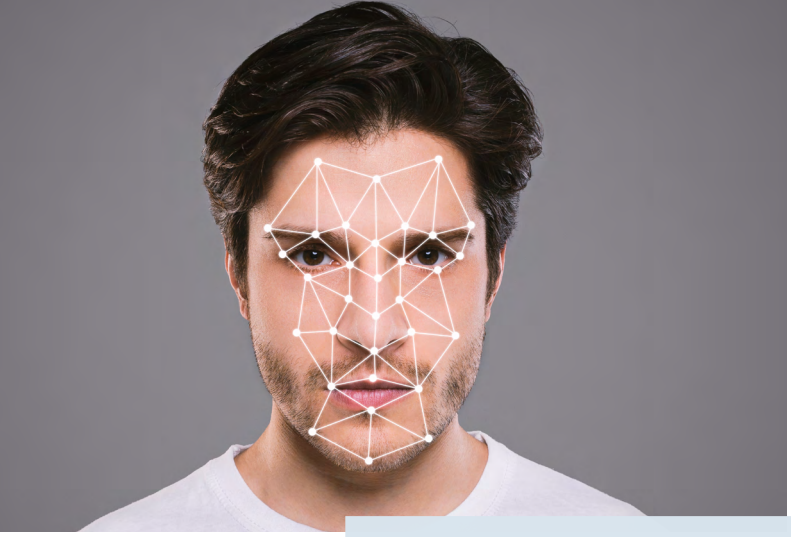
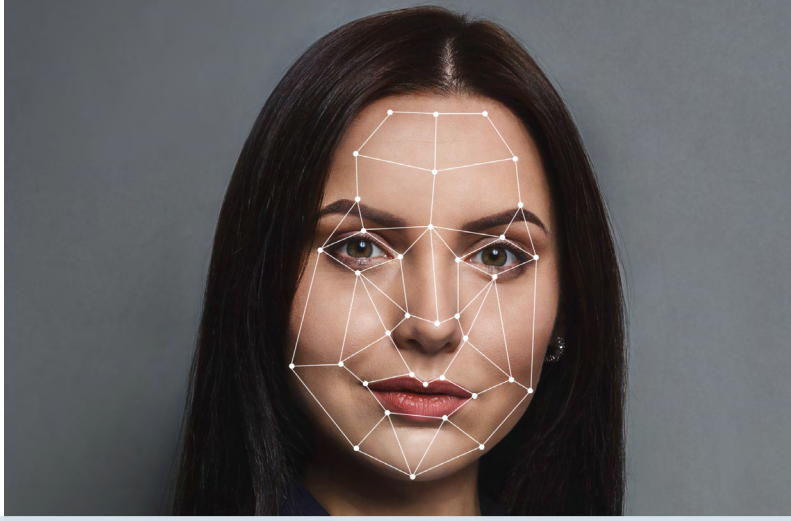
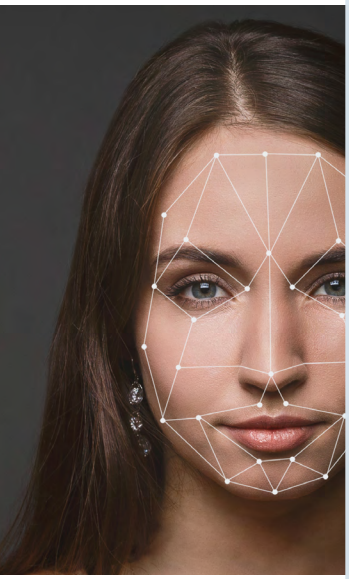
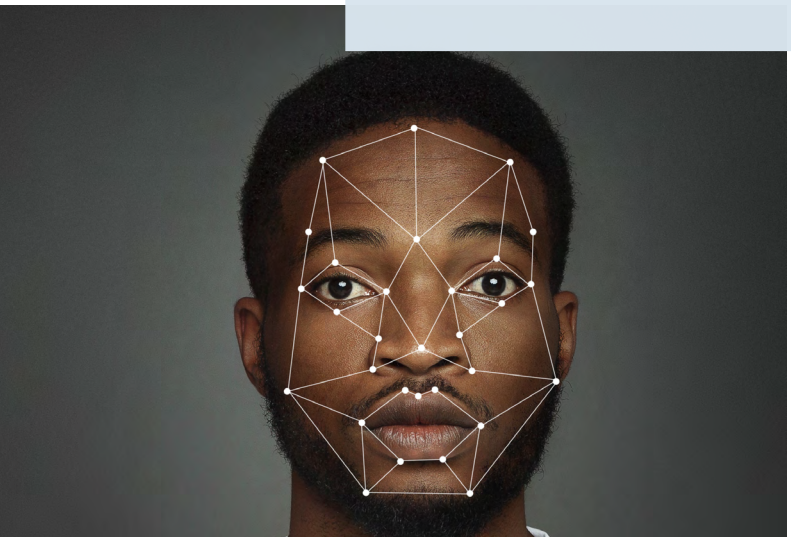
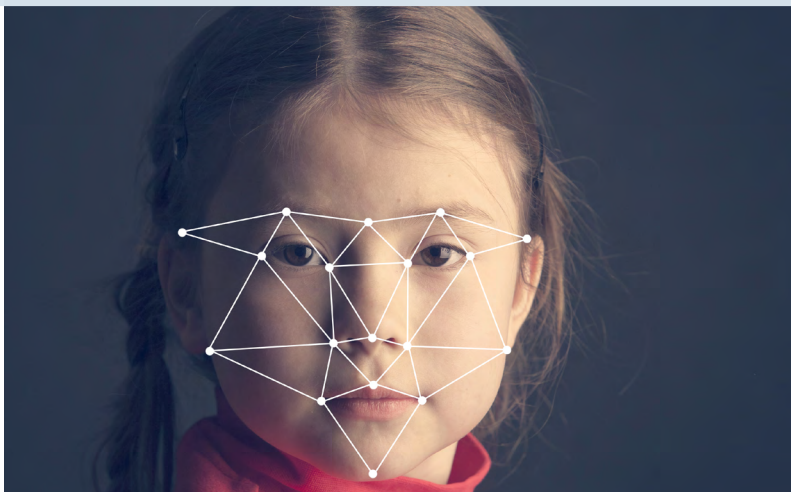





Marzo 2021

Reconocimiento Facial y Derechos Humanos: Guía del Inversor

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY

Acerca de los autores

Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement

Benjamin Chekroun se incorporó a Candriam en 2018 como Deputy Head of Convertible Bonds, y asumió su actual cargo como Analista de Gestión Corporativa ("Stewardship Analyst") en 2020. Anteriormente trabajó en ABN AMRO Investment Solutions desde marzo de 2014, donde era responsable de la estrategia global de bonos convertibles. Benjamin pasó cuatro años en Hong Kong, un año en Nueva York y trece años en Londres, trabajando como operador de renta fija. En 2004, el fondo gestionado por el Sr. Chekroun recibió el galardón "Best Convertible Arbitrage Fund" otorgado por Hedge Fund Review. Benjamin cuenta con un Máster en Comercio Internacional.

Sophie Deleuze

Lead ESG Analyst, Stewardship

Sophie Deleuze se incorporó al Departamento de Investigación ESG en 2005. Después de una década como Analista ESG, se especializó en el sector de Gestión Corporativa, Voto por Delegación y Compromiso de Candriam, coordinando nuestro compromiso con nuestros analistas ESG y con todos nuestros equipos de gestión de inversiones. Antes de trabajar en Candriam, pasó cuatro años como Analista ISR en BMJ CoreRatings y Arese. La Sra. Deleuze cuenta con una Licenciatura de Ingeniería en Tratamiento de Agua y un Máster en Asuntos Públicos Medioambientales.

Quentin Stevenart

ESG Analyst

Quentin se incorporó al Equipo ESG de Candriam como Analista ESG en 2016. Realiza análisis completos ESG del sector TI y sobre temas de gobernanza de carácter intersectorial. Asimismo es responsable de la coordinación de la investigación sobre Economía Circular de Candriam. Cuenta con un Máster en Gestión de la Escuela de Gestión de Louvain, así como una Licenciatura y un Máster en Ingeniería de Negocios por la Universidad Católica de Leuven.

Índice

"Aunque la tecnología conlleva promesas innegables y puede ser una fuerza para el bien, la forma en la que la tecnología de reconocimiento facial está diseñada y es utilizada actualmente conlleva riesgos e implicaciones sociales para las personas, lo que garantiza la acción de los inversores sobre este tema. Por lo tanto, damos la bienvenida a los esfuerzos y al liderazgo intelectual de los inversores, a través de los cuales, por delante de la reglamentación, estos pretenden ampliar la lista tradicional de temas ESG y comprender cómo, dónde y cuándo el reconocimiento facial puede ser utilizado de manera adecuada y por parte de quién."

- **Katherine Ng,** Directora de Investigación Académica, Principios de Inversión Responsable de Naciones Unidas

Sumario Ejecutivo

La inversión responsable es algo más que el hecho de reaccionar a los riesgos y los problemas que afrontamos actualmente. Quiere decir pensar más allá de las huellas de carbono y el cambio climático y mirar hacia los riesgos y las oportunidades del futuro.

La tecnología ha aportado al mundo algunos beneficios maravillosos, además de algunas inversiones maravillosas. La tecnología ha permitido a muchos trabajadores profesionales continuar trabajando desde sus hogares durante la actual pandemia. El Presidente Biden llevó a cabo una parte significativa de su campaña electoral desde su sótano. Aún así debemos ser conscientes de que cualquier nueva tecnología puede generar consecuencias no deseadas.

La Tecnología de Reconocimiento Facial ("Facial Recognition Technology") (TRF) mejora la eficiencia y la seguridad. Utilizamos esta tecnología para desbloquear smartphones de alta gama y para desplazarnos por los aeropuertos. Pero también tiene implicaciones para los derechos humanos. Esta tecnología se ha desarrollado durante décadas, pero solo actualmente empieza a ser ampliamente utilizada.

La encuesta realizada por Candriam en 2021 obtuvo aproximadamente 300 respuestas de inversores. De dichas respuestas, el 30% consideraba que la Tecnología de Reconocimiento Facial era una herramienta conveniente y útil. El 70% manifestó algunas reservas; el 31% consideró que la TRF no era precisa, mientras que el 38% creía que las consideraciones éticas debían estar a la altura de la tecnología.

Las cuestiones engloban la falta de consentimiento y la falta de supervisión. Los incidentes de identificaciones erróneas están al alza, y algunos han provocado detenciones erróneas, en especial de ciudadanos que no son de raza caucásica. En mayo de 2019, la ciudad de San Francisco, Estados Unidos –lugar de nacimiento del Reconocimiento Facial- prohibió su uso en actividades de vigilancia policial. Poco después, diversas grandes empresas tecnológicas anunciaron una moratoria de un año sobre la venta de sus productos de Reconocimiento Facial.

Para comprender las cuestiones de derechos humanos que surgirán en el futuro, los inversores responsables y otros actores clave deben establecer un compromiso hoy.

Este estudio no habría sido posible sin la gran ayuda de las siguientes instituciones y personas. Deseamos expresarles nuestro agradecimiento por su tiempo, sus conocimientos y su paciencia:
- *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*

La Tecnología

¿Cómo funciona?

El Reconocimiento Facial forma parte del ámbito del reconocimiento biométrico. Es el proceso de **identificar** o **verificar la identidad** de una persona utilizando una foto o un video de su cara. Este proceso captura, analiza y compara patrones sobre la base de los detalles faciales de la persona. Algunos sistemas utilizan actualmente imágenes tridimensionales para lograr mayor exactitud.

Existen tres etapas principales en la Tecnología de Reconocimiento Facial:

- **La Detección Facial** es un proceso esencial que detecta y localiza rostros humanos en imágenes y vídeos.
- **La Captura Facial** transforma la información analógica –una cara- en un conjunto de información digital, o datos, que describen los rasgos faciales de la persona. Se miden docenas de rasgos faciales como el espacio entre los ojos, el puente de la nariz, el contorno de los labios, las orejas, el mentón, etc.
- **La Coincidencia Facial** verifica si dos caras se corresponden con la misma persona.

El algoritmo proporciona un resultado con una probabilidad determinada, con un formato estadístico como "*Coincidencia Positiva – John Doe – 97,36% de Probabilidad*".

Una breve historia del Reconocimiento Facial

El Reconocimiento Facial se remonta a la década de 1960. Woody Bledsoe, obispo mormón y cofundador de Panoramic Research en Palo Alto, desarrolló una forma de introducir manualmente las posiciones de los rasgos faciales de una persona en un ordenador. Aunque no resultaba muy efectivo de acuerdo con criterios modernos, demostró que la cara era un valor biométrico válido. La precisión de los sistemas de reconocimiento facial mejoró en la década de 1970 a medida que los investigadores introducían marcadores faciales adicionales. El auténtico progreso se produjo en las décadas de 1980 y 1990, con la aparición de nuevos métodos para localizar una cara en una imagen y extraer sus rasgos, lo que posibilitó un Reconocimiento Facial totalmente automatizado. En 1996, el Programa FERET en EEUU supuso el primer desarrollo de una base de datos faciales. La Super Bowl de 2001 fue la primera prueba masiva de Reconocimiento Facial para tareas de vigilancia policial. Se identificaron 19 criminales buscados entre la multitud. Los avances más decisivos se lograron en 2010 y posteriormente, cuando las redes neuronales profundas mejoraron la tecnología. En 2011, la Tecnología de Reconocimiento Facial ayudó a confirmar la identidad de Osama Bin Laden cuando falleció en un ataque estadounidense. Facebook desarrolló la tecnología de etiquetado fotográfico y en 2014 su programa DeepFace se convirtió en el primero en lograr un rendimiento cuasi-humano en materia de reconocimiento facial. En 2017, el iPhone X fue el primer smartphone de gran difusión en ofrecer desbloqueo facial, lo que supuso la primera comercialización masiva de la Tecnología de Reconocimiento Facial. En mayo de 2019, San Francisco se convirtió en la primera gran ciudad de Estados Unidos en prohibir el uso de la TRF por parte de organismos policiales. El siguiente verano, el CEO de IBM se comprometió a no comercializar software de análisis o RF de IBM de conformidad con sus "Principios de Confianza y Transparencia", seguido por los principales gigantes tecnológicos como Amazon, Facebook y Microsoft, que aprobaron una moratoria de un año sobre la venta de sus productos.

La realización de estas etapas implica la disponibilidad y el uso previos de determinados datos y tecnologías.

- Un sistema de Reconocimiento Facial aprende a reconocer patrones faciales utilizando una **base de datos de formación** de imágenes. Se requiere una base de datos de formación grande, compleja y heterogénea para lograr una precisión más alta.

- La tecnología de Reconocimiento Facial combina el uso de la **Inteligencia Artificial** (el sistema es capaz de aprender mediante el análisis de los datos), el **Aprendizaje Automático** (el sistema es capaz de ampliar su capacidad para procesar y utilizar la información sin intervención humana, aprendiendo de experiencias anteriores), y el **Aprendizaje Profundo** ("**Deep Learning**") (una nueva técnica capaz de realizar un aprendizaje automático inspirada en la forma en la que las redes neuronales operan en el interior del cerebro humano).

Aplicaciones

La tecnología de Reconocimiento Facial generalmente realiza una tarea o una combinación de tareas:

Identificación

"¿Quién eres tú?"

Autenticación

"¿Eres tú realmente el que dices que eres?"

Categorización

"¿A qué grupo / categoría perteneces?"

Los sistemas de Reconocimiento Facial se utilizan mayoritariamente en relación con la seguridad y la vigilancia policial, pero también en los ámbitos de la medicina y el marketing. La lista de aplicaciones se está ampliando rápidamente.

- **Vigilancia policial** – Para localizar criminales / terroristas sospechosos, encontrar personas desaparecidas, así como para el control de accesos y el control de multitudes.
- **Seguridad** – Para desbloquear una puerta / teléfono / sistema, validar una transacción, controlar los pasajeros en un aeropuerto.
- **Centros Educativos** – Para fines de protección, monitorización de la asistencia, monitorización de la atención.
- **Medicina** – Para diagnosticar un pequeño pero potencialmente creciente número de enfermedades, así como para evaluar la gestión del dolor.
- **Redes Sociales** – Para identificar personas en fotos.
- **Marketing** – Para ofrecer publicidad "Inteligente" ('SMART').
- **Interacción Humanos - Máquinas** – Los Humanos Digitales Autónomos ("Autonomous Digital Humans") pronto interactuarán con los seres humanos y adaptarán sus respuestas de acuerdo con el Reconocimiento Facial[1].

Ventajas

Todos nosotros nos reconocemos mutuamente no por mirar nuestras huellas digitales o por los patrones de nuestro iris, sino al mirar nuestras caras.

El Reconocimiento Facial se considera como la forma **más natural de todas las mediciones biométricas**, porque no se requiere interacción física por parte del usuario final. Existen otras características específicas del cuerpo humano, como las huellas digitales, los escaneados de iris, el reconocimiento de la voz, la digitalización de las líneas de la palma de la mano y las mediciones conductuales, pero resultan más difíciles y problemáticas de implementar. El Reconocimiento Facial es **fácilmente accesible, rápido, automático y continuo**.

Los sistemas de Reconocimiento Facial pueden procesar enormes cantidades de imágenes. Por ejemplo, la policía de Reino Unido utiliza un sistema de la empresa japonesa NEC denominado *NeoFace*, capaz de escanear e identificar 300 caras por segundo.

Errores, sí... ...pero los sistemas de Reconocimiento Facial son difíciles de engañar.

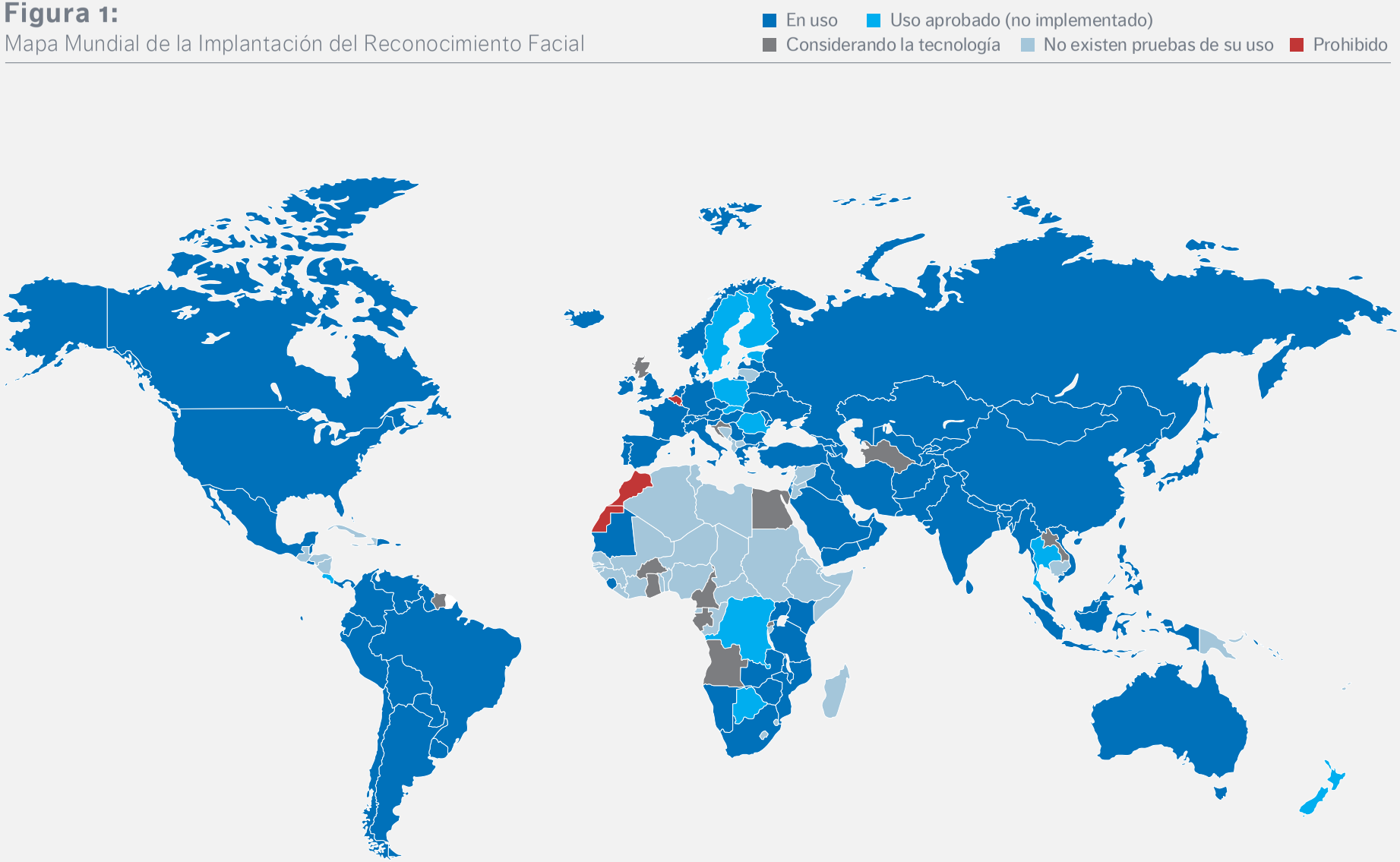
Los activistas de derechos humanos han utilizado las redes sociales para demostrar que existen combinaciones de estilos de peinado y de cosméticos que pueden resultar efectivos a la hora de engañar a los sistemas de Reconocimiento Facial.

¡Pero no todos desean pasear por el mundo con esta imagen!:

Reconocimiento Facial – Implantación en el Mundo

La tecnología se utiliza virtualmente en todo el mundo, con solo algunas modestas excepciones. Bélgica es una de estas excepciones.

Figura 1:
Mapa Mundial de la Implantación del Reconocimiento Facial

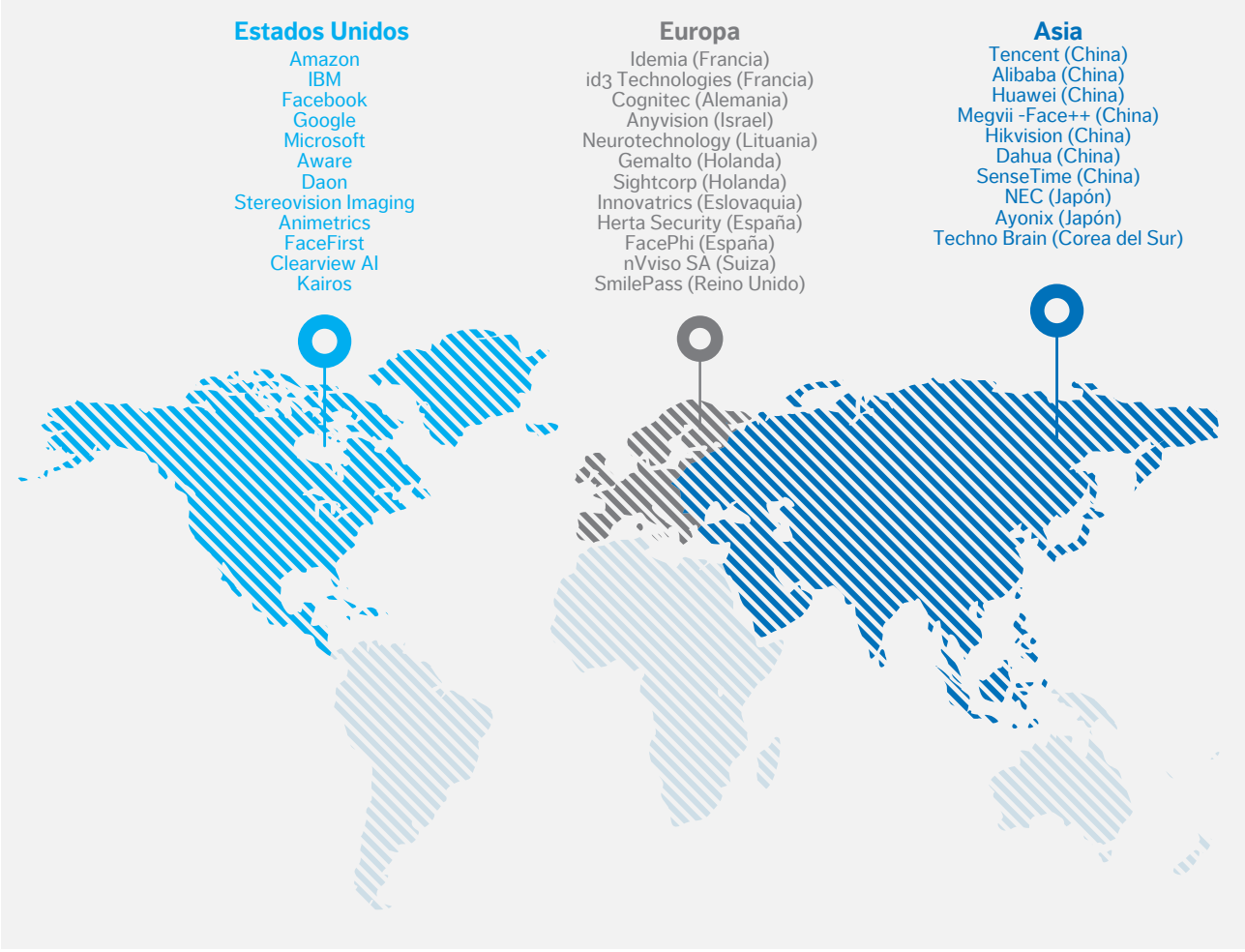


Fuente: visualcapitalist.com, mayo 2020; Candriam

Tamaño del Mercado y Actores Clave

De acuerdo con una encuesta realizada en 2018 por Allied Market Research[2], el mercado del reconocimiento facial crecerá hasta alcanzar los 9.600 millones $ en 2022, con una **tasa de crecimiento anual próxima al 25%**. Pero si consideramos todos los aspectos, este es un sector nicho. Parece que algunos gigantes tecnológicos como Amazon están incluyendo estos sistemas con carácter gratuito como **parte de la suscripción de servicios más lucrativos**.

Figura 2:
Los participantes del mercado



Fuente: Candriam

Riesgos y Controversias

A lo largo de la última década, la emergencia de la Tecnología de Reconocimiento Facial con fines de vigilancia masiva ha planteado grandes preocupaciones para la sociedad, junto con violaciones de los derechos humanos.

Una tecnología invasiva

La vigilancia mediante Reconocimiento Facial **nos afecta a un gran número de nosotros**, en muchos casos **sin nuestro conocimiento**, a medida que desarrollamos nuestras vidas cotidianas. Puede permitir la vigilancia a escala masiva, menoscabando nuestros derechos humanos.

Es cierto asimismo que millones de personas confían y alaban esta tecnología. Muchos usuarios de iPhones de alta gama de Apple utilizan la "ID Facial" para desbloquear sus smartphones. Millones de personas se han registrado en un sistema automatizado y biométrico de control fronterizo, como, por ejemplo, el "Pasaporte Electrónico ('ePassport') de Reino Unido.

En todo el mundo, los organismos policiales ya están desplegando el Reconocimiento Facial a escala masiva. **Se estima que mil millones de cámaras de vigilancia estarán en funcionamiento a finales de 2021**[3]. China es con diferencia el país líder en el uso de este sistema con 600 millones de cámaras en funcionamiento en la actualidad –una cámara por cada 2,3 ciudadanos-. De cerca le sigue Estados Unidos, con la instalación de 140 millones de cámaras –una cámara por cada 2,4 ciudadanos-. La mayoría de estas cámaras son sistemas digitales cuyas imágenes pueden ser explotadas por los sistemas de Reconocimiento Facial.

Hoy en día, los ciudadanos de Detroit, Londres, Mónaco, Moscú, Pekín y de muchos otros lugares pasean sin saber que sus rostros son escaneados por sistemas de reconocimiento facial operados por la policía.

Cuestiones relativas a la Precisión

En enero de 2020, Robert Williams, un ciudadano de Detroit, fue arrestado por la policía por el robo en una tienda tras haber sido identificado de forma errónea, mediante una identificación a través de reconocimiento facial.

En 2018, una prueba de verificación de la tecnología de Amazon, *Rekognition*, que incluía a miembros del Congreso de Estados Unidos identificó erróneamente a 28 congresistas como personas anteriormente arrestadas por haber cometido delitos[4]. La prueba reveló también el sesgo racial de la tecnología, puesto que los congresistas afro-americanos fueron identificados erróneamente de manera desproporcionada como correspondientes a la base de datos de personas arrestadas. Una de estas personas fue el último ganador de la Medalla Presidencial a la Libertad John Lewis.

Incluso los sistemas más precisos disponibles actualmente podrían ser motivo de reflexión. Se puede imaginar un organismo policial de una ciudad pequeña que utilice la tecnología de Reconocimiento Facial con una precisión del 99,9%, en la que 100.000 personas son grabadas a diario por el sistema de videovigilancia. ¿Quién se sentiría cómodo con 100 personas identificadas erróneamente cada día?

En los cuatro años de su implementación, desde 2016, el sistema de vigilancia mediante Reconocimiento Facial en directo de la Policía Metropolitana de Londres ha presentado una imprecisión del 93,59%. En dos de los despliegues realizados en 2020, el sistema 'Met' presentó una tasa de fallos del 100%, siendo incapaz de identificar a una sola persona[5]. La revisión independiente comisionada por la Policía Metropolitana observó asimismo que su sistema de vigilancia mediante Reconocimiento Facial resultaba significativamente impreciso. Su análisis examinó solo seis de las pruebas de verificación realizadas por la policía, y determinó que la precisión del sistema Met fue de solo el 19%, es decir, fue inexacto el 81% del tiempo.[6]

¿Por qué el Reconocimiento Facial, una tecnología que aporta más eficiencia y más seguridad a nuestras vidas cotidianas, puede constituir una amenaza para nuestros derechos humanos?

Isedua Oribhador, Analista Político de AccessNow, Estados Unidos: *""Aunque el reconocimiento facial ha sido publicitado como un medio para mejorar la eficiencia y la seguridad, ya hemos visto pruebas de los riesgos que se derivan del mismo. Desde los sesgos raciales y de género integrados en estos sistemas hasta los riesgos para la privacidad inherentes a la hora de recoger estos datos personales, así como el potencial de permitir la vigilancia masiva de los ciudadanos, la tecnología de reconocimiento facial plantea una amenaza fundamental para muchos derechos fundamentales. Resulta imperativo examinar estos riesgos y establecer líneas rojas cuando el uso de esta tecnología sea incompatible con el respeto de los derechos humanos."*[7]

"Los organismos chinos policiales han utilizado un sistema secreto de Reconocimiento Facial de amplia gama ***con el fin de identificar, monitorizar y controlar a los 11 millones de uigures, una minoría musulmana."***

Análisis de País - China

La Ley de Inteligencia Nacional de China de 2017 exige a las organizaciones y a los ciudadanos que "apoyen, presten asistencia y cooperen con la inteligencia del Estado". Efectivamente, cualquier empresa de software o de hardware en China está obligada a entregar los datos a Pekín si las autoridades manifiestan que existe un problema de seguridad nacional.

Más de 200 millones de cámaras de vigilancia se encontraban en funcionamiento a finales de 2018, y más de 600 millones en 2020. Entre las 10 ciudades con más cámaras en la calle por persona, Chongqing, Shenzhen, Shanghai, Tianjin y Ji'nan lideran la lista.

Las torres de Reconocimiento Facial en las ciudades chinas son emblemáticas de esta estrategia. La tecnología de Reconocimiento facial está siendo utilizada por los oficiales de policía de Pekín, los cuales utilizan actualmente gafas de sol inteligentes que escanean las caras y comunican las coincidencias.

El sistema de vigilancia civil de China se encuentra actualmente vinculado a su "Sistema de Crédito Social" que califica a las personas sobre la base de su conducta. De acuerdo con este sistema, lanzado en 2013, los ciudadanos obtienen recompensas o padecen castigos en función de sus calificaciones.

La policía china está trabajando con empresas de software de inteligencia artificial como Yitu, Megvii, SenseTime y CloudWalk. Los fabricantes de hardware como Dahua y Hikvision se benefician asimismo de los grandes pedidos del gobierno. Todas estas empresas han sido añadidas a la lista negra económica del gobierno de Estados Unidos debido a su participación en la represión del pueblo Uigur.

No obstante, las ambiciones de China en materia de IA y de tecnología RF continúan siendo grandes. El país pretende convertirse en líder mundial en IA en 2030. Como gobierno, China es claramente el mayor inversor en tecnologías avanzadas de vigilancia, IA y RF.

La represión del pueblo Uigur

Las autoridades chinas en la región de Xinjiang han utilizado la tecnología de Reconocimiento Facial con fines de caracterización racial y de vigilancia. Los organismos chinos policiales han utilizado un sistema secreto de Reconocimiento Facial de amplia gama con el fin de identificar, monitorizar y controlar a los 11 millones de uigures, una minoría musulmana. La policía china ha instalado escáneres RF a la entrada de diversas mezquitas de la región. Xinjiang ha sido un importante banco de pruebas para estas empresas, donde han podido operar sin las habituales restricciones.

Sesgo Racial / de Género, y Robo de Datos

Los primeros experimentos de Reconocimiento Facial fueron incapaces de reconocer a las personas de origen afro-americano o asiático. Y lo que es peor, Google se vio obligada a pedir disculpas en 2015 cuando su entonces nueva aplicación *Google Photos* etiquetó a algunas personas de raza negra como "gorilas".

Una encuesta realizada por el Media Lab del MIT en 2018 observó que el software de Reconocimiento Facial podía identificar a un hombre de raza caucásica con una precisión casi perfecta, pero fallaba de manera espectacular a la hora de identificar mujeres con un color de piel más oscuro.

Clearview AI declara que trabaja para más de 2.400 organismos policiales en Estados Unidos. Su CEO, Hoan Ton-That, está vinculado a movimientos políticos de extrema derecha. Clearview ha reunido miles de millones de fotos de Facebook, YouTube y Venmo para construir su base de datos[8]. El CEO y fundador de Banjo, Damien Patton, dimitió tras las acusaciones de estar vinculado al Ku Klux Klan. En aquel momento, Banjo tenía un contrato de servicios de Reconocimiento Facial por un valor de 20 m $ con el estado de Utah.

Las grandes empresas tecnológicas Amazon, Microsoft y la sociedad matriz de Google, Alphabet, han sido demandadas por utilizar fotos sin el consentimiento de las personas en el desarrollo y la formación de su tecnología de Reconocimiento Facial. Facebook pagó una indemnización de 650 millones $ de acuerdo con la ley de privacidad del estado de Illinois[9]. Los documentos filtrados por Edward Snowden demostraban que la Agencia Nacional de Seguridad en Estados Unidos había recogido millones de imágenes faciales. Las filtraciones sugerían que las fotos habían sido recogidas a partir de correos electrónicos, mensajes de texto, redes sociales y chats de vídeo[10].

Uso indebido para obtener beneficios privados e ilegales

Los investigadores sobre los medios en Rusia descubrieron que el acceso al streaming en directo del sistema de videovigilancia de Moscú estaba disponible para su venta en la "Dark Web", a través de oficiales de policía presuntamente corruptos. El centro de la ciudad de Moscú cuenta con una densa red de 175.000 cámaras de videovigilancia, la mayoría de las cuales está equipada con tecnología de Reconocimiento Facial. Puesto que el sistema tiene su base en la nube, los funcionarios corruptos pueden simplemente vender sus credenciales de acceso –por una cantidad tan ínfima como 470 $-, ofreciendo acceso al streaming en directo junto con la grabación de los cinco días previos.

Más allá de la Videovigilancia ("CCTV") – Vigilancia Masiva a través de los Ordenadores, los Smartphones, los Drones,...

Virtualmente cada nuevo smartphone, ordenador personal o tablet vendidos actualmente están equipados con al menos una cámara digital. Cada uno de estos dispositivos puede alimentar un sistema de Reconocimiento Facial.

Otro desarrollo preocupante es el despliegue de tecnología de cámaras militares en drones, como el sistema ARGUS-IS, que podría permitir a los gobiernos grabar de manera continua zonas de hasta 10 millas cuadradas / 26 kilómetros cuadrados, la mitad del tamaño de Manhattan. Estos sistemas son capaces de escanear la cara de cualquier ciudadano dentro de ese radio en cualquier momento[11].

Las Cuestiones

Falta de Consentimiento

La falta de consentimiento se encuentra en el corazón del problema. Ninguna empresa, estado, organismo o gobierno ha pedido su consentimiento a los ciudadanos. Cuando los ciudadanos presentan su foto a las administraciones o a los organismos para obtener un pasaporte, un carnet de identidad o un carnet de conducir, en la mayoría de las jurisdicciones en ningún momento otorgan su acuerdo a la utilización de su imagen con fines de Reconocimiento Facial. Otras formas de identificación biométrica implican el consentimiento de la persona que se está verificando. Las personas escaneadas mediante Reconocimiento Facial en directo probablemente no tienen conocimiento de que son objeto de una verificación de identidad, por lo que no disponen de la oportunidad de otorgar el consentimiento a su utilización o de denegarlo.

En Europa, el Reglamento General de Protección de Datos ("General Data Protection Regulation" -GDPR), aprobado en 2016, establece claramente que los datos biométricos obtenidos mediante la tecnología de Reconocimiento Facial constituyen datos personales. Estos datos están englobados en esta normativa de protección y, por lo tanto, requieren el consentimiento de la persona para que sus datos biométricos sean utilizados por cualquier otra persona, empresa u organismo. Aún así, los organismos policiales en los países de la UE como Reino Unido, Francia, Italia y Grecia ya están utilizando esta tecnología.

Falta de Base Legal

En la mayoría de los países, no existe base legal para el uso policial de la vigilancia en directo mediante Reconocimiento Facial. El Reconocimiento Facial supone una violación de las leyes sobre libertades fundamentales como la Primera Enmienda de la Constitución de Estados Unidos y la Ley de Derechos Humanos en Reino Unido.

Clare Garvie, del Law Center on Privacy & Technology de Georgetown, declaró a Candriam: *"El uso policial del reconocimiento facial actualmente no está regulado en Estados Unidos, a pesar de los esfuerzos locales y estatales por prohibir totalmente su uso, y de las recientes revelaciones que afirman que ha provocado el arresto de al menos tres hombres inocentes. A la luz de los riesgos que plantea para los derechos constitucionales estadounidenses relativos a la privacidad, la libertad de expresión, a un juicio justo y a la aplicación igualitaria de la legislación, el uso del reconocimiento facial debe ser objeto de una moratoria salvo y hasta que se apruebe una reglamentación estricta que proteja dichos derechos."*

Falta de Supervisión

En la mayoría de los países, como, por ejemplo, en Estados Unidos o Europa, se perciben pocas evidencias de una supervisión adecuada e imparcial para controlar el uso de la tecnología de vigilancia por parte de las empresas privadas y de los organismos policiales.

Intrusión Desproporcionada

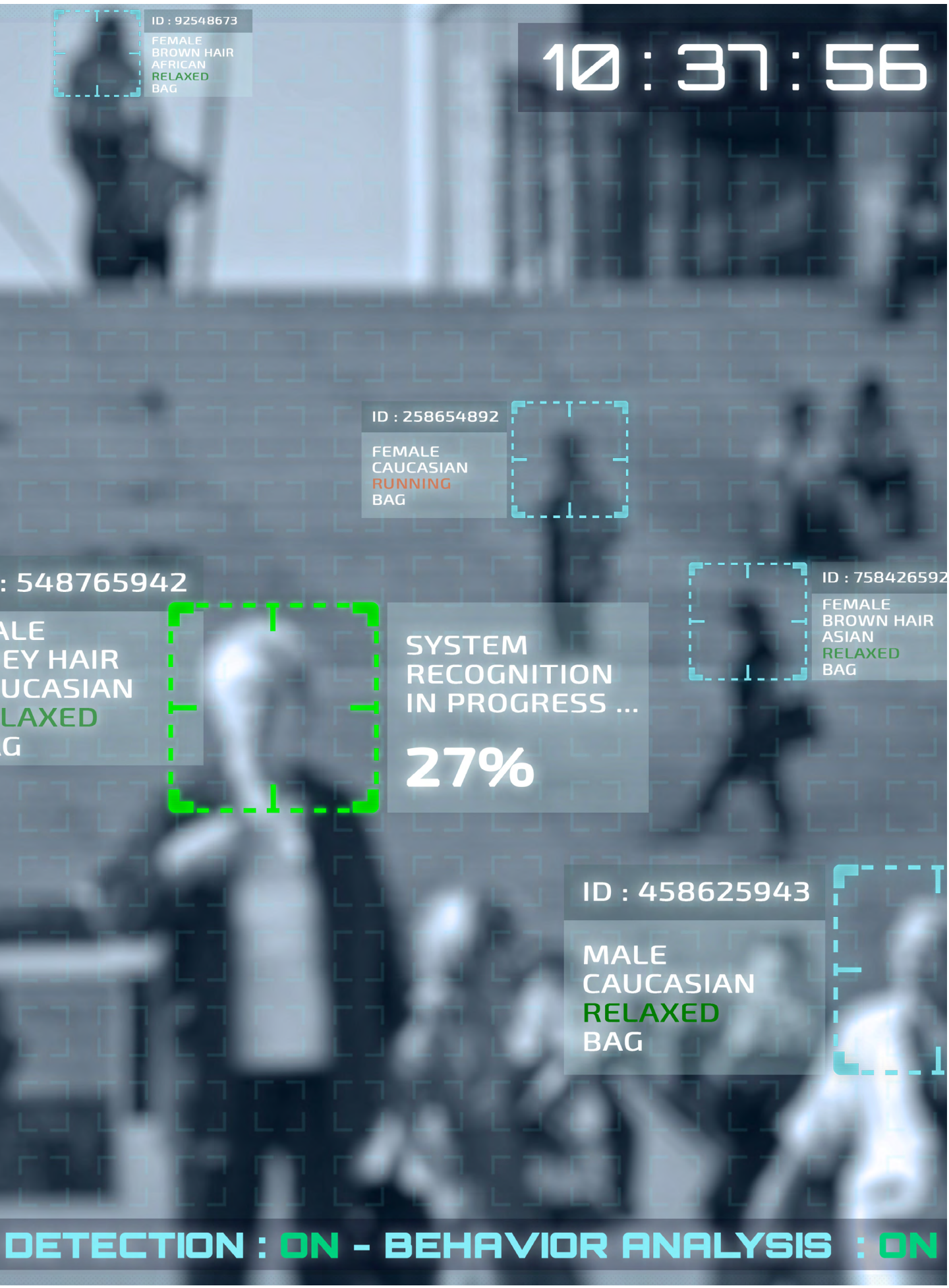
Las múltiples pruebas de verificación realizadas en Reino Unido han determinado que la ratio de éxito ha sido de un criminal buscado identificado por cada 300.000 caras escaneadas. El Comisionado de Videovigilancia ("Surveillance Camera Commissioner") concluyó que el despliegue había sido extremadamente desproporcionado, subrayando que si "se compara la escala y el tamaño del procesamiento de todas las personas que pasan delante de una cámara, el grupo que se podría pretender identificar resultaba extremadamente pequeño".

El derecho al anonimato

Una sociedad próspera se basa en diversas libertades –libertad de expresión, de movimientos, de religión, de asociación-, pero también en el derecho a un anonimato razonable. Nuestra capacidad para desplazarnos a través de espacios públicos de manera anónima ya no está garantizado a causa del amplio despliegue de los sistemas de Reconocimiento Facial. Cualquiera debe poder pasear de manera libre y anónima. Forma parte de la naturaleza humana básica desear vivir sin tener que mirar por encima del hombro. Aún así, la esfera de la vida fuera del escrutinio público se está desvaneciendo rápidamente. Ser identificado por los organismos policiales, las empresas o los gobiernos adonde quiera que vayamos supone un impedimento para nuestra individualidad. En último término implicará una restricción de los movimientos, de la creatividad, de la confianza e incluso de la democracia.

Como ilustración, el informe del Panel de Ética Policial de Londres ("London Policing Ethics Panel") sobre vigilancia policial en directo mediante Reconocimiento Facial observó que el 38% de los jóvenes de 16-24 años se mantiene alejado de eventos o lugares en los que se utiliza la vigilancia mediante Reconocimiento Facial, así como un gran número de personas de color, asiáticas y pertenecientes a minorías étnicas[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

¿La seguridad merece una pequeña pérdida de privacidad?

Cuando se les pregunta cómo se sienten acerca del Reconocimiento Facial, una mayoría de ciudadanos responde que comprende que para tener mayor seguridad se debe perder un poco de privacidad. El argumento de ser capaces de localizar rápidamente a un terrorista sospechoso o a un niño secuestrado toca una fibra sensible.

El sector de la vigilancia aprovecha y utiliza un marketing basado en el miedo. Por ejemplo, el miedo a un ataque terrorista. La ciudad francesa de Niza fue el escenario de un horrible ataque en 2016 cuando un terrorista condujo un camión a través de la multitud situada en el paseo marítimo que celebraba el día de la Bastilla, matando a 87 personas. En respuesta a este ataque, la ciudad equipó a la policía local con el mayor sistema de tecnología de vigilancia y Reconocimiento Facial de Francia.

Como ciudadanos responsables, nos debemos preguntar:

- ¿Queremos ser identificados constantemente mediante algoritmos no verificados y potencialmente inexactos, o sesgados?
- ¿Queremos que nuestro gobierno grabe todos los movimientos que hagamos, todos los lugares que visitamos y todas las personas con las que nos encontramos?
- ¿Queremos que los organismos policiales sean capaces de registrar los nombres de todos los participantes en una manifestación de protesta o en una ceremonia religiosa?
- ¿Queremos otorgar a nuestros gobiernos un poder ilimitado para vigilar ***a Todos, en Todos los Lugares, Todo el Tiempo***?

¿Una Sociedad “Esquizofrénica”?

Cuando permitimos que nuestros gobiernos y organismos policiales desplieguen tecnología de vigilancia para garantizar nuestra seguridad, afirmamos al mismo tiempo que para garantizar la seguridad de todos tenemos que vigilar a todas las personas de manera constante. Algunos sociólogos describen este hecho como una forma de esquizofrenia.

Las Diferencias Culturales Relativas a la Aceptación de la Vigilancia Estatal

No podemos analizar solo las cuestiones de derechos humanos relativas al Reconocimiento Facial a través del prisma de los valores occidentales. Las percepciones acerca de la privacidad y la intrusión varían en gran medida entre las culturas. La mayoría de las personas en China percibe que la vigilancia masiva es una contrapartida normal a cambio de la seguridad. En los últimos años, la combinación del despliegue masivo de la tecnología de vigilancia con el Sistema de Crédito Social (cuadro, página 13) ha contribuido a una drástica reducción de los índices de criminalidad.

La Ronda de Reconocimiento Perpetua

Este concepto, descrito por el Law Centre for Privacy and Technology de Georgetown[13], hace referencia a que nadie tendría que participar voluntariamente en una ronda de reconocimiento en la que una víctima deba identificar al criminal. La víctima te podría identificar a ti por error. Los sistemas de Reconocimiento Facial hacen esto todos los días, prácticamente en todas partes en Estados Unidos y en China[14].

El capitalismo de la vigilancia

En su libro "La Era del Capitalismo de la Vigilancia" ('The Age of Surveillance Capitalism'), Shoshana Zuboff define el capitalismo de la vigilancia como el proceso de ofrecer servicios gratuitos que miles de millones de personas utilizan alegremente, permitiendo a los proveedores de dichos servicios la monitorización de la conducta de estos usuarios de manera asombrosamente detallada, con frecuencia sin su consentimiento explícito. "El capitalismo de la vigilancia alega unilateralmente que la experiencia humana constituye una materia prima gratuita que se puede traducir en datos conductuales." Los capitalistas de la vigilancia obtienen enormes beneficios financieros a través de la monetización de los datos conductuales individuales y colectivos, así como de las predicciones acerca de lo que las personas harán a continuación.

La combinación de la vigilancia estatal y de su contraparte capitalista supone que la tecnología digital está **separando a los ciudadanos de todas las sociedades, los Vigilantes –invisibles, desconocidos y sin restricciones- y los Vigilados**. Este hecho tiene profundas consecuencias para la democracia, puesto que la asimetría del conocimiento se traduce en asimetrías de poder. Pero mientras que la mayoría de las sociedades democráticas disponen al menos de cierto grado de supervisión sobre la vigilancia estatal, actualmente no disponemos de ningún control regulatorio sobre su contraparte privatizada.

Compromiso – Directrices Prácticas

Como inversor responsable, nuestro papel consiste en integrar los factores medioambientales, sociales y de gobernanza (ESG) en nuestras decisiones de inversión, así como en el ejercicio de una titularidad activa. Pretendemos crear valor a largo plazo para nuestros clientes, a través de la generación de un impacto positivo sobre la economía, el medio ambiente y la sociedad en su conjunto.

Es nuestra convicción que la integración de la panorámica completa de la tecnología de Reconocimiento Facial en nuestras inversiones y el compromiso supondrán una contribución a ambos aspectos de nuestro objetivo. Un número siempre creciente de las empresas, los estados y las regiones en las que invertimos participan en esta tecnología. Aunque probablemente no invertimos deliberadamente en emisores puros dedicados al Reconocimiento Facial, la inversión en una empresa que utiliza o vende tecnologías de Reconocimiento Facial debe implicar una diligencia debida adecuada con el fin de:

- Evaluar los riesgos asociados
- Compartir nuestras preocupaciones potenciales con las empresas en las que invertimos
- Apoyar cualesquiera cambios que contribuyan a mitigar los riesgos identificados

Tal y como se describe en nuestro debate acerca de la tecnología y sus cuestiones, las expectativas de los inversores pueden ser numerosas, complejas y variar en función de los actores implicados. A continuación se reseñan algunos objetivos:

Emisores Corporativos

- **Compromiso Directo y/o Colaborativo** para comprender mejor las prácticas corporativas. Difundir las mejores prácticas a través de las empresas, las ONG, etc.

- **Integrar los desarrollos en el análisis ESG** de las empresas. Definir las mejores prácticas, los progresos aceptables, y lo que debería constituir una exclusión.

- **Fomentar la mejora de las conductas corporativas**. Continuar posicionando la ética y el respeto de los derechos humanos en el núcleo de la gobernanza corporativa. Establecer un comité independiente sobre el riesgo para los derechos humanos responsable ante el Consejo de Administración. Promover las empresas que seleccionan a los clientes y a los proveedores de acuerdo con los valores que defienden.

Gobiernos

- **Defender la suspensión del Reconocimiento Facial para tareas de vigilancia policial** hasta que no se promulgue una normativa específica.

Universidades

- **Promover las clases de ética** en los planes de estudio IA/Tecnología.

En Candriam, aunque tenemos previsto debatir este tema con las autoridades europeas, creemos que la forma más inmediata de ejercer nuestra influencia sería el compromiso con los emisores corporativos, y de manera más específica con las empresas cuyos títulos ya están incluidos en nuestras carteras.

Desde esta perspectiva, e inspirados por los intercambios con los especialistas / expertos en Reconocimiento Facial, reseñamos a continuación una serie de preguntas (Figura 2) que deberían ayudar a los inversores a la hora de evaluar el nivel de implicación de las empresas en las que invertimos en relación con el Reconocimiento Facial, así como de determinar el nivel asociado de riesgos para los derechos humanos.

Open MIC ha trabajado con los accionistas durante varios años para ejercer presión sobre las empresas tecnológicas con el fin de que adopten prácticas "éticas" con respecto al reconocimiento facial.

Las grandes empresas tecnológicas han dedicado una energía y unos recursos considerables para oponerse a estos esfuerzos. A pesar de la intensa presión ejercida por los accionistas –además de la presión global de numerosas organizaciones de derechos humanos-, las empresas se niegan en gran medida a reconocer que existe un problema. Como subraya el presente informe, casi todos los productos de reconocimiento facial existentes en el mercado operan actualmente sin el consentimiento de millones de personas cuyas caras son escaneadas de manera diaria. Se ha demostrado que muchos de estos sistemas presentan un sesgo racial. No existe recurso o reparación para aquellas personas cuyos derechos han sido violados, en contra de lo establecido en los Principios Rectores sobre Empresas y Derechos Humanos de Naciones Unidas ("Guiding Principles on Business and Human Rights"). En 2019, el Relator Especial de Naciones Unidas sobre la libertad de opinión y de expresión recomendaba "una moratoria inmediata sobre la venta y la transferencia globales de tecnología de vigilancia privada hasta que se establezcan unas salvaguardas rigurosas en materia de derechos humanos." Aunque no existen salvaguardas para los derechos humanos en vigor, las ventas continúan. En realidad, tal y como sugiere el informe, se trata de un mercado en expansión.

Una cuestión que se plantea es si la perspectiva de una reglamentación y una legislación –tanto en la Unión Europea como en Estados Unidos- hará que las empresas adopten voluntariamente unos estándares sectoriales efectivos. Las empresas ejercerán sin duda una presión conjunta para debilitar cualquier control gubernamental sobre el reconocimiento facial. Los inversores deben definitivamente continuar haciendo lo que ya están haciendo: utilizar todas las herramientas a su disposición para ejercer presión sobre las empresas tecnológicas con el fin de que estas apliquen unas políticas y unas prácticas que marquen la diferencia. Será interesante ver si un gran compromiso colaborativo, como el que se sugiere en este documento, puede hacer que las empresas se comprometan a establecer un diálogo más productivo.

Michael Connor es Director Ejecutivo y fundador de Open MIC, una organización sin ánimo de lucro que trabaja en la promoción de una mayor responsabilidad corporativa en los sectores de la tecnología y los medios de comunicación, principalmente a través del compromiso de los accionistas. Trabajando con inversores socialmente responsables, Open MIC identifica, desarrolla y respalda campañas que promueven los valores de transparencia, equidad, privacidad y diversidad, valores que aportan beneficios a largo plazo para las personas, las empresas, la economía y la salud de una sociedad democrática. Actualmente, Open MIC trabaja en campañas dirigidas a Amazon, Twitter, Google y Facebook.

Directrices de Participación

Nivel de implicación

- ¿Ofrece su empresa productos (hardware, software, bases de datos) relacionados con la Tecnología de Reconocimiento Facial?

- ¿Cuál es el propósito del producto?
  • Vigilancia
  • Identificación
  • Vigilancia policial
  • Categorización (publicidad dirigida,...)
  • Investigación
  • Seguridad
  • Otros (especificar)

- ¿A qué tipo de usuarios suministra su tecnología de Reconocimiento Facial?
  • Gobiernos o Estados
  • Centros educativos
  • Organismos policiales
  • Empresas
  • Ejércitos

Gobernanza

- ¿Ha adoptado su empresa una política cara al público en relación con la tecnología de Reconocimiento Facial? En caso afirmativo, ¿cuál es el impacto que este compromiso ha tenido
  1) sobre las relaciones con sus socios comerciales, por ejemplo, proveedores, subcontratistas, clientes, usuarios finales y
  2) sobre sus actividades de "lobbying"?

- ¿Cuáles son los riesgos que Ud. ha identificado en relación con la tecnología de Reconocimiento Facial y con qué frecuencia presenta informes al respecto al Consejo?

- ¿Realiza su empresa evaluaciones de impacto sobre los derechos humanos para identificar y evaluar los riesgos reales y potenciales derivados de sus tecnologías de Reconocimiento Facial? ¿Cuáles son los riesgos que Ud. ha identificado y cuáles son los actores clave que han participado en esta evaluación? ¿Cómo ha adaptado Ud. sus operaciones y su estrategia? ¿Quién en la empresa (a nivel corporativo / regional / de sucursal) tiene la responsabilidad global y cotidiana de abordar estos riesgos específicos y sus impactos potenciales?

- ¿Cuáles son los procesos que Ud. ha aplicado para definir a qué clientes puede vender? ¿Prohíbe Ud. las ventas / entregas de su producto o servicio a determinados países con regímenes opresivos / no democráticos?

Gestión de los riesgos relacionados con el diseño

- ¿Cuál es su organización interna dedicada a identificar, prevenir y resolver los riesgos relacionados con el Reconocimiento Facial?

De manera más específica:

- ¿Cómo su empresa construyó / obtuvo / adquirió su base de datos de formación de fotos / nombres? Si Ud. no ha construido su propia base de datos, ¿cómo su proveedor construyó / obtuvo / adquirió la base de datos que Ud. utiliza?

- ¿Ha divulgado la precisión de su tecnología, o de la tecnología de su proveedor, tras la medición de una reconocida institución científica de evaluación, como el National Institute of Standards and Technology (NIST)? En caso contrario, debatir

- ¿Cuáles son las pruebas de verificación interna que Ud. ha aplicado para detectar sesgos algorítmicos como la raza, el género o la edad? ¿Y/o su(s) proveedor(es)?

- ¿Existe algún mecanismo de reclamación en vigor para identificar e indemnizar a las personas afectadas erróneamente por la tecnología a este nivel?

Gestión de los riesgos relacionados con el uso

- ¿Sus clientes están sujetos a alguna reglamentación en relación con su uso de la tecnología de Reconocimiento Facial? ¿Se trata de una cuestión que Ud. monitorice?

- ¿Su producto ofrece tecnología de Reconocimiento Facial para su análisis en tiempo real o únicamente para su análisis retroactivo?

- ¿Su producto analiza grabaciones de video en directo o únicamente imágenes estáticas?

- ¿Su producto de tecnología de Reconocimiento Facial ofrece cualquier tipo de categorización, por ejemplo, racial, por género, edad, mental u otros? ¿Su producto de tecnología de Reconocimiento Facial ofrece cualquier tipo de análisis predictivo?

- ¿Existe algún mecanismo de reclamación en vigor para identificar e indemnizar a las personas afectadas erróneamente por la tecnología a este nivel?

Conclusión

Actualmente, el Reconocimiento Facial es un tema que no cuenta con transparencia. Su uso es alabado por algunos, mientras que para otros resulta controvertido. Se puede utilizar de manera indebida, y manifiestamente presenta sesgos y errores.

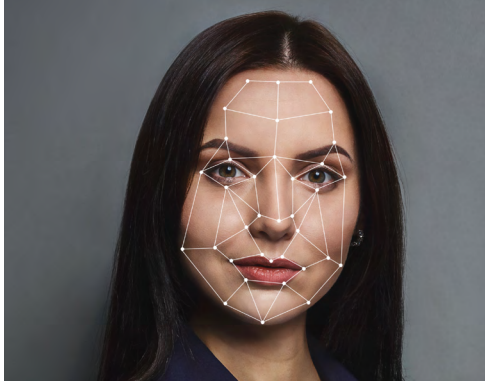
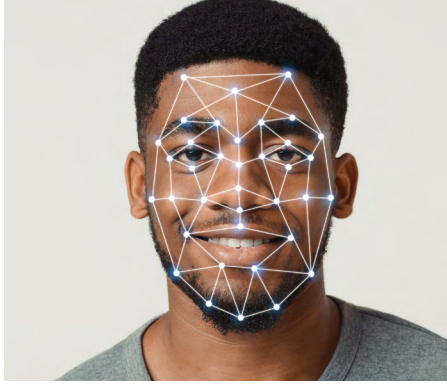
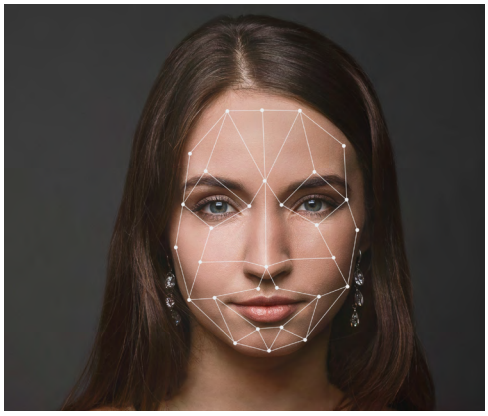
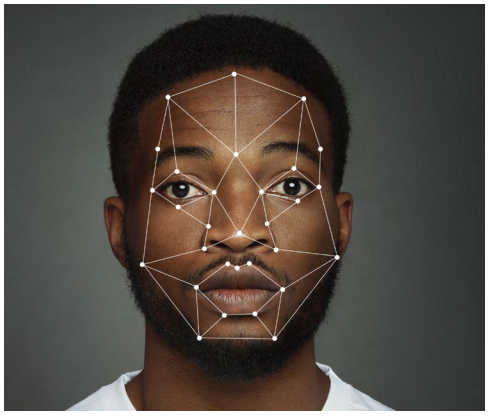
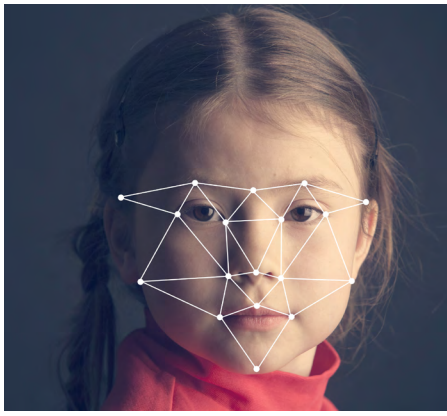
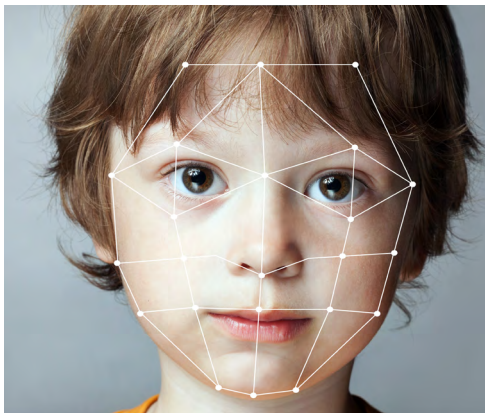
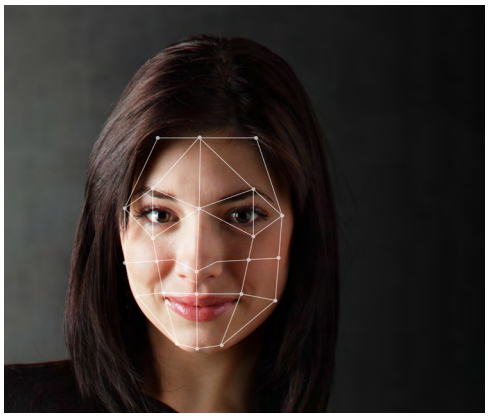
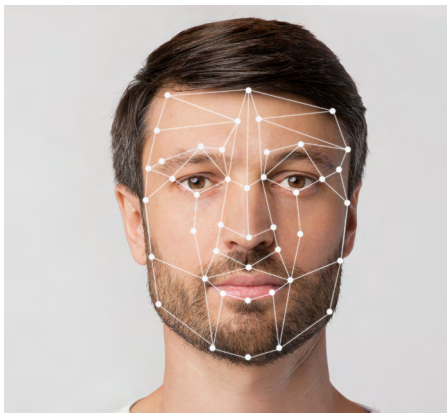
Sin transparencia, no podemos evaluar estas controversias. Para abrir la puerta al análisis y al debate, necesitamos más influencia. Las autoridades locales y nacionales están empezando a actuar. Las empresas están empezando a actuar. El impulso y el debate están creciendo entre el público, y las ONG están lanzando campañas.

Ahora es el momento de actuar para los inversores.

Notas y referencias

[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.

140.000 mill. de €

en activos gestionados
al 31 de diciembre de 2020

570

expertos
a su servicio

25 años

liderando el camino
en inversión sostenible

CANDRIAM. INVESTING FOR TOMORROW.

WWW.CANDRIAM.COM

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY