هوش مصنوعی و حریم خصوصی

مریم سلیمی
دکترای علوم ارتباطات و مدرس دانشگاه
۵ تیر ۱۴۰۲

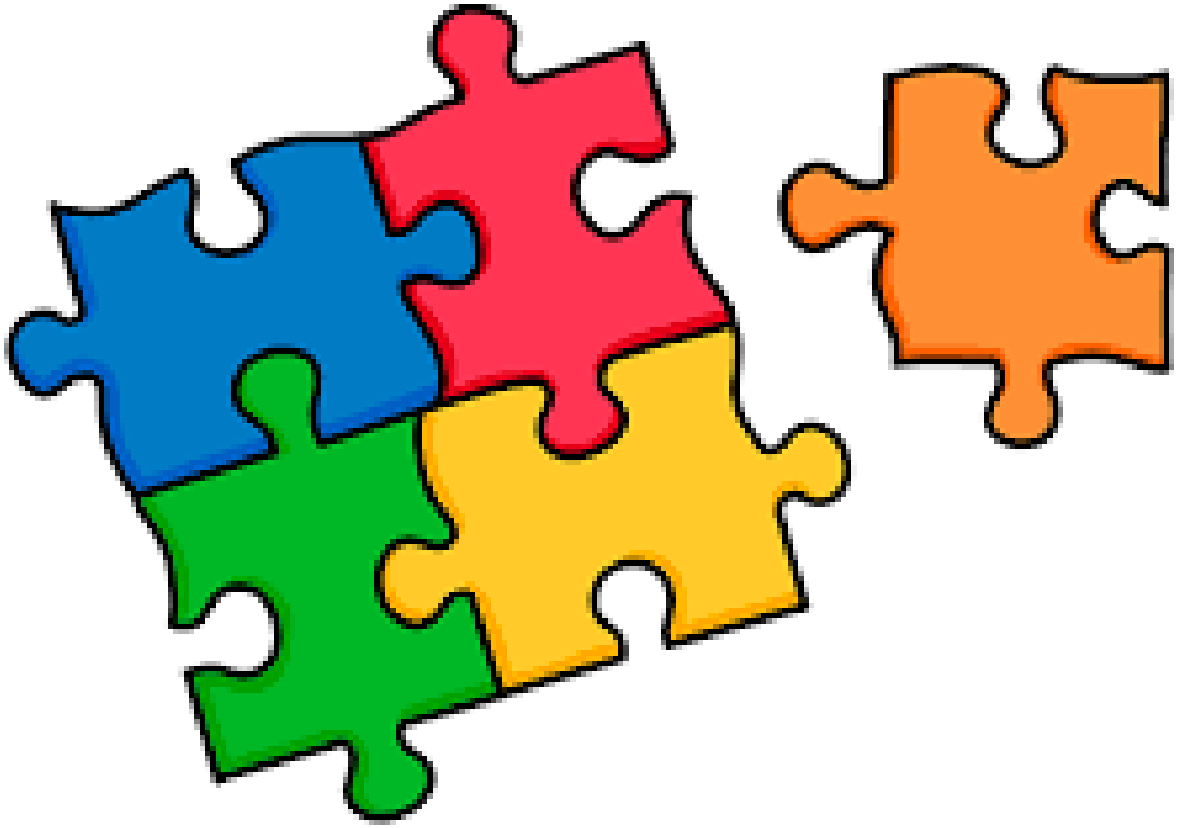
آینده اکنون است

شکل دهی آینده بشر

ظهور هوش مصنوعی یک شمشیر دو لبه است که با خود فرصتها و چالشهایی به همراه دارد. همانطور که به شکل‌دهی آینده با هوش مصنوعی ادامه می‌دهیم، مهم است که هم مزایای بالقوه و هم پیامدهای بالقوه آن را در نظر بگیریم و رویکردی مسئولانه و اخلاقی برای توسعه و استقرار آن داشته باشیم. آینده اکنون است و شیوه ای که ما نقش هوش مصنوعی را در زندگی خود شکل می دهیم تأثیر عمیقی بر آینده بشریت خواهد داشت. (Mal,2023)

سمت و سوی تحولات جهان

نتایج جدید حاصل از اتحادها و همگرایی ها و	بهره گیری از حواس پنجگانه	تعاملی تر شدن	شخصی سازی
استفاده بیشتر از واسطه های مغز و کامپیوتر	بهره گیری از فناوریهای پوشیدنی	دیجیتالی شدن	هوشمندترشدن
پیوند و تعامل بیشتر انسان وهوش مصنوعی ، انسان نماها، رباتها و...	بهره گیری از واقعیتها (ترکیبی، توسعه یافته و...)	بهره گیری بیشتر از تحلیل داده ها و احساسات	پیوند بیشتر دنیای واقعی و مجازی
بهره گیری بیشتر از متادیتاها و بیگ دیتاها	گرایش به غیرمتمرکز شدن (به یاری بلاکچین و...)	تولید محتوای سفارشی به یاری هوش مصنوعی و....	تصویری تر شدن
و...	تغییر الگوهای اخلاقی، ایدئولوژیک و...	اشکال جدید از رسانه، ارتباطات، تفریح و سرگرمی	نقش آفرینی بیشتر ماشینهای یادگیرنده



همگرایی ، اتحاد و تعامل بین فناوریها، بسترها، پلتفرمها و... مختلف با پیوستن به یکدیگر همچون قطعات یک پازل، حجم عظیمی از داده ها و اطلاعات در خصوص هر فرد ایجاد خواهند کرد که از آنها در راستای اهداف مختلف بهره گرفته خواهد شد

عملکرد و فعالیتها در فضای مجازی

رصد و ارزیابی کلیه فعالیتهای ما در رسانه های اجتماعی و به طور کلی فضای مجازی، چه آنچه خواسته و چه آنچه ناخواسته به اشتراک می گذاریم. اطلاعات پروفایل، پستها، کامنتها، لایکها، ارتباطات، دنبال کنندگی، دنبال شوندگی و.... همگی اطلاعات و داده هایی در خصوص ما ارائه می کنند.

بهره گیری از حواس پنجگانه در دنیای متاورس
یعنی دسترسی به حجم انبوه جدیدی از داده های شخصی

متاورس، نشانه یا تکواژی چند وجهی متشکل از دو واژه انگلیسی «متا» و «ورس» است به معنای فراجهان یا واقعیت دیجیتال جایگزین. متا، متاورس را این‌گونه تعریف می‌کند: «مجموعه‌ای از فضاهای مجازی که می‌توانید با افراد دیگری که در فضای فیزیکی مشابه شما نیستند، تعامل و کاوش کنید»

زاکربرگ پیش‌تر برنامه‌های خود را برای تأسیس «متاورس» اینگونه اعلام کرده بود: •من معتقدم متاورس فصل بعدی اینترنت پس از اینترنت موبایلی خواهد بود. •یک اینترنت تجسم یافته، که در آن به جای اینکه فقط محتوا را مشاهده کنید، در آن حضور خواهید داشت.

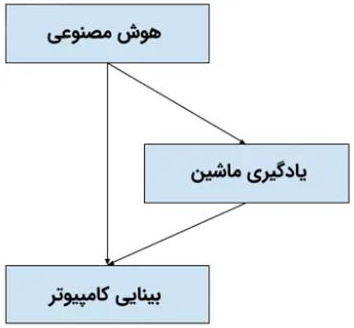
متاورس از طریق همگرایی فناوریهای مختلف تصور و تخیل را به واقعیت تبدیل می کند. (Park & Kim ,2022)

۸ فناوری که امکان تحول از اینترنت به متاورس را فراهم می کنند عبارتند از: (Lee,2021)

- واقعیت توسعه یافته
- تعامل کاربر (انسان و ماشین)
- بلاکچین
- هوش مصنوعی
- اینترنت اشیا و رباتیک
- بینایی کامپیوتر
- رایانش ابری و لبه
- شبکه های موبایلی آینده

بینایی کامپیوتر

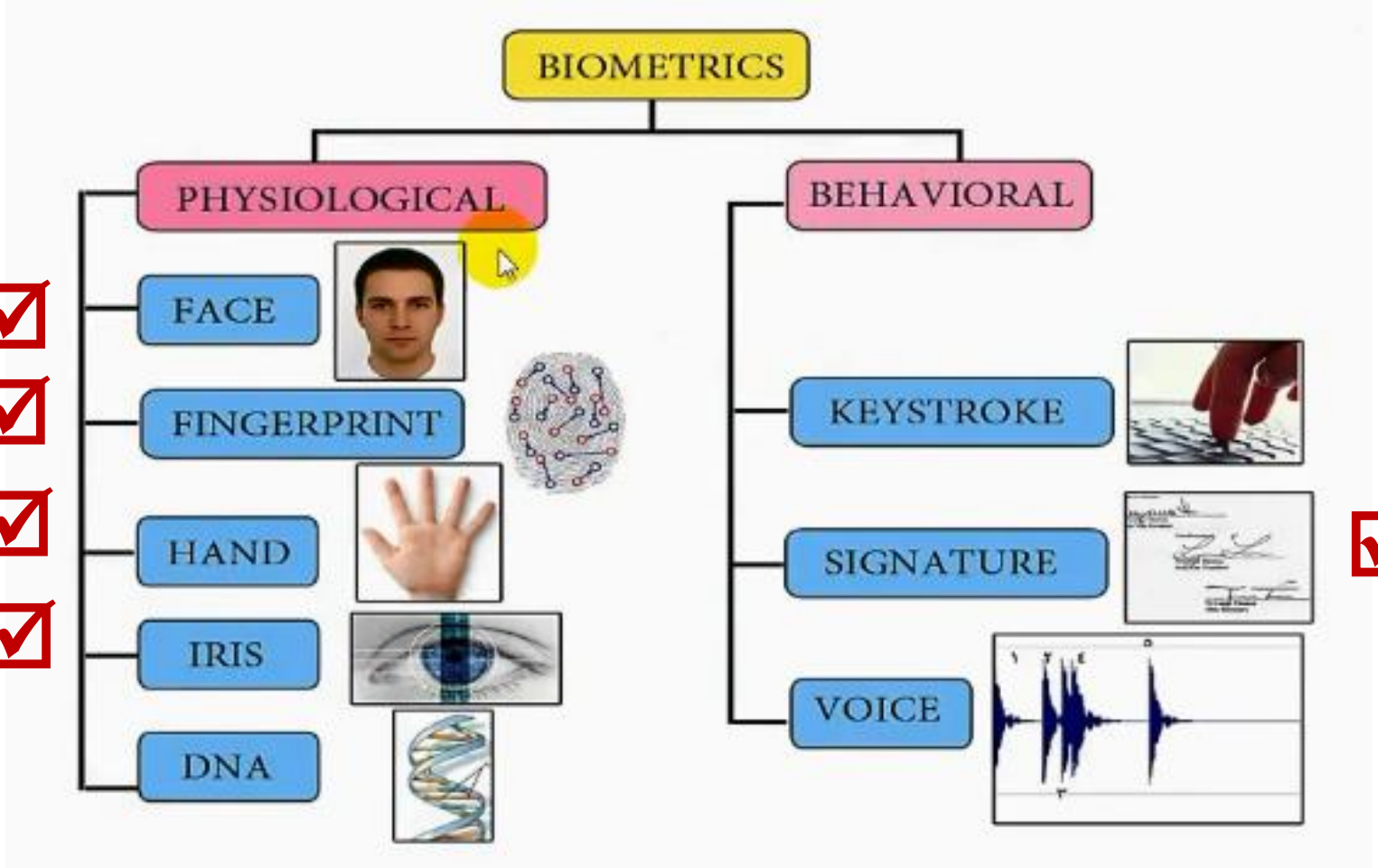
بینایی کامپیوتر شامل روش‌های مربوط به دستیابی تصاویر، دیدن، توصیف، پردازش، آنالیز و درک محتوای آن‌ها است.



بینایی کامپیوتر، حوزه‌ای مطالعاتی است که هدف آن ایجاد چارچوب‌های لازم برای پیاده‌سازی قابلیت بینایی در کامپیوتر و سیستم‌های کامپیوتری است. در سطح انتزاع، هدف سیستم‌های بینایی کامپیوتر، استفاده از داده‌های تصاویر مشاهده شده برای استنتاج در رابطه با جهان پیرامون یا محیط عملیاتی است. بینایی کامپیوتر، یکی از زیرحوزه‌های «چند رشته‌ای» (Multidisciplinary) از هوش مصنوعی و یادگیری ماشین محسوب می‌شود که از روش‌های خاص و الگوریتم‌های عمومی یادگیری برای رسیدن به هدف خود استفاده می‌کند.

بیومتریک

بیومتریک ویژگیهای منحصر به فرد هر انسان است که از آن برای اهداف مختلف از جمله تشخیص یا تأیید هویت یک شخص از طریق مشخصه های فیزیولوژیکی یا رفتاری وی بهره گرفته می شود

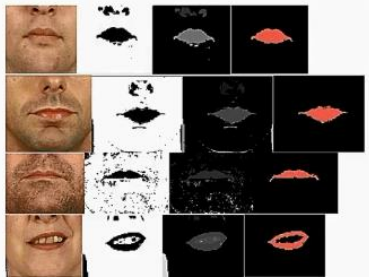


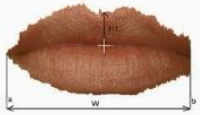
بینایی کامپیوتر در بسیاری از حوزه ها کاربرد دارد از پزشکی تا حتی سینما و....، از جمله کاربردهای آن در حوزه بیومتریک است.

منحصر به فرد بودن هر یک از این ویژگیها در مورد هر فرد

تشخیص حرکت لب (Lip motion detection)

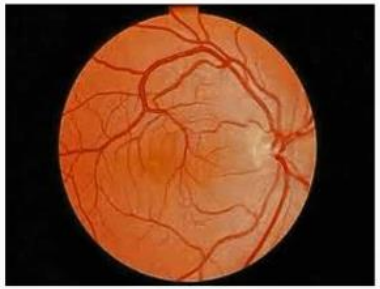
- مقایسه حرکت لب افراد هنگام صحبت‌کردن
- کمک به تشخیص صدا و صحبت‌کردن

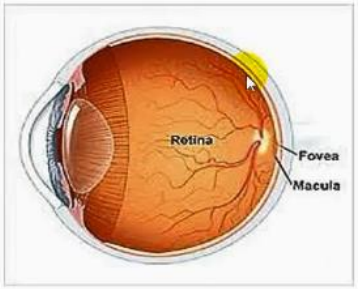




تشخیص شبکیه چشم (Retina recognition)

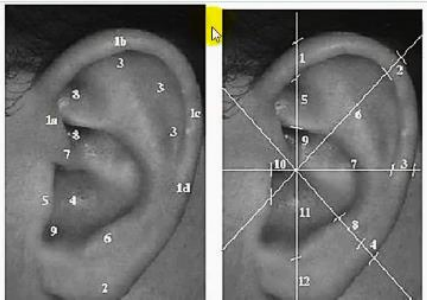
- الگوهای رگ‌های خونی داخل چشم



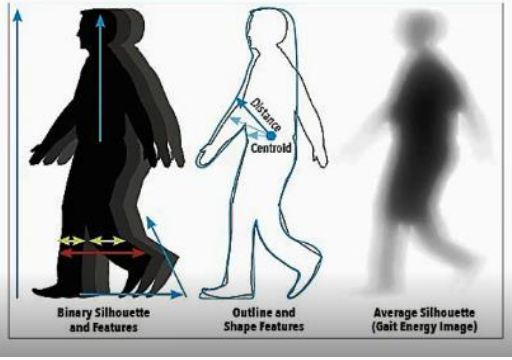


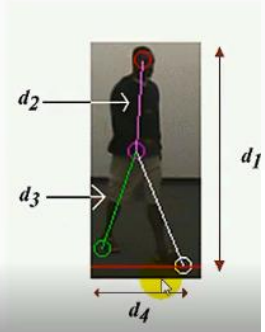
شناسایی گوش (Ear recognition)

- اندازه، عرض و شکل لاله گوش افراد منحصربه‌فرد می‌باشد.
- لاله گوش یک ویژگی بیومتریک برای شناسایی افراد می‌باشد.



تشخیص نحوه راه‌رفتن (Gait recognition)

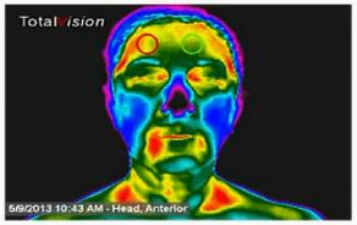




ردیابی و شناسایی چهره

ترموگرام (Thermograms)

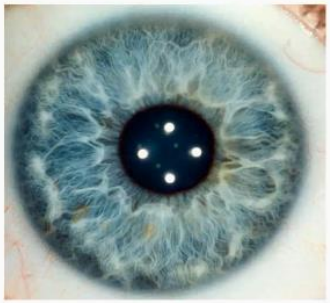
- دوربین اشعه مادون قرمز برای ردیابی الگوهای گرمایی قسمت‌های بدن

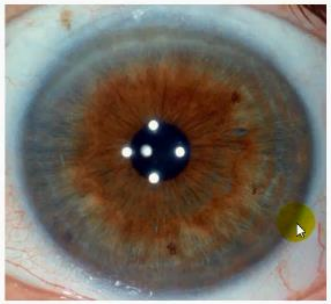


تشخیص هندسه دست (Hand geometry)

Airport - Hand Geometry

تشخیص عنبیه (Iris recognition)

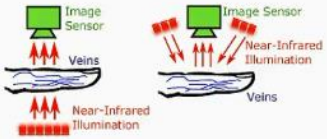


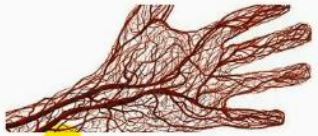


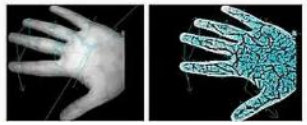
The most safe, accurate biometrics

الگوی رگ (Vein Pattern)

- تعداد، طول و شکل رگ دست افراد منحصربه‌فرد می‌باشد.
- الگوی رگ (Vein Pattern) یک ویژگی بیومتریک برای شناسایی افراد می‌باشد.







بهره گیری از اطلاعات بیومتریک و فردی برای اهداف سیاسی ، تبلیغاتی و...

نگرانی از بهره گیری از کلیه اطلاعات بیومتریک افراد، رفتارها، عادتها، واکنشها، کامنتها، لایکها و....

اطلاعات مربوط به محل فرد، روابط اجتماعی، ارتباطات گفتاری، درخواستها برای سرچ، ترجیحات خرید، حالات بدن، شکل نگاه، اشارات، ابزارهای چهره ای، فاصله میان فردی و... همگی قابل بررسی و رصد هستند.

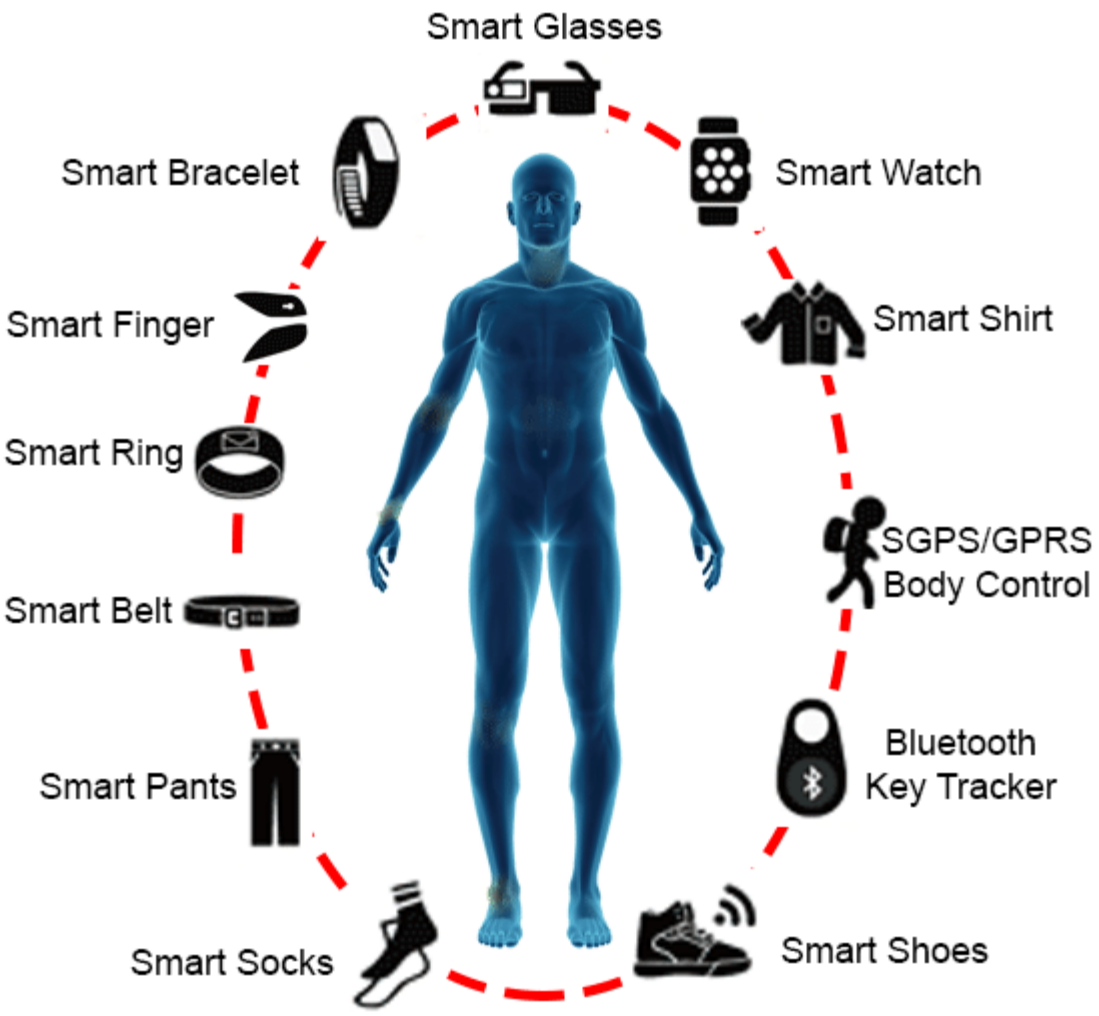
پل اکمن روانشناس برجسته می گوید: رفتارها با صدای بلند از کلمات بیان می شوند. رفتارهای غیرکلامی به میزان زیادی خودکار هستند. اطلاعات مربوط به ارتباطات غیرکلامی برای اهداف تبلیغاتی، سیاسی، شناسایی فرد و الگوهایش بسیار حائز اهمیت است.

بزرگترین بخش اطلاعات جمع آوری شده در سه دسته قابل دسته بندی هستند: رصد دست، رصد چشم و رصد راه رفتن.

در رصد چشم اطلاعات قابل توجه ترکیبی از حالات نگاه کردن، نرخ پلک زدن، گشاد شدن مردمک چشم، حرکتهای عمودی و افقی چشم، فیکس شدن چشم، زمان صرف شده و... هستند. در رصد راه رفتن اطلاعات قابل توجه اندازه گیری و سنجش حرکات بدن، مکانیک بدن، فعالیت ماهیچه ها و... هستند. از همین اطلاعات با اهداف دیگری چون تشخیص بیماریها و مشکلات، رصد وضعیت سربازان و... استفاده می شود. (Pearlman & others, n.d.)

فناوریهای پوشیدنی

فناوریهای پوشیدنی دسته ای از دستگاههای الکترونیکی هستند که می توانند به عنوان لوازم جانبی مانند ساعتهای هوشمند، هدفونهای بلوتوپ، عینک، هدبند، جوراب، لباسهای هوشمند، کفش هوشمند و... به شکلهای مختلف مورد استفاده قرار گیرند این دستگاههای ممکن است به صورت تعبیه شده در لباس، کاشت تراشه، خالکوبی روی بدن و... نیز مورد بهره قرار گیرند. این دستگاه‌های پوشیدنی ابزارهای هندزفری با کاربردهای عملی هستند که توسط میکروکنترلرها و ریزپردازنده‌ها تغذیه می‌شوند که توانایی ارسال و دریافت داده‌ها را از طریق اینترنت، بلوتوث یا فناوری بی‌سیم و غیره را دارند.(Fahad,2020)

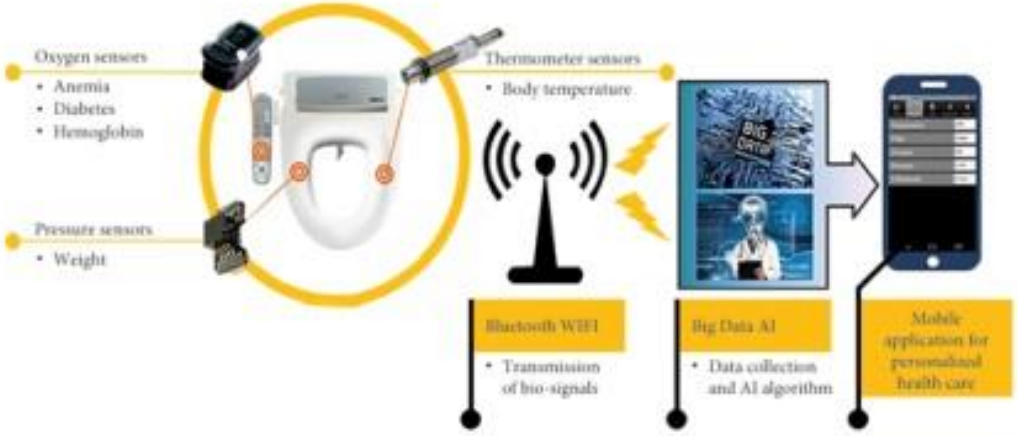


از این ابزار که عموماً نزدیک یا روی سطح پوست قرار می گیرند، با اهداف مختلفی از جمله در خدمت سلامتی، درمان، تناسب اندام، امور ورزشی و پزشکی و.... استفاده می شود. این دستگاهها قادرند کلیه اطلاعات حیاتی، میزان ضربان قلب، شمارش قدم‌ها،سرعت پیاده‌روی، میزان کالری سوزانده شده، میزان و کیفیت خواب و.... را دریافت، ثبت و تجزیه و تحلیل کنند.

اینترنت اشیا

به یاری اینترنت همه اشیاء، همه اشیا قادر به اتصال به اینترنت می شوند، در این شرایط زمینه برای انجام بسیاری امور فراهم می شود همچون: انجام اتوماتیک بیشتر امور استاندارد در خانه با اهدافی همچون مدیریت مصرف انرژی و غیره، نظارت بر سلامتی اعضای خانواده با ارسال گزارش سلامتی آنها از طریق فناوریهای پوشیدنی، حفظ امنیت خانه در برابر حوادث مختلف، کنترل و نظارت بر خانه و همه لوازم و تجهیزات به طور دائم و.. . از سویی به همان نسبت به بازاریابان، فعالان روابط عمومی و .... این فرصت را می دهد تا قلب خانه افراد ورود کرده و پیامهای خود را به یاری اشیا به مشتریان خود برسانند. یا وسایل هوشمند خود به پشتیبانی فنی شرکتهای سازنده متصل شده و از آخرین وضعیتشان اطلاع دهند و...، این اتفاقات شناخت مشتریان را تسهیل کرده و نفوذ عمیق تر شرکتها به زندگی شخصی افراد را در راستای شخصی سازی محصولات و.... هموار می کند.

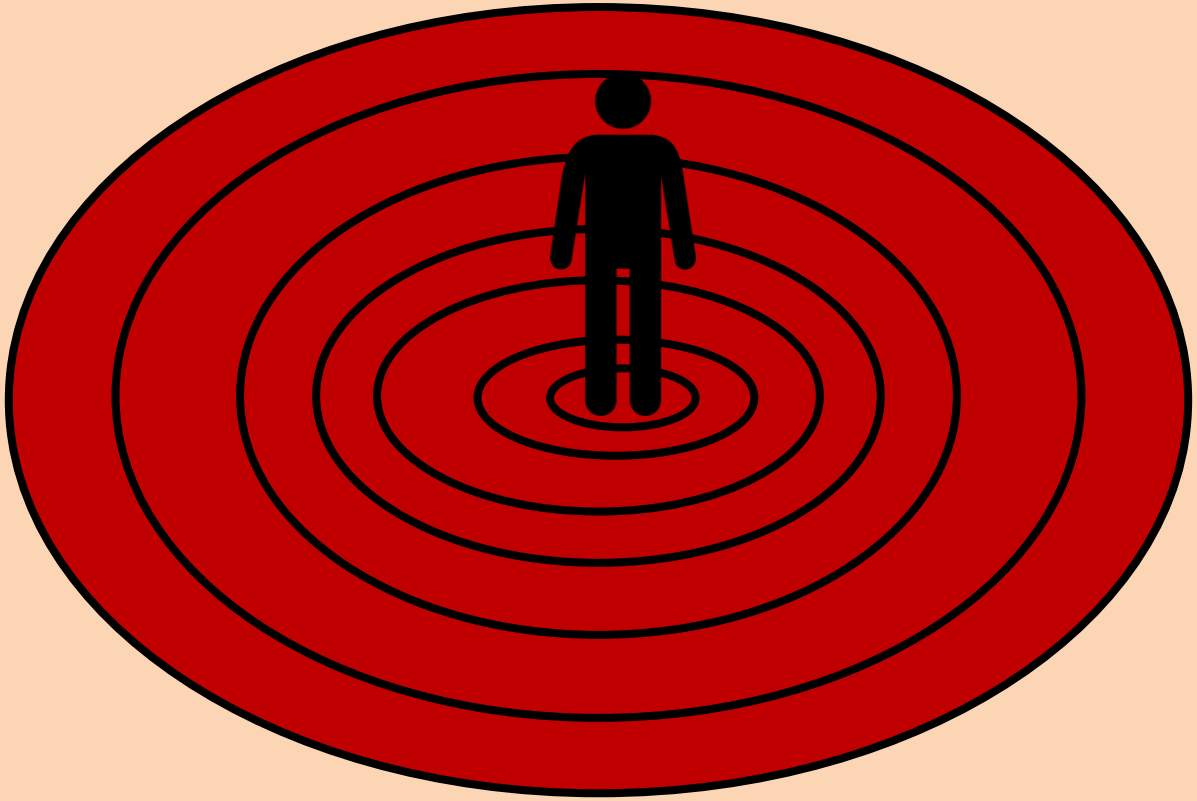
ابزارها و لوازم هوشمند



نفوذ لوازم و ابزار هوشمند تا سرویسهای بهداشتی، حمام و....
برای ارزیابی آخرین وضعیت سلامت بدن، نحوه کارکرد کلیه، دستگاه گوارش و

نرم افزارهای موقعیت یاب و حمل و نقل اینترنتی

کلیه اپلی کیشن های مسیریابی، حمل و نقل اینترنتی و هوشمند و... که حاوی کلیه اطلاعات سابقه حمل و نقل، مبدا و مقاصد پرتکرار و... هستند.



همگرایی و اتحادهای بین تکنولوژیها، بسترها و حوزه های مختلف ، حلقه حریم خصوصی ما را تنگ تر و تنگ تر می کند

هرچه پازل داده های شخصی افراد بیشتر تکمیل می شود، این حلقه تنگتر می شود.

(یک زندگی شخصی کاملاً شیشه ای با امکان رصد همه جزئیات، رفتارها، احساسات و...)

هوش مصنوعی

بهره گیری از هوش مصنوعی از سال ۲۰۲۳ وارد فاز پرشتاب و رقابتی شده و با این سرعتی که پیش می رود، مشخص نیست چه فرجامی پیش روی بشر است. بنابر نظر برخی صاحبنظران، این فرجام بستگی به نحوه هدایت و بهره گیری از هوش مصنوعی دارد. به نوعی آینده، اکنون است.

هوش مصنوعی می تواند در بسیاری حوزه ها انسان را یاری رساند ولی با این حال، چنانچه هوش مصنوعی برای انجام کارهای ویرانگر، غیرانسانی، غیراخلاقی و.... برنامه ریزی شده باشد و یا در مسیر انجام کارهایی مفید، هوش مصنوعی به روشهایی مخرب متوسل شود، می تواند خطرناک یا چالش برانگیز باشد. نگرانی اصلی و عظیم تر، نگرانی از تبدیل هوش مصنوعی به ابرهوش با توانی فراتر از هوش بشری است که در این صورت پایان چندان خوشایندی در انتظار انسان و نسل بشر نخواهد بود.

در ادامه به برخی از چالشها و خطرات هوش مصنوعی اشاره می شود که یکی از آنها خطر تهدید حریم خصوصی در ابعاد مختلف آن است که از این جمله حریم خصوصی ذهن است.

چالشها و خطرات هوش مصنوعی

در کنار مزایای بسیار هوش مصنوعی، از چالشها و خطرات احتمالی زیادی در این میان یاد می شود که برخی از آنها عبارتند از:

نگرانی از اینکه هوش مصنوعی محصول انتخابهای انسانی است که مستعد خطاهای انسانی سوگیریها و... همچون تعصبات، ارزشها ، تبعیضهای جنسیتی، قومی، نژادی و... است

نگرانی از احتمال تصمیمات و اقدامات نادرست و مغرضانه هوش مصنوعی بر پایه داده های نادرست و جانبدارانه یا با کیفیت پایین و....

نگرانی از سوء استفاده از هوش مصنوعی در خدمت رژیمها، حکومتها، تروریستها و حتی یک دانشمند و... در راستای اهدافی خاص (Shahare,2021

نگرانیهایی ناشی از توسعه هوش مصنوعی و صدمات آن از بعد امنیتی، حریم خصوصی، کرامت انسانی و... (olasmagazine,2017)

نگرانی از امکان تولید اخبار و تصاویر جعلی، دیپ فیکها و اطلاعات گمراه کننده توسط هوش مصنوعی (در این خصوص هوش مصنوعی هم زهر و پادزهر است)

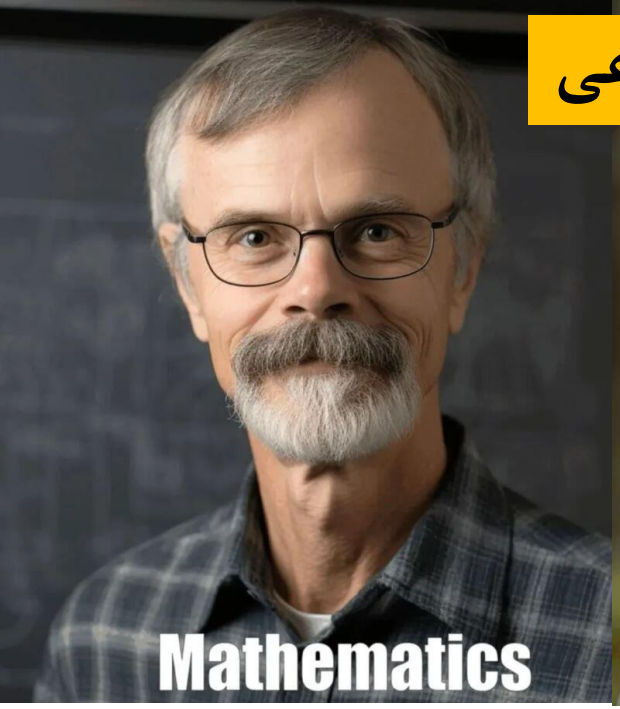
نگرانی از اینکه هوش مصنوعی و فناوریهای مربوطه توسط گروه کوچکی از افراد ایجاد و کنترل شوند مثلاً عمدتاً سفیدپوست، اکثراً مردان و بیشتر مرفه (Sadowski,2021)

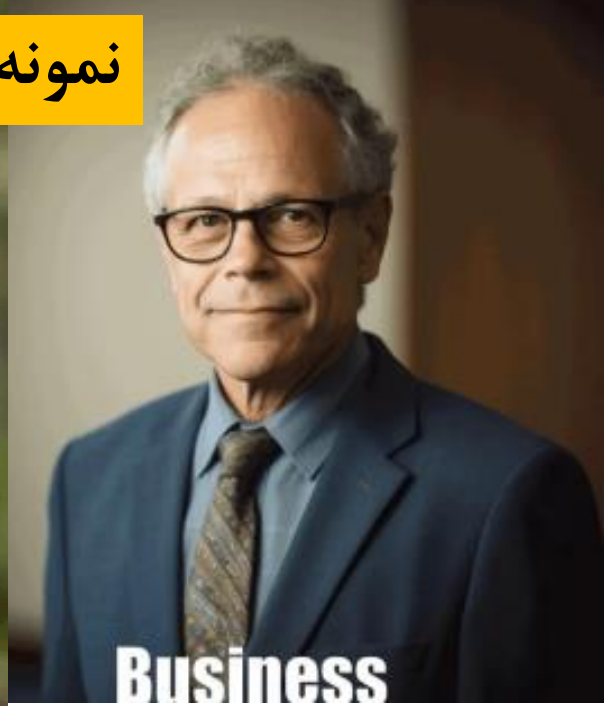
چالشهایی دیگری همچون از بین رفتن برخی مشاغل و....

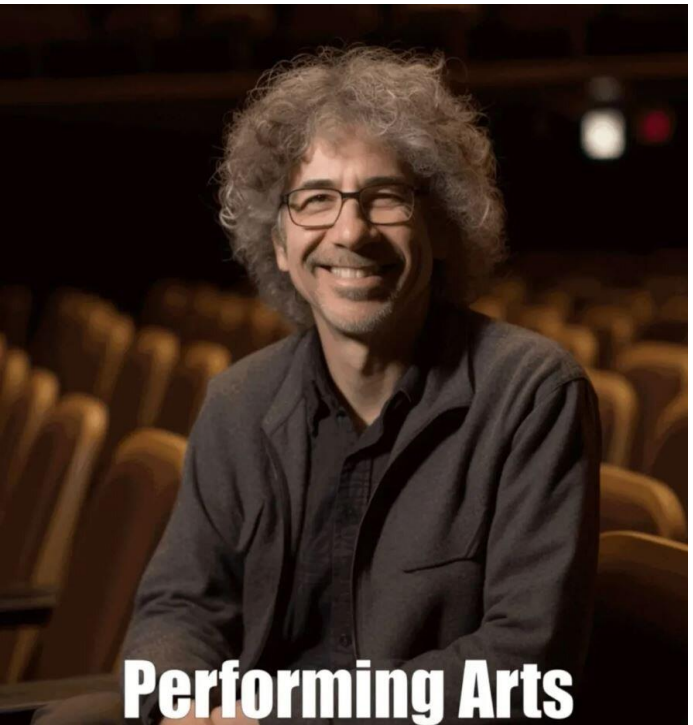
منشور حقوق هوش مصنوعی در آمریکا ، توصیه نامه اخلاق هوش مصنوعی یونسکو و... همه تلاشهایی هستند برای کاربردهای مسئولانه و اخلاق مدارانه هوش مصنوعی

اصولی که در توصیه‌نامه اخلاق هوش مصنوعی به آن‌ها اشاره و تأکید شده است شامل: اصل تناسب و بی‌ضرر بودن، رعایت ایمنی و امنیت، انصاف و عدم تبعیض، پایداری و ثبات، محترم شمردن حریم شخصی، نظارت و برآورد انسانی، شفافیت و توصیف‌پذیری، مسئولیت‌پذیری و پاسخگویی، ارتقاء آگاهی و دانش تکنولوژیک و نظارت و همکاری چندجانبه و هماهنگ کشورهای عضو است.

نمونه خطر سوگیری هوش مصنوعی







سوگیری در بازسازی چهره اساتید بر اساس رشته‌هایشان توسط هوش مصنوعی

zoomit: حکایت از برخی سوگیری‌های ذاتی مدل‌های هوش مصنوعیِ مولدِ تصویر همچون میدجرنی دارد. در ویدئوی ۴۰ ثانیه‌ای که باعنوان «چهره استادان بر اساس رشته‌هایشان» در **ردیت** منتشر شد، به عقیده بر اساس تجاربشان این تصاویر به شدت به واقعیت نزدیک بودند در حالی که برخی دیگر بر این باور بودند که بیشتر این تصاویر فقط مردان جاافتاده و سفیدپوست را در لباس اساتید نشان می‌دهد که در مورد اکثر مؤسسات دانشگاهی مدرن، صادق نیست.

هوش مصنوعی چاقو/شمشیر دو لبه

هوش مصنوعی یک شمشیر دو لبه است که می تواند به عنوان یک راه حل امنیتی یا به عنوان یک سلاح توسط هکرها استفاده شود. (VARINDIA ,2022)

اینکه از آن در مسیر اهداف درست و صحیح بهره بگیریم یا در مسیر اهداف صدمه زننده و یا آسیب زا، همین نگاه را در خصوص حریم خصوصی نیز از بعد کمک به حفظ یا نقض آن صادق باشد.

حریم خصوصی چیست؟

حریم خصوصی شامل قلمرو شخصی و خصوصی فرد، خانواده، محل زندگی و اقامت، مکاتبات شخصی، شرافت، حیثیت و آبروی او می شود. که به این لیست باید کلیه اطلاعات و داده های شخصی افراد و ارتباطات او در فضای واقعی و مجازی را نیز اضافه کرد. برای حفظ حریم خصوصی، قوانین حمایت و مصونیتهایی به افراد می دهد در عین اینکه افراد برای حفظ این حریم، مانند پرچین، موانعی بین خود و دیگران تعریف می کنند. در یک جامعه افراد از طریق حریم خصوصی می‌توانند حد و مرز ارتباطات خود را با دنیای بیرون تعیین کرده و از کنترل اطلاعات خود توسط دیگران (دولت، سازمان و شرکت‌ها و اشخاص حقیقی) جلوگیری کنند.

گونه های حریم خصوصی

حریم خصوصی جسمانی: حق اشخاص در مصونیت از تعرض به تمامیت جسمانی است، از جمله جنبه های مرتبط با سلامت جسمی و روحی و همچنین، ویژگی های محرمانه بدن.

حریم خصوصی در منازل و اماکن: حق اولیه افراد در مصونیت از تعرض به منازل و اماکن و به طور کلی، کلیه مکان های سرپوشیده یا محصور است.

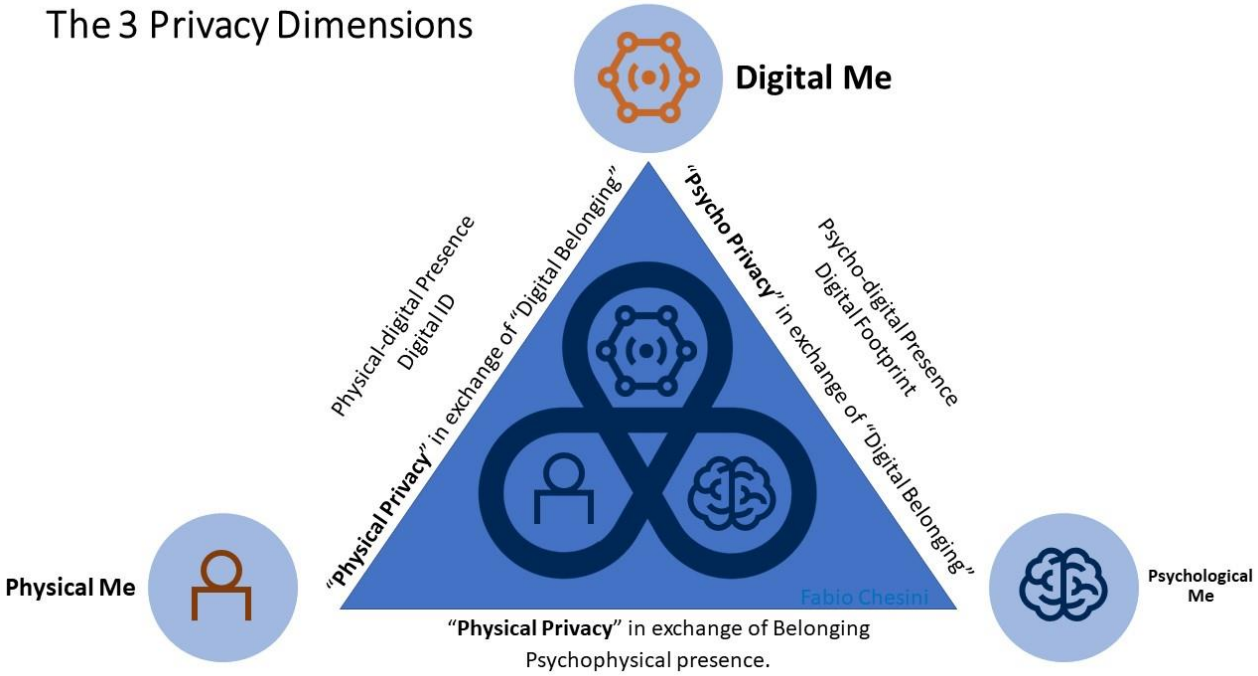
حریم خصوصی ارتباطاتی: حق اشخاص در امنیت و محرمانه ماندن محتوای کلیه اشکال مراسلات است که در آن اشخاص به هر گونه تعرض و تجاوز دیگران به داده هایی که مربوط به ایشان احساس مصونیت می کنند .

حریم خصوصی اطلاعات: حق اولیه افراد در محرمانه ماندن و جلوگیری از تحصیل ، پردازش و انتشار داده های شخصی مربوط به ایشان است، مگر در موارد قانونی.

عناصر حریم خصوصی

- **خصوصی‌بودن**
- آزادی از محدودیت‌های حقوقی
- استقلال انحصاری در تصمیم‌گیری
- **عدم جواز دخالت و نظارت دیگران بر آن**
- **پنهانی بودن آن** و نداشتن جواز ورود به آن یا اطلاع از آن، بدون اجازه

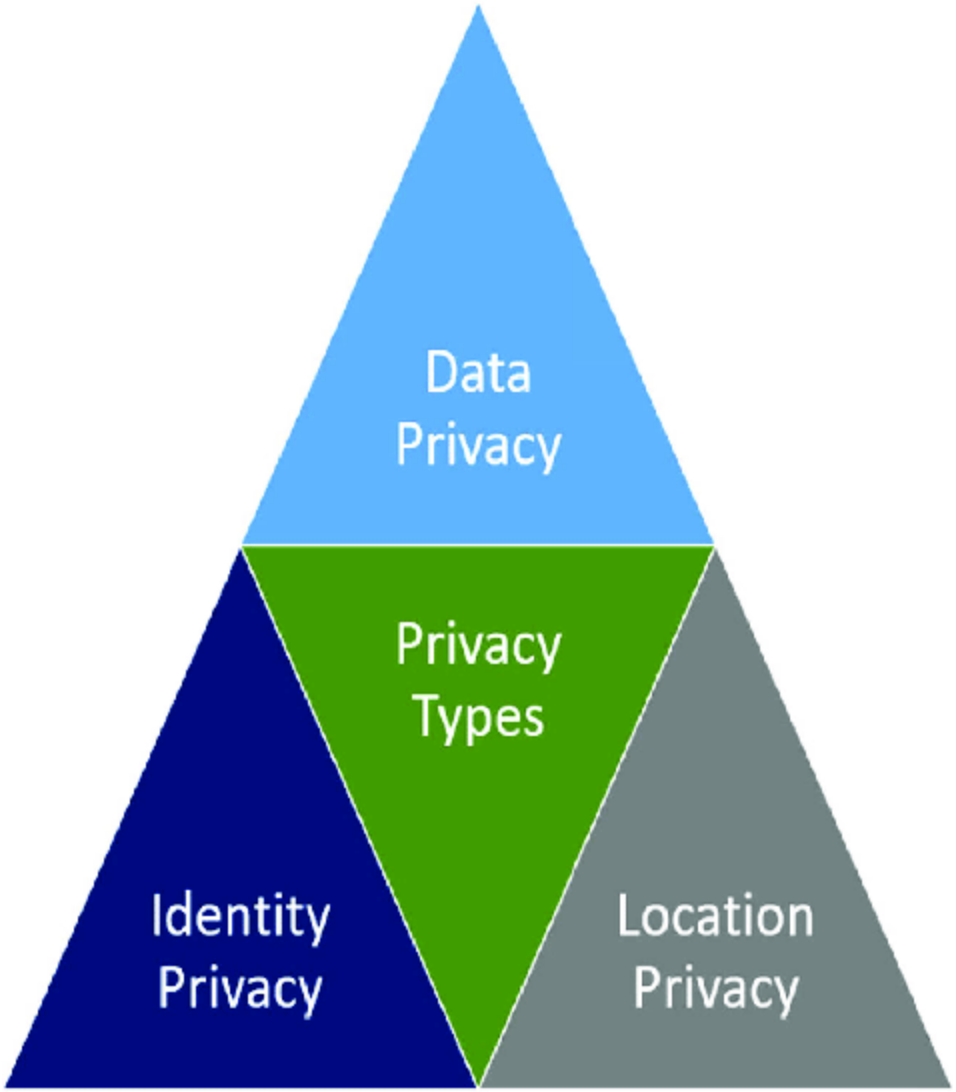
تسلط بر ۳ بعد حریم خصوصی



برای درک بیشتر حریم خصوصی، باید رفتارهای خود را از ۳ بعد مختلف و به هم پیوسته تجزیه و تحلیل کنیم: یک بعد فیزیکی (ملموس) و روانی (عاطفی) و من دیجیتال. این سه بعد دارای مبادلاتی با یکدیگر هستند. ما ممکن است چندین نسخه «من دیجیتال» از خودمان داشته باشیم که توسط چندین پلتفرم دیجیتال فعال شده است. با این حال، همه شخصیت‌های دیجیتال ما به شدت با محدودیت‌های روانی-فیزیکی ما (یک بدن زنده فیزیکی) مرتبط هستند. (Chesini,2020)

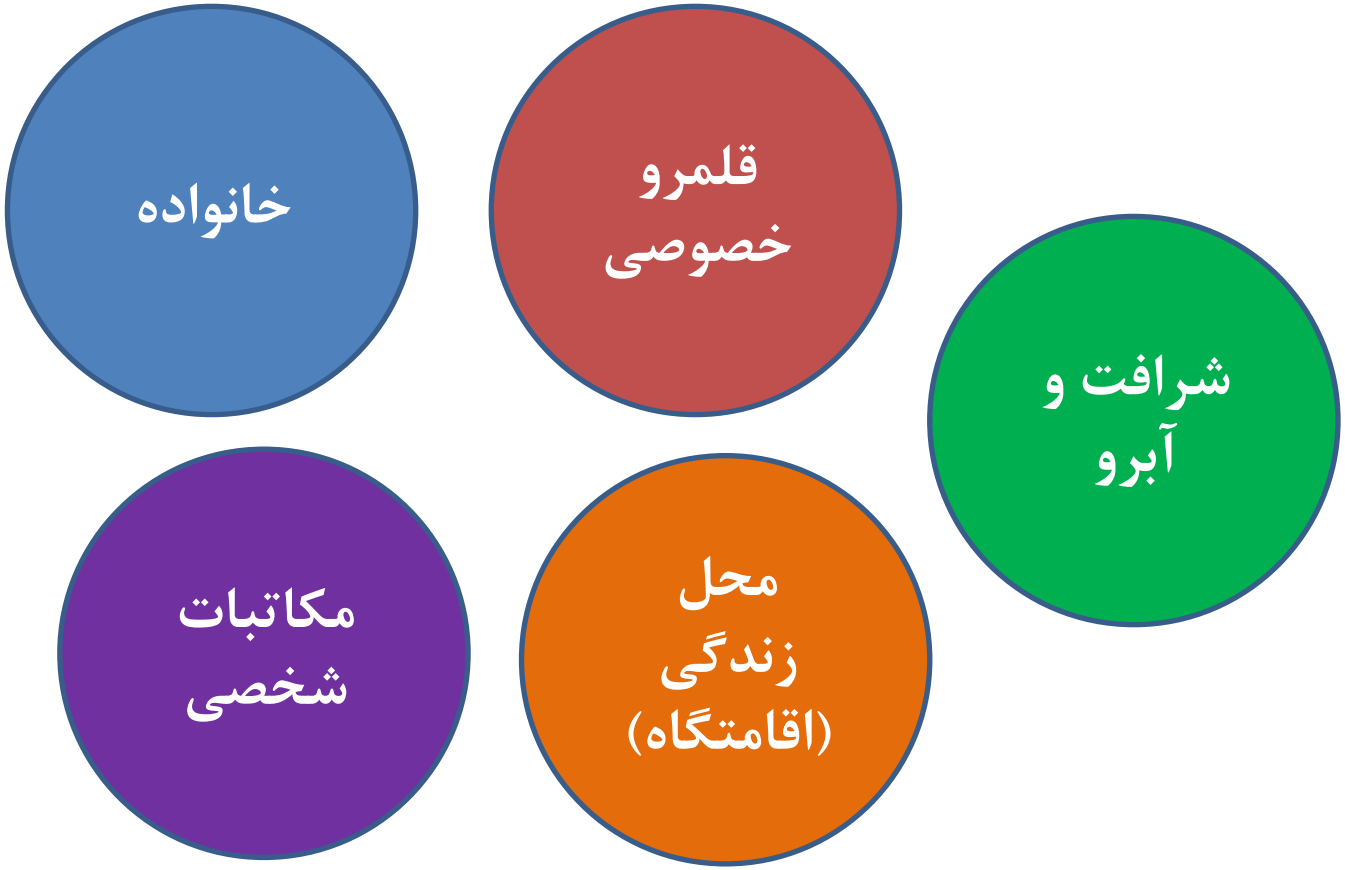
ما هرچه بیشتر با هم در ارتباط باشیم، حریم خصوصی کمتری داریم. در ازای تأمین سلسله نیازهای مازلو، گاه ناچار به از دست دادن بخشی از حریم خصوصی خویش هستیم.

انواع حریم خصوصی



اعلامیه حقوق بشر

ماده ۱۲- احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود، نباید مورد مداخله های خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد حمله قرار گیرد. هر کس حق دارد در مقابل اینگونه مداخلات و حملات مورد حمایت قانون قرار گیرد.

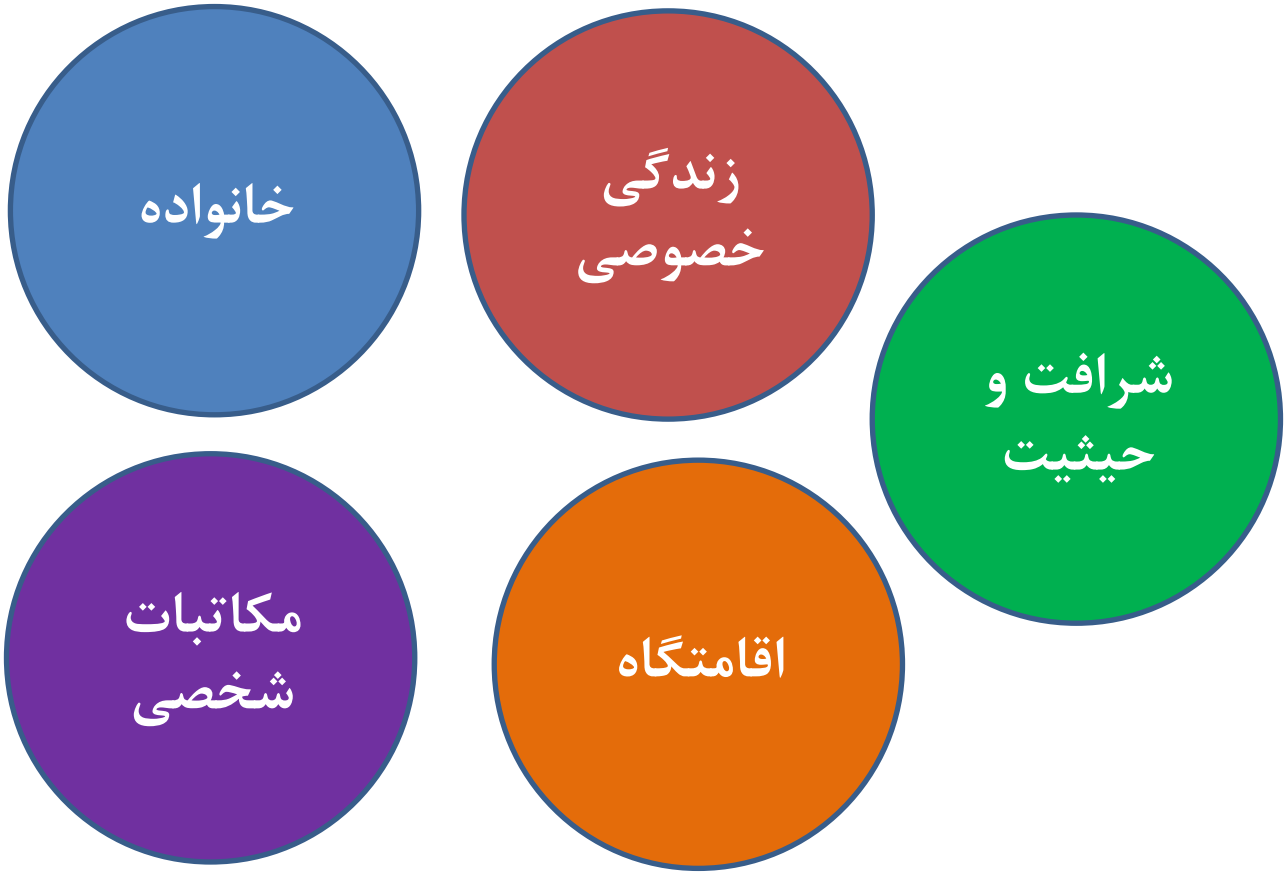


میثاق حقوق مدنی و سیاسی مصوب۱۹۶۶ میلادی

ماده ۱۷

۱. هیچ کس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود.

۲. هر کس حق دارد در مقابل این گونه مداخلات یا تعرض‌ها از حمایت قانون برخوردار گردد.



ماده ۱۷ میثاق تا حدودی همان پیام ماده ۱۲ اعلامیه جهانی حقوق بشر رادارد. با این تفاوت که در ماده ۱۷ورود به حریم خصوصی افراد را بامجوزقانون قبول نموده است.

حریم خصوصی یک حق اساسی است که برای استقلال و حفاظت از کرامت انسانی، ضروری و مهم است و به عنوان یکی از ستون های مفهوم حقوق بشر است.
حریم خصوصی یک حق انسانی است که نتیجه رعایت و حفظ آن احساس امنیت و آرامش افراد یک جامعه است.
حفظ حریم خصوصی افراد ضروری است از آن حیث که هر شخص دارای اطلاعات با ارزشی است که فاش شدن یا دسترسی غیر مجاز به آن اطلاعات ممکن است به نوعی باعث استرس، رنجش و صدمه به او شود.

متن اعلامیه اسلامی حقوق بشر مصوب ۱۴ محرم ۱۴۱۱ قمری
(مطابق با ۵ اوت ۱۹۹۰ میلادی و ۱۵ مرداد ۱۳۶۹ شمسی)
اجلاس وزرای امور خارجه سازمان کنفرانس اسلامی در قاهره

ب. هر انسانی حق دارد که در امور زندگی خصوصی خود (در مسکن و خانواده و مال, ارتباطات) استقلال داشته باشد و جاسوسی یا نظارت بر او, با مخدوش کردن حیثیت او جایز نیست و باید از او در مقابل هرگونه دخالت زورگویانه در این شئون حمایت شود.

عکسها: جورجیو باررا

حریم خصوصی در قانون اساسی

اصل بیست و دوم: حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند.

اصل **بیست و سوم** : تفتیش عقاید ممنوع است و هیچ‌کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مواخذه قرار دارد.

قانون جرائم رایانه ای

ماده۱۷ـ هر کس به وسیله سامانه های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

قانون مطبوعات

ماده ۳۱ - انتشار مطالبی که مشتمل بر تهدید به هتک شرف و یا حیثیت و یا افشای اسرار شخصی باشد ممنوع است و مدیر مسئول به محاکم‌قضایی معرفی و با وی طبق قانون تعزیرات رفتار خواهد شد.

طرح حمایت و حفاظت از داده و اطلاعات شخصی در ایران
(به امضای ۳۱ نماینده مجلس)

هدف اصلی این قانون صیانت از حیثیت و کرامت اشخاص موضوع داده ها و اطلاعات است که از راههای ذیل تحقق می یابد:

لف) تبیین حقوق اشخاص موضوع داده ها و اطلاعات، به ویژه در تعامل با سایر حق های مشروع

ب) ضابطه پذیری پردازش داده ها و اطلاعات شخصی

پ) مسؤولیت پذیری کنشگران پردازش داده ها و اطلاعات شخصی

ت) هم افزایی امور تنظیمی و نظارتی پردازش داده ها و اطلاعات شخصی

ث) جبران پذیری زیانها و آسیبهای ناشی از پردازش داده ها و اطلاعات شخصی.

داده و اطلاعات شخصی عبارت است از داده و اطلاعاتی که به تنهایی یا به همراه داده های دیگر، شخص موضوع داده را می شناساند.

اینکه آن اطلاعات به شخصی مرتبط شد، می توان از آن به عنوان داده های شخصی یاد کرد و ذیل حریم خصوصی آورد.

در جریان آغاز نبرد و رقابت غولهای فناوری بر سر عرضه دستاوردهای خود در حوزه هوش مصنوعی:

- نباید نسبت به حفظ حریم خصوصی افراد بی توجه بوده و از آن غفلت بورزند
- در برابر حفظ حریم خصوصی افراد از جمله حریم خصوصی داده ها و ذهن پایبند بوده
- و در این خصوص پاسخگو باشند
- در زمان اعطای مجوز به فعالیت این شرکتها، بر لزوم پایبندی به حقوق و حریم خصوصی افراد تأکید شده
- در تصویب قوانین حفظ حریم خصوصی متناسب با تحولات مدنظر قرار گیرد

هوش مصنوعی قادر به جمع آوری و پردازش حجم بسیار زیادی از داده ها است و در صورتی که این داده ها شامل اطلاعات حساس یا شخصی افراد باشند، ممکن است به حریم خصوصی آنها آسیب برساند.
به عنوان مثال، در حوزه تحلیل داده ها، هوش مصنوعی قادر به جمع آوری و تحلیل اطلاعات شخصی افراد است. در صورتی که این اطلاعات بدون اجازه یا به صورت غیرمجاز جمع آوری شوند، ممکن است به حریم خصوصی افراد آسیب برساند. همچنین، در حوزه پردازش تصویر و تشخیص چهره، هوش مصنوعی قادر به شناسایی چهره افراد در تصاویر و فیلم ها است. در صورتی که این اطلاعات بدون رضایت افراد استفاده شوند، ممکن است به حریم خصوصی آنها آسیب برساند. (فرادید ، خرداد ۱۴۰۲)

با وجود، توجه به حریم خصوصی در قوانین موجود، ولی در حوزه ابعاد مختلف حریم خصوصی اعم از حریم خصوصی داده ها، حریم خصوصی ذهن و.... به ویژه با آثاری که هوش مصنوعی بر حریم خصوصی دارد، نیازمند قوانین لازم و جدید هستیم.

هوش مصنوعی قادر به جمع آوری و پردازش حجم بسیار زیادی از داده ها است و در صورتی که این داده ها شامل اطلاعات حساس یا شخصی افراد باشند، ممکن است به حریم خصوصی آنها آسیب برساند.
استفاده نادرست از هوش مصنوعی در حوزه هایی مانند تحلیل داده ها و ردیابی فردی نیز ممکن است باعث نگرانی و ترس مردم شود، **به خصوص در صورتی که اطلاعات شخصی و حریم خصوصی افراد به نحوی توسط هوش مصنوعی نقض شود.**
اما برای جلوگیری از استفاده نادرست از هوش مصنوعی، باید قوانین و مقررات مناسبی برای استفاده از آن در نظر گرفته شود و به نحوی طراحی شود که حقوق و حریم خصوصی افراد را به حداکثر محافظت برساند.

تدوین و تصویب قوانین مرتبط با هوش مصنوعی با برخی ملاحظات صورت گیرد:

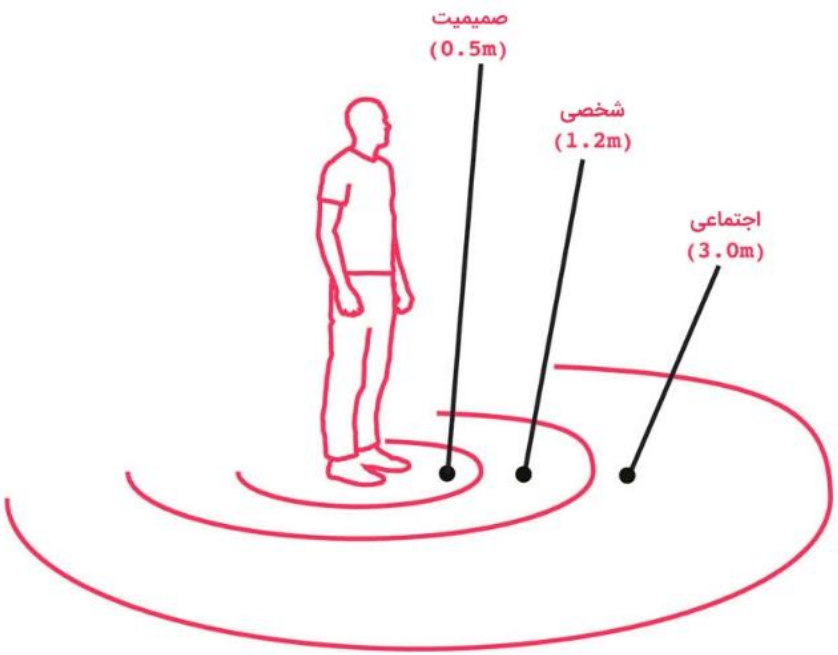
- لزوم بهره گیری از تجارب دیگر کشورها در این حوزه
- توجه به اینکه قوانین مانع از نوآوری های جدید در حوزه هوش مصنوعی نشود
- در تصویب قوانین به سرعت توسعه و تحول هوش مصنوعی به عنوان یک ماشین یادگیرنده توجه شود (پهلوان، ۱۴۰۱)

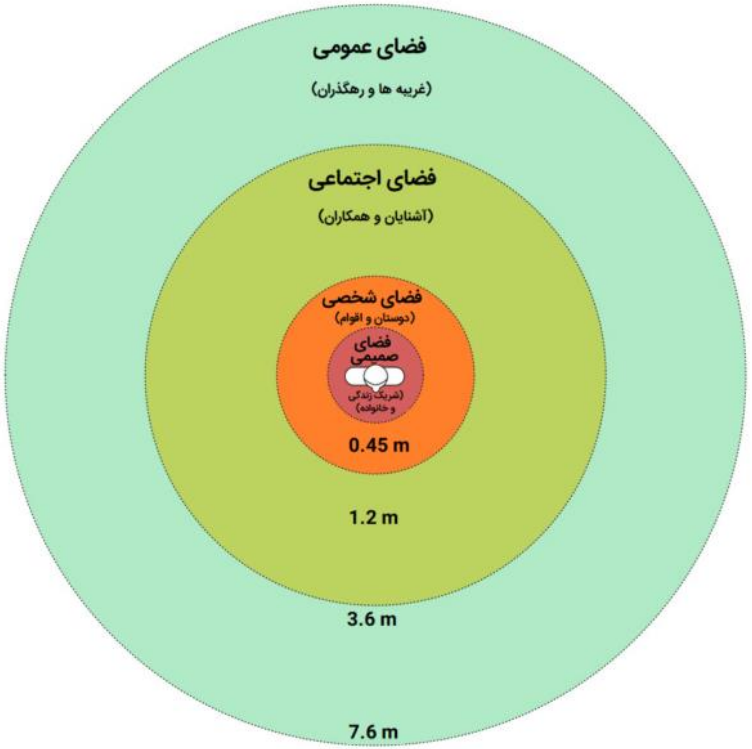
براین اساس لزوم توجه به این نکات در تصویب قوانین جدید مرتبط با هوش مصنوعی:

- رعایت حقوق و ارزشهای اساسی افراد از جمله حریم خصوصی آنها
- تقویت سرمایه گذاری و نوآوری در حوزه هوش مصنوعی
- لحاظ ملاحظات حاکمیتی
- مصرف‌کنندگان دارای حق درک (و انصراف از) فناوری‌های تصمیم‌گیری خودکار را داشته باشند که این شامل هوش مصنوعی هم می شود

قوانین در این حوزه باید پویا بوده و همگام با تحولات به روز شوند.
حفظ حریم خصوصی در این شرایط یک هدف متحرک است.

حریم شخصی جسمانی/ فیزیکی

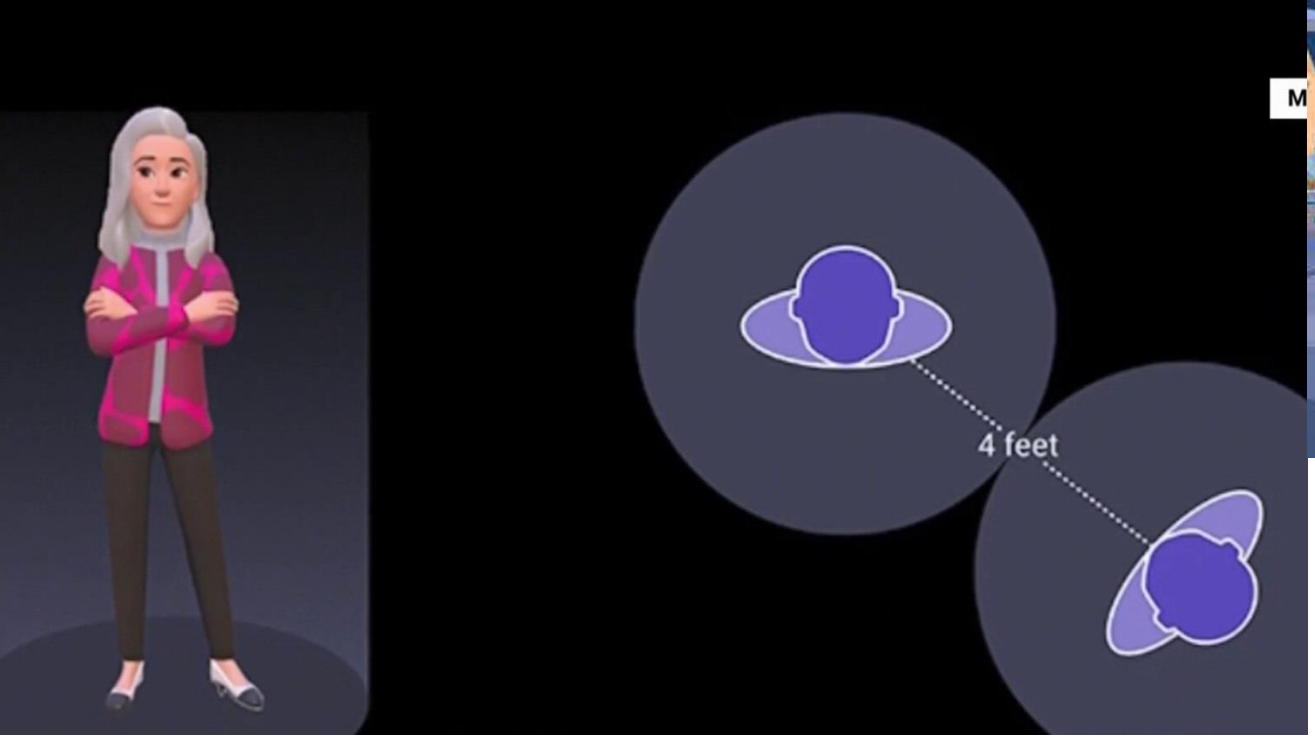




برای حریم خصوصی ابعاد مختلفی قائلند که از این جمله حریم شخصی جسمانی که ذیل آن بر بحث فاصله شخصی تأکید می شود. در فضای شخصی فواصلی بین انسان در محیط های شخصی، خانوادگی، کاری، اجتماعی و... تعریف شده است. در این فضاها افراد یک حباب یا حفاظی نامحسوس در اطراف بدن خود فرض می کنند.

حریم شخصی جسمانی را می‌توان به نوعی جلوگیری از وارد شدن فردی مزاحم به خلوت شخص تعریف کرد که سبب ایجاد حس ناامنی در فرد می‌شود. در برخی کشورها قوانینی جهت حفظ این نوع از حریم خصوصی وضع شده است. به عنوان مثال نوعی از این قوانین رعایت فاصله اشخاص با یکدیگر است که با نام فاصله شخصی (Personal Space) شناخته می‌شود. هرگونه ورود به فضای شخصی و هرگونه تماس جسمانی با فرد بدون رضایت وی، نقض حریم خصوصی و تعرض محسوب می شود. حریم خصوصی فیزیکی در برخی موقعیت ها به طور مثال امنیت پرواز فرودگاه، به دلایل پزشکی و... ممکن است نقض شود.

در کنار قوانین مرتبط با حریم خصوصی، مسائل عرفی نیز در این خصوص موثر است. به طور مثال خیره شدن به یک نفر ممکن است در برخی کشورها نقض یا صدمه زننده به حریم خصوصی افراد تعریف شود.
در بعضی کشورها به روشهای مختلف سعی می شود این مسأله آموزش داده شود. به عنوان مثال، در روسیه به کمک گرافیک نوول به پناه جویان آموزش داده می شود که از انجام برخی رفتارهای نادرست مانند خیره شدن و یا دست زدن به زنان خودداری کنند. (سلیمی و سلیمی، ۱۳۹۶: ۱۳۸)



حفظ حریم فیزیکی افراد به یاری حباب حفاظتی در دنیای متاورس

در پی آزار جنسی صورت گرفته متاورس در تلاش است تا در نسخه بتای خود از یک حباب حفاظتی برای کاربران استفاده کند تا کسی نتواند با کاربر ارتباط لمسی یا امکان صحبت بیابد تا زمانی که این حباب را بردارد. تا زمانی که این نوع محافظتها از کاربران صورت نگیرد، متاورس نمی تواند به مکان کاملاً امن تبدیل شود.

باید در نظر داشت که آزار جنسی فقط فیزیکی نیست بلکه می تواند کلامی نیز باشد. از سوی آزار جنسی فقط محدود به فضای واقعی نیست، می تواند شامل فضای مجازی هم باشد. (Basu,2021)

به نقل از اینستاگرام بی بی سی، متا در پاسخ به گزارشهای مربوط به آزار جنسی در متاورس بین آواراتهار فاصله گذاری کرده و این فاصله حدود ۱.۲ متر یا چهار فیت تعریف شده است. تا به این ترتیب برخوردهای ناخواسته کاهش یابد.

حریم خصوصی ذهن

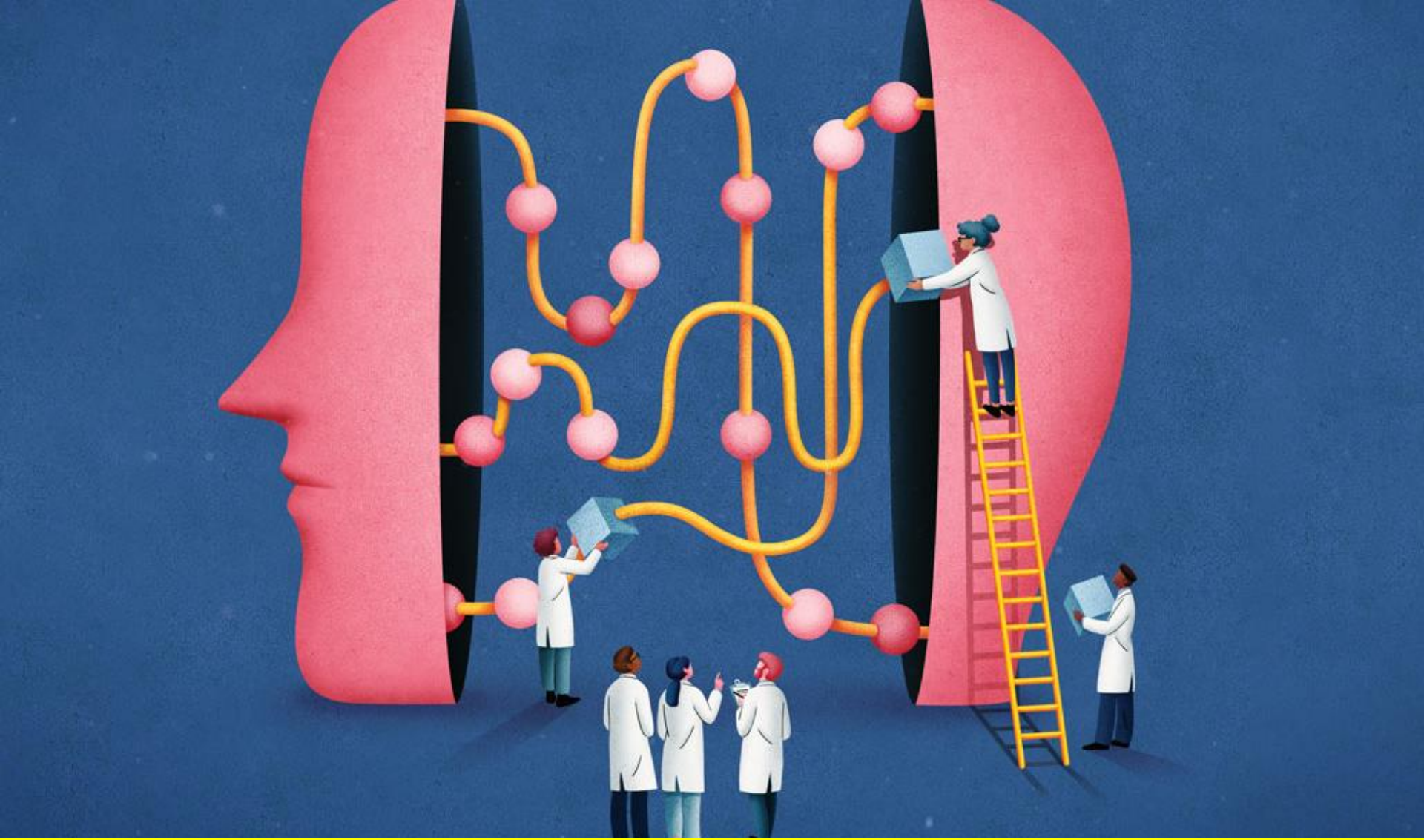
Susie Alegre در کتاب خود در حوزه آزادی ذهن بر **لزوم توانایی خصوصی نگه داشتن افکار**، مصون بودن از دستکاری افکار و عدم مجازات شدن به خاطر افکار تأکید می کند.

