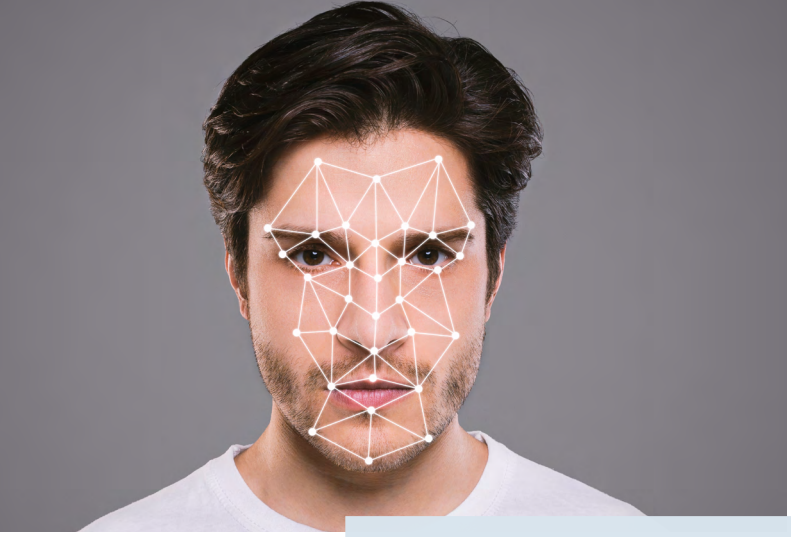
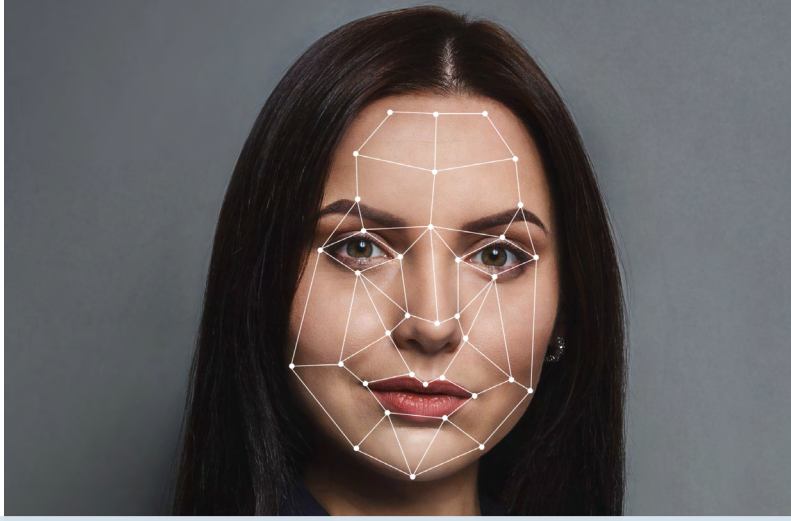
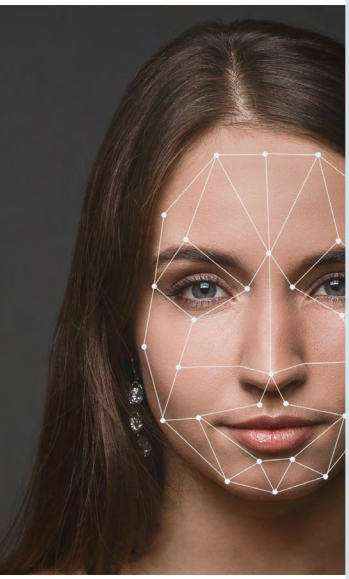
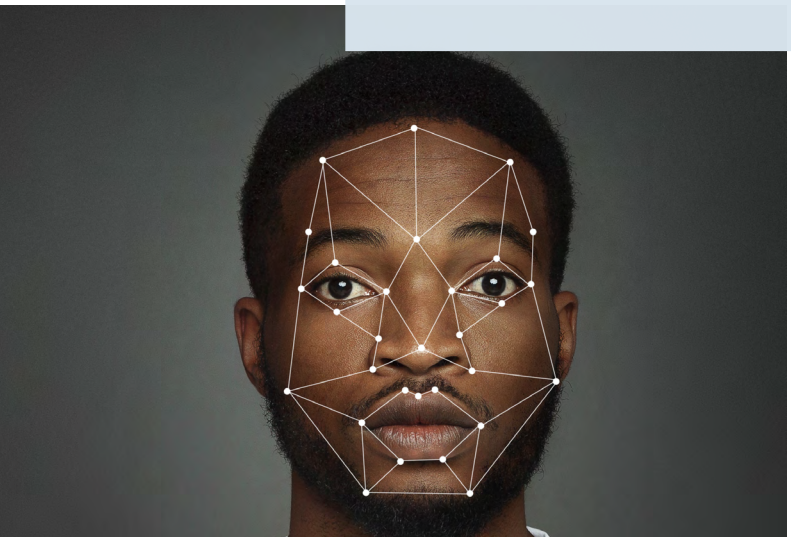
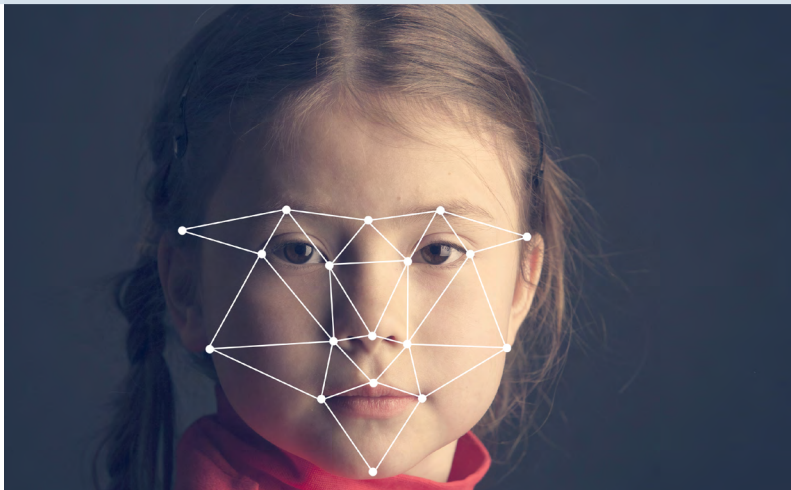




Maart 2021

Gezichtsherkenning en mensenrechten: Richtlijnen voor beleggers

CANDRIAM

A NEW YORK LIFE INVESTMENTS COMPANY

Over de auteurs

Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement

Benjamin Chekroun trad in 2018 in dienst bij Candriam als Deputy Head of Convertible Bonds en begon in 2020 in zijn huidige functie in Stewardship. Daarvoor werkte hij sinds maart 2014 bij ABN AMRO Investment Solutions, waar hij verantwoordelijk was voor de wereldwijde strategie voor converteerbare obligaties. Hij woonde vier jaar in Hongkong, één jaar in New York en dertien jaar in Londen, waar hij werkte als trader in converteerbare obligaties. In 2004 werd het door dhr. Chekroun beheerde fonds door Hedge Fund Review bekroond als Beste Convertible Arbitrage Fund. Benjamin behaalde een masterdiploma in internationale handelswetenschappen.

Sophie Deleuze

Lead ESG Analyst, Stewardship

Sophie Deleuze begon in 2005 in het ESG-researchdepartement van Candriam. Na meer dan tien jaar als ESG-analist heeft ze zich gespecialiseerd in de activiteiten van Candriam op het vlak van Engagement, Proxy voting en Stewardship, waarbij ze onze interactie met de ESG-analyse en al de beleggingsbeheerteams coördineert. Voor ze bij Candriam begon, werkte ze vier jaar als analist bij BMJ CoreRatings en Arese. Mevr. Deleuze behaalde een ingenieursdiploma in waterbehandeling, en een master in publiek ecologisch beheer.

Quentin Stevenart

ESG Analyst

Quentin vervoegde Candriam's ESG-Team als ESG Analyst in 2016. Hij voert complete ESG-analyses uit van de IT-sector, en van governancekwesties in alle sectoren. Hij stuurt ook het onderzoek naar de circulaire economie van Candriam aan. Hij behaalde een Master in Management aan de Louvain School of Management alsook een Master en Bachelor Handelsingenieur aan de Katholieke Universiteit van Leuven.

Inhoud-sopgave

“Hoewel deze technologie onmiskenbaar potentieel heeft en een positief element kan zijn, houdt de manier waarop gezichtsherkenningstechnologie werd ontworpen en vandaag wordt gebruikt risico's en sociale gevolgen in voor mensen. Dat roept op tot actie van beleggers hieromtrent. Daarom staan we positief tegenover de inspanningen en het intellectuele leiderschap van beleggers, die in aanloop naar de regelgeving de traditionele lijst met ESG-problemen willen uitbreiden. Ze willen begrijpen hoe, waar en wanneer gezichtsherkenning correct kan worden gebruikt, en door wie.”

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

Beknopte samenvatting

Verantwoord beleggen gaat verder dan louter reageren op de risico's en problemen waarmee we vandaag worden geconfronteerd. Het gaat om meer dan enkel de koolstofvoetafdruk en klimaatverandering en de risico's en kansen van de toekomst in kaart brengen.

Dankzij technologie heeft de wereld enkele geweldige tools gekregen, en ook enkele fantastische beleggingen. Dankzij de technologie kunnen veel professionals hun werk tijdens de huidige pandemie vanuit huis voortzetten. Zo voerde president Biden een groot deel van zijn verkiezingscampagne vanuit zijn kelder. Toch moeten we ons er bij elke nieuwe technologie van bewust zijn dat er ongewenste gevolgen kunnen optreden.

Gezichtsherkenningstechnologie (GHT) zorgt voor meer efficiëntie en veiligheid. We maken hiervan gebruik om geavanceerde smartphones te ontgrendelen en om door de luchthavencontroles te geraken. Het heeft ook menselijke gevolgen. Deze technologie is immers al tientallen jaren in ontwikkeling, maar begint nu pas op grote schaal te worden toegepast.

Een enquête van Candriam in 2021 leverde zowat 300 reacties op van beleggers. Van die respondenten is 30% van mening dat Gezichtsherkenningstechnologie een handige en nuttige tool is. Zowat 70% heeft echter bedenkingen. Zo meent 31% dat GHT niet nauwkeurig is, en is 38% van mening dat de ethische overwegingen sneller moeten aansluiten bij de technologie.

De problemen zijn onder meer een gebrek aan toestemming en toezicht. Het aantal gevallen van verkeerde identificatie, wat soms leidt tot abuizen bij arrestaties, neemt toe, vooral bij niet-blanke burgers. In mei 2019 verbood de Amerikaanse stad San Francisco – de bakermat van de gezichtsherkenning – het gebruik ervan bij de rechtshandhaving. Kort daarna kondigden verschillende grote technologiebedrijven een moratorium van één jaar aan op de verkoop van hun gezichtsherkenningsproducten.

Om inzicht te krijgen in de mensenrechtenkwesties die zich in de toekomst zullen stellen, moeten verantwoorde beleggers en andere stakeholders nu een vuist maken.

Deze studie zou niet mogelijk zijn geweest zonder de enorme hulp van de volgende instellingen en personen. We willen hen bedanken voor hun tijd, inzichten en 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*

De technologie

Hoe werkt het?

Gezichtsherkenning maakt deel uit van de familie van biometrische herkenningstechnieken. Dat is het proces waarbij de **identiteit** van een persoon wordt **vastgesteld** of **gecontroleerd** aan de hand van een foto of video van zijn gezicht. Het registreert, analyseert en vergelijkt patronen op basis van de gelaatskenmerken van de persoon. Sommige systemen gebruiken nu al driedimensionale beelden die veel nauwkeuriger zijn.

Gezichtsherkenningstechnologie verloopt in drie belangrijke fasen:

- **Gezichtsdetectie** is een essentieel proces voor het detecteren en lokaliseren van menselijke gezichten op beelden en video's.
- **Gezichtsopname** zet analoge informatie - een gezicht - om in een reeks digitale informatie, of gegevens, die de gelaatstrekken van de persoon weergeven. Tientallen gelaatstrekken zoals de afstand tussen de ogen, de neusbrug, de contouren van de lippen, de oren, de kin, enz. worden gemeten.
- **Gezichtscontrole** gaat na of twee gezichten dezelfde persoon zijn.

Het algoritme leidt tot een resultaat met een bepaalde waarschijnlijkheid, in een statistische vorm zoals "*Positieve overeenkomst - Jan Peeters - 97,36% waarschijnlijkheid*".

Een beknopte geschiedenis van gezichtsherkenning

Gezichtsherkenning gaat al terug tot de jaren 60 van de vorige eeuw. Woody Bledsoe, een Mormoonse bisschop en medeoprichter van Panoramic Research in Palo Alto, ontwikkelde een manier om handmatig de posities van iemands gelaatstrekken in een computer in te voeren. Hoewel dat naar moderne maatstaven niet erg doeltreffend was, toonde het wel aan dat het gezicht biometrisch gezien bruikbaar is. De nauwkeurigheid van de herkenningssystemen verbeterde in de jaren 1970, toen onderzoekers bijkomende gezichtskenmerken toevoegden. De echte vooruitgang kwam er pas in de jaren 1980 en 1990, met nieuwe methoden om een gezicht op een afbeelding te lokaliseren en de kenmerken ervan te exporteren, waardoor volautomatische gezichtsherkenning een optie werd. In 1996 werd er met het FERET-programma van de VS voor het eerst een gezichtsdatabank opgebouwd. Tijdens de Super Bowl van 2001 testte de politie voor het eerst op grote schaal gezichtsherkenning. Toen werden er 19 voortvluchtige criminelen geïdentificeerd in het publiek. De meest spectaculaire vooruitgang werd er geboekt in 2010 en later, toen diepe neurale netwerken de technologie verbeterden. In 2011 hielp gezichtsherkenningstechnologie mee om de identiteit van Osama Bin Laden vast te stellen toen hij bij een Amerikaanse inval werd gedood. Facebook rolde de technologie uit voor het taggen van foto's en in 2014 werd zijn DeepFace-programma het eerste in zijn soort dat bijna even goed als een mens gezichten kon herkennen. In 2017 was de iPhone X de eerste ruim verkrijgbare smartphone die je met gezichtsherkenning kon ontgrendelen, de eerste grootschalige release van gezichtsherkenningstechnologie. In mei 2019 werd San Francisco de eerste grote Amerikaanse stad die het gebruik van gezichtsherkenning door de politiediensten verbood. De zomer daarop beloofde de CEO van IBM om IBM FR of analysesoftware niet langer aan te bieden in het kader van hun "Beginselen van vertrouwen en transparantie". Dat voorbeeld werd gevolgd door grote technologiebedrijven zoals Amazon, Facebook en Microsoft, die een moratorium van één jaar instelden op de verkoop van hun producten.

Om deze stappen uit te voeren moeten bepaalde gegevens en technologieën vooraf beschikbaar zijn en worden gebruikt.

- Een gezichtsherkenningssysteem leert om gezichtspatronen herkennen aan de hand van een **trainingsdatabank** van beelden. Voor een grotere nauwkeurigheid is er een grote, complexe en heterogene trainingsdatabank nodig.

- De technologie voor gezichtsherkenning combineert het gebruik van **Artificiële Intelligentie** (het systeem is in staat om te leren door gegevens te analyseren) **Machine Learning** (het systeem is in staat zijn vermogen om informatie te verwerken en te gebruiken zonder menselijke tussenkomst uit te breiden, door te leren uit eerdere ervaringen), en **Deep Learning** (een nieuwe techniek die in staat is machinaal leren uit te voeren, geïnspireerd op de manier waarop neurale netwerken in het menselijk brein werken).

Toepassingen

Gezichtsherkenningstechnologie voert gewoonlijk één of een combinatie van deze taken uit:

Identificatie
"Wie bent u?"

Authenticatie
"Bent u echt degene die u beweert te zijn?"

Categorisering
"Tot welke groep/categorie behoort u?"

Gezichtsherkenningssystemen worden hoofdzakelijk gebruikt voor beveiliging en rechtshandhaving, maar ook in de geneeskunde en marketing. De lijst met toepassingen groeit snel aan.

- **Rechtshandhaving** -- om verdachte criminelen/terroristen op te sporen, een vermiste persoon te vinden, de toegang te controleren, een menigte in bedwang te houden
- **Beveiliging** -- om een deur/telefoon/systeem te ontgrendelen, een transactie te valideren, passagiers op een luchthaven te controleren
- **Scholen** -- met het oog op bescherming, om de aanwezigheid en aandachtigheid op te volgen
- **Geneeskunde** -- om een klein maar potentieel groeiend aantal aandoeningen te diagnosticeren, om pijnbestrijding te evalueren
- **Sociale media** -- om mensen op foto's te identificeren
- **Marketing** -- om 'SMART' advertenties te voorzien
- **Interactie tussen mens en machine** -- Autonome digitale mensen zullen binnenkort in contact staan met mensen en hun reactie aanpassen op basis van gezichtsherkenning.[1]

Voordelen

Wij herkennen elkaar niet door naar onze vingerafdrukken of de patronen in onze irissen te kijken, maar door naar elkaars gezicht te kijken.

Gezichtsherkenning wordt beschouwd als de **meest natuurlijke van alle biometrische metingen**, omdat er geen fysieke interactie vereist is van de eindgebruiker. Er bestaan andere handtekeningen van het menselijk lichaam, zoals vingerafdrukken, irisscans, stemherkenning, digitalisering van de aders in de handpalm, en gedragsmetingen, maar deze zijn moeilijker en omslachtiger te implementeren. Gezichtsherkenning is gemakkelijk toegankelijk, snel, automatisch en werkt naadloos.

Gezichtsherkenningssystemen kunnen enorme hoeveelheden beelden verwerken. De Britse politie gebruikt bijvoorbeeld een systeem van het Japanse bedrijf NEC, *NeoFace* genaamd, dat tot 300 gezichten per seconde kan scannen en identificeren.

Vergissingen, ja... ...maar gezichtsherkenningssystemen kan je niet zo makkelijk foppen.

Mensenrechtenactivisten hebben sociale media gebruikt om combinaties van haarstijlen en cosmetica te demonstreren die doeltreffend kunnen zijn om gezichtsherkenningssystemen te foppen.

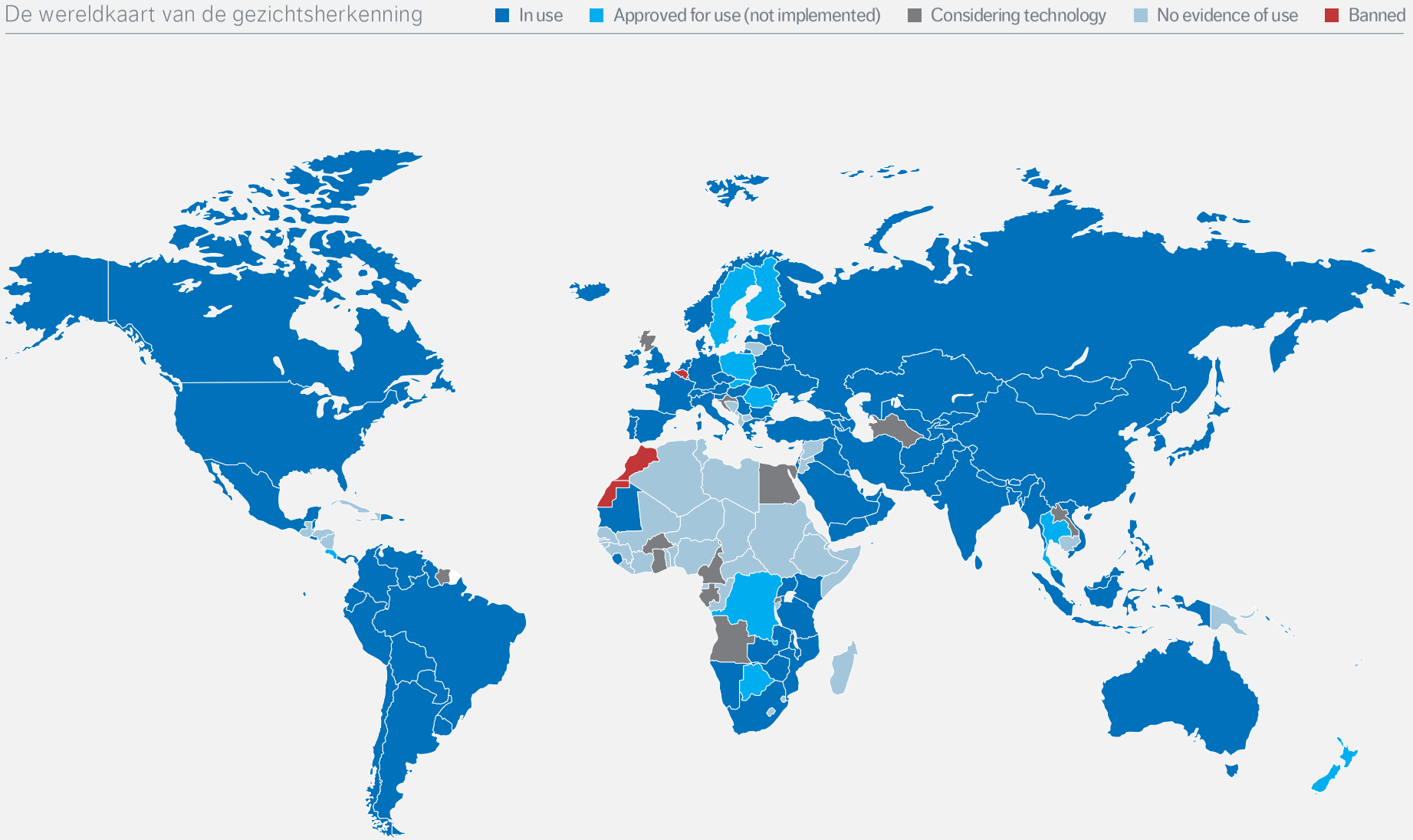
Maar niet iedereen wil er zo uitzien!

Gezichtsherkenning – Wereldwijde aanwezigheid

De technologie wordt vrijwel overal ter wereld gebruikt, met een beperkt aantal uitzonderingen. België is één van die uitzonderingen.

Afbeelding 1:

De wereldkaart van de gezichtsherkenning



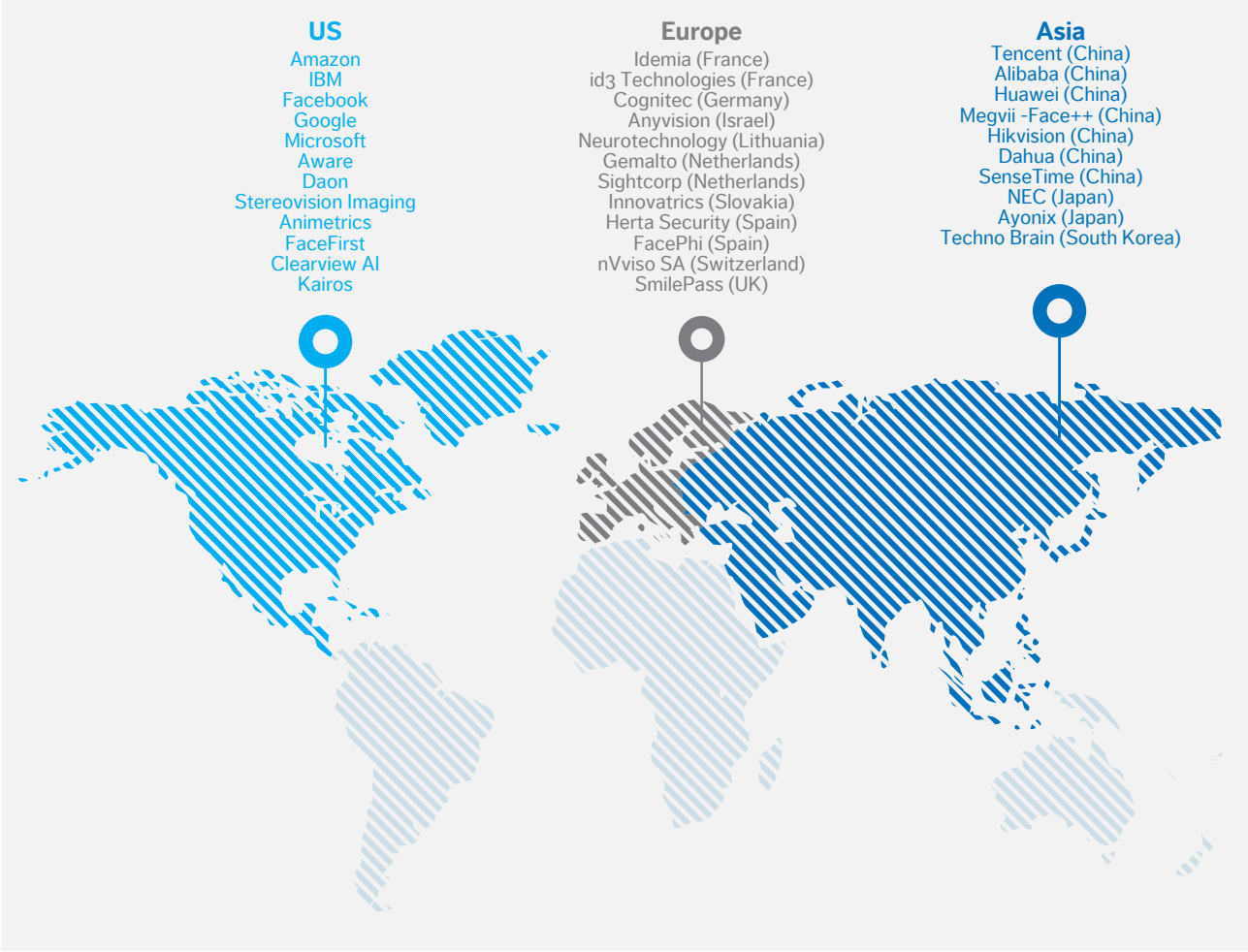
Bron: visualcapitalist.com, mei 2020, en Candriam

Grootte van de markt en belangrijkste spelers

Volgens een onderzoek uit 2018 door Allied Market Research[2] zal de markt voor gezichtsherkenning tegen 2022 aangroeien tot 9,6 miljard dollar, goed voor een **jaarlijks groeipercentage van bijna 25%**. Maar al bij al blijft dit een nichesector. Het ziet ernaar uit dat sommige technologiereuzen zoals Amazon hun systemen gratis aanbieden **als onderdeel van een abonnement op meer lucratieve diensten**.

Afbeelding 2:

Marktspelers



Bron: Candriam

Risico's en controverses

In het afgelopen decennium heeft de opkomst van Gezichtsherkenningstechnologie voor grootschalige bewakingsdoeleinden tot grote bezorgdheid geleid in de samenleving, naast schendingen van de mensenrechten.

Een invasieve technologie

Bewaking met gezichtsherkenning **treft velen onder ons**, vaak **zonder ons medeweten**, in onze dagelijkse bezigheden. Het kan immers bewaking op grote schaal mogelijk maken, waardoor onze mensenrechten in het gedrang komen.

Het klopt ook dat miljoenen vrijwillig op deze technologie vertrouwen en haar toejuichen. Veel gesofisticeerde Apple iPhone-gebruikers vertrouwen op 'Face ID' om hun smartphones te ontgrendelen. Miljoenen mensen hebben zich aangemeld voor geautomatiseerde biometrische grenscontrolesystemen, zoals het "ePassport" van het Verenigd Koninkrijk.

Overal ter wereld maken politionele diensten al op grote schaal gebruik van gezichtsherkenning. **Tegen eind 2021 zullen er naar schatting één miljard bewakingscamera's in werking zijn**.[3] China is veruit koploper wat het gebruik van dergelijke systemen betreft, met naar schatting 600 miljoen camera's die momenteel in werking zijn - dat is één camera voor elke 2,3 burgers. Dat wordt op de voet gevolgd door de Verenigde Staten, waar naar schatting 140 miljoen camera's zijn geïnstalleerd - één camera voor elke 2,4 inwoners. De meeste daarvan zijn digitale systemen waarvan de feeds door gezichtsherkenningssystemen kunnen worden benut.

Vandaag lopen de bewoners van Detroit, Londen, Monaco, Moskou, Peking en andere steden rond zonder te beseffen dat hun gezicht wordt gescand door gezichtsherkenningssystemen die door de politie worden bediend.

Problemen met nauwkeurigheid

In januari 2020 werd Robert Williams, een inwoner van Detroit, door de politie gearresteerd voor winkeldiefstal nadat hij ten onrechte werd beschuldigd door gezichtsherkenning.

In 2018 identificeerde een test van de Amazon-technologie, *Rekognition*, met behulp van leden van het Amerikaanse Congres 28 congresleden ten onrechte als personen die eerder voor misdrijven waren gearresteerd.[4] De test bracht ook de etnische vooringenomenheid van de technologie aan het licht, aangezien Afro-Amerikaanse congresleden onevenredig vaak ten onrechte werden geïdentificeerd als mensen die in de databank met gearresteerde personen zitten. Een van hen was wijlen John Lewis, die de Presidential Medal of Freedom had gekregen.

Zelfs de meest nauwkeurige systemen die vandaag beschikbaar zijn, zetten aan tot nadenken. Stelt u zich een politiedienst voor van een kleine stad die gezichtsherkenningstechnologie gebruikt met een nauwkeurigheid van 99,9%, waar dagelijks 100.000 mensen worden gefilmd met bewakingscamera's. Wie vindt het OK dat er elke dag 100 mensen ten onrechte worden geïdentificeerd?

In de vier jaar dat ze in gebruik is geweest, sinds 2016, is de live gezichtsherkenningsbewaking van de Londense stadspolitie (de 'Met') voor 93,59% onnauwkeurig gebleken. Bij twee van de drie ingebruiknames in 2020 had de "Met" een mislukkingscijfer van 100% - er werd geen enkele persoon geïdentificeerd.[5] Uit het onafhankelijke onderzoek dat in opdracht van de Met is uitgevoerd, is ook gebleken dat hun bewaking met gezichtsherkenning erg onnauwkeurig was. Hun analyse beoordeelde slechts zes van de politietests en wees uit dat de politie het maar in 19% van de gevallen bij het juiste eind had - met andere woorden 81% van de tijd onnauwkeurig was.[6]

Waarom vormt gezichtsherkenning, een technologie die ons dagelijks leven efficiënter en veiliger maakt, ook een bedreiging voor onze mensenrechten?

Isedua Oribhador, US Policy Analyst bij AccessNow: *"Hoewel gezichtsherkenningstechnologie wordt aangeprezen als een tool om de efficiëntie en de veiligheid te verbeteren, hebben we al bewijs gezien van de risico's die eruit voortvloeien. Dat gaat van de etnische en gendervooroordelen die inherent zijn aan zulke systemen, de privacyrisico's die gepaard gaan met het verzamelen van dergelijke persoonsgegevens, tot de mogelijkheid om massaal toezicht te houden op burgers. Daarom vormt gezichtsherkenningstechnologie een ernstige bedreiging voor talrijke grondrechten. Het is absoluut noodzakelijk om deze risico's te onderzoeken en duidelijk aan te geven wanneer het gebruik van deze technologie onverenigbaar is met de naleving van de mensenrechten".*[7]

"Chinese politionele diensten hebben een uitgebreid en heimelijk systeem van gezichtsherkenning gebruikt om de 11 miljoen Oeigoeren, een grotendeels islamitische minderheid, te identificeren, op te sporen en te controleren."

Landenfocus -- China

De Chinese nationale inlichtingenwet van 2017 verplicht organisaties en burgers om "de staatsinlichtingendienst te steunen, bij te staan en mee te werken". In feite is elk soft- of hardwarebedrijf in China verplicht om gegevens aan Peking te overhandigen indien de autoriteiten zich zorgen maken over de nationale veiligheid.

Eind 2018 waren er meer dan 200 miljoen bewakingscamera's in gebruik, in 2020 naar schatting al meer dan 600 miljoen. In de top 10 van steden met de meeste bewakingscamera's op straat per persoon staan Chongqing, Shenzhen, Shanghai, Tianjin en Ji'nan aan kop.

De zogenaamde gezichtsherkenningstorens in Chinese steden staan symbool voor deze ontwikkeling. De gezichtsherkenningstechnologie breidt zich uit naar politieagenten in Peking, die nu slimme zonnebrillen gebruiken waarmee gezichten worden gescand en matches worden gemeld.

China's bewakingssysteem voor burgers is nu gekoppeld aan zijn "Sociaal Kredietsysteem", dat mensen beoordeelt op basis van hun gedrag. Aan de hand van dit systeem, dat in 2013 van start ging, worden burgers beloond of gestraft, naargelang hun score.

De Chinese politie werkt samen met softwarebedrijven gespecialiseerd in artificiële intelligentie, zoals Yitu, Megvii, SenseTime en CloudWalk. Hardwarefabrikanten als Dahua en Hikvision krijgen ook grote overheidsorders. Al deze bedrijven zijn op de economische sanctielijst van de Amerikaanse regering geplaatst omdat ze betrokken zijn bij de onderdrukking van de Oeigoeren.

Niettemin blijven de ambities van China op het gebied van AI- en FR-technologie groot. Het land wil immers tegen 2030 uitgroeien tot een wereldleider op het vlak van AI. Als regering is China met voorsprong de grootste investeerder in geavanceerde bewakingstechnologieën, AI en FR.

Onderdrukking van de Oeigoeren

De Chinese autoriteiten in de regio Xinjiang maken gebruik van gezichtsherkenningstechnologie om etnische profielen op te stellen en om toezicht te houden. Chinese politionele diensten hebben een uitgebreid en heimelijk systeem van gezichtsherkenning gebruikt om de 11 miljoen Oeigoeren, een grotendeels islamitische minderheid, te identificeren, op te sporen en te controleren. De Chinese politie heeft FR-scanners geïnstalleerd bij de ingang van verschillende moskeeën in de regio. Xinjiang is voor deze ondernemingen een belangrijke testomgeving geweest, waar zij zonder de gebruikelijke beperkingen tewerk konden gaan.

Gender- en etnische vooroordelen en gestolen gegevens

De eerste experimenten met gezichtsherkenning waren niet in staat om mensen van Afro-Amerikaanse of Aziatische afkomst te herkennen. Erger nog, Google zag zich in 2015 genoodzaakt zijn excuses aan te bieden toen zijn toen nieuwe applicatie *Google Photos* sommige zwarte mensen als "gorilla's" bestempelde.

Uit een onderzoek van het MIT Media Lab uit 2018 bleek dat bepaalde gezichtsherkenningssoftware een blanke man met bijna perfecte precisie kon identificeren, maar zwaar faalde om vrouwen met een donkere huidskleur te herkennen.

Clearview AI zegt dat het werkt voor meer dan 2.400 politiebureaus in de VS. De CEO, Hoan Ton-That, heeft naar verluidt banden met extreemrechtse politieke bewegingen. Clearview heeft miljarden foto's van Facebook, YouTube en Venmo gehaald om zijn databank samen te stellen.[8] Damien Patton, CEO en oprichter van Banjo, nam ontslag na beschuldigingen dat hij banden zou hebben met de Ku Klux Klan. In die periode had Banjo een contract voor gezichtsherkenningsdiensten ter waarde van 20 miljoen dollar met de staat Utah.

De grote technologiebedrijven Amazon, Microsoft, en Google moedervennootschap Alphabet zijn allemaal aangeklaagd omdat ze foto's hebben gebruikt zonder toestemming van de mensen in kwestie voor hun ontwikkeling en training van hun gezichtsherkenningstechnologie. Facebook betaalde hiervoor een schikking van 650 miljoen dollar op grond van de privacywetgeving van de staat Illinois.[9] Uit documenten die door Edward Snowden zijn gelekt, blijkt dat de National Security Agency in de VS miljoenen gezichtsopnames heeft verzameld. Uit de lekken bleek dat de foto's afkomstig waren van e-mails, sms-berichten, sociale media en videogesprekken.[10]

Misbruik voor eigen en illegaal profijt

Mediaonderzoekers in Rusland ontdekten dat toegang tot de livestream van de CCTV in Moskou op het dark net te koop werd aangeboden door vermoedelijk corrupte politieagenten. Het stadscentrum van Moskou heeft een fijnmazig netwerk van 175.000 bewakingscamera's, waarvan de meeste zijn uitgerust met gezichtsherkenningstechnologie. Aangezien het systeem op de cloud draait, kunnen corrupte ambtenaren hun inloggegevens eenvoudigweg verkopen - voor slechts 470 dollar - en zo toegang krijgen tot de livestream, samen met de opnames van de vorige vijf dagen.

Meer dan camerabewaking - Grootschalige bewaking via computers, smartphones, drones...

Vrijwel elke nieuwe smartphone, personal computer of tablet die tegenwoordig wordt verkocht, is uitgerust met ten minste één digitale camera. Die kunnen allemaal input geven aan een gezichtsherkenningssysteem.

Een andere zorgwekkende ontwikkeling is de toepassing van militaire cameratechnologie met drones, zoals de ARGUS-IS, waarmee regeringen gebieden tot 26 vierkante kilometer continu zouden kunnen registreren -- de helft van de oppervlakte van Manhattan. Deze systemen kunnen het gezicht van elke burger binnen die straal gelijk wanneer scannen.[11]

De problemen

Gebrek aan toestemming

Gebrek aan toestemming is de crux van het probleem. Geen enkel bedrijf, staat, instantie of regering heeft de burgers om toestemming gevraagd. Wanneer burgers hun foto voorleggen aan administraties of overheidsinstanties om een paspoort, een identiteitskaart of een rijbewijs te verkrijgen, stemmen zij er in de meeste rechtsgebieden op geen enkel ogenblik mee in dat hun foto wordt gebruikt voor gezichtsherkenning. Andere vormen van biometrische identificatie vereisen de toestemming van de gecontroleerde persoon. Mensen die zich op het openbaar terrein begeven en die met live gezichtsherkenning worden gescand, zijn zich er waarschijnlijk niet van bewust dat hun identiteit werd gecontroleerd en hebben niet de gelegenheid om al dan niet in te stemmen met het gebruik ervan.

In Europa bepaalt de in 2016 ingevoerde Algemene Verordening Gegevensbescherming (GDPR) duidelijk dat biometrische gegevens die door middel van gezichtsherkenningstechnologie werden verkregen, persoonsgegevens zijn. Dat valt onder de beschermingsverordening en daarom moet elke betrokken persoon toestemming verlenen voor het gebruik van zijn of haar biometrische gegevens door een andere persoon, onderneming of instantie. Toch maken politionele diensten in EU-landen als het Verenigd Koninkrijk, Frankrijk, Italië en Griekenland al gebruik van de technologie.

Gebrek aan wettelijke basis

In de meeste landen is er geen wettelijke basis voor het gebruik van live gezichtsherkenningsbewaking door de politie. Gezichtsherkenning is in strijd met fundamentele vrijheidswetten zoals het Eerste Amendement van de grondwet van de VS en de Human Rights Act in het VK.

Clare Garvie van Georgetown Law's Center on Privacy & Technology, vertelt Candriam: *"Het gebruik van gezichtsherkenning door de politie in de VS is nog steeds grotendeels ongereguleerd, ondanks pogingen van staten en gemeenten om het gebruik ervan volledig te verbieden en recente onthullingen dat het heeft geleid tot de arrestatie van ten minste drie onschuldige mannen. Gezien de risico's voor de grondwettelijke rechten van de VS op privacy, vrijheid van meningsuiting, eerlijke processen en gelijke bescherming van de wet, is een moratorium op het gebruik van gezichtsherkenning gerechtvaardigd, tenzij en totdat er krachtige regelgeving is aangenomen om die rechten te vrijwaren".*

Gebrek aan controle

In de meeste landen, zoals de VS of Europa, zijn er weinig tekenen van een passend en onpartijdig toezicht op het gebruik van bewakingstechnologie door privébedrijven en politionele diensten.

Onevenredige indringing

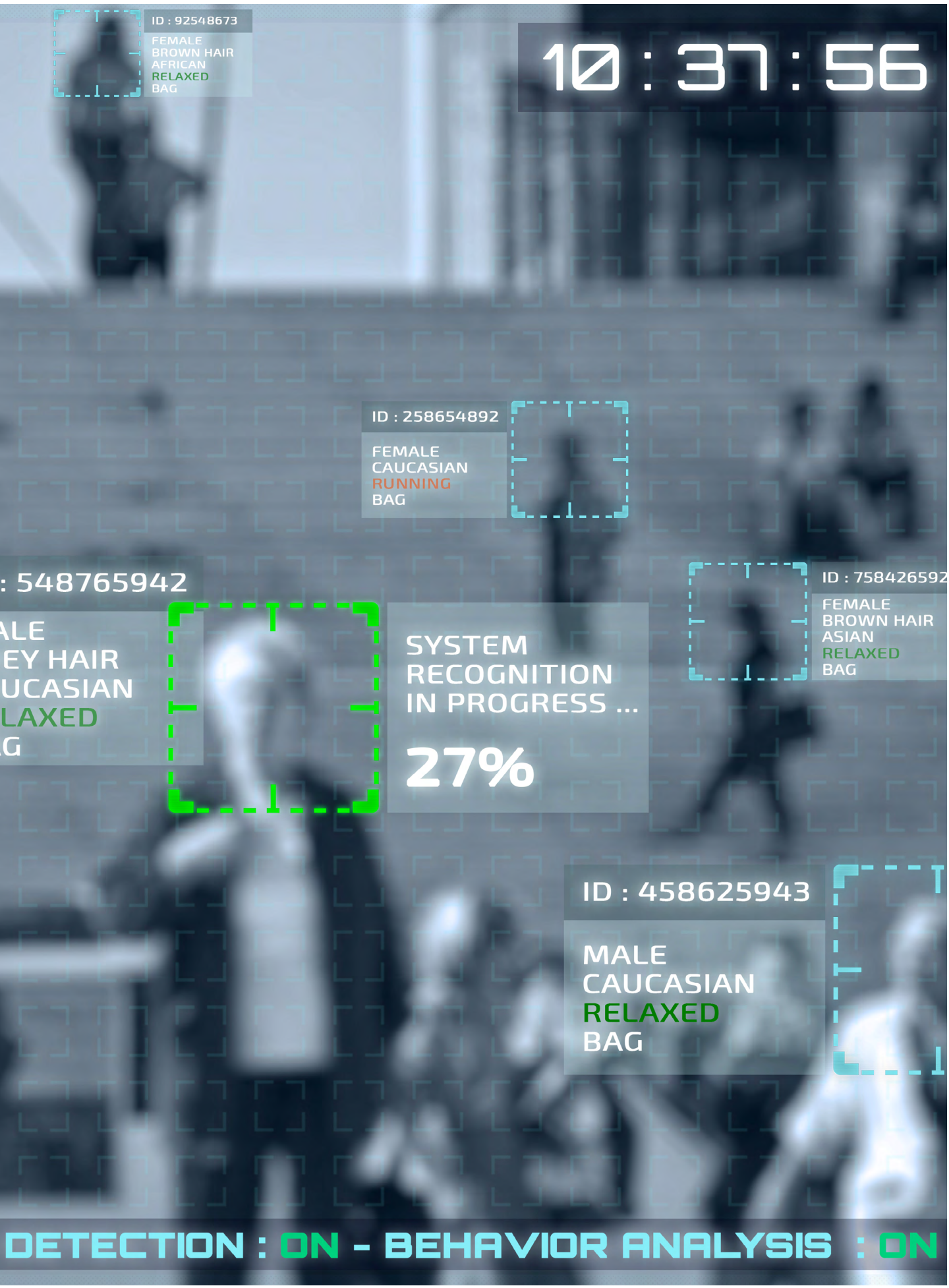
Bij meerdere in het VK uitgevoerde tests is gebleken dat de succesratio uitkomt op één gezochte misdadiger voor elke 300.000 gescande gezichten. De commissaris voor bewakingscamera's concludeerde dat de inzet uiterst onevenredig was en merkte op dat "vergeleken met de schaal en de omvang van de verwerking van alle mensen die een camera passeren, de groep die zij zouden kunnen hopen te identificeren uiterst klein is".

Het recht om anonimiteit

Een bloeiende samenleving is gebaseerd op verschillende vrijheden - vrijheid van meningsuiting, van verkeer, van godsdienst, van vereniging - maar ook op het recht op een redelijke mate van anonimiteit. Onze mogelijkheid om ons anoniem in de openbare ruimte te bewegen is niet langer gegarandeerd door de ruime toepassing van gezichtsherkenningssystemen. Iedereen moet vrij en anoniem kunnen rondlopen. Het ligt in de aard van de mens dat hij wil leven zonder steeds over zijn schouder te moeten kijken. Maar wat je nog kan doen zonder in het openbaar gecontroleerd te worden, wordt in snel tempo steeds beperkter. Overal waar we komen, worden we geïdentificeerd door de politie, bedrijven of regeringen, en dat belemmert onze eigenheid. Het zal uiteindelijk de bewegingsvrijheid, creativiteit, vertrouwen en zelfs democratie beperken.

Ter illustratie: uit het verslag van het London Policing Ethics Panel over live bewaking met gezichtsherkenning door de politie bleek dat 38% van de 16- tot 24-jarigen zou wegblijven van evenementen of plaatsen waar gezichtsherkenningsbewaking wordt gebruikt, evenals grote aantallen zwarte en Aziatische mensen en andere minderheden.[12]


CAM 3
ID : 254876592
MALE
BROWN HAIR
CAUCASIAN
STRESSED
ID
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

Is veiligheid een beperkt verlies aan privacy waard?

Op de vraag wat zij vinden van gezichtsherkenning, antwoordt een meerderheid van de burgers dat zij begrijpen dat zij om veiliger te zijn een beetje privacy moeten opgeven. Het argument dat een vermeende terrorist of een ontvoerd kind snel moet kunnen worden opgespoord, raakt een gevoelige snaar.

De camerabewakingsindustrie maakt gebruik van marketing die teert op angstgevoelens. Denk bijvoorbeeld aan de angst voor een terroristische aanval. De Franse stad Nice was in 2016 het toneel van een gruwelijke aanslag toen een terrorist met een vrachtwagen door de menigte aan het strand reed die Bastille Day vierde, waarbij 87 doden vielen. Als reactie daarop rustte de stad de lokale politie uit met de grootste inzet van gezichtsherkennings- en bewakingstechnologie van alle Franse steden.

Als verantwoordelijke burgers moeten we onszelf afvragen:

- Willen we voortdurend worden geïdentificeerd door niet-geteste en potentieel onnauwkeurige of vooringenomen algoritmen?
- Willen we dat onze regering elke beweging die we maken, elke plaats die we bezoeken en de mensen die we ontmoeten registreert?
- Willen wij dat de politie in staat is de namen te registreren van alle deelnemers aan een protestmars of een religieuze plechtigheid?
- Willen we onze regeringen onbeperkte macht geven om ***iedereen, overal en altijd in*** de gaten te houden?

Een 'schizofrene' samenleving?

Wanneer wij toestaan dat onze regeringen en politionele diensten bewakingstechnologie inzetten om onze veiligheid te waarborgen, zeggen wij ook dat wij, om iedereen veilig te houden, iedereen voortdurend in de gaten moeten houden. Sommige sociologen vinden dit een vorm van schizofrenie.

Het accepteren van overheidstoezicht is cultureel bepaald

We kunnen de mensenrechtenuitdagingen op het vlak van gezichtsherkenning niet alleen bekijken door een westerse bril. De manier waarop privacy en een inbreuk daarop wordt aangevoeld, is immers sterk cultureel bepaald. De meeste mensen in China vinden grootschalige bewaking iets wat ze moeten aanvaarden in ruil voor meer veiligheid. De laatste jaren heeft de combinatie van grootschalige toepassing van bewakingstechnologie met de opzet van het Sociaal Kredietsysteem (kader, pagina 13) ervoor gezorgd dat de misdaadcijfers enorm zijn gedaald.

The Perpetual Line-up

Dit concept, dat werd bedacht door het Centre for Privacy and Technology at Georgetown Law,[13] is dat niemand vrijwillig zou deelnemen aan een line-up waarbij een slachtoffer de misdadiger eruit zou halen! Het slachtoffer zou u immers per abuis kunnen identificeren. Gezichtsherkenningssystemen doen dat dagelijks, zowat overal in de VS en China.[14]

Spionagekapitalisme

In haar boek "The Age of Surveillance Capitalism" omschrijft Shoshana Zuboff spionagekapitalisme als het proces waarbij gratis diensten worden aangeboden waar miljarden mensen maar al te graag gebruik van maken. Zo kunnen de aanbieders van die diensten het gedrag van die gebruikers tot in verbluffend detail volgen -- vaak zonder hun uitdrukkelijke toestemming. "Het spionagekapitalisme eist eenzijdig de menselijke ervaring op als grondstof om te vertalen in gedragsgegevens." Spionagekapitalisten halen enorme financiële voordelen uit de exploitatie van individuele en collectieve gedragsgegevens en de voorspellingen van wat mensen vervolgens gaan doen.

De combinatie van staatsspionage en zijn kapitalistische tegenhanger betekent dat de digitale technologie de **burgers in alle samenlevingen in twee groepen verdeelt: de *Kijkers* - onzichtbaar, onbekend en onbeperkt - en de *Bekekenen*.** Dat heeft ingrijpende gevolgen voor de democratie, omdat asymmetrie van kennis zich vertaalt in asymmetrie van macht. Maar terwijl de meeste democratische samenlevingen op zijn minst een zekere mate van toezicht hebben op het staatsspionage, hebben we momenteel bijna geen regelgevend toezicht op de geprivatiseerde tegenhanger ervan.[15]

Engagement - Praktische richtlijnen

Als verantwoorde belegger is het onze taak om ecologische, sociale en governancefactoren (ESG) in onze beleggingsbeslissingen op te nemen en te handelen als een actieve aandeelhouder. We willen op lange termijn toegevoegde waarde creëren voor onze cliënten, door een positieve invloed uit te oefenen op de economie, het milieu en de samenleving als geheel.

We zijn ervan overtuigd dat we moeten kijken naar het grote plaatje van Gezichtsherkenningstechnologie in onze beleggingen en engagement zal bijdragen tot beide luiken van onze doelstelling. Een steeds groter aantal van de bedrijven, staten en regio's waarin wij beleggen, is voortaan bij deze technologie betrokken. Hoewel wij waarschijnlijk niet doelbewust zouden beleggen in een zuivere gezichtsherkenningsemittent, moet een belegging in een bedrijf dat gezichtsherkenning gebruikt of verkoopt, terdege onderzocht worden om:

- De ermee gepaard gaande risico's in te schatten;
- Onze potentiële bezorgdheden met de bedrijven waarin we beleggen te delen;
- Veranderingen te ondersteunen waarmee de vastgestelde risico's kunnen worden gereduceerd.

Zoals werd beschreven in onze bespreking van de technologie en haar problemen, beleggers talrijke en complexe verwachtingen koesteren die verschillen van stakeholder tot stakeholder. Enkele doelstellingen hieronder:

Bedrijfsemittenten

- **Direct en/of collectief engagement** om de bedrijfspraktijken beter te begrijpen. Uitbreiden van best practices door gesprekken met bedrijven, ngo's, enz.

- **Ontwikkelingen opnemen in de ESG-analyse** van ondernemingen. Bepalen van best practices, aanvaardbare vooruitgang, en wat moet worden uitgesloten.

- **Bedrijven ertoe aanzetten om hun gedrag te verbeteren**. Ethiek en naleving van de mensenrechten blijven centraal staan in deugdelijk bestuur. Oprichting van een onafhankelijk comité voor mensenrechtenrisico's dat rapporteert aan de Raad van Bestuur. Bedrijven aanmoedigen om klanten en leveranciers te kiezen die de waarden die zij verdedigen ook uitdragen.

Overheden

- **Opschorting vragen van het gebruik van gezichtsherkenning bij de rechtshandhaving** tot er specifieke regelgeving komt.

Universiteiten

- Lessen ethiek in AI/Tech curricula aanmoedigen.

Bij Candriam zijn wij voornemens om dit onderwerp met de Europese autoriteiten te bespreken, maar wij geloven dat ons beste pressiemiddel is om rechtstreeks te gaan spreken met bedrijfsemittenten, en meer in het bijzonder met bedrijven waarin we al beleggen.

Vanuit dit oogpunt, en geïnspireerd door gesprekken met specialisten/experts op het gebied van gezichtsherkenning, stellen wij hieronder een reeks vragen (Afbeelding 2) aan de hand waarvan beleggers kunnen inschatten in welke mate de bedrijven waarin we beleggen zich inlaten met gezichtsherkenning. Zo kan ook worden ingeschat in welke mate de mensenrechten mogelijk in het gedrang kunnen komen.

Open MIC werkt al enkele jaren samen met aandeelhouders om druk uit te oefenen op technologiebedrijven om "ethische" praktijken te hanteren op het vlak van gezichtsherkenning.

De grote technologiebedrijven hebben veel energie en middelen gestoken om zich tegen deze initiatieven te verzetten. Ondanks de sterke druk van de aandeelhouders - en de wereldwijde druk van talrijke mensenrechtenorganisaties - weigeren de bedrijven grotendeels te erkennen dat er een probleem is. Zoals in dit verslag wordt benadrukt, werken bijna alle gezichtsherkenningsproducten die momenteel op de markt zijn zonder de toestemming van miljoenen mensen wier gezichten dagelijks worden gescand. Veel van die systemen blijken etnische vooroordelen te hebben. Er is geen verhaalmogelijkheid voor degenen wier rechten zijn geschonden, in tegenstelling tot wat de basisbeginselen van de Verenigde Naties inzake bedrijfsleven en mensenrechten voorschrijven (United Nations Guiding Principles on Business and Human Rights). In 2019 heeft de speciale VN-rapporteur voor vrijheid van mening en meningsuiting aanbevolen "een onmiddellijk moratorium in te stellen op de wereldwijde verkoop en overdracht van particuliere surveillancetechnologie tot er sluitende waarborgen voor de mensenrechten bestaan". Er zijn geen waarborgen op het vlak van mensenrechten, en tot gaat de verkoop gewoon door. Zoals uit dit rapport al blijkt, zit deze markt sterk in de lift.

Een van de vragen is of de voorziene wet- en regelgeving - zowel in de EU als in de VS - bedrijven zal aansporen om vrijwillig doeltreffende sectornormen in te voeren. De bedrijven zullen ongetwijfeld lobbyen om eventuele overheidscontroles op gezichtsherkenning af te zwakken. Beleggers moeten zeker bezig blijven zoals nu: ze moeten gebruik maken van alle instrumenten die zij hebben om druk uit te oefenen op de technologiebedrijven zodat ze beleidslijnen en praktijken invoeren die een verschil zullen maken. Het valt nog af te wachten of een groot en uitgesproken collectief engagement, zoals hetgeen dat hier wordt gesuggereerd, bedrijven ertoe kan aanzetten om een meer productieve dialoog aan te gaan.

Michael Connor is de oprichter en uitvoerend directeur van Open MIC, een non-profitorganisatie die streeft naar een grotere verantwoordingsplicht van bedrijven in de media- en technologiesector, met name door aandeelhoudersengagement. In samenwerking met sociaal verantwoordelijke investeerders identificeert, ontwikkelt en ondersteunt Open MIC campagnes die waarden als openheid, gelijkheid, privacy en diversiteit bevorderen - waarden die op lange termijn in het voordeel spelen van particulieren, bedrijven, de economie en de gezondheid van de democratische samenleving. Open MIC werkt momenteel aan campagnes gericht op Amazon, Twitter, Google en Facebook.

Beleggingsrichtlijnen

Mate van betrokkenheid

- Levert uw bedrijf producten (hardware, software, databases) die verband houden met gezichtsherkenningstechnologie?

- Wat is de bedoeling van het product?
  - Spionage
  - Identificatie
  - Beleidsvoering
  - Categorisering (bv. doelgerichte reclame)
  - Onderzoeksvoering
  - Overige (verduidelijk a.u.b.)
  - Beveiliging

- Aan welk type gebruikers biedt u uw gezichtsherkenningstechnologie aan?
  - Overheden of staten
  - Scholen
  - Politionele diensten
  - Ondernemingen
  - Leger

Governance

- Heeft uw bedrijf een openbaar beleid inzake gezichtsherkenningstechnologie? Zo ja, welke invloed heeft dit engagement gehad
  1) op uw relaties met zakenpartners, bv. leveranciers, onderaannemers, klanten, eindgebruikers? en
  2) op uw lobbyactiviteiten?

- Welke risico's hebt u vastgesteld in verband met de technologie voor gezichtsherkenning en hoe vaak brengt u daarover verslag uit aan de Raad van Bestuur?

- Voert uw bedrijf impactonderzoek uit op het vlak van mensenrechten om de reële en potentiële risico's voor de mensenrechten van uw technologieën voor gezichtsherkenning vast te stellen en te beoordelen? Welke risico's hebt u vastgesteld, en welke stakeholders hebt u bij deze beoordeling betrokken? Op welke manier hebt u uw activiteiten en strategie aangepast? Wie in het bedrijf (op bedrijfs- / regionaal / bijkantoorniveau) draagt de algemene en dagelijkse verantwoordelijkheid voor de aanpak van deze specifieke risico's en potentiële impact?

- Welke processen hebt u ingevoerd om te bepalen aan welke klanten u kunt verkopen? Verbiedt u de verkoop/levering van uw product of dienst aan bepaalde onderdrukkende/ondemocratische landen?

Beheer van ontwerpgerelateerde risico's

- Hoe bent u intern georganiseerd om risico's in verband met gezichtsherkenning op te sporen, te voorkomen en op te lossen?

Meer specifiek:

- Op welke manier heeft uw bedrijf zijn trainingsdatabank met foto's en namen opgebouwd/verkregen/gekocht? Indien u de databank niet zelf hebt opgebouwd, hoe heeft uw leverancier dan de databank die u gebruikt samengesteld/verkregen/gekocht?
- Maakt u de nauwkeurigheid van uw en hun technologie bekend na bepaling door een erkende wetenschappelijke beoordelingsinstelling, zoals het National Institute of Standards and Technology (NIST)? Indien niet, leg uit waarom?
- Welke interne controles past u toe u om vooringenomen van het algoritme zoals etniciteit, gender of leeftijd op te sporen? En/of uw leveranciers?
- Bestaat er een klachtenmechanisme om personen die verkeerdelijk werden beoordeeld door de technologie te identificeren en schadeloos te stellen?

Beheer van gebruiksgerelateerde risico's

- Zijn uw cliënten onderworpen aan enige regelgeving inzake hun gebruik van gezichtsherkenningstechnologie? Is dit iets wat u opvolgt?
- Biedt uw product gezichtsherkenningstechnologie voor real-time analyse, of alleen voor analyse achteraf?
- Analyseert uw product live videobeelden, of alleen statische beelden?
- Voorziet uw technologie voor gezichtsherkenning in enige vorm van categorisering, bijvoorbeeld op etniciteit, gender, leeftijd, geestelijk vermogen of anderszins? Voorziet uw technologie voor gezichtsherkenning in enige vorm van voorspellende analyse?
- Bestaat er een klachtenmechanisme om personen die verkeerdelijk werden beoordeeld door de technologie te identificeren en schadeloos te stellen?

Conclusie

Momenteel is gezichtsherkenning een weinig transparant onderwerp. Sommige omarmen het gebruik ervan, terwijl andere het controversieel vinden. Het kan worden misbruikt en bevat overduidelijk bepaalde vooroordelen en fouten.

Zonder transparantie kunnen wij deze controverses niet beoordelen. Om de deur naar analyse en gesprek te openen, moeten we meer pressie zetten. De nationale en lokale autoriteiten beginnen actie te ondernemen. Ondernemingen beginnen actie te ondernemen. Er ontstaat een dynamiek en een publiek debat en ngo's lanceren allerhande campagnes.

Nu is het aan beleggers om actie te ondernemen.

Opmerkingen en referenties

[1] Mashable.com. *Douglas, the latest step toward realistic AI, is unsettling.* Bijgewerkt op 22 november 2020. https://mashable.com/article/douglas-realistic-ai-unsettling/?europe=true, bekeken op 8 februari 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, bekeken op 8 februari 2021.
[4] The American Civil Liberties Union. ACLU.com. Snow, Jacob. *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots.* 26 juli 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28, bekeken op 8 februari 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, bekeken op 8 februari 2021.
[6] The Human Rights, Big Data and Technology Project. Fussey, Professor Pete en Dr. DaraghMurray. Onafhankelijk verslag over het experiment van de Londense Metropolitan Police Service met technologie voor live gezichtsherkenning. Juli 2019. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf, bekeken op 8 februari 2021.

[7] Isedua Oribhabor is beleidsanalist voor de VS van AccessNow, en houdt zich ook bezig met het bedrijfsleven en de mensenrechten. Door Isedua's werk voor het Leitner Center for International Law and Justice aan Fordham kreeg ze belangstelling voor het bedrijfsleven en de mensenrechten, waardoor zij zich is gaan verdiepen in het onderwerp omdat het verband houdt met de technologiesector. AccessNow is een wereldwijde niet-gouvernementele organisatie die gespecialiseerd is in de verdediging van de mensenrechten op het gebied van technologie. AccessNow richt zich op de volgende domeinen: privacy, vrijheid van meningsuiting, digitale veiligheid, het bedrijfsleven en mensenrechten en netdiscriminatie. AccesNow is internationaal actief met 60 medewerkers in 13 landen.

[8] The New York Times. Hill, Kashmir. *The Secretive Company That Might End Privacy as We Know It.* Bijgewerkt op 31 januari 2021. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, bekeken op 8 februari 2021.

[9] CNET News. Musil, Steven. *Amazon, Google, Microsoft sued over photos in facial recognition database.* 14 juli 2020. https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/, bekeken op 8 februari 2021.

[10] The New York Times. Risen, James and Laura Poitras. *N.S.A. Collecting Millions of Faces From Web Images.* 31 mei 2014. https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html, bekeken op 8 februari 2021.

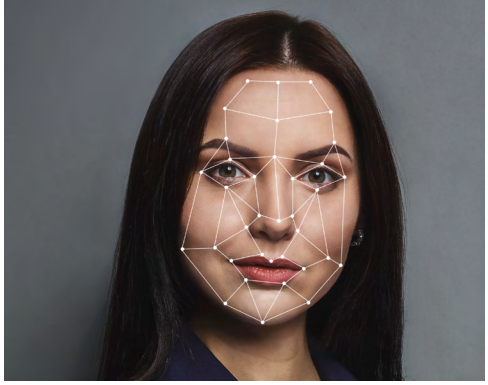
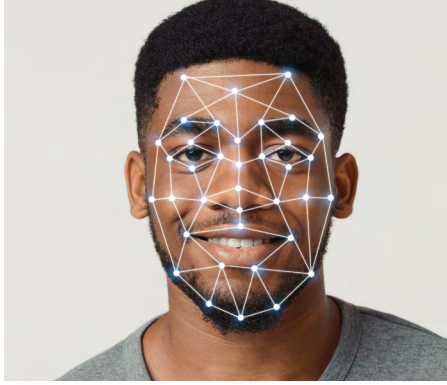
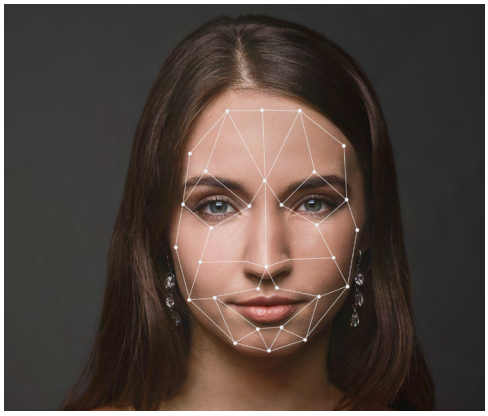
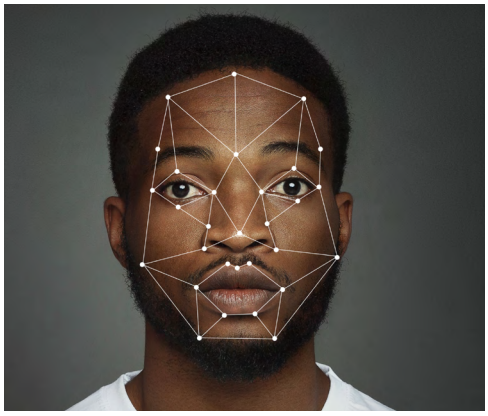
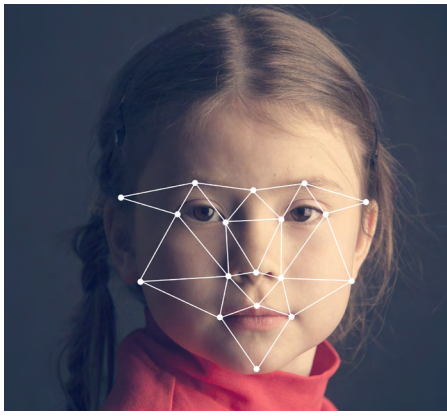
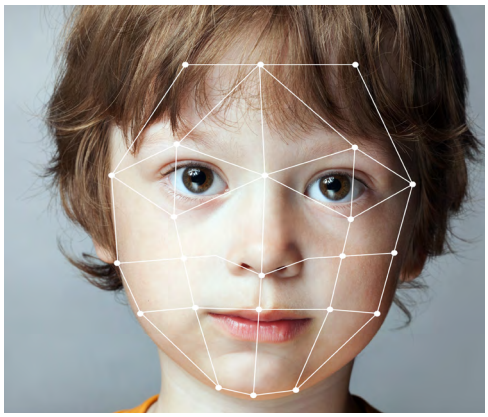
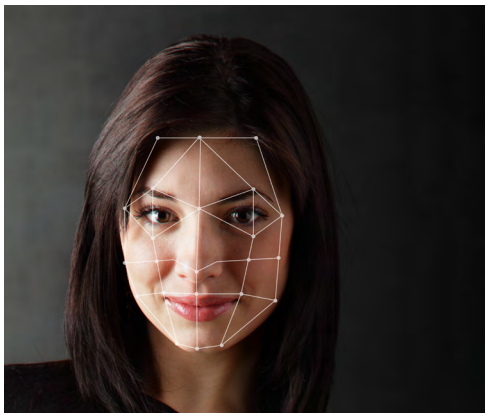
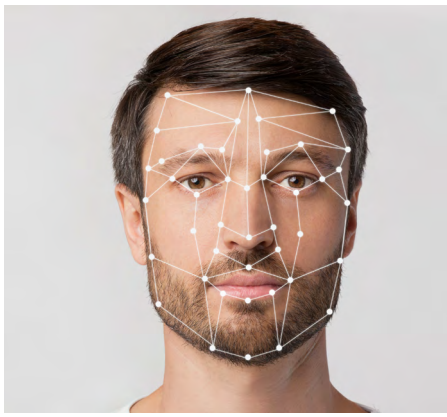
[11] University of Richmond Law Review. Laperruque, Jake. *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance.* Maart 2017. http://lawreview.richmond.edu/files/2017/03/Laperruque-513-website.pdf, bekeken op 8 februari 2021.

[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/, bekeken op 8 februari 2021.

[14] Dit concept werd opnieuw gebruikt in de Arte TV documentaire van Sylvain Louvet genaamd "Tous surveillés, 7 milliards de suspects" (Iedereen wordt in de gaten gehouden, 7 miljard verdachten). Deze documentaire won de Albert Londres prijs (hoogste Franse journalistieke onderscheiding) voor beste documentaire in 2020.

[15] The Guardian. Naughton, John. *'The goal is to automate us': welcome to the age of surveillance capitalism.* 20 januari 2019. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook, bekeken op 8 februari 2021.

140 miljard €

activa in beheer
op 31 december 2020

570

experten
tot uw dienst

25 jaar

Koploper in
duurzaam beleggen

Dit document wordt enkel ter informatie en voor educatieve doeleinden verstrekt en kan de mening en de eigendomsinformatie van Candriam bevatten. De meningen, analyses en standpunten in dit document worden uitsluitend ter informatie gegeven, het vormt geen aanbod om financiële instrumenten te kopen of te verkopen, het is geen beleggingsaanbeveling en het bevestigt geen enkele soort transactie.

Hoewel Candriam de gebruikte gegevens en bronnen met veel zorg selecteert, kunnen fouten of weglatingen niet a priori worden uitgesloten. Candriam kan niet aansprakelijk worden gesteld voor enig direct of indirect verlies als gevolg van het gebruik van dit document. De intellectuele eigendomsrechten van Candriam dienen te allen tijde nageleefd; de inhoud van dit document mag niet worden gereproduceerd zonder voorafgaande schriftelijke goedkeuring.

Onderhavig document vormt geen onderzoek op beleggingsgebied zoals bepaald in Artikel 36, paragraaf 1 van gedelegeerde verordening (EU) 2017/565. Candriam benadrukt dat deze informatie niet is opgesteld overeenkomstig de wettelijke voorschriften ter bevordering van de onafhankelijkheid van onderzoek op beleggingsgebied en evenmin onderworpen is aan een verbod om al vóór de verspreiding van onderzoek op beleggingsgebied te handelen.

Dit document is niet bedoeld om producten of diensten te promoten en/of aan te bieden en/of te verkopen. Het document is ook niet bedoeld om een verzoek tot het verlenen van diensten in te dienen.

CANDRIAM. INVESTING FOR TOMORROW.

WWW.CANDRIAM.COM

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY