf die Nutzerfreundlichkeit und Sicherheit: Ihr Einsatz für die Nutzerauthentifizierung kann den Zugang zu Onlinedienstleistungen erleichtern und beispielsweise



Vertragsabschlüsse, Finanztransaktionen oder den Zugriff auf Onlinekonten vereinfachen. Zudem ermöglicht die Einbindung von biometrischen Merkmalen neue Formen der Zwei-Faktor-Authentifizierung, wenn biometrische Verfahren zusammen mit Passwörtern oder zum Beispiel einem TAN-Generator eingesetzt werden. Für den Zugriff auf besonders schützenswerte Dienste wie Onlinebanking, Onlineshopping oder Onlinespeicher empfiehlt das Bundesamt für Sicherheit (BSI o.J.b) in der Informationstechnik eine solche Zwei-Faktor-Authentifizierung.

Der Nutzung der genannten Chancen stehen jedoch Bedenken hinsichtlich der Manipulierbarkeit und damit insbesondere der Sicherheit biometrischer Identifikationsverfahren gegenüber. So ist es zum Beispiel möglich, Verfahren zur Gesichtserkennung mittels hochauflösender Fotos zu täuschen (Alsbih/Schmitz 2017). Auch konnte gezeigt werden, dass ein mithilfe von KI entwickelter biometrischer Generalschlüssel für Fingerabdrucksensoren – ein sogenannter „deep master print“ – eine Vielzahl gängiger Smartphonemodelle entschlüsseln konnte (WIRED Staff 2018). Der Chaos Computer Club machte ebenfalls auf die Schwächen biometrischer Verfahren aufmerksam, indem dieser die Fingerabdrücke von Wolfgang Schäuble und die Irismerkmale von Angela Merkel erfolgreich fälschte (Alsbih/Schmitz 2017).

Die größten Bedenken bei der Nutzung biometrischer Identifikationsverfahren zur Authentifizierung liegen jedoch in den Feldern Datenschutz und Datensicherheit (Dewa 2017). Diese erscheinen dann berechtigt, wenn biometrische Daten nicht ausreichend sicher verwahrt bzw. auf Servern in Ländern mit weniger strengem Datenschutz gespeichert werden. Es können grundsätzlich zwei Problembereiche unterschieden werden: der Identitätsdiebstahl sowie der Identitätsverlust.

- Bei einem Diebstahl biometrischer Daten können, anders als bei Passwörtern, PINs oder etwa Bankkarten, die biometrischen Merkmale nicht einfach zurückgesetzt werden. Wenn biometrische Daten einer Person gestohlen werden, dann sind die Folgen für die Betroffene oder den Betroffenen gravierend, da sich fremde Personen dauerhaft der biometrischen Identität der bestohlenen Person bemächtigen können. Ist der fremden Person zudem bekannt, wem die Biometriedaten gehören und welche Dienstleistungen damit geschützt wurden, kann sie alle diese Dienstleistungen unbefugt nutzen. In der Folge können die betroffenen Personen die fraglichen Dienstleistungen nicht mehr sicher schützen und in der Konsequenz ggf. auch nicht weiter nutzen (Corcoran/Costache 2016).
- Ein sogenannter Identitätsverlust droht, wenn durch Krankheit, Unfall oder Behinderung biometrische Merkmale eingebüßt werden oder ihre Maschinenlesbarkeit beeinträchtigt wird. Ein solches Szenario wurde in Indien bereits Realität. Hier verlor eine an Lepra erkrankte Frau die Möglichkeit, sich durch Fingerabdrücke oder Irisscan zu identifizieren, was die Voraussetzung für die Fortzahlung ihrer Rente war (Lobe 2018). Eine Weiterzahlung konnte nur auf Basis eines Härtefallantrags einer „biometrischen Ausnahme“ erwirkt werden. Ein solches Beispiel ist nicht nur aus Aspekten der Datensicherheit relevant, sondern verweist auch auf eine mögliche gesellschaftliche Ausgrenzung von Menschen mit fehlenden oder eingeschränkten biometrischen Merkmalen.

Hieraus leitet sich ab, dass die gesellschaftlich akzeptable Gestaltung von Systemen, die anhand biometrischer Merkmale einen Zugang zu sozialen oder anderen Leistungen (z.B. Dienstleistungen im Finanzbereich) ermöglichen, die Barrierefreiheit sowie der Schutz vor Diebstahl bzw. Missbrauch sensibler Daten eine hohe Priorität für die Entwickler bzw. Anbieter solcher Systeme haben sollten.

Datenschutz-Grundverordnung und Bundesdatenschutzgesetz regeln die Nutzung

Biometrische Daten werden durch Artikel 9 Datenschutz-Grundverordnung ausdrücklich zu den besonderen Kategorien personenbezogener Daten gezählt, deren Verarbeitung grundsätzlich nur unter sehr engen Voraussetzungen zulässig ist. Für private Anwendungsformen von biometrischen Identifikationsverfahren beispielsweise zur Authentifizierung beim Smartphone oder Onlinebanking ist Artikel 9 Absatz 2 lit. a Datenschutz-Grundverordnung einschlägig, in dem geregelt ist, dass die betroffene Person der Verarbeitung biometrischer Daten für diesen Zweck ausdrücklich zustimmen muss.

Außer der Anforderung einer ausdrücklichen Einwilligung nennt der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI o.J.). weitere Maßstäbe für die datenschutzkonforme Verarbeitung biometrischer Daten. Wichtige Kriterien bestehen zum Beispiel darin, dass nur solche Verfahren zum Einsatz kommen, die eine Benachteiligung bestimmter Personengruppen weitgehend ausschließen und nur die für den späteren Vergleich notwendigen biometrischen Merkmale, jedoch keine darüber hinausgehenden Informationen aufnehmen und speichern. Ferner soll eine strenge Zweckbindung der Daten sichergestellt sein, wobei die Datensätze nur in einer gesicherten Umgebung (Netzwerk, Datenbank) verarbeitet werden sollten. Dabei sollte auch auf eine zentrale Speicherung der Daten (z.B. auf Servern oder in Clouds) zugunsten einer lokalen Speicherung (z.B. auf dem Smartphone, einer Chipkarte oder einem Ausweis) verzichtet werden. Außerdem sollte auf eine transparente Darstellung biometrischer Verfahren und auf Sicherheitsmechanismen geachtet werden, die vor unbefugtem Zugriff schützen und eine Löschung biometrischer Daten vorsieht, wenn diese nicht mehr verwendet werden.

Inwieweit die aufgeführten Maßstäbe für einen datenschutzkonformen Umgang mit biometrischen Daten bei aktuellen Anwendungen im privaten Bereich umgesetzt werden, kann an dieser Stelle nicht beantwortet werden.

Mögliche vertiefte Bearbeitung des Themas

Aufgrund der aktuellen Entwicklungen und der erheblichen gesellschaftlichen und politischen Relevanz bietet sich das Thema für eine Bearbeitung als TAB-Kurzstudie an. Ziel wäre es, einen Überblick über die wichtigsten biometrischen Identifikationsverfahren zu geben und den aktuellen Stand von Technik und Entwicklung darzustellen. Als Ausgangspunkt könnten die veröffentlichten TAB-Arbeitsberichte Nr. 76 „Biometrische Identifikationssysteme“ (TAB 2002) und Nr. 93 „Biometrie und Ausweisdokumente“ (TAB 2003) dienen. Mit Blick auf die zunehmende Verbreitung von biometrischen Identifikationsverfahren in privaten bzw. unternehmerischen Einsatzkontexten bietet es sich an, hier vorhandene Anwendungspotenziale systematisch zu erheben und darzustellen, um darauf aufbauend künftige Entwicklungspfade abschätzen, Fragen der Nutzerakzeptanz diskutieren und mögliche gesellschaftliche und politische Implikationen analysieren zu können. Auf dieser Basis könnten beispielsweise verbraucher- und datenschutzrechtliche Handlungsoptionen für den Umgang mit biometrischen Identifikationsverfahren in verschiedenen, vorrangig privaten Anwendungskontexten erarbeitet werden.

Literaturverzeichnis

- Alsbih, A.; Schmitz, P. (2017): Biometrische Authentifizierung. 6 Tücken der Biometrie. Security Insider 9.2.2017, https://www.security-insider.de/6-tuecken-der-biometrie-a-579740/ (11.3.2019)
- Alzubaidi, A.; Kalita, J. (2016): Authentication of Smartphone Users Using Behavioral Biometrics. In: IEEE Communications Surveys & Tutorials 18(3), S. 1998–2026
- BfDI (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) (o.J.): Biometrie und Datenschutz. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/BiometrieUndDatenschutz.html (28.3.2019)
- Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) (2016): Interesse an biometrischen Verfahren wächst. Presseinformation, 8.1.2016,https://www.bitkom.org/Presse/Presseinformation/Interesse-an-biometrischen-Verfahren-waechst.html (11.3.2019)
- BSI (Bundesamt für Sicherheit in der Informationstechnik) (o.J.a): Grundsätzliche Funktionsweise biometrischer Verfahren. https://www.bsi.bund.de/DE/Themen/

DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html (11.4.2019)
- BSI (o.J.b): Sicheres Einloggen leicht gemacht. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/2FA-zwei-faktor-authentisierung.html (11.4.2019)
- Bundespolizeipräsidium Potsdam (2018): „Biometrische Gesichtserkennung" am Bahnhof Berlin Südkreuz. https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=B00C5E4B9341D9F8733EF8508A6D9C46.2_cid324?__blob=publicationFile&v=1 (27.3.2019)
- Corcoran, P.; Costache, C. (2016): Biometric Technology and Smartphones. A consideration of the practicalities of a broad adoption of biometrics and the likely impacts. In: IEEE Consumer Electronics Magazin 5(2), S. 70–78
- Dewa, Z. (2017): The Relationship between Biometric Technology and Privacy: A Systematic Review. In: Kapoor, S. (Hg.): Proceedings of the Future Technologies Conference (FTC) 2017, S. 739–748
- Jain, A.K.; Nandakumar, K.; Ross, A. (2016): 50 years of biometric research. Accomplishments, challenges, and opportunities. In: Pattern Recognition Letters 79, S. 80–105
- Jain, A.K.; Ross, A.; Prabhakar, S. (2004): An Introduction to Biometric Recognition. In: IEEE Transactions on Circuits and Systems for Video Technology14(1), S. 4–20
- Kalyani, C. H. (2017): Various Biometric Authentication Techniques. A Review. In: Journal of Biometrics & Biostatistics 8(5), doi: 10.4172/2155-6180.1000371
- Kessem, L. (2018): IBM Security: Future of Identity Study. Consumer perspectives on authentication: Moving beyond the password (Autoren: Lalan, C.; Billings, L.; Mulligan, B.). https://www.ibm.com/downloads/cas/QRBY08NO (11.3.2019)
- Lobe, A. (2018): Wer keine Biometrie hat, ist kein Bürger. Süddeutsche Zeitung, 27.10.2018, https://www.sueddeutsche.de/digital/biometrie-gesichtserkennung-fingerabdruck-spracherkennung-1.4183394 (19.3.2019)
- Spolaor, R.; Li, Q.; Monaro, M.; Conti, M.; Gamberini, L.; Sartori, G. (2016): Biometric Authentication Methods on Smartphones: A Survey. In: PsychNology Journal 14(2-3), S. 87–98
- Statista GmbH (2018): Global biometric hardware market from 2010 to 2021, by segment. https://www.statista.com/statistics/654544/biometric-hardware-global-market-by-segment/ (11.3.2019)
- TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2002): Biometrische Identifikationssysteme (Autoren: Petermann, T.; Sauter, A.). TAB-Arbeitsbericht Nr. 76, Berlin
- TAB (2003): Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung (Autoren: Petermann, T.; Scherz, C.; Sauter, A.). TAB-Arbeitsbericht Nr. 93, Berlin
- Trauring, M. (1963): Automatic comparison of finger-ridge patterns. In: Nature 197, S. 938–940
- Unar, J. A.; Seng, W. C.; Abbasi, A. (2014): A review of biometric technology along with trends and prospects. In: Pattern Recognition 47(8), S. 2673–2688
- WIRED Staff (2018): Eine KI hat einen Master-Fingerabdruck entwickelt, der in Smartphones einbricht. GQ Magazin, 19.11.2018, https://www.wired.de/article/eine-ki-hat-einen-master-fingerabdruck-entwickelt-der-in-smartphones-einbricht (11.3.2019)
- Wojciechowska, A.; Choraś, M.; Kozik, R. (2017): The overview of trends and challenges in mobile biometrics. In: Journal of Applied Mathematics and Computational Mechanics 16(2), S. 173–185

Das Horizon-Scanning ist Teil des methodischen Spektrums der Technikfolgenabschätzung im TAB.

Horizon SCANNING

Mittels Horizon-Scanning werden wissenschaftlich-technische Trends und sozio-ökonomische Entwicklungen in frühen Entwicklungsstadien beobachtet und in den Kontext gesellschaftlicher Debatten eingeordnet. So sollen Innovationssignale möglichst früh erfasst und ihre technologischen, ökonomischen, ökologischen, sozialen und politischen Veränderungspotenziale beschrieben werden. Ziel des Horizon-Scannings ist es, einen Beitrag zur forschungs- und innovationspolitischen Orientierung und Meinungsbildung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung zu leisten.

In der praktischen Realisierung wird das Horizon-Scanning als Kombination softwaregestützter Such- und Analyseschritte und eines expertenbasierten Validierungs- und Bewertungsprozesses durchgeführt.

Herausgeber: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)
Gestaltung und Redaktion: VDI/VDE Innovation + Technik GmbH
Bildnachweise: © NicoElNino/AdobeStock (S. 1), TimeStopper/AdobeStock (S. 3), ivan mogilevchik/AdobeStock (S. 4), svetlana67/AdobeStock (S. 5)
Stand: Mai 2019
ISSN-Internet: 2629-2874