حریم خصوصی ذهن، حریم خصوصی فکر و آزادی اندیشه فراتر از آزادی بیان است و عموم قوانین از آنها حمایت می کند.

اتحادیه اروپا، بر عدم نفوذ هوش مصنوعی به ذهن تأکید کرده چیزی که مورد توجه و دغدغه الگره نیز هست. زیرا "فناوری بزرگ همه ما را در همه جا و همیشه می خواند.با وجود این واقعیت که «استخراج افکار ما بدون رضایت آگاهانه ما مطلقاً نقض حق آزادی فکر ما است».

باید دقت ویژه ای در به کارگیری این فناوری ها در عدالت به عنوان وسیله ای برای قضاوت یا حتی پیشگیری از جرایم صورت گیرد. (Ortega,2022)

ایمپلنت ها ، تراشه ها مغزی، الکترودهای کاشتنی، کلاه، هدست مخصوص و دیگر ابزارهای مشابه که امکان ورود و نفوذ به مغز را می دهند، سبب مشکلات جدی در حفظ حریم خصوصی افراد ایجاد می کنند.
اینکه به کمک واسطه هایی بین مغز و کامپیوتر نه تنها افکار خودآگاه که حتی افکار ناخودآگاه افراد را خواند و از آنها بهره گرفت، یک ترس غایی است. در چنین شرایطی دیگر چه چیزی از حریم خصوصی افراد به ویژه حریم خصوصی ذهن باقی می ماند؟ (Sanders,2021)



در حال حاضر، دسترسی شرکتها به رفتارهای افراد همچون لایکها، کلیکها، تاریخچه خریدها، اطلاعات پروفایلها، کامنتها و بازخوردها و... است که با تحلیل این داده ها و اطلاعات، پیش بینی های خوبی به آنها می دهد.
روزی که به یاری فناوریهای عصبی، به داده های عصبی دسترسی ایجاد شود چه خواهد شد؟ در آن شرایط، شرکتها مستقیماً به آنچه در مغز و ذهن افراد وجود دارد دسترسی خواهند داشت. (Sanders,2021)

در حال حاضر فناوری برای خواندن فعالیت مغز و تغییر آن وجود دارد مانند پیش بینی تشنج یک فرد مبتلا به صرع و جلوگیری از این تشنج، یک نگرانی جدی در حال حاضر، توان دسترسی به مغز و فعالیتهای آن و رفتارهای مربوطه و توان ایجاد تغییر و دستکاری در آن است.

در حال حاضر مهمترین بحث به دست آوردن قلب و ذهن افراد است که هسته اصلی تبلیغات و سیاست را تشکیل می دهد. حال اگر با این تحولات امکان دسترسی به مغز و تغییر و دستکاری فعالیتها و رفتارهای انها در خدمت تبلیغات و سیاست و دیگر اهداف احتمالی فراهم شود، چه خواهد شد؟ (Sanders,2021)

رافائل یوست (Rafael Yuste) یک نوروبیولوژیست در دانشگاه کلمبیا در نیویورک است. او می‌گوید: «ما به توانایی استخراج اطلاعات خصوصی از مغز افراد بسیار نزدیک شده‌ایم».

یوست و دیگرانی مایلند قوانین سختگیرانه ای برای محافظت از حریم خصوصی افراد به خصوص حریم خصوصی مغز و ذهن ایجاد شود. آنها مایلند که داده های سلول مغزی یک نفر باید مانند اندام های ما محافظت شود. هیچ کس نمی تواند کبد کسی را بدون تایید برای اهداف پزشکی خارج کند. این محققان مایلند داده‌های عصبی مانند همانها حفاظت‌ها شوند.

در حال حاضر تلاشهایی بررسی هایی در حال انجام است که چگونه می توان با روشهای حفاظتی جدید، از داده های عصبی محافظت تا شرکت‌ها نتوانند بدون اجازه افراد به آن داده‌های دسترسی پیدا کنند. (Sanders,2021)

به زودی مغز انسان تبدیل به یک دارایی جدید می شود. دارایی که می تواند سود زیادی برای شرکتهای که مشتاق استخراج داده های آن هستند ، پول خوبی به ارمغان بیاورد. افراد باید تصمیم بگیرند آیا حاضرند داده های مغز خود را بفروشند یا خیر؟ اگر کسی از آنچه می فروشد یا می بخشد به خوبی آگاه باشد، فکر می کند که باید این حق را داشته باشد که داده های خود را بفروشد یا آن را با چیزی که می خواهد مبادله کند.

در حال حاضر قوانین و دستورالعملهای موجود برای محافظت از حریم خصوصی پاسخگو نیستند. نیاز به قوانین لازم در حوزه حریم خصوصی ذهن و آزادی ذهنی (یعنی آزادی کنترل زندگی ذهنی خود) است. همچنین نیاز به رعایت مسائل اخلاقی بیش از پیش وجود دارد.

گرچه روشن نبودن مسائل اخلاقی استخراج داده های مغز مانع از سرعت نوروتکنولوژی آینده نمی شود ولی نیاز به بررسی های متفکرانه و قوانین مدیریت کننده لازم در این خصوص است. تا مجموعه این تلاشها به تعیین آنچه در آینده خواهد آمد و نیز محافظت از انسان در برابر آن کمک کند. (**Sanders,2021**)

نگرانی از دریافت مجوز آزمایش بالینی تراشه مغزی روی انسان توسط نورالینک

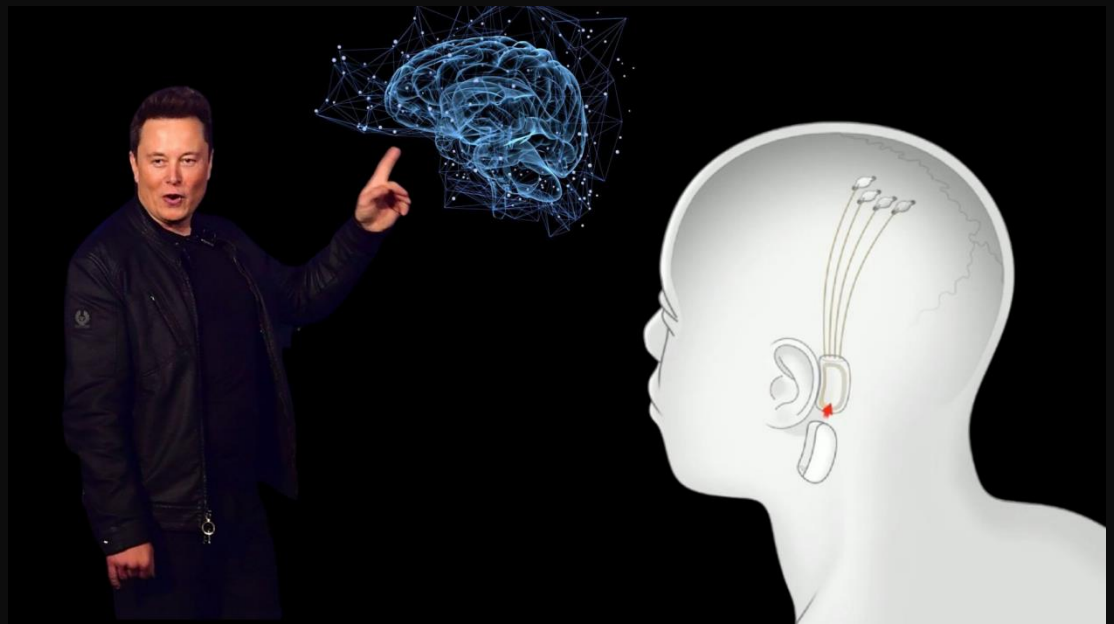
شرکت نورالینک (Neuralink) که به دست ایلان ماسک تاسیس شده، می‌خواهد با استفاده از توسعه تراشه مغزی محدودیت‌های ارتباطی بین انسان و کامپیوتر را بردارد. تا افراد بتوانند با استفاده از آن و اتصال مغزشان به اینترنت، کنترل وسایل دیجیتال را با مغز در دست بگیرند.
بناست از این فناوری برای اهداف پزشکی و درمانی در ارتباط با بیماریهایی مثل صرع، بازیابی بینایی، بازیابی حافظه، قابلیت تکلم و حرکت اندام فجل شده و... استفاده کرد.
در کنار مزایای بالای این فناوری، نگرانیهای بسیاری در خصوص خطرات و تبعات بهره گیری از آن وجود دارد. برخی از افراد معتقدند ممکن است استفاده انسان از N1نورالینک، زمینه بهره‌مندی او از سطوح بالای توانایی‌های هوش مصنوعی را فراهم کند و به این صورت بشر توانایی‌های خطرناکی را به دست آورد.

سپس این الکترودها می‌توانند سیگنال‌های الکتریکی درون مغز شما را تحلیل و آن‌ها را به شکل یک الگوریتم قابل فهم برای دستگاه‌ها و ماشین‌ها ترجمه کنند. به این روش نورالینک در حقیقت افکار انسان را می‌خواند و راهی پیدا می‌کند که بدون نیاز به باز کردن دهان‌تان، با ماشین‌ها ارتباط برقرار کنید. هدف چیپ N1در واقع ثبت و تحریک محرکهای الکتریکی درون مغز است. همچنین به کمک یک اپلیکیشن مخصوص می‌توانید مهارت‌های مختلف را یاد بگیرید.

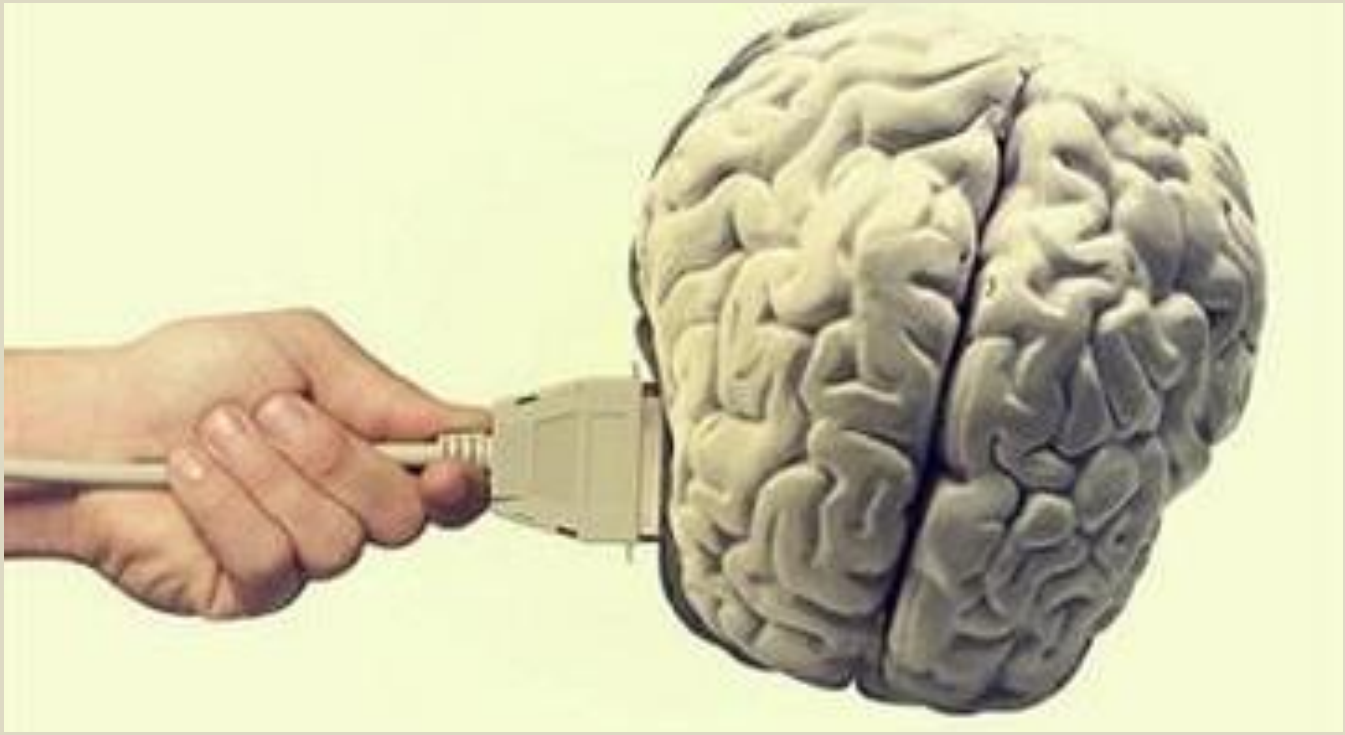
در حال حاضر طبق گفته کمپانی نورالینک تنها می‌توان دستگاه‌های ساده‌ای مثل گوشی موبایل هوشمند و کامپیوتر شخصی را با چیپ Neuralinkکنترل کرد و شاید هم بتوانید با تکرار افکارتان آن‌ها را تایپ کنید!

نورالینک همچنین از فناوری هوش مصنوعی کمک می‌گیرد و پتانسیل‌های بسیاری دارد. تصور کنید که دیگر برای برقراری ارتباط با بقیه مردم نیازی به تلفن همراه نداشته باشید! به این ترتیب احتمال رسیدن به مکالمات ذهنی و بی‌کلام هم خیلی دور از دسترس نیست.

به کمک فناوری جدید ایلان ماسک و کمپانی نورالینک همچنین سرعت برقراری ارتباطات نیز پایین می‌آید، چرا که دیگر نیازی به تایپ یا به زبان آوردن کلمات نیست. اما باید در نظر گرفت که تکنولوژی ثبت افکار و ترجمه کردن آن‌ها به شکل متن یا دستور زمان‌بر است و به این زودی‌ها به مرحله نهایی استفاده نخواهد رسید.
همچنین نگرانی‌هایی از این بابت وجود دارد که اگر دستگاه نورالینک به اینترنت متصل است، چه چیزی مانع هک و دزدیده شدن مستقیم اطلاعات از مغز ما توسط هکرها می‌شود؟ و همچنین اگر کسی مخفیانه به افکارمان گوش کند چه؟ هنوز برای این دو سوال جوابی وجود ندارد و تنها با آزمایش و خطا می‌تواند مشکلات آینده را حل نمود. (نورانی زاده، ۱۴۰۲)

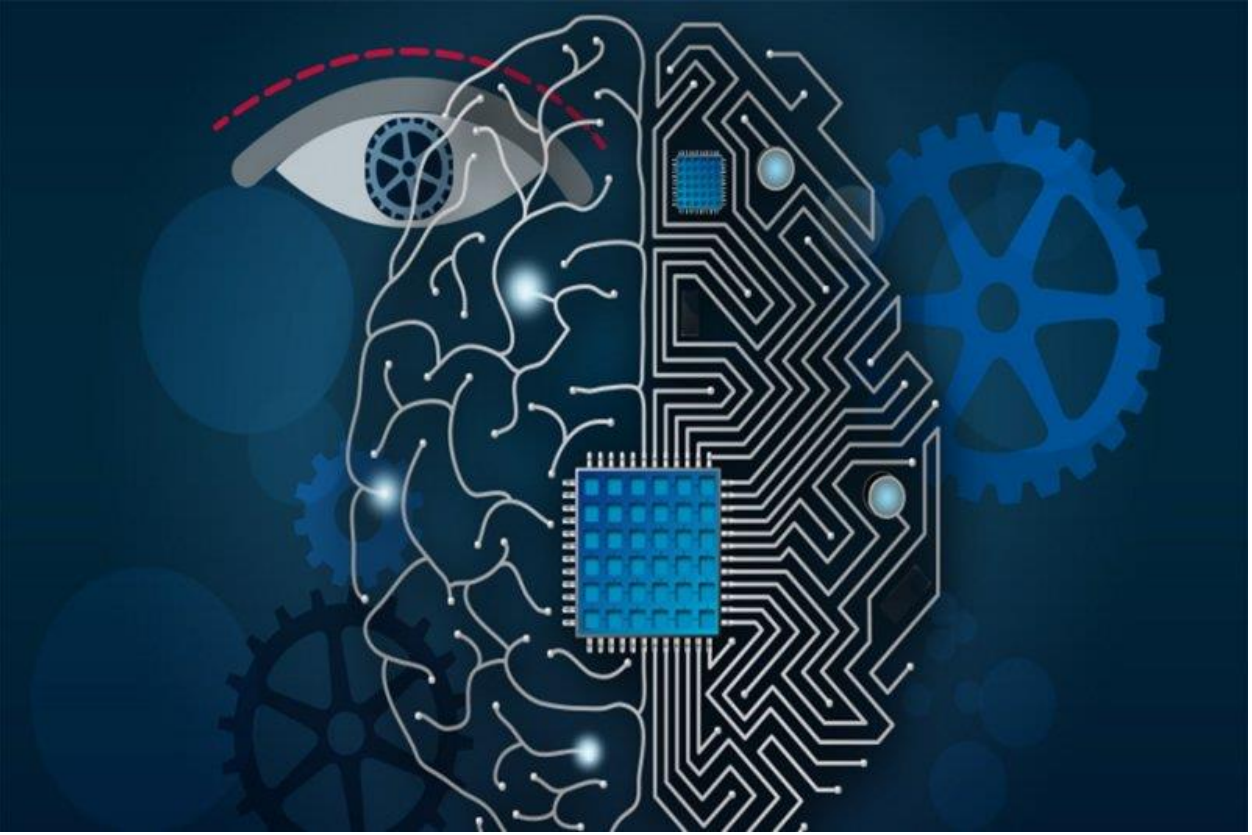


دلنگرانی ها در خصوص انتقال حافظه انسان پس از مرگ به هوش مصنوعی



یکی از تلاشها انتقال اطلاعات مربوط به حافظه انسان به کامپیوتر و هوش مصنوعی و سپس با طراحی یک بدن مصنوعی اطلاعات مغز را زنده نگه داشت.

در خصوص میزان تحقق چنین رویایی احتمالات و اما و اگرهای بسیاری وجود دارد ولی با تحقق ایــن رویــا، این نگرانی وجود دارد که خاطرات، کلیه اطلاعات مربوط حافظه و... پس از مرگ چه فرجامی خواهند یافت. این در شرایطی است که از ذهن انسان به عنوان بخشی از حریم خصوصی او یعنی حریم خصوصی ذهن یاد می شود و انجام چنین حرکتهایی می تواند موجبا نقض این حریم را فراهم کند.

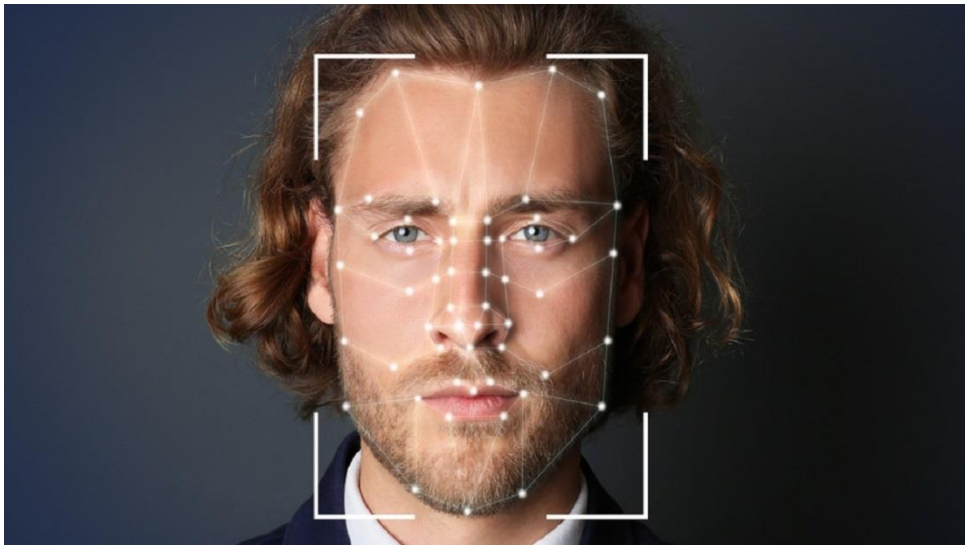


واقعیت این است که مغز صرفاً یک اندام نیست بلکه بستر بیوتکنولوژیکی اساسی برای قوای ذهنی ما همچون هوشیاری، حافظه، زبان، ادراک، احساسات و... است. همین چیزهاست که انسان را می سازند و از این منظر، پرداختن به اخلاقیات در ترکیب مغز انسان با ماشین ها با تأکید بر رعایت اخلاقیات و حفظ حریم خصوصی ذهن باید با دقت و جدیت بیشتری دنبال شود. (Mackenzie,2021)

نوروتکنولوژی می تواند به برخی مشکلات و بیماریها و اختلالات و درمان آنها کمک کند ولی از آن سو ، دست یافته های این حوزه می توانند آینده ای مبهم و پرتنش را پیش روی انسان بگذارند.
در حال حاضر حفظ حریم خصوصی داده های مغز در قوانین مورد توجه برخی کشورها قرار گرفته و تلاش می شود تا قوانین سخت گیرانه و ملاحظات اخلاقی را برای شرکتهای فناوری عصبی به تصویب رسانند. (Mackenzie,2021)

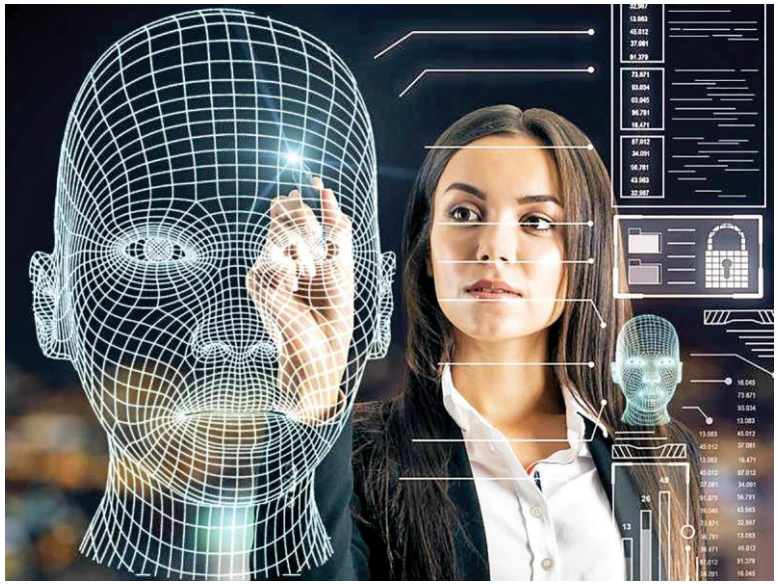
در کنار تصویب قوانین سختگیرانه، بر بحث آموزش و ارائه آگاهی به مردم نیز تأکید می شود اینکه مردم باید بدانند که مغز آنها دارای چه داده ها و اطلاعات ارزشمندی است. تا آنها با کسب توانمندیهای لازم بتوانند در خصوص فضای ذهنی و حریم خصوصی ذهنی خود تصمیمات آزاد و شایسته بگیرند. (Mackenzie,2021)

تشخیص ایدئولوژی سیاسی افراد
با تحلیل چهره آن‌ها توسط هوش مصنوعی



گروهی از محققان دانمارکی در مطالعه‌ای اعلام کرده‌اند که هوش مصنوعی با تجزیه و تحلیل تصاویر به این نتیجه رسیده که افراد راست‌گرا بیشتر در عکس‌ها با چهره شاد و افراد چپ‌گرا با چهره خنثی ظاهر می‌شوند. این بررسی که با عنوان «استفاده از فناوری یادگیری ماشینی برای پیش‌بینی ایدئولوژی از روی عکس‌های چهره» انجام شد، به خوبی نشان داد که هوش مصنوعی می‌تواند با بررسی یک عکس، ایدئولوژی سیاسی افراد را با دقت ۶۱ درصدی پیش‌بینی کند.

متخصصات دانمارکی این شبکه عصبی را با هزاران عکس سیاستمداران آموزش دادند و در این تصاویر فقط مشخصات و ویژگی‌های چهره افراد مشخص بود. درواقع هیچ عنصری در پس‌زمینه که نشان‌دهنده گرایش آن‌ها بود وجود نداشت. (بررسی ۴۶۴۷ عکس) محققان اذعان کردند که این نتایج، تهدید نشأت‌گرفته از فناوری یادگیری عمیق برای حریم خصوصی را تایید می‌کند. از سوی دیگر نگرانی هایی در خصوص احتمال بهره گیری از چنین قابلیتهایی در دست برخی حکومتها در برخورد با افرادی با عقاید و باورهای سیاسی – اجتماعی خاص وجود دارد. (شاهرخ، ۱۴۰۲)



خواندن فکر افراد
به یاری هوش مصنوعی

به گزارش «ایندیپندنت»، گروهی از دانشمندان مدعی‌اند که روشی پیدا کرده‌اند که به کمک آن می‌توانند با استفاده از اسکن مغزی و مدل‌سازی هوش مصنوعی، آنچه را افراد به آن فکر می‌کنند، آوانویسی (نوشتن نمادهای آوایی زبان) کنند. این روش گامی به سوی ذهن‌خوانی توصیف شده است.

دیوید رودریگز-آریاس وایلن، استاد اخلاق زیستی در دانشگاه گرانادای اسپانیا که در این تحقیق شرکت نداشت، گفت که این امر فراتر از آن چیزی پیش رفته است که رابط‌های قبلی مغز و کامپیوتر به دست آورده بودند. او گفت که این مورد ما را به آینده‌ای نزدیک می‌کند که در آن ماشین‌ها می‌توانند «ذهن‌ها را بخوانند و افکار را آوانویسی کنند» و هشدار داد که این امر ممکن است برخلاف میل افراد اتفاق بیفتد؛ مانند زمانی که آنها خواب‌اند. محققان چنین نگرانی‌هایی را پیش‌بینی کرده‌اند.
نها همچنین خواستار قوانینی برای محافظت از حریم شخصی ذهن شدند. رودریگز-آریاس وایلن، متخصص اخلاق زیستی گفت: «ذهن ما تاکنون حافظ حریم شخصی ما بوده است. این کشف می‌تواند نخستین گام برای به خطر انداختن این آزادی در آینده باشد.»

حریم خصوصی داده ها

یکی از عناصر مهم حق حفظ حریم خصوصی، حق حفاظت از داده های شخصی است که برخی از اسناد بین المللی و منطقه ای نیز بر لزوم حفاظت از داده های شخصی تأکید کرده اند که از جمله اینها مقررات حفاظت از اطلاعات عمومی (GDPR) است.

در مقررات حفاظت از اطلاعات عمومی اتحادیه اروپا به تعریف **داده خصوصی یا شخصی** چنین اشاره شده است: داده های خصوصی به داده هایی اطلاق می شود که می توان با استفاده از آن ها به صورت مستقیم و یا غیر مستقیم یک شخص را شناسایی کرد، این داده ها می توانند شامل نام یک فرد، شماره تلفن همراه، ویژگی های فیزیکی خاص، ویژگیهای روانشناختی هر موضوعی که بتوان با آن فردی را شناسایی کرد، باشند.
همچنین به دسته خاصی از اطلاعات شخصی که داده هایی از قبیل ملیت، نوع مذهب، رنگ پوست، دید کاربر به مسائل سیاسی و ... را شامل می شود. و همه این ها نیز جزوی از اطلاعات شخصی اطلاق می شود.

نام و آدرس
شماره های شناسایی منحصر به فرد: اطلاعاتی از جمله شماره های تأمین اجتماعی و شماره کارت های بازنشستگی.
داده های اجتماعی: اطلاعات مربوط به اتصالات اجتماعی یک فرد، از جمله نام دوستان یک فرد یا کسانی که آنها را در رسانه های اجتماعی دنبال می کنند.
دموگرافیک: اطلاعات جمعیتی شامل جنسیت، سن، ترجیحات جنسی، عضویت سیاسی یا درآمد فرد.
محتوای تولید شده توسط کاربر: تصاویر، نظرات، پست های وبلاگ و مقالات تولید شده توسط فرد.
داده های بیومتریک و ژنتیکی: هر گونه داده های بیومتریک یا ژنتیکی مرتبط با فرد.

حریم خصوصی داده ها همان حفاظت از داده‌هاست که شامل جمع‌آوری و نگهداری داده‌ها و اطلاعات دیجیتال یا غیردیجیتال داده‌ها می‌شود که می‌تواند شامل اسناد، مدارک شناسایی، فایل‌های دیجیتال شخصی، امضای دیجیتال، پسورد و غیره باشد.

چگونه هوش مصنوعی از داده های شخصی استفاده می کند؟

سیستم‌های هوش مصنوعی از داده‌های شخصی به روش‌های مختلفی استفاده می‌کنند، مانند:

۱. تجزیه و تحلیل پیش بینی

سیستم های هوش مصنوعی می توانند مقادیر زیادی از داده ها را برای پیش بینی رفتار فردی تجزیه و تحلیل کنند. به عنوان مثال، یک سیستم هوش مصنوعی ممکن است تاریخچه جستجو و فعالیت رسانه های اجتماعی یک فرد را برای پیش بینی علایق و ترجیحات آنها تجزیه و تحلیل کند.

۲. توصیه های شخصی

سیستم‌های هوش مصنوعی از داده‌های شخصی برای ارائه محصولات، خدمات و توصیه‌های محتوای شخصی‌شده استفاده می‌کنند. به عنوان مثال، یک سیستم هوش مصنوعی ممکن است از تاریخچه مرور و خرید یک فرد برای توصیه محصولاتی که احتمالاً به آنها علاقه دارد استفاده کند.

۳. کشف تقلب

سیستم های هوش مصنوعی می توانند از داده های شخصی برای شناسایی کلاهبرداری و سایر انواع فعالیت های مجرمانه استفاده کنند. به عنوان مثال، یک سیستم هوش مصنوعی ممکن است داده های مالی یک فرد را برای شناسایی تراکنش های غیرعادی که نشان دهنده تقلب است، تجزیه و تحلیل کند. (ThinkML,2023)

چند راهکار برای محافظت از حریم خصوصی در برابر هوش مصنوعی

انتخاب سرویس‌های بهره گیرنده از هوش مصنوعی با حریم خصوصی بالا :برخی سرویس‌ها حتی به شما اجازه می‌دهند تا داده‌های شخصی خود را تحت مالکیت خودتان نگه دارید و از آن‌ها بهره‌مند شوید.

استفاده از ابزارهای مدیریت حریم خصوصی :ابزارهایی مانندVPN ، مرورگرهای خصوصی، برنامه‌های مدیریت ردپای دیجیتال و مدیریت کوکی‌ها، برای محافظت از حریم خصوصی خود

محافظت از اطلاعات شخصی :از جمله مهمترین راهکارها برای حفظ حریم خصوصی، محافظت از اطلاعات شخصی (استفاده از رمزنگاری اطلاعات، استفاده از رمز عبورقوی و تغییر دادن آن به طور منظم، عدم اشتراک گذاری اطلاعات شخصی با سرویس‌های نامطمئن ، عدم ذخیره اطلاعات شخصی در دستگاه‌های عمومی مانند کتابخانه‌ها، ایستگاه‌های کامپیوتری و دستگاه‌های تلفن همراه و....)

پاکسازی داده‌های شخصی : بهتر است داده‌های شخصی خود را هرازگاهی پاکسازی کنید. این شامل پاک کردن ایمیل‌ها، پیام‌های متنی و صوتی، تصاویر و سایر فایل‌هایی است که دیگر نیازی به آن‌ها ندارید

آگاهی از نحوه استفاده از داده‌های شخصی:

توسعه الگوریتم‌های حریم خصوصی : این الگوریتم‌ها این امکان را می دهند که اطلاعات شخصی افراد به صورت رمزنگاری شده و مخفیانه به اشتراک گذاشته شوندد.(با استفاده روشهایی همچون افزودن نویز به داده‌های شخصی، جایگزینی داده‌های شخصی با داده‌های مشابه و اجرای عملیات‌ها در داده‌های رمزنگاری شده و...)

کسب اطلاع از به شرایط و قوانین استفاده از سرویس‌هایی که از هوش مصنوعی استفاده می‌کنند

برخی راهکارها برای محافظت از حریم خصوصی داده ها با استفاده از هوش مصنوعی

- از دیگر راهکارهای پیشنهاد دادن آگاهی به افراد در خصوص داده های خاص خواسته شده از آنهاست که این سبب می شود تا به راحتی تنظیمات حریم خصوصی خود را به روشهایی تغییر دهند. (harris,2021)
- توسعه روش های پوشش دهی داده ((data masking، رمز نگاری ((encryptionو ابزارهای محافظت اطلاعات شخصی، می تواند به حفاظت از حریم خصوصی افراد در برابر هوش مصنوعی کمک کند.
- استفاده از الگوریتم های مناسب برای پردازش داده ها و تضمین کنترل دسترسی به داده های شخصی، نیز می تواند به حفاظت از حریم خصوصی افراد کمک کند.
- برخی به استفاده از خود هوش مصنوعی در مسیر حفاظت از حریم خصوصی نیز اشاره می کنند

برخی توصیه ها به شرکتها

به حداقل رساندن داده ها

به حداقل رساندن داده ها به این اصل اشاره دارد که سازمان ها فقط باید حداقل داده های شخصی لازم را برای دستیابی به اهداف خود جمع آوری و پردازش کنند. این شامل پرهیز از جمع‌آوری داده‌های شخصی غیرضروری و محدود کردن نگهداری داده‌های شخصی فقط به مواردی است که برای یک هدف خاص مورد نیاز است. به حداقل رساندن داده ها در حفاظت از حقوق حریم خصوصی افراد و کاهش خطر نقض داده ها و سوء استفاده از داده های شخصی بسیار مهم است.

حریم خصوصی توسط طراحی

حریم خصوصی از طریق طراحی رویکردی برای توسعه سیستم‌های هوش مصنوعی است که از ابتدا حریم خصوصی و حفاظت از داده‌ها را در اولویت قرار می‌دهد. این شامل ادغام اصول حفظ حریم خصوصی و داده ها در طراحی، توسعه و استقرار سیستم های هوش مصنوعی است.

ناشناس سازی و نام مستعار

ناشناس سازی و نام مستعار تکنیک هایی هستند که برای محافظت از داده های شخصی با حذف یا جایگزینی شناسه هایی استفاده می شوند که می توانند داده ها را به افراد خاصی مرتبط کنند. ناشناس سازی به حذف تمام اطلاعات شناسایی از داده ها اشاره دارد، در حالی که نام مستعار شامل جایگزینی شناسه ها با شناسه های منحصر به فرد است که نمی توانند به یک فرد مرتبط شوند.

ارزیابی تأثیر حفاظت از داده (DPIA)

ارزیابی‌های تاثیر حفاظت از داده‌ها (DPIA) ارزیابی‌هایی هستند که سازمان‌ها می‌توانند برای شناسایی و ارزیابی خطرات حریم خصوصی مرتبط با سیستم‌های هوش مصنوعی خود انجام دهند. (ThinkML,2023)

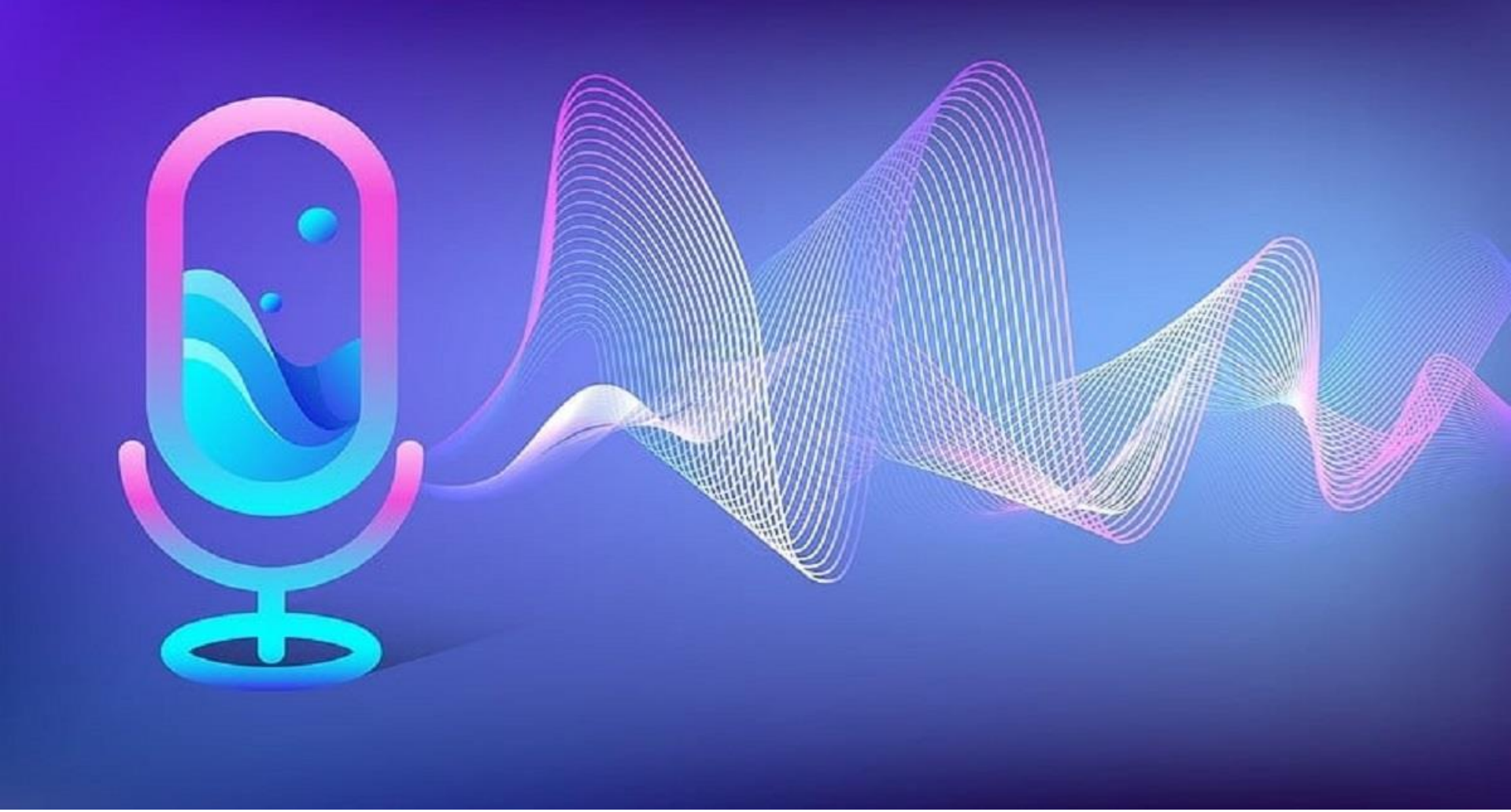
مدل هوش مصنوعی جدیدی که می‌تواند رمزهای عبور را حدس بزند

محققان مدل هوش مصنوعی جدیدی به نام PassGPT را ساخته‌اند که می‌تواند پسوردهای قوی بسازد و رمزهای عبور را حدس بزند.

این مدل روی مجموعه عظیمی از رمزهای عبور نشت‌یافته آموزش داده شده است و می‌تواند توانایی‌های خطرناک هوش مصنوعی را نشان دهد.

پژوهشگران ETH Zurich ، مرکز علم داده‌های سوئیس و SRI International در نیویورک با خلق PassGPT به‌دنبال ارزیابی ایمنی گذرواژه‌ها و کمک به تولید رمزهای عبور مستحکم‌تر بوده‌اند. نوآوری این مدل نه‌تنها در توانایی پیشگویی آن، بلکه در شیوه عملکرد منحصربه‌فرد آن نهفته است.

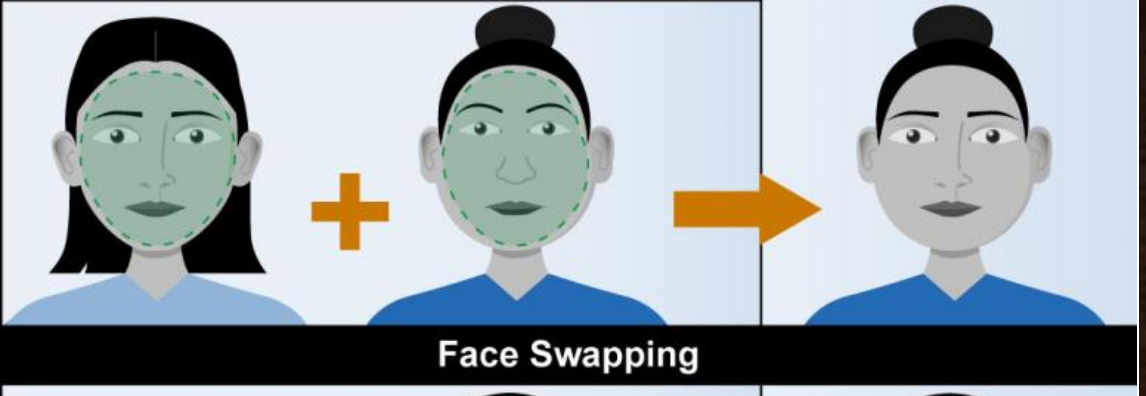
«خاوی راندو»، از خالقان این مدل هوش مصنوعی، می‌گوید PassGPT حدود ۲۰ درصد بهتر از مدل‌های پیشرفته GAN می‌تواند گذرواژه‌ها را حدس بزند. این مدل همچنین می‌تواند رمزهای منحصربه‌فردی را برای شما تولید کند. (Lanz,2023)

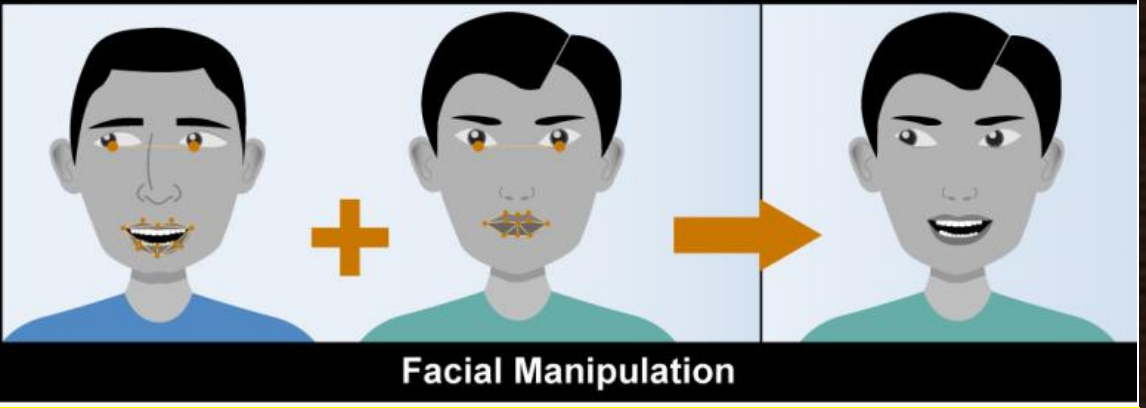


خطر هوش مصنوعی با توان تولید، ویرایش و تقلید صدا برای نقض حریم خصوصی و سوء استفاده های احتمالی

شرکت متا از مدل هوش مصنوعی قدرتمندی برای تبدیل متن به صدا و تولید صدای واقع گرایانه همراه با قابلیتهای جالب رونمایی کرده است می تواند متن ورودی با دقت بالایی به ۶ زبان تبدیل کند.

از جمله قابلیتهای آن توان تقلید صدای یک شخص است. هوش مصنوعی امکان حذف نویز و دیگر صداهای مزاحم را دارد. در کنار مزایای نگرانی هایی در خصوص امکان سوء استفاده بالا از آن وجود دارد.





خطر هوش مصنوعی در کمک به ساخت عکسها جعلی و دیپ فیکها

دیپ فیکها چالشها و مشکلات بسیاری را به وجود می آورد که در کنار تضعیف حقایق، تضعیف اعتماد عمومی، خطرات برای سیاست و امنیت، تأثیرات منفی بر هنر و فرهنگ و....، یکی از بزرگترین آسیبهای آنها به حوزه خصوصی افراد و نقض آن است.
استفاده از دیپ فیکها می تواند با جعل هویت افراد در رسانه ها و رسانه های اجتماعی و افراد با مشکلات از جمله به خطر افتادن امنیت شخصی و تهدید حریم خصوصی روبرو کند.
پیش بینی می شود در گام اول قربانیان دیپ فیکها سیاستمداران، سلبریتی، افراد مشهور و... و در فاز بعدی افراد معمولی با اهدافی چون اخاذی، انتقام جویی، صدمه به حیثیت افراد و... باشد.

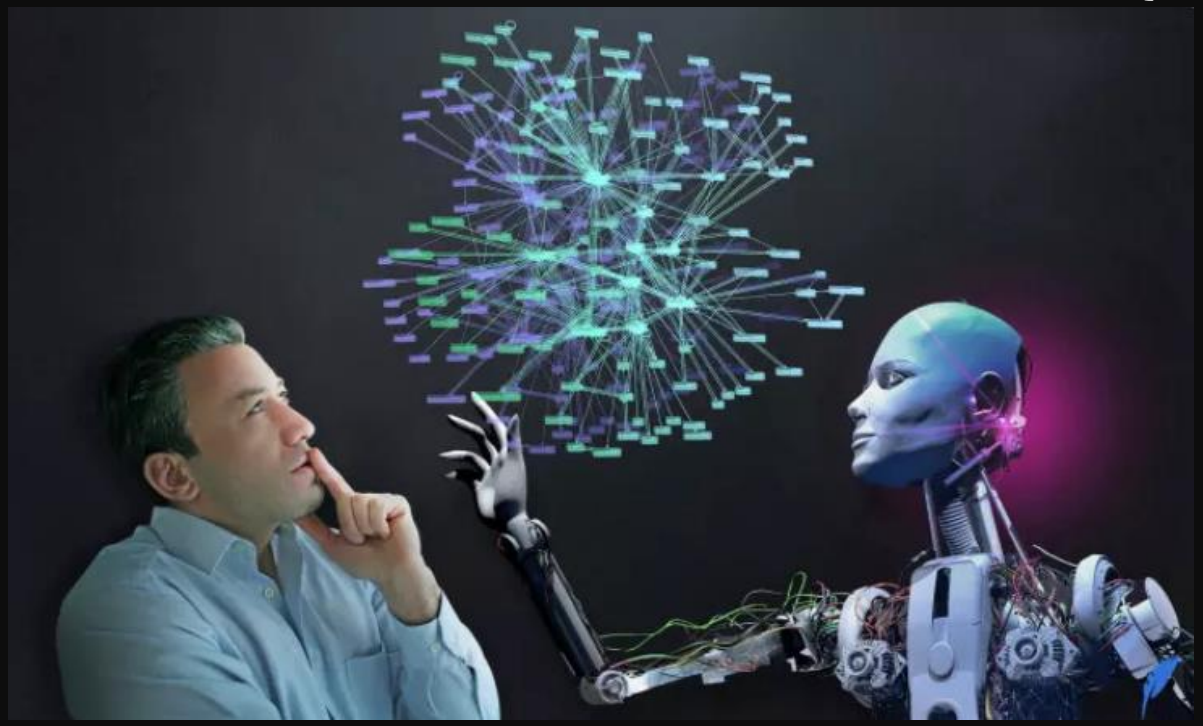
خطر جدی تر در حوزه دیپ فیکها براساس برخی مطالعات که به نگرانی ها دامن زده، قابل اعتمادتر به نظر آمدن چهره های جعلی در مقایسه با چهره های افراد واقعی است.

همین مشکلات را می توان به عکسهای جعلی ساخته شده با هوش مصنوعی تعمیم داد که این عکسها نیز می توانند با مشکلاتی مشابه دیپ فیکها همراه باشند. (نمونه پاپ با کاپشن سفید و دستگیری ترامپ با میدجرنی به یاری هوش مصنوعی ساخته شده اند که منجر به محدودیت دسترسی عمومی به میدجرنی شد)



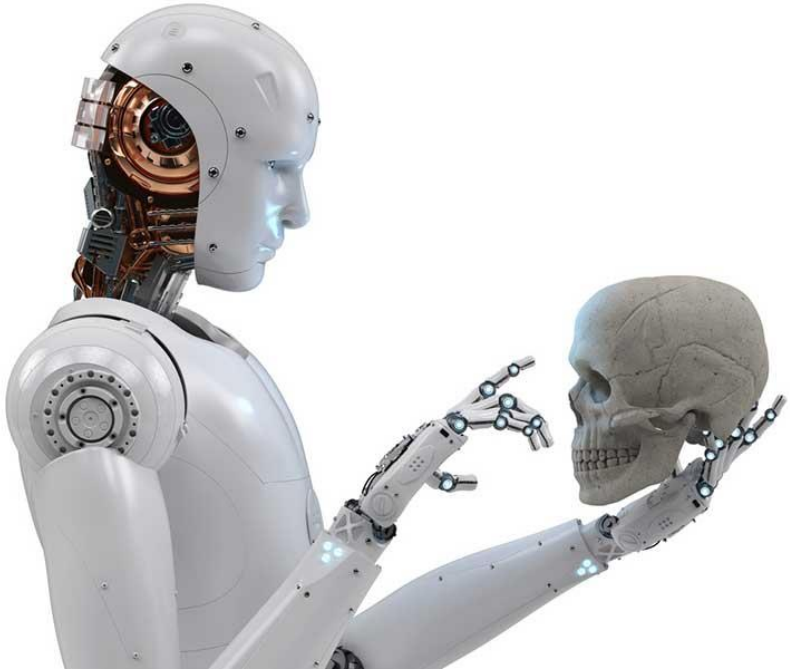

نقش آفرینی هوش مصنوعی در ارتباطات انسانی
از ارتباط میان زندگان تا مردگان

یاری هوش مصنوعی در تلاش برای تسهیل و تسریع در ارتباطات انسانی است ولی این تلاش فقط محدود جهان زندگان نمی شود، بله هوش مصنوعی می کوشد تا بعضاً حتی جهان زندگان و مردگان نیز ایجاد ارتباط کند. به طور نمونه هوش مصنوعی ایری، فرد قبل از مرگ حدود ۷ ساعت باید مقابل دوربین تا هوش مصنوعی بتواند نحوه صدا و حرکتش را یاد بگیرد.



همچنین فرد باید خاطرات و زندگی خود را به هوش مصنوعی ارائه کند تا پس از مرگ هوش مصنوعی بتواند اجازه تدهد تا خانواده متوفی با فرد درگذشته به این شکل در قالب چتهای ویدئویی و... ایجاد ارتباط کنند. (همشهری، ۱۴۰۱)

چالشهای مرده باتها



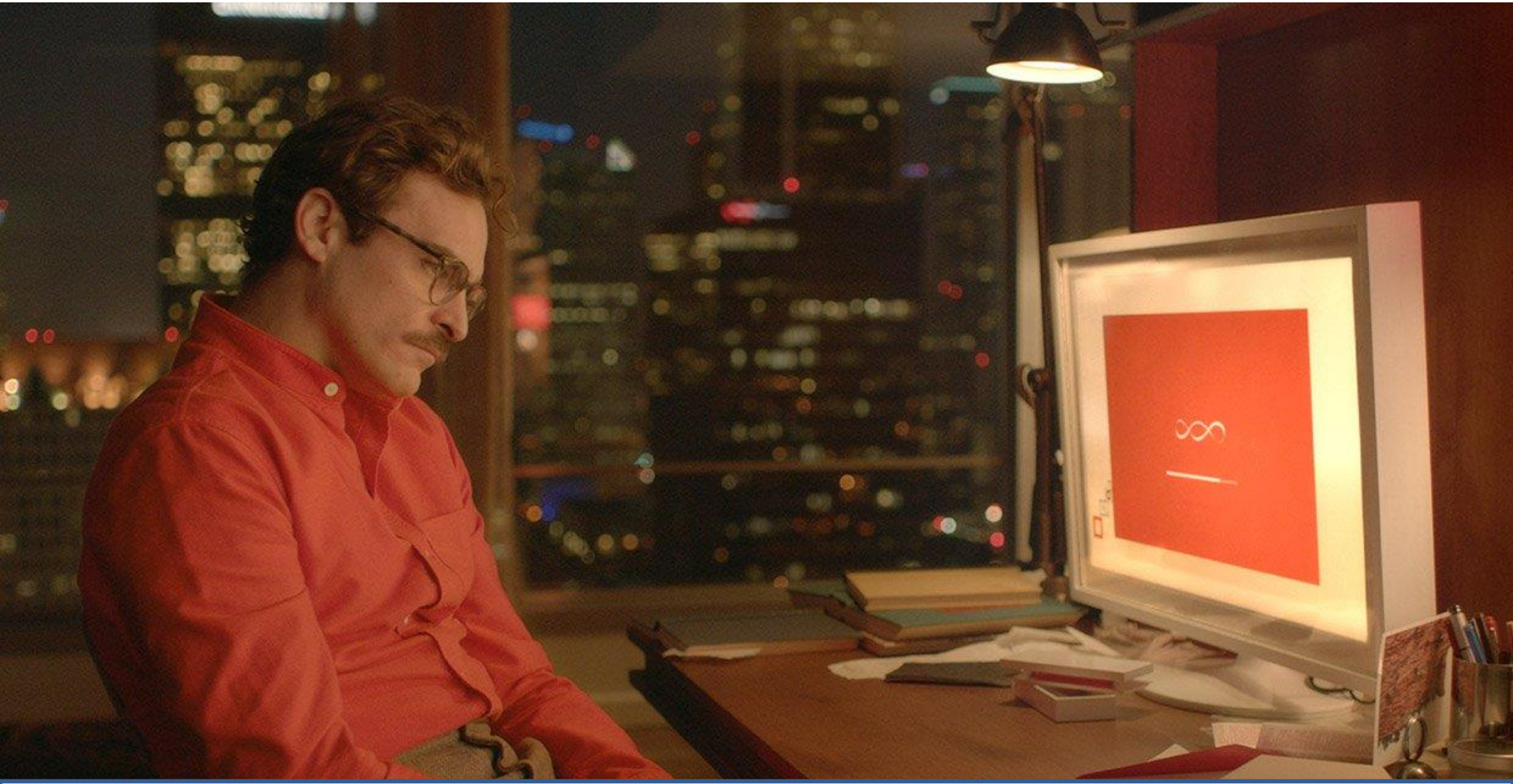
از دیگر نمونه ها ایجاد چت‌بات که «مرده‌بات» یا deadbotsنام دارد به یاری هوش مصنوعی، مسائلی را به لحاظ اخلاقی ایجاد می کند . در قالب چت بات مذکور افراد به ظاهر می توانند با فرد درگذشته پیام متنی رد و بدل کنند.

آیا سوال اینجا که آیا استفاده از این چت‌بات‌هایی که مکالمه انسان‌ها را تقلید می‌کند، کار اخلاقی است؟

در این ارتباط نحوه محافظت از حقوق اساسی مردگان –مانند حریم خصوصی و داده‌های شخصی آنها- چه می شود، زیرا توسعه یک روبات مرده که شخصیت یک فرد را تقلید می‌کند، نیاز به مقادیر زیادی اطلاعات شخصی مانند داده‌های شبکه اجتماعی او دارد. اگر قبول داریم که استفاده از داده‌های شخصی بدون رضایت در زمان زنده بودن غیراخلاقی است، چرا باید این کار بعد از مرگ اخلاقی باشد؟ به همین دلیل کاملا منطقی به نظر می‌رسد که رضایت طرف دوم نیز نیاز است. (Suárez-Gonzalo,2023)

از سویی یکسری اطلاعات شخصی در این میان تبادل می شود که هرگونه دستیابی به آن با احتمال سوء استفاده می تواند آسیب زا از جمله به حریم خصوصی دو طرف باشد.

تأثیرات روانی منفی هوش مصنوعی



وابستگی به هوش مصنوعی و تأثیرات روانی آن در شرایطی همچون ارتباط گریزی و.... و ایجاد ارتباط های عاطفی با هوش مصنوعی، از دیگر خطرات احتمالی در خصوص این فناوری است.

محافظت از خانواده ها در برابر کلاهبرداریهای هوش مصنوعی

توصیه کارشناسان به خانواده ها، تا حد امکان خصوصی کردن صفحات رسانه های اجتماعی است. چراکه از محتواهای آنها ممکن است در مسیر کلاهبرداری بهره گرفته شود

برخی کلاهبرداریها با روشهای باورپذیری همچون کلاهبرداری با ابزار تقلید صدای اعضای خانواده رخ می دهد.

استفاده از ۱۰ دقیقه نمونه صوتی با کمک هوش مصنوعی برای ساخت پیام جعلی صوتی برای دریافت پول و... کافی است.

تمام اعضای خانواده لازم است یک کلمه امنیتی مختص به خود داشته باشند تا در شرایط خاص همچون احتمال ربوده شدن و... بتوانند از همان کلمه اسفاده کنند در صورت وقوع جرایم باید با پلیس تماس گرفته شود

همچنین تماس با فردی که حس می شود ربوده شده، حتماً به طور مستقیم صورت گیرد.

لزوم آشنا کردن خانواده با نحوه مقابله با خطرات هوش مصنوعی و کلاهبرداریهای احتمالی

نگرانی از افزایش حملات سایبری، هک و فیشینگ

اهمیت هوش مصنوعی و حریم خصوصی داده ها در افزایش تعداد نقض اطلاعات و حملات سایبری که در سال های اخیر رخ داده است مشهود است. این حوادث نیاز به اقدامات حفاظتی بهتر از داده ها و مقررات سختگیرانه تر برای حفاظت از اطلاعات شخصی را برجسته کرده است. افزایش هوش مصنوعی همچنین نگرانی هایی را در مورد نحوه جمع آوری، استفاده و ذخیره داده های شخصی و خطرات احتمالی مرتبط با برنامه های کاربردی هوش مصنوعی ایجاد کرده است. بنابراین، درک رابطه پیچیده بین هوش مصنوعی و حریم خصوصی داده ها برای توسعه استراتژی ها و سیاست های موثر برای رفع این نگرانی ها بسیار مهم است.

از جمله این حملات، ایمیل‌های «فیشینگ هدفمند» ایجاد شده توسط هوش مصنوعی یا بدافزارهای مبتنی بر این فناوری است که سازگار می‌شوند و تکامل می‌یابند. «فیشینگ هدفمند» یک تلاش هدفمند برای سرقت اطلاعات حساس از یک قربانی خاص است. این نوع «فیشینگ» اغلب برای دسترسی به حساب های مالی و شخصی قربانی انجام می‌شود. کارشناسان اخیرا بدافزارهای جهش یافته را مشاهده کرده‌اند.

تلاش برای آموزش مفهوم حریم خصوصی حتی به کودکان

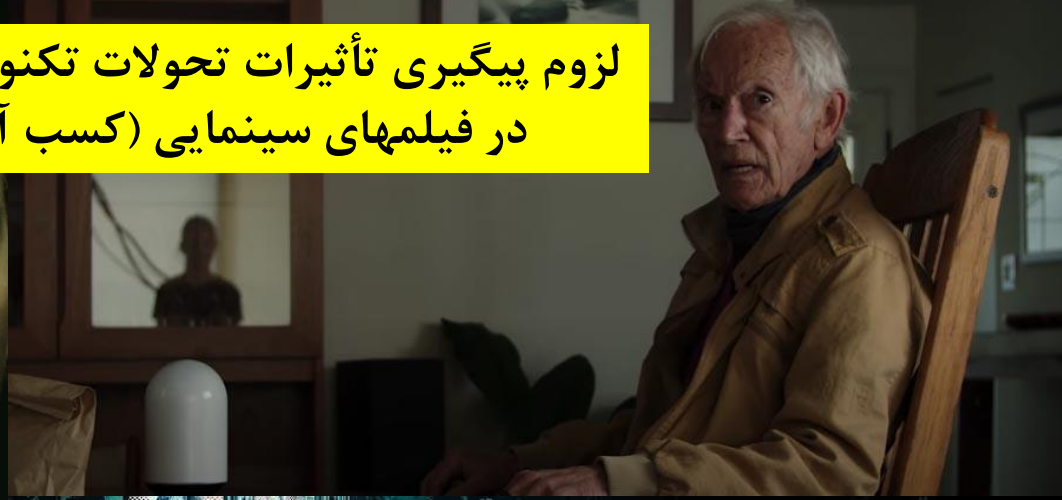
در انیمیشن غارنشینان ۲ به بحث حریم خصوصی نیز اشاراتی دارد، شخصیتها پیش از رسیدن به عصر جدید و آشنایی با خانواده بهتر زاده ها، به صورت تپه ای و در مجاورت هم می خوابند و پسر وقتی به ایپ می گوید در آینده مستقل زندگی کنند، به بحث حریم خصوصی اشاره می کند و می گوید حریم خصوصی یعنی اینکه در آینده تصمیم بگیریم اینکه آیا بوی پا وجود داشته باشد یا نه؟

این دیالوگ در حالی جاری است که در بکگراند تصویر، پدر ایپ شاهد دیالوگهای خصوصی آنهاست.

در جایی در همین انیمیشن وقتی در منزل بهترزاده ها هرکس اتاقی مخصوص به خود می یابد، مجدداً به حفظ حریم خصوصی با اتاقی مستقل اشاره می شود.

ما پیش از اینکه تلاشی برای حفظ حقوق خود داشته باشیم باید حقوق مان را بشناسیم، از جمله حق حفظ حریم خصوصی

لزوم پیگیری تأثیرات تحولات تکنولوژیکی در حریم خصوصی در فیلمهای سینمایی (کسب آمادگی های احتمالی)

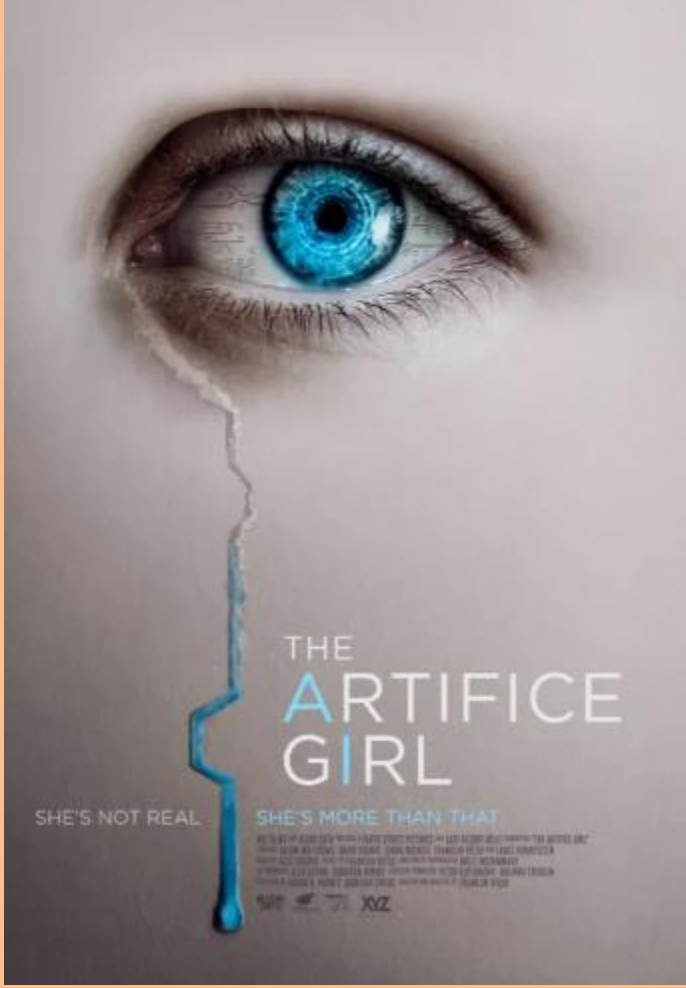


فیلم دختر مصنوعی
The Artifice Girl
تکامل اَبَرهوش‌ها

لیست بلند بالایی از فیلمهای مرتبط با هوش مصنوعی می توان ارائه کرد که یکی از آنها دختر مصنوعی است.
فیلم دختر مصنوعی در سه پرده روایت می‌شود و داستان‌اش را در گذر زمان و تنها با سه کارکتر انسان و یک هوش مصنوعی تعریف می‌کند.

در بخش اول گرت با یکسری شبیه‌سازی‌ها دختری به‌نام گیلاس را می‌سازد، او به کمک کودکان می‌آید تا از آن‌ها در دنیای خشن انسان‌ها محافظت کند. گیلاس با شکارچیان بچه‌ها صحبت می‌کند، پیام می‌دهد و سپس اطلاعات آن‌ها را در اختیار گرت قرار می‌دهد. آدم‌های بد این ماجرا قرار است که بوسیله‌ی هوش مصنوعی گول بخورند و مغلوب این فناوری جدید شوند. در پرده دوم گریت مجبور به همکاری با گروهی ویژه با نامهای دینا و آموس می شود و در این پرده به تدریج فاش می شود که گیلاس دارای احساسات بوده و لذت و درد و... درد می کند. در پرده آخر نیز در پرده‌ی سوم دینا و آموس مرده‌اند و گرت نیز که پیر و فرتوت شده با صندلی چرخداراش به خانه می‌رود، خانه‌ای که سرد و تلخ است و کسی به‌جز گیلاس در آنجا نیست. دختر مصنوعی بعد از سال‌ها به بالاترین نقطه‌ی تکامل ابرهوش‌ها رسیده لحظه‌اش که انسان در حسرت دیدن‌اش است. گیلاس در کالبد یک دختر نوجوان به‌همراه سیم‌هایی که بهش متصل است زندگی می‌کند. او در پلان‌های پایانی فیلم پابه‌پای انسان می‌آید، جسم دارد، حرف می‌زند، از احساسات و عاطفه برخوردار است و همانند انسان‌ها از قوه‌ی ادراک‌اش استفاده می‌کند و بعد از مرگ گرت نیز کاملا شبیه آدم‌ها شده و بدون سیم‌های کنترل‌کننده همانند انسان‌ها می‌رقصد.
در این پرده، نگاهی نقد گونه به استعمار انسان در ارتباط با هوش مصنوعی وجود دارد که در نهایت نیز گرت با آخرین به روزرسانی به گیلاس اختیارات کامل می دهد و او را در انتخاب آزاد می گذارد.

نقض حریم خصوصی در بخشهایی از این فیلم



سرک کشیدن دینا در ایمیلهای خصوصی دینا و اطلاع از بیماری وی با خواندن ایمیلهای او و پزشکش، که در نهایت دینا از او می خواهد که رازش بین او و گیلاس بماند

جمع بندی و نتیجه گیری

هوش مصنوعی به مثابه یک چاقو یا شمشیر دو لبه همچون بسیاری از حوزه های دیگر، در حوزه حریم خصوصی نیز می تواند به شکلی موثر یا مخرب عمل کند به این معنی که هم می تواند به حفظ حریم خصوصی یا نقض آن کمک کند.

این اثرگذاری کلیه ابعاد حریم خصوصی را اعم از حریم خصوصی فیزیکی، روانی، دیجیتالی، داده ای، مالی و.... و از همه مهمتر حریم خصوصی ذهن را شامل شود.

در این مسیر لازم است ضمن شناخت کامل حریم خصوصی و ابعاد آن، اطلاع از قوانین حمایت گر از آن، با هوش مصنوعی و تأثیرات آن بر حریم خصوصی آشنا شد. ضمن شناسایی راههای تأثیرگذاری منفی هوش مصنوعی بر این حریم، از بروز برخی مشکلات، چالشها، کلاهبرداریها و... جلوگیری کرد. بخشی از این اقدامات به یاری تلاشهای فراد در عدم اشتراک گذاری و یا افشای اطلاعات مهم و حساس مربوط و بخشی نیز به مسئولیتهای اجتماعی و اخلاقی شرکتها و بخشی دیگر نیز به اقدامات دولتها در تدوین قوانین و.... نهفته است.

در بحث تدوین و تصویب قوانین مرتبط با هوش مصنوعی ضمن بهره گیری از تجارب دیگر کشورها در این حوزه، لازم است قوانینی تصویب کرد که در کنار حفظ حریم خصوصی افراد، مانع حرکتهای نوآورانه و جدید در حوزه هوش مصنوعی نشود. همچنین در روند این تصویب قوانین باید به سرعت توسعه و تحول هوش مصنوعی به عنوان یک ماشین یادگیرنده توجه شود. همچنین در تصویب قوانین به رعایت حقوق و ارزشهای اساسی افراد از جمله حریم خصوصی آنها، تقویت سرمایه گذاری و نوآوری در حوزه هوش مصنوعی، لحاظ ملاحظات حاکمیتی و حق افراد در تصمیم گیری برای انصراف یا اجازه بهره گیری از داده ها و اطلاعاتشان توسط شرکتها و هوش مصنوعی و نیز پاسخگو بودن شرکتها در بهره گیری از داده های افراد عنایت لازم داشت.

همچنین ارتقای آگاهی در خصوص هوش مصنوعی و نحوه بهره گیری آن از اطلاعات و آنچه رخ خواهد داد ضروری بوده و باید شناخت کافی در این خصوص به خانواده داده شود تا از تبعات منفی احتمالی هوش مصنوعی در حوزه های فیشینگ، دیپ فیکها و اخبار و تصاویرجعلی، انواع سوء استفاده های احتمالی و.... در امان بمانند.

با تشکر از صبر و حوصله شما

salimi1356@yahoo.com

برخی از منابع و مآخذ:

Oaic (n.d.), What is privacy?,https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy

Fahad, Engr (December 29, 2020), Wearable Technology Examples, Advantages, and Types,https://www.electroniclinic.com/wearable-technology-examples-advantages-and-types/

Harris, Jeremie (May 20, 2021), The (Evolving) World of AI Privacy and Data Security, https://towardsdatascience.com/the-evolving-world-of-ai-privacy-and-data-security-8e1bf3b5cdd6

Tirmizi ,Ali Mannan (October 27, 2022) , AI and Data Privacy: Where Do They Intersect?, https://www.dataversity.net/ai-and-data-privacy-where-do-they-intersect/

Sanders ,Laura (February 11, 2021), New technology can get inside your head. Are you ready?, https://www.snexplores.org/article/brain-implant-tech-mental-data-privacy-ethics

J Mackenzie, Ruairi (August 31, 2021), Privacy in the Brain: The Ethics of Neurotechnology, https://www.technologynetworks.com/neuroscience/articles/privacy-in-the-brain-the-ethics-of-neurotechnology-353075

Antonio Lanz, Jose (Jun 10, 2023), Meet PassGPT, the AI Trained on Millions of Leaked Passwords, https://decrypt.co/144004/meet-passgpt-ai-trained-millions-leaked-passwords

Suárez-Gonzalo, Sara(January 17, 2023), 'Deadbots' Can Speak for You After Your Death. Is that Ethical?, https://www.europeanfinancialreview.com/deadbots-can-speak-for-you-after-your-death-is-that-ethical/

Chesini ,Fabio (November 29, 2020), Mastering the 3 Privacy Dimensions, https://blogs.gartner.com/fabio-chesini/2020/11/29/mastering-the-3-privacy-dimensions/

Pearce ,Guy (28 May 2021), Beware the Privacy Violations in Artificial Intelligence Applications, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

ThinkML Team (30 MAR 2023), AI and Data Privacy: Unraveling the Complex Relationship, https://thinkml.ai/ai-and-data-privacy/

Mal, Reejhu (February 5, 2023), The Future is Now: The Rise of AI and its Shaping of Tomorrow , https://moderndiplomacy.eu/2023/02/05/the-future-is-now-the-rise-of-ai-and-its-shaping-of-tomorrow/

VARINDIA (2022-07-01), Artificial intelligence is a double-edged sword, https://varindia.com/news/artificial-intelligence-is-a-doubleedged-sword

Park,Sungjin & Kim,Sangkyun (2022), Identifying World Types to Deliver Gameful Experiences for Sustainable Learning in the Metaverse , https://mdpi-res.com/d_attachment/sustainability/sustainability-14-01361/article_deploy/sustainability-14-01361-v2.pdf

Pearlman,Kavya ,Visner,Sam , Magnano ,Marco & Cameron,Ryan (n.d.), Securing the Metaverse - Virtual Worlds Need REAL Governance https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=52969&PortalId=0&TabId=105

Basu,Tanya ,December 16, 2021, The metaverse has a groping problem already https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/

Lee ,Lik-Hang , Braud ,Tristan , Zhou ,Pengyuan & Wang Lin, Addison (October 2021), All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda, https://www.researchgate.net/publication/355172308_All_One_Needs_to_Know_about_Metaverse_A_Complete_Survey_on_Technological_Singularity_Virtual_Ecosystem_and_Research_Agenda

سلیمی ، مریم، سلیمی ، سمیه (۱۳۹۷)، کاربرد و مزایای آموزشی و ارتباطی گرافیک نوول و کمیک ژورنالیسم،
https://qjmn.farhang.gov.ir/article_68999_069c10f18aa17f50c529b7cfc1d4a0ee.pdf

شاهرخ ، علی (۱تیر ۱۴۰۲)، تشخیص ایدئولوژی سیاسی افراد با تحلیل چهره آن‌ها توسط هوش مصنوعی ؛ قابلیتی ایده‌آل برای حکومت‌های خودکامه!، سایت زندگی با تکنولوژی،
https://techrato.com/2023/06/22/identifying-ideology-analyzing-faces-ai/

فرادرس (اردیبهشت ۱۴۰۰)، بینایی کامپیوتر چیست؟ — به زبان ساده،
https://blog.faradars.org/introduction-to-computer-vision/

امید محمدیان پهلوان (۱۴۰۱)، قوانین جهانی در عصر هوش مصنوعی، چه‌طور از حریم شخصی دفاع می‌کند؟،
https://hamshahritraining.ir/4075

قانون جرائم رایانه ای (۱۳۸۸/۰۳/۰۵)،
https://rc.majlis.ir/fa/law/show/135717

طرح حمایت و حفاظت از داده و اطلاعات شخصی (۱۳۹۹/۰۷/۱۲)،
https://rc.majlis.ir/fa/legal_draft/show/1675111

اعلامیه حقوق بشر (۱۰ دسامبر ۱۹۴۸)، https://iran.un.org/sites/default/files/2019-11/UniversalDeclarationHR_0.pdf

فرادید (خرداد ۱۴۰۲)، هوش مصنوعی چگونه حریم خصوصی و زندگی مردم را تهدید می کند؟، https://faradeed.ir/fa/tiny/news-135709

نورانی زاده، محمدصالح (۱۴۰۲/۰۳/۲۰)، نورالینک (Neuralink) چیست؟ پروژه‌ای بهتر از متاورس به نظر ایلان ماسک!، https://bit24.cash/blog/neuralink/

همشهری (سه‌شنبه ۲۰ دی ۱۴۰۱)، احضار ارواح به کمک هوش مصنوعی | می‌توانید با عزیزان درگذشته حرف بزنید، hamshahrionline.ir/x8fCM