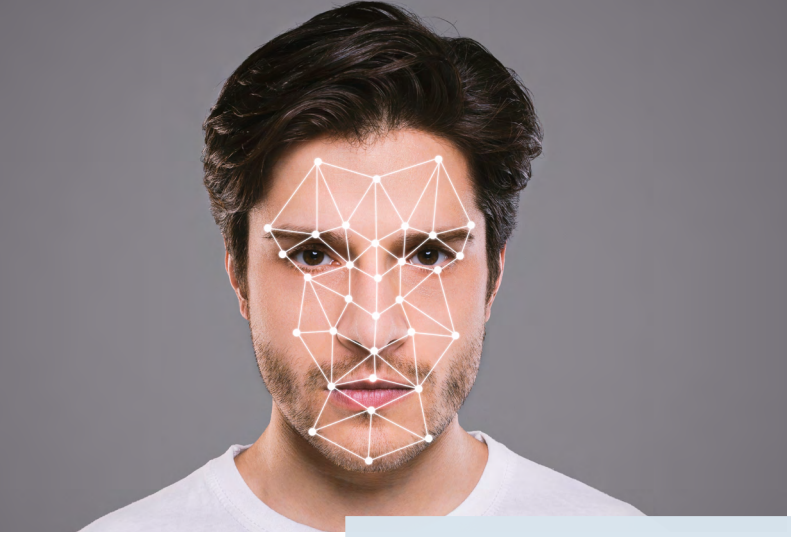
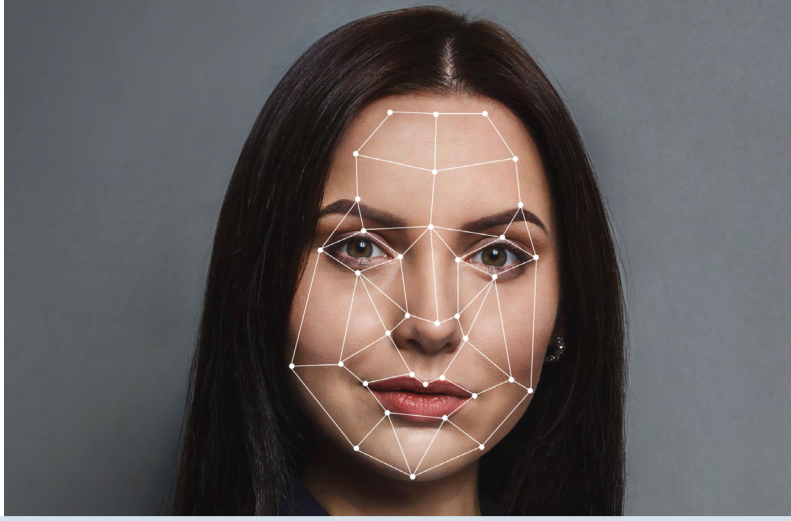
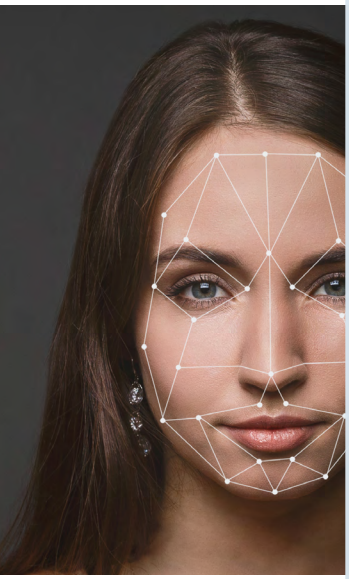
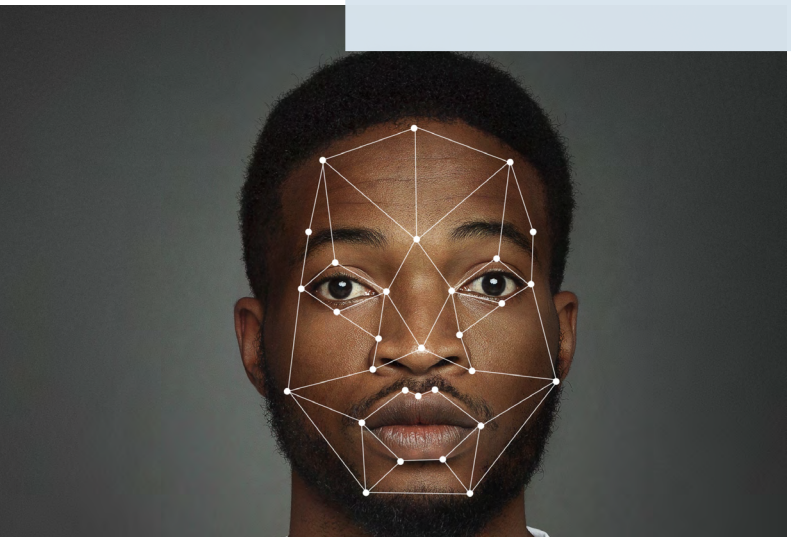
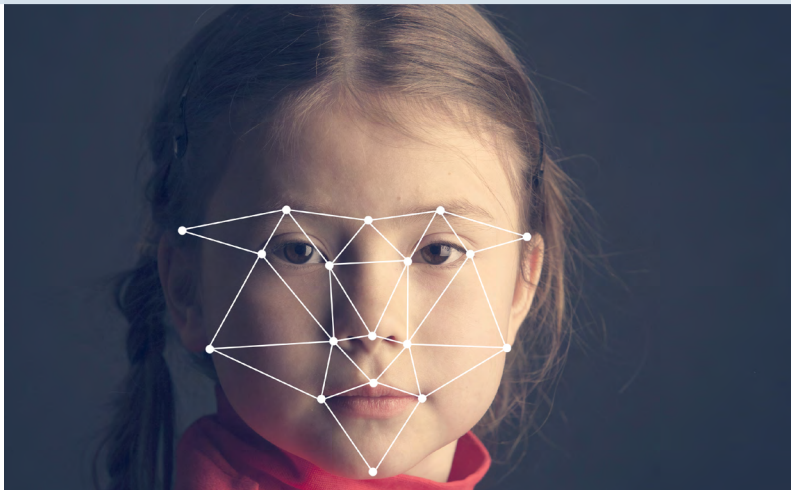





März 2021

Gesichtserkennung und Menschenrechte: Leitfaden für Investoren

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY

Über die Autoren

Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement

Benjamin Chekroun stieß 2018 als Deputy Head of Convertible Bonds zu Candriam und übernahm seine aktuelle Position im Stewardship-Team im Jahr 2020. Zuvor war er seit März 2014 bei ABN AMRO Investment Solutions tätig, wo er die globale Wandelanleihenstrategie leitete. Er verbrachte vier Jahre in Hongkong, ein Jahr in New York und dreizehn Jahre in London, wo er als Wandelanleihen-Trader arbeitete. 2004 wurde der Fonds unter der Leitung von Benjamin Chekroun von Hedge Fund Review als „Best Convertible Arbitrage Fund" ausgezeichnet. Benjamin Chekroun besitzt einen Masterabschluss in International Business.

Sophie Deleuze

Lead ESG Analyst, Stewardship

Sophie Deleuze kam 2005 in die ESG-Research-Abteilung von Candriam. Nach mehr als einem Jahrzehnt als ESG-Analystin spezialisierte sie sich auf die Bereiche Engagement, Proxy Voting und Stewardship bei Candriam. In diesem Rahmen koordinierte sie die Einbindung unserer ESG-Analysen bei allen unseren Investment-Management-Teams. Vor Candriam war sie vier Jahre als SRI-Analystin bei BMJ CoreRatings und Arese. Sophie Deleuze besitzt ein Diplom in Wasseraufbereitung und einen Masterabschluss in Public Environmental Affairs.

Quentin Stevenart

ESG Analyst

Quentin Stevenart stieß 2016 als ESG-Analyst zum ESG-Team von Candriam. Er führt umfassende ESG-Analysen des IT-Sektors durch. Zudem befasst er sich in verschiedenen Branchen mit Fragen zur Corporate Governance. Zudem koordiniert er das Research von Candriam zur Kreislaufwirtschaft. Er besitzt einen Masterabschluss in Betriebswirtschaft der Louvain School of Management und einen Master- sowie einen Bachelorabschluss in Business Engineering der Katholischen Universität Leuven.

Inhaltsverzeichnis

„Die Technologie ist vielversprechend und könnte positive Auswirkungen haben, aber Gesichtserkennung, so wie sie heute konzipiert ist und eingesetzt wird, ist mit Risiken und sozialen Folgen behaftet, die es rechtfertigen, dass Investoren sich mit diesem Thema befassen. Aus diesem Grund begrüßen wir die Bemühungen der vordenkenden Investoren, die, ohne auf Regulierungen zu warten, die herkömmliche Liste der ESG-Themen ausbauen und versuchen zu bestimmen, wie, wo, wann und von wem Gesichtserkennung angemessen eingesetzt werden kann“.

- **Katherine Ng,** Head of Academic Research, UN Principles for Responsible Investment

Zusammenfassung

Verantwortungsvolles Investieren ist mehr als eine Reaktion auf die Risiken und Probleme, denen wir heute gegenüberstehen. Es bedeutet, über den CO2-Fußabdruck und den Klimawandel hinauszudenken und die Risiken und Chancen der Zukunft zu berücksichtigen.

Die Technologie hat der Welt einige wunderbare Vorteile – und Anlagemöglichkeiten – beschert. U.a. ermöglicht sie es vielen Menschen, während der aktuellen Pandemie im Homeoffice zu arbeiten. Präsident Biden leitete einen Großteil seiner Wahlkampagne von seinem Hobbykeller aus. Dennoch dürfen wir nicht vergessen, dass alle neuen Technologien auch unbeabsichtigte Folgen mit sich bringen können.

Gesichtserkennung verbessert die Effizienz und die Sicherheit. Wir verwenden sie, um hochwertige Smartphones zu entsperren und berührungslos durch Flughäfen zu gehen. Sie hat jedoch auch Folgen für die Menschenrechte. Die Technologie wird seit Jahrzehnten entwickelt, findet aber erst jetzt allgemeinere Anwendung.

Candriam führte 2021 eine Umfrage durch, die rund 300 Anleger beantworteten. 30 Prozent hielten die Gesichtserkennung für ein praktisches und nützliches Instrument. Beinahe 70 Prozent hatten Vorbehalte – 31 Prozent meinten, Gesichtserkennung sei nicht genau, während 38 Prozent glaubten, die Technologie würde ethische Fragen aufwerfen.

Dazu gehörten mangelnde Zustimmung und fehlende Aufsicht. Irrtümliche Identifikationen, von denen manche zur Festnahme falscher Verdächtigen führen, kommen immer öfter vor. Im Mai 2019 verbot die Stadt San Francisco, dem Geburtsort der Gesichtserkennung, den Ordnungskräften den Einsatz der Technik. Bald danach gaben große Technologiekonzerne bekannt, dass sie den Vertrieb ihrer Gesichtserkennungsprodukte ein Jahr lang einstellen würden.

Um die Menschenrechtsfragen, die sich in Zukunft stellen dürften, zu verstehen, sollten sich verantwortliche Anleger und sonstige Stakeholder schon heute engagieren.

Diese Studie wäre ohne die Hilfe der folgenden Institutionen und Personen nicht möglich gewesen. Wir danken ihnen für ihre Zeit, ihren Beitrag und ihre Geduld:
- *Clare Garvie, The Center on Privacy & Technology at Georgetown Law*
- *Nabylah Abo Dehman, the United Nations Principles for Responsible Investments*
- *Anita Dorett, The Investor Alliance for Human Rights*
- *Isedua Oribhador, AccessNow*
- *Michael Conner, Open MIC*

Die Technologie

Wie funktioniert die Gesichtserkennung?

Die Gesichtserkennung gehört zu den biometrischen Systemen. Ziel ist die **Identifizierung** oder **Verifizierung der Identität** einer Person anhand eines Fotos oder einer Videoaufnahme des Gesichts. Die Technologie erfasst, analysiert und vergleicht Muster auf Basis der Gesichtszüge der Person. Einige Systeme setzen bereits dreidimensionale Bilder ein, um die Genauigkeit zu erhöhen.

Die Gesichtserkennung umfasst drei Schritte:

- Die **Gesichtserkennung** ist ein wesentlicher Prozess, der menschliche Gesichter in Bildern und Videos erkennt und lokalisiert.
- Die **Gesichtserfassung** wandelt analoge Daten – ein Gesicht – in digitale Informationen um, die die Gesichtszüge der Person darstellen. Dutzende von Merkmalen wie der Abstand zwischen den Augen, der Nasenrücken, die Konturen der Lippen, der Ohren, des Kinns usw. werden gemessen.
- Die **Gesichtsabgleichung** überprüft schließlich, ob zwei Gesichter dieselbe Person sind.

Der Algorithmus berechnet ein Ergebnis mit einer bestimmten Wahrscheinlichkeit in statistischer Form, etwa „*Positive Abgleichung – Max Mustermann – 97,36 Prozent Wahrscheinlichkeit*“.

Eine kurze Geschichte der Gesichtserkennung

Die Gesichtserkennung geht auf die 1960er-Jahre zurück. Woody Bledsoe, Bischof der Kirche Jesu Christi der Heiligen der Letzten Tage und Mitgründer von Panoramic Research in Palo Alto, entwickelte eine Methode, mit der er die Positionen der Gesichtszüge einer Person manuell in einem Computer erfassen konnte. An heutigen Maßstäben gemessen war dieses Vorgehen nicht sehr effektiv, aber es zeigte, dass die biometrischen Daten des Gesichts zur Identifizierung dienen können. Die Genauigkeit der Erkennungssysteme stieg in den 1970er-Jahren, als Forscher zusätzliche Gesichtskennzeichen hinzufügten. In den 1980ern und 1990ern beschleunigte sich der Fortschritt. Neue Methoden erlaubten es, ein Gesicht in einem Bild zu finden und die Gesichtszüge zu erfassen, wodurch die vollautomatische Gesichtserkennung möglich wurde. 1996 wurde die erste Gesichtsdatenbank im Rahmen des amerikanischen FERET-Programms aufgebaut. 2001 prüfte die Polizei anlässlich des Super Bowl erstmals die Gesichtserkennung für ihre Zwecke und identifizierte 19 gesuchte Straftäter in der Menschenmenge. Weitere aufsehenerregende Durchbrüche gelangen ab 2010, als künstliche neuronale Netze die Technologie verbesserten. 2011 trug Gesichtserkennung dazu bei, die Identität von Osama Bin Laden zu bestätigen, der bei einem Angriff von amerikanischen Soldaten getötet wurde. Facebook führte die Technologie für das Foto-Tagging ein. Das DeepFace-Programm erzielte 2014 erstmals beinahe so gute Ergebnisse wie der Mensch. 2017 war das iPhone X das erste marktgängige Smartphone, das mit Gesichtserkennung entsperrt werden konnte. Damit wurde die Technik das erste Mal in einem Massenprodukt eingesetzt. Im Mai 2019 verbot San Francisco als erste amerikanische Großstadt den Ordnungskräften den Einsatz der Gesichtserkennung. Im Sommer darauf verpflichtete sich der CEO von IBM gemäß den Prinzipien für Vertrauen und Transparenz des Unternehmens, keine Gesichtserkennungs- oder Analysesoftware mehr anzubieten. Bald folgten weitere Technologieriesen wie Amazon, Facebook und Microsoft, die den Vertrieb ihrer Produkte ein Jahr lang einstellten.

Diese Schritte setzen die Verfügbarkeit und die Nutzung bestimmter Daten im Vorfeld voraus.

- Ein Gesichtserkennungssystem lernt mit einer **Trainingsdatenbank** aus Bildern, Gesichtsmuster zu erkennen. Je umfassender, komplexer und uneinheitlicher die Datenbank, desto genauer die Erkennung.

- Die Gesichtserkennung kombiniert **künstliche Intelligenz** (das System kann durch die Datenanalyse lernen), **maschinelles Lernen** (das System kann die Datenverarbeitung und -nutzung ohne den Eingriff des Menschen ausbauen, weil es aus früheren Erfahrungen lernt) und **Deep Learning** (eine neue Technik, die maschinelles Lernen anhand neuronaler Netze, wie sie im menschlichen Gehirn zu finden sind, verbessert).

Anwendungen

Gesichtserkennung umfasst in der Regel eine oder mehrere Aufgaben:

Identifizierung
„Wer sind Sie?“

Authentifizierung
„Sind Sie wirklich die Person, die Sie vorgeben zu sein?“

Kategorisierung
„Welcher Gruppe / Kategorie gehören Sie an?“

Gesichtserkennung wird zwar hauptsächlich von Sicherheitspersonal und Polizei eingesetzt, kommt aber auch in der Medizin und dem Marketing zur Anwendung. Die Liste der Anwendung wird täglich länger.

- **Polizei** – Ortung verdächtiger Straftäter / Terroristen, Suche nach Vermissten, Zugangskontrolle, Überwachung von Menschenmengen
- **Sicherheit** – Entsperren von Türen / Telefonen / Systemen, Transaktionsbestätigung, Fluggastkontrolle
- **Schulen** – Schutz, Anwesenheitskontrolle, Aufmerksamkeitsprüfung
- **Medizin** – Diagnose einer kleinen, aber möglicherweise wachsenden Anzahl von Erkrankungen, Beurteilung von Schmerzen
- **Soziale Medien** – Identifizierung von Menschen auf Bildern
- **Marketing** – Bereitstellung „intelligenter“ Werbung
- **Mensch-Maschine-Interaktion** – autonome digitale Menschen interagieren bald mit Menschen und passen ihre Reaktionen auf der Basis von Gesichtserkennung an.[1]

Vorteile

Wir erkennen uns gegenseitig nicht über Fingerabdrücke oder Muster der Iris, sondern über unser Gesicht.

Gesichtserkennung gilt als **das natürlichste aller biometrischen Systeme**, denn sie benötigt keine physische Interaktion. Es gibt andere biometrische Maßstäbe wie Fingerabdrücke, Iris-Scans, Stimmerkennung, Digitalisierung der Venen in der Handfläche und Verhaltensmessungen, aber es ist weitaus schwieriger und umständlicher, sie anzuwenden. Gesichtserkennung verläuft **einfach, schnell, automatisch und nahtlos**.

Gesichtserkennungssysteme können sehr große Mengen von Bildern verarbeiten. Die britische Polizei benutzt ein System der japanischen Firma NEC namens *NeoFace*, das 300 Gesichter pro Sekunde erfassen und identifizieren kann.

Fehler, ja ... ... dennoch ist Gesichtserkennung nur schwer zu täuschen

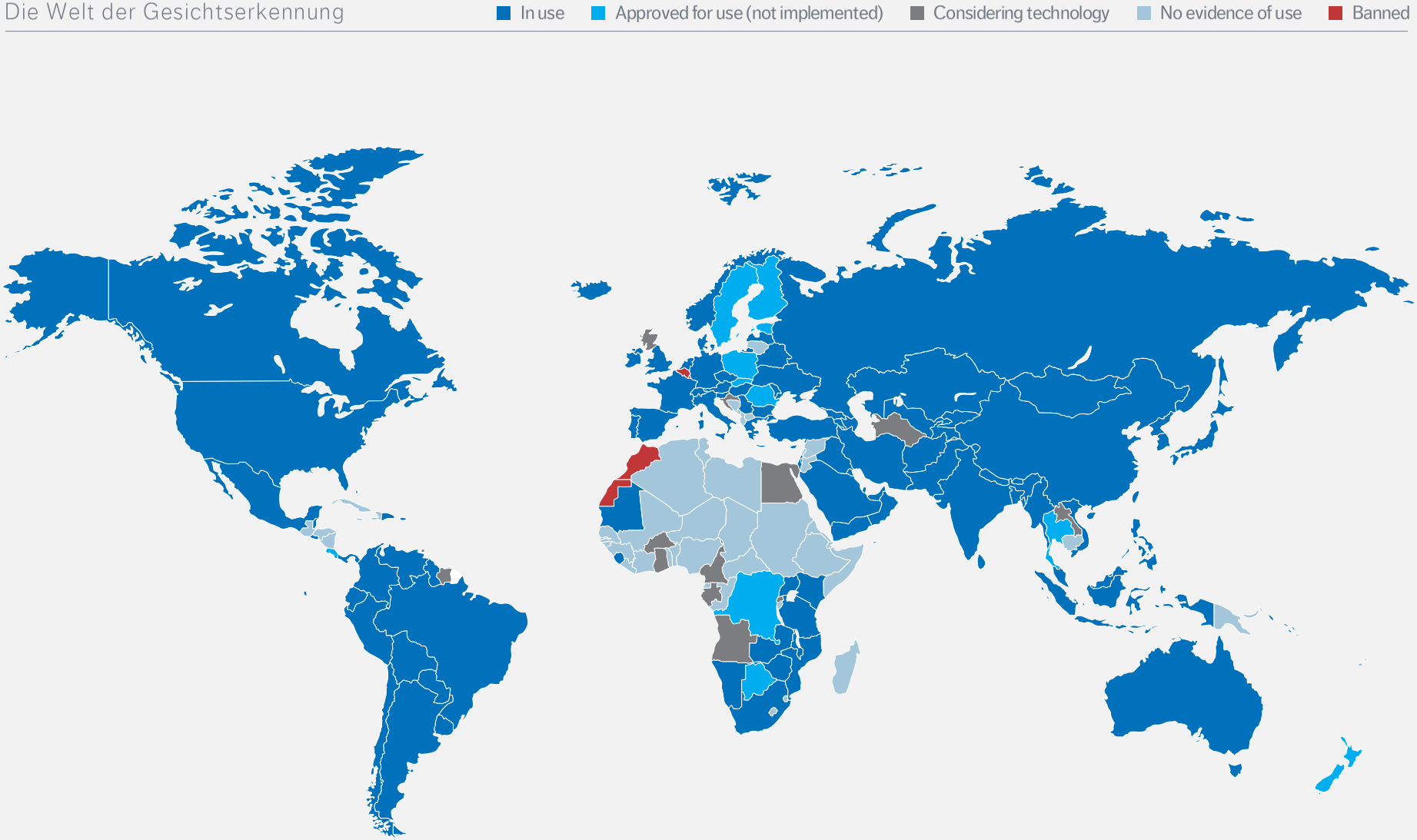
Menschenrechtler zeigen in den sozialen Medien, wie unterschiedliche Frisuren und Make-up Gesichtserkennungssysteme täuschen können.

Aber nicht jeder möchte so aussehen und herumzulaufen!

Gesichtserkennung – weltweit präsent

Die Technologie wird beinahe weltweit eingesetzt, mit nur wenigen Ausnahmen. Belgien gehört dazu.

Abbildung 1:
Die Welt der Gesichtserkennung

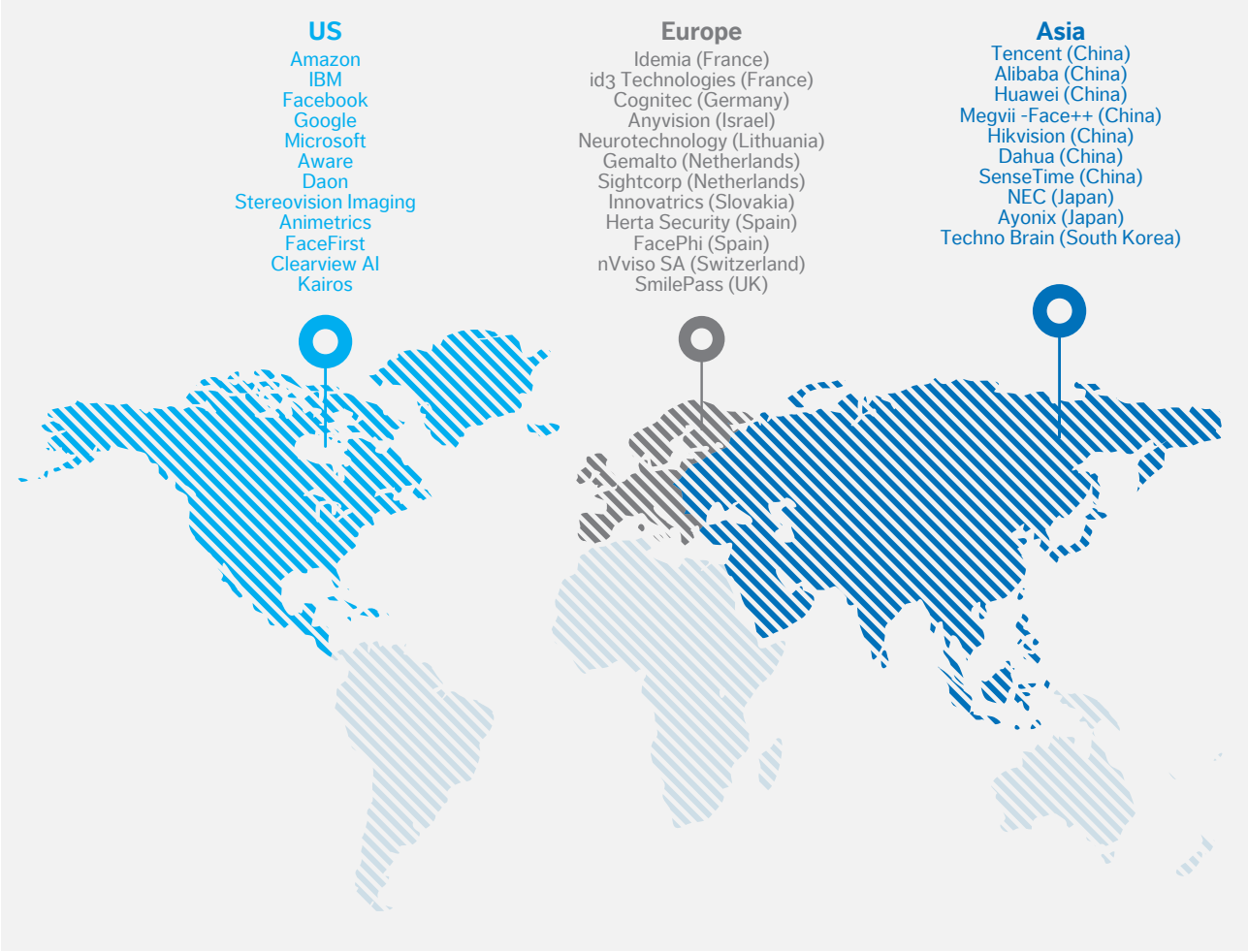


Quelle: visualcapitalist.com, Mai 2020; and Candriam

Marktgröße und wesentliche Akteure

Gemäß einer Umfrage aus dem Jahr 2018 von Allied Market Research[2] dürfte der Markt für Gesichtserkennung bis 2022 auf 9,6 Milliarden USD anwachsen, was einem **Jahreswachstum von knapp 25 Prozent** entspricht. Aber insgesamt gesehen handelt es sich um eine Marktnische. Einige Technologieriesen wie Amazon bieten ihre Systeme kostenlos als **Teil einer lukrativeren Service-Pauschale** an.

Abbildung 2:
Marktteilnehmer



Quelle: Candriam

Risiken und Kontroversen

Im letzten Jahrzehnt beunruhigte der Einsatz von Gesichtserkennung bei der Überwachung von Menschenmengen die Gesellschaft und führte zu Menschenrechtsverletzungen.

Invasive Technologie

Die Überwachung mit Gesichtserkennung **betrifft viele von uns**, in vielen Fällen **ohne unser Wissen**, wenn wir unserem Alltag nachgehen. Sie kann die Massenüberwachung erleichtern und die Menschenrechte verletzen.

Doch verlassen sich auch Millionen Menschen auf die Technologie und begrüßen sie. Viele Apple iPhone Benutzer verwenden Face ID, um ihre Smartphones zu entsperren. Millionen sind bei automatischen biometrischen Grenzkontrollsystemen wie dem britischen ePassport angemeldet.

Auf der ganzen Welt wendet die Polizei bereits Gesichtserkennung im großen Maßstab an. **Ende 2021 sind schätzungsweise 1 Milliarde Überwachungskameras in Betrieb**.[3] China steht heute an der Spitze mit rund 600 Millionen Kameras – eine Kamera für 2,3 Bürger. Knapp dahinter kommen die USA, wo ca. 140 Millionen Kameras installiert sind – eine Kamera für 2,4 Bürger. Die meisten sind digitale Systeme, deren Aufnahmen mit Gesichtserkennungssystemen kompatibel sind.

Heute gehen die Einwohner von Detroit, London, Monaco, Moskau, Beijing und anderen Städten durch die Straßen, ohne daran zu denken, dass ihre Gesichter von polizeilichen Gesichtserkennungssystemen erfasst werden.

Probleme mit der Genauigkeit

Im Januar 2020 wurde Robert Williams in Detroit wegen Ladendiebstahls festgenommen, nachdem ihn die Polizei anhand eines Gesichtserkennungssystems irrtümlich identifiziert hatte.

2018 wurde das System von Amazon, *Rekognition*, mit Mitgliedern des amerikanischen Kongresses getestet, von denen 28 als ehemalige Straftäter identifiziert wurden.[4] Der Test zeigte zudem, dass die Technologie eine ethnische Voreingenommenheit aufweist, denn afroamerikanische Kongressmitglieder wurden im Rahmen des Abgleichs unverhältnismäßig oft falsch identifiziert, da sie mit der Datenbank der festgenommene Personen übereinstimmten. Einer von Ihnen war der 2020 verstorbene John Lewis, Täger der Presidential Medal of Freedom.

Sogar die genauesten heute verfügbaren Systeme sollten zum Nachdenken anregen. Stellen wir uns die Polizei einer Kleinstadt vor, die Gesichtserkennung mit einer Genauigkeit von 99,9% Prozent einsetzt und in der täglich 100 000 Menschen mit Überwachungskameras aufgenommen werden. Wer kann es sich leisten, jeden Tag 100 Menschen falsch zu identifizieren?

Seit der Einführung des Gesichtserkennungssystems der Londoner Polizei im Jahr 2016 beträgt die Fehlerquote 93,59 Prozent. In zwei der drei Einsätze 2020 irrte sich das System sogar zu 100 Prozent und identifizierte keine einzige Person.[6] Auch der unabhängige Prüfungsausschuss der Londoner Polizei kam zu dem Schluss, dass die Gesichtserkennung sehr fehlerhaft war. Er analysierte sechs Tests und fand heraus, dass die Ordnungshüter nur in 19 Prozenten der Fälle recht hatten, die Fehlerquote also bei 81 Prozent lag.[7]

Warum gefährdet die Gesichtserkennung, eine Technologie, die unseren Alltag effizienter und sicherer macht, die Menschenrechte?

Isedua Oribhador, US Policy Analyst bei AccessNow: *„Obwohl man oft hört, dass Gesichtserkennung die Effizienz und die Sicherheit erhöht, beobachten wir bereits, dass sie auch Risiken birgt. Von den Bias in Bezug auf ethnische Herkunft und Geschlecht dieser Systeme über die Datenschutzprobleme, die bei der Erfassung personenbezogener Daten entstehen, bis hin zur Möglichkeit, die breite Bevölkerung zu überwachen, stellt die Gesichtserkennung eine ernste Gefahr für viele Grundrechte dar. Wir müssen diese Risiken prüfen und jene Bereiche abgrenzen, in denen der Einsatz der Technologie nicht mit der Wahrung der Menschenrechte vereinbar ist.“* [7]

„Die chinesische Polizei verwendet ein umfassendes, geheimes Gesichtserkennungssystem, um die 11 Millionen Uiguren, eine hauptsächlich muslimische Bevölkerungsgruppe, zu identifizieren, ihre Spur zu verfolgen und sie zu kontrollieren.“

Ein Land im Fokus – China

Das chinesische Nachrichtendienstgesetz von 2017 zwingt Organisationen und Bürger, „den staatlichen Nachrichtendienst zu unterstützen, ihm zu helfen und mit ihm zusammenzuarbeiten“. Alle Software- und Hardwareunternehmen in China müssen daher Beijing ihre Daten übermitteln, sollten die Behörden sie aus Sicherheitsgründen verlangen.

Ende 2018 waren mehr als 200 Millionen Überwachungskameras in Betrieb, 2020 wurde der Bestand auf mehr als 600 Millionen geschätzt. In den zehn Städten mit den meisten Überwachungskameras pro Person auf Straßen stehen Chongqing, Shenzhen, Shanghai, Tianjin und Ji'nan an der Spitze.

Die Gesichtserkennungstürme in chinesischen Städten sind für diese Entwicklung emblematisch. Die Technologie wird auch in Beijing eingesetzt. Dort sind Polizisten mit intelligenten Brillen ausgestattet, die Gesichter erfassen und das Ergebnis der Abgleichung anzeigen.

Die Überwachung der Zivilbevölkerung in China ist mit dem landeseigenen sozialen Punktesystem verbunden, das Einzelpersonen aufgrund ihres Verhaltens benotet. Auf Basis dieses Systems, das 2013 eingeführt wurde, werden die Chinesen je nach ihrer Bewertung belohnt oder bestraft.

Die chinesische Polizei arbeitet mit Unternehmen zusammen, die sich mit künstlicher Intelligenz befassen, etwa Yitu, Megvii, SenseTime und CloudWalk. Auch Hardwarehersteller wie Dahua und Hikvision erhalten große staatliche Aufträge. Diese Unternehmen wurden von den USA auf die Schwarze Liste gesetzt, weil sie auch an der Unterdrückung der Uiguren mitwirken.

Dennoch bleibt der Ehrgeiz Chinas in Bezug auf künstliche Intelligenz und Gesichtserkennung bestehen. Bis 2030 will es der Weltmarktführer auf dem Gebiet der künstlichen Intelligenz sein. Der chinesische Staat ist zweifelsohne der größte Investor in den Bereichen Überwachungstechnik, künstliche Intelligenz und Gesichtserkennung.

Unterdrückung der Uiguren

Die Behörden in Xinjiang setzen Gesichtserkennung für die Erstellung ethnischer Profile und die Überwachung ein. Die chinesische Polizei verwendet ein umfassendes, geheimes Gesichtserkennungssystem, um die 11 Millionen Uiguren, eine hauptsächlich muslimische Bevölkerungsgruppe, zu identifizieren, ihre Spur zu verfolgen und sie zu kontrollieren. Sie installierte Gesichtserkennungsgeräte am Eingang mehrerer Moscheen in der Region. Xinjiang war ein wichtiges Übungsgebiet für diese Unternehmen, wo sie ohne die üblichen Einschränkungen Tests ausführen konnten.

Gender- und ethnischer Bias, Datendiebstahl

Bei den ersten Gesichtserkennungsexperimenten wurden Menschen afroamerikanischer und asiatischer Herkunft nicht erkannt. Google musste sich 2015 entschuldigen, als die neue Anwendung *Google Photos* einige Schwarze als „Gorillas“ bezeichnete.

Einer Umfrage des MIT Media Lab im Jahr 2018 zufolge konnten einige Gesichtserkennungsprogramme einen Weißen beinahe perfekt identifizieren, hatte aber sehr große Probleme bei Frauen mit dunklerer Haut.

Clearview AI arbeitet nach eigenen Angaben für mehr als 2 400 Polizeibehörden in den USA. Der CEO des Unternehmens, Hoan Ton-That, ist mit rechtsextremen Bewegungen verbunden. Clearview verwendete unerlaubt Milliarden von Fotos von Facebook, YouTube und Venmo, um die Datenbank aufzubauen.[8] Der CEO und Gründer von Banjo, Damien Patton, trat zurück, als im vorgeworfen wurde, dass er dem Ku Klux Klan angehöre. Damals hatte Banjo einen Gesichtserkennungsauftrag des Bundesstaates Utah über 20 Millionen USD erhalten.

Die großen Technologiekonzerne Amazon, Microsoft und Alphabet, die Mutter von Google, wurden gerichtlich belangt, weil sie die Fotos von Menschen ohne deren Zustimmung eingesetzt hatten, um ihre Gesichtserkennungssysteme zu trainieren und weiterzuentwickeln. Facebook zahlte anlässlich eines Vergleichs im Rahmen des Datenschutzgesetzes des Bundesstaats Illinois 650 Millionen USD.[9] Die von Edward Snowden offengelegten Unterlagen zeigten, dass die amerikanische National Security Agency Millionen von Porträts gesammelt hatte. Den Dokumenten nach sollen die Bilder von E-Mails, Textnachrichten sozialen Medien und Video-Chats stammen.[10]

Missbrauch zur Erzielung illegalen Gewinns

Reporter fanden in Russland heraus, dass der Zugang zum Livestream der Überwachungskameras in Moskau im Dark Net wohl von Polizeibeamten zum Verkauf angeboten wurde. Das Zentrum von Moskau ist von einem dichten Netz aus 175 000 Überwachungskameras überzogen. Die meisten davon sind mit Gesichtserkennung ausgestattet. Da das System in der Cloud angesiedelt ist, können korrupte Beamte ganz einfach ihre eigenen Anmeldedaten zu so günstigen Preisen wie 470 USD anbieten und damit Zugang zum Livestream und den Aufzeichnungen der letzten fünf Tage gewähren.

Über Videokameras hinaus – Überwachung der Massen per Computer, Smartphone, Drohnen ...

Praktisch jedes Smartphone, jeder Computer und jedes Tablet, das heute verkauft wird, ist mindestens mit einer Digitalkamera ausgestattet. Sie alle können ihre Daten in ein Gesichtserkennungssystem einspeisen.

Ebenfalls besorgniserregend ist der Einsatz militärischer Erkennungssysteme auf Drohnen, etwa das ARGUS-IS, das es den Behörden ermöglicht, rund um die Uhr eine Fläche von 26 Quadratkilometern, das heißt die Hälfte von Manhattan, zu überwachen. Diese Systeme sind in der Lage, das Gesicht aller Menschen in diesem Umkreis jederzeit zu erfassen.[11]

Die Probleme

Fehlende Zustimmung

Den Kern der Sache bildet die fehlende Zustimmung. Unternehmen, Staaten, Behörden oder öffentliche Einrichtungen bitten niemanden um dessen Zustimmung. Wenn man sein Foto bei Behörden oder öffentlichen Einrichtungen einreicht, um einen Reisepass, einen Personalausweis oder einen Führerschein zu erhalten, erklärt man sich in den meisten Ländern nicht automatisch damit einverstanden, dass das Foto für die Gesichtserkennung eingesetzt wird. Andere Formen der biometrischen Identifizierung erfordern die Überprüfung der Person. Passanten, deren Gesicht von Erkennungssystemen aufgenommen und identifiziert werden, wissen das meistens nicht und haben keine Möglichkeit, dieser Verwendung zuzustimmen oder sie abzulehnen.

Die europäische Datenschutz-Grundverordnung (DSGVO) aus dem Jahr 2016 sieht ausdrücklich vor, dass biometrische Daten, die per Gesichtserkennung erfasst wurden, personenbezogene Daten sind. Sie sind also geschützt und setzen voraus, dass die Person sich mit der Verwendung ihrer biometrischen Daten durch eine andere Person, ein Unternehmen oder eine Behörde einverstanden erklärt. Dennoch benutzen die Ordnungskräfte in den EU-Staaten, etwa in Großbritannien, Frankreich, Italien und Griechenland, die Technik bereits.

Mangelnde rechtliche Grundlage

In den meisten Ländern kann die Polizei sich nicht auf eine rechtliche Grundlage stützen, um Gesichtserkennung einzusetzen. Die Gesichtserkennung verletzt grundlegende Freiheiten wie den ersten Zusatz der amerikanischen Verfassung und das Menschenrechtsgesetz in Großbritannien.

Clare Garvie, Center on Privacy & Technology, Georgetown Law, erklärt Candriam: *„In den USA ist der Einsatz der Gesichtserkennung durch die Polizei eine Grauzone, obwohl auf bundesstaatlicher und lokaler Ebene versucht wird, sie zu verbieten, und sie in jüngster Zeit zur Festnahme von drei Unschuldigen geführt hat. Angesichts der Risiken für die Rechte, die in der amerikanischen Verfassung verankert sind, wie Schutz der Privatsphäre, Meinungsfreiheit, faire Gerichtsverfahren und gleicher Schutz durch das Gesetz, muss die Gesichtserkennung eingestellt werden, bis umfassende Vorschriften diese Rechte angemessen schützen.“*

Mangelnde Aufsicht

In den meisten Ländern, etwa in der EU und in den USA, gibt es kaum unabhängige Aufsichtsbehörden, die mit der Kontrolle der von Privatunternehmen und Ordnungskräften eingesetzten Überwachungstechniken beauftragt sind.

Unverhältnismäßiger Eingriff

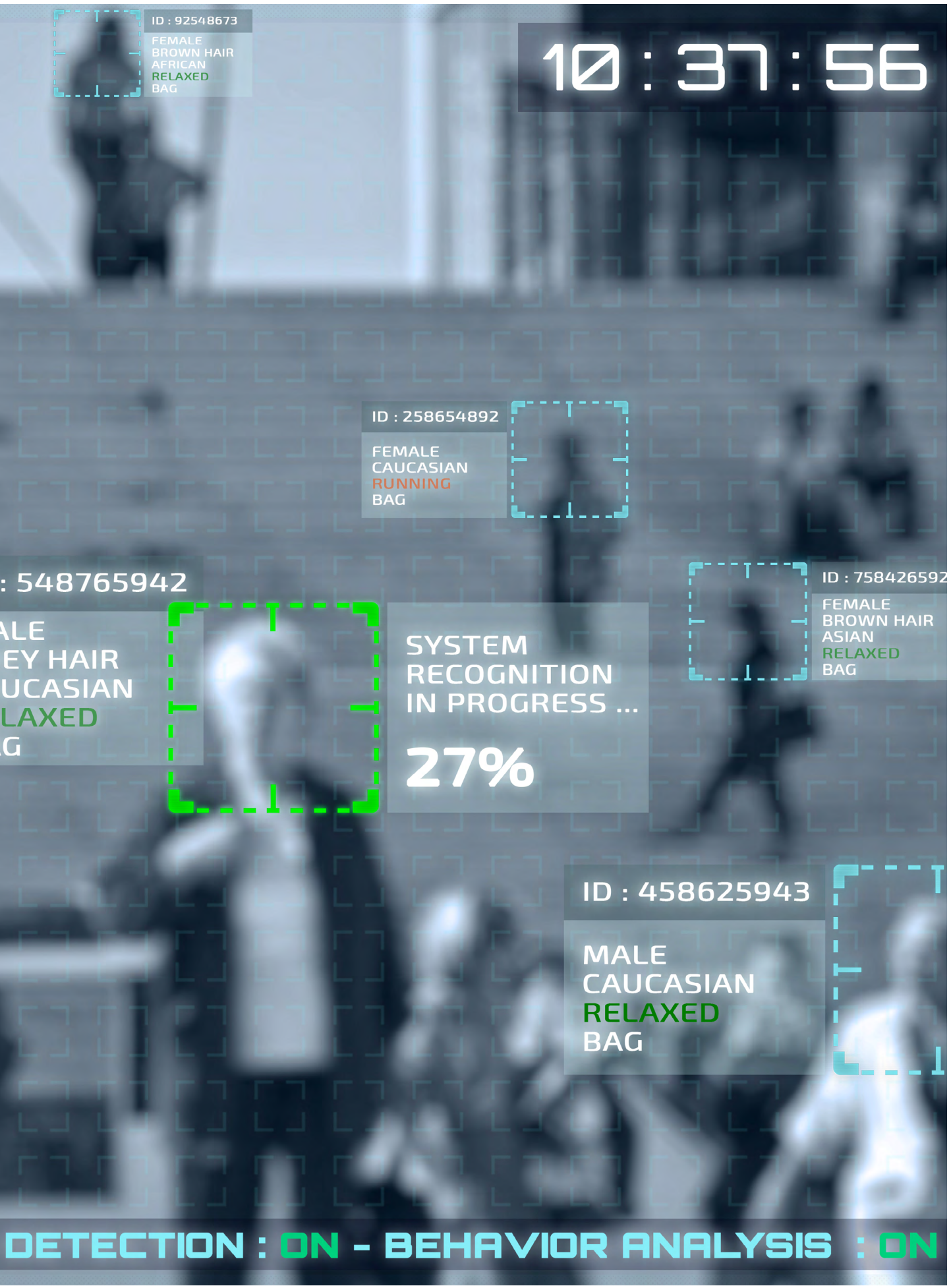
Anlässlich der vielen Testeinsätze in Großbritannien wurde ein gesuchter Straftäter pro 300 000 erfasste Gesichter identifiziert. Der Surveillance Camera Commissioner schloss aus diesem Ergebnis, dass der Eingriff sehr unverhältnismäßig war, weil „gemessen an Umfang und Größe der Daten aller Personen, die an einer Kamera vorbeigehen, die Gruppe, die man identifizieren will, verschwindend klein ist".

Recht auf Anonymität

Eine florierende Gesellschaft baut auf Freiheiten auf – Meinungsfreiheit, Freizügigkeit, Religionsfreiheit, Vereinigungsfreiheit – und auf dem Recht, anonym zu bleiben. Unsere Fähigkeit, uns anonym im öffentlichen Raum zu bewegen, ist seit dem weit verbreiteten Einsatz von Gesichtserkennungssystemen nicht mehr gewährleistet. Jeder sollte in der Lage sein, sich frei und anonym fortzubewegen. Es gehört zur menschlichen Natur, ein Leben anzustreben, in dem man nicht ständig über die Schulter sehen muss. Aber der Umfang des Lebens außerhalb öffentlicher Überwachung schrumpft rasant. Die Identifizierung durch Polizei, Unternehmen oder Behörden, wo auch immer wir sind, hemmt unsere Individualität. Letztlich dürfte sie die Bewegung, die Kreativität, das Vertrauen und sogar die Demokratie einschränken.

Der Bericht des Ethik-Panels der Londoner Polizei über die Gesichtserkennung belegt, dass 38 Prozent der 16- bis 24-Jährigen sowie viele Schwarze, Asiaten und Mitglieder ethnischer Minderheiten sich von Events und Orten fernhalten würden, die Gesichtserkennung einsetzen.[12]


CAM 3
ID : 254876592
MALE
BROWN HAIR
CAUCASIAN
STRESSED
ID
MA
GR
CA
RE
BA
BIOMETRIC IDENTIFICATION : ON - OBJECTS


ID : 92548673
FEMALE
BROWN HAIR
AFRICAN
RELAXED
BAG
10 : 37 : 56
ID : 258654892
FEMALE
CAUCASIAN
RUNNING
BAG
: 548765942
ALE
EY HAIR
UCASIAN
LAXED
G
SYSTEM
RECOGNITION
IN PROGRESS ...
27%
ID : 758426592
FEMALE
BROWN HAIR
ASIAN
RELAXED
BAG
ID : 458625943
MALE
CAUCASIAN
RELAXED
BAG
DETECTION : ON - BEHAVIOR ANALYSIS : ON

Ist die Sicherheit einen kleinen Datenschutzverlust wert?

Auf die Frage nach ihrer Meinung zur Gesichtserkennung antworten viele, dass sie, wenn sie sich sicher fühlen wollen, eben ein bisschen Datenschutz aufgeben müssen. Das Argument, dass man mit den Systemen schnell einen verdächtigen Terroristen oder ein entführtes Kind finden könnte, überzeugt.

Die Überwachungsbranche schürt diese Ängste, um ihre Produkte zu vermarkten. Etwa die Angst vor Terroranschlägen. Nizza war 2016 Schauplatz eines schrecklichen Anschlags. Ein Terrorist raste mit einem Lastwagen am französischen Nationalfeiertag in die Menschenmenge und tötete 87 Passanten. Daraufhin rüstete die Stadt die örtliche Polizei mit den umfassendsten Gesichtserkennungs- und Überwachsungssystemen in ganz Frankreich aus.

Als verantwortungsbewusste Bürger stellen wir uns aber die Frage:

- Wollen wir ständig von ungetesteten und möglicherweise ungenauen oder voreingenommenen Algorithmen identifiziert werden?
- Wollen wir, dass die Behörden jeden Schritt, den wir machen, jeden Ort, den wir besuchen, und alle Personen, die wir treffen, aufzeichnen?
- Wollen wir, dass die Polizei die Namen aller Teilnehmer an einer Demonstration oder einer religiösen Veranstaltung herausfinden kann?
- Wollen wir unseren Behörden die unbegrenzte Macht zugestehen, alle überall und jederzeit zu überwachen?

Eine schizophrene Gesellschaft?

Wenn wir zulassen, dass unsere Behörden und die Polizei Überwachungstechnik einsetzt, um unsere Sicherheit zu gewährleisten, behaupten wir gleichzeitig, dass unsere Sicherheit die permanente Überwachung aller voraussetzt. Manche Soziologen halten diese Einstellung für schizophren.

Kulturelle Unterschiede bei der Akzeptanz der staatlichen Überwachung

Wir können die Verletzung der Menschenrechte durch die Gesichtserkennung nur aus der Sicht westlicher Werte betrachten. Die Wahrnehmung von Privatsphäre und Intrusion hängt stark von der jeweiligen Kultur ab. Die meisten Chinesen meinen, Massenüberwachung sei erforderlich, um die Sicherheit zu gewährleisten. In den letzten Jahren führte die Kombination aus massiver Überwachung und Einführung eines sozialen Benotungssystems (Box, Seite 13) zu einem jähen Rückgang der Kriminalität.

Endlose Gegenüberstellung

Das Centre for Privacy and Technology von Georgetown Law ist der Ansicht,[13] dass niemand freiwillig an einer Gegenüberstellung teilnehmen würde, bei der ein Opfer den vermeintlichen Straftäter aussucht! Das Opfer könnte jemanden irrtümlich identifizieren. Gesichtserkennungssystemen passiert das täglich, sowohl in den USA als auch in China.[14]

Überwachungskapitalismus

Shoshana Zuboff definiert in ihrem Buch „Das Zeitalter des Überwachungskapitalismus" diese Art des Kapitalismus als die Bereitstellung kostenloser Dienstleistungen, die Milliarden von Menschen fröhlich in Anspruch nehmen und die es den Anbietern ermöglichen, das Verhalten dieser Nutzer überraschend genau zu verfolgen – oft ohne deren ausdrückliche Zustimmung. „Überwachungskapitalismus behauptet einseitig, dass die menschliche Erfahrung ein kostenloser Rohstoff ist, der in Verhaltensdaten verwandelt werden darf." Überwachungskapitalisten erzielen einen enormen finanziellen Nutzen, indem sie die individuellen oder kollektiven Verhaltensdaten zu Geld machen und Prognosen aufstellen, was die Menschen voraussichtlich tun werden.

Staatliche Überwachung und Überwachungskapitalismus bewirken zusammen, dass die digitale Technologie **alle Gesellschaften in zwei Gruppen teilt, die *Überwacher* – unsichtbar, unbekannt und ungebremst – und die *Überwachten***. Diese Entwicklung hat ernsthafte Folgen für die Demokratie, da asymmetrisches Wissen zu asymmetrischer Macht führt. Während die meisten demokratischen Gesellschaften die staatliche Überwachung zumindest zu einem gewissen Grad kontrollieren können, gibt es derzeit so gut wie keine gesetzliche Regelung für die private Überwachung.[15]

Engagement – Praktischer Leitfaden

Als verantwortungsvoller Anleger berücksichtigen wir die Faktoren Umwelt, Soziales und Unternehmensführung (ESG) in unsere Investmententscheidungen und treten als aktive Aktionäre auf. Wir sind bestrebt, für unsere Kunden langfristig Wert zu schaffen, indem wir die Wirtschaft, die Umwelt und die Gesellschaft insgesamt positiv beeinflussen.

Wir sind überzeugt, dass die Integration des gesamten Bildes der Gesichtserkennungstechnologie in unsere Investments und unseren Dialog mit den Unternehmen zu beiden Teilen unseres Ziels beiträgt. Immer mehr Unternehmen, Staaten und Regionen, in die wir investieren, setzen diese Technologie ein. Obwohl wir wahrscheinlichl nicht gezielt in einen reinen Gesichtserkennungsanbieter investieren würden, erfordern Anlagen in ein Unternehmen, das Gesichtserkennung einsetzt oder verkauft, umfassende Due-Diligence-Prüfungen. Sie verfolgen den Zweck:

- die damit verbundenen Risiken zu bewerten
- unsere Bedenken bezüglich möglicher Risiken mit den Unternehmen zu besprechen
- alle Maßnahmen zur Risikominderung zu unterstützen

Wie in unserer Beschreibung der Technologie und deren Probleme erwähnt, sind die Erwartungen der Anleger unterschiedlich, komplex und hängen von den einzelnen Stakeholdern ab. Einige Vorgaben:

Unternehmen

- **Direktes und/oder kollaboratives Engagement**, um die Unternehmenspraktiken besser zu verstehen. Best-Practices über Gespräche mit Unternehmen, Nichtregierungsorganisationen usw. ausbauen

- **Integration der Entwicklungen in die ESG-Analyse** der Unternehmen. Best-Practices bestimmen, akzeptable Fortschritte und Ausschlüsse definieren.

- **Förderung besseren Unternehmensverhaltens**. Ethik und Menschenrechte weiterhin in den Mittelpunkt der Unternehmensführung stellen. Einen unabhängigen Menschrechtsausschuss bilden, der dem Vorstand untersteht. Unternehmen dazu auffordern, Kunden und Lieferanten zu suchen, die sich ihren Werten verpflichten.

Staaten

- **Forderung nach Einstellung der Gesichtserkennung durch die Polizei** bis einschlägige Vorschriften eingeführt sind.

Universitäten

- **Förderung des Ethik-Unterrichts** in KI/Tech-Studiengängen.

Obwohl wir diese Themen mit den europäischen Behörden erörtern wollen, ist der Dialog mit den Unternehmen und vor allem den Emittenten, deren Titel wir bereits in unseren Portfolios halten, wohl die beste sofortige Lösung.

Vor diesem Hintergrund und auf der Grundlage von Gesprächen mit Experten und Spezialisten der Gesichtserkennung führen wir unten eine Reihe von Fragen (Abbildung 2) auf, die den Anlegern helfen sollen, die Beteiligung der Unternehmen an Gesichtserkennungstechnik und die damit verbundenen eventuellen Verletzungen der Menschenrechte besser einzuschätzen.

Open MIC arbeitet seit einigen Jahren mit Investoren zusammen, um Technologieunternehmen zu veranlassen, ethische Praktiken in Bezug auf Gesichtserkennung einzuführen.

Die großen Technologiekonzerne widmen dem Widerstand gegen diese Bemühungen viel Energie und Geld. Trotz des deutlichen Drucks der Aktionäre – und zahlreicher Menschenrechtsorganisationen auf internationaler Ebene – wollen die Unternehmen meistens nicht zugeben, dass Gesichtserkennung problematisch ist. Wie dieser Bericht unterstreicht, funktionieren beinahe alle Gesichtserkennungsprodukte auf dem Markt ohne die Zustimmung der Millionen von Menschen, deren Gesichter täglich erfasst werden. Viele Systeme verzeichnen zudem eine noch höhere Fehlerquoten bei der Erkennung nichtweißer Personen. Es gibt weder Abhilfe noch Rechtsmittel für jene, deren Rechte verletzt wurden, obwohl die Leitprinzipien für Wirtschaft und Menschenrechte der Vereinten Nationen das Gegenteil vorsehen. 2019 empfahl der Sonderberichterstatter der Vereinten Nationen für Meinungs- und Ausdrucksfreiheit „eine sofortige Einstellung des internationalen Vertriebs und der Übertragung von Überwachsungstechniken, bis strenge Vorschriften für die Berücksichtigung der Menschenrechte eingeführt worden sind". Solche Vorschriften wurden nicht verabschiedet und der Verkauf wurde nicht verboten. Wie dieser Bericht andeutet, boomt der Markt sogar.

Es stellt sich die Frage, ob die Aussicht auf Regulierungen und Gesetze – in der EU und den USA – die Unternehmen dazu veranlasst, freiwillig wirksame Branchenstandards einzuführen. Zweifelsohne versuchen die Konzerne, über ihre Lobbygruppen die Einschränkungen der Gesichtserkennung zu verwässern. Die Anleger sollten das machen, was sie bereits tun, das heißt alle ihnen zur Verfügung stehenden Instrumente einsetzen, um die Technologiekonzerne zur Einführung von Richtlinien und Praktiken zu veranlassen, die einen Unterschied machen. Es ist zu hoffen, dass ein umfassendes und lautstarkes Engagement, wie es hier vorgeschlagen wird, die Unternehmen dazu anspornt, einen produktiveren Dialog zu führen.

Michael Connor ist Gründer und Executive Director von Open MIC. Die Non-Profit-Organisation setzt sich dafür ein, die Rechenschaftspflicht der Unternehmen im Medien- und Technologiesektor hauptsächlich durch das Stakeholder-Engagement zu fördern. In Zusammenarbeit mit sozial verantwortungsvollen Anlegern identifiziert, entwickelt und unterstützt Open MIC Kampagnen, die Offenheit, Fairness, Privatsphäre und Vielfalt fördern, das heißt Werte, die Personen, Unternehmen und der Gesundheit der demokratischen Gesellschaft langfristigen Nutzen bringen. Open MIC arbeitet derzeit an Kampagnen, die Amazon, Twitter, Google und Facebook im Visier haben.

Engagement-Leitfaden

Ausmass der beteiligung

- Liefert Ihr Unternehmen Produkte (Hardware, Software, Datenbanken) für die Gesichtserkennung?

- Welchen Zweck hat das Produkt?
  - Überwachung
  - Identifizierung
  - Kontrolle
  - Kategorisierung (z.B. gezielte Werbung)
  - Ermittlung
  - Sicherheit
  - Sonstiges (bitte angeben)

- Welche Nutzer versorgen Sie mit Gesichtserkennungstechnik?
  - Behörden oder Staaten
  - Schulen
  - Ordnungskräfte
  - Unternehmen
  - Heer

Governance

- Hat Ihr Unternehmen eine öffentliche Richtlinie zur Gesichtserkennung eingeführt? Wenn ja, welche Auswirkungen hat diese Verpflichtung
  1) auf ihre Beziehungen zu Geschäftspartnern, z.B. Lieferanten, Subunternehmen, Kunden, Endnutzer? und
  2) auf ihre Lobbying-Bemühungen?

- Welche Risiken haben Sie in Bezug auf Gesichtserkennung identifiziert und wie oft melden Sie dem Vorstand diese Risiken?

- Führt Ihr Unternehmen Prüfungen durch, um die tatsächlichen und möglichen Menschenrechtsverletzungen durch Ihre Gesichtserkennungstechnik zu bestimmen und einzuschätzen? Welche Risiken haben Sie identifiziert und welche Stakeholder hat an dieser Einschätzung mitgewirkt? Wie haben Sie Ihren Betrieb und Ihre Strategie angepasst? Wer im Unternehmen (auf Ebene des Unternehmens, der Region, der Standorte) trägt die allgemeine und die laufende Verantwortung für diese besonderen Risiken und möglichen Auswirkungen?

- Welche Prozesse haben Sie eingeführt, um zu bestimmen, welchen Kunden Sie die Produkte verkaufen können? Verbieten Sie den Verkauf / die Lieferung Ihres Produkts oder Ihrer Leistung an repressive / undemokratische Regimes?

Steuerung der konzeptionsverbundenen risiken

- Wie sind Sie intern organisiert, um Risiken betreffend Gesichtserkennung zu identifizieren, ihnen vorzubeugen und sie zu lösen?

Insbesondere:

- Wie hat ihr Unternehmen die Training-Datenbank mit Fotos und Namen erstellt, gekauft, sich beschafft? Wenn Sie die Datenbank nicht selbst erstellt haben, wie hat ihr Lieferant sie erstellt, gekauft, sich beschafft?
- Melden Sie die Genauigkeit der Technologie nach Messung durch eine anerkannte Forschungseinrichtung wie das National Institute of Standards and Technology (NIST)? Wenn nicht, wie gehen Sie vor?
- Welche internen Prüfungen führen Sie intern durch, um Verzerrungen des Algorithmus in Bezug auf ethnische Herkunft, Geschlecht oder Alter zu erkennen? Und/oder Ihr/e Lieferant/en?
- Haben Sie eine Beschwerdesystem eingeführt, um Personen, die auf dieser Ebene durch die Technik geschädigt wurden, zu identifizieren und zu entschädigen?

Steuerung der nutzungsverbundenen risiken

- Unterliegen Ihre Kunden Gesetzen und Vorschriften bezüglich der Verwendung der Gesichtserkennung? Befassen Sie sich mit dieser Frage?
- Ermöglicht Ihre Gesichtserkennungstechnik eine Echtzeitanalyse oder nur Analysen im Nachhinein?
- Analysiert Ihr Produkt Livestreams oder nur statische Bilder?
- Bietet Ihre Gesichtserkennungstechnik eine Kategorisierung nach Ethnie, Alter, Geschlecht, Geisteszustand usw.? Bietet Ihre Gesichtserkennungstechnik zukunftsbezogene Analysen?
- Haben Sie eine Beschwerdesystem eingeführt, um Personen, die auf dieser Ebene durch die Technik geschädigt wurden, zu identifizieren und zu entschädigen?

Fazit

Heute ist Gesichtserkennung ein Thema, dem es an Transparenz fehlt. Ihr Einsatz wird von den einen begrüßt, von den anderen abgelehnt. Sie kann missbraucht werden und ist mit Vorurteilen und Fehlern behaftet.

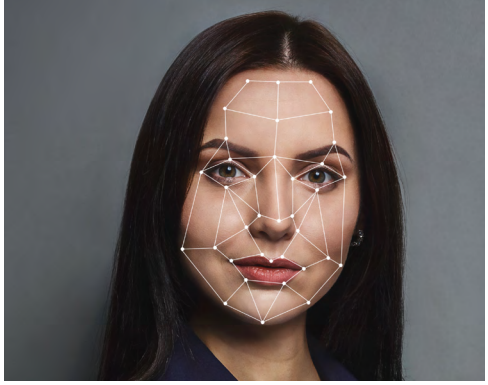
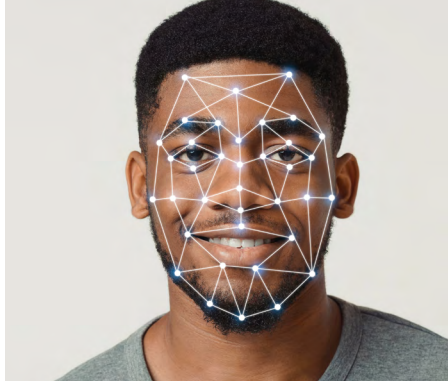
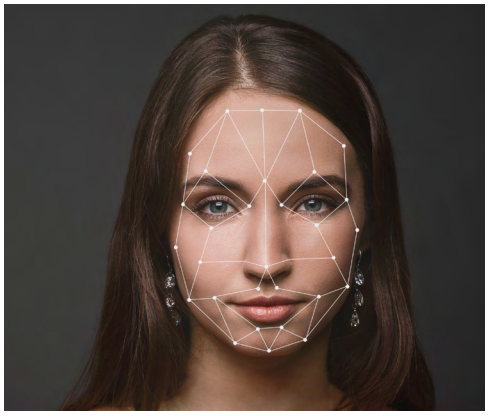
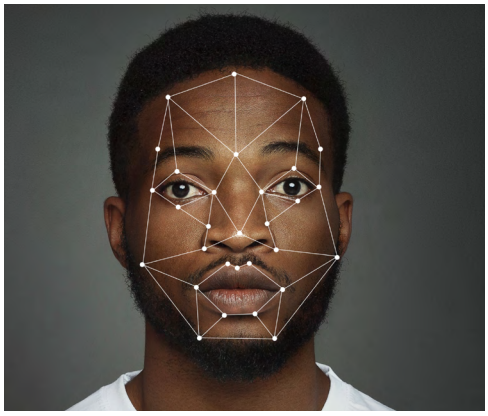
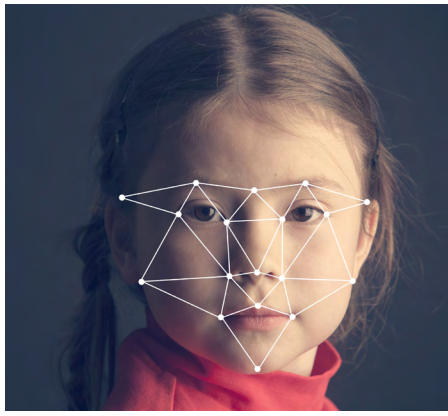
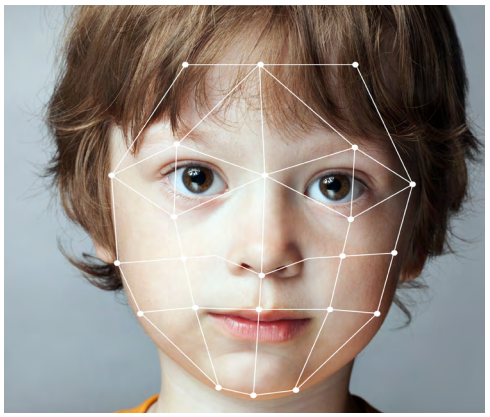
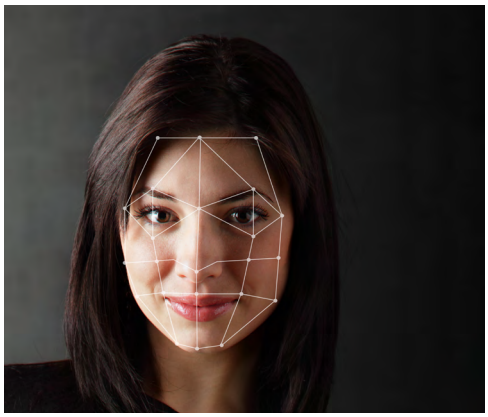
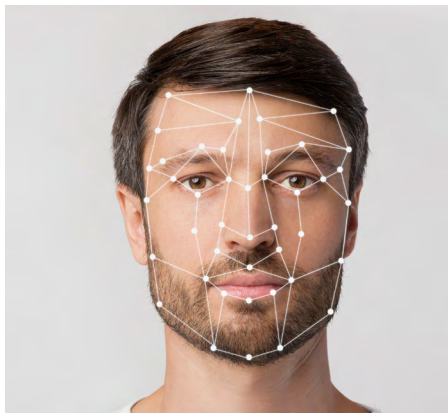
Angesichts der mangelnden Transparenz können wir diese Kontroversen nicht einschätzen. Wir brauchen einen längeren Hebel, um Analysen und Konversationen zu fördern. Nationale und regionale Behörden beginnen, Maßnahmen zu ergreifen. Auch Unternehmen starten allmählich Initiativen. Die Öffentlichkeit nimmt sich der Frage an und Nichtregierungsorganisationen veranstalten Kampagnen.

Jetzt ist es an der Zeit, dass auch Anleger agieren.

Hinweise und Literatur

[1] Mashable.com. *Douglas, the latest step toward realistic AI, is unsettling.* Updated 22 November, 2020. https://mashable.com/article/douglas-realistic-ai-unsettling/?europe=true, accessed 8 February, 2021.
[2] https://www.alliedmarketresearch.com/press-release/facial-recognition-market.html
[3] CNBC. *One billion surveillance cameras will be watching around the world in 2021.* 6 December, 2019. https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html, accessed 8 February, 2021.
[4] The American Civil Liberties Union. ACLU.com. Snow, Jacob. *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. 26 July, 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28, accessed 8 February, 2021.
[5] Metropolitan Police. LIFR Deployments 2020. https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf, accessed 8 February, 2021.
[6] The Human Rights, Big Data and Technology Project. Fussey, Professor Pete and Dr. DaraghMurray. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. July, 2019. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf, accessed 8 February, 2021.
[7] Isedua Oribhabor is AccessNow's US Policy Analyst, also covering Business and Human Rights. Isedua's work with the Leitner Center for International Law and Justice at Fordham sparked her interest in Business and Human Rights, leading her to pursue the topic as it relates to the technology sector. AccessNow is a global non-governmental organization specializing in the defense on human rights in the field of technology. AccessNow focuses on the following fields: privacy, freedom of expression, digital security, business and human rights and net discrimination. AccesNow has an international presence employing 60 staff across 13 countries.

[8] The New York Times. Hill, Kashmir. *The Secretive Company That Might End Privacy as We Know It.* updated 31 January, 2021. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, accessed 8 February, 2021.
[9] CNET News. Musil, Steven. *Amazon, Google, Microsoft sued over photos in facial recognition database.* 14 July, 2020. https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/, accessed 8 February, 2021.
[10] The New York Times. Risen, James and Laura Poitras. *N.S.A. Collecting Millions of Faces From Web Images.* 31 May, 2014. https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html, accessed 8 February, 2021.
[11] University of Richmond Law Review. Laperruque, Jake. *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance.* March 2017. http://lawreview.richmond.edu/files/2017/03/Laperruque-513-website.pdf, accessed 8 February, 2021.
[12] http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf
[13] Georgetown Law Center on Privacy & Technology. Garvie, Clare; Alvaro Bedorya, and Jonathan Frankle. *The Perpetual Line-Up: Unregulated Police Face Recognition in America.* https://www.perpetualline-up.org/, accessed 8 February, 2021.
[14] This concept was again used in the Arte TV documentary by Sylvain Louvet called "Tous surveillés, 7 milliards de suspects" (Everyone is being watched, 7 billion suspects). This documentary won the Albert Londres price (highest French Journalism award) for best documentary in 2020.
[15] The Guardian. Naughton, John. *'The goal is to automate us': welcome to the age of surveillance capitalism.* 20 January, 2019. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook, accessed 8 February, 2021.

140 Mds €

verwaltetes Vermögen
zum 31. Dezember 2020

570

experten in
Ihrem Dienst

25 Jahre

Vorreiter für
nachhaltiges Investieren

CANDRIAM. INVESTING FOR TOMORROW.

WWW.CANDRIAM.COM

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY