Ulla Coester, Bernd Fuhlert

Gesichtserkennung – eine Frage der Ethik?

Die Forschung bezüglich Gesichtserkennung inklusive der daraus resultierenden Fortschritte im Bereich der Einsatzgebiete erscheinen auf den ersten Blick opportun – lassen sich doch daraus nicht zuletzt auch Maßnahmen umsetzen, die zur Erhöhung der Sicherheit beitragen können. Ob diese Euphorie im Weiteren durchgängig gerechtfertigt ist, soll im Rahmen des Artikels diskutiert werden.

1 Einführung

Es gibt zwei Grundannahmen, die im Kontext der Gesichtserkennung unbestritten von Bedeutung sind und somit zunehmend die Diskussion in Deutschland bezüglich deren Einsatz zum Positiven hin beeinflussen. Zum einen gibt es den allgegenwärtig postulierten Anspruch, dass Anwendungen mit einem höheren Nutz- oder Mehrwert ausgestattet sowie stetig komfortabler gestaltet werden müssen. Zum anderen verspricht deren Indienstnahme inklusive der damit verbundenen Optionen zur Überwachung latent einen höheren Grad an Sicherheit, sowohl für den Einzelnen als auch für die Gesellschaft. Um dem – hypothetischen oder antizipierten – Wunsch der Konsumenten nach mehr Bequemlichkeit nachzukommen, werden die Einsatzmöglichkeiten hier kontinuierlich weiterentwickelt: So muten die bestehenden Möglichkeiten zur Authentifizierung per Gesichtserkennung inzwischen beinahe trivial an, da es mittlerweile mit Apple Pay und dem iPhone X etwa in London möglich ist, U-Bahn-Fahrten oder den Wocheneinkauf im Supermarkt mit dem Gesicht zu bezahlen. Unterdessen scheint der Fantasie von Entwicklern im Hinblick darauf, wie sich dieser Trend kapitalisieren lässt, keine Grenzen gesetzt: Das zeigen unter anderem Apps wie FindFace [1] und FaceApp [2], beides Anwendungen aus russischen Software-Schmieden. Wenn auch unterschiedlich im Einsatz – erstere lässt zum Beispiel Gesichter virtuell altern während letztere zufällig aufgenommene Bilder von Menschen mit Social Media-Profilen in Verbindung bringen kann – ist beiden gemeinsam, dass sie keinesfalls konform mit europäischen Datenschutzgesetzen sind. [3] So gibt der Nutzer bei FaceApp nicht nur alle Rechte an seinen Daten ab – was im Detail zum Beispiel bedeutet, dass das Unternehmen dazu berechtigt ist, die hochgeladenen Bilder in jeglicher Art und Weise zu verwenden – sondern erteilt zusätzlich auch noch die Freigabe für diverse Zugriffe, etwa auf Kamera oder Mikrofon des genutzten Endgerätes. FindFace hingegen gibt einen Vorgeschmack darauf, welche Implikationen aus einer Gesichtserkennung resultieren und welche negativen Auswirkungen damit einhergehen können – nicht weniger als der zunehmende Verlust von Privatsphäre, weil aufgrund der Verknüpfung von veröffentlichten Bildern immer mehr über eine Person in Erfahrung gebracht werden kann. Was im Privaten schrittweise Einzug hält, nimmt auch im öffentlichen Sektor langsam Form an. Doch während die Einführung im privaten Bereich eher en passant geschieht und – da oftmals bestimmte Instinkte, wie der Spieltrieb, adressiert werden – nicht kritisch hinterfragt wird, findet bei den staatlichen Vorstößen in diese Richtung des Öfteren eine kontroverse Diskussion über die Technologie statt. Denn diese soll perspektivisch – mit dem Argument von mehr Sicherheit – großflächig eingesetzt werden.

Ulla Coester

ist Coach/Beraterin für Digitale Ethik. Als Gründerin von xethix-Diskurs® beleuchtet sie digitale Trends sowie deren Auswirkungen auf Unternehmen und Gesellschaft. Seit 2018 ist sie Partnerin/wissenschaftliche Leiterin bei Wegesrand.
E-Mail: uc@ucoester.de

Bernd Fuhlert

ist seit 2016 Geschäftsführer der @-yet GmbH. Seine zentralen Handlungsfelder sind Online Reputation Management sowie Datenschutz – unter anderem ist er als externer Datenschutzbeauftragter renommierter Unternehmen bestellt.
E-Mail: bernd.fuhlert@add-yet.de

2 Allgemein: Biometrie

Doch worum geht es überhaupt? Grundlage für die bereits kurz vorgestellten Anwendungen ist die Biometrie. Biometrie wird als „Automatisierte Erkennung von Individuen anhand deren Verhalten und ihrer biologischen Charakteristika" definiert [4] – das bedeutet, die hierüber durchgeführte Authentisierung erfolgt unter Verwendung physiologischer oder verhaltenstypischer, also generell personengebundener, Charakteristika. Daraus resultiert auch der substanzielle Vorteil dieser Verfahren, da die beschriebenen Merkmale weder unmittelbar gestohlen noch leicht kopiert werden können. Zur Messung der Merkmale stehen diverse Verfahren – entweder singulär oder komplementär – zur Verfügung, angefangen beim Tippverhalten an einer Tastatur über die Erfassung des Netzhautmusters oder des genetischen Codes (DNA-Analyse) bis hin zur Gesichtserkennung. [5] Die Voraussetzung für den Einsatz der Gesichtserkennung ist, vereinfacht dargestellt, dass ein erfasstes Gesicht in ein biometrisches Template konvertiert wird – dies geschieht durch die Vermessung der Gesichtsmerkmale und deren Umwandlung in einen digitalen Merkmalsvektor.

3 Speziell: Gesichtserkennung

Im Wesentlichen gibt zwei Bereiche, die für den Einsatz von Gesichtserkennung geeignet sind. Dies ist zum einen die Verifikation, also die Feststellung der Identität einer Person, worüber – ähnlich wie mit einem Passwort – der Nachweis einer Zugangs- und Zugriffsberechtigung zur Verfügung gestellt werden kann. Zum anderen lässt sich darüber lokal automatisiert die Identifikation von einzelnen Personen in großen Menschenmengen durchzuführen. Hierzu findet konkret ein Abgleich statt zwischen aktuell erhobenen biometrischen Referenzdaten eines Einzelwesens und einer Vielzahl von biometrischen Daten, die im Vorhinein in einer Datenbank erfasst wurden. Ziel diesen umfangreichen Prozess ist es, letztendlich ein Individuum herauszufiltern, dessen biometrischer Referenzdatensatz – innerhalb einer definierten Toleranzgrenze – mit den aktuell erfassten Daten übereinstimmt.

Es gibt eine Vielzahl von Verfahren, die zur Gesichtserkennung Anwendung finden können: Von der Mustererkennung, bei der spezifische Merkmale eruiert werden, anhand derer Gesichter sich unterscheiden über holistische, die beispielsweise mittels Diskriminanzanalyse den Zusammenhang zwischen verschiedenen Variablen darstellt und so eine Klassifizierung einzelner Gesichter ermöglicht, bis hin zur Nutzung von Höheninformationen in der Physiognomie als eindeutiges Identifikationsmerkmal. Allgemein ist mittlerweile ersichtlich, dass aufgrund von Maschine Learning in den letzten Jahren immense Fortschritte generiert werden konnten, die darauf basieren, dass anhand von Zigtausenden von Bildern unterschiedlicher Menschen selbstständig gelernt wird, bestimmte wiederkehrende Muster in Gesichtern zu identifizieren. [6]

4 Gesichtserkennung: Beispiele für Anwendungen

4.1 Entsperrung des Mobiltelefons

Während bis vor geraumer Zeit Mobiltelefone lediglich per PIN oder Fingerabdruck entsperrt werden konnten, bieten mittlerweile einige Hersteller auch die Freischaltung per Gesichtserkennung an. Biometrische Authentifizierungs-Systeme sind primär grundsätzlich zweckdienlich – entlasten sie doch den Nutzer davon, sich PINs oder Passwörter merken zu müssen und diese, unter dem Aspekt der Sicherheit, auch kontinuierlich zu wechseln – und komfortabel, hier insbesondere die Gesichtserkennung, da sie keine weitere Interaktion erfordert. Andererseits war anfangs genau dieses Verfahren in Puncto Sicherheit nicht unumstritten, denn aufgrund der Verwendung von 2D war es möglich, bestimmte Mobiltelefone mittels eines Fotos zu entsperren. Inzwischen wird jedoch zunehmend darauf gesetzt – beispielsweise bei Apple mit FaceID – durch Einsatz von Infrarotlicht ein 3D-Bild von dem Gesicht des autorisierten Nutzers zu erstellen, um so die Manipulationsmöglichkeiten zu verringern.

4.2 Grenzkontrolle

Mittlerweile sind Technologien der Gesichtserkennung beispielsweise beim Grenzübertritt in Flughäfen im Einsatz, zum Beispiel in Düsseldorf. Dort steht – bei der Einreise nach Deutschland – dem Fluggast die Möglichkeit zur Verfügung, seinen Reisepass eigenständig hoheitlich auslesen zu lassen und im Anschluss daran einen Schalter zu passieren, an dem ein Scan des Gesichts durchgeführt wird. Hierüber erfolgt im Weiteren dann der Abgleich zur Identitätsfeststellung der Person. Momentan kann diese Option seitens der Passagiere noch freiwillig genutzt werden.

4.3 Überwachungsoptionen, innerstädtisch am Beispiel London und Berlin, Südkreuz

London ist eine der Städte, die nahezu flächendeckend Gesichtserkennung im Realbetrieb zur Identifizierung von Straftätern einsetzt. Denn anders als bei der Grenzkontrolle findet hier der Abgleich mit gesuchten Personen aus der Polizeidatenbank statt, indem jeder Passant nahezu überall gescannt wird. [7] Auch wenn vom Prinzip her die Installation der Überwachungskameras am Südkreuz in Berlin dem gleichen Zweck dienen soll, sind hier die Bedingungen noch nicht entsprechend, da sich das Projekt in der Testphase befindet und somit bislang in dem System zur Validierung der Trefferquote bei der Zuordnung nur freiwillige Testpersonen erfasst sind.

4.4 Überwachungsoptionen, Beispiel Social Credits

Basierend auf den Möglichkeiten der Gesichtserkennung, zusätzlich angereichert mit Sprach- und Gangerkennung, wird in China ein Monitoring-System implementiert. Infolge der Fortschritte in der Technologie ist es heute bereits möglich einzelne Gesichter aus einer großen Menge zu extrahieren. Des Weiteren lässt sich mit einer ebenfalls bereits vorhandenen Software das Gesicht vermessen, ein Bewegungsprofil erstellen und spezielle Merkmale der aufgenommenen Person registrieren, wie etwa der Augenabstand. Diese Daten stehen im Folgenden beständig zur Verfügung – somit lässt sich mit einer hohen Wahrscheinlichkeit garantieren, dass ein Individuum identifizierbar ist, sobald es von einer Kamera erfasst wird, allein aufgrund der Tatsache, dass jedes Gesicht spezielle Merkmale besitzt. Perfektionierend hinzu kommt, dass das System zudem noch lernfähig ist. Intelligente Kameras, die nicht nur überall angebracht sind, sondern tatsächlich alles erfassen was vorbeikommt, senden unmittelbar die mitgeschnittenen Daten an Rechenzentren. Diese werden mittels Künstlicher Intelligenz analysiert, dann in Echtzeit in ausführlichen Profilen systematisiert und letztendlich gespeichert, um beispielsweise für Behörden abrufbar zu sein. [8]

5 Bewertung der Technologie: Fakten

Nicht zuletzt aufgrund der kulturellen Unterschiede ist es schwerlich möglich, die diversen Einsatzszenarien unter einheitlichen Gesichtspunkten zu würdigen. Evaluieren lassen sich hingegen die Fakten hinsichtlich der Effektivität der Technologie und der intendierten Ziele. In London beispielsweise sind geschätzte 500.000 Kameras im Realbetrieb eingesetzt – nicht nur auf der Straße, sondern auch in Bahnhöfen und Eingängen zur U-Bahn. Wer in dieser Stadt unterwegs ist wird im Durchschnitt 300 Mal an einem Tag erfasst. Eine Bewertung der Zweckhaftigkeit ist jedoch momentan schwierig, auch wenn sich bereits verschiedene Forschungsgruppen mit der Auswertung beschäftigt haben: So erhoben zwei Forscher der Universität Sussex in London eine Trefferquote von 19 Prozent und zeigten im Rahmen der Untersuchung unter anderem auch auf, dass bei der Befragung von 42 festgenommenen Personen tatsächlich nur acht gesuchte Straftäter ermittelt werden konnten. Dieses Ergebnis resultierte keinesfalls nur aus technisch bedingten Mängeln der Gesichtserkennungssoftware – die unter anderem daraus resultieren, dass die Erkennungsleistung dadurch nachteilig beeinflusst wird, ob wenn die Gesichtserfassung erfolgt während die Person in Bewegung ist – sondern auch daher, dass Passanten ihr Gesicht mit einem Schal bedeckt oder den Mantelkragen hochgeschlagen hatten und von daher die relevanten Merkmale nicht präzise erfasst werden konnten und somit die Personen schlecht identifizierbar waren. [7]

Der Einsatz der Technologie ist jedoch nicht nur für staatliche Behörden von Interesse, auch Unternehmen wie Amazon oder Google und Facebook setzen zunehmend darauf – nicht zuletzt, um diese wiederum an Regierungsbehörden (etwa der Einwanderungsbehörde ICE) zu verkaufen, wie Amazon vorgeworfen wird, oder schlicht zur Optimierung ihrer Produkte. So haben die beiden letztgenannten Konzerne Programme entwickelt, mittels derer sich alle Gesichter auf Fotos bestimmten Personen zuordnen lassen, da Gesichter von Nutzern per se biometrisch gescannt und gespeichert werden. [9] Um dies realisieren zu können, bedarf es unter anderem, neben der besseren Verfahren zur Mustererkennung, auch Kameras mit hoher Auflösung sowie eine bedeutende Menge an Bilddaten, um die Programme trainieren zu können. Die ausgeprägten Aktivitäten der großen Internetkonzerne lassen darauf schließen, dass ein valides Interesse daran besteht, die Technologie zügig weiterzuentwickeln. Doch ebenso schnell wächst, mit den zunehmenden Einsatzoptionen, ebenso die Kritik daran. Dabei steht momentan unter anderem zur Diskussion, wie zuverlässig sie beispielsweise bei schlechten Lichtverhältnissen ist und ob die Software Menschen mit dunklerer Haut genauso gut erkennt wie Menschen mit heller? Genau hier liegt einer der Knackpunkte: Da die Leistung der Software nicht nur von der Qualität, sondern auch von der Quantität der Daten abhängt, darf es theoretisch nicht vorkommen, dass die Trainingsdaten nach einseitigen Kriterien ausgewählt werden. Wenn diese Regel missachtet wird, kann es beispielsweise vorkommen, dass die maschinelle Gesichtserkennung – wie dies derzeit der Fall ist – die besten Trefferquoten bei der Erkennung weißer Männer erzielt. [10] Dies kann sich besonders in Kontexten, etwa bei der Strafverfolgung gravierend auswirken, da Personen mit dunkler Haut tendenziell eher Gefahr laufen, dass sie verwechselt und somit oftmals zu Unrecht verdächtigt werden – was unter dem Aspekt problematisch ist, dass bei einem automatisierten Nichterkennen die Beweislast bei dem fälschlich Erkannten liegt.

6 Zur Diskussion: Die Würde des Menschen ist unantastbar

Fraglich ist, in welcher Ausprägung der Gesichtserkennung das Recht eines Menschen auf freie Entfaltung tatsächlich eingeschränkt wird. Zur grundsätzlichen Überprüfung kann das Grundgesetz herangezogen werden, da dort der Begriff der Menschenwürde verankert ist. Damit verbunden sind Verpflichtungen, aus denen allgemeingültig Menschenrechte wie das Freiheitsrecht hervorgehen. Im Diskurs zur Digitalisierung ist im Weiteren auch die philosophische Interpretation dienlich: Der Philosoph Immanuel Kant leitet den Begriff der Menschenwürde primär von der Autonomie des Menschen ab. Dies bedeutet, dass jedes Individuum konstant eine Wahl hat (oder haben muss) und über sein Handeln – im Rahmen der Wertvorstellungen einer Gesellschaft – frei entscheiden kann. Eine weitere Dimension, die bei der Bewertung berücksichtigt werden muss, besteht darin, dass der Mensch in seinem Verhalten prinzipiell nicht-linear angelegt ist. Dies bedeutet, dass Entscheidungen aufgrund von bestimmten Umständen jeweils komplett gegensätzlich getroffen werden können, also nicht mit dem gewohnten Verhaltensmuster übereinstimmen. Präzise ausgedrückt: Jedermann kann sich situativ vollkommen anders verhalten, als er das in der Vergangenheit getan hat und dieses Recht muss ihm prinzipiell zugestanden werden. Fraglich ist, ob und inwieweit ein Risiko besteht, dass die Handlungsoptionen durch die Überwachung eingeschränkt werden und der Mensch dadurch die Entscheidungsfreiheit bezüglich seiner eigenen Verhaltensmuster und -weisen sukzessive verliert, weil er nur noch darauf achtet, konform zu agieren, um nicht aufzufallen. Das könnte beispielsweise dazu führen, dass Passanten im Winter ihr Gesicht – trotz Kälte – nicht mehr mit einem Schal bedecken würden. Zu diskutieren wäre hier, wo Grenzen gesetzt werden müssen, da die Ethik fordert, dass keine grundlegenden Rechte wie Privatheit zugunsten eines höheren Zieles völlig aufgegeben werden dürfen. Das verlangt den Diskurs in und mit der Gesellschaft, um sich auf Wertvorstellungen zu verständigen zu können und daraus Kriterien zu entwickeln, wann das Individualrecht nachrangig behandelt werden darf.

Aufgrund des kontinuierlichen Fortschritts sind in diesem Kontext relevante Fragestellungen zu beantworten: Etwa, in welchem Maße der Grundsatz „Die Menschenwürde ist unantastbar" auch weiterhin Bestand haben kann oder ob die Entwicklung in absehbarer Zeit potentiell die Möglichkeiten eines Menschen zur Reifung oder möglichen Korrektur seines Lebensmodells einschränken wird. Denn die Grenzen bezüglich der Erforschung oder Ausforschung von Menschen scheinen zunehmend offen. Das lässt sich in einigen Fällen positiv bewerten, zum Beispiel wenn Forscher herausfinden, dass am Gang eines Menschen erkannt werden kann, ob eine Gefährdung dahingehend besteht, in einigen Jahren an Alzheimer zu erkranken. Andererseits wirft das die Frage auf, welche Wesensmerkmale anhand des Gesichts identifizierbar sind und ob die Grenzen des Möglichen akzeptiert werden. Denn letztendlich könnte das Ziel sein, in bestimmten Anwendungen eine Bewertung mit Hilfe von Gesichtserkennung und Künstlicher Intelligenz automatisiert – also ohne jedwede Überprüfung durch Menschen – zu integrieren. In Israel ist bereits eine Anwendung namens Faception auf dem Markt, die verspricht, so unter anderem die Intelligenz und weitaus intimere Dinge eines Menschen ermitteln zu können. [11] Ist dies unbedingt notwendig und vor allem noch mit dem verbrieften Freiheitsrecht vereinbar? Oder ist es nicht das Recht eines jeden Menschen individuell die Entscheidung darüber zu treffen, was er preisgeben möchte und was nicht. Zumal die Freiheit per se eingeschränkt ist, da sich dieses biometrische Merkmal im Normalfall weder verdecken noch auswechseln lässt und von daher kaum eine Chance besteht dem zu entgehen. Bereits heute wissen die wenigsten Menschen in welcher Datenbank ihr Gesicht gespeichert ist, wofür dies Verwendung findet und ob es ihnen möglich ist, eine Löschung zu beantragen. Dass diese Daten ein Gesicht und damit letztendlich eine Identität und kein Objekt repräsentieren, scheint im Zuge von Effizienz-und Zukunftsorientierung oftmals in Vergessenheit geraten zu sein, dann wenn diese lediglich als Rohstoff zur Fütterung von Algorithmen verwendet werden, beispielsweise um die Gesichtserkennung weiter zu optimieren.

7 Lösung: DSGVO

Nachweislich ermöglicht die Technologie über kurz oder lang tief in die Privatsphäre von Menschen eindringen zu können, zum Beispiel in die Versammlungs- und Bewegungsfreiheit. Denn während sich heute noch der Einzelne auf einer Versammlung vergegenwärtigen kann, von wem er gesehen wird, verliert er die Kontrolle darüber in dem Moment, wenn mittels Drohnen angefertigte Aufnahmen ermöglichen jeden zu identifizieren und er theoretisch von beliebigen Personen, möglicherweise sogar weltweit, angeschaut werden kann. [12]Aus der ethischen Frage, was für ein Menschenbild hinter dem Bedürfnis der Verantwortlichen steckt, ordnend in das Leben und die Gesellschaft eingreifen zu können sowie auch zu müssen und grundsätzlich Bürger:innen als potentiell Kriminelle zu verdächtigen, ergibt sich zwangsläufig die Fragestellung nach dem Mitspracherecht der Gesellschaft und deren Möglichkeit zur Ausübung. Zum möglichen Gebrauch finden sich bereits einige Beispiele: „In Großbritannien gibt es, wie auch in vielen anderen Ländern, bisher keine gesonderte Rechtsgrundlage für automatische Gesichtserkennung. Weil es sich aber um eine Technologie handelt, die besonders invasiv ist, setzen sich immer mehr Organisationen weltweit dafür ein, ihren Einsatz zu verhindern. In Cardiff läuft seit Mai ein Gerichtsprozess. Und in San Francisco hat der Stadtrat automatische Gesichtserkennung gerade erst verboten." [7]

Damit die Gesichtserkennung also nicht für Dritte „zum Fenster zur Seele" wird, bedarf es strikter Regelungen durch den Gesetzgeber. Dieser muss eine Balance schaffen zwischen einem objektiven Sicherheitsbedarf und der Freiheit aller Bürger:innen, da eine automatische Gesichtserkennung schon aufgrund der Fehlerquote infrage zu stellen ist. Hinzu kommt, dass die so generierten sensiblen Daten für Hacker hochattraktiv sind. Denn anders als etwa bei Passwörtern, die der Nutzer immer wieder ändern kann, sind biometrische Daten aus der Gesichtserkennung ein anderes Kaliber. Wenn biometrischen Daten einer Person in die Hände unbefugter Dritter gelangen, können diese die Daten dauerhaft für ihre Zwecke missbrauchen. Des Weiteren ist Gesichtserkennung in Verbindung mit Künstlicher Intelligenz in jeder Form höchst bedenklich, allein aus dem Grund, da die Konsequenzen, die daraus resultieren können, heute nicht abschätzbar sind. Von daher ist die Aufgabe des Staates, und damit der gewählten Volksvertreter, dafür Sorge zu Tragen, dass mit einer eingesetzten Technologie kein Missbrauch betrieben werden kann. Selbst wenn die Technologie lediglich zum Abgleich von Bildern, ohne weitere Auswertung, eingesetzt wird, sollte sie dennoch momentan angesichts der Fehlerquoten – auch wenn diese mittlerweile deutlich geringer sind – nicht zum Einsatz kommen, um die Diskriminierung von Personenkreisen zu verhindern. Ohnehin ist heute die Gesichtserkennung, verbunden mit biometrischer Analyse, auch aufgrund der DSGVO nicht so einfach möglich, da eine Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt und nur in bestimmten Ausnahmefällen – die erheblich sein müssen – gestattet (Art. 9 Abs. 2 DSGVO, § 22 BDSG). Als Kategorie besonderer personenbezogener Daten unterliegen die, aus dem Verfahren der Gesichtserkennung erhobenen Daten dem Schutz aus Art. 9 DSGVO. Grundsätzlich bedarf es nach Art. 9 Abs. 2 lit. g immer einer Umsetzung in nationales Recht, die den Vorgaben aus der DSGVO gerecht werden. Neben den Anforderungen aus der Vorschrift muss der Verhältnismäßigkeitsgrundsatz gewahrt sein. Letztendlich bedarf es hier einer Festlegung der erheblichen Interesse deren Schutz höhergewertet wird, eventuell etwa die öffentliche Sicherheit. [13]

Um Gewissheit für Staat und Bürger herzustellen gilt es zunächst zu gewährleisten, dass die Fehleranfälligkeit erheblich verbessert ist. Erst dann kann überlegt werden, ob sich die Gesichtserkennung für den Einsatz eignet, allein unter dem Aspekt, dass dadurch die latente Gefahr des Missbrauchs in vielerlei Hinsicht besteht.

Literatur

[1] https://en.m.wikipedia.org/wiki/FindFace
[2] https://www.faceapp.com/
[3] Referenz zu GDPR: European Parliament: Regulation (EU) 2016/679. Official Journal of the European Union, L119:1–88, April 2016
[4] https://www.iso.org/standard/55194.html
[5] gemäß N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer Vieweg Verlag, Wiesbaden 2019
[6] R. Ranjan, S. Sankaranarayanan, A. Bansal, N. Bodla, J. Chen, V. M. Patel, C. D. Castillo, and R. Chellappa, "Deep learning for understanding faces: Machines may be just as good, or better, than humans," IEEE Signal Processing Magazine, vol. 35, no. 1, pp. 66–83, 2018.
[7] https://netzpolitik.org/2019/gesichtserkennung-in-london-hat-miserable-trefferquote-und-kann-menschenrechte-verletzen/
[8] https://www.faz.net/aktuell/politik/gesichtserkennung-in-china-totale-kontrolle-15253415.html / https://www.faz.net/aktuell/wirtschaft/unternehmen/china-ueberwachung-durch-gesichtserkennung-15533068.html
[9] https://www.spiegel.de/netzwelt/web/facebook-droht-milliardenstrafe-in-den-usa-wegen-gesichtserkennung-a-1281224-druck.html
[10] https://www.spiegel.de/netzwelt/netzpolitik/rassistische-algorithmen-ki-forscherin-mutale-nkonde-im-interview-a-1271778-druck.html
[11] https://www.tagesspiegel.de/themen/reportage/start-ups-in-israel-terroristen-und-paedophile-am-gesicht-erkennen/13701926-3.html
[12] https://www.sueddeutsche.de/digital/faceapp-gesichtserkennung-biometrie-ueberwachung-1.4533368
[13] https://www.datenschutzbeauftragter-info.de/erlaubt-die-dsgvo-gesichtserkennung-zur-abwehr-von-gefahren/