فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره چهارم | زمستان ۱۴۰۳ | شماره پیاپی ۱۲
وبگاه مجله : https://sanad.iau.ir/journal/cyberlaw
دانشگاه آزاد اسلامی واحد مرانه
ISSN: 2821-126X

An Introduction to the Challenges of Artificial Intelligence Technology in the Realm of Privacy

Abbas Mirshekari
Assistant Professor, Department of Private and Islamic Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran (Corresponding Author)
Email: mirshekariabbas1@ut.ac.ir
Fatemeh Sabetghadam
Master's degree in Private Law, University of Isfahan, Isfahan, Iran
Morteza Asgharnia
PhD in Public Law, University of Tehran, Tehran, Iran

DOI: 10.71488/cyberlaw.2025.1123072
Keywords:
Technology, Artificial Intelligence, Data Protection, Privacy, Regulatory Requirements

Abstract

Artificial intelligence technology, as the foundation of the fifth industrial revolution, with its development and increasing influence in all aspects of the political, economic, social and cultural life of citizens, by creating significant changes in the provision of solutions and services, in addition to creating changes in the quality of life of individuals, has revealed many challenges at different levels for governments and citizens. Among the most important of these emerging challenges mentions can be made of the challenges of artificial intelligence technology in the realm of privacy. Although in the last few years some legal systems have somehow addressed the category of privacy in the relevant laws and regulations, however, the challenges of artificial intelligence technology in the realm of privacy, considering its importance and special complexities, require appropriate legal and legislative measures in order to protect the privacy of people. Therefore, through a library method, the present article has made an to point out the history of artificial intelligence technology and its types, by examining the history of legislation and regulations related to the subject of privacy in the European Union and some leading countries in this field. In this regard, the identified challenges are enumerated and proposed legal solutions in the field of legislation to protect the privacy of individuals in the field of applying artificial intelligence in Iran's legal system are presented.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره چهارم | زمستان ۱۴۰۳ | شماره پیاپی ۱۲

درآمدی بر چالشهای فناوری هوش مصنوعی در حوزه حریم خصوصی

عباس میرشکاری

استادیار گروه حقوق خصوصی و اسلامی دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران (نویسنده مسئول)

پست الکترونیک: mirshekariabbas1@ut.ac.ir

فاطمه ثابت قدم

دانش آموخته کارشناسی ارشد حقوق خصوصی دانشگاه اصفهان، اصفهان، ایران

مرتضی اصغرنیا

دکتری حقوق عمومی دانشگاه تهران، تهران، ایران

تاریخ دریافت : تاریخ پذیرش:

چکیده

فناوری هوش مصنوعی، به عنوان زیربنای انقلاب صنعتی پنجم ، با توسعه و تأثیرگذاری روز افزون در کلیه شئون مختلف حیات سیاسی، اقتصادی، اجتماعی و فرهنگی شهروندان، با ایجاد تحولات چشمگیر در ارائه راهکارها و خدمات، علاوه بر ایجاد تغییر در کیفیت زندگی اشخاص، چالش های متعددی را در سطوح گوناگون پیش روی دولت هاو شهروندان نمایان ساخته است. از جمله مهمترین این چالشهای نوظهور میتوان به چالشهای فناوری هوش مصنوعی در حوزه حریم خصوصی اشاره نمود. اگر چه در چند سال اخیر برخی از نظام های حقوقی به نحوی به مقوله حریم خصوصی در قوانین و مقررات موضوعه پرداخته اند، با این حال چالش های فناوری هوش مصنوعی در این حوزه با توجه اهمیت و پیچیدگی های خاص آن، نیازمند اقدام حقوقی و تقنینی متناسب به منظور صیانت از حریم خصوصی اشخاص می باشد. لذا، در مقاله حاضر که به روش کتابخانه ای تنظیم شده، تلاش گردیده است تا ضمن اشاره به تاریخچه فناوری هوش مصنوعی و انواع آن، با بررسی سابقه تقنینی و مقررات گذاری در ارتباط با حوزه حریم خصوصی در اتحادیه اروپا و برخی کشورهای پیشرو در این زمینه، چالش های شناسایی شده احصاء گردیده و راهکارهای حقوقی پیشنهادی در حوزه قانونگذاری برای صیانت از حریم خصوصی اشخاص در زمینه به کارگیری هوش مصنوعی در نظام حقوقی ایران ارائه گردد.

واژگان کلیدی: فناوری، هوش مصنوعی، حفاظت از داده، حریم خصوصی، بایسته های تقنین

مقدمه

تمایل به ایجاد هوش مصنوعی را می‌توان در فرهنگ عامه، علی‌الخصوص در فرهنگ اروپا جست و جو نمود. پاراسلسوس[1] پزشک و کیمیاگر سوئیسی اظهار می‌داشت که «ما مانند خدایان خواهیم بود و بزرگترین معجزه خداوند که خلقت انسان است را تکرار خواهیم کرد» (khemani,2020:34). این موضوع به مرور زمان مورد استقبال قرار گرفت و در ادبیات و فلسفه رسوخ کرد؛ تا جایی که برخی سخن معروف رنه دکارت: «من می‌اندیشم پس هستم»[2]را هسته‌ی اصلی شکل‌گیری مباحث در خصوص ماهیت هوش مصنوعی به شمار می‌آورند (Khemani,2020:33). توانایی موجودات مصنوعی برای حل مشکلات پیچیده، به عنوان هوش مصنوعی شناخته می‌شود. هوش مصنوعی، به عنوان شاخه‌ای از علوم کامپیوتر که شامل توسعه ماشین‌های هوشمند با قابلیت تقلید از هوش انسانی است، در سال‌های اخیر پیشرفت‌های چشمگیری داشته است (Mujoo, et al, 2022:4598). این زمینه‌ی رو به رشد که اکنون با دارا بودن ANN[3] که از گروهی از پردازنده‌ها به نام نورون ساخته شده و شبیه‌ساز رشته‌های عصبی مغز انسان می‌باشد (Ahmed, et al, 2022: 3366)، آماده است تا با تقویت نحوه‌ی تجزیه و تحلیل اطلاعات و تصمیم-گیری، جنبه‌های مختلف جوامع بشری را متحول کند. این فناوری، نه تنها صنایعی مانند مراقبت‌های بهداشتی و مالی را متحول نموده، بلکه این ظرفیت را داراست که زندگی روزمره انسان‌ها را نیز تحت تأثیر قرار دهد. هوش مصنوعی با استفاده از فناوری های پیشرفته مانند: الگوریتم‌های یادگیری ماشینی، امکان پردازش سریع، تحلیل دقیق و مدیریت مقرون‌به‌صرفه، حجم عظیمی از داده‌های تولید شده امروزی را فراهم می‌نماید (Liang, et al, 2022: 125). ادغام فناوری‌های هوش مصنوعی در همه بخش‌ها مزایای متعددی نظیر: روش‌های تشخیص و درمان پیشرفته در مراقبت‌های بهداشتی، پیش‌بینی‌های مالی دقیق‌تر، سیستم‌های حمل‌ونقل کارآمد و توصیه‌های سرگرمی شخصی‌شده را به همراه داشته است (Hidayat, Satwiko, 2021: 292). هوش مصنوعی، ثابت کرده است که از نظر بهبود کارآیی، دقت و تصمیم‌گیری، تغییر دهنده بازی است و این توانایی بالقوه را دارد که با خودکارسازی وظایف تکراری، بهینه‌سازی تخصیص منابع و فعال کردن رویکردهای نوین مبتنی بر بهره‌برداری از داده‌ها، صنایع را متحول کرده و کارها را به گونه‌ای نظام‌مندتر و روشمندتر از انسان‌ها انجام دهد. از آنجایی که در حال حاضر، هوش مصنوعی به دلیل فواید بسیار زیاد مورد استقبال بخش زیادی از شهروندان قرار گرفته و از آنجا که با دسترسی غیرمجاز به اطلاعات اشخاص و بهره‌گیری ناصحیح و غیرقانونی از آن، امکان نقض حریم خصوصی اشخاص و ورود زیان مادی و معنوی به آن‌ها فراهم می‌گردد، در مقاله حاضر به چالش‌های فناوری هوش مصنوعی در حوزه حریم خصوصی ارتباطاتی و داده ای و وضعیت قانونگذاری کشورها در این زمینه پرداخته شود. از این رو، در مقاله حاضر ابتدا در بند اول و دوم به تاریخچه فناوری هوش مصنوعی و انواع آن اشاره گردیده و سپس با بررسی سابقه تقنینی و مقررات گذاری در ارتباط با حوزه حریم خصوصی در اتحادیه اروپا و برخی کشورهای پیشرو در این زمینه، چالش‌های شناسایی شده احصاء گردیده و راهکارهای حقوقی پیشنهادی در حوزه قانونگذاری به منظور صیانت از حریم خصوصی اشخاص در بستر به کارگیری هوش مصنوعی در نظام حقوقی ایران ارائه می‌گردد. در ادامه خواهیم دید که چالش‌های ایجاد شده در زمینه حریم خصوصی ارتباطاتی و داده ای کدام‌اند؟ با بررسی قوانین تصویب شده در کشورهای خارجی بررسی خواهیم نمود که آیا در کشور ما نیز در این زمینه قانون‌گذاری خاصی صورت گرفته یا صرفاً به استناد قوانین عام می‌بایست محدودیتی برای هوش مصنوعی در حوزه رعایت حریم خصوصی اشخاص قائل شد؟ و شخصی که حق بر حریم خصوصی ارتباطاتی و داده‌ای وی نقض شده به استناد چه قوانینی می‌تواند دادخواهی نماید؟

[1] Paracelsus
[2] I think, therefore, I am
[3] Artificial Neural Networks

۱. پیشینه تحقیق

به علت همه‌گیر بودن هوش مصنوعی و مسائل مرتبط با آن، در سال های اخیر مطالعات و پژوهش های ارزشمند داخلی و خارجی در این زمینه صورت گرفته است که حقوقدانان نیز از این قافله جا نمانده‌اند و نظرات، ایده‌ها و دیدگاه‌های حقوقی خود را در خصوص این موضوع در قالب مقاله بیان نموده‌اند که در ادامه به بیان برخی از آن‌ها بر اساس تاریخ انتشار خواهیم پرداخت.در پژوهش‌های داخلی چند مقاله در خصوص هوش مصنوعی و مسائل مرتبط با آن وجود دارد که به بیان برخی از آن‌ها می‌پردازیم:

۱- مصطفی السان و سوور دهستانی در زمستان ۱۴۰۱ در مقاله خود با موضوع «جنبه‌های حقوقی جعل عمیق» ویژگی‌ها و چالش‌هایی که جعل عمیق ممکن است ایجاد کند را بررسی نموده و به استفاده از مفاد عهدنامه‌های مالکیت فکری برای مدیریت جعل عمیق پرداخته‌اند که وجه تمایز آن با پژوهش حاضر بررسی مشکلات منتج از اعمال جعل عمیق و توسل به عهدنامه‌های مالکیت فکری برای کاهش آن است.

۲- حانیه ذاکری نیا در تابستان ۱۴۰۲ در مقاله خود با عنوان «ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیهٔ اروپا» به بررسی مبانی مسئولیت مدنی ناشی از هوش مصنوعی در ایران و برخی از کشورهای خارجی پرداخته است که وجه تمایز آن با پژوهش حاضر نیز در همین بررسی مبانی مسئولیت مدنی است و به قوانین هوش مصنوعی و چالش‌های مربوط به حوزه حریم خصوصی آن اشاره‌ای ندارد.

۳- فرشته بنافی نیز در زمستان ۱۴۰۲ در مقاله خود با موضوع «حفاظت از حقّ حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی» به بررسی حافظت از حریم خصوصی در مقابل هوش مصنوعی نظامی از منظر حقوق بین‌الملل عمومی پرداخته است و خلأهای قانونی و سیاسی موجود در حقوق بین‌الملل بشردوستانه و حقوق بشر بین‌المللی جهت صیانت از حریم خصوصی در هوش مصنوعی نظامی برای طرف‌های متخاصم را احصاء نموده است که وجه افتراق کار ایشان با پژوهش حاضر نیز در همین موضوع و پرداختن به مقوله حق بر حریم خصوصی از منظر حقوق جنگ و حقوق بین الملل مخاصمات مسلحانه است.

در مقالات دیگر که همگی ارزشمند و منشا اثر هستند به سایر جنبه‌های مرتبط با هوش مصنوعی کم و بیش اشاره شده است که ارتباط جزئی با پژوهش حاضر دارد. در پژوهش‌های خارجی نیز چند مقاله در خصوص هوش مصنوعی و حریم خصوصی و مسائل مرتبط با آن نگارش یافته است که به بیان برخی از مهمترین آن‌ها می‌پردازیم:

۱- Danielle Citron و Robert Chesney در سال ۲۰۱۹ در مقاله Deep Fakes: A Looming Challenge for Privacy Democracy, and National Security به بررسی آثار جعل عمیق در حریم خصوصی، دموکراسی و امنیت ملی می‌پردازند با این وجه تمایز با پژوهش حاضر که بررسی قانونی در این زمینه انجام نداده و چالش‌های هوش مصنوعی را بیان ننموده‌اند.

۲- David Elliott و Eldon Soifer در سال ۲۰۲۲ در مقاله AI Technologies, Privacy, and Security به بررسی آثار فناوری‌های هوش مصنوعی در حریم خصوصی و امنیت پرداخته‌اند و در این پژوهش نیز بررسی قوانین و مقررات مورد نیاز در این زمینه انجام نشده است.

۳- Philipp Hacker نیز، در سال ۲۰۲۳ در مقاله خود با عنوان AI Regulation in Europe: From the AI Act to Future Regulatory Challenges به بررسی قانون هوش مصنوعی در اروپا که در زمان انتشار این مقاله در حال تصویب بود، پرداخته است و در خصوص چالش‌ها و مقررات هوش مصنوعی سایر کشورها سخنی به میان نیاورده است.

۲. تاریخچه فناوری هوش مصنوعی

در زمان کنونی، روزی نیست که صحبتی در ارتباط با هوش مصنوعی در محافل آکادمیک و غیرآکادمیک صورت نگیرد؛ البته به نظر می‌رسد که در این مباحث، موضوع هوش مصنوعی، یک اصطلاح کلی برای صحبت از یک فناوری جدید بوده و هیچ وضوحی ندارد. چنان‌که اتومات‌هایی[1] که نیاز به هوش مصنوعی نداشته و مقدمه‌ای برای ایجاد این هوش بوده‌اند را نیز دربرمی‌گیرد. اتومات از واژه‌ی یونانی «αὐτόματα» به معنای "خودکار" گرفته شده و به دستگاهی که به صورت خودکار دنباله‌ای از عملیات از پیش تعیین شده را ادامه می‌دهد، گفته می‌شود (Khairuddin, et al ,2019:1). اولین نمونه-های ساخت افراد مصنوعی مشابه انسان‌ها به صورت اتومات را می‌توان ۸۵۰ سال قبل از میلاد دانست؛ جایی که خدایان یونانی صحبت، اشاره و پیشگویی می‌کردند و پلک می‌زدند (McCorduck,2004:6). این هنر، سال‌ها در اختیار یونانیان بود تا ۷۵۰ سال بعد از میلاد مسیح که علم ریاضیات در جهان عرب شکوفا شد. علم اعراب در میان قرن هشتم تا دوازدهم وجوه مشترک بسیاری با علوم مدرن داشت؛ برخلاف یونانیان که علمشان محدود به افراد خاصی شده بود، علم آن‌ها به تدریج بین‌المللی شد و توسعه دانش با سرعت زیادی در مراکز علمی شدت گرفت. یکی از نمونه‌های ارزشمند آن، به نام زائرجه[2]را می‌توان نتیجه‌ی کار گروهی از منجمان دانست که آن را از اولین تلاش‌های اعراب برای ایجاد و به کارگیری هوش مصنوعی به شمار می‌آورند. این ایده چنان مورد استقبال قرار گرفت که دانشمندان معتقد بودند این ایده مانند نوزاد تازه متولد شده، آغاز فرایندی بی‌انتها بوده است (Kunze,2020:2). در اروپا اولین تلاش برای ساخت اتومات مدرن را می-توان ساخت قوی نقره‌ای[3] توسط جواهرساز انگلیسی، جیمز کاکس[4] در سال ۱۷۷۳ میلادی دانست که اکنون در موزه بوز[5] در لندن نگهداری می‌شود (Smith,2016:361). با این حال اصطلاح هوش مصنوعی به معنای واقعی به جان مک‌کارتی[6] نسبت داده می‌شود که به همراه ماروین مینسکی[7]، ناتانائیل روچستر[8] و کلود شانون[9] در سال ۱۹۵۶ میلادی یک کنفرانس تابستانی را در کالج دارتموث[10] ترتیب دادند. با دعوت این چهار نفر، تعدادی از دانشمندانِ ریاضی‌دان و روانشناس و مهندسین برق، با این عقیده که آنچه را که ما تفکر می‌نامیم در واقع می‌تواند خارج از جمجمه‌ی انسان نیز اتفاق بیفتد، می-توان آن را به روشی رسمی و علمی درک کرد و بهترین ابزار غیرانسانی برای انجام آن کامپیوتر دیجیتال است، گرد هم آمدند. این کنفرانس محل تلاقی چندین جریان فکری مختلف قرن بیستم بود که از علم ریاضیات، آمار، روانشناسی، مهندسی، زیست‌شناسی، زبان‌شناسی و رشته‌های نوظهور علم مدیریت سرچشمه گرفته بودند (Moor,2006:87؛ Kline,2011:5-16). البته، برخی از دانشمندان حاضر گمان می‌کردند عبارت "هوش مصنوعی" به ذهن اشخاص، این مسئله که همه چیز مصنوعی و ساختگی است و هیچ چیز واقعی وجود ندارد را متبادر می‌کند، به همین دلیل فعالیت‌های خود در این زمینه را با نام پردازش اطلاعات پیچیده منتشر نمودند؛ اما هوش مصنوعی عبارتی بود که ماندگار شد. طراحی برنامه-

[1] Automata
[2] Zairja
[3] Silver Swan
[4] James Cox
[5] Bowes Museum
[6] John McCarthy
[7] Marvin Minsky
[8] Nathaniel Rochester
[9] Claude Shannon
[10] Dartmouth College

های کامپیوتری برای رفتار هوشمندانه بسیار سخت‌تر از چیزی بود که در سال ۱۹۵۶ میلادی تصور می‌شد و پس از کنفرانس مذکور پیشرفت‌های کمی حاصل گردید و اینطور نبود که چیزی بسیار چشم‌گیر در مدت کوتاهی انجام شود و حتی ناامیدی مک‌کارتی هم از جمله‌ی: «فاصله بین آنچه که امیدوار بودم انجام دهم و آنچه انجام دادیم، بسیار بزرگ بود» کاملاً قابل تشخیص بود (Mccorduck,2004:113-118). منبع اصلی تأمین حمایت مالی این پروژه طی دهه‌های ششم و هفتم قرن بیستم میلادی، آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی[۱]، آژانس تحقیق و توسعه وزارت دفاع ایالات متحده آمریکا که مسئولیت توسعه فناوری‌های نوظهور را برای استفاده‌ی ارتش به عهده داشت، بود. این آژانس برای گسترش مرزهای فناوری و علم، اغلب فراتر از نیازهای فوری نظامی ایالات متحده آمریکا، پروژه‌های تحقیق و توسعه را تدوین و اجرا می‌کند (DARPA.mil). پس از آن، دانشمندان زیادی شیفته‌ی هوش مصنوعی شده و معتقد بودند که این موضوع از پرمخاطب‌ترین موضوعات در آینده خواهد بود (Mccorduck,2004:131). در این حین، تحقیقات زیادی در خصوص این موضوع شکل گرفت که منجر به ایجاد پیشرفت‌های شگرف نظری و کاربردی در زمینه‌ی هوش مصنوعی شد. اولین ثمره‌ی این تلاش‌ها در سال ۱۹۶۵ میلادی در دانشگاه استنفورد به شکل یک سیستم خبره[۲] که با استدلال علمی به حل مشکلات می‌پرداخت، ایجاد گردید. این سیستم که "Dendral" نام داشت ترکیبات شیمیایی را بهتر از متخصصان، تجزیه و تحلیل می‌نمود (Feigenbaum, Buchanan,1993:233). از آن پس، بلافاصله یکی پس از دیگری سیستم‌های خبره که تخصص‌های مختلف یک انسان به آنها منتقل شده بود، مانند سیستم SBDS[۳] (Al-Taani, 2005: 457) در جهت تشخیص عیوب ماشین و سیستم MYCIN (Van Melle, 1978: 313) برای تشخیص بیماری‌ها به وجود آمدند (ارجمند و همکاران، ۱۳۹۶: ۲).

۳. انواع هوش مصنوعی و کاربردهای آن

اساساً یادگیری در هوش مصنوعی به سه دسته هوش مصنوعی محدود[۴]، عمومی[۵] و فوق‌العاده[۶] تقسیم می‌شود. این سه دسته، بیشتر نشان‌دهنده‌ی روند تکامل هوش مصنوعی در طول زمان هستند؛ به این صورت که در هوش مصنوعی محدود، این هوش برای کاری محدود و معین و دستوری خاص طراحی شده و نمی‌تواند به طور مستقل مهارت‌هایی فراتر از طراحی آن را بیاموزد. آنها اغلب از یادگیری ماشینی[۷] و الگوریتم‌های شبکه عصبی[۸] مانند: گوگل ترنسلیت و سیستم تشخیص چهره یا چت بات‌های عادی برای تکمیل این وظایف مشخص شده استفاده می‌کنند (Aljaber, Almushaili, 2022: 55). هرگاه صحبت از هوش مصنوعی عمومی به عمل می‌آید، به نوعی از هوش مصنوعی اشاره می‌کنیم که به اندازه یک انسان توانایی خواهد داشت و می‌تواند توانایی‌های شناختی انسان مانند توانایی فکر کردن را تقلید نماید (ذاکری‌نیا، ۱۴۰۲: ۱۳۹) و نظیر انسان‌ها طیف وسیعی از اعمال را بیاموزد و به نحو احسن انجام دهد. هدف از طراحی هوش مصنوعی عمومی این است که بتوان ماشین‌هایی ایجاد کرد که قادر به انجام وظایف چند منظوره باشند و به عنوان دستیاران واقعی و به همان اندازه هوشمند برای انسان‌ها در زندگی روزمره عمل کنند (Aljaber, Almushaili, 2022: 55; Khan,2021: 4). هوش مصنوعی فوق‌العاده یا ابر هوش مصنوعی راهی به سوی آینده است. برای ایجاد آن باید این هوش از انسان پیشی

---

[۱] The Defense Advanced Research Projects Agency (DARPA)
[۲] Expert System
[۳] Service Bay Diagnosis System
[۴] Artificial Narrow Intelligence (ANI)
[۵] Artificial General Intelligence (AGI)
[۶] Artificial Super Intelligence (ASI)
[۷] Machine learning
[۸] Neural network algorithms

بگیرد و توانایی بیشتری از انسان داشته باشد. در سال ۲۰۱۶ پروفسور آرند هیتز[۱]، استاد دانشگاه میشیگان تقسیم‌بندی نوین و جامعی را بر این اساس که چگونه یک هوش مصنوعی از قابلیت‌های یادگیری خود برای پردازش داده‌ها، پاسخ به محرک‌ها و تعامل با محیط خود استفاده می‌کند، ارائه داد که در ذیل بدان پرداخته می‌شود(Khan,2021: 5; coursera.org):

الف) ماشین‌های واکنش‌گرا[۲]: در این نوع از ماشین‌ها، هوش مصنوعی از نوع محدود بوده و قادر به ذخیره حافظه یا یادگیری از تجربیات گذشته نیستند، اما می‌توانند محرک‌های خارجی را در زمان واقعی بخوانند و به آنها پاسخ دهند. این امر، باعث می‌شود که آنها برای انجام عملکردهای مستقل اولیه، مانند فیلتر کردن هرزنامه از صندوق ورودی ایمیل یا توصیه فیلم‌ها بر اساس آخرین جستجوهای Netflix، مفید باشند (Hassani, et al, 2020: 145; builtin.com).

ب) هوش مصنوعی با حافظه محدود[۳]: حافظه محدود، تقریباً سیستم هوش مصنوعی نوع ۲ یعنی هوش مصنوعی عمومی است. این الگوریتم نحوه کار نورون‌های مغز ما با یکدیگر را تقلید می‌کند، به این معنی که با دریافت داده‌های بیشتر برای آموزش، هوشمندتر می‌شود. هوش مصنوعی حافظه محدود، برخلاف ماشین‌های واکنش‌گرا، می‌تواند به گذشته نگاه کند و اشیاء یا موقعیت‌های خاص را در طول زمان نظارت کند. سپس این مشاهدات در هوش مصنوعی برنامه‌ریزی می‌شوند تا اقدامات آن بر اساس داده‌های لحظه گذشته و حال انجام شود اما در حافظه محدود، این داده‌ها در حافظه هوش مصنوعی ذخیره نمی‌شوند بلکه به عنوان تجربه‌ای است که می‌توان از آن یاد گرفت. به طور مثال روشی که انسان‌ها ممکن است از موفقیت‌ها و شکست‌های خود درس بگیرند از جمله این موارد می‌باشد. خودروهای خودران نیز، نمونه شاخصی از هوش مصنوعی با حافظه محدود است که این خودروها با این روش، خودروهای دیگر را در جاده از نظر سرعت، جهت و نزدیکی مشاهده می‌کنند (Hassani, et al, 2020: 145; builtin.com, coursera.org).

ج) نظریه‌ی ذهن[۴]: از نظر پیشرفت هوش مصنوعی، فناوری حافظه محدود آخرین چیزی است که ما به آن دست یافته‌ایم، اما با این حال، مقصد نهایی نیست. ماشین‌های حافظه محدود، می‌توانند از تجربیات گذشته بیاموزند و دانش را به صورت جزئی ذخیره کنند، اما نمی‌توانند تغییرات ظریف محیطی و نشانه‌های احساسی را درک کنند یا به همان سطح هوش انسانی برسند. مفهوم هوش مصنوعی که می‌تواند احساسات دیگران را متوجه شود و از آنها استفاده کند، هنوز به طور کامل درک نشده است. این مفهوم که "نظریه ذهن" نامیده می‌شود، اصطلاحی است که از روانشناسی به عاریت گرفته شده و توانایی انسان در خواندن احساسات دیگران و پیش‌بینی اقدامات آینده بر اساس آن اطلاعات را توصیف می‌کند (Hassani, et al, 2020: 144; Khan,2021: 13). نظریه ذهن، می‌تواند تغییرات مثبت زیادی را در دنیای فناوری به ارمغان بیاورد، اما خطرات خاص خود را نیز به همراه دارد. از آنجایی که نشانه‌های احساسی بسیار ظریف هستند، زمان زیادی طول می‌کشد تا ماشین‌های هوش مصنوعی بتوانند آن‌ها را کامل بخوانند و به طور بالقوه ممکن است در مرحله یادگیری خطاهای بزرگی مرتکب شوند. همچنین، برخی از افراد نگران هستند که پاسخ فناوری‌ها به سیگنال‌های احساسی و همچنین موقعیتی، به معنای اتوماسیون برخی مشاغل باشد (Boucher,2020:28; builtin.com).

[۱] Arend Hintze
[۲] Reactive machines
[3] Limited memory
[4] Theory of mind

د) خودآگاهی[1]: مرحله فراتر از نظریه ذهن، زمانی است که هوش مصنوعی خودآگاهی را توسعه می‌دهد و به عنوان نقطه عطف هوش مصنوعی در دنیای فناوری تلقی می‌شود و به نوعی پایان بزرگ تکامل هوش مصنوعی خواهد بود. گمان می‌رود که وقتی به آن نقطه رسیدیم، ماشین‌های هوش مصنوعی خارج از کنترل ما باشند؛ زیرا آنها نه تنها می‌توانند احساسات دیگران را حس کنند، بلکه حس خود را نیز خواهند داشت (coursera.org). گفته می‌شود که مردم از ایجاد این نوع هوش مصنوعی و از عواقب ایجاد آن می‌ترسند و نگرانند که این نوع هوش مصنوعی مشاغلشان را به سرقت ببرد یا دنیا را تسخیر کند. این در حالی است که اگر این نوع هوش مصنوعی با موفقیت ایجاد شود، هیچ کس نمی‌داند چه تأثیری خواهد داشت. با این وجود، گام‌هایی توسط محققان و مهندسان برای توسعه نسخه‌های ابتدایی هوش مصنوعی خودآگاه در حال انجام است. شاید یکی از معروف‌ترین آنها سوفیا باشد، رباتی که توسط شرکت رباتیک Hanson Robotics ساخته شده است. اگرچه این ربات از نظر فنی خودآگاه نیست، اما کاربرد پیشرفته سوفیا نسبت به فناوری‌های هوش مصنوعی فعلی، نمایی اجمالی از آینده بالقوه خودآگاه هوش مصنوعی ارائه نموده و به همین سبب این امر، نویدبخش آینده‌ای درخشان و شاید پرخطر است!(Hassani, et al, 2020: 146).

بنا به آنچه بیان شد، در حال حاضر استفاده از هوش مصنوعی دیگر به وظایف و عملیات محاسباتی یا آماری محدود نمی‌شود و در واقع هوش مصنوعی اکنون بخشی جدایی ناپذیر از همه‌چیز است؛ از بازی‌های کامپیوتری گرفته تا فرآیندهای پیچیده تجاری. این فناوری، همچنین در اغلب زمینه‌ها کاربرد عملی داشته و به عنوان دستیار انسان‌ها مورد استفاده قرار می‌گیرد که برخی از مهمترین این زمینه‌ها عبارتند از:

الف) در زمینه پزشکی و دندان‌پزشکی: در طول دهه‌ی گذشته تقریباً اغلب صنایع بزرگ با کمک هوش مصنوعی پیشرفت‌های چشم‌گیری داشته‌اند و صنعت بهداشت و درمان نیز از این قاعده مستثنی نبوده است. الگوریتم‌های هوش مصنوعی در این زمینه می‌توانند به‌طور خودکار علائم اولیه بیماری‌هایی مانند سرطان، بیماری‌های قلبی عروقی و اختلالات عصبی و حتی بیماری‌های زنان و زایمان را از تصاویر پزشکی با دقت بالا تشخیص دهند، حتی در مواردی که ناهنجاری‌ها پنهان بوده و توسط متخصصان انسانی به راحتی قابل تشخیص نیستند (Malani, et al,2023: 2). به عنوان مثال، تشخیص بیماری آبله میمون (Almufrah, et al, 2023: 2)، شناخت عوامل خطر قبل از عمل و حین عمل و پیش‌بینی مرگ بعد از جراحی قلب (Fan, et al, 2022: 13)، استفاده در روش‌های آندوسکوپی[2] برای غربالگری و شناخت سرطان دستگاه گوارش (Goyal, et al, 2021: 2; Liang, et al, 2022: 124)، تشخیص، تصمیم‌گیری، برنامه‌ریزی درمان و پیش‌بینی نتایج درمان در علم دندانپزشکی در زمینه‌های پریودنتیکس[3]، ارتودنسی[4]، جراحی دهان و فک و صورت[5] و پروتزها[6] (Ding, et al, 2023: 5-9).

ب) در زمینه آموزش: برنامه‌های کاربردی هوش مصنوعی به سازمان‌های آموزشی در دو بخش کمک می‌کنند: یکی بخش اداری (پذیرش، مشاوره، خدمات کتابخانه و غیره) و دیگری بخش علمی (ارزیابی، بازخورد، تدریس خصوصی و غیره) (Ahmad, et al,2022: 1). به عنوان مثال هوش مصنوعی در آموزش، امکان ارائه مدل‌های پیش‌بینی، شناسایی دانش‌آموزان با عملکرد بالا و در معرض خطر، پیگیری پیشرفت تحصیلی، طراحی و اجرای طرح‌های درسی، آزمون‌ها و ارائه بازخورد

[1] Self-awareness
[2] Endoscopic
[3] Periodontics
[4] Orthodontics
[5] Oral and Maxillofacial Surgery
[6] Prosthodontic

فردی را دارد (Bagunaid, et al, 2022: 2). در سایت Jenni.ai نیز با وارد کردن موضوع، مقاله‌ای به صورت آماده و منطبق با درخواست شخص ارائه خواهد شد. از طرف دیگر، هوش مصنوعی کارهایی که نیاز به خلاقیت دارد را نیز انجام می‌دهد مانند: نوشتن داستان‌های ترسناک یا متن ترانه، ساخت موزیک ویدئوها یا توسعه‌ی آلبوم‌های بلک متال[1] (Martinez,2019: 1021).

