ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

PROJEKTBERICHT

www.oeaw.ac.at/ita

DER KÖRPER ALS SCHLÜSSEL?

Biometrische Methoden für Konsument*innen

ITA-Projektbericht Nr.: 2020-03 | ISSN: 1819-1320 | ISSN-Online: 1818-6556

ITA INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG

DER KÖRPER ALS SCHLÜSSEL?

Biometrische Methoden für Konsument*innen

Endbericht

Institut für Technikfolgen-Abschätzung
der Österreichischen Akademie der Wissenschaften
Projektleitung: Walter Peissl
Autor*innen: Felix Schaber
Stefan Strauß
Walter Peissl

Studie in Kooperation mit der Bundesarbeitskammer

Wien, November 2020

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF 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

Die ITA-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung
der Forschungsergebnisse des Instituts für Technikfolgen-Abschätzung.
Die Berichte erscheinen in geringer Auflage im Druck und werden über das
Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-projektberichte

ITA-Projektbericht Nr.: 2020-03
ISSN: 1819-1320
ISSN-online: 1818-6556
epub.oeaw.ac.at/ita/ita-projektberichte/2020-03.pdf

INHALT

Abbildungsverzeichnis

ZUSAMMENFASSUNG

Die vorliegende Studie beschäftigt sich mit den Auswirkungen des breiten Einsatzes biometrischer Verfahren auf Konsument*innen und die Gesellschaft insgesamt. Sie gibt einen Überblick über gängige Methoden und diskutiert allgemein Chancen und Risiken von Biometrie und dem Umgang mit biometrischen Daten.

Im Abschnitt über technische Grundlagen der Biometrie werden grundlegende Begriffe und Mechanismen geklärt. Biometrische Verfahren dienen in der Regel dazu, Personen durch Erfassung und Analyse bestimmter, für die Person charakteristischer Merkmale zu identifizieren. Diese Merkmale werden biometrische Merkmale genannt. Dazu gehören charakteristische Eigenschaften von Gesicht oder Fingerabdruck ebenso wie verhaltenstypische Merkmale wie Unterschrift, Gangart oder auch Sprachmuster.

Chancen und Risiken

Eines der Wesensmerkmale biometrischer Daten ist deren Inhärenz und damit Unabstreitbarkeit. Sie bleiben immer mit dem Körper und damit mit der betroffenen Person verbunden. So können biometrische Merkmale im Gegensatz zu Wissen (Passwort) oder Besitz (Token) nicht vergessen, verloren oder ohne weiteres weitergegeben werden.[1] Dies kann zu einer erleichterten Bedienbarkeit beitragen. Gleichzeitig ist ein Ändern oder Verbergen dieser Merkmale nicht möglich bzw. nicht praktikabel.[2] Die Inhärenz biometrischer Merkmale wird oft als zusätzliches Sicherheitsmerkmal angesehen, wie sich aber zeigt, ist gerade das durch die weite Verbreitung und den Einsatz in unterschiedlichsten Bereichen ein Einfallstor für Missbrauch und somit ein gesteigertes Risiko.

Authentifizierung, Verifikation und Identifikation

Eine der wichtigsten Funktion biometrischer Merkmale ist die Authentifizierung von Personen, also die Feststellung ob jemand über eine gültige Berechtigung wie z. B. Zugang zu einer Anwendung verfügt. Dabei werden die biometrischen Merkmale die bei der einmalig notwendigen Registrierung im jeweiligen System erfasst wurden mit den gespeicherten bzw. aktuellen Merkmalen verglichen. Stimmen die Merkmale hinreichend überein, wird davon ausgegangen, dass es sich um dieselbe Person handelt. Damit verbundene wichtige Anwendungen sind Verifikation und Identifikation. Werden die biometrischen Merkmale einer einzelnen, bestimmten Person verglichen, handelt es sich um eine Verifikation, beim Vergleich biometrischer Merkmale mit vorerfassten Referenzdaten mehrerer Personen spricht man von Identifikation. Wichtig dabei ist, dass sich biometrische Merkmale über die Zeit verändern und niemals eine 100 %ige De-

[1] Zu berücksichtigen ist allerdings, dass sich biometrische Merkmale über die Zeit graduell ändern bzw. abnutzen können oder etwa durch Unfälle völlig verändert werden.

[2] Siehe z. B. *Jain/Nandakumar/Ross*, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 2016, 80–105.

ckung erreicht werden kann, es sich also immer um eine (möglichst hohe) Wahrscheinlichkeit der Übereinstimmung handelt.

bewusste vs unbewusste Datenerfassung

Neue technischen Möglichkeiten, verbesserte Verfahren führen dazu, dass auch ausgehend von weniger genauen Rohdaten z. B. Profilfotos im Internet eine biometrische Vermessung stattfinden kann. Damit steigt die für Konsument*innen unbewusste Datenerfassung und damit Identifizierbarkeit an, ohne dass diese der Nutzung der Daten zugestimmt haben.

biometrische Daten ieS

und

biometrische Daten iwS

In der rechtlichen Analyse zeigt sich, dass biometrische Daten zweifellos sensible Daten und damit besonders schützenswert sind. Neben der allgemeinen Bewertung biometrischer Daten im Rahmen der Europäischen Datenschutzgrundverordnung[3] (DSGVO) und des Datenschutzgesetzes (DSG), wird insbesondere auf den Umstand verwiesen, dass die DSGVO zwar eine Legaldefinition des Begriffs der biometrischen Daten enthält,[4] diese „biometrische Daten im engeren Sinne" allein besonders zu schützen jedoch aus Sicht des Schutzes der Privatsphäre unzureichend ist. Es gibt eine Reihe von biometrischen Daten, die von dieser Legaldefinition nicht erfasst werden (z. B. Gesichtsbilder im Internet) – so genannte biometrische Daten im weiteren Sinne. Da diese weit verbreitet sind und weitgehend denselben Auswertungsmöglichkeiten unterliegen, wird für eine Ausweitung des Schutzes durch die DSGVO auf diesen weiteren Begriff plädiert.

zunehmende Kommerzialisierung einer Sicherheitstechnologie

Fokus auf Bequemlichkeit

Bei der Darstellung der unterschiedlichen Anwendungsfelder zeigt sich seit einigen Jahren eine Zunahme biometrischer Anwendungen in unterschiedlichen Bereichen mit einer Tendenz zur Verbreitung in Alltagstechnologien und kommerziellen Anwendungen. Damit ergibt sich ein Wandel einer einstigen Sicherheitstechnologie im Kontext militärischer und sicherheitsrelevanter Anwendungen hin zum Einsatz im Consumer-Bereich und damit auch ein veränderter Fokus auf Convenience und weniger auf Sicherheit. Biometrie ist mittlerweile im Finanz- und Banksektor weit verbreitet. Sie wird nach der EU-Zahlungsdienste-Richtlinie oft als zusätzlicher Faktor bei Banken-Apps und im Online-Handel eingesetzt. Die Nutzung am Smartphone zeitigt potenzielle Vorteile bezüglich Nutzbarkeit und Bequemlichkeit. Insgesamt sind jedoch Sicherheitsgewinne oft nur marginal oder sogar gegenteilige Effekte erkennbar. Die damit einhergehenden Gewöhnungseffekte senken die Hemmschwelle bei den Nutzer*innen und damit oft auch Sicherheitsbedenken und das Bewusstsein über die möglichen Gefahren. Dazu zählen neben erhöhtem Missbrauchsrisiko durch biometrische Daten vor allem schleichender Identifizierungszwang in vielen Anwendungsbereichen, die Massenüberwachung mit Biometrie und zu guter Letzt ein mögliches Ende der Anonymität.

---

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119 (4.5.2016), 1–88.

[4] Art 4 Z 14 DSGVO.

Gesichtserkennung als besonders problematische Anwendung

Eine besondere Stellung nimmt in dieser Entwicklung die Gesichtserkennung ein. Obwohl die Systeme immer noch sehr hohe Fehlerraten aufweisen und deshalb immer wieder Personen falsch als Verdächtige einstufen, werden sie von Sicherheitsbehörden eingesetzt. Zudem sind die verwendeten Algorithmen mit Bias behaftet, die Rassismus und Diskriminierung erzeugen können. Insgesamt dient die Gesichtserkennung zur Massenüberwachung, was in den USA wesentlich deutlicher sichtbar ist aber auch in Europa immer mehr an Bedeutung gewinnt. Die wachsende Verbreitung macht diese Technologie zu einer großen Gefahr für die Demokratie.

Nach der umfassenden Darstellung der Anwendungsgebiete und der erkennbaren gesellschaftlichen Auswirkungen des breiten Einsatzes biometrischer Systeme werden Handlungsempfehlungen formuliert:

Datenschutz- und Sicherheitsstandards und das generelle Schutzniveau zu erhöhen

Am vordringlichsten erscheint, den Datenschutz- und Sicherheitsstandards und das generelle Schutzniveau zu erhöhen, um so die Risiken biometrischer Verfahren einzugrenzen. Der Schutz der Privatsphäre wird durch den wachsenden Einsatz von Biometrie in einem noch höheren Ausmaß bedroht als bei herkömmlichen digitalen Verfahren, die keine körperspezifischen Daten erfassen. Erschwerend hinzu kommt, dass Biometrie auch Risiken für die Menschenwürde bedeuten kann, wenn biometrische Daten über Identität und Körpereigenschaften von teil- oder gänzlich automatisierten Prozessen und Algorithmen analysiert werden. Damit ist auch das grundsätzliche datenschutzrechtliche Verbot automatisierter Einzelentscheidungen und Profiling berührt, dass bei Biometrie noch mehr Risiken bezüglich Diskriminierung mit sich bringt. Eine Stärkung des Diskriminierungsverbots durch biometrische Daten erscheint daher angemessen.

Verfahren ohne dauerhafte Speicherung

Es sind Verfahren zu bevorzugen, bei denen es zu keiner dauerhaften Speicherung biometrischer Daten kommt. Die Einhaltung von Datenschutz- und Sicherheitsstandards sollte ebenfalls stärker sanktioniert werden, um zumindest einige Risiken zu reduzieren. Um das notwendige, höhere Schutzniveau zu erreichen sind spezifische Audits und Zulassungsverfahren überlegenswert, die Unternehmen, die Biometrie einsetzen wollen, verpflichtend absolvieren müssen. Dadurch könnte das Problem verringert werden, dass allgemeine, rein auf Rechtskonformität fokussierte Prüfverfahren die technischen Risiken nicht hinreichend erfassen und berücksichtigen können.

Sanktionen und Prüfverfahren

Abbau von rechtlichen Graubereichen wie z. B. bei Gesichtsbildern und Aufnahmen

Lichtbilder und Fotos mit Gesichtern können mit Gesichtserkennung ausgewertet werden und sollten daher grundsätzlich als biometrische Daten gelten. Nach derzeitiger Rechtslage ist das nicht immer eindeutig. Daher sind auch das Schutzniveau und die rechtlichen Anforderungen diesbezüglich unscharf. Daraus ergibt sich ein dringender Anpassungsbedarf, um mehr Klarheit zu schaffen und ein höheres Schutzniveau zu gewährleisten.

Wahlfreiheit und klare Grenzen bei Anwendungen

Bei jeder Biometrie-Anwendung ist vor dem Einsatz genau zu prüfen, ob die Verarbeitung biometrischer Daten notwendig, sinnvoll und verhältnismäßig ist. Daraus ergäbe sich auch eine stärkere Eingrenzung der Anwendungsbereiche. In Anwendungsbereichen, wo Biometrie als ergänzender Authentifikationsfaktor genutzt werden kann, wie etwa beim E-Ban-

king, ist sicherzustellen, dass die Daten vor externen Zugriffen geschützt sind und es zu keinerlei dauerhafter Speicherung von biometrischen Daten oder deren digitaler Komponenten (wie z. B. Hashwerte udgl.) kommt, um Risiken von Missbrauch und Identitätsdiebstahl zu minimieren. Darüber hinaus muss auch weiterhin Wahlfreiheit bei den Authentifizierungsverfahren gewährleistet sein. D. h. jede Konsument*in sollte selbst entscheiden können, ob ihre biometrischen Daten verarbeitet werden dürfen oder nicht.

Verbot von Gesichtserkennung im öffentlichen Raum und von Echtzeitüberwachung

Gesichtserkennung ist jene Technologie, die aus heutiger Sicht die größte Bedrohung für Grundrechte und Demokratie darstellt. Dieser Problemkomplex umfasst erhebliche Risiken, die von technischen Unzulänglichkeiten wie enorm hohen Fehlerraten, technologisch verschärfter Diskriminierung, Rassismus, Unterdrückung, Massenüberwachung bis zum Verlust von Privatsphäre, Anonymität und persönlicher Freiheit reichen. Daher sind im Umgang mit dieser Technologie besondere Vorsicht geboten und enge rechtliche Grenzen für deren Einsatz notwendig.

Aufgrund der enormen Gefahren wird ein klares Verbot von Echtzeitüberwachung empfohlen, um diese Gefahren möglichst einzudämmen. Das sollte auch jede mögliche Form der Verknüpfung öffentlicher und privater Videoüberwachungssysteme umfassen, um der Gefahr einer verdeckten Zentralisierung von Aufnahmen, die biometrische Daten enthalten, und damit verdeckte Massenüberwachung, zu verhindern.

Bedarf nach klaren Regelungen auf nationaler, europäischer und internationaler Ebene

Nach derzeitigem Stand gibt es erhebliche Regulierungslücken bei Gesichtserkennung auf nationaler, europäischer wie internationaler Ebene. Hier ist jedenfalls empfohlen, zu einer harmonisierten Regulierung zu kommen, um zu vermeiden, dass nationale Unterschiede zu einem Regulierungsvakuum führen mit negativen Folgen für den Schutz der Grundrechte. Eine klare Regelung auf EU-Ebene könnte dazu beitragen, dies zu verhindern und zu einer international wirksamen Regulierung von Gesichtserkennung und Biometrie zu gelangen (z. B. im Rahmen der Konvention 108).

1 EINLEITUNG

In der Öffentlichkeit wird zuletzt vermehrt die Frage der Gesichtserkennung im öffentlichen Raum diskutiert. Diese stellt unter anderem ein Überwachungsmittel dar, um Personen anhand ihrer körperlichen Merkmale zu identifizieren. Während diese Anwendungen vor allem von den Sicherheitsbehörden gefordert werden, sind Konsument*innen auch in vielen anderen Bereichen mit der Vermessung und Überwachung körperlicher Merkmale konfrontiert. Der Fingerabdruck zum Entsperren des Laptops, die Sprachanalyse bei Smarten Lautsprechern, die Gesichtserkennung beim Grenzübertritt im Urlaub, der Iris-Scan bei modernen Türschlössern – sie alle verarbeiten biometrische Merkmale.

Struktur der Studie

Die vorliegende Studie „Der Körper als Schlüssel? – Biometrische Methoden für Konsument*innen" gibt einen Überblick über gängige Methoden und diskutiert allgemein Chancen und Risiken biometrischer Informationen. Zu Beginn werden im Rahmen der Beschreibung der technischen Grundlagen der Biometire grundsätzliche Mechanismen und Begriffe geklärt. In der Analyse der rechtlichen Rahmenbedingungen für die Generierung, Speicherung und Verarbeitung biometrischer Daten wird ihre besondere Stellung als sensible Daten und ihre Einbettung in den Rahmen der DSGVO genauer diskutiert. Schließlich wird im Abschnitt über die Anwendungsgebiete deutlich, wie breit dieses Feld ist und welch unterschiedliche Methoden angewendet bzw. erforscht werden. Daran anschließend folgt eine Darstellung gesellschaftlicher Auswirkungen des breiten Einsatzes biometrischer Methoden, sowie ein kurzer Ausblick auf absehbare Entwicklungen in naher Zukunft. Abgeschlossen wird die Studie durch eine Reihe von Handlungsempfehlungen, die insbesondere an den Grundrechten auf Privatsphäre, Autonomie und Aufrechterhaltung demokratischer Strukturen und Prozesse orientiert sind.

Geschichte

Biometrische Daten sind schon lange in Verwendung, denken wir nur an Lichtbildausweis und Unterschrift als klassische, in der analogen Welt verwendete Biometrie. Spezielle biometrische Merkmale, wie zum Beispiel Fingerabdrücke, werden schon geraume Zeit in der Verbrechensaufklärung verwendet. Mit zunehmender Digitalisierung wurden die Methoden aus dem polizeilichen Sicherheitsapparat in private Sicherheitskonzepte überführt und so etwa der Zutritt zu sensiblen (Unternehmens-)Bereichen mittels Fingerabdruckscan ermöglicht. Die Miniaturisierung ermöglichte es, diese Technologie auf Laptops und schließlich auch auf Smartphones zu übertragen. Zeitlich versetzt wurde auch an der Vermessung und Erkennung von Gesichtern gearbeitet. Zuerst fanden diese wieder Eingang in den hoheitlichen Überwachungsapparat mittels sogenannter Smart CCTV Systeme, die klassische Videoanlagen digital aufrüsteten und in der Lage sind Menschen anhand ihres Gesichts in der Masse zu erkennen. Diese Entwicklung fand schließlich über eine „Bequemlichkeitsanwendung" ihren Weg auf die privaten Social Media Seiten, Computer und Smartpho-

nes – Gesichtserkennung, um Freunde einander zuordnen zu können – das wirkt praktisch und wird von manchen bedenkenlos genutzt Mittlerweile dienen biometrische Daten mittels Fingerabdruckscan, Gesichts- und Spracherkennung als Zutrittsschranken zum Smartphone, zum Online-Handel aber auch zum Bankkonto. Daüber hinaus sind eine Vielzahl an biometrischen Daten frei und völlig ungeschützt im Netz verfügbar, insbesondere Gesichtsbilder. Diese sind oftmals bereits ausreichend, um Personen mit Gesichtserkennung zu identifizieren, auch ganz ohne deren Wissen zu nutzen. Diese weite Verbreitung macht das Thema zunehmend relevant, da auch immer mehr biometrische Merkmale in unterschiedlichsten Anwendungen verarbeitet werden. Dies fördert die Intransparenz und macht es den Konsument*innen wesentlich schwieriger bewusste Entscheidungen im Umgang mit diesen Technologien zu treffen.

Abgrenzung

Im Rahmen dieser Studie beschäftigen wir uns vornehmlich mit Anwendungen biometrischer Methoden insofern sie Konsument*innen im Bereich Konsum und Freizeit betreffen. Nicht speziell analysiert werden gewerbliche Aspekte oder auch Fragen des Arbeitnehmer*innenschutzes, wenngleich grundlegende Problematiken hier ähnlich gelagert sein mögen.

Methoden

Die vorliegende Studie beruht vor allem auf umfassenden Recherchen im Internet und bestehender Literatur zum Thema. Literatur- und Dokumentenanalyse bilden so die Basis. Jeder Abschnitt wurde im interdisziplinären Team des ITA aus unterschiedlichen Perspektiven diskutiert, um eine umfassende Sichtweise zu entwickeln.

2 TECHNISCHE GRUNDLAGEN[5]

biometrische Merkmale

Biometrische Verfahren identifizieren Personen durch Erfassung und Analyse bestimmter, für die Person charakteristischer Merkmale. Diese Merkmale werden biometrische Merkmale genannt. Dazu gehören biologische Merkmale wie charakteristische Eigenschaften von Gesicht oder Fingerabdruck ebenso wie verhaltenstypische Merkmale wie Unterschrift oder Gangart.[6] Die Frage, ab wann biometrische Merkmale auch biometrische Daten im rechtlichen Sinne aufgefasst werden können wird in Abschnitt 3 behandelt.

der Körper als Schlüssel – Inhärenz

Biometrische Merkmale unterscheiden sich damit grundlegend von anderen Identifikationsmerkmalen. Sie basieren nicht auf Wissen (z. B. ein Passwort) oder Besitz (z. B. ein physischer Schlüssel), sondern sind direkter Ausdruck der Identität einer Person. Sie sind gewissermaßen eine inhärente Eigenschaft der erfassten Person.

Chancen und Risiken

Im Vergleich mit anderen Identifikationsmerkmalen bieten sie einige Chancen, begründen aber auch eine Reihe zusätzlicher Risiken. So können biometrische Merkmale im Gegensatz zu Wissen oder Besitz nicht vergessen, verloren oder einfach weitergeben werden.[7] Dies kann zu einer erleichterten Bedienbarkeit beitragen. Gleichzeitig ist ein Ändern oder Verbergen dieser Merkmale nicht möglich bzw. nicht praktikabel.[8] Sie sind daher in besonderem Maße missbrauchsgefährdet.

Einerseits kann mithilfe von biometrischen Merkmalen eine Person häufig unbemerkt und ohne ihre Einwilligung identifiziert werden.[9] Andererseits können biometrische Merkmale bei missbräuchlicher Verwendung nicht einfach gesperrt oder für ungültig erklärt werden. Die Umsetzung von

---

[5] Dieses Kapitel stammt aus *Schaber*, Transparenzanforderungen des österreichischem und europäischen Datenschutzrechts an die Verarbeitung biometrischer Daten (2020).

[6] Die Abgrenzung zwischen den verschiedenen Untergruppen ist häufig unscharf, weshalb im Folgenden vorwiegend von biometrischen Merkmalen gesprochen wird. So kann z. B. die Gangart als Ausdruck biologischen Anlagen wie auch angelernter Verhaltensweisen aufgefasst werden.

[7] Zu berücksichtigen ist allerdings, dass sich biometrische Merkmale über die Zeit graduell ändern bzw. abnutzen können.

[8] Siehe z. B. *Jain/Nandakumar/Ross*, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 2016, 80–105.

[9] Vergleiche z. B. das Tagging von Gesichtsbildern auf sozialen Netzwerken wie facebook, welches ursprünglich auch ohne die Einwilligung aller Betroffenen durchgeführt werden konnte. Im Rahmen eines Gerichtsverfahrens zahlte das Unternehmen eine hohe Vergleichssumme für diese Praxis, *Singer/Isaac*, Facebook to Pay $ 550 Million to Settle Facial Recognition Suit, 29.01.2020, https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html, aufgerufen am 18.6.2020.

biometrischen Verfahren sollte daher den besonderen Schutzbedarf der erfassten Daten berücksichtigen.

Registrierung und ...

Biometrische Verfahren werden üblicherweise in zwei Phasen geteilt. In der ersten Phase, der Registrierung, werden die biometrischen Merkmale einer Person erfasst, für einen späteren Vergleich aufbereitet und anschließend gespeichert.

... Authentifizierung

Die Identität wird anschließend in der zweiten Phase, der Authentifizierung, geprüft. Dabei werden die gleichen biometrischen Merkmale wie bei der Registrierung erfasst und mit den bereits gespeicherten Merkmalen verglichen. Stimmen die Merkmale hinreichend überein, wird davon ausgegangen, dass es sich um dieselbe Person handelt.

Verifikation vs Identifikation

Eine wichtige Unterscheidung ist auch, ob der Vergleich mit den biometrischen Merkmalen einer einzelnen, bestimmten Person (Verifikation, 1:1 Vergleich) oder von mehreren Personen (Identifikation, 1:n Vergleich) durchgeführt wird. Bei der Verifikation wird die behauptete Identität einer Person bestätigt oder zurückgewiesen, während bei der Identifikation die beste Übereinstimmung mit den biometrischen Merkmalen vieler Personen ermittelt wird. Systeme zur Identifikation benötigen daher eine deutlich größere Anzahl biometrischer Merkmale, um auch bei einer großen Anzahl von Personen zuverlässig zu bleiben.[10]

Multi-Faktor-Authentifizierung

Im Bereich der Zugangskontrolle werden biometrische Verfahren häufig mit anderen Identifikationsmethoden aus den Bereichen Wissen oder Besitz (z. B. Passwort oder Schlüsselkarte) kombiniert. Solche Verfahren werden Multi-Faktor-Authentifizierung genannt und beruhen auf der Annahme, dass es für einen Angreifer deutliche schwieriger ist, mehrere Überprüfungsverfahren hintereinander erfolgreich zu bestehen. Da diese Methoden jedoch üblicherweise das biometrische Verfahren selbst unverändert lassen, werden sie im Rahmen dieses Kapitels nicht näher behandelt.

Anschließend werden daher die einzelnen Schritte eines biometrischen Verfahrens näher beschrieben.

[10] Siehe z. B. das indische Biometrie System "Aadhaar", in dem neben allen Fingerabdrücken auch Iris-Scans gespeichert sind, um eine zuverlässige Identifizierung auch bei über 1 Milliarde erfasster Personen zu ermöglichen. *Jain/Nandakumar/Ross*, Pattern Recognition Letters 2016, 80–105., S 84.

2.1 DATENERFASSUNG

Am Anfang aller biometrischen Verfahren steht die Datenerfassung. Diese kann, abhängig von den zu erfassenden biometrischen Merkmalen, auf sehr unterschiedliche Art und Weise erfolgen. Allen biometrischen Verfahren ist jedoch gemein, dass sie auf die Erfassung von Sensordaten aus der Umgebung angewiesen sind. Die eingesetzten Sensoren und Umgebungsbedingungen zum Zeitpunkt der Erfassung sind daher wesentliche Kriterien für die zu erwartende Leistung biometrischer Verfahren.

bewusste vs unbewusste Datenerfassung

Gleichzeitig sind diese auch ein wesentlicher Faktor dafür, ob die biometrischen Merkmale einer Person bewusst oder unbewusst erfasst werden. Eine Besonderheit von biometrischen Merkmalen ist, dass diese häufig ohne Wissen oder bewusste Unterstützung der betroffenen Person zur Identifikation verwendet werden können. Die Art des biometrischen Sensors und die Umgebungsbedingungen, innerhalb derer biometrische Merkmale erfasst werden, können daher Hinweise darauf liefern, wie wahrscheinlich den betroffenen Personen die Datenerfassung bewusst ist.

spezielle biometrische Sensoren

Ein erstes Kriterium hierfür ist, ob die verwendeten Sensoren speziell auf die Erfassung von biometrischen Merkmalen ausgerichtet sind oder diese nur als Nebenprodukt ihrer eigentlichen Funktion erfassen. Typische Beispiele für spezifische Sensoren sind Fingerabdruck-Scanner oder Iris-Kameras. Verhaltensmerkmale wie Gangart oder Unterschrift werden hingegen häufig mithilfe von eigentlich für andere Zwecke bestimmten Sensoren wie Beschleunigungssensor, Gyroskop oder Stiftneigungswinkel abgeleitet.[11] Da der Einsatz dieser Sensoren für eine betroffene Person nicht ohne weiteres nachvollziehbar ist, wird die Datenerfassung hier häufig unbewusst erfolgen.

Hybridsysteme

Eine Sonderstellung nehmen Hybridsysteme ein, bei denen der Sensor mit Zusatzfunktionen zur Erfassung biometrischer Merkmale ausgestattet ist, aber das Gesamtsystem vorwiegend für andere Zwecke eingesetzt wird. Ein Beispiel für eine solche Konstellation sind Webcams in Computern oder Smartphones, welche auch im Infrarotbereich Bilder aufnehmen, um hierdurch die Leistung der Gesichtserkennung zu verbessern (z. B. Windows Hello oder Apple FaceID).[12]

---

[11] Siehe z. B. *Buriro et al*, Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication, 2016 IEEE Security and Privacy Workshops (SPW), 05.2016.

[12] Siehe *Microsoft*, Windows Hello-Gesichtsauthentifizierung, 02.05.2017, https://docs.microsoft.com/de-de/windows-hardware/design/device-experiences/windows-hello-face-authentication;
Apple, Informationen zur fortschrittlichen Technologie von Face ID – Apple Support, 02.03.2020, https://support.apple.com/de-at/HT208108, aufgerufen am 18.6.2020.

potenziell biometrische Sensoren

Und schließlich gibt es noch zahlreiche Sensorsysteme, welche neben ihren üblichen Funktionen potenziell für biometrische Zwecke verwendet werden können, ohne dafür mit speziellen Zusatzfunktionen ausgestattet zu sein. Bekannte Beispiele hierfür sind die Aufnahme von Gesichtsbildern einer betroffenen Person durch eine Kamera oder Stimmaufnahmen eines Mikrophons. Aber auch Puls- und EKG-Messungen können unter bestimmten Umständen für biometrische Zwecke verwendet werden.[13] Ob den betroffenen Personen hierbei die Datenerfassung (nicht jedoch auch die Auswertung auf biometrische Merkmale)[14] bewusst ist, wird in vielen Fällen von den Umgebungsbedingungen abhängen.

Bedeutung der räumlichen Nähe zum Sensor

Ein wesentlicher Faktor hierbei ist die räumliche Nähe der betroffenen Person zum Sensor. Bei einer Erfassung durch direkten Kontakt mit dem Sensor, wie dies üblicherweise bei Puls- oder EKG-Messungen der Fall ist, wird der betroffenen Person die Datenerfassung idR. bewusst sein. Bei Datenerfassungen, für die eine gewisse räumliche Nähe ausreichend ist, wie z. B. bei Stimmaufnahmen, ist das Bewusstsein über eine Datenerfassung bereits fraglich. Und bei Aufnahmen von Gesichtsbildern oder Gangart, welche über eine größere Distanz erfolgen können, wird in aller Regel einer betroffenen Person die Datenerfassung ohne weitere Kennzeichnung nicht bewusst sein.

Bedeutung des zeitlichen Zusammenhangs

Auch der zeitliche Zusammenhang kann bei der Frage, ob einer betroffenen Person die Datenerfassung wahrscheinlich bewusst ist, eine wesentliche Rolle spielen. Wird zu einem bestimmten Zeitpunkt durch eine bewusste Handlung der betroffenen Person selbst die Aufnahme ausgelöst, z. B. indem ein Auslöser gedrückt wird, wird dies in aller Regel bewusst stattfinden. Erfolgt die Datenerfassung jedoch kontinuierlich im Hintergrund oder wurde sie von einer anderen Person ohne Kenntnis der betroffenen Person veranlasst, wird häufig eine unbewusste Datenerfassung vorliegen.

Insgesamt lässt sich daher sagen: fehlende bewusste Interaktion, eine große räumliche Distanz zum Sensor und häufige Verwendung des Sensors für andere Funktionen führen potenziell zu verringertem Bewusstsein bei der betroffenen Person über die Datenerfassung. Umso wichtiger ist es, dieses Bewusstsein durch Transparenzmaßnahmen zu steigern und den betroffenen Personen damit einen selbstbestimmten Umgang mit ihren biometrischen Merkmalen zu ermöglichen.[15]

---

[13] *Maron*, Wenn das EKG den Pass und den Fingerabdruck ersetzt, 02.03.2020, https://www.medinside.ch/de/post/forschung-ein-ekg-statt-id-oder-pass, aufgerufen am 18.6.2020.

[14] Ein Bewusstsein über die Datenerfassung führt jedoch nicht zwingend zu einem Bewusstsein über die Datenanalyse, siehe hierzu die Ausführungen im nächsten Abschnitt.

[15] Zu den diesbezüglichen datenschutzrechtlichen Verpflichtungen siehe Abschnitt 3.6.

2.2 DATENANALYSE

Sind die biometrischen Merkmale einmal durch Sensoren erfasst, müssen diese zunächst für die folgende Analyse aufbereitet werden. Hierbei werden die Sensordaten nach bestimmten, für das biometrische Merkmal charakteristische, Eigenschaften durchsucht. Bei biologischen Merkmalen sind dies häufig standardisierte Punkte wie z. B. die Minuzien eines Fingerabdrucks (charakteristische Punkte der Papillarrillen des Fingers),[16] welche auch bei Veränderungen wie Rotation oder Verschiebung des Abdrucks einen Wiedererkennungswert aufweisen. Bei verhaltensbasierten Merkmalen kommt häufig eine zeitabhängige Beobachtung hinzu, deren charakteristische Veränderungen das biometrische Merkmal ausmachen.[17]

Einschränkungen biometrischer Merkmale

Allen biometrischen Merkmalen ist jedoch gemein, dass sie durch die endliche Messgenauigkeit der Sensoren und Änderungen in den Umgebungsbedingungen in ihrer exakten Vergleichbarkeit beschränkt sind. Auch sind biometrische Merkmale nicht notwendigerweise einzigartig.[18] Zusätzlich können sich biometrische Merkmale selbst durch Faktoren wie Alterung (z. B. des Gesichts), Abnutzung (z. B. des Fingerabdrucks) oder Unfall über die Zeit verändern. Sie sind daher ohne weitere Vorkehrungen nicht für einen direkten Vergleich miteinander geeignet.

Matching

In der Praxis wird daher meist bei der Registrierung einer Person im biometrischen System eine biometrische Vorlage (Template) erstellt. Diese Registrierung kann mit Unterstützung der betroffenen Person (z. B. Auflegen verschiedener Bereiche des Fingers auf den Sensor) oder auch ohne deren direkter Mithilfe (z. B. auf Basis von publizierten Aufnahmen) erfolgen. Zur Authentifizierung wird die so erstellte Vorlage mit den Messungen des biometrischen Merkmals verglichen (Matching). Überschreitet die Übereinstimmung einen bestimmten Schwellwert, gilt die Identität der Person als bestimmt.

Abhängig vom gewählten Schwellwert weist daher jedes biometrische System eine gewisse Fehlerrate auf. Diese Rate wird häufig durch zwei Größen charakterisiert: wie häufig Personen fälschlicherweise als übereinstimmend akzeptiert (Falschakzeptanzrate – false positive) und wie häufig sie fälschlicherweise als nicht übereinstimmend zurückgewiesen werden (Falschrückweisungsrate – false negative). Haben mehrere Perso-

---

[16] Zur Standardisierung von Fingerabdruckmerkmalen siehe *ISO*, ISO/IEC 19794-8:2006 (2006), https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/07/40715.html. Aufgerufen am 18.6.2020.

[17] Siehe z. B. *Stylios et al*, A Review of Continuous Authentication Using Behavioral Biometrics, Proceedings of the South East European Design Automation, Computer Engineering, Computer Networks and Social Media Conference on – SEEDA-CECNSM '16, 2016.

[18] Dies ist jedoch von der eindeutigen Identifizierbarkeit im juristischen Sinne zu unterscheiden, siehe hierzu Abschnitt 3.

nen die gleichen biometrischen Merkmale und werden deswegen als übereinstimmend akzeptiert, wird auch dies als fälschliche Übereinstimmung gewertet. Die kleinste erreichbare Falschakzeptanzrate ist daher durch die Einzigartigkeit des erfassten biometrischen Merkmals limitiert.

Falschakzeptanzrate in großen biometrischen Systemen

Soll eine Person anhand eines Vergleichs mit einer Vielzahl von biometrischen Vorlagen identifiziert werden, ist die Falschakzeptanzrate besonders wichtig. Systeme, die auf die Identifizierung einer Person aus sehr großen Personengruppen ausgelegt sind, erfassen daher häufig eine große Anzahl an biometrischen Merkmalen, um die Falschakzeptanzrate zu senken.[19] Soll hingegen die Identität einer vorher bestimmten Person bestätigt werden, ist regelmäßig auch eine geringere Anzahl von biometrischen Merkmalen ausreichend.

Absicherung gegen gezielte Täuschung

Eine niedrige Falschakzeptanzrate bedeutet jedoch nicht, dass das biometrische System gut gegen gezielte Täuschungsversuche geschützt ist. Bei diesem Vorgehen werden häufig zuerst die benötigten Informationen über das biometrische Merkmal erlangt (z. B. auf Oberflächen hinterlassene latente Fingerabdrücke oder öffentlich zugängliche Gesichtsbilder). Anschließend wird auf dieser Basis eine Attrappe erstellt, welche dem System eine Kopie der biometrischen Merkmale präsentiert. Mithilfe dieses Vorgehens konnte in der Vergangenheit bereits eine Reihe von biometrischen Systemen auf der Basis von Fingerabdrücken, Gesichts-, Iris- oder Handvenenscans zu einer fehlerhaften Identifikation gebracht werden.[20]

Falschakzeptanz- und Falschzurückweisungsrate

Jedoch ist eine Kopie der biometrischen Merkmale einer realen Person keine notwendige Voraussetzung für gezielte Angriffe. Auch die Besonderheiten des Abgleichs zwischen biometrischen Vorlagen und gemessenen biometrischen Merkmalen können als Basis für einen Angriff dienen. So wurden bereits Studien zu künstlich erzeugten, statistisch optimierten Fingerabdrücken durchgeführt, welche die praktische Machbarkeit derartiger Angriffe zeigt. Diese Fingerabdrücke würden mit einer Vielzahl von biometrischen Vorlagen realer Fingerabdrücke hinreichend genau übereinstimmen und damit eine Art Generalschlüssel für das biometrische System bilden.[21] Auch die Machbarkeit einer Fusion mehrerer Gesichtsbilder zu einem einzelnen, synthetischen Gesichtsbild wurde bereits gezeigt. Auf dieser Basis sollen mehrere reale Gesichter von einem biometrischen Ge-

---

[19] Siehe z. B. das indische Aadhaar System, in dem alle Fingerabdrücke und die Iris-Scans beider Augen von über 1 Milliarde Personen erfasst sind.

[20] Siehe z. B. *Krempl*, 35C3: Mit Venenbild auf Handattrappe Geld abheben oder beim BND einbrechen, 28.12.2018, https://www.heise.de/newsticker/meldung/35C3-Mit-Venenbild-auf-Handattrappe-Geld-abheben-oder-beim-BND-einbrechen-4259637.html, aufgerufen am 18.6.2020.

[21] Siehe z. B. *Bontrager et al*, DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, arXiv:1705.07386.

sichtserkennungssystem als übereinstimmend mit der biometrischen Gesichtsvorlage beurteilt werden.[22]

Lebenderkennung

Viele Hersteller von Zugangssystemen auf Basis biometrischer Merkmale setzten als Abwehr gegen gezielte Angriffe eine sogenannte Lebenderkennung ein. Hier soll mittels zusätzlicher Messungen von physikalischen und geometrischen Eigenschaften der biometrischen Merkmale verhindert werden, dass das System durch eine Attrappe getäuscht werden kann. Bei Sensoren mit direktem Körperkontakt werden dabei häufig einfach zu erfassende physikalische Eigenschaften wie z. B. der Hautwiderstand erhoben. Bei Messungen auf geringe Entfernungen sind dreidimensionale Merkmale wie Gesichtsform anzutreffen. Durch bewusste Materialwahl oder genaue Nachbildung der biologischen Form durch die Attrappe können jedoch auch viele derartige Lebenderkennungen überwunden werden.[23] Hersteller solcher Systeme müssen also großen Aufwand betreiben, um sicherzustellen, dass die erfassten biometrischen Merkmale von einer natürlichen Person stammen und auch von dieser bewusst dem System präsentiert werden.

Umgekehrt kann es für betroffene Personen sehr schwer einzuschätzen sein, ob erfasste Daten auf biometrische Merkmale hin ausgewertet werden oder nicht. Bei Zugangssystemen, welche die Benutzer*innen explizit zur Erfassung biometrischer Merkmale auffordern, liegt eine spätere Analyse dieser Merkmale aufgrund der Funktionsweise der Systeme nahe. Auf mobilen Plattformen wie Smartphones erhalten Drittanbieter, die biometrische Methoden zur Zugangskontrolle nutzen, üblicherweise nicht die erfassten biometrischen Merkmale, sondern nur das Resultat der Analyse.[24] Allerdings gibt es in Expertenkreisen Zweifel darüber, ob biometrische Daten (wie etwa Gesichtsbilder) auf Smartphones hinreichend vor Weiternutzung durch Dritte geschützt sind. Etwa können auch Drittanbieter Zugriff auf Gesichtsscanner haben, wie am Beispiel iPhone bekannt wurde.[25]

---

22 *Thelen/Horchert*, Biometrie im Reisepass: Peng! Kollektiv schmuggelt Fotomontage in Ausweis – DER SPIEGEL – Netzwelt, 22.09.2018, https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html, aufgerufen am 18.6.2020.

23 *Fingas*, Vietnamese firm trips up iPhone X's Face ID with elaborate mask & makeup, 10.11.2017, https://appleinsider.com/articles/17/11/10/vietnamese-firm-trips-up-iphone-xs-face-id-with-elaborate-mask-makeup, aufgerufen am 18.6.2020.

24 Siehe z. B. *Apple*, LocalAuthentication | Apple Developer Documentation, https://developer.apple.com/documentation/localauthentication, aufgerufen am 18.6.2020.

25 Nellis, S. (2017), App developer access to iPhone X face data spooks some privacy experts. Reuters, Nov2, https://www.reuters.com/article/us-apple-iphone-privacy-analysis/app-developer-access-to-iphone-x-face-data-spooks-some-privacy-experts-idUSKBN1D20DZ? Aufgerufen am 18.6.2020 und
Der Standard (2017), Apple erlaubt Entwicklern doch Zugriff auf Gesichtserkennung. Der Standard Online, 2. Nov, https://www.derstandard.at/story/2000067063427/apple-erlaubt-entwicklern-doch-zugriff-auf-gesichtserkennung, aufgerufen am 18.6.2020.

verborgene Datenanalyse

Findet die Datenerfassung hingegen durch für andere Zwecke vorgesehene Anwendungen statt, ist es für die betroffene Person aus technischer Sicht praktisch unmöglich zu beurteilen, ob die erfassten Daten auf biometrische Merkmale hin ausgewertet werden oder nicht. Für Spaßanwendungen erfasste Daten zur Gesichtsgeometrie könnten beispielsweise von Drittanbietern zur biometrischen Datenanalyse genutzt werden, ohne dass dies den betroffenen Personen bewusst ist.[26] Gleichzeitig erlauben die Systeme in vielen Fällen direkten Zugriff auf die erfassten Daten. Das Risiko einer verborgenen Datenanalyse ist in derartigen Konstellationen deutlich höher.

nachträgliche Datenanalyse

Zusätzlich speichern derartige Anwendungen die erfassten Daten häufig in einer Form, welche auch eine spätere Auswertung auf biometrische Merkmale hin erlaubt. Bei Stimmaufnahmen oder Gesichtsbildern ist z. B. eine Auswertung auch lange Zeit nach der eigentlichen Datenerfassung möglich. Durch den technologischen Vorschritt wurden in der Vergangenheit so bereits große Datenbestände von Gesichtsbildern in sozialen Netzwerken oder online Fotospeicherdiensten nachträglich auf ihre biometrischen Merkmale hin ausgewertet.[27] Auch veröffentlichte Gesichtsbilder wurden bereits im großen Stil auf ihre biometrischen Merkmale hin analysiert.[28]

Umso wichtiger ist daher vollständige Transparenz bei der Auswertung gegenüber betroffenen Personen, um einem Missbrauch ihrer biometrischen Merkmale frühzeitig erkennen zu können.[29] Allerdings ist Transparenz alleine keine ausreichende Schutzmaßnahme vor Missbrauch oder problematischer Verwendung in Hinblick auf Wahrung der Grundrechte.

---

[26] *Nellis*, App developer access to iPhone X face data spooks some privacy experts, 02.11.2017, https://www.reuters.com/article/us-apple-iphone-privacy-analysis-idUSKBN1D20DZ, aufgerufen am 25.08.2020.

[27] Siehe z. B. *Davis*, Google Fights Privacy Suit Over Facial-Recognition Technology, 17.06.2020, https://www.mediapost.com/publications/article/352651/google-fights-privacy-suit-over-facial-recognition.html, aufgerufen am 18.6.2020.

[28] *Hill*, The Secretive Company That Might End Privacy as We Know It, The New York Times, 18.01.2020.

[29] Für eine rechtliche Analyse dieser Problematik siehe Abschnitt 3.2.

2.3 DATENSPEICHERUNG

Nach der erstmaligen Registrierung müssen die erfassten biometrischen Merkmale für eine spätere Wiedererkennung gespeichert werden. Dabei sollten die erfassten Merkmale gut gegen missbräuchliche Zugriffe geschützt sein. Schließlich können sie von der betroffenen Person üblicherweise nicht geändert oder für ungültig erklärt werden und erlauben häufig eine Identifizierung auch gegen ihren Willen. Sie sind daher in besonderer Weise für missbräuchliche Verwendung anfällig.

Speicherform

Ein erstes Kriterium für das Missbrauchspotential ist die Form, in welcher die erfassten biometrischen Merkmale gespeichert werden. Hier gibt es im Wesentlichen zwei Möglichkeiten. Entweder werden die erfassten Rohdaten gespeichert, aus denen bei Bedarf die biometrischen Merkmale extrahiert werden können. Oder die extrahierten Merkmale werden in Form einer biometrischen Vorlage (Template) festgehalten, um sie später mit den analysierten Daten vergleichen zu können. Templates werden üblicherweise bei biometrischen Zugangssystemen verwendet und sollen u. a. eine missbräuchliche Datenverwendung erschweren. Allerdings war das in der Vergangenheit nicht immer der Fall, wodurch biometrische Rohdaten von Fingerabdrücken bestimmter mobiler Geräte leicht zugänglich waren.[30]

Bei gespeicherten Rohdaten, wie z. B. häufig bei für andere Zwecke erstellte Gesichts- oder Tonaufnahmen, ist eine spätere Zweckänderung besonders einfach. Aber auch Templates bieten keinen absoluten Schutz vor Datenmissbrauch. So wurden in der Literatur bereits die Möglichkeit diskutiert, auf Basis von Templates die biologischen Merkmale wiederherzustellen[31] und als mögliche Gegenmaßnahme im Nachhinein durch betroffene Personen widerrufbare Templates vorgeschlagen.[32]

Speicherort

Auch der Speicherort kann wesentlich zur Datensicherheit beitragen. Werden die biometrischen Merkmale ausschließlich auf dem lokalen Endgerät gespeichert, ist ein späterer Datenmissbrauch durch Übernahme einer einzelnen, zentralen Instanz unwahrscheinlicher.[33] Gleichzeitig gibt es auf mobilen Endgeräten häufig speziell abgesicherte Bereiche mit besonderen

---

30 *Gibbs*, HTC stored user fingerprints as image file in unencrypted folder, 10.08.2015, https://www.theguardian.com/technology/2015/aug/10/htc-fingerprints-world-readable-unencrypted-folder, aufgerufen am 18.6.2020.

31 *Ross*/*Shah*/*Jain.*, From Template to Image: Reconstructing Fingerprints from Minutiae Points, IEEE transactions on pattern analysis and machine intelligence 2007, 544–560.

32 *Patel*/*Ratha*/*Chellappa*, Cancelable Biometrics: A review, IEEE Signal Processing Magazine 2015, 54–65.

33 Wenn die zentrale Instanz das Endgerät z. B. durch ein Programmupdate dazu veranlassen kann, die biometrischen Daten weiterzugeben, ist die Datensicherheit jedoch weiterhin von der zentralen Instanz abhängig.

Zugriffseinschränkungen.[34] Die Nutzung dieser Bereiche kann die Datensicherheit weiter erhöhen. Jedoch ist auch dieser Schutz nicht lückenlos. Bei manchen Endgeräten konnte die zusätzliche Absicherung unter bestimmten Umständen überwunden werden.[35] Die lokale Speicherung ist aus Perspektive der Datensicherheit jedoch weiterhin die beste Alternative. Bei vernetzten Applikationen wie speziell auf Smartphones üblich, ist allerdings zu bedenken, dass diverse Apps, die idR. mit Cloudanwendungen verknüpft sind, potenziell vielfältige Zugriffsmöglichkeiten auf Daten haben können. Hoher Vernetzungsgrad und externe Zugriffsmöglichkeiten können sich daher negativ auf das Schutzniveau auch bei lokaler Speicherung auswirken.

zentralisierte Systeme

Insbesondere bei biometrischen Systemen zur Identifizierung einer Vielzahl von Menschen werden aus technischen Gründen die biometrischen Merkmale häufig zentral gespeichert. Bei diesen Systemen muss daher neben der Datenspeicherung auch die Datenweitergabe besonders gut abgesichert werden.

2.4 DATENWEITERGABE

Biometrische Merkmale sind aufgrund ihrer identifizierenden Eigenschaften besonders von Missbrauch gefährdete Daten. Jede Übermittlung bzw. Weitergabe erhöht das Risiko einer missbräuchlichen Verwendung und sollte soweit wie möglich vermieden werden. Das gilt sowohl bei der Kommunikation über Netzwerke als auch innerhalb des Endgerätes selbst.

externe Datenweitergabe

Müssen biometrische Merkmale oder auf ihnen basierende Templates von einem Endgerät zu einer externen Datenbank übermittelt werden, findet diese Kommunikation üblicherweise verschlüsselt statt. Wichtig hierbei ist die Verwendung einer passenden Transportverschlüsselung. Dabei sollten für jedes Endgerät unterschiedliche Schlüssel zum Einsatz kommen. Ein Angreifer könnte sonst durch die vollständige Übernahme eines einzigen Endgeräts Zugriff auf die Kommunikation mit allen anderen Endgeräten kommen bzw. sich gegenüber der externen Datenbank als ein beliebiges Endgerät ausgeben.

interne Datenweitergabe

Auch die Datenweitergabe innerhalb des Endgeräts sollte auf das nötigste reduziert und entsprechend abgesichert sein. Der externe Sensor sollte mit dem Prozessor zur Datenanalyse ausschließlich verschlüsselt kommunizieren. Leider wird die Kommunikation meist nur bei Sensoren mit speziellen biometrischen Aufgaben verschlüsselt, bei für andere Zwecke vorge-

---

[34] Beispiele hierfür sind die iOS secure enclave, oder ARM Trust Zone.

[35] *Grüner*, ARM Trustzone: Google bescheinigt Android Vertrauensprobleme, 25.07.2017, https://www.golem.de/news/arm-trustzone-google-bescheinigt-android-vertrauensprobleme-1707-129113.html, aufgerufen am 18.6.2020.

sehenen bildgebenden oder akustischen Sensoren ist dies üblicherweise nicht der Fall. Von diesen Sensoren erfasste biometrische Merkmale können daher deutlich leichter abgefangen und manipuliert werden. Zusätzlich haben Programme von Drittanbietern in vielen Fällen Zugang zu den Rohdaten der Sensoren.

schwer nachvollziehbare Weitergabe

Bei von diesen Sensoren erfassten biometrischen Merkmalen, welche z. B. innerhalb von Bild oder Tondaten eingebettet sein können, lässt sich eine Weitergabe der Daten von betroffenen Personen nur schwer technisch nachvollziehen. Dies gilt insbesondere für Systeme, welche sich im Bereitschaftsmodus befinden und durch bestimmte Ereignisse aufwachen, wie z. B. digitale Sprachassistenten[36] oder bei Bewegung aktivierte Kameras. Zwar versuchen diese Systeme häufig durch ein optisches oder akustisches Signal auf die Datenweitergabe aufmerksam zu machen, die Verlässlichkeit dieses Indikators hängt jedoch von der konkreten Programmierung des Systems ab.

unbewusste Weitergabe

Andere biometrische Merkmale wie z. B. Fingerabdrücke oder DNA-Spuren werden ständig unbeabsichtigt hinterlassen bzw. weitergegeben. Aber auch durch unbedachte Veröffentlichung von Bild- oder Tonaufnahmen kann es zu einer unbewussten Weitergabe von biometrischen Merkmalen kommen. So konnten auf Basis von hochauflösenden Pressefotos Nachbildungen wichtiger Iris- oder Fingerabdruckmerkmale deutscher Politiker erstellt werden.[37]

---

[36] Siehe hierzu ausführlich *Schaber/Krieger-Lamina/Peissl*, Digitale Assistenten – Endbericht, 2019.

[37] Siehe z. B. *Krempl*, 31C3: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck, 28.12.2014, https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html, aufgerufen am 18.6.2020.

3 RECHTLICHE GRUNDLAGEN[38]

Der Schutz personenbezogener Daten ist sowohl im europäischen als auch im nationalen Verfassungsrecht fest verankert. So sieht bereits die Charta der Grundrechte der Europäischen Union ein solches Recht vor.[39] Die Daten dürfen grundsätzlich nur für festgelegte Zweck nach Treu und Glauben verarbeitet werden. Auch im nationalen Recht befindet sich das Grundrecht auf Datenschutz im Verfassungsrang.[40] Die europäische Datenschutzgrundverordnung (DSGVO) sieht innerhalb ihres sachlichen Anwendungsbereichs[41] eine Reihe weiterer Grundsätze vor. Zusätzlich zur Verarbeitung nach Treu und Glauben für festgelegte Zwecke muss die Verarbeitung rechtmäßig und gemäß dem Grundsatz der Transparenz nachvollziehbar sein.[42] Weiters dürfen nur die für den Zweck notwendigen Daten erhoben werden (Grundsatz der Datenminimierung) und falsche Daten müssen „unverzüglich gelöscht oder berichtigt werden" (Grundsatz der Richtigkeit).[43] Die Speicherdauer muss auf das für den Zweck erforderliche Maß beschränkt (Grundsatz der Speicherbegrenzung) und die Informationssicherheit der Daten gewährleistet sein (Grundsatz der Integrität und Vertraulichkeit).[44] Diese Grundsätze bilden die Basis für viele weitere Bestimmungen der DSGVO und sind vom Verantwortlichen nachzuweisen.[45] All diese Grundsätze kommen auch bei der Verarbeitung biometrischer Daten zur Anwendung.

In Deutschland hat das Bundesverfassungsgericht durch seine Spruchpraxis das Recht auf informationelle Selbstbestimmung geprägt. Demnach gibt es kein „belangloses Datum" mehr, vielmehr können durch die automatisierte Datenverarbeitung laufend neue Verwendungsmöglichkeiten erschlossen werden.[46] Von dieser Problematik sind auch biometrische Merkmale betroffen, die in einer immer größeren Anzahl an Fällen ausgewertet werden können.

---

[38] Dieses Kapitel basiert auf einer gekürzten Fassung von *Schaber*, Transparenzanforderungen des österreichischem und europäischen Datenschutzrechts an die Verarbeitung biometrischer Daten (2020).

[39] Art 8 GRC.

[40] § 1 DSG.

[41] Vom sachlichen Anwendungsbereich ausgenommen sind z. B. ausschließlich persönliche und familiäre Tätigkeiten oder die Tätigkeit von Behörden im Rahmen der Strafverfolgung, Siehe Art 2 Abs 2 lit c und d DSGVO.

[42] Art 5 Abs 1 lit a und b DSGVO.

[43] Ebenda lit c und d DSGVO.

[44] Ebenda lit e und f DSGVO.

[45] Art 5 Abs 2 DSGVO.

[46] BVerfGE 1 BvR 209/83 (15.12.1983), Rz 158.

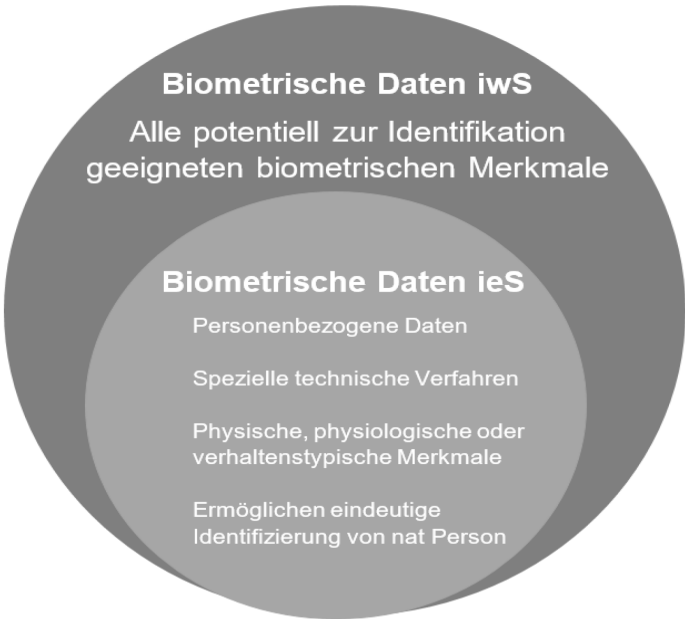

Abbildung 1: Vergleich von allen potentiell für biometrische Anwendungen geeigneten Merkmalen (biometrische Daten iwS) und solche, die zusätzlich die Kriterien nach der DSGVO erfüllen (biometrische Daten ieS); (eigene Darstellung).

Der nächste Abschnitt widmet sich daher dem Begriff der biometrischen Daten und grenzt ihn von anderen personenbezogenen Daten ab. Anschließend werden die Verpflichtungen des Verantwortlichen mit Fokus auf die Rechte der betroffenen Person näher beleuchtet.

3.1 BEGRIFF DER BIOMETRISCHEN DATEN

Biometrie im technischen Bereich

Der Begriff der Biometrie ist vor allem aus dem technischen Bereich bekannt. Hierunter wird die automatisierte Erkennung von Individuen auf Basis von biologischen Merkmalen oder Verhaltensmerkmalen verstanden.[47] Häufig verwendete biologische Merkmale sind beispielsweise Eigenheiten des menschlichen Fingerabdrucks, des Gesichts, der Stimme, der Iris oder der Handvenenstruktur verwendet werden.[48] Manche Messgeräte sind ausschließlich auf Biometrie ausgelegt (z. B. Handvenen-Scanner), während bei anderen Messgeräten Biometrie typischerweise nur eine Nebenfunktion darstellt (z. B. Stimmerkennung auf Basis von Tonaufnahmen).

---

47 *ISO/IEC*, 2382-37:2017(en) Information technology — Vocabulary — Part 37: Biometrics, Rz 3.1.3.

48 Vgl *Hödl* in *Knyrim* (Hrsg), Der DatKomm – Praxiskommentar zum Datenschutzrecht (2018), Art 4 Rz 149.

biometrische Daten iwS

Neben den biologischen Merkmalen können auch Verhaltensmerkmale zur Identifikation verwendet werden. Der Bogen an verwendeten Merkmalen reicht von traditionellen verwendeten Merkmalen wie Schriftbild und Unterschrift bis hin zu Merkmalen wie dem charakteristischen Tippverhalten auf Tastaturen,[49] die erst durch die zunehmende Verbreitung von Computer an Bedeutung gewonnen haben. All diesen Merkmalen ist gemein, dass sie potentiell zur Identifikation von Personen verwendet werden können, aber nicht notwendigerweise auch dafür eingesetzt werden. Im Rahmen dieser Arbeit werden solche, potentiell zur biometrischen Identifikation geeigneten Merkmale, als biometrische Daten im weiteren Sinne bezeichnet, um sie vom nicht zwingendermaßen identen Begriff der biometrischen Daten im Sinne des Datenschutzrechts abzugrenzen (siehe Abbildung 1).

biometrische Daten ieS

Die Europäische Datenschutzgrundverordnung[50] (DSGVO), welche grundsätzliche Bestimmungen für die Verarbeitung von personenbezogenen Daten umfasst,[51] enthält auch eine Legaldefinition des Begriffs der biometrischen Daten. Demnach sind biometrische Daten

> „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen".[52]

Diese Daten werden im Folgenden in Abgrenzung vom technischen Begriff der Biometrie als biometrische Daten im engeren Sinne bezeichnet.

---

[49] *Artikel 29-Datenschutzgruppe*, WP 80, Arbeitspapier über Biometrie (1.8.2003), 4.

[50] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119 (4.5.2016), 1–88.

[51] In wichtigen Bereichen des europäischen Datenschutzrechts gibt es speziellere Bestimmungen, die der DSGVO vorgehen (z. B. die RL 2002/58/EG im Bereich elektronischer Kommunikation).

[52] Art 4 Z 14 DSGVO.

3.2 PERSONENBEZUG

Der Begriff der personenbezogenen Daten ist von fundamentaler Bedeutung für das Datenschutzrecht.[53] Sind Daten nicht personenbezogen, so fallen sie aus dem sachlichen Anwendungsbereich zentraler datenschutzrechtlicher Normen hinaus.[54,55] Die DSGVO definiert personenbezogene Daten als

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen [...] „[56]

Aufgrund seiner herausragenden Stellung des Begriffs im Datenschutzrechts gibt es eine fortwährende Diskussion darüber, ab wann Daten personenbezogen sind.[57]

Identifizierbarkeit mittels Kennung

In der Praxis ist hierfür meist die Identifizierbarkeit das entscheidende Kriterium.[58] Dabei ist es auch ausreichend, wenn die Daten unter einer beliebigen Kennung mit Personenbezug zusammengefasst werden können.[59] Die Legaldefinition von personenbezogenen Daten schließt explizit „Merkmale[n], die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind" in der Definition mittelbarer Identifizierbarkeit mit ein.[60]

Wahrscheinlichkeit der Identifikation

Oft ist auf Basis biometrischer Daten iwS jedoch keine Identifizierung mit hundertprozentiger Sicherheit möglich. Aus technischen Gründen gibt es eine gewisse Wahrscheinlichkeit, dass eine Person fälschicherweise erkannt oder nicht erkannt wird.[61] In der Literatur herrscht jedoch weitgehende Einigkeit darüber, dass eine wahrscheinliche Identifizierung ausreichend ist.[62] Auch die Spruchpraxis von OGH und EuGH deuten in diese Richtung.[63]

---

53 *Artikel-29-Datenschutzgruppe*, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (20.6.2007), 3ff.

54 Vgl Art 2 Abs 1 DSGVO und § 1 DSG

55 *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG Datenschutzgesetz – Kommentar (2018), § 1 Rz 4ff.

56 Art 4 Z 1 DSGVO.

57 Vgl *Artikel-29-Datenschutzgruppe*, WP 136, 3.

58 Vgl *Feiler/Forgó*, DSGVO, 4.

59 Vgl *Feiler/Forgó*, DSGVO Art 4 Rz 4.

60 Art 4 Z 1 DSGVO.

61 Für eine ausführlichere Behandlung dieser Thematik siehe Kapitel 2.2.

62 Vgl *Feiler/Forgó*, DSGVO Art 4 Rz 3; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9.

63 Vgl OGH 20.12.2006, 9 ObA 109/06d, EuGH 19.10.2016, C-582/14 (Breyer) Rz 44ff, DSB.

Bedeutung des technischen Fortschritts

Insbesondere für potentiell biometrisch auswertbare Daten wie Sprachaufnahmen oder Gesichtsbilder könnte der technische Fortschritt zu einer leichten Identifizierbarkeit für den technisch durchschnittlich ausgestatteten Verantwortlichen führen. So wird beispielsweise die automatisierte Gruppierung von Gesichtsaufnahmen häufig in sozialen Netzwerken[64] oder in Online-Diensten zur Speicherung von Bildern[65] angeboten. Auch eine Suche nach ähnlichen Bildern in öffentlich verfügbaren Bildquellen[66] kann zu einer leichten Identifizierung beitragen.

Identifizierbarkeit als Momentaufnahme

Bei der Beurteilung der Identifizierbarkeit ist jedoch auf den Stand der Technik und die verfügbaren Datenquellen zum Zeitpunkt der Verarbeitung abzustellen. Ein neuer Stand der Technik oder der Zugang zu neuen Datenquellen kann daher dazu führen, dass vormals nicht personenbezogene Daten durch ihre Identifizierbarkeit personenbezogen werden. Insbesondere biometrischen Daten iwS wie Puls oder EKG Aufzeichnungen können durch verbesserte Auswertungsmöglichkeit schnell zu personenbezogenen Daten werden, ohne das hierzu eine Verknüpfung mit anderen Kennungen notwendig wäre.

3.3 BIOMETRISCHE DATEN ALS BESONDERE KATEGORIE

sensible Daten

Bestimmte Kategorien von personenbezogenen Daten bergen ein erhöhtes Risiko, bei ihrer Verarbeitungen die Rechte und Grundfreiheiten der betroffenen Personen zu beeinträchtigen.[67] Im Rahmen der DSGVO werden solche Informationen einer besonderen Kategorie von personenbezogenen Daten zugeordnet („sensible Daten").[68] Aufgrund ihres erhöhten Risikos unterliegt die Verarbeitung von derartigen „sensiblen Daten" besonderen Beschränkungen. So ist deren Verarbeitung nur auf Basis von anderen und i. A. restriktiveren Rechtsgrundlagen als bei „normalen" personenbezogenen Daten erlaubt.[69] Gleichzeitig geht die Verarbeitung von „sensiblen Daten" mit erweiterten Verpflichtungen für den Verantwortlichen z. B. bei

---

[64] Siehe z. B. https://de-de.facebook.com/help/122175507864081, aufgerufen am 15.04.2020.

[65] Siehe z. B. https://support.google.com/photos/answer/6128838?co=GENIE.Platform%3DAndroid&hl=de, aufgerufen am 15.04.2020.

[66] Siehe z. B. https://support.google.com/websearch/answer/1325808?co=GENIE.Platform%3DDesktop&hl=de, aufgerufen am 15.04.2020.

[67] Vgl ErwGr 51 DSGVO und *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 9 DSGVO Rz 3f.

[68] Vgl ErwGr 10 DSGVO, wo die Bezeichnung „sensible Daten" für besondere Kategorien von personenbezogenen Daten verwendet wird.

[69] Vgl Art 9 Abs 2 und Art 6 Abs 1 und 4 DSGVO.

Verlust von Daten einher (Benachrichtigung der betroffenen Person bei einer Verletzung des Schutzes personenbezogener Daten).[70]

Legaldefinition

Für einen Verantwortlichen ist es daher wesentlich, zwischen den verschiedenen Datenkategorien klar zu unterscheiden. Die DSGVO enthält zwar keine Legaldefinition der besonderen Kategorien von personenbezogenen Daten, deren Umfang geht jedoch klar aus Art 9 DSGVO hervor. Demnach gehören zu den besonderen Kategorien

> „[…] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
>
> sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung […]"[71] [Absatz hinzugefügt]

Daraus ist ersichtlich, dass biometrische Daten ieS jedenfalls zu den besonderen Kategorien personenbezogener Daten gezählt werden können. Daran vermag auch die Einschränkung, dass die Daten zur eindeutigen Identifizierung einer natürlichen Person geeignet sein müssen, nichts zu ändern, da diese Bedingung bereits in der Legaldefinition von biometrischen Daten ieS dies fordert.[72]

mittelbar bestimmbare sensible Daten

Gemäß dem Wortlaut der Definition zerfallen besondere Kategorien personenbezogener Daten wiederrum in zwei Unterkategorien. Innerhalb der ersten Unterkategorie müssen die „sensible Daten" nur aus den erfassten Daten hervorgehen. Diese Formulierung wird gemäß hA dahingehend ausgelegt, dass auch eine bloß mittelbare Bestimmbarkeit dieser Merkmale ausreicht.[73] Eine konkrete Verarbeitung mit dem Ziel, diese Merkmale zu bestimmen, ist demnach nicht erforderlich, um diese als „sensible Daten" zu klassifizieren.[74]

Zu beachten ist dabei, dass auch ohne Identifizierung der betroffenen Person u. U. geschützte Merkmale aus der Verarbeitung hervorgehen können (z. B. ethnische Herkunft bei Lichtbildern). Wird eine Auswertung zu diesen Zwecken vorgenommen (z. B. im Rahmen einer statistischen Einordnung von Kundenströmen in einem Geschäftslokal) werden derartige Informationen wohl jedenfalls als „sensible Daten" einzustufen sein.

biometrische Daten ieS

Bei der zweiten Unterkategorie von „sensiblen Daten", zu denen auch biometrische Daten ieS zählen, wird hingegen explizit auf die Verarbeitung

---

[70] Vgl Art 34 Abs 1 DSGVO iVm *König/Schaupp* in *Knyrim*, DatKomm Art 33 Rz 29, wonach bei einem Verstoß gegen die Schutzpflichten iZm besonderen Kategorien von personenbezogenen Daten ein hohes Risiko sehr wahrscheinlich ist.

[71] Art 9 Abs 1 DSGVO.

[72] Vgl Art 4 Z 14 DSGVO, in der dies als Ermöglichung bzw. Bestätigung der eindeutigen Identifikation einer natürlichen Person bezeichnet wird.

[73] *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 9 Rz 19.

[74] Ebenda Rz 18.

von bestimmten Datenkategorien abgestellt. Bei biometrischen Daten ieS ist dies auch bereits in ihrer Legaldefinition angelegt, die auf eine Gewinnung der Daten mittels „spezieller technischer Verfahren" abstellt.[75] Solche Verfahren können u. A. die Erkennung von physiologischen Merkmalen, wie z. B. bei Finger- oder Irisscan, beinhalten. Eine Begrenzung auf bestimmte technische Verfahren findet jedoch nicht statt, somit können auch analoge Verfahren wie die Abnahme von Fingerabdrücken mittels Druckerschwärze unter diesen Begriff fallen.[76] Durch diese Formulierung ist eine Einbeziehung neu entwickelter technischer Identifikationsverfahren für die Beurteilung von biometrischen Daten möglich.

Die daraus resultierenden Anforderungen an den Verarbeitungszweck werden im folgenden Abschnitt dargestellt.

3.4 BEDEUTUNG DES VERARBEITUNGSZWECKS

Bei der Beurteilung, ob die Verarbeitung biometrischer Daten iwS zum Vorliegen von „sensiblen Daten" führt, wird gemäß h. A. auf den Verarbeitungszweck abgestellt.[77] Abgeleitet wird dies insbesondere für Lichtbilder aus ErwGr 51, wonach diese nur als „sensible Daten" angesehen werden sollten, wenn diese mithilfe spezieller technischer Verfahren zur Identifizierung oder Authentifizierung einer natürlichen Person verarbeitet werden.[78]

Bei einer solchen Verarbeitung sind diese jedoch jedenfalls als „sensible" Daten mit den entsprechenden Rechtsfolgen anzusehen, unabhängig davon, ob die betroffene Person dem Verantwortlichen bekannt ist oder nicht. So kann beispielsweise die automatisierte Auswertung von Gesichtsbildern im öffentlichen Raum ohne tragfähige Rechtsgrundlage aller (potentiell) betroffenen Personen unzulässig sein.[79] Insbesondere wird der Verantwortliche sich hier nur schwer auf die Rechtsgrundlage der ausdrücklichen Einwilligung stützen können, da ihm häufig nicht alle betroffenen Personen bekannt sein werden.[80]

---

75 Art 4 Z 14 DSGVO.

76 *Hödl* in *Knyrim*, DatKomm Art 4 Rz 148.

77 Vgl *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 9 Rz 27; *Feiler/Forgó*, Art 9 Rz 3.

78 ErwGr 51 S 3 DSGVO.

79 *EDPB*, Guidelines 3/2019 on processing of personal data through video devices (29.1.2020), Rz 84.

80 Dies gilt im Rahmen des sachlichen Anwendungsbereichs der DSGVO. Bildverarbeitung ausschließlich für persönliche oder familiäre Tätigkeiten fallen jedoch aus diesem heraus, siehe hierzu § 12f DSG für den Privatbereich.

Sind Lichtbilder sensible Daten?

Ob Lichtbilder von Personen auch unabhängig davon aufgrund der möglichen Verarbeitung z. B. von Informationen zu Ethnie (über die Hautfarbe) oder Gesundheitszustand (das Tragen einer Brille oder die Verwendung von Gehhilfen) dennoch als „sensible Informationen" einzustufen sind, ist in der Literatur umstritten.

Abstellen auf den konkreten Verarbeitungszweck

Dabei lassen sich im Wesentlichen zwei Grundpositionen unterscheiden. Für ein Abstellen auf den Verarbeitungszweck spricht demnach die starke Abhängigkeit von Umfang und Kontext des verwendeten Datensatzes. So könne beispielsweise aus Körpergewicht und Größe alleine keine Gesundheitsinformationen abgeleitet werden, eine Kombination beider Werte ermögliche jedoch die Berechnung des BMI[81], woraus Aussagen über den Gesundheitszustand getroffen werden könnten.[82]

Die gleichen Daten könnten je nach Verarbeitungszweck unterschiedlich starke Auswirkungen auf die Privatsphäre der Betroffenen haben und sollten daher unterschiedlich beurteilt werden.[83] Für ein Abstellen auf den Verarbeitungszweck spricht demnach auch die Stellungnahme des Europäischen Datenschutzausschusses, wonach Lichtbilder nur dann biometrische Daten ieS darstellen sollten, wenn sensible Daten extrahiert oder zur Identifizierung verwendet werden.[84] Und schließlich wäre eine solche Auslegung auch aus Gründen der Praktikabilität geboten, da sonst bei vielen alltäglichen Datenanwendungen wie z. B. Gruppenfotos im Geschäftskontext von jedem einzelnen Betroffenen eine ausdrückliche Einwilligung eingeholt werden müsste.[85]

Abstellen auf objektive Umstände der Verarbeitung

Die zweite Grundposition besagt hingegen, dass es auf die objektiven Umstände der Verarbeitung und damit nicht auf den subjektiven Verarbeitungszweck des Verantwortlichen ankomme.[86] Interessanterweise wird hier ebenfalls mit der Praktikabilität argumentiert, diesmal allerdings aus der Perspektive der betroffenen Person. Demnach würde ein Abstellen auf den subjektiven Verarbeitungszweck des Verantwortlichen den Persönlichkeitsschutz der betroffenen Person unterlaufen. Denn aufgrund der ursprünglichen Verarbeitungssituation könnten Daten als nicht „sensible" Informationen eingestuft werden, unabhängig davon, ob der Verarbeitungszweck sich später ändere.[87] Als Beispiel werden Bilder von Beschäftigten genannt, die auf der Unternehmenshomepage veröffentlicht und später

---

81 Body Mass Index als Verhältnis zwischen Gewicht[kg] und Größe[m]^2.

82 *Knyrim*, Bilddaten: immer sensibel?, JusIT, 102 (2016), 237.

83 Ebenda.

84 *EDPB*, Guidelines 3/2019, Rz 62f.

85 *Knyrim*, Bilddaten: immer sensibel?, 238.

86 Vgl *Bergauer*, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf Knyrim, S 242 Bilddaten: immer sensibel?, jusIT, 103 (2016), 241ff.

87 Ebenda.

von einem Dritten auf „sensible Daten“ wie z. B. die Ethnie der Beschäftigten ausgewertet werde könnten.[88]

Diese Einschätzung werde auch durch die Entscheidung des EuGH gestützt, wonach auch die Information über einen partiellen Krankenstand als Daten über die Gesundheit einer betroffenen Person anzusehen sein, auch wenn diese Information offensichtlich für einen völlig anderen Verarbeitungszweck veröffentlicht wurden.[89]

missbräuchliche Verarbeitung

Die Gefahr der missbräuchlichen Verwendung von Gesichtsbildern ist überaus real. In der Praxis sind bereits Fälle von möglichen Datenschutzverstößen durch die massenhafte Auswertung von Gesichtsbildern, auch zur Bestimmung biometrische Merkmale, bekannt geworden.[90] Bei anderen biometrischen Daten iwS wie z. B. Sprachaufnahmen sind ähnliche Entwicklungen zu erwarten.

Verwaltungspraxis

Aus der Spruchpraxis der DSB ergibt sich klar, dass die Behörde bei Lichtbildern auf den Verarbeitungszweck abstellt und somit grundsätzlich nicht vom Vorliegen „sensibler“ Daten ohne dezidierte Auswertung hierzu ausgeht.[91] In der Literatur wird jedoch kritisiert, dass diese rechtliche Feststellung regelmäßig ohne nähere Begründung erfolge.[92] Es wird daher wohl einer oberstgerichtlichen Entscheidung bedürfen, um diese Frage für biometrische Daten iwS letztgültig zu beantworten.

3.5 RECHTSGRUNDLAGE DER DATENVERARBEITUNG

Um personenbezogene Daten verarbeiten zu dürfen, muss der Verantwortliche sich auf eine entsprechende Rechtsgrundlage stützen können. Diese finden sich in Art 6 DSGVO und sind für eine rechtmäßige Datenverarbeitung zwingend erforderlich.[93] Bei sensiblen Daten (welche jedenfalls auch biometrische Daten ieS umfassen) kommen hingegen die Rechtsgrundlagen des Art 9 DSGVO zur Anwendung, welche die Verarbeitung grundsätzlich verbietet und nur für bestimmte Fälle Ausnahmen vom Verarbeitungsverbot vorsieht.

---

88 Ebenda 245.

89 Ebenda 245; Vgl auch EuGH 6.11.2003, C-101/01 (Lindqvist) Rz 50f, sowie die Ausführungen zum mittelbaren Hervorgehen von „sensiblen Daten“ in Kapitel 3.3.

90 Vgl z. B. https://www.datenschutz-notizen.de/hmbbfdi-prueft-clearview-datenschutzverstoesse-en-masse-5925301/, aufgerufen am 20.04.2020.

91 Vgl DSB-D202.207/0001-DSB/2018.

92 Vgl *Jahnel*, DSB: Bilddaten als nicht-sensible Daten, jusIT, 32 (2019), 89ff.

93 Art 5 Abs 1 lit a iVm Art 6 ABs 1 DSGVO.

Im Vergleich zu Art 6 gibt es hier einige Unterschiede. So entfallen die überwiegend berechtigten Interessen des Verantwortlichen als Rechtsgrundlage und für die Rechtsgrundlage der Einwilligung ist nun eine ausdrückliche bestätigende Handlung der betroffenen Person erforderlich.[94] Gerade bei Verantwortlichen des Privatrechts, welche sich häufig auf Einwilligung oder überwiegend berechtigte Interessen als Rechtsgrundlage stützen, stellt dies eine wesentliche Änderung dar. Bei biometrischen Daten ieS werden betroffene Personen hier also häufig um eine ausdrückliche Einwilligung ersucht werden.

Es gibt jedoch auch Ausnahmen vom Verarbeitungsverbot des Art 9, welche sich in Art 6 DSGVO nicht finden. Für biometrische Daten besonders relevant ist hier die Ausnahme vom Verarbeitungsverbot für Daten, die von der betroffenen Person selbst öffentlich gemacht wurden.[95] Häufig betrifft dies öffentlich zugängliche Gesichtsbilder oder Stimmaufnahme der betroffenen Person.

Es stellt sich also die Frage, in welchem Verhältnis die beiden Artikel bei der Verarbeitung von sensiblen Daten stehen. Die Art-29-Datenschutzgruppe vertritt hierzu die Ansicht, dass bei der Verarbeitung von sensiblen Daten die Bedingungen des Art 6 und Art 9 DSGVO gemeinsam erfüllt werden müssen.[96] Nach dieser Ansicht muss sich der Verantwortliche auf Rechtsgrundlagen beider Artikel stützen. Wurden die biometrischen Daten von der betroffenen Person selbst öffentlich gemacht, ist somit weiterhin eine Rechtsgrundlage des Art 6 erforderlich.

3.6 VERPFLICHTUNGEN DES VERANTWORTLICHEN GEGENÜBER DER BETROFFENEN PERSON

Der datenschutzrechtliche Verantwortliche ist im Anwendungsbereich der DSGVO verpflichtet, der betroffenen Person eine Reihe von Rechten einzuräumen. Der Großteil dieser Rechte muss von der betroffenen Person selbst eingefordert werden. Eine Ausnahme bilden die Informationspflichten sowie die Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten, welche der Verantwortliche der betroffenen Person auch ohne explizites zur Verfügung stellen muss.

---

94 Vgl Art 6 Aba 1 lit a und f mit Art 9 Abs 2 lit a iVm Art 7 DSGVO.

95 Art 9 Abs 1 lit e DSGVO.

96 *Art-29-Datenschutzgruppe*, WP 193, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien (27.4.2012), 18.

3.6.1 INFORMATIONSPFLICHTEN DES VERANTWORTLICHEN

Der Verantwortliche ist verpflichtet, betroffenen Personen eine Reihe von Informationen bezüglich der Verarbeitung von personenbezogenen Daten aktiv[97] zukommen zu lassen. Dieser Anforderung wird üblicherweise durch eine Datenschutzerklärung nachgekommen.

Auch standardisierte Bildsymbole sind eine Möglichkeit, um betroffenen Personen einen transparenten Überblick über die Datenverarbeitung zu erleichtern. Die DSGVO erlaubt explizit, standardisierte Bildsymbole in Kombination mit weiteren Informationen zu verwenden und spricht in diesem Zusammenhang von einer „leicht wahrnehmbare[n], verständliche[n] und klar nachvollziehbare[n]" Form der Darstellung.[98]

Insbesondere bei biometrischen Daten iwS, wo das Risiko für betroffenen Personen besonders stark von der konkreten Verarbeitung abhängt, könnte eine einfach zugängliche, universelle Darstellung von Informationen wie Verarbeitungszweck oder Empfänger (oder das Fehlen weiterer Empfänger bei lokaler Speicherung) der Daten von großer Bedeutung sein. Aber auch bei biometrischen Daten ieS können graphische Informationen für betroffene Personen sehr hilfreich sein, um das Risiko der Datenverarbeitung vorab zu beurteilen.

Die EU Kommission kann mithilfe delegierter Rechtsakte festlegen, welche Informationen durch Bildsymbole darzustellen sind und „Verfahren für die Bereitstellung standardisierter Bildsymbole" erlassen.[99] Die Bestimmung spricht hier ganz allgemein von Bildsymbolen, wobei hierunter wohl standardisierte Bildsymbole zu verstehen sind.[100] Ob die Kommission neben den darzustellenden Informationen auch festlegen darf, welche konkreten standardisierten Bildsymbole verwendet werden müssen, ist umstritten[101] Zum aktuellen Zeitpunkt[102] hat die EU Kommission noch keinen entsprechenden Rechtsakt erlassen, weshalb es Verantwortlichen weiterhin freigestellt ist, ob sie standardisierte Bildsymbole einsetzen.

Im Folgenden werden daher einzelne, für biometrische Daten besonders relevante Aspekte der Informationspflichten näher beschrieben.

---

97 Vgl *Artikel-29-Datenschutzgruppe*, WP 260, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (11.4.2018), Rz 3.

98 Art 12 Abs 7 DSGVO.

99 Art 12 Abs 8 DSGVO.

100 Vgl *Paal/Hennemann* in *Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz (2018), Art 12 Rz 78.

101 Ebenda.

102 Stand 18.8.2020.

datenschutzrechtlich Verantwortlicher

Wer die elektronische Verarbeitung von biometrischen Daten[103] veranlasst, wird in aller Regel über die Mittel und Zwecke der Datenverarbeitung entscheiden und daher als Verantwortlicher iSd DSGVO anzusehen sein.

Werden die biometrischen Daten einer anderen Person dem Anbieter des biometrischen Systems zur Erfassung übermittelt, wird auch der Übermittler zum Verantwortlichen, wenn er über die Verarbeitungszwecke mitentscheiden kann.[104] In diesem Fall werden Übermittler und Anbieter zu gemeinsamen Verantwortlichen. Die betroffene Person kann sich in diesem Fall idR aussuchen, an welchen Verantwortlichen sie sich bei einer Geltendmachung ihrer Rechte wendet.[105]

Dabei ist zu beachten, dass nach der Rechtsprechung des EuGH bereits eine geringfügige Entscheidungshoheit über die im Einzelfall aktivierten Auswertungsfunktionen ausreichen kann, um als Verantwortlicher zu gelten.[106] Von einer solchen Entscheidungshoheit wird auszugehen sein, wenn biometrische Daten iwS einer anderen Person (z. B. Gruppenfotos mit mehreren erkennbaren Gesichtern) übermittelt werden, und der Übermittler hierbei die Funktion zur Auswertung biometrischer Merkmale aktiviert. Auch bei einer lokalen Auswertung der Daten kann es zu einer gemeinsamen Verantwortlichkeit iZm biometrischen Daten kommen, wenn Funktionen zur biometrischen Auswertung aktiviert werden, denn auch die Erhebung von und der Abgleich mit personenbezogenen Daten stellen Verarbeitungen iSd DSGVO dar.[107]

Es kommen dabei nach der Legaldefinition des Begriffs grundsätzlich auch natürliche Personen als Verantwortliche in Betracht.[108] Hier ist allerdings der sachliche Anwendungsbereich der DSGVO zu beachten, wonach natürliche Personen bei ausschließlich persönlicher und familiärer Tätigkeit von den Bestimmungen ausgenommen sind.[109] Das nationale Grundrecht auf Datenschutz kommt unabhängig vom Konzept eines Verantwortlichen weiterhin zur Anwendung, da durch seine unmittelbare Drittwirkung auch Private verpflichtet werden.[110] Dieses Grundrecht sieht jedoch keine mit der Informationspflicht gegenüber Betroffenen gemäß der DSGVO vergleichbare Verpflichtung vor.

---

[103] Ob es sich hierbei um biometrische Daten ieS oder iwS handelt ist für diese Frage unerheblich, da auch biometrische Daten iwS personenbezogene Daten darstellen.

[104] Vgl allgemein zu möglichen Formen der Mitentscheidung *Artikel-29-Datenschutzgruppe*, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (16.2.2010), 16ff.

[105] Art 26 Abs 3 DSGVO.

[106] Vgl EuGH 05.07.2018, C-210/16 (Wirtschaftsakademie Schleswig-Holstein) Rz 36ff, wonach bereits die Kontrolle über die Parameter einer statistischen Auswertung ausreichend ist, um als Verantwortlicher iSd DSGVO zu gelten.

[107] Vgl Art 4 Z 2 DSGVO und EuGH 05.07.2018, C-210/16 Rz 38.

[108] Art 4 Z 7 DSGVO.

[109] Art 2 Abs 2 lit c DSGVO.

[110] Vgl *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG § 1 Rz 6.

Zeitpunkt der Information

Werden die Informationen bei der betroffenen Person selbst erhoben, ist den Informationspflichten spätestens zum Zeitpunkt der Erhebung nachzukommen, sofern die betroffene Person nicht bereits über diese Information verfügt.[111] Im Zusammenhang mit biometrischen Daten ieS ist beim Begriff der Erhebung der Daten besondere Vorsicht geboten. Unter Erhebung bei der betroffenen Person wird dabei laut hA die bewusste Datenübermittlung im Rahmen einer Kontaktaufnahme oder dem sonstigen aktiven Tun der betroffenen Person verstanden.[112] Zwar stammen biometrische Daten ieS immer ursprünglich von der Person, deren Identifikation sie erlauben. Jedoch erlauben manche biometrische Methoden diese Daten auch ohne Wissen oder aktives Handeln der betroffenen Person zu erheben, insbesondere wenn die Datenerfassung auf Distanz stattfindet.[113]

Gleiches gilt, wenn der betroffenen Person zwar die Datenerfassung iwS bewusst ist, nicht jedoch ihre Übermittlung an weitere Empfänger und darauffolgende Auswertung als biometrische Daten ieS zu einem späteren Zeitpunkt.[114] Da in diesem Fall das Element der bewussten Datenübermittlung bzw des aktiven Tuns fehlt, können auf diese Weise erlangte biometrische Daten ieS nicht als bei der betroffenen Person erhoben gelten.[115]

Die bereitzustellenden Informationen sollen dabei soweit als möglich ohne Wechsel des Kommunikationsmediums („Medienbruch“) abrufbar sein, um die Zugänglichkeit zu erleichtern.[116] Bei Kommunikation über elektronische Medien könnten diese beispielsweise durch einen Link zugänglich gemacht werden.

Nach Ansicht der Art-29-Datenschutzgruppe sind diese Informationen aus Gründen der Transparenz frühzeitig und daher wenn möglich schon vor Beginn der Datenerhebung zu übermitteln.[117] Ebenso wirke die Informationspflicht auch nach der ersten Erhebung der Daten fort. Nach der gleichen Ansicht müssen wesentliche Änderungen der betroffenen Person aktiv mitgeteilt werden, auch wenn eine solche Verpflichtung in der DSGVO nicht explizit festgeschrieben ist.[118] Ausdrücklich gesetzlich gefordert wird eine solche Mitteilung hingegen bei nachträglicher Änderungen des Verarbeitungszwecks.[119] Bei biometrischen Daten ieS ist dies von besonderer Relevanz, stellt doch bereits die Erfassung dieser Daten ein Risiko für die betroffene Person dar.[120]

---

111 Art 13 Abs 1 S 1 iVm Abs 4.

112 Vgl *Bäcker* in *Kühling/Buchner*, DS-GVO BDSG (2018), Art 13 DSGVO Rz 20f.

113 Vlg zu den technischen Hintergründen Kapitel 2.

114 Vgl *Artikel-29-Datenschutzgruppe*, WP 260 Rz 26.

115 Vgl hierzu allgemeiner auch *Feiler/Forgó*, DSGVO, Art 13 DSGVO Rz 2.

116 Vgl *Bäcker* in *Kühling/Buchner*, DS-GVO Art 13 DSGVO Rz 58.

117 *Artikel-29-Datenschutzgruppe*, WP 260 Rz 28.

118 Vgl *Illibauer* in *Knyrim*, DatKomm Art 13 Rz 61.

119 Ebenda Rz 29.

120 Zum diesbezüglichen technischen Hintergrund siehe Abschnitt 2.

Abweichende Fristen kommen zur Anwendung, wenn die Informationen nicht bei der betroffenen Person selbst erhoben wurden. In diesem Fall müssen betroffene Personen zum Zeitpunkt der Kontaktaufnahme oder Offenlegung gegenüber weiteren Empfängern informiert werden.[121] Findet eine solche nicht statt, ist in einer angemessenen Frist, spätestens innerhalb eines Monats zu informieren.[122] Die Informationspflicht gegenüber den einzelnen betroffenen Personen entfällt, wenn die Erteilung der Information unmöglich ist oder einen unverhältnismäßigen Aufwand verursachen würde.[123]

Bei biometrischen Daten iwS kann es beispielsweise vorkommen, dass trotz eindeutiger Identifizierbarkeit die Kontaktdaten einer betroffenen Person nicht ermittelt werden können. Eine Veröffentlichung der Informationen zur Datenverarbeitung wird in einem solchen Fall jedoch angezeigt sein, um Transparenz gegenüber allen (potentiell) betroffenen Personen herzustellen.[124]

Umfang der Information

Der Verantwortliche hat der betroffenen Person eine Reihe von Informationen bereitzustellen. Der Umfang dieser Informationen ist in Art 13 und 14 DSGVO festgelegt, wobei Art 13 zur Anwendung kommt, wenn die Informationen bei der betroffenen Person erhoben, ansonsten ist Art 14 einschlägig. Die zu erteilenden Informationen ist in beiden Artikeln in jeweils zwei Absätze gegliedert, wobei in der Literatur mehrheitlich davon ausgegangen wird, dass die Informationen beider Absätze unterschiedslos zu erteilen sind.[125]

Demnach jedenfalls zu erteilen sind die Kontaktdaten des Verantwortlichen, Zwecke und Rechtsgrundlage der Datenverarbeitung sowie die Speicherdauer oder zumindest Kriterien zur Festlegung dieser Dauer. Zusätzlich muss über die Betroffenenrechte und das Beschwerderecht an die Aufsichtsbehörde informiert werden.[126]

Falls vorhanden müssen auch die Kontaktedaten des Datenschutzbeauftragten, die berechtigten Interessen des Verantwortlichen, geplante Übermittlungen an ein Drittland, Empfänger bzw. Kategorien von Empfängern der Daten angegeben werden angegeben sowie auf das Recht, eine erteilte Einwilligung zu widerrufen, hingewiesen werden. Besteht eine automatisierte Entscheidung im Einzelfall (inkl. Profiling), muss auch hierauf hingewiesen werden.[127]

---

121 Art 14 Abs 3 lit b und c DSGVO.

122 Art 14 Abs 3 lit a DSGVO.

123 Art 14 Abs 4 lit b DSGVO.

124 Vgl Art 14 Abs 4 lit b letzter Satz DSGVO, wo eine solche Maßnahme zum Schutz der betroffenen Person gefordert wird.

125 Vgl *Bäcker* in *Kühling/Buchner*, DS-GVO Art 13 Rz 20f und *Feiler/Forgó*, DSGVO Art 13 Rz 1 idS; differenzierter hingegen *Paal/Hennemann* in *Paal/Pauly*, DSGVO Art 13 Rz 22ff.

126 Art 13 Abs 1 und 2 sowie Art 14 Abs 1 und 2 DSGVO.

127 Ebenda.

Werden die personenbezogenen Daten bei der betroffenen Person erhoben, müssen zusätzlich darüber informiert werden, ob eine Bereitstellung der Daten verpflichtend ist und welche Folgen eine Nichtbereitstellung für die betroffene Person hätte.[128]

Werden die Daten hingegen nicht bei der betroffenen Person erhoben, müssen die Kategorien der erlangten personenbezogenen Daten sowie die Datenquellen angegeben werden.[129]

Im Folgenden werden die für biometrische Daten besonders wichtigen Informationen zu Empfänger sowie zum Verarbeitungszweck näher beschrieben.

Empfänger oder Kategorien von Empfängern

Ob dem Verantwortlichen ein freies Wahlrecht zukommt, konkrete Empfänger oder Kategorien von Empfängern zu nennen, geht aus dem Wortlaut der DSGVO nicht eindeutig hervor.[130] Aus Gründen der Transparenz wird dieses Wahlrecht gemäß hA verneint. Auch sind konkrete Empfänger zu nennen, wenn diese zum Zeitpunkt der Information bekannt sind.[131]

Offen bleibt nach dem Wortlaut auch, nach welchen Kriterien die Kategorien von Empfängern voneinander abzugrenzen sind.[132] Die Art-29-Datenschutztruppe empfiehlt in diesem Zusammenhang eine Abgrenzung ua nach der Art der durchgeführten Aktivitäten und des Empfängerstandorts, wobei diese Festlegung so genau wie möglich erfolgen soll.[133]

Angabe des Verarbeitungszwecks

Wie präzise ein Verarbeitungszweck beschrieben sein muss, ist in der Literatur umstritten.[134] Mehrheitlich wird im Schrifttum eine möglichst konkrete Beschreibung des Verarbeitungszwecks gefordert, um diesen für die betroffene Person nachvollziehbar zu gestalten.[135] In der Praxis werden von Unternehmen jedoch auch sehr allgemeine Verarbeitungszwecke wie „Entwicklung neuer Dienste“ oder „für Forschungszwecke“ genannt. Die Art-29-Datenschutzgruppe rät in ihren Leitlinien zur Transparenz explizit von der Verwendung derartiger Formulierungen ab.[136] Anstelle dessen sollte klar benannt werden, welche Datenkategorien für welche Dienste oder Forschungszwecke herangezogen werden. Ansonsten könnten die biometrischen Daten einer Person für „Forschungszwecke“ zur Entwicklung neuer Verfahren zur Identifikation anderer Personen genutzt werden, ohne dass dies für die betroffene Person nachvollziehbar ist.

---

128 Vgl Art 13 Abs 1 und 2 sowie Art 14 Abs 1 und 2 DSGVO.

129 Ebenda.

130 Vgl *Illibauer* in *Knyrim*, DatKomm, Art 13 Rz 32.

131 Vgl ebenda sowie *Bäcker* in *Kühling/Buchner*, DS-GVO Art 13 Rz 30.

132 Vgl *Illibauer* in *Knyrim*, DatKomm Art 13 Rz 35.

133 Vgl *Artikel-29-Datenschutzgruppe*, WP 260 46f.

134 Vgl *Paal/Hennemann* in *Paal/Pauly*, DS-GVO Art 13 Rz 16.

135 Vgl ebenda; *Bäcker* in *Kühling/Buchner*, DS-GVO Art 13 Rz 26; *Illibauer* in *Knyrim*, DatKomm Art 13 Rz 27.

136 *Artikel-29-Datenschutzgruppe*, WP 260 Rz 12.

Bei biometrischen Daten ieS kann hierbei auch der Hinweis auf die zugrundgelegte Rechtsgrundlage aufschlussreich sein. Wird bei der Rechtsgrundlage auf Art 9 DSGVO Bezug genommen, kann die betroffene Person somit von einer Verarbeitung von besonderen Kategorien personenbezogener Daten ausgehen. Insbesondere bei der Verarbeitung von biometrischen Daten iwS (wie z. B. Gesichtsbildern oder Sprachaufnahmen), kann die Rechtsgrundlage unabhängig vom Verarbeitungszweck Aufschluss darüber geben, ob die erhobenen Daten auch als biometrische Daten ieS ausgewertet werden. Denn wenn die biometrischen Daten bei der betroffenen Person selbst erhoben wurden, muss der Verantwortliche nicht vorab über die Kategorien der erhobenen Daten informieren.[137]

Dabei ist auch denkbar, dass die erhobenen Daten erst im Nachhinein als biometrische Daten ieS weiterverarbeitet werden sollen. Bei einer Weiterverarbeitung für einen andern Zweck hat der Verantwortliche den neuen Zweck sowie alle anderen maßgeblichen Informationen der betroffenen Person vor der Weiterverarbeitung mitzuteilen.[138] Für biometrische Daten iwS bedeutet dies beispielsweise, dass die betroffene Person vor einer zukünftigen Auswertung als biometrische Daten ieS informiert werden muss. Die Information sollte dabei mit angemessenem zeitlichem Vorlauf erfolgen, um der betroffenen Person Gelegenheit zur Ausübung ihrer Rechte zu geben.[139]

3.6.2 BENACHRICHTIGUNG DER BETROFFENEN PERSON BEI VERLETZUNG DES SCHUTZES BIOMETRISCHER DATEN

Beim Umgang mit personenbezogenen Daten kann es zu technischen und organisatorischen Fehlern kommen, wodurch deren Schutz verletzt werden kann. Geschützt werden soll hierbei insbesondere die Vertraulichkeit (Datenzugang ist auf berechtigte Personen beschränkt), Integrität (Schutz vor Datenmanipulation und Datenverlust) sowie Verfügbarkeit (Daten sind für berechtigte Personen abrufbar).[140] Die DSGVO sieht daher Meldepflichten des Verantwortlichen vor, um die Rechte und Freiheiten natürlicher Personen auch in derartigen Situationen zu schützen.[141]

Bei biometrischen Daten ist insbesondere die Verletzung der Vertraulichkeit von großer praktischer Bedeutung, da hierdurch biometrische Daten auch Empfängern ohne entsprechende Berechtigung zugänglich werden können. Eine solche Verletzung der Vertraulichkeit wird auch als Datenleck bezeichnet und kann für betroffene Personen aufgrund der Dauerhaf-

---

137 Vgl Art 13 Abs 1 und 2 sowie Art 14 Abs 1 und 2 DSGVO.

138 Art 13 Abs 3 DSGVO.

139 *Artikel-29-Datenschutzgruppe*, WP 260 Rz 30f.

140 Vgl für Gesichtsbilder *EDPB*, Guidelines 3/2019, Rz 132 sowie allgemein Art 32 Abs 1 lit b DSGVO.

141 Vgl Art 33 Abs 1 und Art 34 Abs 1 DSGVO.

tigkeit von biometrischen Merkmalen zu einer langfristigen Gefährdung ihrer Privatsphäre führen.

Eine derartige Verletzung des Schutzes der personenbezogenen Daten ist der Aufsichtsbehörde unverzüglich, möglichst jedoch innerhalb von 72 Stunden zu melden.[142] Eine Ausnahme besteht nur, wenn die Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt".[143] Da biometrische Daten ieS jedoch zu den besonderen Kategorien personenbezogener Daten zählen und ihre Verarbeitung daher als besonders risikoreich gilt,[144] wird in aller Regel von einem voraussichtlichen Risiko bei diesbezüglichen Datenlecks auszugehen sein, sofern die Daten zumindest teilweise für Dritte zugänglich waren.[145]

Zusätzlich muss unverzüglich eine Meldung an die betroffenen Personen selbst erfolgen, wenn es aus dem Datenleck ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Ausnahmen bestehen, wenn die Daten durch geeignete Schutzmaßnahmen für Unbefugte unzugänglich sind,[146] wenn das hohe Risiko durch Maßnahmen des Verantwortlichen „aller Wahrscheinlichkeit nach nicht mehr besteht" oder wenn eine derartige Mitteilung mit einem unverhältnismäßigen Aufwand verbunden wäre.[147]

Da das Missbrauchsrisiko nach einem Leck von biometrischen Daten nur schwer gemindert werden kann, kommt insbesondere der letztgenannten Ausnahme praktische Relevanz zu. Ist eine Information der betroffenen Personen unverhältnismäßig, z. B. weil die Kontaktdaten der betroffenen Personen nur mit unverhältnismäßigem Aufwand ermittelt werden können,[148] muss jedoch eine öffentliche Bekanntmachung oder eine vergleichbare, wirksame Maßnahme zur Information der betroffenen Personen erfolgen.[149]

Somit ist die Frage zentral, welches Risiko für betroffene Personen von einer Verletzung des Schutzes biometrischer Daten besteht. Das Risiko setzt sich hierbei aus Eintrittswahrscheinlichkeit und Schwere der Folgen einer Verletzung der Vertraulichkeit zusammen.[150]

---

142 Art 33 Abs 1 S 1 DSGVO.

143 Ebenda.

144 Vgl ErwGr 51 S 1 DSGVO.

145 Vgl diesbezüglichen beispielhaften Katalog der *Art-29-Datenschutzgruppe*, WP 250, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Datengemäß der Verordnung (EU) 2016/6791 (6.2.2018), 36ff.

146 Zur Frage eines effektiven Schutzes durch Verschlüsselung vgl *Art-29-Datenschutzgruppe*, W P250, 21ff.

147 Art 34 Abs 3 DSGVO.

148 Vgl *Art-29-Datenschutzgruppe*, WP 250, 26.

149 Art 34 Abs 3 lit c DSGVO.

150 Vgl Erwäg 75.

Bei biometrischen Daten ieS ist aufgrund ihrer Legaldefinition davon auszugehen, dass diese zur eindeutigen Identifikation von natürlichen Personen verwendet werden. Häufig wird diese Information verwendet, um einer Person Zutritt zu einem bestimmten Bereich zu erlauben oder zu verwehren. Dabei kann es sich um physische Räumlichkeiten, aber auch um den Zugang zu digitalen Endgeräten handeln. Sind biometrische Daten ieS, welche eine Rekonstruktion der biometrischen Merkmale erlauben einmal kompromittiert, können sich Dritte mithilfe dieser Informationen unberechtigten Zutritt zu diesem Bereich verschaffen (Zugang durch Identitätsdiebstahl). Die Folgen eines Identitätsdiebstahls können für die betroffene Person sehr schwerwiegend sein. Beispielsweise könnten Dritte Handlungen der betroffenen Person fingieren oder Rechtsgeschäfte in ihrem Namen abschließen.

Ein wichtiger Faktor für die Eintrittswahrscheinlichkeit ist auch die Dauer, innerhalb derer Folgen der Verletzung des Schutzes biometrischer Daten auftreten können. Die betroffene Person selbst kann ihre biometrischen Daten üblicherweise nicht ohne unverhältnismäßigen Aufwand verändern oder verbergen. Auch sind biometrische Merkmale üblicherweise so gewählt, dass sie über lange Zeiträume stabil bleiben. Aus technischer Sicht sind daher unberechtigten Dritten zugänglich gewordene biometrische Daten auf unbestimmte Zeit für eine sichere Authentifizierung unbrauchbar geworden. Sie können die betroffene Person daher dauerhaft beeinträchtigen.

Zusätzlich bergen über Distanz erfassbare biometrisch Merkmale wie z. B. Gesichtsbilder oder Sprachaufnahmen das Risiko für betroffene Personen, ohne ihr Wissen auch durch Dritte identifiziert werden zu können. Somit besteht ein permanentes Risiko hinsichtlich der Sicherheit zukünftiger Identifikationsvorgänge und der Privatsphäre der betroffenen Person. Die Wahrscheinlichkeit eines zukünftigen Eintritts einer derartigen Folge ist somit hoch.

Eine Verletzung des Schutzes von biometrischen Daten ieS, bei denen diese Daten Dritten zugänglich werden, stellt aus all diesen Gründen mE daher grundsätzlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person dar.

Bei biometrischen Daten iwS kommt es zu einer ähnlichen Problemstellung. Diese Daten erlauben die Identifikation von natürlichen Personen, selbst wenn sie vom Verantwortlichen nicht auf biometrische Merkmale hin ausgewertet werden. Sind die Daten jedoch einmal einem unbestimmten Personenkreis zugänglich gemacht worden, besteht ein großes Risiko, dass Dritte diese Daten faktisch zur biometrischen Identifikation verwenden, unabhängig davon, ob eine derartige Nutzung datenschutzrechtlich zulässig ist.

Für biometrische Daten iwS besteht daher aus Sicht der betroffenen Person eine ähnlich große Missbrauchsgefahr durch Dritte wie bei biometrischen Daten ieS. Daher kann auch ein Datenleck von biometrischen Daten iwS häufig zu einem hohen Risiko für betroffene Personen führen.

3.6.3 AUSKUNFTSRECHT DER BETROFFENEN PERSON

Neben den Informationspflichten hat die betroffene Person auch das Recht, vom Verantwortlichen Auskunft über die konkret verarbeiteten Daten zu verlangen.[151]

Für biometrische Daten ist eine derartige Auskunft auch deswegen interessant, weil sie grundsätzlich vollständig und in verständlicher Form zu erfolgen hat.[152] Bei biometrischen Daten ieS lässt eine vollständige Auskunft über die konkret genutzten Daten auch Rückschlüsse darauf zu, ob die Speicherung von biometrischen Daten in geschützter Form (z. B. in gehashten Templates)[153] oder in Form von Rohdaten erfolgt. Gleichzeitig muss die Darstellung allgemein verständlich sein,[154] weshalb nicht die reine Angabe der gehashten Templates in Rohform ausreicht, sondern in aller Regel weitere Erläuterungen notwendig sein werden. Der Verantwortliche sollte hier beispielsweise darlegen, dass es sich bei gehashten Templates um eine besondere Speicherform von biometrischen Daten handelt, bei denen eine Rückführung auf die biometrischen Quellmerkmale erschwert ist.

Eine Auskunft geringen Umfangs kann bei biometrischen Daten durchaus im Interesse der betroffenen Person sein, solange die Auskunft tatsächlich vollständig erfolgt. Erfolgt eine Identifizierung der betroffenen Person ausschließlich am lokalen Endgerät ohne weitere Datenübermittlung, verfügt der Verantwortliche nämlich über keine biometrischen Daten, über die er der betroffenen Person Auskunft geben kann.

Zusätzlich zu den konkreten Daten besteht auch Anspruch auf weitere Informationen, die sich inhaltlich jedoch stark mit den Informationspflichten gemäß Art 13 und 14 DSGVO überlappen. Für biometrische Daten relevante Unterschiede bestehen nur punktuell. So sind die Kategorien der personenbezogenen Daten bekanntzugeben, auch wenn die Daten bei der betroffenen Person selbst erhoben wurden.[155]

Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, sind jedoch nur „alle verfügbaren Informationen über die Herkunft der Daten“ bereitzustellen. In der Literatur wird daher teilweise die Meinung vertreten, wenn der Verantwortliche über keine Informationen bezüglich Herkunft der konkreten Daten verfüge, müsse diese Herkunft den betroffenen Personen demnach auch nicht mitgeteilt werden.[156] Bei biometrischen Daten würde dies bedeuten, dass die Herkunft der kon-

---

151 Vgl *Haidinger* in *Knyrim*, DatKomm Art 15 Rz 29 sowie Art 15 Abs 1 DSGVO.

152 Ebenda Rz 33f.

153 Zu den technischen Hintergründen dieses Begriffs und weiteren diesbezüglichen Grundlagen siehe Kapitel 2.3.

154 Vgl *Haidinger* in *Knyrim*, DatKomm Art 15 Rz 34.

155 Art 15 Abs 1 lit b DSGVO.

156 Vgl *Haidinger* in *Knyrim*, DatKomm Art 15 Rz 43.

kreten Daten der betroffenen Person bei spärlicher Dokumentation des Verantwortlichen unklar bleiben kann. Die allgemeinen Datenquellen müssen jedoch jedenfalls weiterhin vom Verantwortlichen dokumentiert werden, um den Informationspflichten nachkommen zu können

3.6.4 RECHT AUF BERICHTIGUNG UND RECHT AUF LÖSCHUNG

Das Recht auf Berichtigung erlaubt der betroffenen Person, vom Verantwortlichen die Korrektur unrichtiger personenbezogener Daten zu verlangen. Bei biometrischen Daten wird dieses Recht wohl nur in Ausnahmefällen zum Tragen kommen, z. B. wenn irrtümlich die falsche Person unter dem Namen der betroffenen Person erfasst wurde.

In der Praxis bedeutsamer ist das Recht der betroffenen Person, bei Vorliegen bestimmter Gründe die Löschung der personenbezogenen Daten zu verlangen. Biometrische Daten ieS werden häufig auf der Rechtsgrundlage der Einwilligung verarbeitet. Wird die Einwilligung von der betroffenen Person widerrufen, stellt dies einen Grund dar, vom Verantwortlichen die Löschung der biometrischen Daten zu verlangen.[157]

Hat der verantwortliche die Daten zu diesem Zeitpunkt bereits öffentlich gemacht, hat er andere Verantwortliche über das Löschbegehren der betroffenen Person zu informieren, soweit dies mit angemessenem Aufwand möglich ist.[158] Bei biometrischen Daten könnte dies z. B. öffentlich verfügbare Daten zur Gesichtsform oder zu Stimmprofilen betreffen. Auch weitere Empfänger der Daten sind vom Löschbegehren zu informieren, soweit dies mit verhältnismäßigem Aufwand möglich ist, und der betroffenen Person sind auf Verlangen die weiteren Empfänger offenzulegen.[159]

Allerdings erstreckt sich das Löschbegehren nur auf den adressierten Verantwortlichen und die weiteren Verantwortlichen sind nicht automatisch verpflichtet, die bei ihnen vorliegenden biometrischen Daten ebenfalls zu löschen.[160] In der Praxis ist das Recht auf Löschung bei der Übermittlung an weitere Verantwortlich nur beschränkt wirksam und führt in aller Regel nicht zu einer automatischen Löschung biometrischer Daten bei allen Verantwortlichen.

---

[157] Art 17 Abs 1 lit b DSGVO.

[158] Art 17 Abs 2 DSGVO.

[159] Art 19 DSGVO.

[160] *Herbst* in *Kühling/Buchner*, DS-GVO, Art 17 Rz 64.

3.6.5 EINSCHRÄNKUNG DER VERARBEITUNG UND WIDERSPRUCHSRECHT

Werden überwiegend berechtigte Interessen des Verantwortlichen als Rechtsgrundlage herangezogen, kann die betroffene Person aus Gründen ihrer „besonderen Situation" Widerspruch gegen die Verarbeitung anmelden.[161] Die DSGVO legt dabei nicht näher fest, was in diesem Zusammenhang unter einer „besonderen Situation" zu verstehen ist. Das Widerspruchsrecht ist vor allem für biometrische Daten iwS von Bedeutung, da biometrische Daten ieS einer anderen Rechtsgrundlage als des überwiegend berechtigten Interesses eines Verantwortlichen bedürfen. Betreffen könnte dies z. B. Gesichtsbilder, wenn diese noch nicht auf ihre biometrischen Merkmale hin analysiert werden.

Bis eine Entscheidung über den Widerspruch erfolgt, ist die Verarbeitung der biometrischen Daten einzuschränken, wobei eine weitere Verarbeitung (mit Ausnahme der Speicherung) nur noch aus bestimmten Gründen erfolgen darf.[162]

3.6.6 RECHT AUF DATENÜBERTRAGBARKEIT

Beruht eine automatisierte Datenverarbeitung auf einer Einwilligung ist für den Vertragsabschluss notwendig, hat die betroffene Person das Recht, ihre Daten in einem maschinenlesbaren Format zu erhalten und die Übertragung an einen anderen Verantwortlichen zu verlangen.[163]

Bei biometrischen Daten ieS wird dieses Recht wohl nur in Ausnahmefällen zum Tragen kommen. In vielen Fällen wird die erneute Erfassung der biometrischen Merkmale der betroffenen Person in beim neuen Verantwortlichen zielführender sein, zumal auch die Datenübermittlung selbst ein Risiko darstellt.

Bei biometrischen Daten iwS ist ein solche Datenübertragung in einer größeren Anzahl von Szenarios denkbar. So könnten die bei einem Verantwortlichen gespeicherten Stimmaufnahmen oder Gesichtsbilder der betroffenen Person an einen anderen Verantwortlichen übertragen werden, um sie dort biometrisch auswerten zu können.

---

161 Art 21 Abs 1 DSGVO.

162 Art 18 Abs a lit c iVm Abs 2 DSGVO.

163 Art 20 Abs 1 und 2 DSGVO.

3.6.7 AUTOMATISIERTE ENTSCHEIDUNGEN UND PROFILING

Weitere Rechte existieren bei Entscheidungen im Einzelfall, welche betroffenen Personen gegenüber rechtlicher Wirkung entfalten oder in ähnlicher Weise erheblich beeinträchtigen, wovon auch Profiling umfasst ist.[164] Eine erhebliche Beeinträchtigung könnte z. B. die Verweigerung eines Vertragsschlusses auf Basis dieser Entscheidung sein. In diesem Fall kann die betroffene Person grundsätzlich verlangen, nicht einer solchen Entscheidung unterworfen zu werden.

Bei besonderen Kategorien von personenbezogenen Daten wie biometrischen Daten ieS kann der Verantwortliche der betroffenen Person dieses Recht nur verwehren, wenn die Daten auf Basis einer ausdrücklichen Einwilligung oder aus Gründen eines erheblichen öffentlichen Interesses erforderlich verarbeitet werden.[165] Da die betroffene Person jedoch die Einwilligung jederzeit widerrufen kann, kommt ihr in diesem Fall ein effektives Widerspruchsrecht zu.

Basierte die Entscheidung auf biometrischen Daten iwS welche nicht zu den besonderen Kategorien von personenbezogenen Daten gehören, muss der Verantwortliche der betroffenen Person auch dann kein Widerspruchsrecht einräumen, wenn die Verarbeitung für einen Vertragsschluss erforderlich oder aufgrund spezifischer nationaler oder unionrechtlicher Rechtsvorschriften zulässig ist.[166] Diese Rechtsvorschriften müssen jedoch Maßnahmen zur Wahrung der Rechte der betroffenen Person vorsehen. Bei einer Verarbeitung, die für einen Vertragsschluss erforderlich oder ist oder auf Basis einer Einwilligung erfolgt, muss die betroffene Person zumindest das Recht auf Anfechtung der Entscheidung bei einer natürlichen Person haben.[167] Diese Person muss dabei auch die faktische Kompetenz haben, die automatisierte Entscheidung notwendigenfalls auch abzuändern[168] und die betroffene Person hat das Recht, ihren eigenen Standpunkt darzulegen.

---

[164] Art 22 Abs 1 DSGVO.

[165] Art 22 Abs 4 DSGVO.

[166] Art 22 Abs 2 lit a und b DSGVO.

[167] Art 22 Abs 3 DSGVO.

[168] *Buchner* in *Kühling/Buchner*, DS-GVO, Art 22 Rz 15.

3.7 SONSTIGE VERPFLICHTUNG DES VERANTWORTLICHEN MIT BESONDERER BEDEUTUNG FÜR BIOMETRISCHE DATEN

Neben den Rechten der betroffenen Person treffen den Verantwortlichen noch eine Reihe weiterer Verpflichtungen. Von besonderer Bedeutung für biometrische Daten sind hier die Datensicherheitsmaßnahmen. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („Privacy by default and by design") sind ebenfalls für einen effektiven Schutz biometrischer Daten in der Praxis essenziell. Die Datenschutzfolgenabschätzung soll schließlich dazu beitragen, mögliche Risiken im konkreten System zu erkennen und frühzeitig gegenzusteuern. Diese Verpflichtungen werden im Folgenden näher beschrieben.

3.7.1 DATENSICHERHEITSMAßNAHMEN

Die nach Artikel 32 DSGVO geforderten Datensicherheitsmaßnahmen zielen darauf ab, mittels technischer und organisatorischer Maßnahmen ein angemessenes Schutzniveau für die betroffene Person zu erreichen.[169] Dafür werden neben dem Risiko der Datenverarbeitung ua auch die technische Machbarkeit sowie die Implementierungskosten herangezogen.

Bei der Verarbeitung von biometrischen Daten kann insbesondere die Offenlegung oder der Zugang unbefugter Personen schwerwiegende Folgen für die betroffene Person, z. B. in Form von Identitätsdiebstahl oder unbewusster Überwachung, haben. Diese sind bei der Beurteilung eines angemessenen Schutzniveaus zu berücksichtigen,[170] wodurch bei biometrischen Daten ein hohes Schutzniveau erforderlich sein wird.

In Artikel 32 werden auch einige Maßnahmen zur Datensicherheit beispielhaft[171] angeführt. Von den dort vorgeschlagenen Maßnahmen sind die Verschlüsselung sowie Sicherstellung der Vertraulichkeit biometrischer Daten von zentraler Bedeutung. Pseudonymisierung scheidet hingen bei biometrischen Daten ieS aus, da diese Daten inhärent personenbezogen sind.

Auch kann sich die Wirksamkeit dieser Datensicherheitsmaßnahmen mit der Zeit verändern. Insbesondere bei biometrischen Daten kommen durch den technischen Fortschritt laufend neue Auswertungsmöglichkeiten dazu. Um die Datensicherheit weiterhin zu gewährleisten sind die getroffenen

---

169 *Jandt* in *Kühling/Buchner*, DS-GVO, Art 32 Rz 5; neben Verantwortlichen sind hierzu auch Auftragsverarbeiter verpflichtet.

170 Art 32 Abs 2 DSGVO.

171 *Jandt* in *Kühling/Buchner*, DS-GVO, Art 32 Rz 14.

Maßnahmen daher in regelmäßigen Abständen zu überprüfen.[172] Dieser Zeitabstand wird nicht konkret vorgegeben, sondern soll nach hA risikoabhängig erfolgen.[173] Bei einem zentralisierten biometrischen System wären demnach häufigere Überprüfungen erforderlich, als bei einer ausschließlich lokalen Auswertung auf einem einzelnen Endgerät. Viele dieser Maßnahmen entfalten ihre volle Wirksamkeit nur, wenn sie bereits bei der Systemgestaltung berücksichtigt werden. Die diesbezüglichen Vorgaben der DSGVO werden im nächsten Abschnitt näher erläutert.

3.7.2 DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Datenschutz durch Technikgestaltung (häufig auch nach der englischen Sprachfassung „privacy by design" genannt) verpflichtet Verantwortliche, bereits bei der Wahl der Mittel der Datenverarbeitung (Zeitpunkt der Technikgestaltung) die Datenschutzgrundsätze durch technisch organisatorische Maßnahmen wirksam umzusetzen.[174] Exemplarisch wird der Grundsatz der Datenminimierung genannt, die Regelung umfasst jedoch auch die weiteren Grundsätze des Art 5 Abs 1 DSGVO.[175] Die Verpflichtungen richteten sich explizit nur an den Verantwortlichen, treffen indirekt aber auch Hersteller biometrischer Systeme, da den Verantwortlichen eine Pflicht zur Auswahl datenschutzfreundlicher Mittel trifft. [176] Auch hier hängen die zu treffenden Maßnahmen vom zu erwartenden Risiko der Datenverarbeitung ab, wobei hier die gleichen Kriterien wie bei Art 32 DSGVO zur Anwendung kommen.[177]

Wie bereits im vorherigen Abschnitt dargelegt, ist dieses Risiko bei der Verarbeitung von biometrischen Daten ieS iA hoch. Es sind daher bereits bei der Technikgestaltung geeignete Maßnahmen zum Schutz der betroffenen Personen zu treffen. Umfassen könnte dies z. B. eine ausschließlich lokale Datenverarbeitung, eine Speicherung in besonders geschützten Bereichen sowie in Form von gehashten Templates, welche eine Rekonstruktion des ursprünglichen biometrischen Merkmals erschweren.

Weiteres ist der Verantwortliche verpflichtet, datenschutzfreundliche Voreinstellungen zu wählen (privacy by default). Dies bedeutet insbesondere, dass nur die für den Verarbeitungszweck erforderlichen Daten erfasst und gespeichert werden dürfen. Ein Abweichen hiervon benötigt ein aktives

---

[172] Art 32 Abs 1 lit d DSGVO.

[173] Vgl *Jandt* in *Kühling/Buchner*, DS-GVO, Art 32 Rz 30.

[174] Art 25 Abs 1 DSGVO.

[175] *Hartung* in *Kühling/Buchner*, DS-GVO, Art 25 Rz 14.

[176] *Hartung* in *Kühling/Buchner*, DS-GVO, Art 25 Rz 13.

[177] Vgl Art 32 Abs 1 und Art 25 Abs 1 DSGVO.

Eingreifen durch die betroffene Person.[178] Es kann daher als eine Konkretisierung der Grundsätze der Datenminimierung, Speicherbegrenzung und Zweckbindungen verstanden werden. Bei biometrischen Daten iwS wie z. B. Gesichts- oder Stimmaufnahmen, welche für andere Zwecke erhoben wurden, dürfen somit beispielsweise nicht per Voreinstellung biometrisch ausgewertet werden.

Auch dürfen die erhobenen Daten nicht per Voreinstellung einer unbestimmten Anzahl von Personen zugänglich gemacht werden.[179] Für biometrische Daten iwS ist dies von besonderer Relevanz, da bei einer Veröffentlichung diese von Dritten für biometrische Zwecke ausgewertet werden können.[180]

3.7.3 DATENSCHUTZ-FOLGENABSCHÄTZUNG

Im Datenschutzrecht wird an vielen Stellen auf das Risiko für die Rechte und Freiheiten natürlicher Personen abgestellt. Hierbei ist der Verantwortliche verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Verarbeitung voraussichtlich zu einem hohen Risiko führt.[181] Dabei wird neben weiteren Kriterien auch auf den Umfang, Umstände und Zwecke der Datenverarbeitung sowie auf die Verwendung neuer Technologien abgestellt.[182]

Zusätzlich löst eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten“[183] eine Pflicht zur Datenschutz-Folgenabschätzung aus, wobei biometrische Daten ieS jedenfalls in die als besondere Kategorie von personenbezogenen Daten gelten. Systeme, welche biometrische Daten ieS verarbeiten werden daher regelmäßig eine Datenschutz-Folgenabschätzung notwendig machen. Aber auch bei Systemen, welche biometrische Daten iwS verarbeiten, kann eine Datenschutz-Folgenabschätzung notwendig sein. Denkbar ist dies z. B. wenn Sammlungen von Gesichtsbildern oder Stimmaufnahmen betroffener Personen Dritten zugänglich gemacht und somit von ihnen potentiell auf biometrische Merkmale ausgewertet werden können. Derartige Sammlungen können die Rechte einer großen Zahl von betroffenen Personen berühren und die Verarbeitung kann aufgrund der Umstände für betroffene Personen schwer nachvollziehbar sein.

---

178 Vgl *Hartung* in *Kühling/Buchner*, DS-GVO, Art 25 Rz 24 wonach vorausgewählte datenschutzunfreundliche Einstellungen einen Verstoß gegen diese Pflicht darstellen.

179 Art 25 Abs 2 S 2 DSGVO.

180 Für Beispiele einer solchen nachträglichen biometrischen Auswertung siehe Kapitel 5.

181 Art 35 Abs 1 S 1 DSGVO.

182 Ebenda; Vgl auch *Jandt* in *Kühling/Buchner*, DS-GVO Art 35 Rz 7f.

183 Art 35 Abs 3 lit b DSGVO.

Eine Datenschutz-Folgenabschätzung hat jedenfalls eine systematische Beschreibung der Verarbeitung inklusive der verfolgten Zwecke sowie eine Bewertung der Notwendigkeit und Verhältnismäßigkeit sowie der Risiken für betroffene Personen zu enthalten.[184] Die geplante Bewältigung dieser Risiken durch geeignete Abhilfemaßnahmen wie z. B. Garantien oder Sicherheitsvorkehrungen ist ebenfalls zu dokumentieren.[185] Die Wirksamkeit dieser Abhilfemaßnahmen ist für biometrische Daten von besonders großer Bedeutung, gehen von deren Verarbeitung doch besonders langfristige Risiken, z. B. in Form von Überwachung oder Identitätsdiebstahl aus.

[184] Art 35 Abs 7 lit a bis c DSGVO.

[185] Art 35 Abs 7 lit d DSGVO.

4 ANWENDUNGSGEBIETE

4.1 SZENARIEN

4.1.1 ZUGANGSKONTROLLE

Die Zugangskontrolle ist eines der traditionellen Anwendungsgebiete biometrischer Methoden. Um Zugang zu einem physischen oder virtuellen Raum zu erhalten muss eine Person dabei anhand ihrer biometrischen Merkmale erfolgreich identifiziert werden können. Häufig verwendete Merkmale sind hier Fingerabdruck und Analyse der Gesichtsform,[186] bei Zugang zu besonders gesicherten physischen Räumen im Unternehmensumfeld kommen auch Iris- oder Handgeometrie zum Einsatz.

Lebenderkennung

Gleichzeitig sollten solche Systeme unterscheiden können, ob die Merkmale direkt von lebenden Menschen oder von einer biometrischen Attrappe stammen. Eine solche Funktion wird meist als Lebenderkennung bezeichnet und ist essentiell für eine verlässliche Zugangskontrolle. In der Vergangenheit konnten Systeme zur Gesichtserkennung beispielsweise mit einem einfachen Ausdruck eines Gesichtsbilds getäuscht werden.[187] Bei der Gesichtserkennung können Konsument*innen aufgefordert werden zu lächeln,[188] bei dem Fingerabdruck können Strukturen knapp unterhalb der Hautoberfläche vermessen werden.[189]

Einen wesentlichen Unterschied macht auch, ob die Identität mittels Vergleiches mit den Merkmalen einer bestimmten Person (Verifikation) oder einem großen Kreis an Personen (Identifikation) bestimmt wird.[190]

Verifikation

Im Privatbereich werden elektronische Geräte wie Smartphones oder Tablets häufig nur von einer einzigen Person verwendet. In diesem Bereich ist daher eine Zugangskontrolle durch Verifikation anhand von lokal erfassten biometrischen Merkmalen üblich. Beispiele aus diesem Bereich sind Face ID oder Touch ID zur Gesichts- bzw. Fingerabdruckerkennung bei

---

186 *Datenschutzkonferenz*, Positionspapier zur biometrischen Analyse, 03.04.2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf. S 16f.

187 *Ryne*, Samsung Galaxy S10 face unlock can be fooled by a photo, video, or even your sister, Android Police, 09.03.2019, 10.

188 *Xinhua*, Guangzhou subway adopts facial recognition, 10.09.2019. https://www.chinadaily.com.cn/a/201909/10/WS5d7766cea310cf3e3556ad0e.html, aufgerufen am 24.11.2020.

189 *Apple*, Informationen zur fortschrittlichen Sicherheitstechnologie von Touch ID. https://support.apple.com/de-at/HT204587, aufgerufen am 24.11.2020.

190 Siehe hierzu Kapitel 2.

iOS sowie die Biometrics API[191] für Android Geräte. Benötigte Daten zur Verifikation können direkt am lokalen Endgerät gespeichert werden, eine Übertragung zu einer zentralen Datenbank ist aus technischer Sicht nicht erforderlich. Wird das Gerät von mehreren Personen verwendet, kann durch die Auswahl des Kontos bestimmt werden, welche Person verifiziert werden soll.[192]

Mehrfaktor Authentifizierung

Gleiches gilt, wenn biometrische Merkmale gemeinsam mit anderen Methoden der Identitätsbestimmung verwendet werden sollen. So können beispielsweise Passwörter oder Schlüsselkarten gemeinsam mit biometrischen Methoden eingesetzt werden. Solche Methoden werden Mehrfaktor-Authentifizierung genannt, da sie die Identität einer Person mittels mehrerer Methoden bestimmen. Da durch den weiteren Faktor üblicherweise bekannt ist, die Identität welcher Person überprüft werden soll, kann auch hier Verifikation zum Einsatz kommen.

Bei Smartphone Apps zur Verwaltung von Bankguthaben und Freigabe von Zahlungen kommen biometrische Merkmale häufig zum Einsatz.[193] Die Mehrfaktor-Authentifizierung ist hier gesetzlich vorgeschrieben,[194] wobei für den zweiten Faktor häufig Biometrie gewählt wird. Werden biometrische Faktoren hingegen alternativ zu anderen Methoden zur Identitätsbestimmung verwendet, handelt es sich hierbei um keine echte Mehrfaktor-Authentifizierung. Beispiele sind die Entsperrung von elektronischen Geräten oder eines Passwortmanagers entweder mittels biometrischer Merkmale wie Fingerabdruck oder Gesichtsform oder alternativ mittels PIN oder Passwort.

Ist jedoch nicht im Vorhinein bekannt, welche Person von den biometrischen Systemen erwartet wird, ist eine Identifikation der Person anhand ihrer biometrischen Merkmale erforderlich. Identifikation wird häufig verwendet, wenn biometrische Systeme den Zugang zu einem von vielen Personen nutzbaren Bereich gewähren sollen und aus Komfort keine Kontoauswahl oder zweiter Faktor verwendet wird. In einem Referenzprojekt wurden berechtigte Schüler anhand ihres Fingerabdrucks identifiziert, um die Zugangsberechtigung zur Schulbibliothek zu überprüfen.[195] Die dafür benötigten biometrischen Templates wurden auf einem zentralen Server

---

[191] *Google*, Show a biometric authentication dialog | Android-Entwickler, https://developer.android.com/training/sign-in/biometric-auth?hl=de, aufgerufen am 24.11.2020.

[192] Akzeptiert das System mehrere Fingerabdrücke unterschiedlicher Personen, handelt es sich aus technischer Sicht nicht mehr um eine Verifikation, sondern um eine Identifikation.

[193] *Schneider*, Fingerabdruck statt Passwort: Biometrische Verfahren werden beim Banking beliebter, 14.08.2020, https://www.handelsblatt.com/technik/sicherheit-im-netz/fingerabdruck-statt-passwort-biometrische-verfahren-werden-beim-banking-beliebter/26093358.html.

[194] § 87 Abs 1 Zahlungsdienstegesetz 2018 idgF.

[195] *Bitkom*, Biometrie Referenzprojekte, 2008, https://bitkom.org/sites/default/files/file/import/Biometrie-Broschuere.pdf, 9.

gespeichert. Aufgrund des hohen Missbrauchspotentials dieser Templates ist können derartige Systeme zum Einsatz kommen. In einem weiteren Referenzprojekt wurde so die Schließanlage durch eine biometrische Zugangskontrolle auf Basis von Fingerabdrücken ersetzt.[196] Durch den technischen Fortschritt werden die dafür benötigten technischen Systeme kleiner und mobiler. Biometrische Zugangssysteme auf der Basis von Fingerabdrücken können so beispielsweise auch in Reisekoffern integriert werden.[197]

Biometrie als Komfortfunktion

Insgesamt ist im Bereich der biometrischen Zugangskontrolle eine deutliche Veränderung zu bemerken. Ursprünglich wurden biometrische Zugangskontrollen vor allem als zusätzliche Absicherung für besonders geschützte Räume gesehen. Zunehmend werden diese auch als Komfortfunktion verwendet, um die Nutzung von Passwörtern oder Schlüsselkarten zu vermeiden. In dieser Rolle kommen sie auch in elektronischen Geräten von Konsument*innen wie Smartphones, Laptops oder Tablets zum Einsatz. Auch neue Gerätekategorien wie smarte Brillen oder Wearables erweitern die möglichen Einsatzgebiete. Biometrische Methoden zur Zugangskontrolle sind damit endgültig im Alltag vieler Konsument*innen angekommen.

Zugangskontrolle und Arbeitszeiterfassung

Systeme zur biometrischen Zugangskontrolle protokollieren üblicherweise jeden Zugriffsversuch. Dieses Protokoll kann auch für andere Zwecke herangezogen werden. Im Unternehmenskontext können solche Systeme beispielsweise zur Arbeitszeiterfassung der Mitarbeiter*innen verwendet werden. Zu beachten ist allerdings, dass die Verwendung von Biometrie die Menschenwürde der erfassten Mitarbeiter*innen berührt. Der OGH hat daher bereits 2006 entschieden, dass eine biometrische Arbeitszeiterfassung auf der Basis von Fingerabdrücken der Zustimmung des Betriebsrats bedarf.[198]

4.1.2 VERHALTENSTRACKING

Ein wesentlicher Unterschied zu den oben beschriebenen Zugangskontrollmechanismen, die sich biometrischer Daten bedienen, steht eine andere Spielart der Überwachung: die Überwachung körpereigener Parameter und damit zusammenhängend die Verhaltenskontrolle. Im Unterschied zu Zugangskontrollen, die sich meist auf bestimmte Bereiche bzw. Zeiträume beziehen und in ihrer Anwendung meist eine bewusste Handlung, die auch eine Ablehnung sein kann, notwendig machen, ist die Messung körpereigener Parameter oft unsichtbar, zumeist weniger bewusst und vor allem oft über undefinierte Zeiträume gedehnt. Insgesamt ist ein Trend zu erkennen, dass die uns umgebenden Technologien der Überwachung dem

196 Ebenda S 12.

197 Siehe z. B. *Kabuto*, Smart Luggage Kabuto, https://mykabuto.com/.

198 OGH 9ObA109/06d (20.12.2006).

Menschen und seiner Lebensweise immer näherkommen. „Sie nisten sich rasch zwischen uns ein, kommen uns sehr nahe und sind sogar in uns selbst, sodass sie uns immer besser kennen lernen und sogar menschliche Züge annehmen. Kurz gesagt, wir sind zu Mensch-Maschine-Gemischen, zu Cyborgs geworden."[199]

Realisierungen dieses Trends sind Gesundheits-, Fitness-, Sport- und Abnehm-Apps und ihre sensorbestückten Pendants in Form von Smart-Watches, Fitnessarmbändern, Amuletten/Anhängern bis hin zum gewöhnlichen Smartphone, das auch in der Lage ist als Schrittzähler zu fungieren. Die zunehmende Quantifizierung von körperlichen Merkmalen und Leistungen in der Quantified Self Bewegung[200] sowie die Datafizierung des Körpers[201] beschreiben einen qualitativen Sprung in der Überwachung.

Gesundheitsbezogene Webseiten und Plattformen machen schon lange einen großen Teil des Internets aus. Als Weiterentwicklung werden so genannte m-Health Apps – mobile Anwendungen oft über Smartphones realisiert – entwickelt. Diese dedizierten Anwendungen im Bereich e-Health/m-Health und Telemedizin beziehen sich zu einem Großteil auf Diabetes, psychische Gesundheit und Adipositas[202] und zunehmend auch zur Blutdruckmessung[203] stehen jedoch nicht im Fokus dieser Studie.

4.1.3 PERSONENERKENNUNG

Personenerkennung ist ein weiteres traditionelles Anwendungsszenario von biometrischen Methoden. Im Gegensatz zur Zugangskontrolle sollen hier betroffene Personen regelmäßig auch durch unbewusste Datenauswertung ohne aktive Unterstützung durch die betroffene Person wiedererkannt werden.

Ursprünglich war dieses Szenario vorwiegend im Bereich der Sicherheitsbehörden anzutreffen, durch den technischen Fortschritt erhält es jedoch auch zunehmend im Unternehmens- und Privatbereich Einzug. Im Privatbereich geht es hierbei vorwiegend um die Suche auf Basis von Gesichtsbildern. Häufig wird hier ein Gesichtsbild als Suchanfrage verwendet und es werden weitere Aufnahmen gesucht, auf denen dieselbe Person abgebildet ist. Auch können Aufnahmen, die ein Gesichtsbild derselben Person enthalten automatisch gruppiert werden.

Einen großen Unterschied macht hier die Datenbasis, in der nach Gesichtsbildern gesucht wird. Während Programme zur Gruppierung sich vorwiegend auf die privaten Fotoalben von Benutzer*innen beschränkten,

---

199 *Est et al*, 2014.

200 Siehe https://quantifiedself.com, aufgerufen am 19.10.2020.

201 *Mager/Mayer* 2019.

202 *Byambasuren et at*, 2018.

203 *Luo et al*, 2019, *Klatt* 2019.

durchsuchen Fotosuchmaschinen große Teile des öffentlich zugänglichen Internets nach möglichen Übereinstimmungen. Manche Unternehmen sehen die Suche auf Basis von Gesichtsbildern auch als Möglichkeit, meist auf Basis von Gesichtsbildern aus Überwachungskameras, nach „unerwünschten Personen" Ausschau zu halten.[204] Auf die weitreichenden gesellschaftlichen Auswirkungen derartiger universeller Gesichtssuchen wird in Kapitel 5 näher eingegangen.

4.2 OPTISCHE PERSONENERFASSUNG

Kamerasysteme sind im Alltag von Konsument*innen weit verbreitet. Die optische Personenerfassung umfasst daher eine Vielzahl möglicher Anwendungsgebiete.

Das wohl bekannteste biometrische Anwendungsgebiet aus diesem Bereich ist die Gesichtserkennung. Diese benötigt keinen direkten Kontakt mit der betroffenen Person und kann aus technischer Sicht auch ohne deren Kenntnis erfolgen. Neben dem Gesicht sind auch andere biometrische Merkmale zur optischen Personenerfassung geeignet. Auch eine Analyse des charakteristischen Gangs einer betroffenen Person kann Aufschluss über ihre Identität bieten. Diese Analyse benötigt kein erkennbares Gesicht und kann daher typischerweise aus größerer Distanz erfolgen. Sie ist daher in besonderem Maße zur Überwachung von Personen geeignet.[205]

Erfassung mit Abstand

Ein weiteres Einsatzgebiet der Gesichtserkennung ist die Gruppierung von Abbildungen, welche Gesichtsbilder der gleichen Person enthalten. Hierbei werden häufig für andere Zwecke erfasste Gesichtsbilder für biometrische Analysen wiederverwendet. Problematisch ist dabei insbesondere, dass die betroffenen Personen praktisch keine Möglichkeit haben, auf diese Form der Datenauswertung Einfluss zu nehmen, da sie ihnen vielfach nicht bewusst sein wird. Neben Gesichtsbildern können auch andere optisch erfassbare Merkmale wie der charakteristische Gang einer Person zur Identifizierung herangezogen werden. Derartige Verfahren können auch dann zum Einsatz kommen, wenn die betroffene Person sich von der Kamera abwendet oder ihr Gesicht auf den Aufnahmen nicht ausreichend erkennbar ist und erweitern somit den räumlichen Einsatzbereich optischer Verfahren.

Erfassung auf kleine Distanz

Andere optische Verfahren benötigen hingegen eine größere Nähe zur erfassten Person als Gesichtserkennung. Eine Form der Authentifizierung basiert auf den Eigenschaften des Nagelbettes und soll – so die Autoren – als

---

[204] Siehe z. B. https://www.facewatch.co.uk/, aufgerufen am 14.11.2020.

[205] *Synek*, Gait recognition tech can identify people even with their backs turned, 07.11.2018, https://www.techspot.com/news/77298-gait-recognition-tech-can-identify-people-even-their.html.

ein vollständig automatisierter und einheitlicher Ansatz basierend auf Oberflächenbildern eingesetzt werden können. Die Keratin-Schicht im Nagelbett bricht das Licht ca. doppelt so stark wie das umgebende Gewebe. Mittels der Interferometer-Technik wird versucht, die Phasenänderung des zurückgeworfenen Lichtes zu ermitteln und entsprechend der Amplituden in einen eindimensionalen „Barcode" umgewandelt werden.[206]

Um möglichst hohe Sicherheit der Authentifizierung zu erreichen, wird vor allem an nur schwer oder gar nicht veränderbaren Merkmalen gesucht. Eines davon sind die Muster der unter der Haut verlaufenden Venen. Venenmuster hängen von inneren biologischen Informationen ab und können daher nicht leicht beschädigt, verändert oder verfälscht werden. Sie sind idR von außen nicht „sichtbar" und daher auch weniger leicht „zugänglich". Hier stellen vor allem Cyber-Attacken auf Server mit den entsprechenden Daten ein Sicherheitsrisiko dar.[207] Ein aktuelles Beispiel aus einem begrenzten Projekt, das aber einen Ausblick auf mögliche weitere Verbreitung unter Konsument*innen gibt, ist das Zahlungssystem der Firma Nets in Dänemark. Studenten und Besucher der Copenhagen Business School können mittels Fingervenen in der Cafeteria bezahlen. Dazu muss man im Besitz einer „Dankort" (das dänische Inlandskartensystem) sein, und seinen Fingervenenscan im Zuge der Registrierung mit dem Konto verknüpfen [208]

4.3 AKUSTISCHE PERSONENERFASSUNG

Die akustische Personenerfassung hat ihre weiteste Verbreitung sicherlich in den Sprachassistenten wie Siri, Alexa oder Google Assistant. Dort werden Spracheingaben als zentrales Medium genutzt und gleichzeitig Knowhow zum Thema Spracherkennung aufgebaut, optimiert und unter anderem auch zur Authentifizierung eingesetzt[209]

Sprache und Stimme haben unterschiedlichste Ausprägungen, sodass Sprach- bzw. Sprachmustererkennung auch in anderen Bereichen eingesetzt werden kann. Eine Bank in UK verwendet „Voice-ID" als verhaltensbiometrisches Authentifizierungs-Verfahren. Anstelle eines Passwortes wird dabei Stimmerkennung zur Authentifizierung eingesetzt. Die Technologie ermöglicht es den Kund*innen mit ihrer Stimme als Passwort auf Bankkonten zuzugreifen. Der Satz „My voice is my password" wird dabei gesprochen und stellt das „Passwort" dar. Die Differenzierung erfolgt nach Charakteristika der Stimme (Betonung, physikalische Eigen-

[206] *Kumar et al*, 2014.

[207] *Wua et al.*, 2013.

[208] *The_Paypers*, 2018.

[209] Siehe dazu *Schaber et al.*, 2019.

schaften, Sprechgeschwindigkeit etc.). Voice-ID wird derzeit von 1,6 Millionen Konsumenten in Großbritannien verwendet.[210]

Auch im Bereich der Smartphones soll demnächst Authentifizierungen über Spracherkennung möglich werden. Eine der Anwendungen ist die Demo-App Verint VoiceVault ViGo 2. Zur Authentifizierung müssen entweder Phrasen (z. B. „VoiceVault knows me by my voice") oder Ziffernfolgen ausgesprochen als bzw. Verifizierung verwendet werden. Die App ist bei Google Play erhältlich.[211]

Herkömmliche Authentifizierungen die Stimmbiometrie nutzen sind allerdings anfällig für Spoofing durch Replay-Angriffe. Um die Sicherheit anzuheben experimentiert VoiceGesture mit adaptierten Smartphones, die als Doppler-Sonargerät (liveness detection system) genutzt werden. Dabei wird durch die Lautsprecherboxen des Smartphones ein hochfrequenter Ton ausgesendet und die Frequenzverschiebungen in der Stimme des Benutzers beim Sprechen erfasst. Die entstehenden Doppler-Verschiebungen werden dann zur Live-Benutzererkennung analysiert. Diese Verschiebungen sind für jede Person einzigartig, so dass VoiceGesture diese Kennungen mit der ursprünglichen Stimmprobe des Benutzers vergleichen und so seine Identität bestätigen kann. Ein Vorteil dieser Anwendung liegt darin, dass weder besondere Aktivitäten noch zusätzliche Hardware benötigt werden, sondern nur Lautsprecher und Mikrofon, mit welchen Smartphones bereits ausgestattet sind. Das Projekt wird an der Florida State University in Tallahasse durchgeführt.[212]

Die neue Concept-i Automobilserie von Toyota soll durch KI-Systeme und Anwendung von Biometrie die Emotionen des Fahrers durch die Analyse des Gesichtsausdruckes und des Tonfalles erkennen. So soll auch, wenn das System (der A.I. Agent Yui) erkennt, dass der Fahrer gestresst ist, in den autonomen Fahrbetrieb umschalten („Mobility Teammate Concept"). Alternativ sollen auch Seh-, Tastsinn und Geruchssinn des Fahrers stimuliert werden können, um den Fahrer in einen Alarmzustand zu versetzten, falls das System Zeichen von verringerter Wachsamkeit registriert. So soll dann durch Gerüche etc. der Stresspegel erhöht werden, aber auch vice versa erniedrigt werden können. Zudem ist das System so designt, dass es auch eine Reihe an Daten der Social Media Plattformen zurückgreifen kann, sowie auf deren Aktivität und Gesprächsinhalte, um die Präferenzen des Users zu erkennen.[213] Des weiteren hat Toyota angekündigt, wie einige andere Hersteller aus dem automotive Bereich, eine Partnerschaft mit Microsoft eingegangen zu sein.[214]

---

210 *Price* 2019.

211 *Verint* 2020.

212 *Zhang et al.* 2017; *Owano* 2017.

213 *Cheng,* 2017.

214 *Dudley*, 2016, aufgerufen am 28.9.2020.

4.4 WEITERE MERKMALE ZUR PERSONENERFASSUNG

Neben den bekannten biometrischen Merkmalen wie Fingerabdruck, Gesichtsform oder Stimme werden in der Literatur auch laufend weitere Merkmale zur biometrischen Zugangskontrolle vorgeschlagen. Ein wesentlicher Faktor sind hier neue Gerätekategorien.

Für smarte Brillen mit integriertem Lautsprecher und Mikrophon wurde beispielsweise eine Messung der charakteristischen Ausbreitung von Schallwellen im Kopf (Knochenschallleitung) vorgeschlagen.[215] Diese ist abhängig von der exakten Form der Schädelknochen der erfassten Person und somit grundsätzlich als biometrisches Merkmal geeignet.

Die Erfassung der biometrischen Merkmale kann zu einem bestimmten Zeitpunkt (diskrete Erfassung) oder aber kontinuierlich durchgeführt werden. Für die Zugangskontrolle werden heute vorwiegend Systeme zur diskreten Erfassung verwendet. Solche Systeme bauen üblicherweise auf spezialisierten biometrischen Sensoren auf und fordern Konsument*innen explizit zur Präsentation ihrer biometrischen Merkmale auf. Für Konsument*innen sind sie daher meist eindeutig erkennbar, dass eine biometrische Analyse durchgeführt wird.

kontinuierliche Erfassung

Bei der kontinuierlichen Erfassung werden Benutzer*innen häufig anhand von Verhaltensmerkmalen anstatt von biologischen Merkmalen identifiziert. Eine beliebte Plattform sind Smartphones, ermöglichen sie doch die kontinuierliche Erfassung des Verhaltens von Konsument*innen mittels einer Vielzahl von Sensoren. So wurde in der Literatur eine Erfassung des charakteristischen Gangs einer Person mittels Beschleunigungssensoren oder des charakteristischen Nutzungsverhaltens auf Touchscreens vorgeschlagen.[216] In der Praxis haben diese Systeme noch keine weitere Verbreitung gefunden, was u. A. mit ihrer hohen Falscherkennungsrate (false positive/negativ) zusammenhängt.[217]

Neben den oben bereits ausführlich beschrieben Merkmalen gibt es noch weitere Anwendungen, die meist eher ausgefallene biometrischer Parameter in den Fokus nehmen. Viele davon befinden sich noch in Entwicklung oder haben es bisher nicht zum Durchbruch geschafft. Diese zeigen jedenfalls die großen Anstrengungen in Forschung und Entwicklung die

---

215 *Carman*, Researchers are using the vibration of your skull to identify you, 25.04.2016, https://www.theverge.com/2016/4/25/11501704/skullconduct-biometric-password-authentication.

216 *Stylios et al*, A Review of Continuous Authentication Using Behavioral Biometrics, Proceedings of the South East European Design Automation, Computer Engineering, Computer Networks and Social Media Conference on – SEEDA-CECNSM '16, 2016. S 6.

217 Ebenda S 6.

Individualität der Menschen in unterschiedlichster Weise maschinell verarbeitbar zu machen.

innere biometrische Merkmale

Während externe Körperteile wie das Gesicht, Fingerabdrücke oder die Netzhaut häufig für die biometrische Identifizierung verwendet werden, kann auch davon ausgegangen werden, dass innere Organe, die mit biomedizinischen Bildgebungsgeräten abgebildet werden, ebenfalls eine biometrische Identifizierung ermöglichen können. Eine Studie etwa untersuchte MRT-Bildern zum Zweck der biometrischen Identifizierung und konnte zeigen, dass die Genauigkeit der Personenidentifizierung mit Hilfe von Knie-MRTs signifikant höher ist als rein nach dem Zufallsprinzip. Da die MRT zur Abbildung innerer Körperteile verwendet wird, kann dieser Ansatz der biometrischen Identifizierung potenziell eine hohe Täuschungsresistenz bieten. Jene Methode könnte verwendet werden, um Personen in einer sich bewegenden Schlange schnell zu registrieren und zu identifizieren, wenn sie sich z. B. der Passkontrolle auf Flughäfen nähern oder durch den Eingang eines Bürogebäudes gehen.[218] Einen Überblick über aktuelle Entwicklungen zeigt Thomas,[219] dabei wird deutlich, dass zunehmend aufdringliche, um nicht zu sagen eindringliche, Methoden angewandt werden. Geforscht wird derzeit an Laser zur Erkennung von Herzschlag und Mikrobiom, individuellen Bewegungen zur Überwachung von Verhaltensmustern, Geruch (Geruchsbiometrie) usw.

kontinuierliche Gangerkennung

Einen neuen Weg beschreitet hier ein System, das noch in Entwicklung ist aber bereits am Smartphone vorhandene Technik nutzt, um die Benutzer anhand ihres Ganges kontinuierlich zu authentifizieren und so sicherzustellen, dass das Gerät vom richtigen Besitzer getragen wird. Sobald die Authentifizierung erfolgreich war, bleibt sie kontinuierlich aktiv, war das Ergebnis negativ, wird eine vorherbestimmte E-Mail adressiert, die den rechtmäßigen Besitzer über den Verbleib des Smartphones informiert[220]

tragbare Sensoren

Im allgemeinen Gebrauch am weitesten verbreitete, tragbare Sensoren sind Smartphones, Fitnessarmbänder und Smart Watches, die z. B. Puls, EKG und Blutsauerstoff sowie Schlafrhythmen aufzeichnen können. Durch die gleichzeitige Aufzeichnung von Bewegungsprofilen über eingebaute GPS-Sensoren ergibt sich nicht nur ein umfassendes Bild des Verhaltens der Menschen (wo wohnen und schlafen sie, wo arbeiten sie, wo kaufen sie ein, etc.?). Die biologischen Parameter geben darüber hinaus Auskunft über Fragen wie: wie oft und wie schnell gehen die Menschen, wie lange liegen sie am Sofa, welche Anstrengungen bedeuten Stufen, wie bewegt oder ruhig ist ihr Schlaf? Aus all diesen Daten kann auf den Gesundheitszustand oder Stresslevel geschlossen werden. Wenn dazu Daten aus dem Zahlungsverkehr und der Warenwirtschaft kommen, kann man nicht nur einschätzen was der Mensch isst, sondern sehr genau auch welcher Typ Mensch er oder sie ist.

---

218 *Inderscience Publishers*, 2013.

219 *Thomas*, 2019.

220 *Fadelli* 2019; *Mufandaidza et al,* 2018, aufgerufen am 26.9.2020.

unbewusste Datenanalyse

Viele dieser Daten werden von den Anwender*innen freiwillig aufgezeichnet, ohne sich der weiteren Bedeutung bewusst zu sein. Zweck ist oft eine effizientere Trainingsgestaltung im Hobbysport, allgemein gefordertes Körperbewusstsein und Vorsorgedenken oder die Unterstützung bei diätetischen Vorhaben. Diese singulären Zwecke werden aber oft über Apps realisiert, die die Daten nicht lokal am jeweiligen Endgerät erheben, verarbeiten und dort belassen, sondern oft auch auf Servern der Anbieter von Plattformen und dazugehöriger Communities speichern. Damit werden die Daten potentiell – abhängig von den AGBs und Einstellungen der Plattformen sowie vor allem auch den Privatheitseinstellungen der Anwender*innen – weltweit zugänglich und damit begehrtes Handelsgut. Hier kommt wieder das Ungleichgewicht im Wissen und den Möglichkeiten der Datenanalyse ins Spiel: während der/die Anwender*in vor allem den konkreten Wert z. B. Puls beim letzten Lauf oder Gewichtsabnahme der letzten Woche im Blick hat, kann ein*e professionelle*r Nutzer*in der Daten mit medizinischem und statistischem Wissen Langzeitanalysen durchführen, die unterschiedlichen Daten zueinander in Beziehung setzen und so versuchen, Aussagen über den aktuellen Gesundheitszustand des/der Anwender*in und sogar über deren zukünftige Entwicklung zu treffen. Wer beim Sport seinen Puls misst, muss sich nicht unbedingt der Bedeutung dessen bewusst sein, dass er/sie damit langfristig auch ein eindeutiges Muster zur Identifizierung liefert.

Wearables

Am weitesten gehend sind sogenannte Wearables, die eine Vielzahl an Sensoren in Wäsche integrieren und so die Messung für die Anwender*innen sehr bequem machen. So ist z. B. die kommerzielle Einführung eines waschbaren smarten T-Shirts angekündigt, womit sechs physiologische biometrische Schlüsselparameter überwacht werden sollen, um Prävention, Risikominderung und Fernüberwachung zu ermöglichen. Die Plattform Nexkin™ verwendet dabei 10 biometrische Scanner in einem maschinenwaschbaren T-Shirt. Dieses ist in der Lage, das EKG, die Bauch- und Brustatmung, die Körpertemperatur, die körperliche Aktivität und die Lungenimpedanz eines Benutzers kontinuierlich aufzuzeichnen. Die Daten werden vom T-Shirt über Bluetooth an das Smartphone des Benutzers übertragen, wo Daten von mehreren Sensoren mit Hilfe von Algorithmen integriert werden können, um genaue und umsetzbare Informationen zum Gesundheitszustand zu liefern, die anschließend heruntergeladen oder auf Server übertragen werden können, damit sie von medizinischem Fachpersonal überprüft werden können.[221]

medizinische Diagnose

Ebenfalls zur Anwendung für fachliches Personal aber auch für Angehörige ist jene Anwendung bei der versucht wird aufgrund biometrischer Daten auf den Zustand von Menschen mit Autismus zu schließen und so bei Bedarf vorsorglich bzw. zeitgerecht beruhigend auf sie einwirken zu können. Im Autism Together Raby Hall-Pflegeheim in Wirral wird derzeit eine Methode getestet, bei der mit Hilfe von Armbandsensoren für Hauttempe-

[221] *Chronolife* 2019, aufgerufen am 26.09.2020.

ratur, Schweiß, Herzfrequenz und Gliedmaßenbewegungen Anzeichen von Angst erkannt werden sollen und so Pfleger, Ärzte, Angehörige etc. informiert werden können, sodass diese entsprechend reagieren können. Dies soll unter anderem helfen, unnötige Medikamentationen zu verhindern und auch Autisten unterstützen, die sich nicht verbal mitteilen können. Das Armband erkennt einen „aggressiven" Vorfall anhand physiologischer Parameter und soll dies 60 Sekunden vor dem prognostizierten Vorfall ankündigen. Es gibt damit den Angehörigen, Ärzten etc. gerade genug Zeit die Person zu beruhigen und für alle das Sicherheitsrisiko zu verringern. Biometrische Technologien könnten so die Pflege für Autisten verbessern.[222]

[222] *Yecla* 2019; *Bush* 2018 zuletzt aufgerufen 26.9.2020.

5 GESELLSCHAFTLICHE AUSWIRKUNGEN

Biometrie ist verlockend, weil es auf den ersten Blick wie eine verlässliche Technologie klingt, die erhöhte Eindeutigkeit und höhere Sicherheit verspricht. Doch wie realistisch ist dieses Versprechen? Biometrie ist keine neue Technologie, aber neuartig ist ihr wachsender Einsatz in Alltagstechnologien und kommerziellen Anwendungen. Dadurch verändern sich die gesellschaftlichen Effekte.

potenzielle Nutzbarkeitsvorteile aber marginale Sicherheitsgewinne

Biometrie kann in bestimmten Anwendungskontexten durchaus nützlich sein, um Identifizierungs- und Authentifizierungsverfahren mit einer zusätzlichen Sicherheitskomponente auszustatten. Ein wesentlicher Grund liegt in der potenziell einfacheren Nutzbarkeit im Vergleich zu Verfahren die primär auf den Faktoren Wissen und oder Besitz von Nutzer*innen basieren (wie typischerweise Passwörter oder PINs). Biometrische Merkmale sind substantielle Identitätsinformation,[223] daher untrennbar mit einer Person verbunden und ermöglichen den zusätzlichen Faktor der „Inhärenz" (siehe auch Abschnitt 2). Biometrie erfordert (zumindest in der Theorie) die physische Anwesenheit jener Person, die über ihre biometrischen Merkmale einen Vorgang auslöst. Typisches Beispiel sind Zugangskontrollen: Ein Eingabegerät erfasst etwa das Gesicht der Person und gewährt Zutritt, sowohl physisch als auch virtuell. Bei letzterem dient häufig das Smartphone als Eingabegerät. Klassische Verfahren mit Passwort benötigen dagegen keinerlei Präsenz. Daher wird häufig argumentiert, Biometrie vereinfache Identifizierungs- und Authentifizierungsverfahren grundsätzlich und erhöhe die Sicherheit. Dieses Argument ist aber in mehrfacher Hinsicht unzutreffend. Verfahren mit Biometrie können sinnvoll sein, wenn sie in sicherer Umgebung und in einem klar definierten, geschützten Anwendungskontext eingesetzt werden.[224] D. h. wenn die Risiken von Datenmissbrauch sehr gering sind, der Lebenszyklus der Daten kurz ist, die Daten weder zentral verarbeitet noch gespeichert werden und die biometrischen Daten oder die Funktionalität, die sie ermöglichen (z. B. Systemzugang), nicht ohne weiteres technisch replizierbar sind.

In der Praxis bestehen allerdings zahlreiche Angriffsvarianten[225] (vgl. auch Abschnitt 2) auf biometrische Verfahren und es gibt erhebliche Missbrauchsrisiken. Ein Beispiel für einen solchen Missbrauch ist das Kopieren biometrischer Information: Etwa durch simples Erfassen eines Fingerabdrucks

---

223 *Strauß*, 2019, 241ff.

224 *Schneier*, 1999; Clarke, 2001.

225 Vgl. u. a. Adler/Schuckers, 2009; Bolle et al. 2013; Hadid et al. 2015; Ramachandra/Busch, 2017, Dong et al. 2020.

mittels Klebestreifen oder noch einfacher mittels eines Fotos eines Fingerabdrucks von einem Glas, wie von Sicherheitsforschern demonstriert. Dadurch kann ein synthetischer Abdruck erzeugt werden, der dann missbräuchlichen Zugang ermöglicht, ohne den ursprünglichen Fingerabdruck zu benötigen.[226] Herkömmliche Digitalkameras sind sogar ausreichend, um komplexere biometrische Verfahren wie Iris-Scans zu überlisten.[227] Darüber hinaus lässt sich auch gänzlich ohne physische Präsenz biometrische Information erfassen. Gesichtserkennung ist hier besonders anfällig, weil Gesichtsbilder millionenfach ungeschützt im Internet auffindbar sind. Daraus können gänzlich aus Distanz biometrische Daten von Personen generiert und missbraucht werden. Etwa ist die Sperre eines Smartphons bei aktiviertem Login per Gesichtserkennung leicht mittels Gesichtsbild umgehbar.[228] Weitere Möglichkeiten bestehen durch Kopieren eindeutiger Hashwerte der biometrischen Merkmale. Etwa durch Eindringen in biometrische Datenbanken, um die entsprechenden Informationen zu entwenden. Solche Fälle nehmen seit einigen Jahren zu, wie diverse Hacks großer biometrischer Datenbanken im staatlichen wie im privaten Bereich zeigen (näheres siehe unten).

Es gibt also vielfältige Möglichkeiten, Biometrie zu missbrauchen, um die Identität einer Person vorzutäuschen. Selbst die physische Präsenz der betroffenen Person ist daher auch kein Garant für ein sicheres Verfahren. Schon aufgrund der Vielzahl an Angriffsformen sind die Anforderungen für einen sicheren Biometrieeinsatz grundsätzlich nicht trivial und sehr hoch. Hinzu kommt, dass sich Biometrie grundsätzlich nicht als Ersatz für Zugangsdaten wie Passwörter oder PINs eignet. Der Grund ist naheliegend: Zugangsdaten wie Passwörter, PINs etc. basieren auf dem Prinzip „Wissen um ein Geheimnis" zwischen Nutzer*in und System. D. h. ohne diese geheime Information erfolgt kein Zugang. Dieses Prinzip erfüllen biometrische Daten grundsätzlich nicht, weil sie eindeutig an den Körper einer Person gebunden sind und dieser physische Spuren (und je nach technischer Lösung auch digitale) hinterlässt, die replizierbar sind (das gilt insbesondere für das Gesicht oder auch Fingerabdrücke). Die Idee, biometrische Daten in der Analogie eines Schlüssels zu verwenden ist daher irreführend und bringt keinerlei Sicherheitsgewinn.[229] Biometrische Daten eignen sich daher eher für Anwendungsbereiche, wo eindeutige Identifizierung einer Person in ihrer physischen Präsenz tatsächlich notwendig ist. Ein Beispiel hierfür sind Lichtbilder und andere biometrische Merkmale im Reisepass. Für internationale Reisefreiheit und die damit verbundenen Zwecke der nationalen Sicherheit und polizeilicher Fahndung haben diese Daten einen zusätzlichen Nutzen. Für den alleinigen Zweck der Reisefreiheit sind zumindest theoretisch keine biometrischen Merk-

[226] Arthur, 2013.

[227] *Krempl, 2014.*

[228] Vgl *Foltýn*, 2019.

[229] Vgl. u .a. *Schneier* 1999.

male auf einem behördlich genehmigten Reisedokument nötig. Allerdings sind sie in der Praxis aufgrund der raschen Abgleichsmöglichkeit (insbes. zwischen Gesicht und Lichtbild) seit langem etabliert. Ein damit verbundener Vorteil ist jener der Nichtabstreitbarkeit der Identität. Diese Vorteile gelten aber primär für jene Akteure, die biometrische Daten verarbeiten bzw. Biometrie in ihren Anwendungen integrieren.

Aus Sicht der betroffenen Person, deren biometrische Daten verarbeitet werden, kann Biometrie zwar Convenience-Vorteile durch potenziell einfachere (intuitivere) Nutzung bringen, aber Sicherheitsgewinne gibt es für Betroffene/Endanwender*innen kaum. Sicherheitsgewinne betreffen eher Betreiber von Anwendungen, die die Biometrie als zusätzlichen zweiten oder dritten Authentifikationsfaktor einsetzen in Kombination mit PIN odgl. Dadurch relativiert sich aber auch der Convenience-Vorteil für Nutzer*innen wieder, weil hier noch ein zusätzlicher Faktor berücksichtigt werden muss und Anwendungen dann statt Username und Passwort zusätzlich noch ein biometrisches Merkmal erfassen.

Bei Anwendungen, die Biometrie tatsächlich als Ersatz für andere Verfahren einsetzen, ist äußerste Vorsicht geboten, denn hier kann das Sicherheitsniveau sogar erheblich abnehmen – sowohl für Nutzer*innen als auch für Anwendungsbetreiber. Für Angreifer verringert sich der zu betreibende Aufwand enorm, weil anstatt einer grundsätzlich beliebig änderbaren Information (z. B. Passwort) nur noch Kenntnis über personenspezifische, quasi-unwiderrufbare Information erlangt werden muss. Diese Information öffnet dann buchstäblich alle Türen. Mit wachsender Anzahl an Anwendungen mit Biometrie gilt das umso mehr. …

Ein wesentlicher Grund für den Zuwachs an Angriffen auf biometrische Systeme wie Diebstahl biometrischer Daten liegt am hohen Missbrauchspotenzial bei vergleichsweise geringem Aufwand. Aus Sicht eines Angreifers bietet der Diebstahl biometrischer Daten vielfältige Möglichkeiten für Identitätsdiebstahl und wird mit zunehmender Verbreitung von Biometrie immer lukrativer. Dadurch nehmen längerfristig auch potenzielle Sicherheitsvorteile gesamtgesellschaftlich gesehen sogar ab.

Kommerzialisierung biometrischer Daten als wachsendes Problem

Die Anwendungen für Biometrie waren lange Zeit auf Bereiche mit spezifischen Sicherheitsanforderungen begrenzt (militärischer Bereich, Zugangskontrollen für Sicherheitsschleusen in sensiblen Unternehmensbereichen mit erhöhen Sicherheitsanforderungen usw.). Seit einigen Jahren kam es jedoch zu einer erheblichen Verbreiterung in den Anwendungsfeldern. Es ist hier ein Wandel von einer ursprünglichen Sicherheitstechnologie mit spezifischen Anwendungen hin zu einer Convenience-Technologie mit breitem Anwendungsspektrum zu beobachten. Diese Entwicklung ist vor allem auf technische Ausstattung und hohen Verbreitungsgrad von Smartphones zurückzuführen. Fingerprintsensoren und Gesichtserkennung gehören mittlerweile zur Standardausstattung herkömmlicher Geräte. D. h. einerseits können die Geräte selbst biometrische Daten erfassen und verarbeiten, wenn diese z. B. zur Entsperrung genutzt werden. Zudem gibt es immer mehr Apps, die Biometrie zur Identifizierung und Authentifi-

zierung von Nutzer*innen einsetzen. Das gilt immer mehr auch für kommerzielle Anwendungen, insbesondere im Bankensektor und bei Bezahlvorgängen (siehe Abschnitt 4.1.1). Vor einigen Jahren haben Banken und Zahlungsdienstleister weltweit begonnen, biometrische Verfahren in ihre Anwendungen zu integrieren. Im asiatischen Raum sind solche Anwendungen schon lange etabliert und US-amerikanische Dienstleister wie z. B. Mastercard oder Visa sind seit längerem diesbezüglich aktiv. Auch in Europa ist ein Zuwachs an biometrischen Verfahren zu beobachten. Die Unicredit-Gruppe hat bereits seit 2013 Anwendungen mit Authentifikation via Palm-Scan[230] und Kreditkartenfirmen wie z. B. Mastercard bieten seit 2016 u. a. Bezahlvorgänge mittels Gesichtserkennung („Pay-by-Selfie") auch in Europa an.[231]

Diese Entwicklung wurde auch politisch auf europäischer Ebene begünstigt. Die seit 2016 geltende eIDAS-Verordnung der Europäischen Union hat den Weg für elektronische Identifizierung im digitalen Binnenmarkt weiter geebnet.[232] Ein Ziel ist dabei die Interoperabilität unterschiedlicher Identifizierungssysteme und grenzüberschreitende Abwicklung von Verwaltungs- und Zahlungsdienstleistungen. In Ergänzung zu der überarbeiteten europäischen Zahlungsdiensterichtlinie (PSD2 – Payment Services Directive 2) sollte damit auch der Online-Handel einfacher und sicherer gemacht werden. Um den seit September 2019 geltenden Anforderungen gerecht zu werden, setzen einige Unternehmen verstärkt auf Biometrie, wenngleich keine explizite Notwendigkeit dazu besteht. Seit September 2019 gelten durch die PSD2 höhere Sicherheitsanforderungen bei Bezahlvorgängen. D. h. die Identität einer Person muss seit dem mit zwei von drei Sicherheitsfaktoren überprüft werden (Wissen, Besitz oder Inhärenz wie eben biometrische Merkmale).[233] Konsument*innen sind seither mit veränderten Authentifizierungsvorgängen mittels 2. Faktor konfrontiert wie etwa beim Online-Banking oder spezifischen Apps, die biometrische Daten verarbeiten. Die beiden Hauptformen sind hier Fingerabdruck und Gesichtsbiometrie, die auch in Österreich häufig zum Einsatz kommen. Zudem sind weitere Anwendungen angedacht. Zum Beispiel ist mit der Novelle des E-Government-Gesetzes geplant, nun auch biometrische Daten zur Identifikation heranzuziehen. Der Fokus liegt dabei auf der Erweiterung der bisherigen Bürgerkartenumgebung zu einer E-ID-Lösung mittels Smartphone-App. Unter anderem kritisiert der Datenschutzrat in seiner Stellungnahme Teile der Regierungsvorlage als zu weitreichend und unpräzise. Es müsse jedenfalls auch weiterhin Wahlfreiheit bei der Art der Identifikation für

---

230 *Sayer*, 2013.

231 *Leyden*, 2016.

232 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, OJ L 257, 28.8.2014, 73-114.

233 https://www.oesterreich.gv.at/themen/steuern_und_finanzen/bankgeschaefte/Seite.750111.html, aufgerufen am 24.11.2020.

Betroffene bestehen und es dürfe keinen Zwang zur Erfassung biometrischer Daten geben.[234] D. h. für Konsument*innen sind biometrie-freie Alternativen bereitzustellen.

Im Entwurf ist zudem vorgesehen, dass auch Dritte das E-ID-System nutzen können. Der DSR fordert hier eine Eingrenzung und Klärung darüber, „welchen ‚Dritten' unter welchen Auflagen und Voraussetzungen zu welchem konkreten Zweck die Nutzung des E-ID-Systems eröffnet (bzw. ermöglicht) werden kann" sowie präzise Kriterien für die Zuverlässigkeitsprüfung Dritter.[235]

Risiko externer Zugriffe auf biometrische Daten

Die Erweiterung des Anwendungsspektrums biometrischer Daten ist mit einigen Risiken verbunden. Insbesondere durch Zugriffe externer Dritter. Selbst wenn die Verarbeitung biometrischer Daten lediglich lokal auf einem Gerät wie etwa einem Smartphone oder einem PC stattfindet, ist nicht auszuschließen, dass auch externe Dienste auf biometrische Daten zugreifen. Es gibt einige Belege und Indizien dafür, dass etwa externe Programmierschnittstellen (APIs) solche Zugriffe ermöglichen.[236] Das hat zur Folge, dass etwa auch bei rein lokaler Verarbeitung eines Fingerprints oder des Gesichts diese Daten über den Umweg externer Dienste von Dritten verarbeitet werden. Ein wesentlicher Teilaspekt ist hierbei die hohe Abhängigkeit zu Unternehmen außerhalb der europäischen Union und damit auch außerhalb europäischer Datenschutz- und Sicherheitsstandards. So ist etwa die Entwicklung von Smartphone-Apps ohne Einbindung externer APIs (etwa von Google/Android, Apple etc.) kaum möglich. Der Verwendungszweck und die rechtskonforme, nicht missbräuchliche Verwendung der Daten sind damit noch schwerer kontrollierbar. Zum einen verschärft sich dadurch das Problem der Zweckentfremdung, wodurch die Privatsphäre noch weiter bedroht wird. Zum anderen auch das Problem der erhöhten Angriffsfläche auf biometrische Daten. Das Angriffspotenzial steigt mit der Anzahl an Anwendungen mit Biometrie. Die Zunahme an Angriffen auf biometrische Datenbanken verdeutlicht dieses Problem. Aus einem Gesichtserkennungssystem des US-Department of Homeland Security wurden ca. 184.000 Datensätze gestohlen und im Darknet angeboten. Unter den Daten sind u. a. Gesichtsbilder von Reisenden und Scans von Kfz-Kennzeichen.[237] Solche Fälle gibt es immer wieder und sie nehmen zu: Im Jahr 2019 stellten Sicherheitsforscher fest, dass die Datenbank eines weltweit verbreiteten biometrischen Zugangssystems für Ge-

---

234 Stellungnahme des Datenschutzrats zu dem Ministerialentwurf betreffend Bundesgesetz, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden, https://www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_17654/imfname_839271.pdf, abgerufen am 24.11.2020.

235 DSR, S. 5.

236 Vgl. u. a. https://www.infosecurity-magazine.com/news-features/apis-risks-potential-solutions/, https://android-developers.googleblog.com/2019/10/one-biometric-api-over-all-android.html, https://developer.visa.com/capabilities/biometrics, aufgerufen am 24.11.2020.

237 *Krempl*, 25.09.2020.

bäudesicherheit (Biostar 2) mit fast 28 Millionen Einträgen offen zugänglich war. Die Daten enthalten u. a. Fingerabdrücke, Gesichtsbilder und Zugangsdaten wie Passwörter.[238] Anfang 2020: Ungeschützter Zugang zu einer Biometriedatenbank mit über 2 Millioneneinträgen in Brasilien mit rund 76.000 betroffenen Datensätzen von Fingerabdrücken.[239] Die biometrische Datenbank des israelischen Innenministeriums mit mehreren Millionen Einträgen wurde in den letzten Jahren bereits mehrfach gehackt.[240] Das weltweit größte Biometriesystem in Indien, Aadhaar, das über eine Milliarde Einträge hat, wurde ebenfalls bereits mehrfach angegriffen und manche Daten wurden sogar per Whatsapp für 10 US-Dollar angeboten.[241] Diese Beispiele sind keineswegs nur Einzelfälle und verdeutlichen, wie der Ausbau von Biometrie die Gefahr von Datenmissbrauch und Identitätsdiebstahl sogar noch erhöhen kann.

Habituation und Gewöhnungseffekte

Mit steigender Verbreitung von Biometrie in kommerziellen Anwendungen im Alltag gehen Gewöhnungseffekte einher. Personen werden einerseits durch regelmäßige Konfrontation mit der Technologie in Alltagssituationen (Smartphones, Bezahlvorgänge usw.) daran gewöhnt, anhand biometrischer Merkmale identifiziert zu werden. Das kann einen kritischen Umgang mit der Technologie oder auch bewusste Entscheidungen einzelner Personen zur Nicht-Nutzung erschweren, weil der damit verbundene Aufwand mit wachsender Verbreitung der Technologie zunimmt, während zugleich der Aufwand für die Nutzung abnimmt. Dadurch verringert sich auch die Wirksamkeit das datenschutzrechtlichen Schutzkonzepts der aktiven, informierten Zustimmung („informed consent").[242] Die grundsätzliche Wahlfreiheit Betroffener, der Verarbeitung ihrer Daten zuzustimmen oder die Verarbeitung zu untersagen, wird untergraben, wenn biometrische Anwendungen zum Status Quo werden, ohne dass gleichwertige Alternativen bestehen. Das ist besonders problematisch, wenn eine bewusste Nichtnutzung einer biometrischen Anwendung negative Folgen für Betroffene hat wie z. B. kein Zugang zu bestimmten Leistungen. Die vermeintliche Einfachheit biometrischer Personenerfassung kann zudem die Gefahren von Function und Mission Creep – also schleichende Erweiterung der Verwendungszwecke – weiter begünstigen. Damit geht das Risiko einher, dass die de jure höheren Schutzstandards (biometrische Merkmale sind sensible, besonders schutzwürdige Daten) schrittweise ausgehöhlt werden.

Unabstreitbarkeit und fehlerhafte Identifizierung als neue Risiken

Im technischen Sinn ist Biometrie u. a. definiert als „automatisierte Erkennung von Personen basierend auf ihren spezifischen verhaltensbezogenen und biologischen Merkmalen".[243] Entgegen der gängigen Meinung sind

---

238 *Porter*, 2019.

239 *Hautala*, 2020.

240 *Goichman*, 2020.

241 *Malhotra*, 2018.

242 Vgl *Strauß*, 2019, 198ff.

243 *ISO*, 2006.

biometrische Verfahren weder fehlerfrei noch zwingend eindeutig. Biometrie ist eine Form von Mustererkennung, bei der die Wahrscheinlichkeit, dass ein bestimmtes Muster in biometrischer Information (z. B. Fingerprint) gültig ist, als Basiskriterium für einen bestimmten Vorgang (idR. Authentifizierung oder Identifizierung) dient[244]. Auch biometrische Verfahren sind daher kein Schutz vor fehlerhafter Identifikation udgl. (siehe auch Abschnitt 2). Zahlreiche Studien zeigen erhebliche Risiken für Sicherheit und Privatsphäre durch Biometrie.[245]

Problematisch ist das insbesondere für Betroffene, weil biometrische Merkmale und damit auch Verfahren als eindeutiger gelten. Datenschutzrechtlich dürfte hier das Recht Betroffener auf Richtigstellung beeinträchtigt sein, weil die Richtigstellung fehlerhafter biometrischer Verfahren für Betroffene schwerer sein dürfte. Der vermeintliche Vorteil aus Anwendungssicht – die Unbestreitbarkeit der Identität – kann für Betroffene daher auch schnell zum Nachteil werden. Die negativen Konsequenzen durch technische Fehler können für Betroffene dementsprechend gravierend sein. Etwa durch „Verwechslung" aufgrund fehlerhafter Identifizierung und Klassifizierung als vermeintliche Straftäter. Ein solcher Fall ist u. a. 2017 im britischen Wales bei einem Champions-League Spiel passiert. Ein „smartes" Überwachungssystem hat mittels Gesichtserkennung über 2.000 Menschen fälschlicherweise als Verdächtige klassifiziert. Das entspricht einer Fehlerrate von 92 Prozent.[246] Ein weiteres Beispiel ist die Stadt Detroit mit einer Fehlerquote von rund 96 Prozent.[247] Das sind aber keineswegs nur Einzelfälle, sondern nur Beispiele von unzähligen Fehlern von Gesichtserkennungstechnologie und dem Problem algorithmischer Diskriminierung (siehe unten). Noch weitaus gravierender als technische Fehler ist daher das Problem des erhöhten Kontrollverlusts über biometrische Daten für Betroffene.

wachsender Kontrollverlust über biometrische Daten

Institutionelle Anbieter und Nutznießer biometrischer Verfahren (insbes. Plattformbetreiber, Unternehmen, Behörden) haben grundsätzlich mehr Kontrolle über die verarbeiteten biometrischen Daten als die Betroffenen. Das gilt für alle Formen personenbezogener Daten. Biometrische Daten erhöhen diese Form von Informationsasymmetrie, die individuelle Identitäten betrifft erheblich.[248]

Schon das Erfassen biometrischer Daten impliziert den Verwendungszweck der Identifikation, weil die Daten untrennbar mit der Identität einer Person verbunden sind. Diese starke Bindung an die Identität erhöht auch das Risikopotenzial für Missbrauch und Verletzungen von Grund- und

244 Wilson, 2010.

245 Vgl. u. a. Clarke 2001; Prabhakar et al. 2003; Lyon 2009; Acquisti et al. 2014; Sharif et al. 2016; Adler/Schuckers, 2009; Bolle et al. 2013; Hadid et al. 2015; Ramachandra/Busch, 2017; Dong et al., 2020.

246 Burgess, 4.5.2018.

247 *Muzayen*, 2020.

248 *Strauß*, 2019, 145ff.

Freiheitsrechten. Permanente Identifizierbarkeit wurde daher insbesondere im richtungsweisenden Volkszählurteil des Deutschen Bundesverfassungsgerichts von 1983[249] als Gefahr für die Demokratie bewertet. Damals sprach sich das Höchstgericht klar gegen die Einführung eines bundesweiten Personenkennzeichens aus, weil es unverhältnismäßige Grundrechtseingriffe mit sich brächte.

Die Verarbeitung biometrischer Daten ist letztlich vergleichbar mit der Problematik des Einsatzes eines einheitlichen Personenkennzeichens über die Grenzen unterschiedlicher Anwendungskontexte hinweg, deren Verwendungszweck für die Betroffenen nicht kontrollierbar ist. Damit ist ein zentrales Datenschutzgebot – die Zweckbindung – verletzt. Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden, und dieser Zweck muss grundrechtlich legitimiert sein. Es ist äußerst fraglich, ob Daten, deren bloße Existenz bereits Identifikationszwecke ermöglicht, wie eben Biometrie, überhaupt dem Gebot der Zweckbindung entsprechen können, weil durch sie personenbezogene Daten aus unterschiedlichen Anwendungsbereichen noch einfacher als bisher verknüpft werden können. Damit verschärft sich auch das Problem des Profilings.

Je mehr biometrische Anwendungen es gibt, desto mehr Verwendungszwecke entstehen. Eine solche Entwicklung ist auch völlig konträr zu wesentlichen Datensicherheitskonzepten, die zur Risikominimierung variierende Zugangsdaten und unterschiedliche Benutzerdaten vorsehen, um Angriffe und Missbrauchspotenzial zu erschweren. Biometrische Daten konterkarieren das schon alleine deshalb, weil sie nicht änderbar sind. Zugangsdaten wie Username, Passwort, lassen sich ändern und können beliebig variiert werden. Ein Fingerprint kann dagegen theoretisch für alle entsprechenden Anwendungen genutzt werden. D. h. ein Angreifer hat geringeren Aufwand bei gleichzeitig höherem Schadenspotenzial.

Die Zunahme an biometrischen Identifikationsverfahren verschärft ein Grundproblem der Digitalisierung noch weiter: „Identifiability-by-Default" bzw. die permanente Identifizierbarkeit von Individuen.[250] Das hat zur Folge, dass die Kontrolle Betroffener über ihre Daten weiter abnimmt und gleichzeitig bestehende Datenschutz- und Sicherheitskonzepte an Wirksamkeit verlieren. Dass diese Gefahren nicht nur theoretischer Natur, sondern durchaus real sind, zeigt u. a. der Skandal um die Firma Clearview AI, die über Jahre hinweg systematisch mehrere Milliarden Gesichtsbilder aus dem Internet sammelte, um ihre mit Gesichtserkennung arbeitende Überwachungstechnologie zu optimieren.[251] Auch Behörden weltweit verarbeiten immer mehr biometrische Daten und nutzen u. a. Gesichtserkennungstechnologien (siehe unten). Es ist allerdings fraglich, ob das mit europäischen Datenschutzstandards vereinbar ist. Der Europäische Datenschutzausschuss warnte ausdrücklich vor dem Einsatz solcher Technolo-

[249] BVerfGE 1 BvR 209/83 (15.12.1983).

[250] *Strauß*, 2019.

[251] Hill (2020).

gien Strafverfolgung. Für Dienste wie jene von Clearview AI gebe in Europa keine Rechtsgrundlage.[252]

Biometrie kann Rassismus und Diskriminierung weiter verschärfen

Das globale Problem von Rassismus und Diskriminierung wird parallel zur steigenden Verbreitung von Biometrie immer deutlicher sichtbar und droht, sich durch den Technologieeinsatz noch weiter zu verschärfen. Das gilt im besonderen Maße für Gesichtserkennung, die nicht nur in den USA seit einigen Jahren für erhebliche Kontroversen sorgt. Die systematische Diskriminierung anhand der Hautfarbe durch Gesichtserkennungstechnologie ist vielfach belegt und ein wachsendes Problem. Einer umfassenden US-Studie zufolge werden etwa Menschen mit asiatischem oder afroamerikanischem Aussehen von gängigen Gesichtserkennungstechnologien bis zu 100mal häufiger falsch identifiziert als Weiße.[253]

Das ist zum einen dem Problem von Bias und inhärenter Diskriminierung in der Technologie selbst geschuldet. Bias in algorithmischen Systemen, Machine Learning Algorithmen etc., wie sie notwendigerweise auch bei Biometrie zum Einsatz kommen, ist vielfach belegt.[254] Gesichtserkennungstechnologien sind diesbezüglich besonders anfällig: trotz technologischem Fortschritt ist mangelnde Genauigkeit nach wie vor ein großes Problem und sie bedrohen die Privatsphäre in hohem Maß.[255] Zum anderen sind Diskriminierung und Racial Profiling ein grundlegendes Problem, das durch das Erfassen von Personen anhand ihrer biometrischen Merkmale mithilfe von Technologie noch weiter verschärft wird. Menschen anderer Herkunft oder Hautfarbe werden grundsätzlich meist häufiger als Verdächtige eingestuft[256] und Systeme, die das begünstigen, können dadurch leicht zur selbsterfüllenden Prophezeiung werden, ohne dass ein faktischer Verdacht vorliegen muss.

In autoritären Staaten wie z. B. China oder Russland dient Gesichtserkennung u. a. zur Verfolgung von Regierungskritikern. In China ist umfassende Überwachung sehr weit fortgeschritten und Gesichtserkennung ist ein zentraler Baustein des social-credit Systems zur automatisierten Kontrolle und Disziplinierung der Bevölkerung. Eine Folge davon sind massive Beschränkungen der individuellen Freiheit sowie Diskriminierung von Personen und sozialen Gruppen. Die Technologie dient in China auch dazu, die dort geächtete Gruppe der Uiguren gezielt zu verfolgen und zu diskriminieren. Aber auch in demokratischen Staaten nehmen Rassismus und Diskriminierung durch Technologie stetig zu.

---

252 Krempl, (2020).

253 NIST (2019).

254 *Guynn*, 19.10.2020; Johnson 24.10.2019; vgl. u. a. O'Neil 2016; Chander 2016; Noble 2018; Strauß 2018; Serna at al. 2019.

255 GAO, 2020.

256 Thompson, 2020.

Getragen von der Black Lives Matter Bewegung und dem massiven Rassismusproblem in den USA wurde Gesichtserkennung in einigen Metropolen (z. B. San Francisco, Berkeley, Oakland, Boston, Portland) verboten.[257] Das Verbot in San Francisco wurde allerdings später mit einigen Ausnahmen versehen. Ironischerweise u. a., damit Behördenmitarbeiter weiterhin legal FaceID auf ihren iPhones nutzen können.[258] Gleichzeitig werden immer wieder Fälle bekannt, wo Gesichtserkennung von Behörden eingesetzt wird, um Demonstrant*innen zu identifizieren.[259]

Gesichtserkennung ist aber nicht nur in den USA ein kontroverses Thema, sondern zunehmend auch in Europa. Großbritannien verfügt seit langem über eine enorm hohe Dichte an Videoüberwachungssystemen die zusehends auch mit Gesichtserkennung arbeiten. Unter anderem das Überwachungssystem in South Wales, wo aufgrund einer Klage von mehreren Bürgerrechtsorganisationen ein Gerichtsverfahren über Verletzungen der Privatsphäre und Diskriminierung gegen das polizeiliche Gesichtserkennungssystem eingeleitet wurde.[260] Das Gericht kam zu dem Schluss, dass automatisierte Gesichtserkennung illegal ist.[261] Ein weiteres Beispiel ist Nizza, wo ein System an zwei Tagen im Fasching (19. Und 20. Februar), mit besonders großem Menschenaufkommen auf den Straßen, zunächst mit 1.000 Personen getestet wurde. Das System nutzt Gesichtserkennung in einem Verbund von rund 2.600 Überwachungskameras, um die Stadt zu überwachen. Weitere Experimente fanden in Schulen statt. Nach Einsprüchen der Datenschutz-Behörde wurden diese Tests nicht fortgeführt.[262]

Auch in Österreich wird seit kurzem ein Gesichtserkennungssystem von der Polizei zu Fahndungszwecken eingesetzt. Nach einer Testphase ging das System im August 2020 in den Regelbetrieb.[263] Polizei und Innenministerium haben mehrfach beteuert, das System nur zur Identifizierung von Straftätern zu nutzen und keinerlei Echtzeitüberwachung stattfinde. Später wurde allerdings bekannt, dass das System im September 2020 im Zuge von Auseinandersetzungen bei Demonstrationen auch eingesetzt wurde, um Personen zu identifizieren. Laut einer kürzlich beantworteten parlamentarischen Anfrage kam die Software zwischen Dezember 2019 und Oktober 2020 931 Mal zum Einsatz, wobei 1.343 Verdächtige überprüft wurden.[264] Die Behörden berufen sich hier auf das Sicherheitspolizeigesetz als Rechtsgrundlage. Dem widersprechen Datenschützer wie epicenter.works, wonach es gar keine Rechtsgrundlage dafür gebe, außer es handle sich tatsächlich um das Vorliegen schwerer Straftaten. Medienbe-

---

[257] Krempl, 11.9.2020.

[258] Futurezone, 24.12.2019.

[259] Reuter, 16.10.2020.

[260] Bowcott, (2020).

[261] Stokel-*Walker C*. (2020).

[262] Dubedout, *C*., (2020).

[263] Wimmer, *B*. (2020).

[264] Sulzbacher, (2020b).

richten zufolge wurde das System jedenfalls auch genutzt, um antifaschistische Demonstrant*innen ausfindig zu machen. Über die Ausforschung Rechtsextremer sei nichts bekannt.[265]

Risiko von schleichendem Identifizierungszwang, Massenüberwachung mit Biometrie und dem Ende der Anonymität

Biometrie zählt in Summe zu den bedrohlichsten Formen von Überwachungstechnologie.[266] Diese frühe kritische Einschätzung von Roger Clarke ist heute relevanter denn je. Mit wachsender Verbreitung von Biometrie nimmt das Risiko von Massenüberwachung weiter zu. Insbesondere dann, wenn biometrische Identifikation zum fixen Bestandteil in Geräten und Anwendungen des Alltags wird. Am deutlichsten sichtbar ist dieses Risiko derzeit beim zunehmenden Einsatz von Gesichtserkennungstechnologie. Das Sammeln und Verarbeiten biometrischer Daten ist allerdings schon länger ein globaler Trend. Seit einigen Jahren ist ein deutlicher Anstieg an Menge und Datenbestand biometrischer Datenbanken erkennbar. Die Einführung biometrischer Reispässe liegt bereits lange zurück[267] und hat die Bedeutung von Biometrie in der Sicherheitspolitik weltweit erhöht. Sicherheitsbehörden erfassen verstärkt biometrische Daten. Bereits 2011 hat die US-Bundespolizei FBI etwa das „next generation identification program" gestartet, um die weltweit größte Biometriedatenbank zu schaffen. Darin sind neben Fingerprints und Gesichtsbildern auch Sprachmuster und DNA-Profile erfasst. Die Daten wurden aus verschiedenen Quellen zusammengeführt wie etwa diverse Polizeidatenbanken, Passregister, Führerscheinregister sowie private und öffentliche Überwachungssysteme.[268] Gesichtserkennung gilt als Kernanwendung des Systems. Laut einer Studie aus 2016 waren damals bereits rund 117 Millionen Gesichtsbilder erfasst. Die meisten davon von unbescholtenen Bürgern ohne kriminelle Vergangenheit.[269] Der wachsenden Anzahl an Datenbanken stehen vergleichsweise geringe Erfolge bei der Bekämpfung von Straftaten mit Gesichtserkennung gegenüber. So wurde etwa einer der Täter des Bombenanschlags beim Boston-Marathon 2013 nicht mit Gesichtserkennung, sondern mit klassischen Methoden und manueller Sichtung von Bildmaterial identifiziert. Die Technologie wurde zwar eingesetzt, lieferte aber keine brauchbaren Ergebnisse.[270] Allerdings kann die Technologie die Fahndungsarbeit unterstützen. Das LKA Bayern nutzt Gesichtserkennung, um Bildmaterial von Straftaten mit Fahndungsdaten abzugleichen und konnte dadurch die Anzahl identifizierter Straftäter in den letzten Jahren erhöhen.[271] Dem stehen aber

---

265 Sulzbacher, (2020a).

266 Clarke, 2002.

267 Mit der Idee von Reisedokumenten mit biometrischen Merkmalen befasst sich die internationale zivile Luftfahrbehörde (ICAO), eine Suborganisation der UN schon seit 1998. Nach den Terroranschlägen am 11.09.2001 kam es weltweit zu verstärkten Forderungen der Einführung. In der EU wurde die Einführung 2004 beschlossen. In Österreich werden seit 2009 biometrische Reisepässe ausgestellt.

268 Reardon (2012); EPIC (2016).

269 Garvie et al. (2016).

270 Standard (2013).

271 Schultejans (2020); Spiegel (2020).

auch hohe Fehlerraten gegenüber. Ein mehrmonatiger Test des deutschen Bundeskriminalamts in Mainz zeigte geringe Treffer und hohe Fehlerraten auf. Die durchschnittliche Trefferquote bei drei erprobten Systemen lag nur bei ca. 30 %. Bei schlechteren Lichtverhältnissen kann diese noch geringer ausfallen.[272] False Positives können zudem erheblichen Schaden bei Personen verursachen, die fälschlicherweise als Verdächtige eingestuft werden. Eine US-Studentin wurde etwa 2019 in Sri Lanka kurz nach einem Anschlag fälschlicherweise von einem System erfasst, zur Fahndung ausgeschrieben und erhielt in Folge Morddrohungen.[273] Neben teilweiser Überschätzung der Technologie wird die Fähigkeit von Menschen, Gesichter zu erkennen, unterschätzt. So gibt es Menschen mit besonderer Begabung (sog. „Super Recognizer"),[274] die auch von Strafverfolgungsbehörden eingesetzt werden. Eine Londoner Polizeibehörde verfügt etwa seit 2015 über eine eigene Abteilung mit der innerhalb weniger Monate über 500 Verdächtigte erkannt wurden.[275]

Biometrie spielt auch eine Rolle in der Entwicklungshilfe und im humanitären Kontext.[276] In Entwicklungsländern wie z. B. Indien, Kenya, Nigeria oder Brasilien wird seit einigen Jahren intensiv daran gearbeitet, biometriebasierte ID-Systeme zu schaffen. Die Weltbank hat 2014 das Programm „Identification for Development" ins Leben gerufen, mit dem Ziel, Menschen in Entwicklungsländern besseren Zugang zu öffentlichen Leistungen wie Sozialsystem und Bankwesen zu ermöglichen. Ähnliche Initiativen gibt es auch seitens der Vereinten Nationen.[277] Trotz dieses begrüßenswerten Ziels ist allerdings äußerst fraglich, inwieweit hierbei wichtige Datenschutz- und Sicherheitsstandards eingehalten werden. Im Fahrwasser der globalen Corona-Pandemie werden solche Initiativen weiter forciert.[278] Ein weitere Initiative ist die u. a. von Microsoft, der Gates-Stiftung und Accenture finanzierte Digital Identity Alliance ID 2020, ein Public Private Partnership, das durch Schaffung eines Systems für transnationale digitale Identitäten Reisefreiheit und Rechtsfähigkeit von Personen und damit u. a. Zugang zu staatlichen Leistungen und digitalen Diensten stärken will.[279] Solche Programme laufen derzeit beispielsweise in Thailand und Indonesien. Die ID 2020 Allianz ist jedoch nicht unumstritten. Zum einen sehen Verschwörungstheoretiker befeuert durch die Corona-Krise eine globale Bedrohung, weil die in ID2020 eingebundene Impfallianz Gavi eingebunden ist und eines der Vorhaben, die Umsetzung digitaler Impfpässe unterstützt. Derartige Befürchtungen diverser Anhänger von Verschwörungs-

---

272 Schulzi-Haddouti (2020).

273 Holland (2019).

274 Obermüller (2020).

275 Forster, G. (2016).

276 Vgl. u. a. Oxfam (2020).

277 Johnson/Campbell (2020).

278 *Subramanian*, 13.8.2020.

279 https://id2020.org, abgerufen am 24.11.2020.

mythen wie etwa der Irrglaube von Chipimplantaten sind relativ leicht mit Fakten widerlegbar.[280] Seriösere Kritikpunkte an der Allianz sind jedoch die Entwicklung intransparenter proprietärer Technologien und die starke Rolle der involvierten Konzerne und Stiftungen, womit u. a. Risiken einer Kommerzialisierung staatlicher Aufgaben wie jener der Identifizierung von BürgerInnen und der Verwaltung von Identitätsdaten verbunden sind.[281] Es ist davon auszugehen, dass die in solche Programme involvierten Unternehmen nicht rein altruistisch agieren, sondern durchaus auch Eigeninteressen verfolgen. So können gerade in Entwicklungsländern Technologien im größeren Stil getestet werden, ohne an Datenschutz- und Sicherheitsstandards in Europa oder auch den USA gebunden zu sein. Die Gefahr, dass hier schleichend Systeme realisiert werden, die auch zur Massenüberwachung missbraucht werden können, wie von einigen Kritikern befürchtet, ist daher nicht ganz von der Hand zu weisen.

Zahlreiche private Unternehmen verfügen über große Mengen an biometrischen Daten. Gesichtsbilder sind hier besonders häufig, weil sie mit geringem Aufwand und einfachen Mitteln erfassbar sind. Stichwort: selfies. Neben dem genannten Fall der US-Firma Clearview AI, das hauptsächlich Behördenanwendungen bereitstellt, sind auch in Europa ähnliche Praktiken bekannt geworden. Die polnische Suchmaschine PimEyes verfügt bspw. über rund 900 Millionen Gesichtsbilder, die mit geringem Aufwand durchsuchbar sind.[282] Trotz solch fragwürdiger Geschäftsmodelle ist in Europa derzeit noch kein Verbot von privater Gesichtserkennung absehbar.[283] Ursprüngliche Pläne der EU-Kommission in diese Richtung wurden wieder auf Eis gelegt.[284]

Aus den genannten Gründen ist Biometrie und Gesichtserkennung im speziellen besonders stark umstritten und wird mittlerweile selbst von Entwicklerfirmen der Technologie als zu weitreichend und problematisch beurteilt.[285] Zentrale Problemfelder sind enorme Datenschutzrisiken und Gefahren für die Privatsphäre sowie – eng damit verbunden – Bias und Diskriminierung. In Summe bedeutet der breite Einsatz von Gesichtserkennung eine erhebliche Bedrohung für die Demokratie. Unzählige Beispiele belegen, dass diese Gefahren nicht nur theoretischer Natur sind. Zahlreiche nationale und internationale Menschenrechtsorganisationen und Datenschutzeinrichtungen[286] sowie der Europäische Datenschutzbeauftragte (EDSB) beurteilen Gesichtserkennungstechnologie als gefährlichen Schritt in Richtung Massenüberwachung mit enormen Gefahren für Freiheit und

[280] Kasprak, (2020).

[281] Wagner, (2020).

[282] Dachwitz/Laufer/Meineck, 19.10.2020.

[283] Reda, 20.7.2020.

[284] Vollmer, 19.10.2020.

[285] Sulzbacher, (2020).

[286] Wiener Zeitung (2020).

Menschenrechte und fordern daher seit längerem Verbote.[287] Der europäische Datenschutzbeauftragte und die globale Datenschutzversammlung (global privacy assembly) warnen in einer Resolution ausdrücklich vor den Gefahren von Gesichtserkennung für die Demokratie. Gefordert wird insbesondere, bevor der Technologieeinsatz überhaupt in Erwägung gezogen wird, eine klare Regulierung in Einklang mit Datenschutzstandards, verpflichtendes Privacy-by-Design, Minimierung von Risiken und Begrenzung der Einsatzbereiche mit klar definiertem Zweck und eindeutiger rechtlicher Basis, unter Einhaltung grundlegender Prinzipien wie Zweckmäßigkeit und Verhältnismäßigkeit, Fairness und Transparenz, individuellen Grundrechten sowie klare, nachvollziehbare und überprüfbare Verwaltungsstrukturen. Zudem fordert die Versammlung einen Schulterschluss von Behörden, Stakeholdergruppen auf internationaler Ebene, um die Risiken der Technologie zu minimieren und wirksame Schutzmaßnahmen zu erarbeiten.[288] Auch die geplante Erweiterung des Prümer Vertrags (next generation Prum), die u. a. den verstärkten polizeilichen Austausch von Kfz-Daten, DNA und biometrischen Daten sowie die Schaffung eines übergreifenden Datenverbunds zur Gesichtserkennung vorsieht, ist umstritten und wird vom Grundrechts-Komitee des EU-Parlaments als problematisch erachtet. Die Abgeordneten verweisen in ihrer Kritik u. a. auf eine Studie über Datenaustausch, die erhebliche Fehlerraten, mangelnde Standards und Probleme bei Transparenz und Überprüfbarkeit aufzeigt. Sie waren vor den Folgen von Fehlern und Gefahren von politischem Machtmissbrauch durch die Technologie und fordern genaue faktenbasierte Evaluierung des Systems bevor es zu einer Erweiterung des Prümer Abkommens kommt.[289]

[287] *Stolton* 19.10.2020.

[288] GPA (2020).

[289] Stolton, S. (2020).

6 AUSBLICK

zunehmende Verschmelzung physischer und digitaler Umgebungen durch Biometrie

Biometrie verdeutlicht, wie sich die Grenzen zwischen Technologie und Körper verschieben und Körpermerkmale wie Fingerprints oder Gesichtsbilder algorithmisch abgebildet und verarbeitet werden.[290] Körpereigenschaften werden so letztlich zu einer Art Code,[291] der bereits heute für verschiedene Zwecke verwendet wird mit steigender Tendenz. Wie in Kapitel 4 gezeigt, ist Biometrie längst nicht mehr auf das Erfassen herkömmlicher biometrischer Merkmale wie Fingerprints oder Gesichtsbildern beschränkt. Das Anwendungsspektrum umfasst bereits heute automatisierte Analysen individueller Verhaltensmuster wie die individuelle Art eines Menschen zu gehen ebenso wie Gesichts- und Emotionserkennung, die durch ihre enormen gesellschaftlichen Risiken besonders umstritten sind. Emotionserkennung wird nicht nur in der Werbebranche, sondern zum Teil auch bereits bei Bewerbungsgesprächen, in Callcentern eingesetzt und auch in der Robotik/KI-Entwicklung wird u. a. daran geforscht[292] (etwa im Bereich autonomer Fahrzeuge oder für Mensch-Roboter-Interaktionen[293]). Solche Ansätze sind auch in der KI-Forschung selbst umstritten, sowohl hinsichtlich Wissenschaftlichkeit als auch Sinnhaftigkeit und eine Reihe von Expert*innen fordern Verbote von Emotionserkennung.[294] Neben intensiver Entwicklung von biometrischen Sensoren für Robotik und KI ist auch seit einigen Jahren zu beobachten, dass noch intensiver an Sicherheits- und Überwachungstechnologien geforscht wird, die zusehends nicht nur äußerliche Körpermerkmale erfassen, sondern auch Verhaltensmuster und sogar innerkörperliche Aktivitäten wie etwa Herzschlagmuster mittels Lasertechnologie aus Distanz[295] oder die Analyse von Biomen (mikrobiologischen Zellen) um Aktivitätsmuster einer Person zu rekonstruieren.[296]

Mit wachsendem Anwendungsspektrum, Einsatzbereichen und Zweckerweiterung von Biometrie verschärft sich ein zentrales Grundproblem der Digitalisierung noch weiter: Die erhöhte Identifizierbarkeit durch Technologienutzung.[297] Das heißt, es wird noch schwieriger, essentielle Datenschutzkonzepte wie Zweckbindung, Trennung unterschiedlicher Anwendungskontexte und Unverkettbarkeit personenbezogener Daten aufrechtzuerhalten. Das liegt insbesondere am Wesenszug biometrischer Merkma-

290 Lyon (2009), 17.

291 Strauß (2019), 173.

292 Masoner, 29.6.2020.

293 Schreiner, 2.4.2020.

294 Honey/Stiele, 25.2.2020.

295 Hambling (2019).

296 Thomas (2019).

297 Strauß (2019).

le, die eng an die Identität einer Person gekoppelt sind und Identifizierbarkeit erhöhen. Biometrie bindet daher Technologienutzung und dabei generierte Daten noch stärker an die Identität. Anonyme oder pseudonyme Nutzung und Trennung verschiedener Anwendungen, so dass nicht ohne weiteres Daten verkettet werden können, ist dadurch erschwert. Teil dieses Problemfeldes ist die zunehmende Vermischung zwischen Authentifizierung und Identifizierung. Authentifizierung ist der Nachweis einer bestimmten Eigenschaft und diese benötigt nicht zwingend auch die Feststellung der Identität einer Person. D. h. für Zwecke der Authentifizierung müssen auch keine Identitätsdaten verarbeitet und ausgewertet werden. Allerdings lässt sich das auf Anwendungsebene gerade durch den Einsatz von Biometrie, die unweigerlich eng mit der Identität einer Person verbunden ist, nur schwer trennen. Ein simples Beispiel ist die Feststellung einer altersgebundenen Berechtigung wie z. B. einer Fahrerlaubnis. Dazu reicht Kenntnis über das Alter einer Person, die Identität ist für diesen Zweck irrelevant. Ein einfaches digitales Verfahren würde hier z. B. das Geburtsdatum mit dem Tagesdatum abgleichen, um das Alter festzustellen und damit die Berechtigung. Sobald biometrische Daten im Spiel sind, wird der Vorgang schwieriger, weil die Identifizierbarkeit eine Eigenschaft ist, die biometrischen Daten inhärent ist. Die im Sinne von Datenschutz und Sicherheit wesentliche, klare Trennung zwischen Authentifizierung und Identifizierung ist beim Einsatz von Biometrie deutlich schwieriger. Die Einhaltung grundlegender Datenschutzprinzipien ist daher bei Anwendungen mit Biometrie noch stärker gefordert als bisher und zugleich noch schwieriger zu realisieren.

Die aktuell schwierige Situation auf globaler Ebene durch die Covid19-Pandemie verdeutlicht, wie rasch es zu einer Ausweitung biometrischer Datenerfassung kommen kann. Einige Länder nutzen etwa verstärkt biometrische Systeme, um den Gesundheitszustand von Personen zu messen. An Flughäfen werden Passagiere bereits zusätzlich zu smarten Videoüberwachungssystemen und Gesichtserkennung an Gates mit Wärmesensor-Kameras erfasst um etwa erhöhte Temperaturen zu messen und ggfs. Personen auszusondern. Mit der Dauer der Pandemie ist hiermit das Risiko noch tieferer Eingriffe in die Privatsphäre verbunden. Insbesondere dann, wenn sensible Daten über den Gesundheitszustand von Personen erfasst und gesammelt werden.

Doch auch unabhängig von der Pandemie besteht das Problem, dass mit der steigenden Erfassung biometrischer Merkmale die dazu eingesetzten Technologien intrusiver werden. Das heißt zusätzlich zur Problematik von Eingriffen in die Privatsphäre wird immer mehr auch die Menschwürde berührt, wenn körperspezifische Eigenschaften oder sensible Gesundheitsdaten in den Fokus technologischer und daran gekoppelte staatliche oder wirtschaftliche Prozesse rücken. Die Wirksamkeit von Schutzmechanismen für Datenschutz und Sicherheit ist daher essentiell.

7 HANDLUNGSEMPFEHLUNGEN

Datenschutz- und Sicherheitsstandards und generelles Schutzniveau erhöhen um die Risiken von biometrischen Verfahren einzugrenzen

In Anbetracht der enormen Gefahren, die von einer wachsenden Anzahl an Anwendungen, die biometrische Daten erfassen und verarbeiten, ausgeht, ergibt sich zusätzlicher Schutz- und Steuerungsbedarf. Biometrische Daten sind besonders sensibel und schützenwert. In der Datenschutzgrundverordnung (Art. 9 DSGVO) werden sie daher auch explizit angeführt als Daten, deren Verarbeitung grundsätzlich verboten ist. Eine Verarbeitung ist nur unter bestimmten Voraussetzungen erlaubt. Schon allein daraus ergibt sich Bedarf für ein deutlich höheres Schutzniveau auf technisch-organisatorischer, rechtlicher und gesellschaftlicher Ebene. Sofern biometrische Daten nicht zur eindeutigen Identifizierung einer Person genutzt werden, sondern nur zur Authentifizierung, dann gilt Art. 6 Abs. 1 DSGVO, um die Zulässigkeit der Verarbeitung festzustellen. In jedem Fall ist eine Datenschutzfolgenabschätzung (Art. 35 DSGVO) zwingend durchzuführen und der Schutz durch angemessene technisch-organisatorische Maßnahmen zu gewährleisten. Allerdings ist fraglich, ob technisch-organisatorische Datenschutz- und Sicherheitsmaßnahmen bei biometrischen Verfahren ausreichen, um die Risiken einzugrenzen, wie die in den Kapiteln 2 und 5 aufgezeigten, vielfältigen Missbrauchsmöglichkeiten verdeutlichen. Neben Missbrauchsrisiken bestehen zudem vor allem eine Reihe ethischer und grundrechtlicher Probleme. Der Schutz der Privatsphäre wird durch den wachsenden Einsatz von Biometrie in einem noch höheren Ausmaß bedroht als bei herkömmlichen digitalen Verfahren, die keine körperspezifischen Daten erfassen. Erschwerend hinzu kommt, dass Biometrie auch Risiken für die Menschenwürde bedeuten kann, wenn biometrische Daten über Identität und Körpereigenschaften von teil- oder gänzlich automatisierten Prozessen und Algorithmen analysiert werden. Damit ist auch das grundsätzliche datenschutzrechtliche Verbot automatisierter Einzelentscheidungen und Profiling berührt, dass bei Biometrie noch mehr Risiken bezüglich Diskriminierung mit sich bringt. Eine Stärkung des Diskriminierungsverbots durch biometrische Daten erscheint daher angemessen.

Wo immer möglich sind Verfahren zu bevorzugen, wo es zu keiner dauerhaften Speicherung biometrischer Daten kommt. Die Einhaltung von Datenschutz- und Sicherheitsstandards sollte ebenfalls stärker sanktioniert werden, um zumindest einige Risiken zu reduzieren. Um das notwendige, höhere Schutzniveau zu erreichen sind spezifische Audits und Zulassungsverfahren überlegenswert, die Unternehmen, die Biometrie einsetzen wollen, verpflichtend absolvieren müssen. Dadurch könnte das Problem verringert werden, dass allgemeine rein auf Rechtskonformität fokussierte Prüfverfahren die technischen Risiken nicht hinreichend erfassen und berücksichtigen können.

mehr Rechtssicherheit und klare Trennung zwischen Authentifizierung und Identifizierung

Beim Einsatz von Biometrie spielen die oben angeführten Aspekte aufgrund des hohen Risikopotenzials eine noch größere Rolle. Zentrale Datenschutzgrundsätze wie Rechtmäßigkeit, Datenminimierung, Zweckbindung, Verhältnismäßigkeit, Transparenz und Überprüfbarkeit etc. sind durch den sensiblen Charakter biometrischer Daten besonders berührt. Bereits bei nicht-sensiblen personenbezogenen Daten besteht nach wie vor das Problem, dass Grundsätze wie Datenminimierung und Zweckbindung durch die Vielzahl technischer Datenverarbeitungsformen immer mehr untergraben werden. Bei biometrischen Daten verschärfen sich diese Probleme erheblich weiter. Es ist daher zweckmäßig zu prüfen, ob sich daraus Bedarf nach zusätzlicher Regulierung ergibt, um das Schutzniveau insgesamt zu erhöhen. In jedem Fall sind allgemeine Begründungen für die Erfassung und Verarbeitung von biometrischen Daten unzureichend. Sie zählen zu den besonders schützenswerten Daten und machen eine Datenschutzfolgenabschätzung zwingend erforderlich. In der Praxis gibt es aber eine Reihe von Graubereichen. Am deutlichsten ist das derzeit im Bereich der optischen Datenerfassung sichtbar: Lichtbilder und Fotos mit Gesichtern eignen sich aufgrund des technischen Fortschritts bereits heute in unzähligen Fällen für die Identifikation von Personen durch Gesichtserkennung. Rechtlich ist es allerdings unklar, inwieweit diese Daten als biometrisch gelten. Daher sind auch das Schutzniveau und die rechtlichen Anforderungen diesbezüglich unklar. Hier besteht daher dringender Bedarf, um mehr Klarheit zu schaffen und ein höheres Schutzniveau zu gewährleisten. Das gilt auch für u. a. in Kapitel 6 angeführte Problematik der unklaren Trennung zwischen Authentifizierung und Identifizierung und diesbezügliche Graubereiche: Je nach Auslegung könnten für biometrische Verfahren, die rein für Authentifizierung eingesetzt werden, derzeit rein rechtlich geringere Schutzanforderungen bestehen, was aber zu hinterfragen ist, da biometrische Daten sich grundsätzlich zur Identifikation eignen. Es ist daher fraglich, ob hier der Zweck der Authentifizierung alleine hinreichend vor Identifizierung schützen kann. Auch hier besteht Klärungs- und Regelungsbedarf.

Wahlfreiheit und klare Grenzen bei Anwendungen

In Anbetracht der zahlreichen Problemfelder, mannigfaltigen Risiken und Gefahren von Missbrauch ergibt sich aus Sicht des Konsumentenschutzes im Endconsumer-Bereich wenig Potenzial für sinnvolle Anwendungen. Im Gegenteil wäre hier eine stärkere Eingrenzung der Anwendungsbereiche anzudenken. Anwendungsbereiche, wo Biometrie als ergänzender Authentifikationsfaktor genutzt werden kann, wie etwa beim E-Banking, ist sicherzustellen, dass die Daten vor externen Zugriffen geschützt sind und es zu keinerlei dauerhafter Speicherung von biometrischen Daten oder deren digitaler Komponenten (wie z. B. Hashwerte udgl.) kommt, um Risiken von Missbrauch und Identitätsdiebstahl zu minimieren. Darüber hinaus muss auch weiterhin Wahlfreiheit bei den Authentifizierungsverfahren gewährleistet sein. D. h. jede/r Konsument*in sollte selbst entscheiden können, ob seine/ihre biometrischen Daten verarbeitet werden dürfen oder nicht. Aus IT-Sicherheitsperspektive sind beispielsweise Authentifizierungsverfahren mit Security Tokens ohne Online-Anbindung wie cardTAN-Generatoren (die auch einige Banken anbieten), sicherer als reine Smartphone-

Apps. Die Tokens sind weder online angreifbar, noch generieren sie persistente Codes. Diese Variante ist daher empfehlenswerter als spezifische Apps, die biometrische Daten wie Fingerprints oder Gesichtszüge als zusätzlichen Faktor verarbeiten. Die Missbrauchsrisiken sind bei letzterem potenziell höher. Sinnvolle Anwendungen können überall dort gegeben sein, wo die spezifischen Eigenschaften biometrischer Merkmale und die enge Kopplung an die Identität einer Person tatsächlich Vorteile bringen und die Risiken vergleichsweise gering sind. Eine mögliche Anwendung von Biometrie mit hoher Sicherheitsrelevanz, bei der die Eigenschaft der inhärenten Identifikation einen Mehrwert bietet, ist etwa die Verknüpfung biometrischer Merkmale an Gefahrengüter wie Schusswaffen. Das könnte z. B. wesentlich dazu beitragen, den Missbrauch von Waffen oder anderen Gefahrgütern zu reduzieren.

Bei jeder Biometrie-Anwendung ist vor deren Einsatz genau zu prüfen, ob die Verarbeitung biometrischer Daten notwendig, sinnvoll und verhältnismäßig ist. Durch das hohe Risiko- und Schadenspotenzial insbesondere bezüglich Missbrauchs und Zweckentfremdung biometrischer Daten sind diese Aspekte essentiell. Grundsätzlich sind immer jene Verfahren zu bevorzugen, die keine sensiblen Daten verarbeiten und geringe Risiken mit sich bringen. Die Anreize für Missbrauch sind grundsätzlich sehr hoch, weil mit steigender Verbreitung von Biometrie enormer Schaden auf individueller wie wirtschaftlicher und gesamtgesellschaftlicher Ebene verursacht werden kann. Hierbei spielt insbesondere die Kommerzialisierung von biometrischen Daten eine erhebliche Rolle. Gerade im Endconsumer-Bereich nehmen mit wachsender Anzahl von Biometrie-Anwendungen die Möglichkeiten von Zweckentfremdung, Identitätsdiebstahl und Datenmissbrauch erheblich zu und Angriffe auf die damit verbundenen Systeme werden dadurch noch lukrativer. Zusätzlich zur Erhöhung der Schutzstandards ist daher ist eine Verschärfung von Sanktionen und Strafen bei der missbräuchlichen oder schadhaften Verwendung von Biometrie überlegenswert, um die Anreize für Missbrauch zu verringern. Ähnliches gilt für unzureichende Schutzniveaus. Auch die Kommerzialisierung von und der Handel mit biometrischen Daten sowie die Weitergabe an externe Dritte sollte grundsätzlich verboten und mit hohen Strafen sanktioniert sein. Das trägt auch dazu bei, die Möglichkeit von Angriffen etwa durch Eindringen in Biometrie-Datenbanken (siehe Kapitel 5) zu verringern und gleichzeitig den Aufwand für die Durchführung von Angriffen zu erhöhen.

Verbot von Gesichtserkennung im öffentlichen Raum und von Echtzeitüberwachung

Gesichtserkennung ist jene Technologie, die aus heutiger Sicht die größte Bedrohung für Grundrechte und Demokratie darstellt. Wie in Kapitel 5 erläutert, umfasst dieser Problemkomplex erhebliche Risiken wie technischen Unzulänglichkeiten etwa enorm hohen Fehlerraten, technologisch verschärfter Diskriminierung, Rassismus, Unterdrückung, Massenüberwachung und Verlust von Privatsphäre, Anonymität und persönlicher Freiheit. Daher ist im Umgang mit dieser Technologie besondere Vorsicht geboten und enge rechtliche Grenzen für deren Einsatz notwendig.

Aufgrund der enormen Gefahren wird ein klares Verbot von Echtzeitüberwachung empfohlen, um diese Gefahren möglichst einzudämmen. Das sollte auch jede mögliche Form der Verknüpfung öffentlicher und privater Videoüberwachungssysteme umfassen, um der Gefahr einer verdeckten Zentralisierung von Aufnahmen, die biometrische Daten enthalten, und damit verdeckte Massenüberwachung, zu verhindern.

Grundsätzlich sollte jede Form von Gesichtserkennungstechnologie streng reguliert sein mit besonderem Augenmerk auf rechtsstaatlicher Überprüfung der Verhältnismäßigkeit. Daher sollte jeder mögliche Anwendungsfall der Technologie zunächst eindringlich unter Abwägung grundrechtlicher und demokratiepolitischer Folgen überprüft werden, bevor die Technologie zum Einsatz kommt. Jeder Anwendungsfall von Gesichtserkennung sollte generell nur unter strengen Auflagen und nur in Ausnahmefällen möglich sein. Das bedeutet ein klares Verbot von Systemen, die Personen anhand ihrer Gesichtsmerkmale vollständig automatisiert identifizieren können und damit Echtzeitüberwachung ermöglichen. In allen Bereichen, wo der grundrechtskonforme Einsatz der Technologie verhältnismäßig denkbar sind, sollten der Einsatz in jedem Fall möglichst eng begrenzt sein und nur mit klar definiertem Zweck, eindeutiger rechtlicher Grundlage und nur bei verpflichtend implementierten Privacy-by-Design Mechanismen und Default-Anonymisierung mit wirksamen technischen Verfahren, um das Risiko genereller Überwachung von Personen möglichst gering zu halten. Verfahren wie bloße Schwärzung der Augenpartie oder dergleichen ist aufgrund der raschen technologischen Entwicklung und der laufenden Verbesserung von Gesichtserkennungsalgorithmen unzureichend. Diese Anforderungen sollten auch für Videoüberwachungssysteme gelten, um das Risiko verdeckter Identifikation zu reduzieren.

Auch von jeder Möglichkeit des vollständig automatisierten Abgleichens von Gesichtsbildern aus Fahndungssystemen zur Identifikation von Verdächtigten wird dringend abgeraten. Die hohen Fehlerraten und grundlegenden technischen Probleme von Gesichtserkennung erzeugen einerseits in vielen Fällen false positives mit erheblichen negativen Konsequenzen für die Betroffenen sowie zusätzlichen Aufwand der Behörden, diese Fehler zu korrigieren. Hinzu kommt, dass false positives in der Strafverfolgung auch einen Vertrauensverlust in die Behörden bedeuten können. Unbestritten ist, dass Gesichtserkennung für Behörden als zusätzliches Hilfsmittel sinnvoll sein kann, um Fahndungsarbeit und Aufklärung von Straftaten zu unterstützen. Technologien sollte diese Arbeit aber unterstützen, nicht vollständig automatisieren. Dass eine Automatisierung hier nicht zweckmäßig sondern eher kontraproduktiv ist, zeigen auch die diversen Probleme und Fehlerraten der entsprechenden Systeme (siehe auch Kapitel 5).

Überall dort, wo der Einsatz von Gesichtserkennung zur Strafverfolgung geplant oder bereits im Einsatz ist, gilt es unter Einhaltung zentraler Prinzipien wie Zweckmäßigkeit und Verhältnismäßigkeit, Fairness und Transparenz, und Bewahrung individueller Grundrechte, die Notwendigkeit des Technologie-Einsatzes nachzuweisen. Grundsätzlich sollte der Einsatz nur

unter strengen Auflagen, nur bei konkretem Verdacht schwerer Straftaten und nur unter richterlicher Genehmigung erfolgen. Um Transparenz, Nachvollziehbarkeit und Überprüfbarkeit als essentielle Grundvoraussetzungen bei Einsatz der Technologie sicherzustellen, sollte im laufenden Betrieb die Funktionsweise und Fehleranfälligkeit der Systeme regelmäßig von unabhängigen Kontrollinstanzen genau überprüft werden.

In Anbetracht der bereits heute existierenden technischen Möglichkeiten und des Fortschritts im Bereich Künstlicher Intelligenz sollten Gesichtsbilder grundsätzlich als biometrische, sensible und daher besonders schützenswerte Daten (nach Art. 9 DSGVO) behandelt werden. Hier erscheint eine rechtliche Nachschärfung nötig, um diesen Graubereich aufzulösen, der mit der wachsenden Verbreitung von Biometrie und Gesichtserkennung im speziellen zusehends problematischer wird. Das würde auch dazu beitragen, das derzeit häufig unzureichende Schutzniveau bei Anwendungen im Konsumbereich zu verbessern.

Bedarf nach klaren Regelungen auf nationaler, europäischer und internationaler Ebene

Nach derzeitigem Stand gibt es erhebliche Regulierungslücken bei Gesichtserkennung auf nationaler, europäischer wie internationaler Ebene. Hier ist jedenfalls empfohlen, zu einer harmonisierten Regulierung zu kommen, um zu vermeiden, dass nationale Unterschiede zu einem Regulierungsvakuum führen mit negativen Folgen für den Schutz der Grundrechte. Eine klare Regelung auf EU-Ebene könnte dazu beitragen, dies zu verhindern. Auf internationaler Ebene könnte eine enge Regulierung von Gesichtserkennung und Biometrie zum Beispiel im Rahmen der Konvention 108[298] angedacht werden. Die Konvention 108 wurde 2018 modernisiert und enthält seither u. a. auch Bestimmungen bezüglich biometrischer Daten und Algorithmen. Eine Stärkung der Bestimmungen in Hinblick auf die Gefahren von Gesichtserkennung und Biometrie hätte den Vorteil, dass damit eine Verankerung innerhalb international geltender Datenschutzregulierung geschaffen werden könnte. Die genauere Prüfung eines solchen Vorhabens wird daher empfohlen.

[298] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Council of Europe 2018, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

LITERATUR

Acquisti, A., Gross, R. and Stutzman, F. (2014), Face Recognition and Privacy in the Age of Augmented Reality. Journal of Privacy and Confidentiality, 6(2): 1-20

Adler A., Schuckers S. (2009), Biometric Vulnerabilities, Overview. In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA, https://doi.org/10.1007/978-0-387-73003-5_65

Art-29-Datenschutzgruppe (27.4.2012), WP 193, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien

Art-29-Datenschutzgruppe (6.2.2018), WP 250, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Datengemäß der Verordnung (EU) 2016

Artikel 29-Datenschutzgruppe (1.8.2003), WP 80, Arbeitspapier über Biometrie

Artikel-29-Datenschutzgruppe (11.4.2018), WP 260, Leitlinien für Transparenz gemäß der Verordnung 2016/679

Artikel-29-Datenschutzgruppe (16.2.2010), WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“

Artikel-29-Datenschutzgruppe (20.6.2007), WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“

Bergauer (2016), Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf Knyrim, S 242 Bilddaten: immer sensibel?, jusIT, 103, 241ff

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., and Senior, A. W. (2013), Guide To Biometrics, Springer Science & Business Media, Berlin, Germany,

Bontrager et al (2018), DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, arXiv:1705.07386

Bowcott, (2020) The Guardian, UK’s facial recognition technology ‘breaches privacy rights’, June 23, https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights

Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (2018), DSG Datenschutzgesetz – Kommentar

Burgess (4.5.2018), Facial recognition tech used by UK police is making a ton of mistakes, https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival, abgerufen am 19.10.2020

Buriro et al (05.2016), Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication, 2016 IEEE Security and Privacy Workshops (SPW)

Carman (25.04.2016), Researchers are using the vibration of your skull to identify you, https://www.theverge.com/2016/4/25/11501704/skullconduct-biometric-password-authentication

Chander, A. (2016), The Racist Algorithm? Legal Studies Research Paper No. 498. 2016. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795203

Clarke, R. (2001), Biometrics and Privacy, http://www.rogerclarke.com/DV/Biometrics.html

Clarke, R. (2002), Biometric, http://www.rogerclarke.com/DV/BiomThreats.html

Dachwitz/Laufer/Meineck (18.7.2020), Gesichtserkennung ist eine Waffe, https://netzpolitik.org/2020/npp-204-pimeyes-gesichtserkennung-ist-eine-waffe/

Dachwitz/Laufer/Meineck, 19.10.2020

Datenschutzkonferenz (03.04.2019), Positionspapier zur biometrischen Analyse, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf

Davis (17.06.2020), Google Fights Privacy Suit Over Facial-Recognition Technology, https://www.mediapost.com/publications/article/352651/google-fights-privacy-suit-over-facial-recognition.html

Dong, X., Jin, Z., Teoh, A. B. J., Tistarelli, M. and Wong, K. (2020), On the Security Risk of Cancelable Biometrics, Preprint submitted to Pattern Recognition, https://arxiv.org/pdf/1910.07770.pdf

Dubedout, C., (2020), Safe City Project in Nice: Testing Facial Recognition. AI-Regulation.com Febr. 24, https://ai-regulation.com/wp-content/uploads/2020/02/DUBEDOUT-C-Safe-City-Project-in-Nice-Testing-Facial-Recognition-.pdf

EDPB (29.1.2020), Guidelines 3/2019 on processing of personal data through video devices

EPIC – Electronic Privacy Information Center (2016), EPIC v. FBI – Next generation identification – seeking documents about the FBI's expansive biometric identification database, https://epic.org/foia/fbi/ngi/

Feiler/Forgó (2017), EU-DSGVO – Kurzkommentar

Fingas (10.11.2017), Vietnamese firm trips up iPhone X's Face ID with elaborate mask & makeup, https://appleinsider.com/articles/17/11/10/vietnamese-firm-trips-up-iphone-xs-face-id-with-elaborate-mask-makeup

Foltýn, T. (2019), Face unlock on many Android smartphones falls for a photo, https://www.welivesecurity.com/2019/01/10/face-unlock-many-android-smartphones-falls-photo

Forster, G., (2016), Manche Menschen erinnern sich an alle Gesichter. Welt, 27. Oktober, https://www.welt.de/wissenschaft/article159095120/Manche-Menschen-erinnern-sich-an-alle-Gesichter.html

Futurezone (24.12.2019), San Francisco lockert Verbot von Gesichtserkennung, https://futurezone.at/netzpolitik/san-francisco-lockert-verbot-von-gesichtserkennung/400711806

GAO – U.S. Government Accountability Office (2020), Facial Recognition Technology – Privacy and Accuracy Issues Related to Commercial Uses, https://www.gao.gov/assets/710/708045.pdf

Garvie, C., Bedoya, A. M. and Frankle, J. (2016), The Perpetual Line-Up: Unregulated police face recognition in America. Washington DC: Georgetown Law Center for Privacy and Technology, www.perpetuallineup.org

Gibbs (10.08.2015), HTC stored user fingerprints as image file in unencrypted folder, https://www.theguardian.com/technology/2015/aug/10/htc-fingerprints-world-readable-unencrypted-folder

Goichman (24.6.2019), Breaches of Israel's Biometric Database Kept Secret Until Watchdog Happened Upon Reports, https://www.haaretz.com/israel-news/.premium-breaches-of-israel-s-biometric-database-kept-secret-until-watchdog-found-reports

GPA (2020), 42nd Closed Session of the Global Privacy Assembly, October 2020, Adopted Resolution on Facial Recognition Technology, https://edps.europa.eu/sites/edp/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf

Grüner (25.07.2017), ARM Trustzone: Google bescheinigt Android Vertrauensprobleme, https://www.golem.de/news/arm-trustzone-google-bescheinigt-android-vertrauensprobleme-1707-129113.html

Guynn (1.7.2015), Google Photos labeled black people 'gorillas', https://eu.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465/

Hadid, A., Evans, N., Marcel, S. and Fierrez, J. (2015), Biometrics systems under spoofing attack: an evaluation methodology and lessons learned, IEEE Signal Processing Magazine, 32(5): 20–30

*Hautala (*11.3.2020), Thousands of fingerprint files exposed in unsecured database, research finds, https://www.cnet.com/news/thousands-of-fingerprint-files-exposed-in-unsecured-database-research-finds

Hill (10.2.2020), The Secretive Company That Might End Privacy as We Know It, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hill, K. (2020), The Secretive Company That Might End Privacy as We Know It. New York Times, Jan. 18, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Holland, M. (2019), Fehler bei Gesichtserkennung: Unschuldige auf Fahndungsaufruf in Sri Lanka. Heise, 30. April, https://www.heise.de/newsticker/meldung/Fehler-bei-Gesichtserkennung-Unschuldige-auf-Fahndungsaufruf-in-Sri-Lanka-4410155.html

Honey/Stieler (25.2.2020), Expertenstreit über Emotionserkennung durch KI, https://www.heise.de/newsticker/meldung/Expertenstreit-ueber-Emotionserkennung-durch-KI-4667496.html

ISO (2006), ISO/IEC 19794-8:2006, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/07/40715.html, abgerufen am 19.10.2020

Jahnel (2019), DSB: Bilddaten als nicht-sensible Daten, jusIT 2019, 32, 89ff

Jain/Nandakumar/Ross (2016), 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 2016

Johnson (24.10.2019), Racial bias in a medical algorithm favors white patients over sicker black patients, https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/

Johnson, M., Campbell, E. (2020), Biometrics, refugees, and the Middle East: Better data collection for a more just future. Middle East Institute, August 25, https://www.mei.edu/publications/biometrics-refugees-and-middle-east-better-data-collection-more-just-future

Kasprak, A. (2020), Are Bill Gates and the ID2020 Coalition Using COVID-19 To Build Global Surveillance State? Snopes, April 22, https://www.snopes.com/fact-check/bill-gates-id2020/ https://www.presseportal.de/pm/133833/4581365

Knyrim (2016), Bilddaten: immer sensibel?, JusIT, 102, 237

Knyrim (2018), Der DatKomm – Praxiskommentar zum Datenschutzrecht

Krempl (11.09.2020), Portland beschließt Verbot von Gesichtserkennung auch durch private Firmen, https://www.heise.de/news/Portland-beschliesst-Verbot-von-Gesichtserkennung-auch-durch-private-Firmen-4892247.html

Krempl (24.9.2020), Ruf nach dauerhaftem Verbot von Gesichtserkennung in der EU, https://www.heise.de/news/Petition-Ruf-nach-dauerhaftem-Verbot-von-Gesichtserkennung-in-der-EU-4910540.html

Krempl (25.09.2020), Gesichtserkennung: US-Ministerium räumt Hack sensibler Biometriedaten ein, https://www.heise.de/news/Gesichtserkennung-US-Ministerium-raeumt-Hack-sensibler-Biometriedaten-ein-4912807.html

Krempl (28.12.2014), 31C3: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck, https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html

Krempl (28.12.2018), 35C3: Mit Venenbild auf Handattrappe Geld abheben oder beim BND einbrechen, https://www.heise.de/newsticker/meldung/35C3-Mit-Venenbild-auf-Handattrappe-Geld-abheben-oder-beim-BND-einbrechen-4259637.html

Krempl, S. (2020) Gesichtserkennung: EU-Datenschützer warnen Strafverfolger vor Clearview. Heise, 11. Juni, https://www.heise.de/news/Gesichtserkennung-EU-Datenschuetzer-warnen-Strafverfolger-vor-Clearview-4781188.html

Kühling/Buchner (2018), DS-GVO BDSG

Leyden (5.10.2016), Mastercard rolls out pay-by-selfie across Europe, https://www.theregister.com/2016/10/05/mastercard_selfie_pay

Lyon, D. (2009), Identifying Citizens: ID cards as surveillance. Cambridge: Polity Press.

Malhotra (8.1.2018), The World's Largest Biometric ID System Keeps Getting Hacked, https://www.vice.com/en/article/43q4jp/aadhaar-hack-insecure-biometric-id-system

Maron (02.03.2020), Wenn das EKG den Pass und den Fingerabdruck ersetzt, https://www.medinside.ch/de/post/forschung-ein-ekg-statt-id-oder-pass

Masoner (29.6.2020), Wenn sich Maschinen für unsere Emotionen interessieren, https://oe1.orf.at/artikel/673110/Wenn-sich-Maschinen-fuer-unsere-Emotionen-interessieren

Muzayen (30.6.2020), Polizei von Detroit: Gesichtserkennung liegt in 96 Prozent der Fälle falsch, https://www.derstandard.at/story/2000118416980/polizei-von-detroit-gesichtserkennung-liegt-in-96-prozent-der-faelle

*Nellis (*02.11.2017), App developer access to iPhone X face data spooks some privacy experts, https://www.reuters.com/article/us-apple-iphone-privacy-analysis-idUSKBN1D20DZ

NIST – National Institute of Standards and Technology (2019), NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. Dec. 19, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Noble, S. U. (2018), Algorithms of Oppression: How search engines reinforce racism, New York: New York University Press

O'Neil, C. (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy; New York: Crown

Obermüller, E. (2020), Test erkennt die besten „Super-Recognizer. ORF Online, 17. Nov, https://science.orf.at/stories/3202964/

Oxfam (2020), Biometrics in the humanitarian sector, research report, the Engine Room/Oxfam, https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf

Paal/Pauly (2018), Datenschutz-Grundverordnung Bundesdatenschutzgesetz

Porter (14.8.2019), Huge security flaw exposes biometric data of more than a million users, https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data

Prabhakar, S., Pankanti, S. and Jain, A. K. (2003), Biometric Recognition: Security and privacy concerns. IEEE Security and Privacy, 99(2): 33-42

Ramachandra, R. and Busch, C. (2017), Presentation attack detection methods for face recognition systems: a comprehensive survey, ACM Computing Surveys, 50(1):1–37

Reardon, S. (2012), FBI launches $1 Billion Face Recognition Project. New Scientist, Sept. 7, https://www.newscientist.com/article/mg21528804-200-fbi-launches-1-billion-face-recognition-project/

Reda (20.7.2020), Edit Policy: PimEyes & Gesichtserkennung in Europa – wo bleibt der Aufschrei?, https://www.heise.de/news/Edit-Policy-PimEyes-Gesichtserkennung-in-Europa-wo-bleibt-der-Aufschrei-4847531.html

Reuter (16.06.2020), Polizeibehörden in den USA können mit Gesichtserkennung Protestierende identifizieren, https://netzpolitik.org/2020/briefcam-dutzende-staedte-in-den-usa-haben-gesichtserkennung-fuer-demonstrationen/

Ross/Shah/Jain (2007), From Template to Image: Reconstructing Fingerprints from Minutiae Points, IEEE transactions on pattern analysis and machine intelligence 2007, 544–560

*Ryne (*09.03.2019), Samsung Galaxy S10 face unlock can be fooled by a photo, video, or even your sister, https://www.androidpolice.com/2019/03/09/samsung-galaxy-s10-face-unlock-can-be-fooled-by-a-photo-video-or-even-your-sister/

Schaber (2020), Transparenzanforderungen des österreichischem und europäischen Datenschutzrechts an die Verarbeitung biometrischer Daten

Schneider (14.08.2020), Fingerabdruck statt Passwort: Biometrische Verfahren werden beim Banking beliebter, https://www.handelsblatt.com/technik/sicherheit-im-netz/fingerabdruck-statt-passwort-biometrische-verfahren-werden-beim-banking-beliebter/26093358.html

Schneier, B. (1999), The uses and abuses of biometrics, Communications of the ACM, 42(8), 136-136

Schreiner (2.4.2020), Diese KI soll Emotionen am Gang erkennen, https://mixed.de/diese-ki-soll-emotionen-am-gang-erkennen/

Schultejans, B. (2020), Are Bill Gates and the ID2020 Coalition Using COVID-19 To Build Global Surveillance State? Snopes, April 22, https://www.snopes.com/fact-check/bill-gates-id2020/

Schulzi-Haddouti, C. (2020), https://www.ingenieur.de/karriere/arbeitsleben/arbeitssicherheit/biometrische-gesichtserkennung-fuer-fahndung-ungeeignet/

Serna, I., Morales, A., Fierrez, J., Cebrian, M., Obradovich, N. and Rahwan, I. (2019), Algorithmic Discrimination: Formulation and Exploration in Deep Learning-based Face Biometrics. ArXiv preprint, December, https://arxiv.org/abs/1912.01842

Seyer (4.3.2013), Fujitsu Names Unicredit As First European Customer for Palm-scan Authentication, https://www.cio.com/article/2387857/fujitsu-names-unicredit-as-first-european-customer-for-palm-scan-authentication.html

Sharif, M. Bhagavatula, S., Bauer, L. and Reiter, M. K. (2016), Accessorize to a Crime: Real and stealthy attacks on state-of-the-art face recognition. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24-28, Vienna, Austria, 1528-1540.

Singer/Isaac (29.01.2020), Facebook to Pay $550 Million to Settle Facial Recognition Suit, https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html

Spiegel (2020), Polizei findet schon jetzt Hunderte Täter per Gesichtserkennung. Der Spiegel, 2. Feb., https://www.spiegel.de/netzwelt/netzpolitik/polizei-findet-schon-jetzt-hunderte-taeter-per-gesichtserkennung-a-5463cfec-602a-4065-abac-2685954768c3

Standard (2013), Bostons Polizeichef: Gesichtserkennung hat nichts gebracht. Der Standard, 22. April, https://www.derstandard.at/story/1363708749918/bostons-polizeichef-gesichtserkennung-hat-nichts-gebracht

Stokel-Walker C. (2020), Is police use of face recognition now illegal in the UK? New Scientist, August 11, https://www.newscientist.com/article/2251508-is-police-use-of-face-recognition-now-illegal-in-the-uk/

Stolton (1.9.2020), Gesichtserkennung: EU-Datenschutzagentur will Kommission von Verbot überzeugen, https://www.euractiv.de/section/digitale-agenda/news/gesichtserkennung-eu-datenschutzagentur-will-kommission-von-verbot-ueberzeugen/

Stolton, S. (2020), MEPs raise concerns on EU plans for police facial recognition database, Euractiv Sept. 22

Strauß, S. (2018), From Big Data to Deep Learning: A Leap Towards Strong AI or 'Intelligentia Obscura'? Big Data and Cognitive Computing 2(3), 16, https://doi.org/10.3390/bdcc2030016

Strauß, S., Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment, 2019, Abingdon/New York: Routledge

Stylios et al (2016), A Review of Continuous Authentication Using Behavioral Biometrics, Proceedings of the South East European Design Automation, Computer Engineering, Computer Networks and Social Media Conference on – SEEDA-CECNSM '16, 2016

Subramanian (13.8.2020), Biometric Tracking Can Ensure Billions Have Immunity Against Covid-19, https://www.bloomberg.com/features/2020-covid-vaccine-tracking-biometric/

Sulzbacher, M. (2020), Massenüberwachung und Rassismus: IBM steigt aus Geschäft mit Gesichtserkennungssoftware aus. Der Standard, 9. Juni, https://www.derstandard.at/story/2000117966303/wegen-massenueberwachung-und-rassismus-ibm-steigt-aus-geschaeft-mit-gesichtserkennungssoftware

Sulzbacher, M. (2020a), Polizei nutzt neue Gesichtserkennung, um Demonstranten zu identifizieren. Der Standard, 15. Sept, https://www.derstandard.at/story/2000119996329/polizei-nutzt-neue-gesichtserkennung-um-demonstranten-zu-identifizieren

Sulzbacher, M. (2020b), Polizei setzt neue Gesichtserkennungssoftware mehrmals täglich ein. Der Standard, 23. Nov., https://www.derstandard.at/story/2000121911862/polizei-setzt-neue-gesichtserkennungssoftware-mehrmals-taeglich-ein

Synek (07.11.2018), Gait recognition tech can identify people even with their backs turned, https://www.techspot.com/news/77298-gait-recognition-tech-can-identify-people-even-their.html

Thelen/Horchert (22.09.2018), Biometrie im Reisepass: Peng! Kollektiv schmuggelt Fotomontage in Ausweis – DER SPIEGEL – Netzwelt, https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

Thompson, E. V. (2020), Racial Profiling, institutioneller Rassismus und Interventionsmöglichkeiten. Bundeszentrale für politische Bildung, 27. April, https://www.bpb.de/gesellschaft/migration/kurzdossiers/308350/racial-profiling-institutioneller-rassismus-und-interventionsmoeglichkeiten

Vollmer (30.1.2020), EU will Gesichtserkennung doch nicht verbieten, https://t3n.de/news/eu-gesichtserkennung-verbieten-1247698/

Wagner, E. (2020), ber Impfstoffe zur digitalen Identität? Heise Telepolis, https://www.heise.de/tp/features/Ueber-Impfstoffe-zur-digitalen-Identitaet-4713041.html?seite=all

Wiener Zeitung (2020), Das Ende der Anonymität. Wiener Zeitung, 25. März, https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055533-Das-Ende-der-Anonymitaet.html

Xinhua (10.09.2019), Guangzhou subway adopts facial recognition, https://www.chinadaily.com.cn/a/201909/10/WS5d7766cea310cf3e3556ad0e.html

ANHANG

ABKÜRZUNGSVERZEICHNIS

aF ..... alte Fassung
ABl ..... Amtsblatt
API ..... Application Programming Interface
BGBl ..... Bundesgesetzblatt
Bsp ..... Beispiel
BVerGE ..... Entscheidung des (deutschen) Bundesverfassungsgerichts
bzw ..... beziehungsweise
dh ..... Das heißt
DSB ..... Österreichische Datenschutzbehörde
DSG ..... Datenschutzgesetz
DSR ..... Datenschutzrat
DSGVO ..... Datenschutzgrundverordnung
EDSB ..... Europäischer Datenschutzbeauftragter
EKG ..... Elektrokardiogram
EMRK ..... Europäische Menschenrechtskonvention
ErwGr ..... Erwägungsgrund
etc ..... et cetera
EuGH ..... Europäischer Gerichtshof
EU-PolKG ..... EU – Polizeikooperationsgesetz
GRC ..... Charter der Grundrechte der Europäischen Union
hA ..... herrschende Ansicht
Hrsg ..... Herausgeber
iA ..... im Allgemeinen
idgF ..... in der geltenden Fassung
idF ..... in der Fassung
idR ..... in der Regel
ieS ..... im engeren Sinne
insbes ..... insbesondere
inkl ..... inklusive
IP-Adresse ..... Internetprotkoll-Adresse
iSd ..... im Sinne des
iwS ..... im weiteren Sinne
iZm ..... im Zusammenhang mit
mE ..... meines Erachtens
mwN ..... mit weiteren Nennungen
OGH ..... Oberster Gerichtshof
PSD2 ..... Payment Service Directive 2
Rz ..... Randziffer
SPG ..... Sicherheitspolizeigesetz
ua ..... unter anderem
udgl ..... und dergleichen
uU ..... unter Umständen
VfGH ..... Verfassungsgerichtshof
vgl ..... vergleiche
VwGH ..... Verwaltungsgerichtshof
z. B. ..... zum Beispiel

GLOSSAR

Authentifizierung

Bezeichnet den Identitätsnachweis einer Person gegenüber einem System. Bei biometrischen Verfahren wird hier häufig ein Abgleich mit den Merkmalen einer einzigen, bestimmten Person vorgenommen (Verifikation, 1:1 Vergleich). An diesen Nachweis ist üblicherweise die Berechtigung geknüpft, bestimmte Funktionen des Systems zu verwenden.

Betroffene Person

Person, auf die sich die erfassten Daten beziehen. Im Kontext dieser Arbeit ist dies meist die Person, von der die erfassten biometrischen Daten ursprünglich stammen.

Biometrische Daten ieS

Daten zu den biometrischen Merkmalen einer Person, welche auch biometrische Daten im Sinne der DSGVO sind. Hierfür müssen die Daten unter anderem durch spezielle technische Verfahren ausgewertet werden, welche eine Identitätsbestimmung ermöglicht. Nicht auf ihre biometrischen Merkmale ausgewertete Gesichtsbilder sind daher aus dieser Definition ausgenommen

Biometrische Daten iwS

Alle Daten, welche potentiell auf biometrischen Merkmale hin ausgewertet werden können, unabhängig davon, ob es sich dabei um biometrische Daten im Sinne der DSGVO handelt. So fallen beispielsweise auch nicht auf ihre biometrischen Merkmale ausgewerteten Gesichtsbilder oder Stimmaufnahmen unter diese Defintion.

Biometrische Merkmale

Biologische (z. B. Fingerabdruck) oder verhaltenstypische Merkmale (z. B. Gangart) einer Person, welche ihre Identifikation ermöglichen.

Biometrisches Template

Eine besondere Form der Speicherung von biometrischen Merkmalen. Anstelle der Rohdaten eines Sensors werden nur die für einen späteren Vergleich wesentlichen Eigenschaften des biometrischen Merkmales gespeichert. Gehashte Templates sollen zusätzlich eine Rekonstruktion des ursprünglichen biometrischen Merkmals aus dem biometrischen Template erschweren.

Convenience-Technologie

Hierbei handelt es sich um Technologien, die hauptsächlich der Bequemlichkeit der Anwender*innen dienen. Ein Beispiel sind elektronische Geräte, welche neben einem Passwort auch mithilfe des Fingerabdrucks oder Gesichtsscans entsperrt werden können. Dies soll die Entsperrung des Geräts beschleunigen, bietet jedoch keinen Sicherheitsgewinn, da auch das Passwort alleine für eine Entsperrung des Gerätes ausreichend ist.

Datafizierung

Zunehmende quantitative Vermessung und Speicherung von Aspekten des menschlichen Lebens, die anschließend automatisiert ausgewertet werden können. Im Bereich der biometrischen Merkmale kommen durch den technologischen Fortschritt laufend neue Erfassungs- und Auswertungsmöglichkeiten hinzu.

Datenschutz-Folgenabschätzung

Systematische Abschätzung und Bewertung der Risiken für natürliche Personen durch eine beabsichtigte Datenverarbeitung. Zum Umfang einer solchen Analyse nach der DSGVO siehe Kapitel 3.7.3.

Dritter

Grundsätzlich alle Empfänger von personenbezogenen (biometrischen) Daten, welche nicht an der ursprünglichen Datenverarbeitung beteiligt sind. An der Datenverarbeitung beteiligt sind z. B. neben der betroffenen Person selbst der Verantwortliche und etwaige Auftragsverarbeiter.[299]

Endgerät

Das physische Gerät, mit dem der/die Nutzer*In direkt interagiert.

Falschakzeptanzrate – FAR

Häufigkeit, mit denen unterschiedliche biometrische Merkmale irrtümlich als übereinstimmend eingestuft werden (Falschakzeptanz). Eine solche Falschakzeptanz wird auch als „false postiv" bezeichnet. Bei biometrischen Zugangskontrollen ist die FAR z. B. ein Maß dafür, wie häufig unautorisierten Personen der Zugang erhalten.

Falschzurückweisungsrate – FRR

Häufigkeit, mit denen die gleichen biometrische Merkmale irrtümlich als unterschiedlich eingestuft werden (Falschzurückweisung). Diese irrtümliche Zurückweisung wird auch als „false negative" bezeichnet. Eine solche Falschzurückweisung führt bei biometrischen Zugangskontrollen z. B. dazu, dass einer berechtigten Person der Zugang irrtümlich verweigert wird.

Identifizierung

Bezeichnet die Identitätsbestimmung einer unbekannten Person. Bei biometrischen Verfahren wird die Identität durch einen Vergleich mit den Merkmalen vieler Personen ermittelt (1:N), was sie von der Verifikation unterscheidet. Die Identifizierung kommt häufig bei den Szenarien der Personenerkennung oder des Verhaltenstracking zum Einsatz

Lebenderkennung – Liveness detection

Die Lebenderkennung soll sicherstellen, dass das biometrische Merkmal direkt bei einer realen Person erfasst wird. Insbesondere soll damit die Vortäuschung von biometrischen Merkmalen mittels einer Attrappe (biometric Spoofing) erkannt werden.

---

[299] Zur genauen juristischen Definition siehe Art 4 Z 9 und 10 DSGVO.

Matching

Bezeichnet den Vergleich eines erfassten biometrischen Merkmals mit einer biometrischen Vorlage. Üblicherweise wird anhand eines Schwellwerts (threshold) entschieden, ob das erfasste Merkmal ähnlich genug der Vorlage ist, dass von einer Übereinstimmung (match) auszugehen ist.

Multi-Faktor-Authentifizierung

Bei der Multi-Faktor-Authentifizierung werden Faktoren aus unterschiedlichen Bereichen zur Authentifizierung benötigt. Neben biometrischen Merkmalen (Bereich Inhärenz) können hier z B. Schlüsselkarten (Bereich Besitz) oder Passwörter (Bereich Wissen) zum Einsatz kommen. Dies soll die Sicherheit von Zugangskontrollen erhöhen, da alle Faktoren für einen erfolgreichen Zugang benötigt werden. Bei 2 Faktoren wird dieses Verfahren auch 2-Faktor-Authentifizierung genannt.

Sensible personenbezogene Daten

Personenbezogene Daten zu bestimmten, besonders geschützten Kategorien wie z. B. Gesundheitsdaten oder ethnische Herkunft. Auch genetische Daten sowie biometrische Daten ieS fallen in die besondere Kategorie von personenbezogenen Daten. Zur weiteren Abgrenzung dieser Kategorien siehe Kapitel 3.3.

Wearable

Unter Wearables werden Mincomputer mit direktem Körperkontakt wie z. B. Fitnessarmbänder, Smartwatches oder Textilien mit integriertem Minicomputer (e-textiles) verstanden. Durch ihren direkten Körperkontakt sind sie häufig in der Lage, biometrische Merkmale wie Puls oder EKG kontinuierlich erfassen.

INSTITUT FÜR
TECHNIKFOLGEN
ABSCHÄTZUNG

ISSN: 1819-1320 | ISSN-Online: 1818-6556