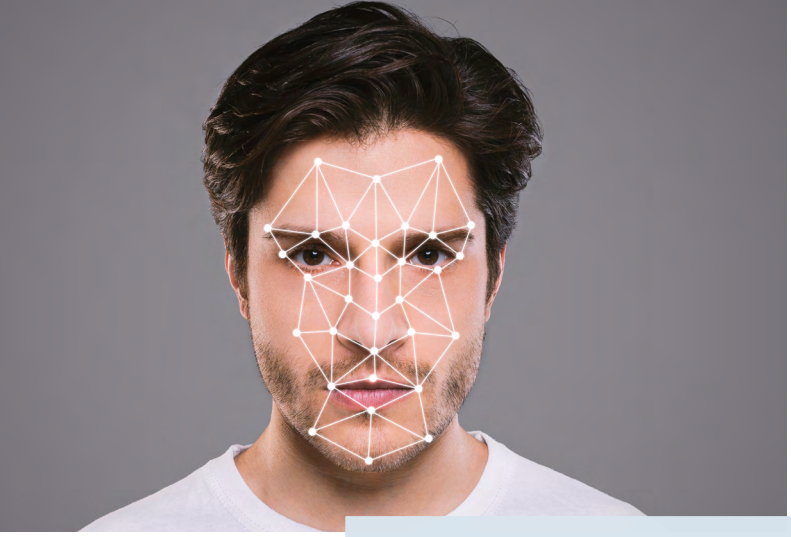
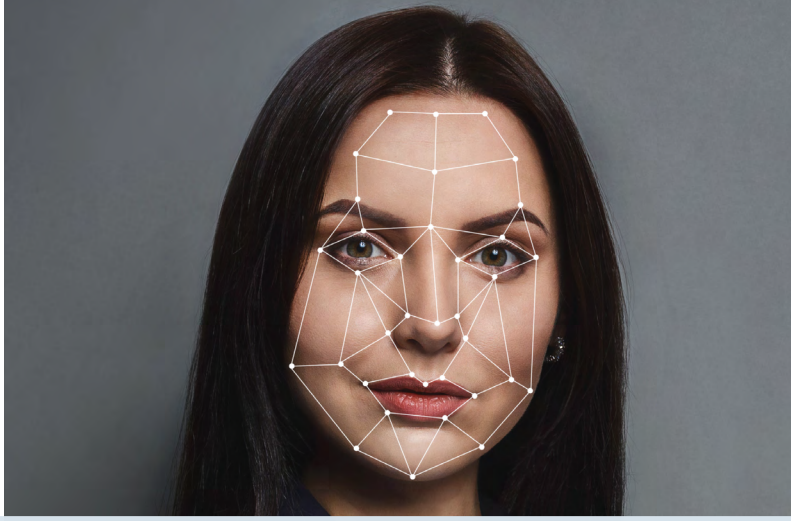
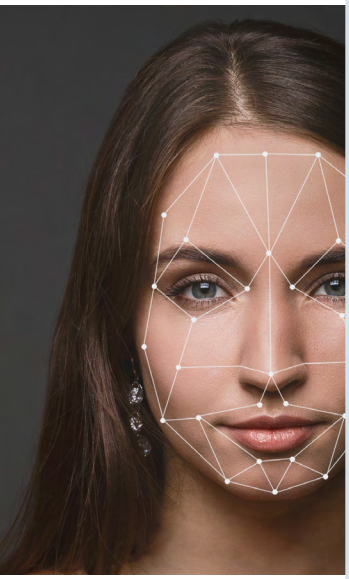
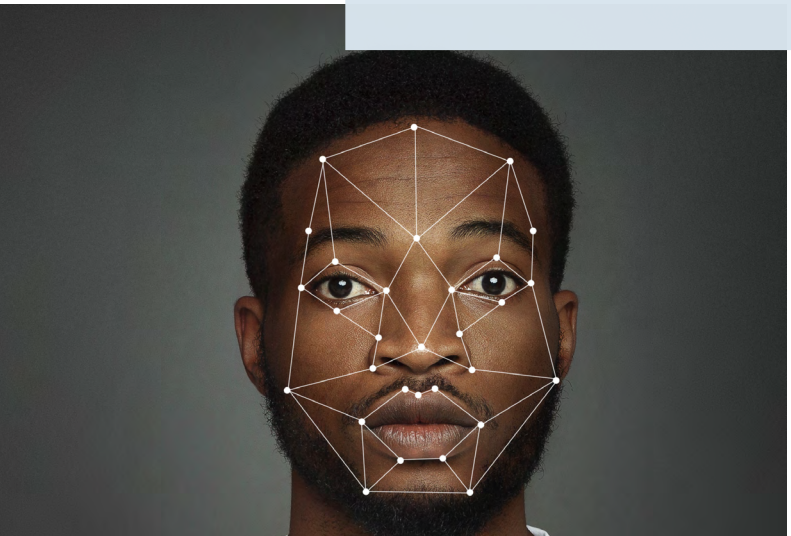
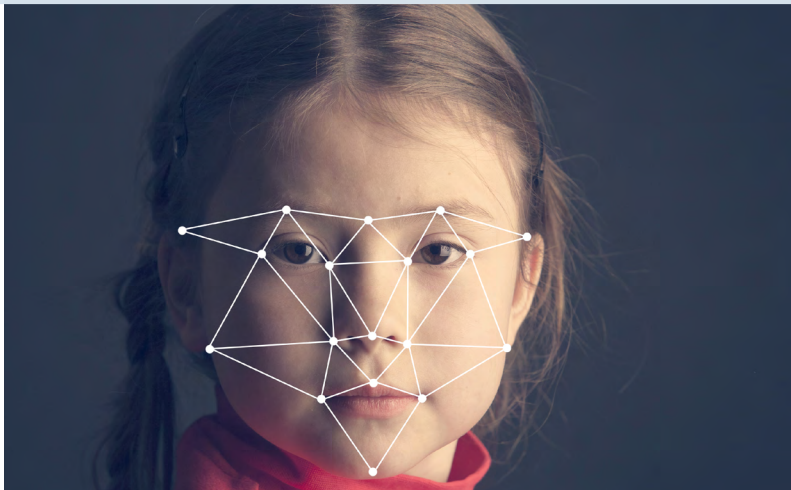





Marzo 2021

Riconoscimento facciale e diritti umani: linee guida per gli investitori

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY

Informazioni sugli autori

Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement

Benjamin Chekroun si è unito a Candriam nel 2018 nella veste di viceresponsabile Obbligazioni convertibili e nel 2020 ha assunto il suo attuale ruolo nella Gestione responsabile. Prima di unirsi a Candriam, era impiegato dal 2014 presso ABN AMRO Investment Solutions, dove si occupava della strategia delle obbligazioni convertibili globali. Ha trascorso quattro anni a Hong Kong, un anno a New York e tredici anni a Londra, lavorando come agente di borsa specializzato in obbligazioni convertibili. Nel 2004, il fondo gestito da Chekroun ha vinto il premio Best Convertible Arbitrage Fund (per il miglior fondo con strategia di arbitraggio convertibile) conferito da Hedge Fund Review. Benjamin è specializzato in economia aziendale internazionale.

Sophie Deleuze

Lead ESG Analyst, Stewardship

Sophie Deleuze è entrata a far parte del reparto di ricerca ESG di Candriam nel 2005. Dopo più di un decennio nelle vesti di analista ESG, si è specializzata nelle attività di Candriam relative a engagement, voto per delega e gestione responsabile, coordinando il nostro impegno con l'analisi ESG e tutti i team di gestione degli investimenti. Prima di lavorare per Candriam, è stata analista SRI per quattro anni presso BMJ CoreRatings e Arese. Laureata in Ingegneria del trattamento delle acque, Sophie si è specializzata in Affari pubblici ambientali.

Quentin Stevenart

ESG Analyst

Quentin è entrato a far parte del team ESG di Candriam come analista nel 2016. Si occupa dell'analisi ESG completa del settore IT e delle problematiche relative alla governance comuni a tutti i settori. Coordina inoltre le attività di ricerca di Candriam relative all'economia circolare. Quentin si è laureato in Management presso la Louvain School of Management e in Ingegneria gestionale presso l'Université catholique de Louvain.