ج) در زمینه تجارت و کسب و کار: می‌توان عنوان نمود که در عصر دیجیتالی شدن اقتصاد قرار گرفته‌ایم و هوش مصنوعی در این زمینه نیز در حال تغییر پایه‌های اقتصاد سنتی است. برای نمونه، بهبود خدمات مشتریان به دلیل افزایش سطح سفارشی‌سازی، توانایی پاسخگویی سریع‌تر به درخواست‌های مشتریان و افزایش و بهبود میزان رضایت‌مندی آن‌ها، افزایش سطح بهره‌وری کسب و کار توسط فناوری‌های نوآورانه و کاهش هزینه‌های مبادله (Dudnik, et al, 2021: 2)، کاهش خطرات با افزایش دقت پیش‌بینی، انجام وظایف اداری معمول و تجزیه و تحلیل داده‌های بزرگ و مدل‌سازی فرآیندهای تجاری مختلف را می‌توان نام برد. به عبارت دیگر، امروزه هوش مصنوعی در تجزیه و تحلیل استراتژیک عوامل مختلف محیط کلان و خرد سازمان (Kitsios, Kamariotu ,2021: 2)، تجزیه و تحلیل نقاط قوت و ضعف، فرصت‌ها و تهدیدها، تجزیه و تحلیل پورتفولیوی شرکت‌ها امری ضروری به شمار می‌رود (Chernov, et al, 2020: 22). حتی هوش مصنوعی اکنون برای سرمایه‌گذاری در وال استریت[2] مورد استفاده قرار می‌گیرد و می‌تواند ۱۹۳۰۰۰ معامله در روز انجام دهد. علاوه بر این، پیش‌بینی‌های رفتار مصرف‌کننده که توسط بازاریابان خرده فروشی آنلاین به کار گرفته می‌شود توسط یک الگوریتم هوش مصنوعی با دقت بسیار بالا ایجاد شده است (Martinez, 2019: 1020). در کنیا، Vital Signs داده‌های مربوط به کشاورزی و اکوسیستم را جمع‌آوری کرده و از داده‌های تصاویر ماهواره‌ای برای تخمین الگوهای بارندگی و خشکسالی استفاده می‌کند. در نیجریه، Zenvus یک پلتفرم مبتنی بر داده است که بر اساس داده‌های جمع‌آوری‌شده از حسگرها و ابزارهای دیگر، اطلاعات تحلیلی را در اختیار کشاورزان قرار می‌دهد (Sadeski, et al, 2019: 121).

د) در زمینه چت بات‌ها: چت‌بات، یک برنامه کامپیوتری است که در جهت گفت‌وگوی محاوره‌ای بین انسان و ربات عمل می‌کند (Gupta, 2020: 255). چت‌بات‌ها به طور کلی به دو دسته‌ی چت‌بات‌های مبتنی بر قاعده۳ و چت‌بات‌های مبتنی بر هوش مصنوعی۴ تقسیم می‌شوند. تفاوت اصلی این دو دسته از چت‌بات‌ها این است که یک چت‌بات مبتنی بر قاعده بر روی قوانین از پیش تعریف شده و بدون قابلیت خودآموزی کار می‌کند. این در حالی است که چت‌بات‌های هوش مصنوعی از فناوری‌های هوش مصنوعی و یادگیری ماشین پشتیبانی کرده و می‌توانند معنای رفتار کاربران را درک کنند (Supreetha, 2020: 688). در حال حاضر، از این چت‌بات‌ها در زمینه‌های مختلف مانند: آژانس‌های مسافرتی برای پیدا کردن هتل و رستوران و رزرو بلیط، بانک‌ها برای ارائه خدمات و مشاوره به مشتریان و دولت‌ها برای فروش بلیط پارکینگ استفاده می‌شود (Supreetha, 2020: 691; Pariyani, et al,2020: 1157). اما از مهم‌ترین چت‌بات‌ها که مبتنی بر هوش مصنوعی بوده و با استقبال گسترده‌ی مردم عادی رو به رو شده چت‌بات Chat GPT است. Chat GPT، نوعی از مدل زبان هوش مصنوعی است که توسط شرکت Open AI توسعه یافته و از شبکه‌های عصبی عمیق برای پردازش مقادیر زیادی از داده‌های متنی و یادگیری الگوهای زبان استفاده می‌کند (Božić, Poola, 2023: 2; Deng, Lin, 2023: 82). این چت‌بات،

[1] Black metal albums
[2] Wall Street
[3] Rule-based chatbot
[4] AI chatbots

می‌تواند به تمامی سؤالات کاربران خود مانند رژیم غذایی و برنامه ورزشی متناسب با هر فرد، مشاوره، تولید متن در مورد موضوعی خاص، ترجمه متن، پاسخ به سؤالات حقوقی، بانکی، پزشکی، زیبایی، مطالعه و ... پاسخ دهد.

۴. چالش‌های هوش مصنوعی در حوزه حریم خصوصی

هوش مصنوعی و مهم‌ترین نمونه فعلی آن، یادگیری ماشینی، در سال‌های اخیر پیشرفت چشمگیری داشته است. از زمانی که شرکت OpenAI، ChatGPT را در دسامبر ۲۰۲۲ و نسخه پیشرفته GPT-4 را کمی بعد معرفی کرد، هوش مصنوعی بخشی از زندگی بسیاری از افراد شده است. حتی قبل از آن، هوش مصنوعی بسیاری از برنامه‌های مهم اقتصادی و اداری، از تشخیص چهره گرفته تا تشخیص سرطان و از کنترل هرزنامه تا رمزگشایی دست خط و ابزارهای کاهش تغییرات آب و هوا و مانند این‌ها که در بخش قبل ذکر شد را تأمین کرده است. با ظهور سیستم‌های هوش مصنوعی مولد، مانند ChatGPT، Bard، یا Stable Diffusion، هوش مصنوعی با سرعتی بی‌سابقه در هر گوشه از جوامع بشری گسترش یافته است. این روند اگرچه دارای ظرفیت‌های قابل توجهی است، اما نگرانی‌ها و چالش‌هایی را نیز در زمینه‌های مختلف برای دولت‌ها و مردم ایجاد می‌نماید. بر اساس نظر ۲۵۰ متخصص در زمینه هوش مصنوعی و اخلاق از جمله: کارشناسان فنی، نمایندگان صنعت، سیاست‌گذاران و... ۳۹ چالش مورد شناسایی قرار گرفته که یکی از این زمینه‌ها چالش فناوری هوش مصنوعی در حوزه حریم خصوصی است (Stahl,2020:35).

حفظ و رعایت حریم خصوصی اشخاص، از جمله تکراری‌ترین نگرانی‌هایی است که شهروندان در مورد هوش مصنوعی دارند. در حالی که مفهوم حریم خصوصی، مفهومی نسبتاً مبهم بوده و حتی برخی آن را به یک باتلاق ناشناخته[1] تشبیه می‌کنند (Inness, 1996: 14) اما می‌توان آن را توانایی کنترل اطلاعات مربوط به خود، به شکل داشتن حق جلوگیری از دستیابی یا استفاده دیگران از آن اطلاعات بدون رضایت دانست (Elliott, Soifer, 2022: 1). به عبارت دیگر حریم خصوصی محدوده‌ای است که شخص انتظار دارد از دسترس دیگران اعم از دولت یا اشخاص حقیقی یا حقوقی دیگر مصون بماند (فتحی، شاهمرادی، ۱۳۹۶: ۲۲۹). در آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۹۳ در تعریف حریم خصوصی آمده که «قلمروی از زندگی شخصی فرد که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، وارد شدن، نظاره کردن، شنود و دسترسی اطلاعات شخصی فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره شده خصوصی نظیر هتل و کشتی، همچنین آنچه که حسب قانون فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات». این حریم در اسناد و قوانین داخلی و خارجی از جمله اصول ۲۲ تا ۲۵ قانون اساسی، کنوانسیون اروپایی حقوق بشر و اعلامیه حقوق بشر اسلامی قاهره، مورد حمایت دولت‌ها قرار گرفته است. حریم خصوصی در آیین‌نامه مذکور و لایحه حریم خصوصی که در سال ۱۳۸۴ به مجلس تقدیم شد دارای ابعاد متنوعی است که از این ابعاد می‌توان در طبقه‌بندی حریم خصوصی استفاده نمود که عبارتند از: حریم خصوصی جسمانی، حریم خصوصی در محل کار، حریم خصوصی ارتباطات، حریم خصوصی اطلاعات، حریم خصوصی اماکن و منازل. از بین این پنج نوع حریم، فناوری هوش مصنوعی می‌تواند دو حریم را تحت تأثیر خود قرار دهد: حریم خصوصی ارتباطاتی که به تسلط اشخاص بر اطلاعات ارسال شده‌ی آن‌ها از طریق فضای مجازی گفته می‌شود و حریم خصوصی داده‌ای که موضوع آن تسلط بر داده‌های شخصی اشخاص است که توسط شرکت‌ها و موسسات جمع‌آوری

[1] Unknown swamp

گردیده (صادقی، ۱۳۸۸: ۱۱۷). لذا، دو چالش اصلی و مهمی که ممکن است از طریق هوش مصنوعی در دو حریم خصوصی ارتباطاتی و داده ای (اطلاعاتی) ایجاد شود را می‌توان نظارت جمعی و جعل عمیق دانست که در ادامه مورد بررسی قرار خواهند گرفت:

۴-۱. نظارت جمعی[1]:

یکی از مهم‌ترین دلایلی که شهروندان عموماً نگران حفظ و کنترل اطلاعات و حریم خصوصی خود هستند، این است که این امکان وجود دارد که دیگران با دستیابی به این اطلاعات از آن‌ها سوء استفاده نمایند و قصد آسیب به آن اشخاص را داشته باشند. موضوعی که سال‌هاست وجود داشته و به نوعی منافع امنیتی و حریم خصوصی اشخاص را تهدید می‌نموده نظارت جمعی نام دارد که در گذشته این نظارت توسط دولت صورت می‌گرفته و حقوقدانان در صدد محدود نمودن آن بوده‌اند (Königs, 2022: 4) اما این تعارض میان حریم خصوصی اشخاص و هوش مصنوعی زمانی ممکن است به وجود بیاید که هوش مصنوعی به جمع‌آوری و پردازش خودکار داده‌های افراد بپردازد (Macnish, 2020: 10). این داده‌ها بر اساس ماده ۹ قانون حفاظت از اطلاعات اتحادیه اروپا[2] می‌تواند داده‌های قومی-نژادی، عقاید سیاسی، باورهای دینی و فلسفی، اطلاعات ژنتیکی و بیومتریک باشد. نظارت جمعی که توسط هوش مصنوعی انجام می‌شود، اکنون تهدیدی واقعی-تر از هر زمان دیگری برای اشخاص در تمام جهان محسوب می‌شود. گسترش روز افزون به کارگیری ابزارهای دیجیتال مانند: لپ‌تاپ، رایانه، تبلت، تلفن‌ها، ساعت‌ها، ماشین‌ها و یخچال‌های هوشمند و ... همراه با افزایش اتصال به اینترنت منجر به ایجاد جهانی شده است که در آن، همه ما در هر دقیقه از حیاتمان تحت نظارت و ضبط داده‌های مرتبط هستیم. از طرف دیگر، به نظر می‌رسد شبکه‌های اجتماعی آنلاین مانند یوتیوب می‌دانند چگونه اشخاص را به مدت طولانی‌تر و بیش از حد در پلتفرم خود نگه‌دارند و اشخاص از لحاظ شخصی، سیاسی و تجاری به چه چیزی علاقه دارند. یکی از دلایل این امر می‌تواند دو فناوری محاسبات فراگیر[3] که وظیفه دارد نرم‌افزار را در تار و پود زندگی روزمره اشخاص ببافد تا زمان استفاده از آن قابل تفکیک از زمان‌های دیگر نباشد و هوش محیطی[4] که طراحی شده تا افراد را بشناسد و نیازهای ذهنی و خواسته‌های آن‌ها را پیش‌بینی نماید، باشد (Weiser,1991: 94). این امکانات، امکان جمع‌آوری و پردازش داده ها و اطلاعات را در مقیاسی که هرگز اتفاق نیفتاده بود فراهم آورده و این موضوع منجر به نقض بخش قابل توجهی از حریم خصوصی اشخاص شده است. به عنوان مثال، در نیمه اول سال ۲۰۱۹ میلادی، ۳۸۰۰ نقض داده در سراسر جهان گزارش شده است که ۴,۱ میلیارد رکورد داده را در معرض خطر قرار داده است. با وجود حملات سایبری و نشت داده‌ها در همه بخش‌ها از مراقبت‌های بهداشتی گرفته تا امور مالی، خرده فروشی گرفته تا دولت و غیره، عجیب نیست که چنین حوادثی به طور مکرر در اخبار گزارش شوند (Hinds, et al, 2020: 3). رسوایی فیس‌بوک-کمبریج آنالیتیکا[5] یکی از گسترده‌ترین نقض‌های داده در سال ۲۰۱۸ میلادی بوده است. پس از افشای اینکه داده‌ها و اطلاعات حدود ۸۷ میلیون کاربر فیسبوک به طور غیرقانونی و بدون رضایت آنها جمع‌آوری شده است (Cadwalladr, 2018, theguardian.com ؛ Skirchy, 2018, theguardian.com) و علاوه بر آن، از این داده‌ها برای ایجاد تبلیغات روان‌شناختی استفاده شد که ظاهراً با هدف تأثیرگذاری بر ترجیحات رأی‌دهی مردم در انتخابات ریاست‌جمهوری ۲۰۱۶ میلادی ایالات متحده آمریکا بوده است، مقیاس سوء استفاده از داده‌ها همراه با چنین ادعاهای بزرگ دستکاری انبوه، خشم جهانی را برانگیخت و اعتراضات

[1] Mass Surveillance
[2] General Data Protection Regulation (GDPR)
[3] Ubiquitous computing
[4] Ambient intelligence
[5] Cambridge Analytica

متعددی را سبب گردید که طی آن از مردم خواسته شد تا حساب‌های کاربری خود را حذف نمایند. بر این اساس، می‌توان مشاهده نمود که در پلتفرم‌های اجتماعی مانند فیس بوک و شرکت‌های تحلیلی مانند: کمبریج آنالیتیکا، چگونه چیزهای ساده و به ظاهر بی‌اهمیت مانند پست‌های به اشتراک گذاشته شده و پسندیده شده، نظرات و این گونه موارد می‌تواند مبنایی برای ارزیابی شخصیت اشخاص باشد (Kanakia, et al, 2019: 5).

۲-۴. جعل عمیق:

یکی دیگر از چالش‌هایی که فناوری هوش مصنوعی در زمینه‌های مختلف ایجاد می‌نماید، توانایی هوش مصنوعی مدرن برای جعل هویت افراد است که در اصطلاح، Deep fake نام دارد و در مواردی مانند آسیب رساندن به افراد یا سازمان‌ها، آسیب به جامعه از طریق تضعیف دیپلماسی یا امنیت عمومی، تشدید شکاف‌های اجتماعی، دستکاری در انتخابات و از این دست موارد استفاده می‌شود (Citron, Chesney, 2019: 1778). اگرچه، قدمت دستکاری رسانه‌های دیداری و شنیداری به میزان عمر خود رسانه‌هاست؛ اما ورود اخیر جعل عمیق یک جهش قابل توجه و رو به جلو و نقطه عطفی در این زمینه بوده است. جعل عمیق محتوای رسانه‌ای فریبنده می‌باشد که توسط فناوری‌های هوش مصنوعی ایجاد شده و ابزاری مهم برای انتشار اطلاعات غلط و جعل هویت دیجیتالی و به عبارت دیگر آلودگی داده‌ها محسوب می‌شود (بنافی، ۱۴۰۲: ۱۶۵) که تشخیص آن، حتی برای اشخاص متخصص نیز سخت است. جعل عمیق توسط الگوریتم‌های یادگیری ماشینی در دو قسمت شبکه‌های عصبی و شبکه مولد تخاصمی[1] ترکیب شده با نرم‌افزار نقشه‌برداری چهره ایجاد می‌شوند که می‌توانند آن داده‌ها را بدون اجازه در محتوای دیجیتال وارد کنند (buffett.northwestern.edu; Santana, 2022: 118). در مارس ۲۰۲۲، اندکی پس از آغاز تهاجم روسیه به اوکراین، عموم مردم اوکراین با دیدن ویدئویی از ولودیمیر زلنسکی[2] رئیس جمهور اوکراین که از ارتش می‌خواست سلاح‌های خود را زمین بگذارند و تسلیم شوند، شگفت‌زده شدند. با پخش شدن این ویدئو در رسانه‌های اجتماعی و جلب توجه در اخبار، دفتر زلنسکی به سرعت صحت آن را رد کرد. در واقع، این ویدئو با استفاده از فناوری مذکور توسط مبلغان روسی تولید شد که این مورد، اولین نمونه‌ی استفاده از جعل عمیق در یک درگیری مسلحانه بود (Burgess,2022, news.sky.com). چالش‌های احتمالی این فناوری در حریم خصوصی افراد را می‌توان دو مورد دانست. اولین و بیشترین استفاده از آن، تغییر تصاویر افراد و ایجاد تصاویر و فیلم‌های غیراخلاقی و یا غیردلخواه است. این موضوع در سال‌های گذشته بسیار پرکاربرد بوده و برای تهدید، ارعاب و وارد کردن آسیب روانی استفاده گشته و حتی موجب اختلال در زندگی روزمره افرادی که در فیلم‌های جنسی جعلی به تصویر کشیده شده‌اند، گردیده است (Dodge, Spencer,2017: 657). از جمله نرم‌افزارهایی که به صورت رایگان در اختیار همگان قرار گرفته و برای تغییر چهره کاربرد دارد می‌توان ری فیس[3] و دیپ فیس لب[4] را نام برد. دیگر مورد استفاده از جعل عمیق که می‌تواند موجب ایجاد چالش در زمینه حریم خصوصی شود، توانایی این فناوری در فریب سامانه‌های احراز هویت بیومتریک است که از آن می‌توان برای دست‌یابی به اطلاعات محرمانه اشخاص مانند جعل هویت برای ورود و دست‌یابی به اطلاعات شرکت‌های رمز ارز مانند بایننس[5] استفاده نمود (السان، دهستانی، ۱۴۰۱: ۱۹۶) .

۵. اقدامات تقنینی نظام‌های حقوقی در زمینه صیانت از حریم خصوصی در حوزه فناوری هوش مصنوعی

[1] Generative Adversarial Networks (GAN)
[2] Volodymyr Zelenskyy
[3] Reface
[4] Deepfacelab
[5] Binance

تلاش برای درک رابطه میان نگرانی‌های مربوط به حریم خصوصی اشخاص و رفتار آن‌ها اغلب نشان می‌دهد که این دو به نوعی در تضاد هستند و این پدیده‌ای به نام پارادوکس حریم خصوصی[1] است (Barnes, 2006: 3). به این صورت که مردم اغلب ادعا می‌نمایند که نگران حریم خصوصی خود هستند، با این وجود به دلیل عدم درک ریسک و اطلاعات ناکافی در خصوص محافظت از حریم خصوصی برای استفاده از تخفیف فروشگاهی، درآمد یا تاریخ تولد و یا برای استفاده از خدمات مالی، شماره تلفن یا آدرس منزل خود را به راحتی ارائه می‌نمایند (Beresford, et al, 2012: 25). به همین دلیل، لازم به نظر می‌رسد که دولت‌ها برای جلوگیری از سوء استفاده از این اطلاعات و ایجاد هرج و مرج در جامعه چه از طریق خرید و فروش اطلاعات، استفاده امنیتی و یا تعرض به حریم خصوصی به وسیله جعل عمیق، قوانین و مقررات مورد نیاز را از طریق مراجع قانونگذار و نهادهای مقررات‌گذار مصوب نموده و برخورد حقوقی لازم را در نظر داشته باشند. مشاهده خطرات در حال گسترش، دولت‌ها و سازمان‌های بین‌المللی را بر آن داشت تا با تصویب قوانین و چارچوب‌های حقوقی لازم برای حکمرانی در حوزه فناوری، مانع بروز و گسترش اینگونه خطرات شوند که در ذیل به بررسی برخی از اینگونه قوانین و مقررات خواهیم پرداخت:

۵-۱- اتحادیه اروپا: خطرات مذکور در اتحادیه اروپا توسط قانونگذاران به رسمیت شناخته شده و اقداماتی نیز برای مقابله و مواجهه با آن‌ها انجام شده است. با این حال، نهادهای قانونگذار و مقررات گذار در اروپا، خیلی زود متوجه این امر شده اند که قوانین موجود نمی‌توانند با رشد سریع تغییرات فناورانه هماهنگی داشته باشند. بنابراین، مقررات عمومی حفاظت از داده‌ها[2] به عنوان اقدامی اصلاحی در ۲۷ آوریل ۲۰۱۶ تصویب و در ۲۵ می ۲۰۱۸ لازم‌الاجرا گشت. این قانون به ایجاد مقررات، توضیح فرایندهای مرتبط با داده‌های شخصی اشخاص اعم از حقیقی و حقوقی و پردازش آن‌ها، تضمین حفاظت از داده‌های شخصی، حقوق و آزادی‌های اشخاص حاضر در اتحادیه اروپا می‌پردازد. بر طبق ماده ۳ این قانون هر شخصی که داده‌های اشخاص را به منظور فروش کالا یا خدمات به شهروندان اتحادیه اروپا پردازش می‌نماید باید مفاد این قانون را اجرا کند حتی اگر خارج از اتحادیه اروپا باشد یا تابعیت اروپایی نداشته باشد (رضایی و همکاران، ۱۳۹۶: ۸). این قانون، حفاظت از داده‌های اتحادیه اروپا را برای مقابله با چالش‌های حریم خصوصی جدید ناشی از توسعه فناوری‌های دیجیتال تقویت می‌کند به عبارت دیگر اطلاعات اشخاص باید از طریق مستعارسازی یا بی‌نام سازی، ذخیره شده و به صورت پیش-فرض حداکثر محرمانگی در نظر گرفته شود، به گونه‌ای که داده‌ها بدون رضایت و به طور عمومی در دسترس نباشند. هیچ اطلاعات شخصی نمی‌تواند پردازش شود، مگر آنکه مطابق با مبنای قانونی که به وسیله مقررات تعیین شده انجام شود یا آنکه پردازنده داده‌ها اجازه صریح صاحب داده‌ها را دریافت کرده باشد و در صورت نقض آن جریمه‌ی مالی برای آن‌ها درنظر گرفته شده است (Li, et al, 2019: 2). یک سال پس از اجرای این قانون، شرکت Open AI اعلام کرد مدل زبانی این شرکت با نام GPT-2 با قابلیت تولید متن، به‌دلیل نگرانی‌های مرتبط با استفاده مخرب از این فناوری، برای عموم مردم منتشر نخواهد شد. به همین دلیل این شرکت پیشنهاد داد که دولت‌ها نظارت نظام‌مند بر تأثیرات اجتماعی و ترکیب فناوری های AI با یکدیگر را گسترش دهند و بر روند پیشرفت توانایی‌های سیستم‌های هوش مصنوعی نیز نظارت داشته باشند. بسیاری از عملیات‌های پردازش توسط سیستم‌های هوش مصنوعی از نقطه نظر قانون حفاظت از داده اتحادیه اروپا ممنوع شده بود. این ممنوعیت به عنوان یک محدودیت در نظر گرفته می‌شد که به موجب آن، این قانون، بسیار ناقص و مانعی برای توسعه سیستم‌های هوش مصنوعی تلقی می‌گردید. بنابراین پیش‌نویس مقررات ویژه سیستم‌های هوش مصنوعی در

[1] privacy paradox
[2] The General Data Protection Regulation (GDPR)

سال ۲۰۲۱ به کمیسیون اتحادیه اروپا ارائه شد با این قصد که مقررات سیستم‌های هوش مصنوعی را در سطح اتحادیه اروپا هماهنگ کند. قابل ذکر است که برخی از مقررات وضع شده در قانون موسوم به هوش مصنوعی[1] می‌تواند شکاف‌های موجود در GDPR را در مورد پردازش داده‌های شخصی پر کند (Hetchely, 2022: 1-33). پیش‌نویس این قانون در دسامبر ۲۰۲۲ همراه با اصلاحات در شورای اتحادیه اروپا به تصویب رسید و در ۱۲ جولای ۲۰۲۴ منتشر و ۲۰ روز بعد در کشورهای عضو لازم‌الاجرا شد. کشورهای اتریش، بلژیک، قبرس، فرانسه، بلغارستان، آلمان، رومانی، اسلواکی، ایتالیا، اسپانیا، مجارستان، سوئد، دانمارک، فنلاند، هلند، پرتغال، مالت، ایرلند، چک، کرواسی، لتونی، یونان، لهستان، اسلوونی، استونی، لوکزامبورگ و لیتوانی اعضای اتحادیه اروپا هستند.

۵-۲- بریتانیا: بریتانیا در سال ۲۰۱۸ قانون حفاظت از داده[2] را به تصویب رسانده است. این قانون، قوانین حفاظت از داده‌ها را در بریتانیا به روز و مقررات حفاظت از داده‌های عمومی (GDPR) را تکمیل کرده و دستورالعمل اجرای قانون اتحادیه اروپا (LED) را اجرا و حفاظت از داده‌ها را گسترش داده است (Hacker, 2023: 1-2).

۵-۳- برزیل: LGPD [3] اولین مقررات جامع حفاظت از داده ها در برزیل است و به طور گسترده با قانون حفاظت از داده‌های اتحادیه اروپا (GDPR) همسو است. اگرچه این قانون از سال ۲۰۲۰ لازم الاجرا بوده است، مجازات‌های مندرج در آن، در ۱ اوت ۲۰۲۱ قابل اجرا شد. این قانون دستورالعمل‌هایی را برای جمع آوری، استفاده، پردازش و ذخیره داده‌های شخصی در برزیل تعیین می‌کند (Belli, et al, 2023: 1-13).

۵-۴-کانادا: در ژوئن ۲۰۲۲، دولت کانادا قانون هوش مصنوعی و داده‌ها[4] را به عنوان بخشی از لایحه C-27 قانون اجرای منشور دیجیتال، بر این مبنا که طراحی، توسعه و استفاده از سیستم‌های هوش مصنوعی باید ایمن باشد و به ارزش‌های شهروندان کانادا احترام گذاشته شود، ارائه نمود (Scassa, 2023: 1-30).

۵-۵-چین: کشور چین در خصوص هوش مصنوعی تا پیش از سال ۲۰۲۳ دو قانون مهم تصویب نمود که عبارتند از دستورالعمل‌های اخلاقی برای مقابله با هوش مصنوعی مصوب ۲۰۲۱ و قوانین ۲۰۲۲ در خصوص محتواهای تولید شده اما در آگوست سال ۲۰۲۳ اولین و پیشرفته‌ترین قانون هوش مصنوعی در جهان را مصوب نمود که در آن به طور خاص در خصوص هوش مصنوعی مولد نیز صحبت به میان آمده است (Sheehan, 2023: 3-37).

۵-۶-: سازمان ملل متحد: در ورای قانونگذاری‌های داخلی، برای تقویت یک رویکرد فراگیر در سطح جهانی، دبیر کل سازمان ملل متحد یک هیئت مشورتی چندجانبه در سطح بالا در زمینه هوش مصنوعی تشکیل داد تا تجزیه و تحلیل و پیشبرد توصیه‌هایی را برای حاکمیت بین‌المللی هوش مصنوعی انجام دهد (Un.org). در این راستا، گوترش در بیانیه‌ای اعلام نمود:« من خواستار یک گفتگوی جهانی، چند رشته‌ای و چندجانبه در مورد حاکمیت هوش مصنوعی شده‌ام تا مزایای آن برای بشریت – همه بشریت – به حداکثر برسد و خطرات آن مهار شود و یا کاهش یابد». تشکیل هیئت مشورتی هوش مصنوعی گام مهمی در خصوص تلاش‌های سازمان ملل برای رسیدگی به مسائل حاکمیت بین‌المللی هوش مصنوعی است. وظایف فوری این هیئت شامل ایجاد یک اجماع علمی جهانی در مورد خطرات و چالش‌ها، کمک به مهار هوش

[1] Artificial Intelligence Act (AIA)
[2] Data Protection Act
[3] Lei Geral de Proteção de Dados
[4] Artificial Intelligence and Data Act (AIDA)

مصنوعی برای اهداف توسعه پایدار و تقویت همکاری بین‌المللی در زمینه مدیریت هوش مصنوعی تا تابستان ۲۰۲۴، پیش از اجلاس سران آینده است.

۵-۷- ایران: همانطور که مشاهده نمودیم، اکثر کشورها از سال ۲۰۱۸ در تکاپوی تصویب قانونی در جهت حفظ داده‌ها و حریم خصوصی شهروندان خود هستند. در سالیان اخیر، در ایران نیز تلاش بر آن بوده که در جهت توسعه بسترهای زیرساختی و قانونی اقداماتی به عمل آید که از مهم‌ترین آن‌ها می‌توان به قانون انتشار و دسترسی آزاد به اطلاعات و قانون مدیریت داده‌ها و اطلاعات ملی اشاره نمود. (در تحلیل این دو قانون، ر.ک.به: میرشکاری و دیگران، ۱۴۰۳: ۳۰۸) پس از آن در راستای گسترش شرکت‌های فناوری مرتبط با هوش مصنوعی قوانینی مانند قانون جهش تولید دانش بنیان و قانون حمایت از شرکتها و مؤسسات دانش بنیان و تجاری‌سازی نوآوری‌ها و اختراعات به تصویب رسید.

در سال ۱۴۰۱ که بحث در خصوص هوش مصنوعی و چالش‌های آن شدت گرفت، شورای عالی فضای مجازی سندی به نام سند راهبردی جمهوری اسلامی ایران در حوزه فضای مجازی را تصویب و منتشر نمود که مطابق آن طراحی نظام حقوقی فضای مجازی به معاونت حقوقی رئیس جمهور، طراحی نظام قضایی فضای مجازی به رئیس قوه قضاییه و طراحی نظام به کارگیری فناوری‌های نوین فضای مجازی از جمله هوش مصنوعی و علوم داده، برعهده معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری قرار گرفته است. از آن پس در قوانین جدیدالتصویب، هوش مصنوعی به طور محدود مورد توجه قرار گرفت.

در بند الف ماده ۱۱۳ قانون برنامه هفتم پیشرفت جمهوری اسلامی ایران چنین مقرر شده است: «به‌منظور تسهیل رسیدگی به پرونده‌های قضائی و رفع اختلافات مردم، قوه قضائیه و وزارت دادگستری با رعایت قانون مدیریت داده‌ها و اطلاعات ملی حسب مورد مکلف به انجام اقدامات زیر هستند: الف- تا پایان سال دوم برنامه، امکان انجام اموری از قبیل ارجاع پرونده، تعیین وقت و انتخاب کارشناس را با استفاده از فناوری‌های نوین از جمله هوش مصنوعی برای کمک به قاضی با حفظ مسؤولیت شخص قاضی فراهم نمایند. آیین‌نامه اجرائی این بند در چهارچوب سیاست‌های ابلاغی شورای‌عالی فضای مجازی تهیه می‌شود و به‌تصویب رئیس قوه قضائیه می‌رسد». همچنین، در بند ج ماده ۶۵ قانون یاد شده نیز چنین آمده است: «دولت مکلف است در راستای حمایت از توسعه زیست‌بوم تحول‌آفرین هوش مصنوعی قابل اعتماد و پایدار و به‌منظور تعیین چهارچوب‌ها و ساز و کار تعامل تمامی ذی‌نفعان، فراهم نمودن دانش و زیرساخت‌های دانش فنی، اجتماعی، اخلاقی و حقوقی، ترویج و افزایش آگاهی در مورد کارکردهای هوش مصنوعی در زمینه‌های مختلف و خطرات بالقوه آن حداکثر ظرف شش‌ماه از لازم‌الاجرا شدن این قانون نسبت به اجرای «برنامه ملی توسعه هوش مصنوعی» با رعایت سیاست-های کلی نظام، مصوبات شورای‌عالی انقلاب فرهنگی و سند راهبردی جمهوری اسلامی ایران در فضای مجازی اقدام قانونی به عمل آورد».

همچنین، در تاریخ ۱۴۰۳/۰۴/۳۰ مصوبه شورای عالی انقلاب فرهنگی به نام سند ملی هوش مصنوعی جمهوری اسلامی ایران ابلاغ شد. این سند به بیان اصول و مبانی ارزشی، چشم‌انداز، اهداف کلان و شاخص‌های ارزیابی، سیاست‌های راهبردی، راهبردها و اقدامات ملی و اولویت‌های ملی به کارگیری هوش مصنوعی پرداخته است. در این سند، «رعایت حریم خصوصی و حفاظت از امنیت داده ها و اطلاعات در زیست‌بوم هوش مصنوعی» به عنوان یکی از اصول و مبانی ارزشی سند یاد شده و در بند یک از ماده ۵ این سند، «تدوین لوایح قانونی لازم به منظور ایجاد زیرساخت‌های حقوقی مورد نیاز جهت بهره‌گیری و مواجهه با مخاطرات هوش مصنوعی در کشور از قبیل... رعایت حریم خصوصی» به عنوان

یکی از زیرساخت‌های حکمرانی معرفی شده است. بنابراین در حال حاضر که قوانین مختص به هوش مصنوعی در جهت استفاده از مزایای آن و رفع و جلوگیری از چالش‌های آن وجود ندارد، برای حفاظت از حریم خصوصی اشخاص و ممانعت از سوءاستفاده از داده‌ها در ایران باید به قوانین سابق‌التصویب که در حوزه محافظت از داده‌ها قابل استفاده هستند، استناد کرد، مواردی همچون اصل ۲۵ قانون اساسی، قانون مسئولیت مدنی، قانون جرایم رایانه‌ای و قانون تجارت الکترونیکی. همچنین، در صورت نقض حریم خصوصی اشخاص از طریق انتشار اطلاعات واقعی و یا غیرواقعی، می‌توان از ظرفیت ماده۲۱ قانون انتشار و دسترسی آزاد به اطلاعات استفاده کرد. بر اساس این ماده، «هر شخصی اعم از حقیقی یا حقوقی که در نتیجه انتشار اطلاعات غیرواقعی درباره او به منافع مادی و معنوی وی صدمه وارد شده است حق دارد تا اطلاعات مذکور را تکذیب کند یا توضیحاتی درباره آنها ارائه دهد و مطابق با قواعد عمومی مسئولیت مدنی جبران خسارت‌های وارد شده را مطالبه نماید». بر اساس تبصره این ماده نیز، «در صورت انتشار اطلاعات واقعی بر خلاف مفاد این قانون، اشخاص حقیقی و حقوقی حق دارند که مطابق قواعد عمومی مسئولیت‌های مدنی، جبران خسارت‌های وارد شده را مطالبه نمایند» با این حال، روشن است که نصوص فوق در برابر تهدید نقض حریم خصوصی ارتباطاتی و حفاظت از داده ها از طریق هوش مصنوعی کارآ نبوده و لازم است برنامه جامعی در این خصوص طراحی شود. در واقع، با توجه به چالش‌های بروز یافته و قابل ظهور در زمینه تهدید حریم خصوصی اشخاص به سبب توسعه روزافزون به کارگیری فناوری هوش مصنوعی در حیات اجتماعی شهروندان و تجربه بسیار اندک نهادهای قانونگذار و مقررات‌گذار در حوزه تقنین و تنظیم‌گری در ارتباط با فناوری هوش مصنوعی و نیز نظر به ارتباط بسیار نزدیک فناوری هوش مصنوعی با اطلاعات هویتی اشخاص و حقوق مرتبط با شخصیت افراد، راهکارهای حقوقی ذیل به منظور صیانت هر چه مطلوب‌تر از حریم خصوصی و بهره‌مندی صحیح از مزایای آن در ارتباط با فناوری هوش مصنوعی در نظام حقوقی ایران پیشنهاد می‌گردد:

- تدوین قانون یا مقرره جامع در زمینه صیانت از حریم خصوصی در به کارگیری فناوری هوش مصنوعی و ارائه تعاریف، الزامات، حدود اختیارات و تکالیف قانونی نهادهای ناظر و مسئولیت مدنی اشخاص در زمینه رعایت حریم خصوصی در خصوص فناوری هوش مصنوعی
- تمهید شرایط حقوقی و قانونی لازم به منظور تضمین حق بر حریم خصوصی کاربران و صاحبان سکوها و پلتفرم‌های آنلاین فناوری هوش مصنوعی از یک طرف و پیش‌بینی ساز و کارهای قانونی لازم به منظور پاسخگو و مسئولیت‌پذیر نمودن صاحبان سکوها و پلتفرم‌های آنلاین فناوری هوش مصنوعی
- الزام قانونی صاحبان سکوها و پلتفرم‌های آنلاین فناوری هوش مصنوعی به احراز هویت چند مرحله‌ای اشخاص پیش از ارائه خدمات با توجه به لزوم احترام و رعایت حق حفظ حریم خصوصی اشخاص
- ارائه نشان کیفیت برای کمک به اعمال استانداردهای استفاده و توسعه هوش مصنوعی و صدور تاییدیه و گواهینامه برای شرکت‌های بهره‌مند از اطلاعات کاربران
- ایجاد کمیته اخلاق در حوزه هوش مصنوعی جهت توسعه هوش مصنوعی اخلاق‌مدار
- ایجاد کمیته راهبری در زمینه‌های مختلف اعم از: سلامت، حمل و نقل و مدیریت شهری، مسائل زیست محیطی، اقتصاد دیجیتال و... برای بهره از فواید هوش مصنوعی در رفع مشکلات موجود

نتیجه‌گیری

حریم خصوصی، یک حق اساسی است که پیش از این تنها با فضاهای فیزیکی افراد مرتبط بود؛ اما با ظهور انقلاب دیجیتال و ورود کاربران به این دنیای نوین، مفهوم مذکور عمیقاً تغییر شکل داده است. اکنون دیگر حفظ حریم خصوصی به فضاهای فیزیکی منحصر نبوده و کاربری ممکن است در یک فضای بستهٔ فیزیکی باشد، ولی حریم خصوصی‌اش نقض شود و داده‌های مهم اطلاعاتی‌اش به دست افراد سودجو بیفتد. بر این اساس، حفاظت از حریم خصوصی کاربران و داده‌هایشان در این فضا، اهمیت بسیار زیادی پیدا کرده است. در این زمینه افزایش پیچیدگی در جمع‌آوری، ذخیره‌سازی و تجزیه و تحلیل داده‌ها، نگرانی‌هایی در مورد افشای اطلاعات شخصی و احتمال نقض حق حریم خصوصی ایجاد کرده است. همانگونه که بیان شد، هوش مصنوعی با سرعت بسیار بالایی وارد زندگی اشخاص شده و مورد استقبال قشر گسترده‌ای از آن‌ها قرار گرفته به صورتی که به انحاء گوناگون وارد تار و پود زندگی‌شان گشته است. از طرفی عدم آگاهی کامل انسان‌ها از چگونگی سوءاستفاده از اطلاعات آنها موجب شده که گاهی خودشان این اطلاعات را در اختیار سازمان‌ها و فروشگاه‌ها و افراد ناشناس قرار دهند، غافل از آنکه ممکن است با این اقدام در دام نظارت جمعی و جعل عمیق گرفتار شوند و حریم خصوصی اطلاعاتی و ارتباطاتی آن‌ها در معرض خطر قرار بگیرد. بنابراین، با بررسی چالش‌های بروز یافته در این حوزه مشاهده نمودیم که امر قانونگذاری و اقدامی سریع در خصوص ایجاد ضوابط و چارچوب های مورد نیاز در این حوزه امری لازم و ضروری به نظر می‌رسد. در ادامه بیان نمودیم که دولت‌ها از سال ۲۰۱۸ در حیطه داخلی و بین-المللی اقدام به تصویب قوانین متعدد در این‌باره نموده اند و هرگونه تعرض به حریم خصوصی اشخاص و استفاده‌ی بی-اجازه و خرید و فروش اطلاعات آن‌ها را منع می نمایند. همچنین، در پایان این مقاله بیان گردید که در حال حاضر همچنان به مقوله حمایت از حریم خصوصی ارتباطاتی و داده ای اشخاص در مواجهه با فناوری هوش مصنوعی به صورت مکفی پرداخته نشده است. از این رو، با توجه به سرعت بسیار زیاد و پرشتاب پیشرفت فناوری هوش مصنوعی و خدمات وابسته به آن، تصویب قانون یا مقرره‌ای خاص با در نظر داشتن راهکارهای حقوقی پیشنهادی در این مقاله به منظور تبیین جوانب حقوقی و سازوکارهای حمایت از حریم خصوصی اشخاص در به کارگیری این فناوری در حال توسعه، امری لازم و ضروری به نظر می‌رسد. البته از دو سال گذشته مقدمات تصویب قانون هوش مصنوعی در کشورمان هم در حال انجام است اما تاکنون تنها در برنامه هفتم توسعه پیشرفت به طور محدود و نیز در ذیل سند ملی هوش مصنوعی جمهوری اسلامی ایران از آن نام برده شده است و تا زمان تصویب قانونی خاص در این زمینه می‌توان با استناد به موادی از قوانین عام موضوعه کشور جهت دادخواهی در این حوزه استناد نمود.

منابع

۱. ارجمند، مسعود؛ ابراهیم‌زاده، مجید؛ کاظمی، ابوالفضل. (۱۳۹۶). طراحی سیستم خبره برای عیب‌یابی و رفع عیب موتور ماشین، *سومین کنفرانس بین‌المللی مهندسی صنایع و سیستم‌ها*، ۱-۷.

۲. السان، مصطفی؛ دهستانی، سوور. (۱۴۰۱). جنبه‌های حقوقی جعل عمیق، *فصلنامه تحقیقات حقوقی ویژه‌نامه حقوق و فناوری*، دوره ۲۵، ۱۹۳-۲۱۸.

۳. بنافی، فرشته. (۱۴۰۲). حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، *پژوهش حقوق خصوصی*، سال دوازدهم، شماره ۴۵، ۱۴۹-۱۷۶.

۴. ذاکری‌نیا، حانیه. (۱۴۰۲). ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیهٔ اروپا، *مجله حقوق خصوصی*، سال بیستم، شماره ۱، ۱۳۵-۱۵۲.

۵. رضایی، امیرمهدی؛ مباشری، مازیار؛ مرادحاصل، نیلوفر. (۱۳۹۶). مقررات اتحادیه اروپا در مورد حفاظت از افراد حقیقی نسبت به پردازش داده‌های شخصی و انتقال آزاد داده‌ها، *انتشارات سازمان فناوری اطلاعات ایران*، تهران، ۱-۲۴۳.

۶. سند ملی هوش مصنوعی جمهوری اسلامی ایران

۷. صادقی، حسین. (۱۳۸۸). مسئولیت مدنی در ارتباطات الکترونیک، *انتشارات میزان*، جلد اول، تهران، ۱-۳۰۴.

۸. فتحی، یونس؛ شاهمرادی، خیرالله. (۱۳۹۶). گستره و قلمرو حریم خصوصی در فضای مجازی، *مجله حقوقی دادگستری*، سال هشتاد و یکم، شماره ۹۹، ۲۲۹-۲۵۲.

۹. قانون برنامه هفتم پیشرفت جمهوری اسلامی ایران

۱۰. میرشکاری، عباس؛ پیشنماز، سید امین؛ رکنی، امیر عباس. (۱۴۰۳). تراست داده، سازوکاری برای مدیریت منافع ذی نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران، *مطالعات حقوق تطبیقی معاصر*، سال ۱۵، شماره ۳۴ ، ۲۷۹-۳۲۰.

11. Ahmad Fayaz Ahmad; Alam Mansoor Alam; Rahmat Khairil Rahmat; Mubarik Muhammad Shujaat; Hyder Syed Irfan. (2022). Academic and Administrative Role of Artificial Intelligence in Education, *Sustainability*, Vol 14, 1-11.
12. Ahmed Wajeeha; Chaudhary Areeshia; Naqvi Gulfraz. (2022). Role of Artificial Neural Networks in AI, *Neuro Quantology*, Vol20, Issue13, 3365-3373.
13. Aljaber Sohajaber; Almushaili Tahani. (2022). Artificial Intelligence, *International Journal of Engineering Research and Application*, Vol. 12, Issue 1, 52-57.
14. Almufrah Maram; Tehsin Samabia; Humayun Mamoona; Kausar Sumaira. (2023). A Transfer Learning Approach for Clinical Detection Support of Monkeypox Skin Lesions, *Diagnostics*, Vol13, Issue8, 2-16.
15. Al-Taani Ahmad. (2005). An Expert System for Car Failure Diagnosis, *International Enformatika Conference*, Vol7, 457-460.
16. Bagunaid Wala; Chilamkurti Naveen; Veeraraghavan Prakash. (2022). AISAR: Artificial Intelligence-Based Student Assessment and Recommendation System for E-Learning in Big Data, *Sustainability*, Vol 14, no. 17, 2-22.
17. Barnes Susan. (2006). A Privacy Paradox: Social networking in the United States, First Monday, Vol 11, No 9,1-13.
18. Belli Luca, Curzi Yasmin, Gaspar Walter. (2023). AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience, *Computer Law & Security Review*, Vol 48, 1-28.
19. Beresford Alastair; Kübler Dorothea; Preibusch Sören, (2012), Unwillingness to pay for privacy: A field experiment, *Economics Letters*, Vol 117, Issue 1, 25-27.
20. Boucher Philip. (2020). Artificial intelligence: How does it work, why does it matter, and what can we do about it?, *EPRS | European Parliamentary Research Service*, 1-64.
21. Božić Velibor; Poola Indrasen. (2023). Chat GPT and education, 1-9.
22. Chernov Alexey; Chernova Victoria; Komarova Tatiana. (2020). The Usage of Artificial Intelligence in Strategic Decision Making in Terms of Fourth Industrial Revolution, *Proceedings of the 1st International Conference on Emerging Trends and Challenges in the Management Theory and Practice (ETCMTP 2019)*, Vol 19, 22-25.

23. Citron Danielle; Chesney Robert. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, Vol107, 1753-1820.
24. Deng Jianyang; Lin Yijia. (2023). The Benefits and Challenges of ChatGPT: An Overview. *Frontiers in Computing and Intelligent Systems*, Vol 2, No 2, 81-83.
25. Ding Hao; Wu Jiamin; Zhao Wuyuan; Matinlinna Jukka; Burrow Michael; Tsoi James. (2023). Artificial intelligence in dentistry—A review, *Frontiers in Dental Medicine*, Vol 4, 153-158.
26. Dodge Alexa; Spencer Dale. (2017). Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth, *Social & Legal Studies*, Vol 27, No 3, 636- 675.
27. Dudnik Olesya; Vasiljeva Marina; Kuznetsov Nikolay; Podzorova Marina; Nikolaeva Irina; Vatutina Larisa; Khomenko Ekaterina; Ivleva Marina. (2021). Trends, Impacts, and Prospects for Implementing Artificial Intelligence Technologies in the Energy Industry: The Implication of Open Innovation, *Journal of Open Innovation: Technology, Market, and Complexity*, Vol 7, No 2, 2-27.
28. Elliott David; Soifer Eldon. (2022). AI Technologies, Privacy, and Security, *Frontiers in Artificial Intelligence*, Vol 5, 1-8.
29. Fan Yunlong; Dong Junfeng; Wu Yuanbin; Shen Ming; Zhu Siming; He Xiaoyi; Jiang Shengli; Shao Jiakang; Song Chao. (2022). Development of machine learning models for mortality risk prediction after cardiac surgery, *Cardiovascular Diagnosis & Therapy*, Vol 12, Issue 1, 12-23.
30. Feigenbaum Edward; Buchanan Bruce. (1993). DENDRAL and Meta-DENDRAL: roots of knowledge systems and expert system applications, *Artificial Intelligence*, Vol59, No1-2, 233-240.
31. Goyal Hemant; Sherazi Syed; Mann Rupinder; Gandhi Zainab; Perisetti Abhilash; Aziz Muhammad; Chandan Saurabh; Kopel Jonathan; Tharian Benjamin; Sharma Neil; Thosani Nirav. (2021). Scope of Artificial Intelligence in Gastrointestinal Oncology, *Cancers*, Vol 13, No 21, 2-2023.
32. Gupta Aishwarya. (2020). Introduction to AI Chatbots, *International Journal of Engineering Research and Technology (IJERT)*, Vol 9, Issue 7, 255-258.
33. Hacker Philipp. (2023). AI Regulation in Europe: From the AI Act to Future Regulatory Challenges, *Oxford Handbook of Algorithmic Governance and the Law*, Oxford University Press, 1-15.
34. Hassani Hosein, Sirimal Silva Immanuel, Unger Stephane, Tajmazinani Maedeh, Mac feely Stephan. (2020). Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future?, *AI*, Vol 1, Issue 2, 143-155.
35. Hetchely Christiane. (2022). The Potential Impact of the Future AI Act on the GDPR, Master's thesis, *Information and Communication Technology Law at the University of Oslo*, 1-31.
36. Hidayat Nurharyadi Fajar; Satwiko Prasasto. (2021). The Implementation of Artificial Intelligence in the Environmental Licensing Process, *International Webinar on Digital Architecture 2021 (IWEDA 2021)*, Vol671, 291-296.
37. Hinds Joanne; Williams Emma; Joinson Adam. (2020). It wouldn't happen to me: Privacy concerns and perspectives following the Cambridge Analytica scandal, *International Journal of Human-Computer Studies*, Vol 143, 1-14.
38. https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf
39. https://builtin.com/artificial-intelligence/types-of-artificial-intelligence
40. https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789
41. https://rc.majlis.ir/fa/report?tag=%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87%20%D9%87%D9%81%D8%AA%D9%85%20%D8%AA%D9%88%D8%B3%D8%B9%D9%87&tag_lang=fa&order_index=0&page=1
42. https://www.bmc.com/blogs/artificial-intelligence-types/
43. https://www.coursera.org/articles/types-of-ai
44. https://www.darpa.mil/about-us/about-darpa
45. https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump
46. https://www.theguardian.com/us-news/2018/apr/06/facebook-suspends-aggregate-iq-cambridge-analytica-vote-leave-brexit
47. https://www.un.org/techenvoy/ai-advisory-body
48. Inness Julie. (1996). Privacy, Intimacy, and Isolation, *Oxford University Press*, New York.
49. Kanakia Harshil; Shenoy Giridhar; Shah Jimit. (2019). Cambridge Analytica – A Case Study, *Indian Journal of Science and Technology*, Vol 12, No 29, 1-5.
50. Khairuddin Hajar; Azrin ahmad; Mohammad, Adzhar, Noraziah. (2019). Splicing System in Automata Theory: A Review, *Journal of Physics Conference Series*, Vol 1366, No 1, 1-10.
51. Khan Hanif. (2021). Types of AI | Different Types of Artificial Intelligence Systems, *fossguru*, Vol 9, 1-13.
52. Khemani Deepak. (2020). Artificial Intelligence, The Age-old Quest for Thinking Machines, *Resonance Journal*, Vol.25, No.1, 33-41.

53. Kitsios Fotis; Kamariotou Maria. (2021). Artificial Intelligence and Business Strategy Towards Digital Transformation: A Research Agenda, *Sustainability*, Vol 13, No 4, 2-16.
54. Kline Ronald. (2011). Cybernetics, Automata Studies, and the Dartmouth Conference on Artificial Intelligence, *IEEE Annals of the History of Computing*, Vol33, No4, 5-16
55. Königs Peter. (2022). Government Surveillance, Privacy, and Legitimacy, *Philosophy & Technology*, Vol 35, No 8, 1-22.
56. kunze Don. (2020). Zairja-Thinking: A Second Virtuality for Design, *ACSA 108th Annual Meeting*, Vol 11, 1-11.
57. Li He, Yu Lu, He Wu. (2019). The Impact of GDPR on Global Technology Development, *Journal of Global Information Technology Management*, Vol 22, 1-16.
58. Liang Feng; Wang Shu; Zhang Kai; Liu Tong-Jun; Li Jian-Nan. (2022). Development of artificial intelligence technology in diagnosis, treatment, and prognosis of colorectal cancer, *World Journal of Gastrointestinal Oncology*, Vol14, Issue1, 124-152.
59. Macnish Kevin. (2020). Mass Surveillance: A Private Affair?, *Moral Philosophy and Politics*, Vol 7, No 1, 1-14.
60. Malani Sagar; Shrivastava Deepti; Raka Mayur. (2023). A Comprehensive Review of the Role of Artificial Intelligence in Obstetrics and Gynecology. *Cureus*, Vol 15, No 2, 1-10.
61. Martinez Rex. (2019). Artificial Intelligence: Distinguishing between Types & Definitions, *Nevada Law Journal*, Vol 19, Issue 3, 1015-1037.
62. McCorduck Pamela. (2004). Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence, *W. H. Freeman*, 2nd.
63. Moor James. (2011). The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years, *AI Magazine*, Vol27, No4, 87-91.
64. Mujoo S.; Najmi H.; Alhazmi F.; Shibli A.; Mobaraki A.; Dubey A. (2022). Knowledge, attitudes, and perceptions regarding the future of artificial intelligence in oral radiology in Jazan, Saudi Arabia, *International Journal of Health Sciences*, Vol6, Issue7, 4597-4604.
65. Pariyani Harsha; Sinha Anshika; Bhat Preeti; Rote Roshni; Mulla, Nilofar. (2020). A Literature Survey of Recent Advances in Chatbots, *Journal of Emerging Technologies and Innovative Research*, Vol 7 Issue 5, 1153-1159.
66. Sadeski Francie; Kouacou Karine; Poteau Xavier, et al. (2019). Potential of the fourth industrial revolution in Africa, *Study report unlocking the potential of the fourth industrial revolution in Africa, Technopolis & Research ICT Africa & Tambourine Innovation Ventures*, 1-270.
67. Santana Miosotis. (2022). Justice for Women: Deep fakes and Revenge Porn, *3rd Global Conference on Women's Studies*, Rotterdam, The Netherlands, 113-128.
68. Scassa Teresa. (2023). Regulating in Canada: a critical look at the proposed artificial intelligence and data act, *Emerging Issues in Technology Law and Intellectual Property*, Vol 101, No 1, 1-30.
69. Sheehan Matt. (2023). China's AI Regulations and How They Get Made, *Carnegie Endowment for International Peace*, Publications Department, Washington, DC, 1-27.
70. Smith Roger. (2016). James Cox's Silver Swan An eighteenth century automaton in the Bowes Museum, *Artefact Journal*, Vol4, 361-365.
71. Stahl Bernd. (2021). Artificial Intelligence for a Better Future, *Springer Briefs in Research and Innovation Governance*. Springer, Cham, 1-128.
72. Supreetha H V. (2022). A Survey on Various Types of Chatbots, *International Research Journal of Engineering and Technology (IRJET)*, Vol 9, Issue 7, 688-692.
73. Van mille William. (1978). MYCIN: a knowledge-based consultation program for infectious disease diagnosis, *International Journal of Man-Machine Studies*, Vol10, Issue 3, 313-322.
74. Weiser Mark. (1991). The computer for the 21st century, *Scientific American*, Vol256, 94-104.