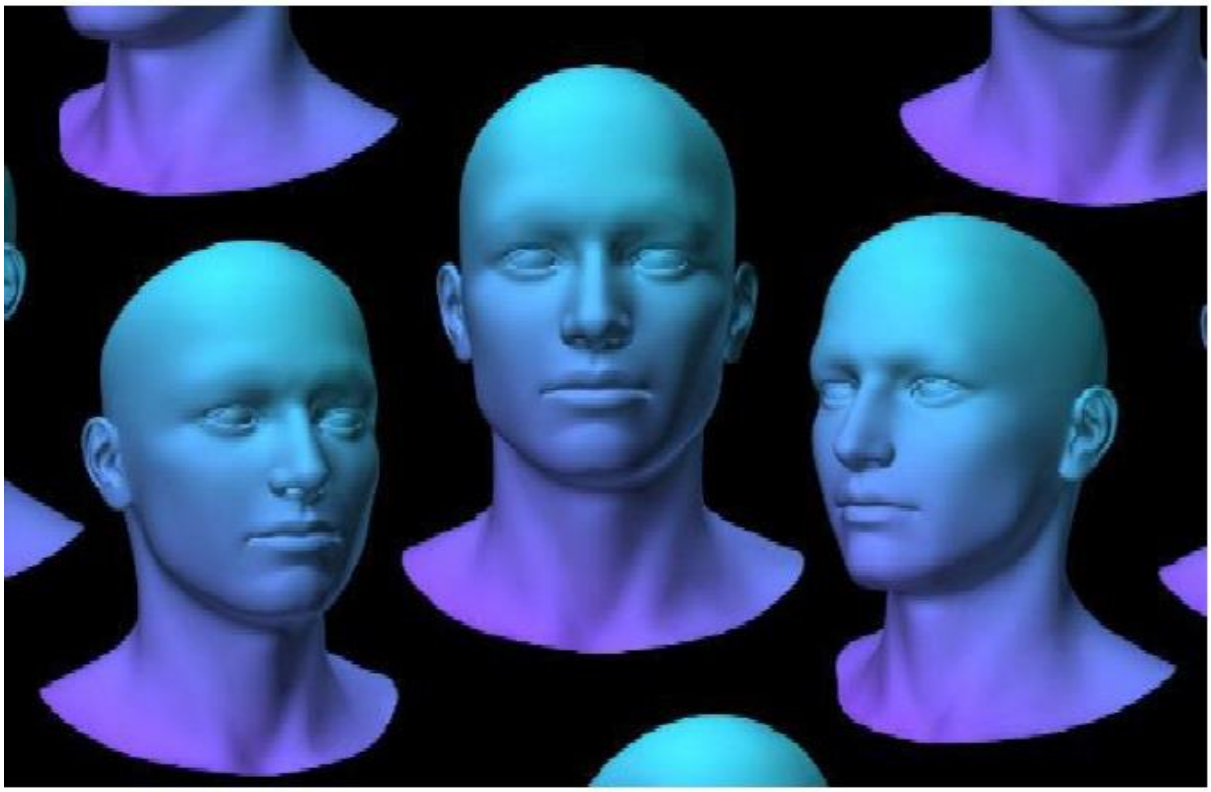
تکنولوژی تشخیص‌چهره به بخشی از زندگی بسیاری از مردم در سراسر جهان تبدیل شده است. از دوربین‌های نظارت همگانی در خیابان‌ها و فروشگاه‌ها گرفته تا تگ‌کردن دوستان در شبکه‌های اجتماعی و تدابیر امنیتی در موبایل‌های هوشمند، تشخیص چهره را اکنون می‌توان به صورت گسترده در اماکن و ابزارهای مختلف یافت و انتظار می‌رود میزان استفاده از آن به مرور زمان، افزایش یابد.

تمام تکنولوژی‌ها مزایا و معایب خاص خود را دارند، موضوع فقط وابسته به اینست که چطور از آنها استفاده می‌کنید. طبیعتا تکنولوژی تشخیص‌چهره هم از این قاعده مستثنی نیست. بیایید مروری داشته باشیم بر اینکه تکنولوژی تشخیص-چهره چیست و چه مزایا و معایبی با خود به همراه می‌آورد.

مزایای تشخیص‌چهره



استفاده از تشخیص‌چهره می‌تواند مزایای مختلفی برای جامعه داشته باشد، مزایایی مانند افزایش امنیت، جلوگیری از جرایم و کاهش تعاملات انسانی. این تکنولوژی حتی می‌تواند در امور پزشکی نیز یاری‌رسان باشد.

کمک به یافتن افراد گمشده: آژانس‌های قانونی از تشخیص‌چهره برای یافتن افراد گمشده استفاده می‌کنند و تا به امروز بارها داستان پیداشدن کودکانی را شنیده‌ایم که از والدین خود جدا افتاده بودند و سپس به آغوش آنها بازگشتند. وقتی هم که این تکنولوژی را با نرم‌افزارهای پیش‌بینی سن ادغام کنید، می‌توانید تشخیص دهید یک کودک با گذشت چند سال چه شمایلی یافته است و امکان یافتن کودکانی که برای چند سال گم شده‌اند مهیا می‌گردد.

مراقبت از کسب‌وکارها در برابر سرقت: صاحبان کسب‌وکار از نرم‌افزار تشخیص‌چهره همراه با دوربین‌های امنیتی استفاده می‌کنند تا قادر به شناسایی افرادی باشند که احتمالا دست به سرقت از فروشگاه زده‌اند. از آنجایی که مردم در

صورت اطلاع از اینکه در حال تماشا شدن هستند به احتمال کمتری مرتکب جرم می‌شوند، این تکنولوژی می‌تواند نقش یک عامل پیشگیرانه را نیز ایفا کند.

بهبود تدابیر امنیتی: تشخیص‌چهره می‌تواند به بهبود امنیت منجر شود. بسیاری از فرودگاه‌های جهان اکنون از تکنولوژی تشخیص‌چهره به صورت مداوم در چک‌پوینت‌ها استفاده می‌کنند و بنابراین قادر به شناسایی مجرمان با تهدیدات احتمالی علیه خطوط هوایی و مسافران هستند. بانک‌ها و دیگر موسسات مشابه هم از تشخیص‌چهره برای جلوگیری از کلاهبرداری بهره می‌برند، زیرا این تکنولوژی می‌تواند افرادی که قبلا مرتکب جرم شده‌اند را شناسایی کرده و به بانک هشدار دهد.

کاهش تعامل انسانی: تشخیص‌چهره نیازمند منابع انسانی بسیار کمتری نسبت به دیگر تدابیر امنیتی نظیر حسگرهای اثرانگشت است. این تکنولوژی نیازی به تماس یا تعامل مستقیم و فیزیکی انسانی ندارد. در عوض همه‌چیز توسط هوش‌مصنوعی و در پروسه‌های کاملا اتوماتیک و سریع مدیریت می‌شود. از طرف دیگر، نیاز به تعامل فیزیکی هنگام بازکردن قفل درها یا تلفن‌های هوشمند، برداشتن پول نقد از عابربانک یا هر کاری که معمولا نیازمند واردکردن یک پین یا یک پسوورد یا یک کلید است، نخواهد بود.

بهینه‌ترشدن روند خرید: اما مزایای تکنولوژی تشخیص‌چهره را می‌توان در حوزه‌هایی حتی فراتر از امنیت نیز جستجو کرد. برای مثال هنگام خرید در فروشگاه‌ها، به جای استفاده از کارت‌اعتباری یا پول نقد، تشخیص‌چهره می‌تواند چهره شما را شناسایی کند و هزینه محصولات را مستقیما از حساب بانکی شما کسر کنند.

بهبود دسته‌بندی تصاویر: با قابلیت تشخیص‌چهره، می‌توان روی تصاویر ذخیره شده در فضای ابری شرکت‌هایی مانند اپل و گوگل تگ زد. این‌کار باعث می‌شود که دسته‌بندی، یافتن و اشتراک‌گذاری تصاویر به شکلی بسیار آسان‌تر صورت بگیرد. همین سیستم است که تگ‌کردن افراد مختلف در تصاویر فیسبوکی را نیز به شما پیشنهاد می‌دهد.

بهبود روندهای درمانی: یکی از کاربردهای غافلگیرکننده تکنولوژی تشخیص‌چهره، امکان شناسایی اختلالات ژنتیک است. با تحلیل ویژگی‌های ظریف چهره، نرم‌افزار تشخیص‌چهره می‌تواند در برخی موارد به شناسایی جهش‌های ژنتیکی ناشی از سندروم‌های مشخص بپردازد. این تکنولوژی ضمنا سریع‌تر و ارزان‌قیمت‌تر از تست‌های ژنتیک سنتی به حساب می‌آید.

مزایای تشخیص‌چهره

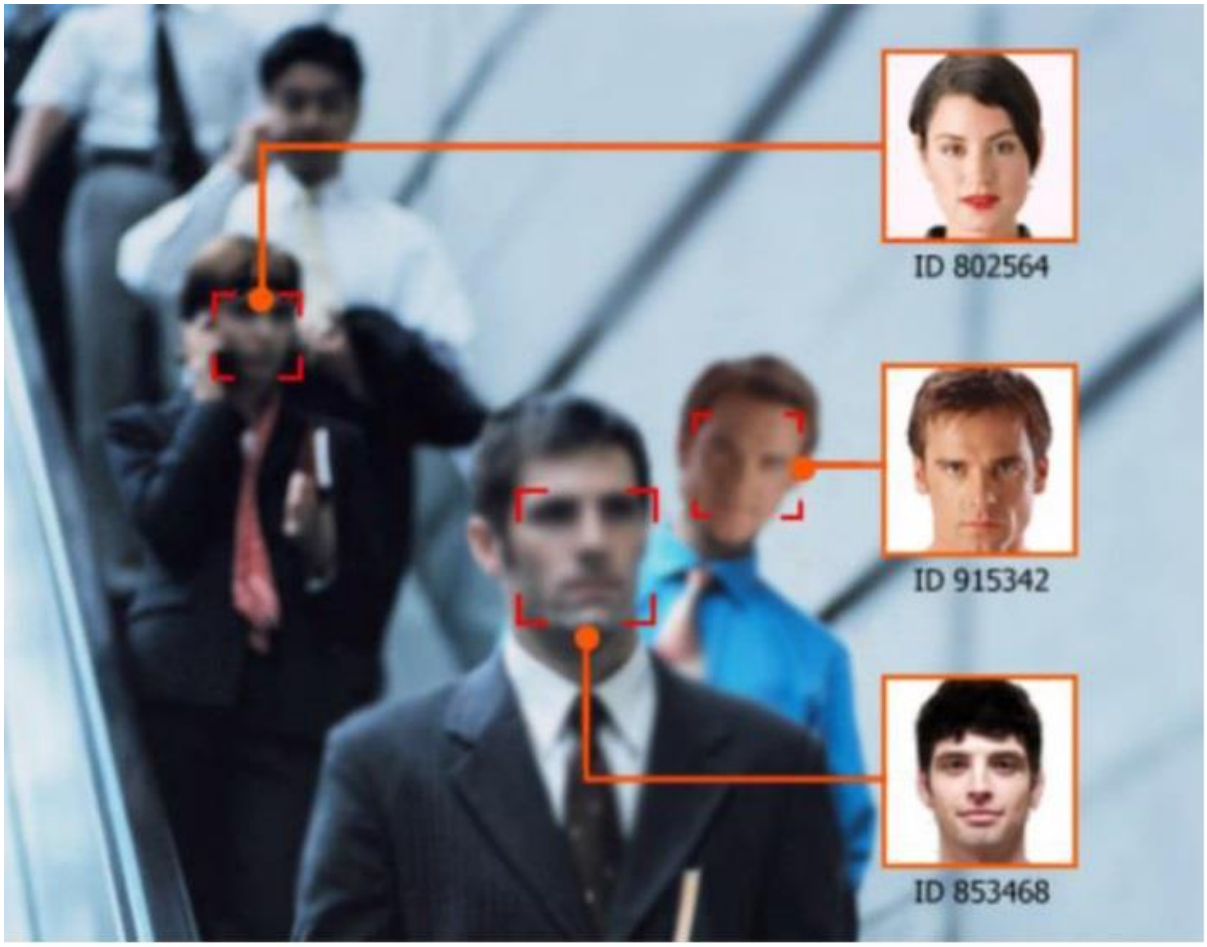
مثل هر تکنولوژی دیگری، استفاده از تشخیص‌چهره می‌تواند معایب خاص خود را به همراه داشته باشد: معایبی نظیر ازبین‌رفتن حریم شخصی، نقض آزادی‌های فردی، سرقت بالقوه اطلاعات و جرایم مشابه. ضمنا به خاطر نواقص موجود در این تکنولوژی، همواره احتمال خطا نیز وجود دارد.

تهدید حریم شخصی و اجتماعی: تهدیدات احتمالی علیه حریم شخصی، یکی از بزرگ‌ترین معایب تکنولوژی تشخیص چهره است. هیچ‌کسی دوست ندارد که چهره‌اش ضبط و در مراکزداده مختلف ثبت شود تا در آینده مورد استفاده قرار گیرد. حریم شخصی آن‌قدر مقوله مهمی است که در برخی شهرهای بزرگ مانند سانفرانسیسکو و کمبریج، استفاده مراجع قانونی از تکنولوژی تشخیص‌چهره بلادرنگ ممنوع اعلام شده است. در این موارد، پلیس می‌تواند از

ویدیوهای ضبط‌شده از طریق ابزارهای امنیت ویدیویی شخصی استفاده کند، اما مجاز به استفاده از نرم‌افزار تشخیص-چهره به‌صورت زنده نیست.

تهدید آزادی فردی: استفاده همیشگی از تکنولوژی تشخیص‌چهره باعث می‌شود که مردم فکر کنند همواره در حال پایش و قضاوت شدن بابت رفتارهای خود هستند. از طرف دیگر، پلیس می‌تواند با استفاده از این تکنولوژی، به اسکن چهره تمام مردم در مرکز داده خود بپردازد تا مظنونین را شناسایی کند. چنین‌کاری یعنی بدون هیچ دلیل واقعی، با شما مثل شخصی که مظنون به جرم و جنایت است رفتار شده است.

زیر پا گذاشتن حقوق فردی: در کشورهایی که آزادی فردی یا به شکلی محدود وجود دارد و یا اصلا وجود ندارد، استفاده از تشخیص‌چهره برای جاسوسی‌کردن از مردم و دستگیری آنهایی‌که دردسر درست می‌کنند، امری عادی به حساب می‌آید.



احتمال ایجاد آسیب‌پذیری: یکی از بزرگترین نگرانی‌ها راجع به مراکز داده که شامل داده‌های مربوط به تشخیص-چهره می‌باشد اینست که احتمال وجود آسیب‌پذیری و امکان رخنه در آنها بالاست. هکرها در گذشته نیز توانسته‌اند به مراکز داده‌ی اسکن‌های چهره که توسط بانک‌ها، نیروهای پلیس و شرکت‌های دفاعی تهیه شده‌اند، رخنه کنند.

فرصت‌های احتمالی برای کلاهبرداری و سایر جرایم: قانون‌شکنان می‌توانند از تکنولوژی تشخیص‌چهره برای ترتیب‌دادن جرایم خود علیه قربانیان بیگناه استفاده کنند. آنها می‌توانند اطلاعات‌شخصی افراد، نظیر تصاویر و ویدیوهای به‌دست‌آمده از اسکن‌های چهره را جمع‌آوری کنند و دست به سرقت هویت بزنند. از طرف دیگر، با دسترسی به چنین اطلاعاتی، یک سارق می‌تواند یک حساب بانکی به نام شخص قربانی باز کند. فراتر از دنیای کلاهبرداری و جرایم مشابه، افراد بدطینت می‌توانند به تعقیب و آزار قربانیان از طریق تکنولوژی تشخیص‌چهره بپردازند. برای مثال با جستجوی معکوس تصاویر ثبت شده در یک مکان عمومی، می‌توان اطلاعاتی بیشتری راجع به قربانیان کسب کرد و آدرس مکان زندگی آنها را نیز به‌دست آورد. ضمنا از آن جایی که جرایم تکنولوژی با سرعتی بالاتر از قانون حرکت می‌کنند، مردم ممکن است تبدیل به قربانی یک روشی بشوند که هنوز به عنوان جرم در نظر گرفته نمی‌شود.

تکنولوژی بی‌نقص نیست: تشخیص‌چهره به هیچ وجه بی‌نقص نیست. برای مثال این تکنولوژی، مردان سفیدپوست را راحت‌تر از زنان یا اشخاص رنگین‌پوست شناسایی می‌کند. این تکنولوژی برای شناسایی سوژه‌ها، کاملا متکی بر الگوریتم است. این الگوریتم‌ها درشناسایی افراد سفیدپوست موفق‌تر عمل می‌کنند چون داده بیشتری از مردان سیاه-پوست نسبت به زبان و افراد رنگین‌پوست دریافت کرده‌اید. بنابراین نوعی جهت‌گیری ناخواسته در الگوریتم شکل می-گیرد.

احتمال محکومیت افراد بی‌گناه: نرم‌افزار تشخیص‌چهره ممکن است افرادی را به‌اشتباه به‌عنوان مجرم شناسایی کند و بنابراین برخی اوقات شخصی بی‌گناه، به خاطر گناه ناکرده دستگیر می‌شود. درحالی‌که افراد سیاه‌پوست در حال حاضر هم‌چنان با نژادپرستی دست‌وپنجه نرم می‌کنند، اشتباهات این‌چنینی می‌تواند به دودستگی‌های اجتماعی دامن بزند.

تکنولوژی را می‌توان فریب داد: تنها الگوریتم نیست که به تشخیص‌چهره افراد می‌پردازد و فاکتورهای دیگری مانند زوایای دوربین، میزان نور و کیفیت ویدیو یا تصویر هم هنگام استفاده از این تکنولوژی وجود دارد. مجرمان خیلی ساده با پوشیدن لباس مبدل یا تغییر اندک در ظاهر خود می‌توانند تکنولوژی تشخیص‌چهره را نیز به خطا بیندازند.