Indice

“Sebbene la tecnologia in sé sia promettente e possa essere utilizzata in modo positivo, il modo in cui oggi si progettano e si utilizzano i sistemi di riconoscimento facciale comporta alcuni rischi e ha diverse implicazioni sociali per chi investe in questo segmento. Sono quindi benvenuti l’impegno e gli sforzi degli investitori che assumono un ruolo di guida sul piano etico al fine di anticipare la direzione che prenderanno le normative e ampliare l’elenco dei convenzionali problemi di ESG per capire come, dove, quando e da chi il riconoscimento facciale possa essere utilizzato in modo corretto.”

- Katherine Ng, Responsabile Ricerca accademica, UN, Principi di investimento responsabile

Sintesi

Investire in modo responsabile non significa solo affrontare i rischi e i problemi del mondo di oggi. Significa pensare spingendosi oltre i limiti dell'impronta ecologica e del cambiamento climatico, valutando i rischi e le opportunità che ci riserva il futuro.

La tecnologia ha assicurato al mondo incredibili benefici e straordinarie possibilità di investimento. È grazie alla tecnologia che molti professionisti hanno potuto continuare a lavorare da casa durante la pandemia ancora in atto. Una parte significativa della campagna elettorale del presidente Biden è stata portata avanti da casa sua. Tuttavia, dobbiamo essere consapevoli che ogni nuova tecnologia può avere conseguenze negative.

La tecnologia di riconoscimento facciale (FRT) consente di aumentare efficienza e sicurezza. Può essere utilizzata per sbloccare gli smartphone più all'avanguardia e per i controlli di imbarco negli aeroporti. Ha però alcune implicazioni sul piano dei diritti umani. La FRT viene sviluppata ormai da diversi decenni, ma solo adesso inizia a diffondersi su larga scala.

Nel 2021 circa 300 investitori hanno risposto a un questionario proposto da Candriam. Il 30% ha dichiarato di ritenere la tecnologia di riconoscimento facciale uno strumento utile e comodo. Circa il 70% aveva alcune riserve in merito: il 31% non riteneva la FRT accurata, mentre il 38% riteneva necessario valutare l'utilizzo di questa tecnologia dal punto di vista etico.

La tecnologia pone infatti alcuni problemi sul piano etico, come la mancanza del consenso delle persone interessate e di un'adeguata supervisione. Sono infatti in aumento i casi di identificazione errata, che a volte sfociano in arresti ingiusti, in particolare per le persone non di pelle bianca. Nel maggio del 2019, la città di San Francisco, dove la tecnologia di riconoscimento facciale ha mosso i primi passi, ne ha vietato l'utilizzo da parte delle forze dell'ordine. Poco dopo, diverse grandi aziende del settore della tecnologia hanno annunciato l'intenzione di sospendere per un anno la vendita dei propri prodotti per il riconoscimento facciale.

Per comprendere i problemi che possono emergere in futuro sul piano dei diritti umani, è necessario che gli investitori responsabili e gli altri soggetti interessati prendano posizione fin da ora.

Non sarebbe stato possibile condurre questo studio senza il prezioso sostegno delle organizzazioni e delle persone elencate di seguito. Desideriamo pertanto ringraziarle per i contributi dati nonché per il tempo e la pazienza dedicati a questo progetto:
- *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 tecnologia

Come funziona?

La FTR fa parte della famiglia delle tecnologie di riconoscimento biometrico. Il riconoscimento facciale è il processo di **identificazione** o di **verifica dell'identità** di una persona mediante un'immagine o un filmato che ne ritrae il viso. Comporta l'acquisizione, l'analisi e il confronto dell'immagine con schemi basati sui tratti somatici della persona. Per garantire una maggiore accuratezza, alcuni sistemi utilizzano immagini tridimensionali.

La tecnologia di riconoscimento facciale opera secondo una procedura costituita da tre fasi:

- **Il rilevamento del volto** è una fase fondamentale in cui il sistema rileva e individua i volti umani all'interno di immagini e filmati.
- **L'acquisizione del volto** trasforma informazioni di tipo analogico, ovvero il volto stesso, in una serie di dati digitali che descrivono i tratti somatici della persona. In questa fase vengono misurate decine di parametri relativi al volto, come la distanza tra gli occhi, la lunghezza del naso, il contorno di labbra, orecchie, mento, ecc.
- **Il confronto tra volti** verifica se due volti corrispondono alla stessa persona.

L'algoritmo fornisce un risultato associato a un valore probabilistico, ad esempio "*Corrispondenza positiva – Pinco Pallino – Probabilità del 97,36%*".

Breve storia del riconoscimento facciale

Il riconoscimento facciale nasce negli anni '60. Woody Bledsoe, un vescovo mormone co-fondatore di Panoramic Research a Palo Alto (California) sviluppò un sistema per inserire manualmente in un computer i tratti somatici del viso di una persona. Sebbene il sistema non possa essere considerato efficace secondo gli standard attuali, dimostrò che il viso era un parametro biometrico valido. L'accuratezza dei sistemi di riconoscimento aumentò nel corso degli anni '70, man mano che i ricercatori aggiungevano ulteriori marcatori facciali. Negli anni '80 e '90 la tecnologia FTR fece un vero balzo in avanti grazie a nuovi metodi per l'individuazione del viso in un'immagine e per l'estrazione dei tratti rilevanti, che resero finalmente possibile la completa automatizzazione del riconoscimento facciale. Nel 1996 il programma statunitense FERET portò alla creazione del primo database di volti. In occasione del Super Bowl del 2001 le forze dell'ordine collaudarono per la prima volta il riconoscimento facciale di massa, identificando tra la folla 19 criminali ricercati. I progressi più significativi sono quelli compiuti dal 2010 in avanti, che hanno consentito di migliorare la tecnologia utilizzando le reti neurali profonde. Nel 2011 la tecnologia di riconoscimento facciale ha contribuito alla verifica dell'identità di Osama Bin Laden quando venne ucciso nel corso di un raid statunitense. Facebook adottò la FRT per aggiungere tag alle foto e, nel 2014, il suo programma DeepFace fu il primo a ottenere prestazioni di riconoscimento facciale paragonabili a quelle degli esseri umani. Nel 2017, l'iPhone X fu il primo smartphone disponibile al pubblico con la funzionalità di sblocco mediante riconoscimento facciale e segnò l'inizio della diffusione di massa di questa tecnologia. Nel 2019, San Francisco è stata la prima grande città degli USA a vietare agli organismi preposti all'applicazione della legge l'uso del riconoscimento facciale. L'estate seguente, l'amministratore delegato di IBM si è impegnato a non fornire più software IBM per il riconoscimento facciale o per analisi correlate nel rispetto dei "Principi di fiducia e trasparenza" dell'azienda; il gesto è stato in seguito imitato dai principali giganti del settore informatico, compresi Amazon, Facebook e Microsoft, che hanno sospeso per un anno la vendita dei prodotti correlati.

Per applicare una dopo l'altra queste procedure è necessario avere prima a disposizione e poter utilizzare determinati dati e tecnologie.

- I sistemi di riconoscimento facciale imparano a riconoscere gli schemi presenti nei volti esercitandosi su un **database di immagini di addestramento**. Per avere risultati estremamente accurati è necessario che il database di addestramento sia ampio, eterogeneo e con un buon grado di complessità.

- La tecnologia di riconoscimento facciale unisce l'utilizzo dell'**intelligenza artificiale** (il sistema è in grado di imparare analizzando i dati), dell'**apprendimento automatico** (il sistema è in grado di aumentare la propria capacità di elaborazione e di utilizzare le informazioni autonomamente, senza l'intervento umano, imparando dalle esperienze precedenti) e dell'**apprendimento profondo** (detto anche *deep learning*, una nuova tecnica di apprendimento automatico basata su meccanismi ispirati al funzionamento delle reti neurali all'interno del nostro cervello).

Applicazioni

La tecnologia di riconoscimento facciale esegue generalmente una o più delle attività seguenti:

Identificazione

"Chi sei?"

Autenticazione

"Sei davvero chi dici di essere?"

Classificazione/ profilazione

"A che gruppo/ categoria appartieni?"

I sistemi di riconoscimento facciale vengono utilizzati prevalentemente per garantire la sicurezza e l'applicazione della legge, tuttavia sono utili anche in ambito medico e nel settore del marketing. L'elenco delle potenziali applicazioni cresce rapidamente.

- **Applicazione della legge**: rintracciamento di sospetti criminali/ terroristi, ritrovamento di persone scomparse, controllo degli accessi, controllo della folla
- **Sicurezza**: sblocco di porte/telefoni/sistemi, validazione di transazioni, controllo passeggeri in aeroporto
- **Scuole**: sicurezza, rilevamento presenze, monitoraggio dell'attenzione
- **Medicina**: diagnosi di alcune malattie (per ora si tratta di un numero ridotto di condizioni, che potrebbe però aumentare in futuro), valutazione della gestione del dolore
- **Social network**: identificazione delle persone nelle immagini
- **Marketing**: funzioni di pubblicità "smart"
- **Interazione uomo-macchina**: presto dei veri "esseri umani digitali" autonomi potranno interagire con gli esseri umani e adattare le proprie risposte alla situazione grazie a funzioni di riconoscimento facciale.[1]

Vantaggi

Per riconoscerci, nella vita quotidiana non ci basiamo sulle impronte digitali o gli schemi di linee presenti nelle iridi, ci guardiamo semplicemente in viso.

Il riconoscimento facciale è considerato **la forma di riconoscimento biometrico più naturale**, perché non richiede alcuna interazione fisica da parte dell'utente finale. Esistono altri sistemi per individuare tratti identificativi nel corpo umano, ad esempio l'analisi delle impronte digitali, la scansione dell'iride, il riconoscimento vocale, la digitalizzazione dei vasi sanguigni visibili nel palmo della mano; si possono inoltre individuare alcuni parametri comportamentali, che sono però più complessi e difficili da utilizzare. Il riconoscimento facciale è **facilmente accessibile, rapido, automatico e immediato**.

I sistemi per FTR sono in grado di elaborare grandi quantità di immagini. Ad esempio, la polizia del Regno Unito utilizza *NeoFace*, un sistema prodotto dall'azienda giapponese NEC, capace di scansionare e identificare fino a 300 volti al secondo.

I sistemi FRT possono sbagliare... ...ma non è semplice ingannarli.

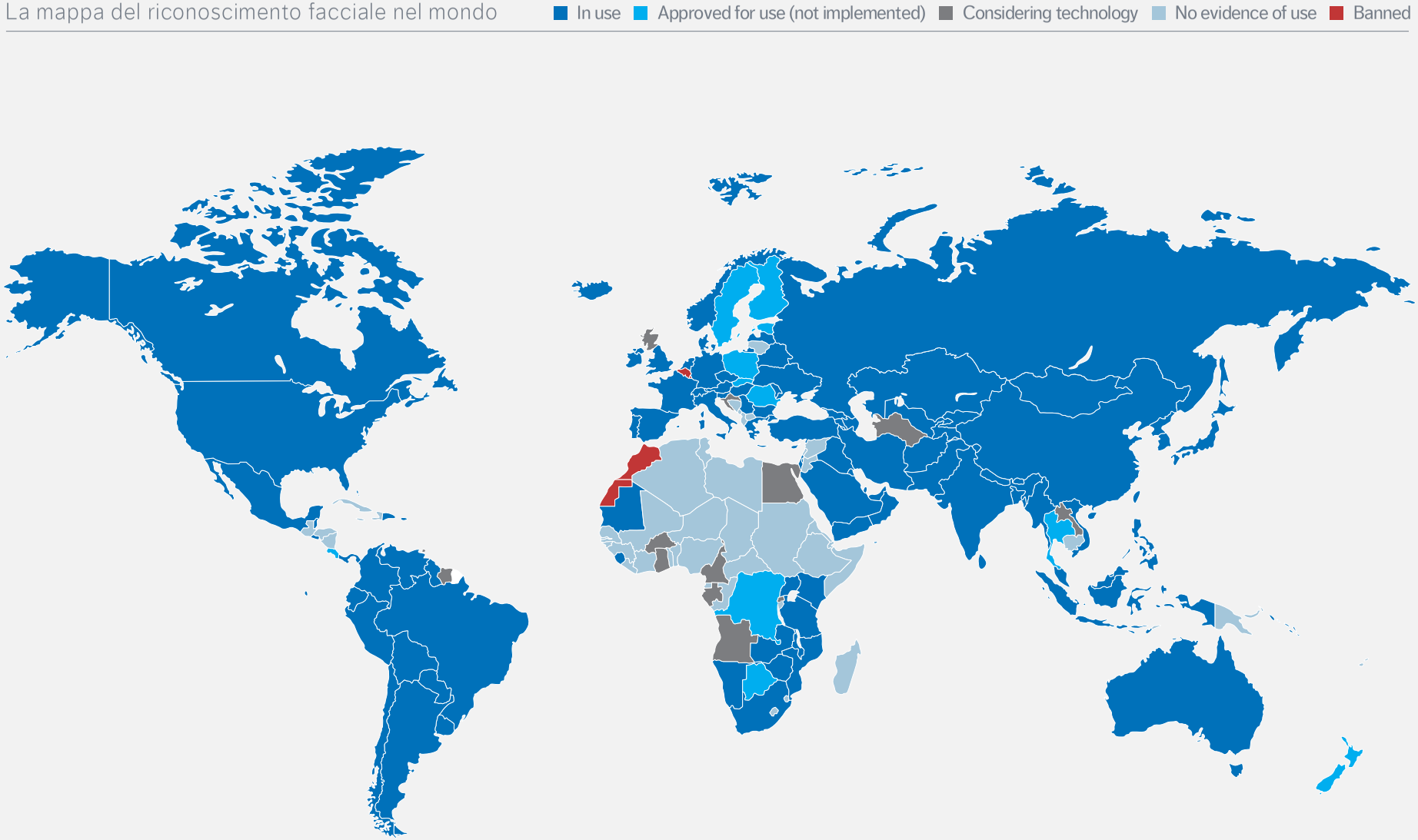
Gli attivisti per i diritti umani hanno utilizzato i social network per mostrare combinazioni di pettinatura e trucco che possono rivelarsi efficaci per ingannare i sistemi di riconoscimento facciale.

Ma poche persone sarebbero disposte ad andare in giro pettinate così:

Il riconoscimento facciale nel mondo

La FTR è una tecnologia utilizzata praticamente in tutto il mondo, con qualche piccola eccezione. Il Belgio è una di queste eccezioni.

