ANWENDUNGSFALL

FACE ID – GESICHTSERKENNUNG DURCH KI

Künstliche Intelligenz (nachfolgend: KI) sorgt seit geraumer Zeit für einen großen Umschwung in der Technik-Branche. So ermöglicht die Technologie viele neue Anwendungen, welche den Alltag der Nutzer*innen und deren Lebensweise erleichtern soll.
Mit der Einführung des iPhone X im Jahre 2017 veröffentlichte Apple eine neue Authentifikationsmöglichkeit namens Face ID, welche durch maschinelles Lernen realisierbar wurde. Diese neuartige Technologie ermöglicht allen Nutzer*innen ein bequemes Entsperren ihres Smartphones durch Gesichtserkennung.

ZAHLEN UND FAKTEN ÜBER DAS UNTERNEHMEN

Apple Inc. ist ein US-amerikanisches Unternehmen mit Sitz in Cupertino, Kalifornien. Gegründet wurde das Unternehmen 1976 von Steve Jobs, Ronald Wayne und Stephen Wozniak und gehört zu den führenden Konzernen in der Technik-Branche im Bereich Computer, Smartphones und Unterhaltungselektronik. Das Unternehmen beschäftigt weltweit ca. 154.000 Mitarbeiter*innen und verfügt über einen Jahresumsatz von 366 Milliarden US-Dollar. Davon wird über 50% durch den Verkauf von iPhone-Geräten generiert.

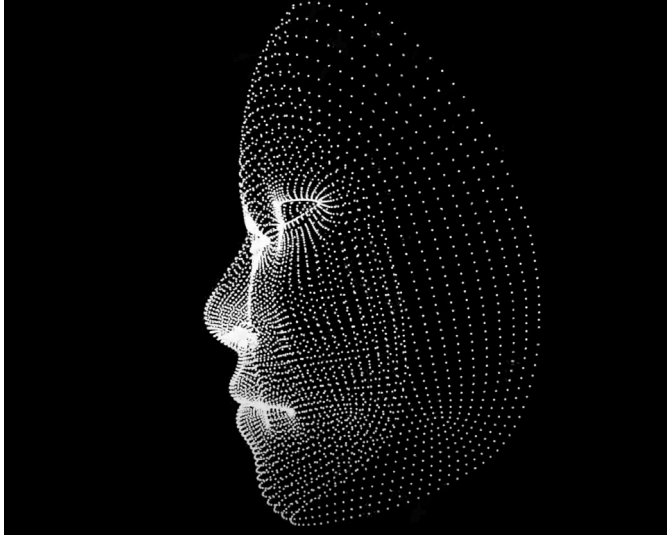
ZAHLEN UND FAKTEN ÜBER DIE ANWENDUNG

Face ID wurde erstmalig am 12. September 2017 im Zusammenhang mit dem neuen iPhone X vorgestellt. Seitdem wird die Anwendung aktualisiert und ist zum jetzigen Zeitpunkt in mehreren neuen iPhone und iPad Pro Modellen integriert. Durch eine lange Entwicklung, die laut Expert*innen über fünf Jahre gedauert hat, konnte Apple eine massentaugliche Gesichtserkennung entwickeln. So kosten alle verwendeten Sensoren und Teile der Face ID-Technologie den Konzern 16,70 US-Dollar pro Gerät. Die verbaute Rückkamera des iPhone X kostete im Vergleich über das Doppelte mit einem Preis von 35 US-Dollar pro Stück.

Nutzerperspektive

Um Face ID nutzen zu können, muss diese auf einem Apple-Gerät eingerichtet werden. So leitet das Gerät die Nutzer*innen schrittweise durch die Einrichtung. Bei der Registrierung muss unter normalen Umständen das Gesicht vollständig aus allen Winkeln gescannt werden. Dabei muss das Smartphone oder Tablet hochkant und mit 30 Zentimetern Abstand vor das Gesicht der Besitzer*innen gehalten werden. Benutzer*innen mit körperlichen Behinderungen können während der Kalibrierung „Optionen für Bedienungshilfen“ wählen. Bei dieser Einstellung müssen nicht alle Kopfbewegungen ausgeführt werden, um die verschiedenen Winkel zu erfassen. Blinde Personen oder Personen mit Seheinschränkungen, haben auch die Möglichkeit, die Face ID mit geschlossenen Augen zu verwenden. Dies benötigt jedoch eine besondere Einverständniserklärung der Nutzer*innen, da hierfür verschiedene Sicherheitsfeatures deaktiviert werden müssen.

Face ID besitzt zusätzliche Features, um die Benutzung so einfach wie möglich zu gestalten. So passt sich die KI automatisch an Veränderungen im Aussehen, wie Make-Up, Bartwuchs oder des Alterungsprozesses an. Durch den selbstständigen Lernprozess der KI, kann das Gesicht auch trotz Accessoires wie Hüte, Schals, Brillen, Kontaktlinsen oder den meisten herkömmlichen Sonnenbrillen erkannt werden. Sollte das Aussehen einmal trotzdem nicht identifiziert werden, fordert das Gerät zur Bestätigung der Identität einen PIN-Code an. Darüber hinaus funktioniert Face ID sogar in völliger



Dunkelheit oder im Freien bei hoher Lichteinstrahlung. Trotz dieser Weiterentwicklungen ist es Apple noch nicht gelungen, auch eine zuverlässige Entsperrung beim Tragen eines Mundschutzes zu gewährleisten. Das Gerät entsperrt sich wegen der Verhüllung des Mundes und der Nase meist nicht. Apple versuchte bereits mit mehreren Updates dieses Problem zu mildern, eine erfolgreiche Lösung gibt es zum jetzigen Zeitpunkt aber noch nicht.
Um das Nutzererlebnis zu verbessern, kann Face ID feststellen, ob der*die jeweilige Benutzer*in aufmerksam ist, indem überprüft wird, ob seine/ihre Augen geöffnet sind und dieser/diese dem Gerät gerade Beachtung schenkt. Somit wird auch für andere Personen erschwert, das Gerät ohne Erlaubnis zu entsperren. Wenn der*die Besitzer*in beispielsweise schläft oder absichtlich seine/ihre Augen verdeckt oder geschlossen hält, kann dies nicht zu einer Entsperrung des Gerätes führen. Auch hier wird durch mehrmalige Fehlversuche ein PIN-Code zur Sicherheit angefordert.

Ebenso kann Face ID für Käufe im iTunes Store, App Store oder dem Book Store, sowie Zahlungen mit Apple Pay, verwendet werden. Auch kann das Feature für Apps von Drittanbietern genutzt werden, um hier den Nutzer*innen eine einfache Authentifizierungsmöglichkeit zur Verfügung zu stellen.

Alle Anwendungen, welche bereits auf das Sicherheitsfeature Touch ID zurückgreifen, können auch mit Face ID benutzt werden. Dies gewährleistet einen komfortablen Umstieg, beispielsweise von einem alten zu einem neuen iPhone.

Technologische Perspektive

Apple verwendet für Face ID das TrueDepth Kamerasystem, welches aus mehreren Tiefenkameras besteht. Diese haben die Eigenschaft Distanzen zu messen, indem sie erfasste Ausschnitte mittels eines Lichtpulses ausleuchten. So misst das System für jeden Bildpunkt die Zeit, die das Licht bis zum Objekt und wieder zurück braucht. Somit kann für jeden Bildpunkt die Entfernung des darauf abgebildeten Objektes erfasst werden. Diese Technologie wird bei Face ID dafür verwendet, um die Geometrie des Gesichts genau abzubilden und dadurch eine intuitive und sichere Identitätsprüfung zu gewähren. Die TrueDepth Kamera erfasst hierzu Gesichtsdaten, indem sie über 30.000 unsichtbare Punkte projiziert. Dadurch wird mit Hilfe von KI eine detailgetreue und einzigartige Gesichtstiefenkarte erstellt, welche zur Entsperrung des Gerätes verwendet wird.

Neben der TrueDepth Kamera nutzt das Kamerasystem auch maschinelles Lernen, um die Software noch sicherer und weniger fehleranfällig zu gestalten. Dies geschieht durch einen Teil der neuronalen Engine der Bionic-Chips. Bei Bionic-Chips handelt es sind um von Apple produzierte Mikrochips, welche erstmalig 2017 zum Einsatz kamen und zu den schnellsten und effektivsten Chips auf dem Markt zählen. Zur Verschlüsselung der Daten wandeln diese die Gesichtstiefenkarten und Infrarotbilder des TrueDepth Kamerasystems in matematische Darstellungen um. Die gesammelten Aufnahmen bilden somit einen individuellen Code und werden intern auf dem iPhone verschlüsselt und nur auf dem Endgerät geschützt gespeichert. Diese Werte werden nun nach jedem Entsperren mit neu aufgenommenen „Live-Bildern“ verglichen.
Die gespeicherten Daten können intern mit der Nutzung von Face ID weiter verfeinert und aktualisiert werden, um die Benutzererfahrung nach jeder erfolgreichen Authentifizierung zu verbessern. Die KI der Gesichtserkennung überarbeitet diese Daten und den dazu gehörigen individuellen Code auch dann, wenn eine unvollständige Übereinstimmung gefunden wurde und das Smartphone von dem*der Nutzer*in nachträglich durch einen Code entsperrt wird. Dies soll die Fehleranfälligkeit nochmals reduzieren. Dabei bleiben alle Daten stets auf dem Apple Gerät und werden zu keinem Zeitpunkt in einer Cloud weitervermittelt oder an einer anderen Stelle gesichert.
Selbst wenn die Nutzer*innen sich nicht für Face ID registrieren, wird die TrueDepth Kamera auf intelligente Weise aktiviert, um Erkennungsfunktionen zu unterstützen. Zu diesen zählen beispielsweise das Dimmen oder Abschalten des Displays, wenn dem Gerät keine Beachtung geschenkt wird. Bei der Verwendung bestimmter Anwendungen kann das Gerät somit erkennen, ob die Nutzer*innen es gerade verwenden. Wenn dies nicht der Fall sein sollte, schaltet sich das Smartphone oder Tablet automatisch aus, um den Akku zu schonen. Diese Funktionen können jederzeit in den Einstellungen deaktiviert werden.

Wirtschaftliche Perspektive

Die Anwendung ist fester Bestandteil aller iPhone Modelle seit der Generation iPhone X, welche sich seit 12. September 2017 auf dem Markt befindet. Ebenso ist die Technologie in den iPad Pro Modellen seit der 3. Generation enthalten. Face ID steht somit ab dem Erwerb des jeweiligen Apple Produktes ohne Mehrkosten zur Verfügung und kann so lange genutzt werden, wie von den Nutzer*innen gewünscht. Somit besitzt das Produkt an sich keinen zusätzlichen monetären Wert für das Unternehmen. Jedoch steigert der Konzern mit solch einer Funktion das Ansehen und Prestige seiner Marke und den zugehörigen Produkten. Da ein großer Teil Apples Erfolgs auf ständiger Innovation und Weiterentwicklung beruht, hat Face ID noch einen weiteren wirtschaftlichen Nutzen: Die Position des Unternehmens an der Spitze der Technologie-Unternehmen zu sichern. Ebenso bieten neue Innovationen einen Anreiz zum Upgrade für bestehende Nutzer*innen. Da Apple mit einer langen Serviceleistung wirbt und auch bekannt für eine lange Nutzungsdauer ist, müssen Interessent*innen auf anderen Wegen zum erneuten Kauf überzeugt werden. Neue exklusive Features sind hierfür ein perfekter Anreiz, um bereits nach kürzester Zeit Kund*innen wieder zu gewinnen. So konnte Face ID Apple bereits im Jahr der Einführung einen Umsatzwachstum von 20% im Segment der Smartphones bescheren. Es wurden beispielsweise im dritten Quartal 2018 5,08 Milliarden US-Dollar mehr umgesetzt als im selben Quartal ein Jahr zuvor, in welchem nur iPhones mit Touch ID Funktion verkauft wurden.

Aber auch für Apps von Drittanbietern ist Face ID eine wirtschaftliche Bereicherung. Besonders im Bankgeschäft lohnt sich eine Investition in diese Technologie. Die biometrische Gesichtserkennung kann den Verwaltungsaufwand enorm reduzieren, wenn beispielsweise vergessene Passwörter neu beantragt werden müssen. Nicht zu unterschätzen ist ebenso, dass sich in diesem Sektor die Erwartungshaltung der Kund*innen schnell ändern kann. Wenn sich Banken somit wichtige Wettbewerbsvorteile sichern möchten, sollten diese auch eine zusätzliche Gesichtsverifikation verwenden. Apple kann von solchen Prozessen ebenso wirtschaftlich profitieren. Durch die Nutzung und externe Werbung der Banken für die Authentifizierungsmöglichkeit können weitere Apple-User*innen hinzugewonnen werden.

ANWENDUNGSFALL

FACE ID – GESICHTSERKENNUNG DURCH KI

Rechtliche Perspektive

Face ID wird von Apple als revolutionäres Sicherheitsfeature angepriesen. Jedoch werden auch auf vielen Seiten immer wieder Bedenken über Sicherheit und fehlender rechtlicher Grundlagen betont. Bei Manchen könnte an dieser Stelle die Erinnerung aufkommen, dass bereits andere Gesichtserkennungsvarianten, wie etwa von Samsung, kläglich gescheitert sind. So konnte bei diesem Hersteller das Endgerät bereits entsperrt werden, als ein Foto des*der Besitzer*in in die Kamera gehalten wurde. Apple hingegen versichert, dass durch die dreidimensionale Funktionsweise der TrueDepth Kamera des iPhones solch eine Fehlfunktion fast nie passieren könne. Es wird darauf verwiesen, dass es nur eine Fehlerquote von eins zu einer Million gebe und die Technologie damit noch sicherer sei als der Fingerabdrucks-Scanner, welcher eine Wahrscheinlichkeit einer falschen Identifikation im Verhältnis 1 zu 50.000 besitzt.

Doch was bedeutet diese Technik für den Datenschutz? Aus gutem Grund bestehen innerhalb Deutschlands und der EU hohe Anforderungen gegenüber Face ID und der darin verwendeten Gesichtserkennung. Da alle Nutzer*innen nahezu einzigartige Merkmale besitzen, ist dieser mit einer etwaigen Verbreitung, Verarbeitung oder externen Speicherung der Daten jederzeit identifizierbar. Mittlerweile ist es dank der verbesserten Software hinter Face ID auf Grundlage der KI auch möglich eine Entsperrung und Zuordnung des*der Besitzer*in, trotz größerer Veränderungen, wie einem anderen Haarschnitt, oder dem Tragen einer Brille, erfolgreich durchzuführen.

Deswegen müssen nach deutschem Recht einige Hürden überwunden werden, um den Einsatz solch einer Technologie so sicher wie möglich zu gestalten. So wird zuerst eine Einwilligung der Nutzer*innen benötigt, die ihn über Themen, wie die Verarbeitung von Daten, aufklärt und sie über die ständige Aufnahme von Bildern und der Erstellung einer Tiefenkarte bittet. Ebenfalls ist der geschützte Code, welcher bei jeder Entsperrung mit dem Muster des „Live Bilds“ verglichen und verbessert wird besonders schützenswert und darf nicht verbreitet oder zu anderen Zwecken genutzt werden. Dieser könnte sonst auch extern zur Identifikation der Nutzer*innen missbraucht werden.

Regelungen wie diese sind in der Datenschutz-Grundverordnung (DSGVO) gemäß Art 9. Abs. 1 und 2 zu finden und untersagen explizit solch eine Datenweiterverbreitung durch den Staat oder dem Unternehmen selbst. So darf der deutsche Staat die gesammelten Daten nicht zur externen Entsperrung des iPhones durch eine Drittperson in Situationen wie der Strafverfolgung einsetzen. Ebenfalls dürfen Personen nicht von Strafverfolgern dazu aufgefordert werden ihr Gerät per Gesichtserkennung zu entsperren, um somit an höchst private Daten zu gelangen. Das Gesetz führt auch dazu, dass Apple die aufgenommenen Werte nicht geräteübergreifend zur Entwicklung oder Verbesserung der Face ID Technologie und der dahinter steckenden KI, benutzen kann.
Leider werden die Nutzerdaten in anderen Ländern mit keiner solch großen Sorgfalt geschützt. So ist es in den USA bereits in mehreren Fällen geschehen, dass Personen ihr Smartphone über Face ID zur Strafverfolgung entsperren mussten. Im amerikanischem Recht besitzen biometrische Daten nicht den gleichen Schutz, wie z.B. ein PIN-Code, der durch den fünften Zusatzartikel in der Verfassung der Vereinigten Staaten abgesichert ist. Behörden können somit Personen gegen ihren Willen dazu zwingen, ihr iPhone per Face ID zu entsperren. Apple selbst unternimmt sogar etwas gegen diese Gesetzeslücke: IOS-Geräte benötigen einen PIN-Code, sobald das Gerät länger als 48 Stunden nicht entsperrt wurde. Selbst im entsperrten Zustand verlangt das Smartphone nach einem Code, sobald es an einen Rechner angeschlossen wird oder eine Person Zugriff auf sensible Daten verlangt.

Gesellschaftliche Perspektive

Seit der Einführung des iPhone X wurden ca. 850 Millionen Smartphones durch Apple verkauft. Ein Großteil davon sind Geräte mit Gesichtserkennungsfunktion. Ebenso kommen noch weitere Millionen iPad Pro Geräte mit gleicher Funktion hinzu. Apple hat es somit geschafft, die Gesichtserkennung zu einem wesentlichen Bestandteil seiner Geräte zu machen. Natürlich ist auch zu erwähnen, dass das Unternehmen nicht der alleinige Pionier der Funktion war. Handymarken wie Samsung oder Huawei haben eine ähnliche Technologie schon Jahre früher auf den Markt gebracht. Doch einen großen Unterschied gab es trotzdem: Alle Funktionen zuvor waren stark fehleranfällig und genossen deshalb nur sehr geringes Vertrauen der allgemeinen Bevölkerung. Durch Face ID hat sich dieses Bild stark geändert. Allein durch die hohe Nutzerzahl lässt sich vermuten, dass ein ständiges Scannen des Gesichts für viele Nutzer*innen kein großes Problem darstellt.

Doch gab es zur Einführung bereits viel Kritik an der neuen Technologie. So bleibt die Frage, ob Apple wirklich langfristig auf den großen Datensatz verzichten will, der durch Face ID entsteht. So hat zum Beispiel Google bei der Entwicklung von KI einen deutlichen Vorsprung zur Konkurrenz, weil das Unternehmen Daten aus dem Nutzerverhalten nutzt, um seine Programme zu perfektionieren.

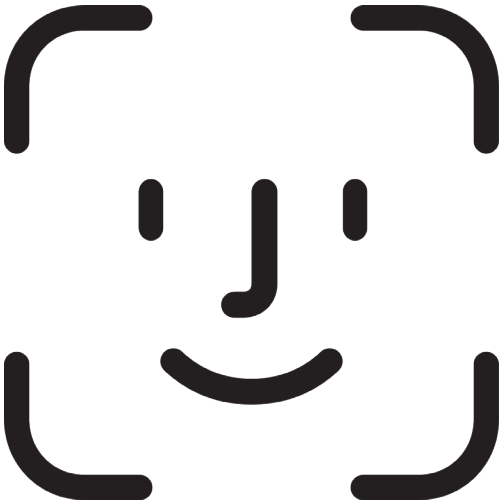
Ebenfalls besteht die Bedrohung, dass Trojaner oder andere Schadstoffsoftwares trotzdem Zugang zu dem System bekommen und somit an private Daten gelangen. Diese Gefahren schüchtern einen Teil der Gesellschaft gegenüber Face ID weiterhin ein. So finden 32% der deutschen Bevölkerung, dass biometrische Gesichtserkennung keine sichere Alternative zu anderen Authentifikationsmöglichkeiten bietet. Hierbei werden bei den größten Bedenken auf Datenmissbrauch, Identitätsdiebstahl und Datenschutzverlet-

zungen verwiesen. Ebenso bevorzugen 59% aller Beteiligten immer noch die Nutzung von Passwörtern über jegliche Alternativen wie Gesichtserkennung, Fingerabdrucksensoren und Co. zur Identifikationsprüfung. Auch geben nur 35% der befragten Personen an, dass sie Apple bei der Verarbeitung der Daten vertrauen.

Weitere Kritikpunkte gibt es auch zur Täuschung der Gesichtserkennung. Da Face ID auf die Gesichtsproportionen achtet, kann das Gerät von Personen mit identischen Zügen entsperrt werden, was besonders bei eineiigen Zwillingen der Fall sein kann. Auch bei sehr ähnlichen Geschwistern soll es dazu kommen können, dass Face ID das iPhone unberechtigterweise frei gibt. Für letzteres gibt es jedoch noch keine fundierten oder aussagekräftigen Ergebnisse. Ebenso wurde bereits versucht, Gesichtszüge von verschiedenen Personen anhand mehrerer Modelle nachzubilden, um das System zu überlisten. Apple forscht bereits an Lösungsansätzen, um solche Sicherheitslücken zu beheben.

Fazit

Aktuell ist Face ID für zwei wesentliche Funktionen gedacht: Sichere Entsperrung des Gerätes und das Freigeben von Informationen für Zahlungen oder Anmeldungen. So haben neben Apple auch Drittanbieter weitreichenden Zugriff auf die Funktion und können somit den Nutzer*innen großen Komfort ermöglichen. Es ist für jede Person möglich mit einem aktuellen iPhone oder iPad Pro Modell auf die Funktion zuzugreifen und deren Vorteile zu genießen. Auch für Apple ist die Gesichtserkennung ein großer Erfolg. Doch werden kritische Stimmen auch 4 Jahre nach der Einführung von Face ID immer noch laut. Da mit Hilfe von KI digitale Gesichtserkennung längst viel mehr kann, als nur Personen zu identifizieren, kann in den nächsten Jahren noch mit weiteren Funktionen gerechnet werden. So werden jetzt schon ähnliche KI-unterstützte Systeme dazu verwendet, um Emotionen oder Krankheiten bei verschiedenen Personen zu erkennen.



ANWENDUNGSFALL - FACE ID

QUELLEN

- Adjouri N. (2018): In der Natur der Marke. Das Streben nach Erfolg. In: Alles was Sie über Marken wissen müssen. Springer Gabler, Wiesbaden.
- Apple Support (2021): Informationen zur Fortschrittlichen Face ID Technologie. Internet: https://support.apple.com/de-de/HT208108, 09.01.2022.
- Beiersmann, Stefan (2017): HIS schätzt Materialkosten des iPhone X auf 370 Dollar. Internet: https://www.zdnet.de/88317747/ihs-schaetzt-materialkosten-des-iphone-x-auf-370-dollar, 09.01.2022.
- Conrad Conrad (2017): Gesichtserkennung ein Schlüssel für alles. Internet: https://www.datenschutz-notizen.de/gesichtserkennung-ein-schluessel-fuer-alles-4519093/, 09.01.2022.
- DSGVO (2021): Datenschutz-Grundverordnung. Internet: https://dsgvo-gesetz.de/, 09.01.2022.
- Euronews (2017): Internet: https://de.euronews.com/2017/11/15/gar-nicht-so-einfach-face-id-des-neuen-iphone-tauschen, 09.01.2022.
- Frommer, Dan (2018): What's really driving Apple's growth? Internet: Apple earnings: What's really driving Apple's growth? - Vox, 09.01.2022.
- Geiger Joerg (2021): iPhone trotz Maske entsperren;. Internet: https://www.chip.de/news/iPhone-trotz-Maske-entsperren-Apple-bringt-neues-Feature_183273235.html, 09.01.2022.
- Jäger, Moritz (2017): Face ID: Wie gut ist Apples neues Sicherheitssystem. Internet: https://www.security-insider.de/face-id--wie-gut-ist-apples-neues-sicherheitssystem-a-643390, 09.01.2022.
- Kollmann, Ralf (2017): Internet: https://www.fides-online.de/themen/artikelarchiv/iphone-x-apple-face-id-und-die-datenschutzgrundverordnung, 09.01.2022.
- Kubiv, Halyna (2018): Galaxy S9 Gesichtserkennung unsicherer als Face ID. Internet: https://www.macwelt.de/a/galaxys-s9-gesichtserkennung-unsicherer-als-face-id,3438623, 09.01.2022.
- Owen Malcom (2018): Apples future biometric security might be scanning veins in users face. Internet: https://appleinsider.com/articles/18/05/15/apples-future-biometric-security-might-be-scanning-veins-in-users-face, 09.01.2022.
- Resch, Rene (2018): FBI zwingt Person zur iPhone Entsperrung per Face ID. Internet: https://www.macwelt.de/a/fbi-zwingt-person-zur-iphone-entsperrung-per-face-, 09.01.2022.
- Statistica (2021): Internet: https://de.statista.com/themen/597/apple/#dossierKeyfigures, 09.01.2022.
- Statistica (2021): Internet: https://de.statista.com/statistik/daten/studie/203584/umfrage/absatz-von-apple-iphones-seit-dem-geschaeftsjahr-2007/, 09.01.2022.
- Sauer, Marc (2017): Apple A11 Bionic Chip nutzt eigene GPU und Deep Learning. Internet: https://www.golem.de/news/apple-a11-bionic-iphone-chip-nutzt-eigene-gpu-und-deep-learning-1709-130014.html, 09.01.2022.
- Teixeron, Guillaume (2018): Wie Face ID Sicherheit zur Identifizierung bieten kann. Internet: https://www.it-finanzmagazin.de/das-gesicht-als-code-wie-face-id-sicherheit-zur-identifizierung-bieten-kann-68994/, 09.01.2022.
- Tillmann, Maggie (2021): Was ist Apple Face ID und wie funktioniert es. Internet: https://www.pocket-lint.com/de-de/handy/news/apple/142207-was-ist-apple-face-id-und-wie-funktioniert-es, 09.01.2022.
- Abbildung 1: https://support.apple.com/de-de/guide/iphone/iph6d162927a/ios 15.01.2022.
- Abbildung 2: Apple Deutschland (2021): iPhone - Face ID Daten - Apple. Internet: https://www.youtube.com/watch?v=WIttDeyvccA, 09.01.2022.
- Abbildung 3: Wikipedia (2022): Face ID. Internet: https://en.wikipedia.org/wiki/Face_ID, 18.01.2022.