Figura 1:
La mappa del riconoscimento facciale nel mondo

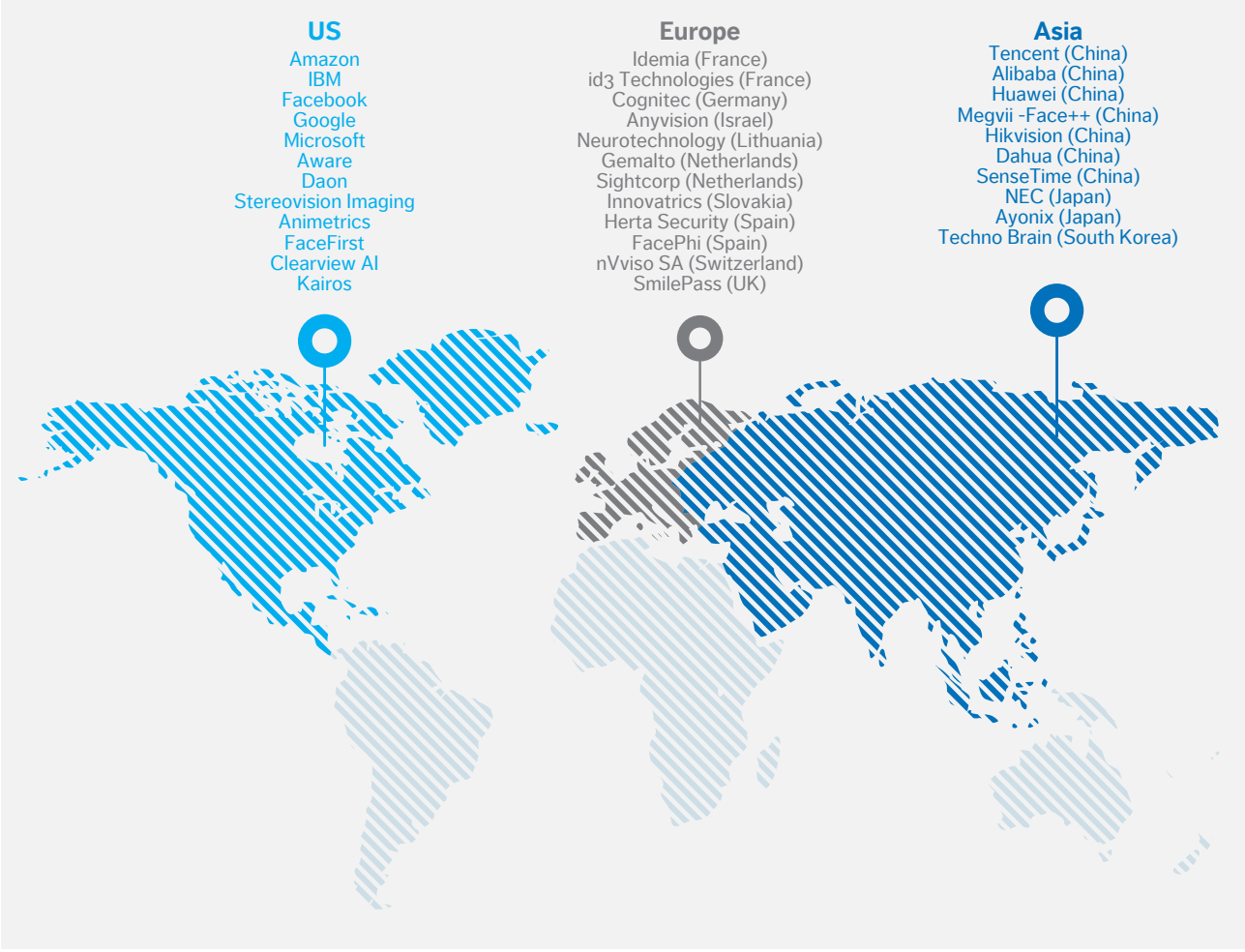


Fonte: visualcapitalist.com, maggio 2020; Candriam

Dimensioni del mercato e principali protagonisti

Secondo i dati di un sondaggio condotto nel 2018 da Allied Market Research[2], il mercato del riconoscimento facciale crescerà fino a toccare i 9,6 miliardi di dollari USA entro il 2022, con un **tasso di crescita annuale vicino al 25%**, eppure si tratta, tutto considerato, di un settore di nicchia. Sembra che alcune grandi aziende del settore tecnologico stiano includendo a titolo gratuito i propri sistemi FTR in **pacchetti di abbonamento a servizi più remunerativi**.

Figura 2:
Operatori del mercato



Fonte: Candriam

Rischi e aspetti controversi

Nel corso dell'ultimo decennio, la diffusione della tecnologia di riconoscimento facciale per la sorveglianza di massa ha fatto emergere alcune preoccupazioni a livello sociale affiancate a violazioni dei diritti umani.

Una tecnologia invadente

La sorveglianza mediante riconoscimento facciale **interessa un numero elevato di persone** e in molti casi viene effettuata **senza che noi ne siamo a conoscenza** in contesti che frequentiamo quotidianamente. Questa tecnologia consente una sorveglianza di massa su larga scala, con implicazioni anche sul fronte dei diritti umani.

Tuttavia, milioni di persone fanno volontariamente affidamento sul riconoscimento facciale e sono felici di poterlo utilizzare. Molti utenti di iPhone Apple di fascia alta usano l'identificazione tramite riconoscimento facciale per sbloccare i propri smartphone. Milioni di persone si sono registrate su sistemi automatici per il controllo biometrico di frontiera, come l'ePassport del Regno Unito.

In tutto il mondo, le forze dell'ordine stanno già utilizzando il riconoscimento facciale su larga scala. **Si stima che entro la fine del 2021 il numero delle videocamere di sorveglianza attive toccherà il miliardo**[3]. La Cina è di gran lunga il Paese in cui la FTR è più utilizzata: si stima che ad oggi vi siano 600 milioni di videocamere attive, una ogni 2,3 cittadini. Seguono a poca distanza gli Stati Uniti, dove si stima che le videocamere installate siano 140 milioni, una ogni 2,4 cittadini. Nella maggior parte dei casi si tratta di sistemi digitali le cui immagini possono essere sfruttate dai sistemi di riconoscimento facciale.

I cittadini di Detroit, Londra, Monaco, Mosca, Pechino e altre città passeggiano ignari del fatto che i loro volti vengono scansionati da sistemi di riconoscimento facciale gestiti dalle forze dell'ordine.

Problemi di accuratezza

Nel gennaio del 2020 Robert Williams, un abitante di Detroit, è stato arrestato dalla polizia per taccheggio in seguito a un errore di identificazione avvenuto a causa dell'utilizzo di un sistema di riconoscimento facciale.

Nel 2018 è stato effettuato un test della tecnologia di Amazon, Rekognition, sui membri del Congresso statunitense; il sistema di riconoscimento ha identificato 28 parlamentari come persone già arrestate in precedenza per aver commesso un reato[4]. Il test ha inoltre messo in luce il problema legato alle diverse prestazioni della tecnologia a seconda del profilo razziale: i parlamentari afroamericani sono infatti stati vittime di una frazione sproporzionata degli errori del sistema, che ha associato i loro volti a persone già arrestate presenti nel database. Uno di loro era John Lewis, insignito della Medaglia presidenziale della libertà.

Anche i sistemi più accurati attualmente disponibili possono sbagliare in modo significativo. Immaginate cosa succederebbe se le forze dell'ordine di una cittadina utilizzassero una tecnologia di riconoscimento facciale accurata al 99,9% sulle 100.000 persone filmate quotidianamente dalle videocamere a circuito chiuso. Chi sarebbe disposto ad avere ben 100 persone ogni giorno identificate in modo errato?

Nell'arco di quattro anni, a partire dal 2016, il sistema di sorveglianza con riconoscimento facciale in tempo reale utilizzato dalla polizia metropolitana di Londra ha dimostrato un'inaccuratezza del 93,59%. Il cosiddetto "Met" è stato utilizzato tre volte nel 2020 e in due occasioni su tre ha registrato un tasso di errore del 100%, ovvero non è riuscito a identificare neanche una persona[5]. Anche la verifica indipendente commissionata dalla polizia metropolitana ha confermato che il sistema di sorveglianza mediante riconoscimento facciale era estremamente inaccurato. Sono stati analizzati solo sei dei test effettuati dalla polizia, calcolando un tasso di accuratezza del Met di appena il 19%, il che significa che il sistema sbagliava l'81% delle volte[6].

Perché il riconoscimento facciale, una tecnologia che rende più efficienti e sicure le nostre attività quotidiane, rappresenta anche una minaccia per i diritti umani?

Isedua Oribhabor, specializzata nell'analisi della politica statunitense per AccessNow, osserva: *"Nonostante la tecnologia di riconoscimento facciale sia stata presentata come un mezzo per aumentare l'efficienza e la sicurezza, abbiamo già alcune prove dei rischi che comporta. A partire dalle distorsioni delle prestazioni legate a razza e sesso intrinseche di questi sistemi fino ai rischi per la privacy associati alla raccolta di questo genere di dati personali, passando per il potenziale utilizzo come strumento per la sorveglianza di massa dei cittadini, la FTR rappresenta una grave minaccia per molti diritti fondamentali. È essenziale che questi rischi vengano analizzati e che venga tracciato un confine oltre il quale l'utilizzo di questa tecnologia non è compatibile con la tutela dei diritti umani."*[7]

*“Le forze dell’ordine cinesi hanno utilizzato un sistema di riconoscimento facciale segreto ad ampio raggio **per identificare, monitorare e controllare gli 11 milioni di Uiguri, una minoranza in gran parte musulmana.**”*

Approfondimento: la Cina

La legge cinese sull'intelligence nazionale promulgata nel 2017 impone a organizzazioni e cittadini di sostenere, assistere e cooperare con i reparti di intelligence del governo. Di fatto, qualsiasi azienda cinese che si occupi di software o hardware è obbligata a fornire i dati in suo possesso alle autorità qualora si sospetti una minaccia per la sicurezza nazionale.

Alla fine del 2018 si contavano oltre 200 milioni di videocamere di sorveglianza attive e si stima che questo dato abbia superato i 600 milioni nel 2020. Chongqing, Shenzhen, Shanghai, Tianjin, e Jinan sono in testa alla lista delle 10 città con il maggior numero di videocamere per persona negli spazi pubblici.

I pali per il riconoscimento facciale installati nelle città cinesi sono il simbolo di questa scelta. L'uso della FTR si sta diffondendo tra la polizia di Pechino, che utilizza occhiali da sole "smart" in grado di scansionare i volti e segnalarne l'eventuale presenza nei database.

Il sistema di sorveglianza dei civili adottato dalla Cina è collegato a un "sistema di credito sociale" che assegna una valutazione ai singoli individui in base al loro comportamento. Il sistema è entrato in funzione nel 2013 e distribuisce ai cittadini ricompense o punizioni a seconda del punteggio che ottengono.

La polizia cinese collabora inoltre con aziende che sviluppano software basati sull'intelligenza artificiale, come Yitu, Megvii, SenseTime e CloudWalk. Anche i produttori di hardware come Dahua e Hikvision possono trarre vantaggio dai considerevoli ordini di prodotti effettuati dal governo. Tutte queste aziende sono state aggiunte alla blacklist economica del governo statunitense a causa del loro coinvolgimento nella repressione degli Uiguri.

Nonostante questo, la Cina continua a puntare in alto nel settore della FTR e dell'intelligenza artificiale (IA) per diventare entro il 2030 uno dei leader mondiali nel campo dell'IA. Il governo cinese è ovviamente il più grande investitore nel settore delle tecnologie di sorveglianza avanzate, IA e FTR.

La repressione degli Uiguri

Le autorità cinesi della regione di Xinjiang si sono servite della tecnologia di riconoscimento facciale per effettuare attività di sorveglianza e profilazione razziale. Le forze dell'ordine cinesi hanno utilizzato un sistema di riconoscimento facciale segreto ad ampio raggio per identificare, monitorare e controllare gli 11 milioni di Uiguri, una minoranza in gran parte musulmana. La polizia cinese ha installato scanner per il riconoscimento facciale all'ingresso di diverse moschee della regione. Quello avvenuto a Xinjiang è stato un test importante per le aziende coinvolte, che hanno potuto operare senza sottostare alle normali limitazioni.

Distorsione delle prestazioni per sesso/razza e furto di dati

Durante i primi esperimenti di riconoscimento facciale i sistemi non riuscivano a riconoscere le persone di origine asiatica o afroamericana. Ma c'è di peggio: Google nel 2015 fu costretto a scusarsi quando la nuova applicazione *Google Foto* etichettava alcune persone di colore come "gorilla".

Da un sondaggio effettuato dal MIT Media Lab nel 2018 è emerso che alcuni software di riconoscimento facciale erano in grado di identificare un uomo bianco con un'accuratezza quasi perfetta, mentre commettevano errori colossali cercando di identificare donne con la pelle più scura.

Clearview AI afferma di collaborare con oltre 2.400 organi di polizia statunitensi. L'amministratore delegato dell'azienda, Hoan Ton-That, è legato a movimenti politici di estrema destra. Clearview AI ha costruito un database prelevando miliardi di immagini da Facebook, YouTube e Venmo[8]. L'amministratore delegato della società di software di sorveglianza Banjo, Damien Patton, si è dimesso dopo essere stato accusato di avere un legame con il Ku Klux Klan In quel periodo Banjo aveva stretto con lo stato dello Utah un contratto per servizi di riconoscimento facciale da 20 milioni di dollari.

Le grandi società tecnologiche Amazon, Microsoft e Alphabet (la società che controlla Google) sono state denunciate per aver utilizzato fotografie senza avere i consensi necessari allo scopo di sviluppare e addestrare la propria tecnologia di riconoscimento facciale. Facebook ha dovuto corrispondere per questo motivo 650 milioni di dollari nel rispetto della normativa sulla privacy dello stato dell'Illinois[9]. Alcuni documenti diffusi da Edward Snowden dimostrano che l'NSA (l'agenzia nazionale di sicurezza statunitense) ha raccolto milioni di immagini di volti. I documenti diffusi suggeriscono che le foto raccolte siano state prelevate da e-mail, messaggi di testo, social network e *videochat*[10].

Abusi a scopo di profitto personale e illegale

In Russia, durante un'indagine sui mezzi di informazione, è emerso che i video trasmessi in tempo reale dalle telecamere a circuito chiuso di Mosca erano in vendita sul *dark web*, presumibilmente messi a disposizione da membri corrotti delle forze dell'ordine. Il centro di Mosca è coperto da una fitta rete di 175.000 videocamere a circuito chiuso, la maggior parte delle quali è dotata di tecnologia per il riconoscimento facciale. Poiché il sistema è basato su *cloud*, il personale corrotto poteva semplicemente vendere le proprie credenziali di accesso per cifre che partivano da appena 470 dollari USA, consentendo così di accedere ai video trasmessi in tempo reale e alle registrazioni dei cinque giorni precedenti.

Oltre il circuito chiuso: la sorveglianza di massa attraverso PC, smartphone, droni, ecc.

Praticamente ogni nuovo smartphone, computer o tablet moderno è provvisto di almeno una fotocamera digitale. Ogni fotocamera può inviare dati a un sistema di riconoscimento facciale.

Un altro sviluppo preoccupante è dato dall'impiego su droni della tecnologia delle videocamere militari, come il sistema ARGUS-IS, che potrebbe consentire ai governi di registrare in modo continuativo immagini di zone fino a 26 km quadrati di estensione, ovvero grandi la metà di Manhattan. Questi sistemi sono in grado di scansionare in ogni momento il volto di qualsiasi cittadino che si trovi entro il loro raggio di azione[11].

I problemi

Assenza del consenso

La mancata richiesta di consenso è il cuore del problema. Nessuna azienda, nessuno stato, ente o governo ha chiesto il consenso dei cittadini. Quando una persona invia la propria fotografia a un organo amministrativo o a un'organizzazione per richiedere il passaporto, la carta d'identità o la patente, nella maggior parte delle giurisdizioni non fornisce in alcun punto della procedura burocratica il suo consenso all'utilizzo della propria immagine per il riconoscimento facciale. Per l'utilizzo di altre forme di identificazione biometrica, il consenso della persona controllata viene ritenuto implicito. Ma è poco probabile che una persona qualunque che viene scansionata da un sistema di riconoscimento facciale in tempo reale sappia di essere sottoposta a una verifica dell'identità e non ha quindi la possibilità di scegliere se accettare o rifiutare l'utilizzo di tale tecnologia.

In Europa, il Regolamento generale per la protezione dei dati personali (GDPR) in vigore dal 2016 afferma chiaramente che i dati biometrici ottenuti mediante tecnologie di riconoscimento facciale rientrano nella categoria dei dati personali. Sono pertanto normati dal regolamento e qualsiasi altra persona, organizzazione o società deve avere il consenso dell'interessato per poterli utilizzare. Nonostante questo, le forze dell'ordine di Paesi dell'UE come il Regno Unito, la Francia, l'Italia e la Grecia utilizzano già questa tecnologia.

Mancanza di basi giuridiche

Nella maggior parte dei Paesi non esiste una base giuridica che giustifichi l'utilizzo dei sistemi di sorveglianza con riconoscimento facciale in tempo reale. La FTR infrange le normative fondamentali sulla libertà, come il Primo emendamento della Costituzione degli Stati Uniti e lo Human Rights Act del Regno Unito.

Clare Garvie, membro del centro dedicato a privacy e tecnologia Georgetown Law, spiega a Candriam: *"Nonostante gli sforzi compiuti a livello statale e locale per vietarlo interamente, l'utilizzo del riconoscimento facciale da parte della polizia negli Stati Uniti è ancora poco regolamentato e recentemente è emerso che ha portato all'arresto di almeno tre persone innocenti. Alla luce della minaccia che rappresenta per il diritto alla privacy, alla libertà di parola, a un giusto processo e a un uguale tutela da parte della legge, l'utilizzo del riconoscimento facciale deve essere sospeso a meno che non venga approvata una solida normativa in grado di garantire e proteggere i diritti sopraelencati."*

Assenza di un'adeguata supervisione

Nella maggior parte dei Paesi, ad esempio negli Stati Uniti o in Europa, vi sono poche prove a supporto della presenza di una supervisione adeguata e imparziale che tenga sotto controllo l'utilizzo delle tecnologie di sorveglianza da parte di aziende private e forze dell'ordine.

Invadenza sproporzionata

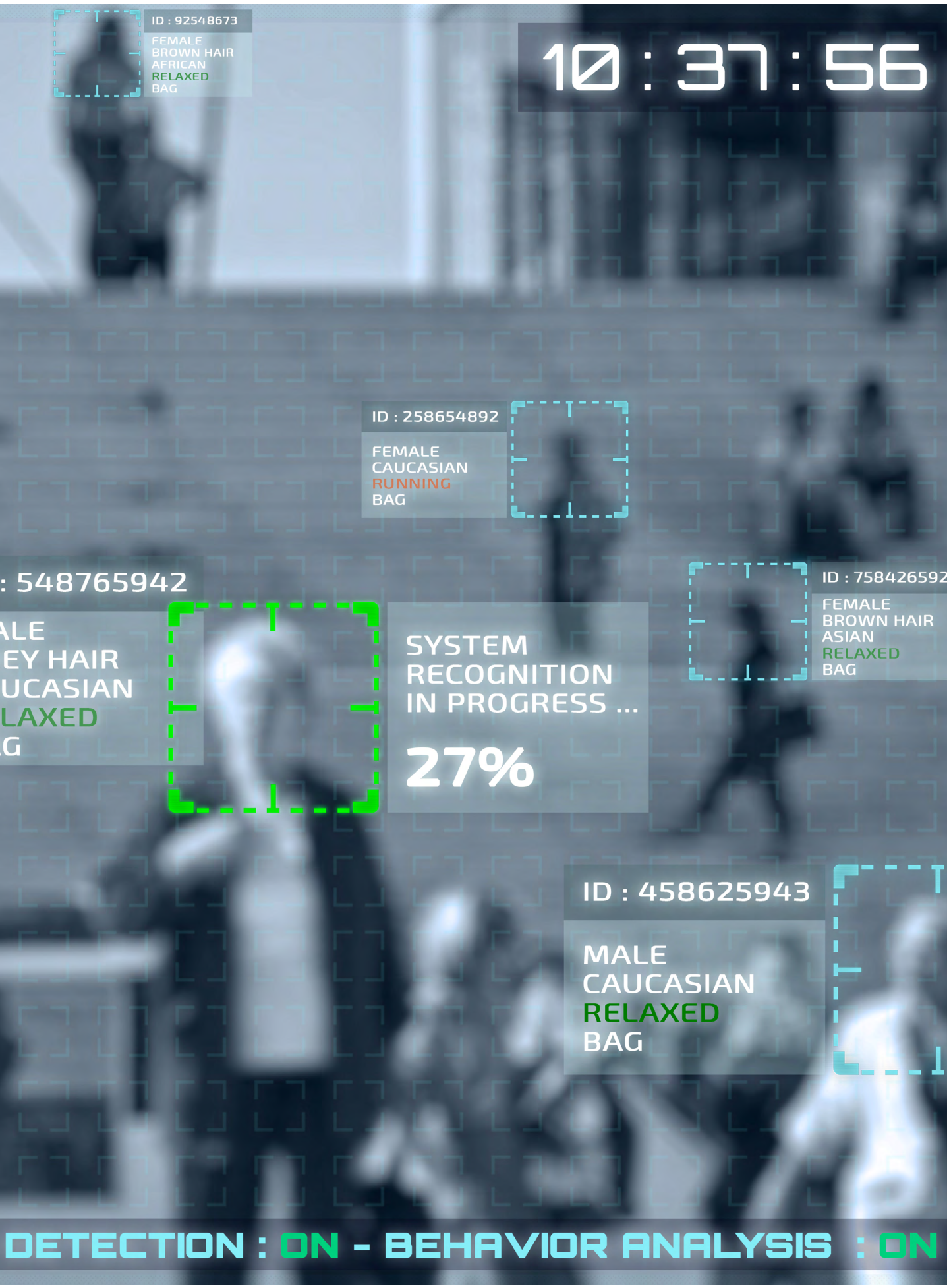
Diversi test condotti nel Regno Unito hanno determinato che il tasso di successo di questi sistemi equivale a un ricercato identificato ogni 300.000 volti scansionati. Il Surveillance Camera Commissioner (l'ente del Regno Unito che vigila sull'utilizzo dei sistemi di sorveglianza) ha concluso che l'utilizzo di queste tecnologie è pesantemente sproporzionato, sottolineando che "rispetto alla portata di un'analisi effettuata su ogni persona che passa davanti a una telecamera, il gruppo di persone che si può sperare di identificare è estremamente ridotto".

Il diritto all'anonimato

Una società fiorente si basa su una serie di libertà, come la libertà di espressione, di movimento, di religione e di associazione, ma si fonda anche sul diritto a un ragionevole anonimato. La possibilità di attraversare un luogo pubblico senza rivelare la propria identità non è più garantita a causa dell'ampio utilizzo dei sistemi di riconoscimento facciale. Chiunque dovrebbe avere la possibilità di passeggiare liberamente restando anonimo. Il desiderio di vivere senza doversi guardare continuamente le spalle è parte della natura umana. Nonostante questo, la possibilità di vivere senza un costante controllo pubblico sta sparendo rapidamente. Il fatto di essere identificati ovunque andiamo da forze dell'ordine, aziende o governi ci impedisce di vivere la nostra vita da persone qualunque. Se portato all'estremo, questo sistema finisce per limitare il movimento, la creatività, la fiducia e persino la democrazia.

Per fare un esempio, il London Policing Ethics Panel (il comitato londinese per l'etica nell'attività delle forze dell'ordine) nella sua relazione dedicata alla sorveglianza con riconoscimento facciale in tempo reale riporta che il 38% delle persone di età compresa fra i 16 e i 24 anni non si recherebbe in luoghi o a eventi sottoposti a sorveglianza con riconoscimento facciale, e lo stesso vale per moltissime persone di colore, asiatiche o appartenenti a minoranze etniche[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

Vale la pena di rinunciare a un po' di riservatezza in nome della sicurezza?

Se si chiede alle persone cosa pensano del riconoscimento facciale, la maggior parte dichiara di essere consapevole che per aumentare la sicurezza è necessario rinunciare a un po' di riservatezza. La possibilità di individuare rapidamente la posizione di un sospetto terrorista o di un bambino rapito è un'argomentazione convincente.

Il settore della sorveglianza si appoggia a un marketing costruito sulla paura, ad esempio la paura di un attacco terroristico. Nel 2016 la città di Nizza è stata teatro di un terribile attacco compiuto da un terrorista alla guida di un camion che si è diretto contro la folla presente sul lungomare per i festeggiamenti in ricordo della presa della Bastiglia, uccidendo 87 persone. In risposta, la città ha dotato la polizia locale della più grande infrastruttura cittadina di sistemi di riconoscimento facciale e tecnologie di sorveglianza di tutta la Francia.

In qualità di cittadini responsabili dovremmo chiederci:

- Vogliamo davvero essere costantemente identificati da algoritmi non testati e potenzialmente inaccurati o con prestazioni distorte?
- Vogliamo davvero che il nostro governo registri ogni nostro spostamento, ogni luogo in cui ci rechiamo, ogni persona che incontriamo?
- Vogliamo davvero che le forze dell'ordine abbiano la possibilità di registrare i nomi di tutti coloro che partecipano a una marcia di protesta o a una cerimonia religiosa?
- Vogliamo davvero concedere ai nostri governi l'illimitato potere di guardare ***tutti, ovunque e in ogni momento***?

Può una società essere schizofrenica?

Quando permettiamo ai governi e alle forze dell'ordine di utilizzare sistemi di sorveglianza tecnologici per garantire la nostra sicurezza, stiamo anche affermando che per garantire la sicurezza di tutti è necessario sorvegliare costantemente ogni singolo individuo. Alcuni sociologi riconoscono in questa logica una forma di schizofrenia.

Le differenze culturali ci spingono ad accettare la sorveglianza da parte dello stato

Non possiamo limitarci a esaminare i problemi che il riconoscimento facciale comporta per i diritti umani dal punto di vista della società occidentale. La percezione della riservatezza e dell'invadenza cambia molto da una cultura all'altra. In Cina, la maggior parte delle persone ritiene che la sorveglianza di massa sia un prezzo equo da pagare in cambio della sicurezza. Negli ultimi anni, la diffusione delle tecnologie di sorveglianza di massa unita all'avvento del sistema di credito sociale (vedere riquadro a pagina 13) ha contribuito a ridurre drammaticamente la frequenza dei reati nel Paese.

Un "*line-up*" permanente

La metafora è stata introdotta dal centro dedicato a privacy e tecnologia Georgetown Law[13] e si riferisce alla procedura di identificazione comune negli Stati Uniti in cui si chiede alla vittima di identificare il criminale tra una serie di potenziali candidati schierati uno accanto all'altro. Nessuno vorrebbe volontariamente partecipare a un *line-up*, perché la vittima potrebbe identificare per errore anche un innocente. I sistemi di riconoscimento facciale eseguono ogni giorno questa procedura, in quasi tutto il territorio di Stati Uniti e Cina[14].

Il capitalismo della sorveglianza

Nel suo libro "Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri" Shoshana Zuboff definisce "capitalismo della sorveglianza" il sistema che, grazie alla fornitura di servizi gratuiti a miliardi di persone che sono felici di utilizzarli, consente ai fornitori di tali servizi di monitorare il comportamento degli utenti con incredibile dovizia di particolari e spesso senza il loro consenso esplicito. "Il capitalismo della sorveglianza reclama unilateralmente l'esperienza umana come materia prima da tradurre in dati comportamentali." I capitalisti della sorveglianza ottengono incredibili profitti monetizzando i dati sul comportamento individuale e collettivo e le previsioni sul futuro comportamento delle persone.

La combinazione della sorveglianza statale e della sua controparte capitalista fa sì che le tecnologie digitali **suddividano i cittadini di ogni società in due gruppi, i *sorveglianti*, invisibili, ignoti e liberi di agire senza restrizioni, e i *sorvegliati***. Questo ha conseguenze profonde sulla democrazia, poiché l'asimmetria sul piano dell'informazione si traduce in uno squilibrio di potere. Tuttavia, sebbene la maggior parte delle società democratiche preveda in qualche misura una supervisione della sorveglianza statale, attualmente la sua controparte privata non è quasi per nulla regolamentata[15].

Engagement: Linee guida pratiche

Come investitori responsabili, il nostro compito è integrare i fattori ESG (ambientali, sociali e di governance) nelle nostre decisioni in materia di investimenti e optare per l'azionariato attivo. Il nostro obiettivo è creare valore a lungo termine per i nostri clienti esercitando un impatto positivo sull'economia, l'ambiente e la società tutta.

Siamo fermamente convinti che svolgendo le attività di investimento ed engagement con una conoscenza completa dei diversi aspetti della tecnologia di riconoscimento facciale sia possibile realizzare più facilmente entrambi gli aspetti di questo obiettivo. Una frazione crescente delle aziende, degli stati e delle regioni in cui investiamo si confronta con questa tecnologia. Anche se probabilmente non investiremmo intenzionalmente in una società dedita esclusivamente alla produzione di sistemi di riconoscimento facciale, per investire in un'azienda che utilizza o vende tra le altre cose anche tecnologie di riconoscimento facciale è necessario effettuare un'attenta analisi dell'investimento per:

- Valutare i rischi associati
- Condividere i potenziali dubbi con le aziende interessate
- Fornire sostegno a ogni cambiamento che contribuisca a mitigare i rischi identificati

Come già specificato parlando della FTR e dei problemi che comporta, le aspettative degli investitori possono essere molteplici, complesse e molto diverse a seconda del soggetto considerato. Vediamo di seguito alcuni obiettivi:

Emittenti aziendali

- **Engagement diretto e/o collaborativo** per comprendere meglio le prassi aziendali. Ampliare le best practice mediante conversazioni con aziende, ONG, ecc.

- **Integrare gli sviluppi nell'analisi ESG** delle aziende. Definire le best practice, i progressi accettabili e i motivi di esclusione.

- **Incoraggiare comportamenti aziendali migliori**. Continuare a porre l'etica e il rispetto dei diritti umani al centro della governance aziendale. Costituire un comitato indipendente per i rischi legati ai diritti umani che risponda direttamente al Consiglio di amministrazione. Incoraggiare le aziende a scegliere clienti e fornitori allineati con i valori che intendono difendere.

Governi

- **Orientarsi verso la sospensione dell'utilizzo del riconoscimento facciale da parte delle forze dell'ordine** finché non vengono stilate normative specifiche.

Università

- **Incoraggiare i corsi di etica** nei *curricula* attinenti a intelligenza artificiale/tecnologia.

Mentre ci prepariamo a parlare di questo argomento con le autorità europee, noi di Candriam riteniamo che la strategia migliore nell'immediato sia coinvolgere gli emittenti aziendali e in particolare le aziende i cui titoli fanno già parte dei nostri portafogli.

Adottando questo approccio e appoggiandosi agli scambi avuti con esperti e specialisti di riconoscimento facciale, elenchiamo di seguito (Figura 2) una serie di domande che possono aiutare gli investitori a valutare il livello di coinvolgimento delle società partecipate nell'utilizzo del riconoscimento facciale e a individuare il livello di rischio per i diritti umani a esso associato.

Open MIC collabora da molti anni con gli azionisti per spingere le società del settore tecnologico ad adottare prassi "etiche" per quanto riguarda il riconoscimento facciale.

Le grandi aziende del settore hanno investito energia e risorse considerevoli per resistere a queste sollecitazioni. Nonostante le marcate pressioni esercitate dagli azionisti e il contributo dato a livello globale da numerose organizzazioni per i diritti umani, gran parte delle aziende si rifiuta di riconoscere che c'è un problema. Come evidenzia questa relazione, quasi tutti i prodotti per il riconoscimento facciale attualmente presenti sul mercato operano senza il consenso dei milioni di persone i cui volti vengono scansionati quotidianamente. È stato dimostrato che molti di questi sistemi hanno prestazioni che variano a seconda del profilo razziale. Non è previsto alcun meccanismo per risarcire le persone i cui diritti sono stati violati, al contrario di quanto richiesto dai Principi guida delle Nazioni Unite su imprese e diritti umani. Nel 2019, il Relatore speciale delle Nazioni Unite sulla libertà di opinione e di espressione ha consigliato "la sospensione immediata su scala globale della vendita e del trasferimento di tecnologie di sorveglianza private fino all'adozione di rigorose misure per la salvaguardia dei diritti umani." Non esiste alcuno strumento di tutela dei diritti umani, eppure le vendite proseguono. Anzi, come suggerisce questa relazione, si assiste a un vero e proprio boom del mercato.

È lecito chiedersi se la prospettiva di una normazione e regolamentazione (sia nell'UE, sia negli Stati Uniti) indurrà le aziende ad adeguarsi volontariamente a standard di settore efficaci. Indubbiamente, le imprese cercheranno attivamente di indebolire gli eventuali controlli governativi sul riconoscimento facciale. Gli investitori devono sicuramente continuare a fare quel che hanno fatto finora, ovvero utilizzare gli strumenti a loro disposizione per spingere le società del settore tecnologico ad adottare politiche e prassi in grado di fare la differenza; sarà interessante scoprire se un engagement collaborativo ampio e marcato come quello suggerito in questo documento sarà sufficiente a incoraggiare le aziende a intraprendere un dialogo più produttivo.

Michael Connor è fondatore e direttore esecutivo di Open MIC, un'organizzazione non-profit che si impegna a stimolare le aziende ad agire in modo più responsabile nei settori dei media e della tecnologia, prevalentemente attraverso l'engagement degli azionisti. Collaborando con investitori socialmente responsabili, Open MIC identifica, sviluppa e sostiene campagne di promozione dei valori di apertura, equità, riservatezza e diversità, valori che garantiscono vantaggi a lungo termine per i singoli, le aziende, l'economia e il benessere della società democratica. Open MIC sta attualmente lavorando a campagne rivolte ad Amazon, Twitter, Google e Facebook.

Linee Guida per l'Engagement

Livello di coinvolgimento

- La vostra azienda si qualifica come fornitore di prodotti (hardware, software, database) correlati alla tecnologia di riconoscimento facciale?

- Qual è lo scopo del prodotto?
  - Sorveglianza
  - Identificazione
  - Attività delle forze dell'ordine
  - Classificazione/profilazione (ad esempio, pubblicità mirata)
  - Indagine
  - Sicurezza
  - Altro (specificare)

- A che tipo di utenti viene fornita la tecnologia di riconoscimento facciale?
  - Governi o stati
  - Scuole
  - Forze dell'ordine
  - Aziende
  - Esercito

Governance

- La vostra azienda ha adottato pubblicamente una specifica linea di condotta riguardo alla tecnologia di riconoscimento facciale? In caso affermativo, che conseguenze ha avuto questo impegno
  1) sul rapporto con i partner aziendali come fornitori, subappaltatori, clienti, utenti finali e
  2) sulle attività di lobby?

- Quali rischi legati alla tecnologia di riconoscimento facciale avete identificato e con quale frequenza li comunicate al Consiglio?

- La vostra azienda effettua valutazioni dell'impatto della propria attività sui diritti umani volte a identificare e stimare i rischi reali e potenziali per i diritti umani che derivano dalle vostre tecnologie di riconoscimento facciale? Quali rischi avete identificato e quali soggetti interessati avete coinvolto in questa valutazione? In che misura avete adattato di conseguenza la vostra attività aziendale e la vostra strategia? All'interno dell'azienda (a livello generale/regionale/locale) chi è il responsabile della gestione di questi specifici rischi e delle loro potenziali conseguenze a livello globale e quotidiano?

- Quali procedure avete adottato per stabilire a quali clienti potete vendere i vostri prodotti? Avete bloccato le vendite/le consegne dei vostri prodotti o servizi a specifici Paesi con regimi non democratici/repressivi?

Gestione dei rischi relativi alla tecnologia

- Come vi siete organizzati a livello interno per identificare, prevenire e risolvere i problemi legati al riconoscimento facciale?

Più specificamente:

- In che modo la vostra azienda ha costruito/ottenuto/acquistato il database di immagini/nomi utilizzato per l'addestramento delle tecnologie? Se non avete costruito voi stessi il database, in che modo il vostro fornitore ha costruito/ottenuto/acquistato il database che utilizzate?

- Avete reso pubblica l'accuratezza della vostra tecnologia e di quella dei fornitori dopo averla fatta misurare a un istituto scientifico di valutazione riconosciuto come il NIST (Istituto nazionale statunitense per gli standard e la tecnologia)? In caso di risposta affermativa, come argomentate la vostra scelta?

- Quali verifiche interne effettuate per rilevare eventuali distorsioni delle prestazioni dell'algoritmo, ad esempio quelle relative a razza, sesso o età? E/o i vostri fornitori?

- Le vostre attuali procedure prevedono un meccanismo di reclamo per identificare e risarcire le persone che hanno subito senza motivo le conseguenze della tecnologia in questione?

Gestione dei rischi relativi all'utilizzo

- I vostri clienti sono sottoposti a qualche forma di regolamentazione per quanto riguarda l'uso della tecnologia di riconoscimento facciale? Monitorate questo aspetto?

- Il vostro prodotto mette a disposizione la tecnologia di riconoscimento facciale per l'analisi in tempo reale o esclusivamente per l'analisi retroattiva?

- Il vostro prodotto analizza videoregistrazioni in tempo reale o elabora esclusivamente immagini fisse?

- Il vostro prodotto con tecnologia di riconoscimento facciale offre la possibilità di effettuare qualche genere di classificazione o profilazione, ad esempio sulla base di razza, sesso, età, pensiero o altro? Il vostro prodotto con tecnologia di riconoscimento facciale è dotato di funzionalità di analisi predittiva?

- Le vostre attuali procedure prevedono un meccanismo di reclamo per identificare e risarcire le persone che hanno subito senza motivo le conseguenze della tecnologia in questione?

Conclusioni

Oggi il riconoscimento facciale è un tema trattato in modo poco trasparente. C'è chi lo accoglie come uno strumento positivo, mentre per altri si tratta di una tecnologia controversa. È possibile abusare di questo strumento ed è stato dimostrato che commette errori ed è soggetto a distorsioni.

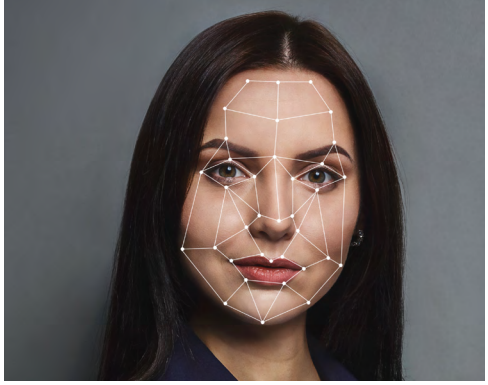
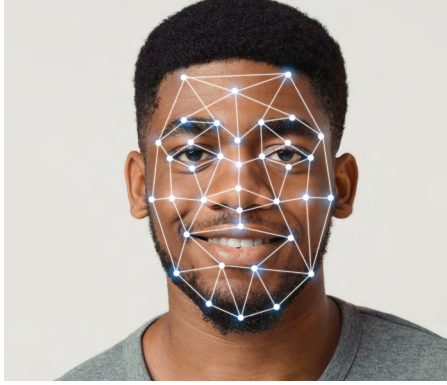
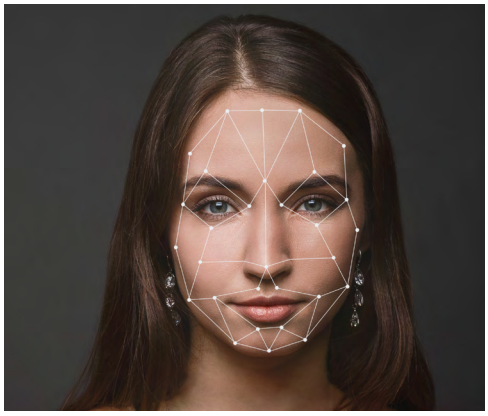
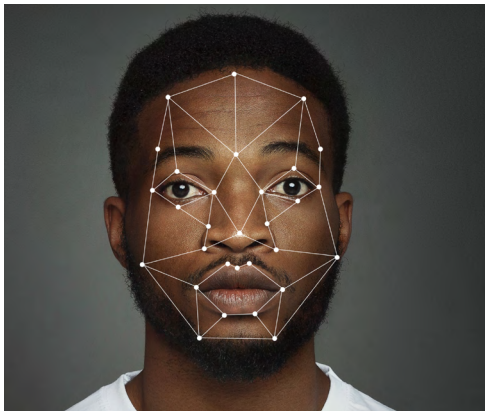
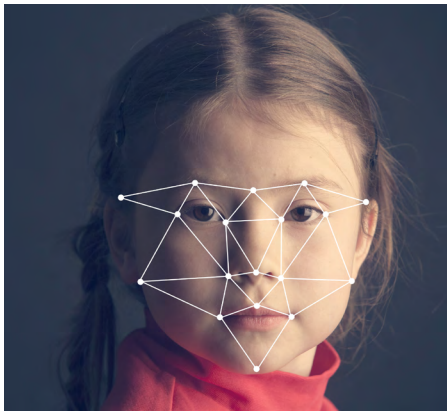
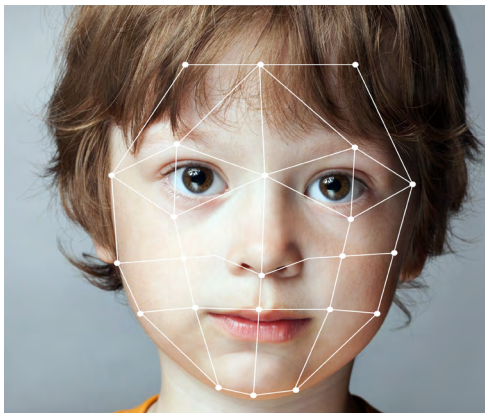
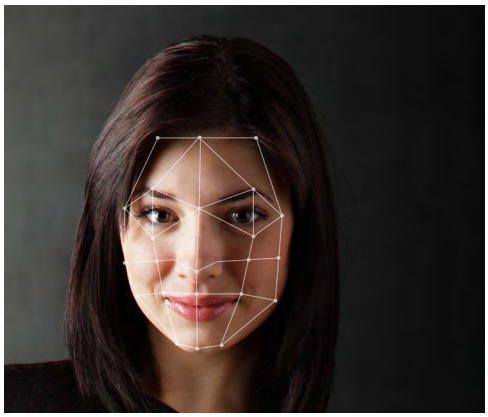
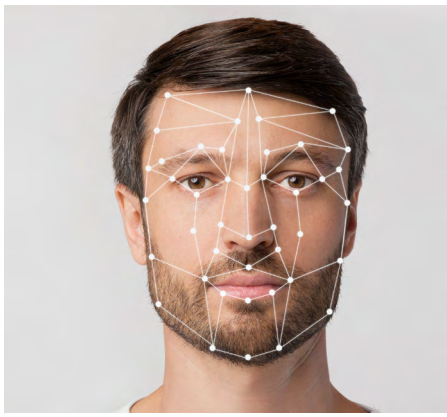
Senza trasparenza, non possiamo valutare adeguatamente gli aspetti controversi. Per aprire la strada all'analisi e al dialogo, dobbiamo aumentare la nostra influenza sugli attori che si muovono in questo panorama. Le autorità nazionali e locali stanno iniziando a muoversi. Le aziende stanno iniziando a reagire. Il tema sta diventando più scottante per l'opinione pubblica e le ONG stanno lanciando numerose campagne.

Anche per gli investitori è arrivato il momento di giocare le proprie mosse.

Note e riferimenti

[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 Mld di €

di attivi in gestione
al 31 dicembre 2020

570

esperti al
vostro servizio

25 anni

Aprendo la strada agli
investimenti sostenibili

CANDRIAM. INVESTING FOR TOMORROW.

WWW.CANDRIAM.COM

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY