فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال چهارم / شماره اول (شماره پیاپی ۱۳) / بهار ۱۴۰۴
وبگاه مجله: https://sanad.iau.ir/journal/cyberlaw
ISSN: 2821-126X

# Privacy in artificial intelligence-based technologies

**Tayyebeh Zafarian**
Department of Private Law, ShK.C., Islamic Azad University, Shahrekord, Iran
(Corresponding Author) bamdadb51@gmail.com
**Rahim Eslami Farsani**
Department of Private Law, ShK.C., Islamic Azad University, Shahrekord, Iran
**Morteza Sadeghi Dehsahraei**
Department of Private Law, ShK.C., Islamic Azad University, Shahrekord, Iran

Keywords:
privacy,
artificial intelligence,
technology

Abstract
Artificial intelligence-based technologies have been widely developed in recent years due to their unique capabilities, including the analysis and processing of massive data, deep learning. These technologies have played a significant role in improving services and improving the quality of human life. The value of privacy in modern societies, including maintaining individual dignity, protecting personal freedoms and public trust in social and technological mechanisms to exchange information between people.The purpose of the current research in the discussion of privacy in artificial intelligence-based technologies from a legal point of view is to ensure the protection of personal rights and characteristics of people against the use, access, and processing of personal data collected by these technologies. The basic question in this article is how to guarantee people's personal rights against the collection, use and processing of personal data by artificial intelligence systems?And in terms of the direction of the research, it was of the type of theoretical research, in terms of the nature of the problem, it was of the type of documentary research, and in terms of the research method, it was of the type of Descriptive-analytical research. The results have shown that: privacy protection in artificial intelligence technologies requires an appropriate combination of laws, technology, monitoring and accountability, which is necessary to ensure respect for the basic rights of users and the general society.

فصلنامه علمی
مطالعات حقوقی فضای مجازی

صفحات مقاله ۴۲ الی ۵۵

# حفظ حریم خصوصی در تکنولوژی های مبتنی بر هوش مصنوعی

**طیبه ظفریان**

گروه حقوق خصوصی، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران (نویسنده مسئول)

پست الکترونیک: bamdadb51@gmail.com

**رحیم اسلامی فارسانی**

گروه حقوق خصوصی، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران

**مرتضی صادقی دهصحرایی**

گروه حقوق، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران

تاریخ دریافت : ۲۳ آبان ماه ۱۴۰۳ تاریخ پذیرش: ۰۳ اسفند ماه ۱۴۰۳

سال چهارم / شماره اول (پیاپی ۱۳) / بهار ۱۴۰۴

## چکیده

تکنولوژی‌های مبتنی بر هوش مصنوعی به دلیل قابلیت‌های بی‌نظیر خود، از جمله تحلیل و پردازش داده‌های حجیم، یادگیری عمیق در سال‌های اخیر به شکل گسترده‌ای توسعه یافته‌اند. این تکنولوژی‌ها نقش بسزایی در بهبود خدمات و بهبود کیفیت زندگی انسان‌ها داشته‌اند ارزش حریم خصوصی در جامعه‌های مدرن، از جمله حفظ کرامت فردی، حفاظت از آزادی‌های شخصی و اعتماد عمومی به سازوکارهای اجتماعی و فناورانه برای تبادل اطلاعات بین افراد است. هدف پژوهش حاضر در بحث حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی از دیدگاه حقوقی، اطمینان از حفظ حقوق شخصی و خصوصیت افراد در مقابل استفاده، دسترسی، و پردازش داده‌های شخصی است که توسط این فناوری‌ها جمع‌آوری شده اند. سؤال اساسی در نوشتار حاضر این است که چگونه می‌توان حقوق شخصی افراد را در برابر تجمیع، استفاده و پردازش داده‌های شخصی توسط سیستم‌های هوش مصنوعی تضمین کرد؟ و از نظر جهت گیری پژوهش، از نوع پژوهش های نظری، از نظر ماهیت مسأله از نوع پژوهش های اسنادی و از نظر روش تحقیق از نوع پژوهش های توصیفی- تحلیلی بوده است. نتایج نشان داده است که: حفظ حریم خصوصی در تکنولوژی‌های هوش مصنوعی نیازمند یک ترکیب مناسب از قوانین، فناوری، نظارت و مسئولیت‌پذیری است که به منظور تضمین احترام به حقوق اساسی کاربران و جامعه عمومی، لازم است.

**واژگان کلیدی:** حریم خصوصی، هوش مصنوعی، تکنولوژی

## مقدمه

موضوع حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی، به عنوان یکی از مسائل حیاتی در دوران فعلی توسعه فناوری، از اهمیت بالایی برخوردار است. با گسترش روزافزون این فناوری‌ها، تجمع داده‌ها و تحلیل آن‌ها به منظور بهبود خدمات و تجربه کاربری، به یکی از مباحث اساسی در حوزه حریم خصوصی تبدیل شده است. این مقدمه به بیان مسائل اساسی حاکم بر حفظ حریم خصوصی در این حوزه می‌پردازد. تکنولوژی‌های مبتنی بر هوش مصنوعی به دلیل قابلیت‌های بی‌نظیر خود، از جمله تحلیل و پردازش داده‌های حجیم، یادگیری عمیق در سال‌های اخیر به شکل گسترده‌ای توسعه یافته‌اند.

این تکنولوژی‌ها نقش بسزایی در بهبود خدمات و بهبود کیفیت زندگی انسان‌ها داشته‌اند، اما همچنین با خود چالش‌ها و مسائلی در حوزه حریم خصوصی نیز ایجاد کرده‌اند. حریم خصوصی به عنوان حق اساسی هر انسان، مرتبط با محافظت از اطلاعات شخصی افراد در مقابل دسترسی، استفاده، یا انتشار بدون موافقت آنها تعریف می‌شود. ارزش حریم خصوصی در جامعه‌های مدرن، از جمله حفظ کرامت فردی، حفاظت از آزادی‌های شخصی و اعتماد عمومی به سازوکارهای اجتماعی و فناورانه برای تبادل اطلاعات بین افراد است. با پیشرفت تکنولوژی هوش مصنوعی، چالش‌های زیادی برای حفظ حریم خصوصی به وجود آمده است، انبوهی از داده‌های شخصی که توسط سامانه‌های هوش مصنوعی جمع‌آوری می‌شوند، شامل اطلاعات زندگی روزمره، مکان‌یابی، علایق و حتی اطلاعات پزشکی، می‌تواند به حفظ حریم خصوصی خدشه وارد کند. تحلیل و پردازش داده‌های بزرگ به وسیله الگوریتم‌های هوش مصنوعی می‌تواند منجر به شناسایی غیرمستقیم افراد، حتی در صورت عدم انتشار مستقیم اطلاعات شخصی شود.

تکنیک‌هایی مانند تولید محتوای مصنوعی  می‌توانند به دسترسی به اطلاعات حساس و تخریب حریم خصوصی منجر شوند. حفظ حریم خصوصی افراد به عنوان یکی از حقوق اساسی انسانی، در دنیای دیجیتال و با توجه به پیشرفت هوش مصنوعی، اهمیت بیشتری پیدا کرده است. به دلیل قدرت و قابلیت‌های هوش مصنوعی، داده‌های شخصی افراد به راحتی می‌توانند تجزیه و تحلیل شوند و در نتیجه حقوق شخصی و حریم خصوصی تهدید شود. با پیشرفت هوش مصنوعی و ابزارهای تجزیه و تحلیل داده، داده‌های شخصی به معنای واقعی کلمه ثروتی ارزشمند برای شرکت‌ها و سازمان‌ها هستند. این داده‌ها می‌توانند برای تبلیغات هدفمند، تحلیل‌های بازاریابی، تصمیم‌گیری‌های مدیریتی و حتی در پژوهش‌های علمی استفاده شوند. اما استفاده از این داده‌ها باید با رعایت حریم خصوصی و حقوق افراد صورت گیرد.حفظ حریم خصوصی در هوش مصنوعی می‌تواند به افزایش اعتماد عمومی به فناوری‌های نوین کمک کند. افراد تنها زمانی که اطمینان دارند  داده‌های شخصی‌شان به امانت نگهداری می‌شوند و استفاده مناسبی از آن‌ها صورت می‌گیرد، می‌توانند به طور کامل از فواید هوش مصنوعی بهره‌مند شوند.

یکی از چالش‌های مهم در حفظ حریم خصوصی در هوش مصنوعی، تعادل بین نفع عمومی (مانند پیشرفت تکنولوژی، بهبود خدمات و ...) و حقوق خصوصی افراد است. توسعه قوانین و سیاست‌های مؤثر برای محافظت از حریم خصوصی، باید این تعادل را حفظ کنند تا هم از پیشرفت فناوری بهره‌برداری شود و هم حقوق افراد مورد احترام قرار گیرد. حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی از اهمیت بالایی برخوردار است و نیازمند راهکارهای مبتنی بر قوانین، فناورانه و فرهنگی است تا این امکان را فراهم کند که افراد بتوانند از فواید این فناوری‌ها بهره‌مند شوند بدون اینکه حریم خصوصی آن‌ها به خطر بیفتد. بنابراین، حفظ حریم خصوصی در زمینه هوش مصنوعی نه تنها مسئله فنی بلکه یک چالش اجتماعی و اخلاقی نیز محسوب می‌شود که نیازمند راهکارهای جامع و مؤثر برای حل آن است.

پژوهش های متعددی در خصوص حریم خصوص و هوش مصنوعی انجام شده است از جمله: موهانتی[1] و همکاران(۲۰۲۲) در پژوهش« فراتر از حریم خصوصی: اعمال حریم خصوصی متفاوت در حوزه های کلیدی هوش مصنوعی، تراکنش های IEEE[2]بر روی دانش و مهندسی داده» نشان داده اند که حریم خصوصی می‌تواند تفاضلی بیشتر از صرف حفظ حریم خصوصی انجام دهد که برای بهبود امنیت، پایدار کردن یادگیری، ساخت مدل‌های عادلانه و اعمال ترکیب در بخش‌های منتخب هوش مصنوعی نیز استفاده می شود. مقاله مذکور ارائه دیدگاهی جدید در مورد

[1] . Mohanty

[۲] . یک مجله علمی ماهانه است که مقالات معتبر و قابل توجهی را در رابطه با تئوری، مدل‌سازی، طراحی، عملکرد و قابلیت اطمینان دستگاه‌ها و اتصالات مدار مجتمع الکترون و یون، شامل عایق‌ها، فلزات، منتشر می‌کند.

بسیاری از امکانات برای بهبود عملکرد هوش مصنوعی با استفاده از تکنیک‌های حریم خصوصی تفاضلی است. چاکرابورتی، اس.، و شارما، آر[1] (۲۰۲۰) در پژوهش« چالش های قانونی و اخلاقی در حفاظت از حریم خصوصی هوش مصنوعی » به بررسی چالش‌های قانونی و اخلاقی که در زمینه حفاظت از حریم خصوصی در سیستم‌های هوش مصنوعی ایجاد می‌شود، پرداخته اند.

نویسندگان به مشکلاتی مانند جمع‌آوری داده‌های شخصی بدون اجازه، استفاده غیرمجاز از داده‌ها و پیچیدگی‌های مربوط به شفافیت الگوریتم‌ها اشاره می‌کنند. گوگول، آ.، و کسلر. ام[2](۲۰۲۱) در پژوهش « هوش مصنوعی، حریم خصوصی و قانون: پیمایش در منظر اخلاقی»به تحلیل چالش‌های اخلاقی و قانونی در حفاظت از حریم خصوصی در دوران دیجیتال و با استفاده از هوش مصنوعی می‌پردازد و نیز به مسائل اخلاقی نظیر حقوق فردی، دسترسی به داده‌های شخصی، و تصمیم‌گیری‌های خودکار توسط هوش مصنوعی پرداخته و نیاز به تدوین چارچوب‌های قانونی بین‌المللی برای مقابله با این چالش‌ها را مورد بحث قرار داده‌اند. کونر،سی؛ مانتلر، ای[3](۲۰۲۲) در مقاله« حریم خصوصی داده ها در عصر هوش مصنوعی: یک چشم انداز جهانی » به بررسی مقررات جهانی پیرامون حفاظت از حریم خصوصی در کاربردهای هوش مصنوعی می‌پردازد. به ویژه، تأثیر قوانین حریم خصوصی مانندحفاظت از داده ها بر توسعه و پیاده‌سازی الگوریتم‌های هوش مصنوعی و چالش‌های آن‌ها در حفاظت از داده‌ها بررسی می‌شود. همچنین به چالش‌های بین‌المللی ناشی از تفاوت‌های قوانین حریم خصوصی در کشورهای مختلف پرداخته‌اند. زنگ، وای؛ ژنگ، اس[4](۲۰۲۳) در مقاله،« حریم خصوصی و اخلاق هوش مصنوعی: مطالعه تطبیقی چارچوب های قانونی » به مقایسه چارچوب‌های قانونی مختلف در برابر چالش‌های حفظ حریم خصوصی در هوش مصنوعی پرداخته شده است. همچنین توجه ویژه‌ای به ملاحظات اخلاقی در تنظیم قوانین حفاظت از داده‌ها و چگونگی ایجاد استانداردهای بین‌المللی برای کنترل استفاده از داده‌های شخصی در سیستم‌های هوش مصنوعی صورت گرفته است.

هدف کلی در بحث حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی از دیدگاه حقوقی، اطمینان از حفظ حقوق شخصی و خصوصیت افراد در مقابل استفاده، دسترسی، و پردازش داده‌های شخصی است که توسط این فناوری‌ها جمع‌آوری می‌شوند. سؤال اساسی در نوشتار حاضر این است که "چگونه می‌توان حقوق شخصی افراد را در برابر تجمیع، استفاده و پردازش داده‌های شخصی توسط سیستم‌های هوش مصنوعی تضمین کرد؟" پژوهش حاضر از نظر جهت گیری پژوهش، از نوع پژوهش های نظری، از نظر ماهیت مسأله از نوع پژوهش های اسنادی و از نظر روش تحقیق از نوع پژوهش های توصیفی بوده است به گونه ای که علاوه بر تصویرسازی آنچه که هست به تشریح و توضیح دلایل چگونه بودن و چرایی وضعیت مسئله و ابعاد آن می پردازد. برای تبیین و توجیه دلایل، نیاز به تکیه گاه استدلالی محکمی دارد. این تکیه گاه از طریق جستجو در ادبیات و مباحث نظری پژوهش و نوشتن گزاره ها و قضایای کلی موجود دربارهٔ آن فراهم می شود. به عبارتی از نظر منطقی جزئیات مربوط به مسئله تحقیق را با گزاره های کلی مربوطه مرتبط می سازد و به نتیجه گیری می پردازد.

## گفتار اول: تعاریف و مفاهیم

### بند اول-مفهوم حریم خصوصی

حریم خصوصی به معنای حفظ حقوق و اطلاعات شخصی افراد است که از دسترسی، استفاده، یا انتشار بدون موافقت افراد جلوگیری می‌کند. مبانی حقوقی حریم خصوصی در بسیاری از قوانین و استانداردهای بین‌المللی و ملی تأکید می‌کند. حریم خصوصی به عنوان یک جنبه از حقوق بشر در میان بسیاری از منشورها و اسناد بین‌المللی از جمله اعلامیه جهانی حقوق بشر و کنوانسیون اروپایی حقوق بشر قرار دارد(گودمن و

[1] .Chakraborty, S., & Sharma, R
[2] .Gogol, A., & Kessler, M
[3] .Kuner, C., & Mantelero, A
[4] .Zeng, Y., & Zheng, S

فلکسمن[1]، ۲۰۱۷: ۵۰)، در بسیاری از کشورها، قوانین خاصی مانند، مقررات عمومی حفاظت از داده ها۲ در اتحادیه اروپا و قانون حفظ حریم خصوصی مصرف کنندگان کالیفرنیا۳ در ایالات متحده آمریکا(بیل، ۲۰۱۹: ۲۲) برای حفاظت از داده‌های شخصی وجود دارد.

بسیاری از صنایع، مانند صنعت بانکداری و بهداشت، نیاز به رعایت مقررات خاصی در خصوص حفاظت از اطلاعات شخصی دارند. در صورتی که حقوق حریم خصوصی فرد نقض شود، افراد می‌توانند به دادگاه‌ها مراجعه کنند و از حقوق خود دفاع نمایند. بسیاری از سازمان‌های بین‌المللی مانند سازمان ملل متحد وجود دارند که حریم خصوصی را به عنوان حقوق اساسی مورد تأکید قرار داده‌اند. این مبانی حقوقی به عنوان یک چارچوب حقوقی برای تضمین حریم خصوصی افراد، موجب می‌شوند که دولت‌ها، سازمان‌ها و شرکت‌ها مسئولیت حفاظت از داده‌های شخصی را به طور جدی به عهده بگیرند و حقوق اساسی افراد را در زمینه حریم خصوصی تأمین کنند( کاسترن، ۱۴۰۲: ۱۹-۱۸). حقوق مرتبط با حریم خصوصی به عنوان یکی از موارد مهم در حقوق بین‌المللی و داخلی، شامل مجموعه‌ای از اصول و قوانین است که به حفاظت از اطلاعات شخصی افراد می‌پردازد. در ادامه، به برخی از مفاهیم اصلی حقوقی مرتبط با حریم خصوصی اشاره می‌کنیم:

۱. حق حریم خصوصی: این حق شامل حفظ سرپرستی بر فعالیت‌ها و داده‌های شخصی فرد در مقابل دیگران است.
۲. مقررات حفاظت داده‌های شخصی: این مقررات شامل قوانین و مقرراتی هستند که تعیین می‌کنند که چگونه داده‌های شخصی باید جمع‌آوری، ذخیره، پردازش و مورد استفاده قرار گیرند.
۳. حق اطلاع رسانی: افراد حق دارند که اطلاعات دقیق در مورد جمع‌آوری و استفاده از داده‌های شخصی خود را بدانند. شامل اطلاعاتی مانند هدف جمع‌آوری داده‌ها و شرایط استفاده از آنها می‌شود.
۴. حق تصحیح و حذف داده‌ها: این حق به افراد امکان می‌دهد که اطلاعات شخصی خود را تصحیح کنند و در برخی موارد، خواسته‌هایشان برای حذف داده‌ها را اعمال کنند.
۵. مسئولیت مالیاتی: شامل مسئولیت مالیاتی برای شرکت‌ها و سازمان‌ها که از داده‌های شخصی استفاده می‌کنند و باید اطمینان حاصل کنند که اطلاعات مالیاتی افراد محفوظ می‌ماند.(جمشیدی، ۱۳۹۷: ۵۵)

حریم خصوصی به حق افراد برای کنترل اطلاعات شخصی خود و نحوه جمع‌آوری، پردازش و استفاده از آن‌ها اشاره دارد. در عصر دیجیتال، اطلاعات شخصی می‌تواند شامل هر چیزی باشد؛ از جمله داده‌های پزشکی، اطلاعات مالی، رفتار آنلاین، محل سکونت، علاقه‌ها و حتی داده‌های ژنتیکی. با توجه به حجم زیاد داده‌های تولید شده توسط کاربران در دنیای دیجیتال و تجزیه و تحلیل‌های پیشرفته‌ای که توسط سیستم‌های هوش مصنوعی انجام می‌شود، حفظ حریم خصوصی به چالشی جدی تبدیل شده است.

## بند دوم- مفهوم هوش مصنوعی[4] و کاربردهای آن در حفظ حریم خصوصی

با پیشرفت‌های روزافزون در زمینه هوش مصنوعی (AI)، مسائل مختلفی در زمینه‌های مختلف زندگی بشر مطرح شده است. یکی از مهم‌ترین این مسائل، حفظ حریم خصوصی در استفاده از تکنولوژی‌های مبتنی بر هوش مصنوعی است. هوش مصنوعی می‌تواند اطلاعات حساس و شخصی بسیاری را پردازش کند و در بسیاری از زمینه‌ها مثل بهداشت، آموزش، تجارت، حمل‌ونقل، و حتی دولت‌ها استفاده می‌شود. این استفاده‌ها

---

[1] Goodman, Bryce; Flaxman, Seth

[2] General Data Protection Regulation (GDPR)

مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده در اتحادیه اروپا و منطقه اقتصادی اروپا وضع شده‌است. هدف این مقررات اساساً، برای اعطای کنترل داده ها به شهروندان و ساکنان این منطقه و ساده‌سازی محیط مقررات گذاری برای کسب و کارهای بین‌المللی از طریق یکسان‌سازی مقررات است. این مقررات جایگزین قانون حفاظت از داده اتحادیه اروپا شده‌است و شامل احکام و الزاماتی مرتبط با پردازش اطلاعات شخصی قابل تشخیص در اتحادیه اروپا می‌شود و در خصوص همه کسب و کارهایی که با این منطقه اقتصادی مراوده کاری دارند، صرفنظر از مکان استقرارشان، می‌شود. بدین ترتیب، فرایندهای کسب و کار که اطلاعات شخصی را اداره می‌کنند، باید مبتنی بر «حفاظت اطلاعات از طریق طراحی و به‌طور پیش فرض» باشند؛ یعنی اطلاعات شخصی باید با استفاده از مستعارسازی یا بی‌نام سازی ذخیره شود و و حداکثر محرمانگی به‌طور پیش فرض در نظر گرفته شود، به گونه ای که داده‌ها بدون رضایت صریح به‌طور عمومی در دسترس نباشد و بدون اطلاعات اضافی جداگانه برای تعیین هویت اشخاص قابل استفاده نباشد.

[3] California Consumer Privacy Act (CCPA)

لایحه‌ای است که حقوق حریم شخصی و حمایت از مصرف‌کننده افراد مقیم ایالت کالیفرنیا در کشور ایالات متحده آمریکا را بهبود می‌دهد. لایحه توسط مجلس ایالتی کالیفرنیا به تصویب رسیده‌است و توسط جری براون فرماندار این ایالت در ۲۸ جون سال ۲۰۱۸ امضا شده و به تبدیل به قانون شده‌است. این قانون از ابتدای ژانویه سال ۲۰۲۰ اجرایی خواهد شد

[4] – هوشی است که توسط ماشین‌ها ظهور پیدا می‌کند، در مقابل هوش طبیعی که توسط جانوران شامل انسان‌ها نمایش می‌یابد.

علاوه بر مزایای زیادی که دارند، نگرانی‌های زیادی نیز در خصوص حفظ حریم خصوصی به همراه دارند. هوش مصنوعی (AI)به عنوان یک زمینه فناوری گسترده، در بسیاری از صنایع و حوزه‌های مختلف زندگی انسانی کاربردهای متعددی دارد. (کاپلان[1]، ۲۰۱۹:۲۵-۱۵)در حوزه حفظ حریم خصوصی، هوش مصنوعی می‌تواند کاربردهای متعددی داشته باشد:

هوش مصنوعی می‌تواند به شناسایی و محافظت از اطلاعات حساس کاربران کمک کند. (بنافی، ۱۴۰۲: ۱۷۶-۱۴۹)به عنوان مثال، می‌توان از الگوریتم‌های یادگیری ماشین برای شناسایی و رمزگذاری داده‌های شخصی به طور خودکار استفاده کرد تا دسترسی غیرمجاز به آن‌ها محدود شود. با استفاده از هوش مصنوعی می‌توان تهدیدات امنیتی را به طور پیشرفته شناسایی کرد. این سیستم‌ها قادر به تحلیل رفتارهای مشکوک در شبکه‌ها و شناسایی حملات سایبری یا نقض حریم خصوصی به صورت خودکار هستند(جعفری و رهبرپور، ۱۳۹۶: ۷۴-۴۳).

هوش مصنوعی می‌تواند به شناسایی و حذف اطلاعات غیرمجاز یا نادرست که به نقض حریم خصوصی منجر می شود، کمک کند(گلی زاده: ۱۳۹۶، ۱۱-۱). به عنوان مثال، از AI برای شناسایی محتوای آسیب‌زننده یا اطلاعات خصوصی در شبکه‌های اجتماعی استفاده می‌شود. بسیاری از فناوری‌های مبتنی بر AI می‌توانند برای کنترل سطح دسترسی به اطلاعات شخصی در هنگام تعاملات آنلاین مورد استفاده قرار گیرند. ( دهقان‌پور فراشاه و رهبر: ۱۴۰۰، ۷۱۵-۶۹۵)به عنوان مثال، سیستم‌های AI می‌توانند تشخیص دهند که چه نوع اطلاعاتی باید برای حفظ حریم خصوصی کاربران مخفی یا فیلتر شود( قاسم‌زاده لیاسی و رئیسی دزکی، ۱۳۹۹: ۶۱۶-۵۹۷). با استفاده از هوش مصنوعی، می‌توان سیستم‌هایی برای حفظ حریم خصوصی به طور غیرمتمرکز طراحی کرد، به طوری که داده‌ها و اطلاعات شخصی تنها در اختیار خود کاربران باقی بماند و هیچ مرکز مرکزی به آن‌ها دسترسی نداشته باشد. هوش مصنوعی به عنوان ابزاری مفید می‌تواند برای تقویت حفاظت از حریم خصوصی و امنیت داده‌ها در دنیای دیجیتال امروز مورد استفاده قرار گیرد و به سیستم‌ها این توانایی را می‌دهند تا مانند انسان‌ها فکر کنند، یاد بگیرند و تصمیم‌گیری کنند. این سیستم‌ها می‌توانند وظایف مختلفی را از جمله پردازش داده‌ها، تحلیل اطلاعات، شبیه‌سازی تفکر انسان و حل مشکلات پیچیده انجام دهند. همچنین، هوش مصنوعی در بسیاری از زمینه‌های دیگر همچون حمل و نقل، ترافیک، سیاست‌گذاری، هنر و طراحی، موسیقی و غیره نیز کاربردهای متنوعی دارد. این فناوری در حال توسعه مداوم است و پتانسیل بالقوه‌ای برای تغییر زندگی انسان‌ها در آینده دارد.

## گفتار دوم: رویکردهای نظری حفظ حریم خصوصی در دوران هوش مصنوعی

منشور حقوق بشر بهترین چارچوب برای قاعده مند کردن هوش مصنوعی و حفظ حریم خصوصی می باشد. منشور حقوق بشر به‌طور کلی به حقوق اساسی و غیرقابل‌مساوم انسان‌ها پرداخته است، و به همین دلیل می‌تواند به‌عنوان چارچوبی ارزشمند برای قاعده‌مند کردن هوش مصنوعی و حفظ حریم خصوصی در دنیای دیجیتال مطرح شود. ترکیب اصول حقوق بشر با فناوری‌های نوین مانند هوش مصنوعی می‌تواند به ایجاد تعادل بین بهره‌برداری از مزایای این فناوری‌ها و حفاظت از حقوق افراد کمک کند. منشور حقوق بشر، که به عنوان یک سند بین‌المللی برای تأمین حقوق و آزادی‌های اساسی افراد شناخته می‌شود، می‌تواند به عنوان چارچوبی برای هدایت استفاده از هوش مصنوعی و حفظ حریم خصوصی عمل کند. در واقع، از آنجایی که هوش مصنوعی با جمع‌آوری و پردازش داده‌های شخصی ارتباط مستقیم دارد، اصول حقوق بشر می‌توانند راهنمایی‌های مهمی برای تضمین استفاده اخلاقی از این فناوری‌ها فراهم کنند.

### بند اول-نظریه حق به حریم خصوصی:

– یکی از مهم‌ترین اصول در منشور حقوق بشر، حق هر فرد به حریم خصوصی است. طبق اصول منشور حقوق بشر، هر فرد حق دارد که از حریم خصوصی خود محافظت کند. در زمینه هوش مصنوعی، این بدین معناست که باید اطمینان حاصل شود که داده‌های شخصی افراد تنها با رضایت آنها جمع‌آوری و پردازش می‌شود و استفاده از این داده‌ها باید شفاف و محدود به اهداف خاصی باشد. این حق به‌طور مستقیم در برابر جمع‌آوری و پردازش داده‌های شخصی توسط سیستم‌های هوش مصنوعی قرار می‌گیرد. اگر هوش مصنوعی به‌طور گسترده‌ای داده‌های حساس را جمع‌آوری کند، باید اطمینان حاصل شود که این داده‌ها با رضایت افراد جمع‌آوری می‌شوند و از دسترسی غیرمجاز به آن‌ها جلوگیری می‌شود این رویکر بر این اصل تأکید دارد که هر فرد حق دارد که اطلاعات خصوصی خود را کنترل کند و استفاده از آنها را تعیین کند. در زمینه هوش مصنوعی، این نظریه کمک می‌کند تا اطمینان حاصل کنیم که داده‌های شخصی فرد تنها با موافقت او یا با رعایت استانداردهای حفاظت از حریم خصوصی استفاده می‌شوند.(مولایی و حاجپور، ۱۳۹۷:۳۳۴-۲۰۹)

### بند دوم- نظریه حق برابری و عدم تبعیض:

[1]Kaplan

در استفاده از هوش مصنوعی، نباید هیچ فردی تحت تبعیض قرار گیرد. همه افراد باید از فرصت‌های برابر برای دسترسی به تکنولوژی‌ها و حقوق خود برخوردار باشند. این به معنای جلوگیری از تبعیض در فرآیندهای تصمیم‌گیری مبتنی بر هوش مصنوعی است. هوش مصنوعی باید به‌گونه‌ای طراحی و پیاده‌سازی شود که تبعیض نداشته باشد و به حقوق برابر افراد احترام بگذارد. الگوریتم‌های هوش مصنوعی ممکن است تحت تأثیر داده‌های نادرست یا تبعیض‌آمیز قرار گیرند و به نتایج ناعادلانه منجر شوند. بنابراین، ایجاد سیاست‌ها و دستورالعمل‌هایی برای تضمین عدم تبعیض در هوش مصنوعی از اهمیت ویژه‌ای برخوردار است. حق برابری و عدم تبعیض شامل حقوق اساسی همه افراد است که در برابر تکنولوژی‌های هوش مصنوعی مخاطراتی مانند تبعیض، نقض حریم خصوصی و کنترل غیرقانونی را به حقوق افراد تأمین می‌کند. این حقوق شامل حقوق به حریم خصوصی و حقوق به داده‌های شخصی نیز می‌شود.(صادقی، ۱۳۸۹: ۴۰)

**بند سوم-نظریه حق بر دسترسی به اطلاعات و شفافیت:**

هوش مصنوعی باید به گونه‌ای توسعه یابد که الگوریتم‌ها و فرآیندهای تصمیم‌گیری آنها برای کاربران شفاف و قابل درک باشد. افراد باید از چگونگی استفاده از داده‌های خود آگاه باشند و بدانند که چگونه تصمیمات هوش مصنوعی می‌تواند بر آنها تأثیر بگذارد. حق دسترسی به اطلاعات به افراد این امکان را می‌دهد که بدانند داده‌های شخصی‌شان چگونه جمع‌آوری و استفاده می‌شود. در حوزه هوش مصنوعی، شفافیت در عملکرد سیستم‌ها و تصمیمات آنها امری ضروری است. الگوریتم‌های یادگیری ماشین و دیگر مدل‌های هوش مصنوعی باید قابل توضیح باشند، به‌گونه‌ای که افراد بتوانند درک کنند چگونه داده‌هایشان پردازش و تصمیمات گرفته می‌شود. این رویکرد بر اهمیت حفظ حقوق در انتقال داده‌ها و اطلاعات تأکید دارد. در تکنولوژی‌های هوش مصنوعی، داده‌ها از منابع مختلف جمع‌آوری می‌شوند و باید اطمینان حاصل شود که این فرآیند با رعایت حقوق کاربران و صاحبان داده‌ها انجام می‌شود. این نظریه می‌تواند به تعیین مسائل مانند مالکیت داده‌ها، اجازه نحوه استفاده از آنها، و تضمین حقوق دسترسی معتبر کمک کند.(برتینو[1]،۲۰۱۹: ۱۶-۲۶)

**بند چهارم- نظریه حق بر آزادی بیان:**

حق آزادی بیان در منشور حقوق بشر یکی از اصول بنیادی است که بر آزادی افراد برای ابراز نظرات و دریافت اطلاعات بدون محدودیت تأکید دارد. این حق در زمینه هوش مصنوعی و حفظ حریم خصوصی می‌تواند به عنوان چارچوبی برای قاعده‌مند کردن توسعه و استفاده از این فناوری‌ها عمل کند. به این معنا که باید از آزادی بیان به‌عنوان ابزاری برای محافظت از حقوق افراد در دنیای دیجیتال بهره برداری شود، در حالی که در عین حال حقوق حریم خصوصی و امنیت داده‌ها نیز رعایت گردد. این حق به افراد این آزادی را می‌دهد که نظرات خود را بدون ترس از تبعات بیان کنند. در دنیای دیجیتال و با وجود هوش مصنوعی، حفظ این حق بسیار مهم است. اگر هوش مصنوعی در کنترل رسانه‌ها و شبکه‌های اجتماعی نقش دارد، باید اطمینان حاصل شود که این سیستم‌ها به‌طور عادلانه و بی‌طرفانه عمل می‌کنند و آزادی بیان کاربران را نقض نمی‌کنند. (انصاری، ۱۳۹۰،:۴۱)

**بند پنجم-نظریه حق بر تصمیم‌گیری آزادانه:**

نظریه «حق بر تصمیم‌گیری آزادانه»(طباطبایی پور، ۱۴۰۲ : ۵۳ ) که در منشور حقوق بشر به آن اشاره شده است، به معنای توانایی افراد برای اتخاذ تصمیمات مستقل و آزادانه در امور زندگی خود، به‌ویژه در زمینه‌های شخصی و اجتماعی، است. این حق شامل دسترسی به اطلاعات، انتخاب آزادانه بر اساس آگاهی و اراده خود، و حفاظت از آزادی‌های فردی است. در دنیای هوش مصنوعی، این نظریه می‌تواند چارچوبی برای قاعده‌مند کردن این فناوری و حفظ حریم خصوصی باشد. افراد باید حق داشته باشند که خود تصمیم بگیرند که آیا می‌خواهند داده‌های شخصی‌شان در سیستم‌های هوش مصنوعی پردازش شوند یا نه. این حق به معنای اختیار کامل افراد برای کنترل داده‌های شخصی خود است، به‌ویژه در زمینه‌هایی که ممکن است تصمیمات خودکار از طرف هوش مصنوعی بر زندگی افراد تأثیر بگذارد. نظریه «حق بر تصمیم‌گیری آزادانه» می‌تواند به عنوان چارچوبی برای تضمین اینکه هوش مصنوعی به‌طور شفاف، عادلانه، و با احترام به حریم خصوصی افراد طراحی و استفاده شود، عمل کند. این چارچوب به‌ویژه در جلوگیری از سوءاستفاده از داده‌ها و ایجاد سیستم‌های تبعیض‌آمیز نقش کلیدی دارد و به افراد این اطمینان را می‌دهد که تصمیمات آنها به‌طور آزادانه و بدون هیچ‌گونه فشار نادرست یا دخالت‌های خارجی گرفته می‌شود. (صادقی، ۱۳۸۹ : ۴۰)

**بند ششم-نظریه حق بر عدالت و دادرسی**

[1] Bertino

طبق منشور حقوق بشر، هر فرد باید از دسترسی به محاکمه عادلانه و منصفانه برخوردار باشد. این اصول می‌توانند به نحوه طراحی و استفاده از هوش مصنوعی در سیستم‌های قضائی و اجرائی کمک کنند تا از تصمیمات تبعیض‌آمیز یا ناعادلانه جلوگیری شود. الگوریتم‌های هوش مصنوعی که در فرآیندهای قانونی یا دادرسی استفاده می‌شوند باید شفاف، قابل‌ملاحظه و منصفانه باشند، تا به هیچ‌وجه حقوق انسانی فردی نقض نشود.طبق منشور حقوق بشر، حریم خصوصی افراد باید محافظت شود. در دنیای دیجیتال و با استفاده از هوش مصنوعی، حفظ حریم خصوصی یکی از چالش‌های اصلی است. از آنجا که بسیاری از مدل‌های هوش مصنوعی به داده‌های شخصی نیاز دارند، تدوین قوانین برای قاعده‌مند کردن استفاده از این داده‌ها و تضمین حریم خصوصی افراد به منظور جلوگیری از نقض حقوق بشر ضروری است. همچنین، در استفاده از هوش مصنوعی در فرآیندهای حقوقی، باید از امنیت داده‌ها و جلوگیری از استفاده‌های سوء از آن‌ها اطمینان حاصل شود. (طباطبایی پور، ۱۴۰۲: ۵۳ )

یکی از مهم‌ترین جنبه‌های تدوین چارچوب‌های حقوقی در استفاده از هوش مصنوعی، تعریف و نظارت بر اصول اخلاقی و حقوقی است که باید در طراحی و پیاده‌سازی الگوریتم‌ها رعایت شوند. اصولی مانند شفافیت، انصاف، و امکان‌پذیری برای نظارت و ارزیابی عملکرد سیستم‌های هوش مصنوعی برای حفظ عدالت و حقوق افراد از جمله مواردی هستند که در منشور حقوق بشر تأکید شده و می‌توانند به‌عنوان راهنما برای استفاده از هوش مصنوعی در زمینه‌های حقوقی و قضائی مورد توجه قرار گیرند. در صورتی که سیستم‌های هوش مصنوعی تصمیمات ناعادلانه‌ای درباره افراد بگیرند، افراد باید حق داشته باشند که به تصمیمات این سیستم‌ها اعتراض کنند و برای اصلاح آن‌ها اقدام کنند. این به‌ویژه در سیستم‌هایی که از هوش مصنوعی برای تصمیم‌گیری در امور حساس مانند استخدام، اعتبار مالی یا حتی نظام قضائی استفاده می‌شود، اهمیت دارد (براهویی، ۱۳۹۹: ۲۳ ).

### بند هفتم-نظریه مسئولیت‌پذیری و نظارت

نظریه مسئولیت‌پذیری و نظارت در منشور حقوق بشر می‌تواند چارچوب مهمی برای قاعده‌مند کردن هوش مصنوعی و حفظ حریم خصوصی افراد فراهم کند. این نظریه بر اهمیت شفافیت، مسئولیت‌پذیری و نظارت مؤثر بر فرآیندها و تصمیمات متمرکز است، به‌ویژه در زمینه‌هایی که ممکن است تأثیرات عمیق و بلندمدتی بر زندگی افراد و حقوق آنها داشته باشد. برای جلوگیری از سوءاستفاده و اطمینان از رعایت حقوق بشر، باید سیستم‌های هوش مصنوعی تحت نظارت و مسئولیت‌پذیری قرار گیرند. این به معنای ایجاد نهادهای مستقل برای نظارت بر توسعه و پیاده‌سازی هوش مصنوعی است که به بررسی تأثیرات اجتماعی و انسانی آن بپردازند(براهویی، ۱۳۹۹: ۲۳ ). نظریه مسئولیت‌پذیری و نظارت در منشور حقوق بشر برای قاعده‌مند کردن هوش مصنوعی و حفظ حریم خصوصی به‌ویژه از این جهت اهمیت دارد که می‌تواند چارچوبی فراهم کند که در آن حقوق انسان‌ها در برابر سوءاستفاده‌های ممکن توسط هوش مصنوعی محافظت شود(طباطبایی پور، ۱۴۰۲: ۵۳ )

منشور حقوق بشر می‌تواند چارچوبی اصولی و اخلاقی برای قاعده‌مند کردن هوش مصنوعی ارائه دهد. این اصول نه‌تنها به حفاظت از حقوق فردی و حریم خصوصی کمک می‌کند، بلکه تضمین می‌کند که هوش مصنوعی به‌طور عادلانه، شفاف و مسئولانه توسعه یابد. برای موفقیت در پیاده‌سازی این اصول، نیاز به همکاری میان دولت‌ها، شرکت‌ها و جوامع بین‌المللی است تا اطمینان حاصل شود که فناوری هوش مصنوعی به نفع همه افراد و جوامع عمل می‌کند.

## گفتار سوم: چالش‌ها و تهدیدهای حریم خصوصی در هوش مصنوعی

حق حریم خصوصی به عنوان یکی از حقوق افراد در تمامی جوامع مورد پذیرش قرار گرفته و احترام به حق حریم خصوصی و عدم نقض آن توسط افراد و حکومت مورد انتظار قانون‌گذاران می‌باشد؛ به عبارت دیگر چنان‌چه بدون مجوز قانونی حریم خصوصی افراد اعم از حریم ارتباطی، اطلاعاتی، جسمانی، مکانی و شخصیتی مورد تعرض قرار گیرد. مسئولیت حقوقی و کیفری به دنبال خواهد داشت. باید توجه داشت احترام به حریم خصوصی امری مطلق نیست؛ به عبارت دیگر در صورت تزاحم مصلحت فردی با مصالح اجتماعی و با تشخیص حاکم و مجوز قانونی امکان ورود به حریم خصوصی برای افراد ذی‌صلاح منتفی نمی‌باشد. البته این امر مورد تأکید قانون‌گذار می‌باشد که ورود به حریم خصوصی افراد جز به حکم قانون و رعایت مقررات و تحت نظارت مقام قضایی مجاز نیست و در هر صورت انجام اقدامات قضایی نباید به گونه‌ای اعمال شود که به کرامت و حیثیت افراد صدمه وارد نماید.

### بند اول-چالش‌های حقوقی نقض حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی

استفاده گسترده از داده‌های شخصی برای آموزش الگوریتم‌های هوش مصنوعی، به چالش حفظ حریم خصوصی افراد و کنترل بر داده‌های خود افراد می‌انجامد. الگوریتم‌های هوش مصنوعی ممکن است به دلیل برنامه‌ریزی نادرست یا داده‌های تبعیض‌آمیز، تبعیض ایجاد کنند و باعث نقض حقوق انسانی و عدالت اجتماعی شوند. کیفیت تصمیم‌گیری الگوریتم‌های هوش مصنوعی و ابهام در مسئولیت قانونی برای خسارت‌های

ناشی از این تصمیم‌گیری‌ها، یک چالش مهم حقوقی است. نیاز به شفافیت در استفاده از الگوریتم‌های هوش مصنوعی و اطمینان از شرکت‌پذیری در فرایندهای تصمیم‌گیری می‌تواند چالش‌هایی را ایجاد کند. اطمینان از اینکه هوش مصنوعی به طور عادلانه و بدون تبعیض، به همه افراد خدمت می‌کند، یکی از چالش‌های مهم حقوقی است. مسائل مربوط به حقوق مالکیت فکری در خصوص الگوریتم‌ها و داده‌های استفاده شده در هوش مصنوعی، نیاز به تعیین حقوق و توافقات قانونی دارند. تضمین اینکه فعالیت‌های هوش مصنوعی با قوانین موجود در حوزه‌های مختلف، از جمله حریم خصوصی، حقوق مصرف‌کننده و قوانین حقوق بشر، تطابق دارند، یک چالش مهم است. این چالش‌ها نشان می‌دهند که هوش مصنوعی به‌طور کلی نیاز به یک چارچوب حقوقی مناسب دارد تا از دیدگاه‌های حقوقی، اخلاقی و اجتماعی محافظت شود و به نفع انسان‌ها استفاده گردد.(تخشید، ۱۴۰۰ : ۲۵۰-۲۲۷) جلوه‌های نقض حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی می‌تواند به روش‌های مختلفی صورت گیرد. این نقض‌ها معمولاً به دلیل جمع‌آوری، پردازش و استفاده از داده‌های شخصی به صورت غیرمجاز یا غیرمناسب اتفاق می‌افتند:

- عدم شفافیت در استفاده از داده‌ها: در بسیاری از سیستم‌های مبتنی بر هوش مصنوعی، کاربران اغلب از نحوه جمع‌آوری، پردازش و استفاده از داده‌های شخصی خود بی‌خبر هستند. این مسئله به ویژه زمانی مشکل‌ساز می‌شود که داده‌ها به صورت گسترده برای مقاصد مختلف (مانند تبلیغات هدفمند، تحلیل رفتار و غیره) استفاده شوند. از این رو، ایجاد استانداردهای قانونی و اخلاقی برای شفاف‌سازی و آگاهی‌سازی کاربران در خصوص استفاده از داده‌های شخصی ضروری است.
- حفظ تعادل بین نوآوری و حقوق فردی یکی از بزرگترین چالش‌ها این است که در بسیاری از مواقع تکنولوژی‌های هوش مصنوعی ممکن است به سرعت گسترش یابند، اما از آن‌طرف نیاز است که از حقوق فردی و حریم خصوصی افراد محافظت شود. قوانین و دستورالعمل‌های موجود باید قادر باشند بین پیشرفت‌های فناوری و حفظ حقوق انسانی تعادل برقرار کنند.
- نقص در قوانین حفاظت از داده‌ها قوانین فعلی در بسیاری از کشورهای جهان هنوز نمی‌توانند به طور کامل نیازهای مربوط به حفاظت از داده‌های شخصی در عصر هوش مصنوعی را پوشش دهند. به‌طور مثال، ممکن است قوانینی مانند GDPR (مقررات عمومی حفاظت از داده‌ها) در برخی کشورها به‌خوبی اجرا نشود یا در شرایط خاص و به‌ویژه در مواجهه با فناوری‌های نوین مانند یادگیری ماشین و شناسایی چهره نواقصی داشته باشند.
- تهدیدات ناشی از نظارت بی‌رویه:فناوری‌های نظارتی مبتنی بر هوش مصنوعی، مانند سیستم‌های شناسایی چهره و تحلیل رفتار آنلاین، تهدیدی جدی برای حریم خصوصی افراد ایجاد می‌کنند. استفاده از این تکنولوژی‌ها بدون نظارت و چارچوب قانونی مناسب می‌تواند به سوءاستفاده‌های گسترده، نقض حریم خصوصی و آزادی‌های فردی منجر شود.
- تبعیض و پیش‌داوری‌های نادرست: بسیاری از سیستم‌های هوش مصنوعی به‌ویژه آن‌هایی که در فرآیند تصمیم‌گیری‌های مهم مانند استخدام، اعتبارسنجی یا حتی دسترسی به خدمات بهداشتی و اجتماعی به کار می‌روند، ممکن است به دلیل استفاده از داده‌های تاریخی و نادرست دچار پیش‌داوری و تبعیض شوند. این امر می‌تواند منجر به نقض حقوق بشر و تبعیض علیه اقلیت‌ها و گروه‌های آسیب‌پذیر شود.
- چالش‌های حقوق مالکیت داده‌ها: یکی دیگر از چالش‌های قانونی، تعیین مالکیت داده‌های جمع‌آوری‌شده توسط هوش مصنوعی است. آیا این داده‌ها متعلق به فردی است که اطلاعاتش جمع‌آوری شده، یا شرکت یا سازمانی که این داده‌ها را پردازش کرده است؟ این پرسش‌ها نیاز به پاسخ‌های قانونی روشن دارند تا حقوق افراد در قبال داده‌هایشان حفظ شود.
- امنیت داده‌ها و محافظت در برابر حملات سایبری: در صورت هک شدن یا سرقت داده‌های حساس، اطلاعات شخصی افراد می‌تواند در معرض خطر قرار گیرد. از آنجایی که هوش مصنوعی اغلب حجم عظیمی از داده‌ها را پردازش می‌کند، هرگونه نقض امنیتی می‌تواند پیامدهای جدی داشته باشد. به همین دلیل، نیاز به تقویت امنیت سایبری و قوانین مرتبط با حفاظت از داده‌ها بسیار ضروری است.
- مسئولیت‌پذیری در تصمیمات هوش مصنوعی: یکی از چالش‌های اخلاقی بزرگ این است که در صورت وقوع اشتباه یا نقض حقوق افراد به دلیل تصمیمات الگوریتمی، مسئولیت چه کسی است؟ اگر هوش مصنوعی باعث آسیب شود، آیا مسئولیت آن به عهده سازنده، کاربر یا خود سیستم است؟ این پرسش‌ها باید از لحاظ قانونی روشن شوند.
- مخاطرات در استفاده از داده‌های شخصی برای آموزش مدل‌های هوش مصنوعی: مدل‌های هوش مصنوعی معمولاً با استفاده از حجم وسیعی از داده‌های شخصی آموزش می‌بینند. استفاده از داده‌های حساس بدون رضایت آگاهانه فرد می‌تواند منجر به نقض حریم خصوصی و ایجاد خطرات امنیتی برای کاربران شود. به همین دلیل، قوانین باید محدودیت‌هایی برای استفاده از داده‌ها در فرآیند آموزش مدل‌ها وضع کنند.

- چالش‌های مربوط به نظارت بر هوش مصنوعی:نظارت و تنظیم دقیق بر استفاده از هوش مصنوعی در سطح جهانی یک چالش جدی است. بسیاری از کشورهای مختلف با قوانین متفاوت و استانداردهای گوناگون به این مسئله پرداخته‌اند. این تفاوت‌ها می‌تواند باعث ایجاد مشکلاتی برای کاربران بین‌المللی و حتی ایجاد فضای مبهم برای شرکت‌ها شود.رهبری و شعبانپور، ۱۴۰۰: ۴۴۴-۴۱۹)

حفظ حریم خصوصی در عصر تکنولوژی‌های هوش مصنوعی یک چالش پیچیده است که نیازمند یافتن راه‌حل‌های متعادل و جامع در حوزه‌های قانونی، اخلاقی و فناورانه است.

**بند دوم-چالش‌های اخلاقی نقض حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی**

جمع‌آوری و استفاده از داده‌های شخصی توسط شرکت‌ها و سازمان‌ها، به ویژه با پیشرفت تکنولوژی‌های هوش مصنوعی، مسائل اخلاقی و قانونی زیادی را به همراه دارد.

- جمع‌آوری داده‌های شخصی بدون رضایت: یکی از رایج‌ترین نقض‌ها، جمع‌آوری داده‌های شخصی بدون آگاهی و رضایت افراد است. بسیاری از سیستم‌های هوش مصنوعی مانند دستیارهای صوتی، سیستم‌های نظارتی و خدمات آنلاین، داده‌های کاربران را بدون اطلاع یا تایید قبلی جمع‌آوری می‌کنند. این داده‌ها می‌توانند شامل اطلاعات شخصی حساس مثل موقعیت جغرافیایی، تاریخچه جستجو، الگوهای رفتاری و حتی مکالمات صوتی باشند.
- استفاده غیرمجاز از داده‌ها: در بسیاری از موارد، داده‌های جمع‌آوری‌شده توسط هوش مصنوعی ممکن است به هدف‌هایی خارج از آنچه که برای آن‌ها جمع‌آوری شده است، استفاده شوند. به عنوان مثال، اطلاعات شخصی ممکن است به شرکت‌های تبلیغاتی یا دیگر نهادها فروخته شوند، بدون اینکه افراد از این استفاده مطلع باشند.(عباسی، ۱۳۹۹: 130-115)
- تحلیل و دستکاری داده‌ها: الگوریتم‌های هوش مصنوعی می‌توانند برای شبیه‌سازی رفتار انسان‌ها و دستکاری آنها استفاده شوند. این دستکاری می‌تواند شامل تغییرات در نحوه نمایش تبلیغات، جهت‌دهی به انتخاب‌های سیاسی یا حتی دستکاری در اطلاعات شخصی افراد باشد. استفاده از داده‌های نامناسب یا ناقص برای آموزش مدل‌های هوش مصنوعی می‌تواند به نتایج اشتباه یا ناعادلانه منجر شود. این اشتباهات می‌توانند پیامدهای منفی بر افراد و جوامع بگذارند. (فرزین و سمیعی، ۱۴۰۲: ۸-۱)

**گفتار چهارم : تبیین** سازوکارهای **حفاظت از حریم خصوصی در قبال چالش‌ها و تهدیدها**

**بند اول-سازوکارهای حقوقی تقویت حفظ حریم خصوصی**

برای تقویت حفظ حریم خصوصی، مجموعه‌ای از روش‌های حقوقی و قانونی وجود دارد که در اینجا به برخی از آن‌ها اشاره می‌کنیم:

-قوانین حریم خصوصی و حمایت از داده‌ها: مانند حق دسترسی به داده‌های شخصی در اتحادیه اروپا، حقوق مصرف‌کنندگان در کالیفرنیا، انتقال داده‌های شخصی در برزیل و حفاظت از اطلاعات پزشکی در آمریکا که حقوق مشخصی برای افراد در برابر داده‌های شخصی فراهم می‌آورند. این قوانین بر حقوق دسترسی، اصلاح، حذف و انتقال داده‌های شخصی و همچنین نیاز به رعایت استانداردهای حفاظتی در مورد اطلاعات شخصی تأکید دارند.

-استفاده از تکنولوژی‌های رمزنگاری و امنیت داده: بر اساس برخی قوانین حریم خصوصی، استفاده از رمزنگاری و امنیت داده‌ها می‌تواند برای حفظ حریم خصوصی بسیار مؤثر باشد. که شامل استفاده از رمزنگاری انتها به انتها، کنترل دسترسی و محافظت در برابر نفوذ است.

-سیاست‌های داخلی و توافقنامه‌های قراردادی: شرکت‌ها باید سیاست‌ها و رویه‌های داخلی را برای حفظ حریم خصوصی تدوین کنند که شامل گزینه‌هایی برای مدیریت و حذف داده‌های شخصی می‌شود. همچنین باید توافقنامه‌های مناسب با شرکای تجاری و ارائه دهندگان خدمات برای اطمینان از رعایت حفاظت از داده‌ها بست.

-آموزش و آگاهی‌بخشی: آموزش مستمر و آگاهی‌بخشی به کارکنان در مورد اهمیت حفظ حریم خصوصی و رعایت قوانین مرتبط از اهمیت بسزایی برخوردار است. کارکنان باید آگاه باشند که چگونه با داده‌های شخصی برخورد کنند و چگونه موارد خاصی مانند نقض داده‌های شخصی را گزارش دهند.

- تأمین مکانیسم‌های شکایت و حق رسیدگی: قوانین حریم خصوصی باید مکانیسم‌هایی را فراهم آورند که افراد بتوانند در صورت نقض حقوق حریم خصوصی خود شکایت کنند و دولت نیز باید مکانیسم‌هایی را برای رسیدگی به این شکایات فراهم آورد.(رهبری و شعبانپور، ۱۴۰۱: ۴۴۴-۴۱۹)

این روش‌ها نشان می‌دهند که حفظ حریم خصوصی به یک تلاش چند جانبه نیاز دارد که شامل تأمین حقوق قانونی، استفاده از فناوری‌های مناسب، توسعه سیاست‌های داخلی و آموزش و آگاهی‌بخشی است. این تلاش‌ها با همکاری افراد، شرکت‌ها و دولت‌ها می‌تواند به حفظ حریم خصوصی بهتری برسد.

### بند دوم-ساز و کارهای قانونی تقویت حفظ حریم خصوصی

توسعه و اجرای قوانین جدید برای تقویت حفظ حریم خصوصی از اهمیت بسیاری برخوردار است، به ویژه در دورانی که فناوری‌های دیجیتال و اطلاعات شخصی به طور فزاینده‌ای در زندگی روزمره و کسب و کارها جایگاه دارند. در اینجا چند نکته مهم برای توسعه و اجرای قوانین حفظ حریم خصوصی را بررسی می‌کنیم:

۱. توسعه قوانین مطلوب و جامع: قوانین باید جامع و شامل باشند و به طور دقیق به مسائلی مانند جمع‌آوری، استفاده، انتقال و حفظ داده‌های شخصی پرداخته شود. این قوانین باید با توجه به پیشرفت‌های فناوری و نیازهای جامعه به‌روزرسانی شوند.

۲. تأمین حقوق فردی: قوانین باید حقوق فردی مانند حق دسترسی، اصلاح، و حذف داده‌های شخصی را تأمین کنند. همچنین باید مکانیسم‌های شکایت و رسیدگی به نقایص را فراهم آورند.

۳. نظارت و اجرا: برای اطمینان از رعایت قوانین، نیاز به نظارت و اجرای مؤثر داریم. دولت‌ها باید نهادهای نظارتی قدرتمندی را تأسیس کنند و توانایی پیگیری و پاسخگویی به نقایص را داشته باشند.

۵. همکاری بین‌المللی: چون حریم خصوصی یک مسئله بین‌المللی است، همکاری بین‌المللی برای تطبیق قوانین و هماهنگی در مقابله با تهدیدات عبری به حریم خصوصی بسیار حیاتی است.

۶. تشویق به نوآوری و تکنولوژی: توسعه تکنولوژی‌هایی که به رعایت حریم خصوصی کمک می‌کنند، نیازمند حمایت و تشویق دولتی و خصوصی است. این شامل رمزنگاری قوی، فناوری‌های تشخیص و جلوگیری از نقض حریم خصوصی و ... (قاسم‌زاده لیاسی و رئیسی دزکی، ۱۳۹۹: ۶۱۶-۵۹۷)

### بند سوم-تبیین ساز و کارهای اثربخشی سیاست‌های حفظ حریم خصوصی در فناوری‌های مبتنی بر هوش مصنوعی

سیاست‌های حفظ حریم خصوصی در قرن ۲۱ اهمیت بسیاری پیدا کرده‌اند به دلیل پیشرفت‌های فناوری و افزایش نگرانی‌های مرتبط با حفظ حریم خصوصی افراد. این سیاست‌ها تأثیرات گسترده‌ای در جوامع و کسب و کارها داشته‌اند که به برخی از آنها اشاره می شود:

۱. تأمین حقوق فردی: سیاست‌های حفظ حریم خصوصی تضمین می‌کنند که افراد حقوقی مانند دسترسی به داده‌های خود، اصلاح اطلاعات نادرست و حذف داده‌های خود را دارند. این حقوق اساسی برای کنترل خود اطلاعات در دنیای دیجیتال است.

۲. محدودیت بر تجمع و استفاده از داده‌ها: قوانین حفظ حریم خصوصی محدودیت‌هایی را برای جمع‌آوری، استفاده و انتقال داده‌های شخصی اعمال می‌کنند. این اقدامات به کاهش خطر سواستفاده از اطلاعات شخصی کمک می‌کنند.

۳. تنظیمات امنیتی و حفاظتی: سیاست‌های حفظ حریم خصوصی اجباری می‌کنند که سازمان‌ها و شرکت‌ها برای حفاظت از داده‌های شخصی استانداردهای امنیتی را رعایت کنند. این شامل استفاده از رمزنگاری قوی، محافظت از دسترسی‌های غیرمجاز و اجرای سیاست‌های دسترسی است.

۴. توسعه فناوری با رعایت حریم خصوصی: توسعه فناوری‌های مبتنی بر حفظ حریم خصوصی مانند تکنولوژی‌های مبتنی بر رمزنگاری، سیستم‌های تشخیص نقض حریم خصوصی و ابزارهای مدیریت تنظیمات حریم خصوصی.

۵. تأثیرات اقتصادی و اجتماعی: سیاست‌های حفظ حریم خصوصی می‌توانند تأثیرات گسترده‌ای بر اقتصاد داشته باشند، از جمله تسهیل تجارت الکترونیکی و افزایش اعتماد عمومی به خدمات دیجیتال. (رهبری و شعبانپور، ۱۴۰۱: ۴۴۴-۴۱۹)

سیاست‌های حفظ حریم خصوصی در قرن ۲۱ نقش مهمی در تعادل بین استفاده از فناوری و حفظ حقوق شهروندان دارند و به تعمیق این فضای حقوقی و اجتماعی کمک می‌کنند که از اهمیت بسیاری برخوردار است.

حفظ حریم خصوصی در حوزه هوش مصنوعی یکی از چالش‌های اساسی و مهم است که در آینده نیازمند رویکردها و سیاست‌های جدیدی خواهد بود. اولین گام در حفظ حریم خصوصی در هوش مصنوعی، تعریف دقیقی از حریم خصوصی و حفاظت از اطلاعات شخصی است. که شامل قوانین و مقررات مشخصی برای جمع‌آوری، استفاده و انتقال داده‌ها توسط سامانه‌های هوش مصنوعی می‌شود. فناوری‌هایی مانند رمزنگاری قوی، مدیریت دسترسی داده‌ها، فناوری‌های محافظت از حریم خصوصی و کنترل داده‌ها می‌توانند به طراحی سامانه‌های هوش مصنوعی کمک کنند تا از حریم خصوصی کاربران حفاظت کنند. در طراحی سامانه‌های هوش مصنوعی، اهمیت ارتباط و تعامل موثر بین انسان

و ماشین، از جمله در مسائل مربوط به حریم خصوصی، بسیار حائز اهمیت است. رویکردهایی که انسان را در مدیریت داده‌ها و تصمیم‌گیری‌های مربوط به حریم خصوصی تقویت کنند، می‌توانند موثر باشند. تنظیمات پیش‌فرضی که از طرف سازندگان و متخصصان هوش مصنوعی برای حریم خصوصی تعیین می‌شود، می‌تواند به کاربران کمک کند تا از ابتدا در ارتباط با سامانه‌های هوش مصنوعی حق حریم خصوصی خود را به درستی تعیین کنند. توسعه و تدوین قوانین و مقررات جهانی برای حفظ حریم خصوصی در هوش مصنوعی، به عنوان یک چالش بزرگ، نیازمند همکاری بین المللی و توافقات بین کشوری است تا بتوان از حقوق اساسی هر فرد در این حوزه حفاظت کرد. با توجه به رشد سریع فناوری هوش مصنوعی، توجه به حریم خصوصی به عنوان یکی از اصول اساسی و اخلاقی در طراحی و استفاده از این فناوری، بسیار حائز اهمیت است تا از پیامدهای ناخواسته و منفی مانند نقض حریم خصوصی و نابرابری‌های دیجیتالی جلوگیری شود.(تخشید،۱۴۰۰: ۲۵۰-۲۲۷)

## نتیجه‌گیری

حریم خصوصی بخشی از زندگی هر فرد که در آن بازخواست و کیفر حقوقی نمی‌شود و دیگران بدون رضایت او حق ورود، کسب اطلاع و مداخله در آن را ندارند. افراد در حریم خصوصی خود استقلال در تصمیم‌گیری دارند. محدوده حریم خصوصی با توجه به نوع فرهنگ و حاکمیت جامعه، محدود یا گسترده خواهد شد. حقِ داشتن حریم خصوصی یا حق خلوت از پایه‌های تحقق حقوق بشر در نظام‌های مردم‌سالار دانسته شده که انسان را در مقابل تعرضات دیگران به زندگی خصوصی‌اش و نیز در برابر مداخلات دولت، مورد حمایت قرار می‌دهد. این حق از ارزشمندترین مفاهیم نظام‌های حقوقی محسوب شده که ارتباط تنگاتنگی با حفظ کرامت، حیثیت، آزادی، استقلال و تعیین سرنوشت انسان دارد و زمینه همزیستی مسالمت‌آمیز در جامعه را فراهم می‌آورد محدوده حریم خصوصی بسته به نوع فرهنگ حاکم بر جامعه از نظر مذهبی یا غیر مذهبی بودن و همچنین با توجه به نوع حاکمیت آن جامعه از نظر استبدادی یا دموکراتیک بودن، گسترده یا محدود خواهد بود. بررسی حقوقی حفظ حریم خصوصی در فناوری های مبتنی بر هوش مصنوعی نتایج متعددی را به دنبال دارد. حقوق حریم خصوصی معمولاً به طور مشخص در قوانین و مقررات تعریف شده است که چگونه داده‌های شخصی باید جمع‌آوری، ذخیره، استفاده و انتقال شوند. تکنولوژی‌های هوش مصنوعی نیز باید با این قوانین همخوانی داشته باشند، به خصوص اگر داده‌های حساسی مانند اطلاعات پزشکی یا مالی درگیر باشند. قوانین مسئولیت‌های خاصی برای توسعه‌دهندگان و استفاده‌کنندگان از تکنولوژی‌های هوش مصنوعی تعیین می کنند که شامل تضمین امنیت داده‌ها، اطمینان از حفظ حریم خصوصی کاربران و پاسخگویی در مواقع نقض حریم خصوصی است. حفظ حریم خصوصی در هوش مصنوعی می‌تواند تأثیرات گسترده‌ای بر اقتصاد و جامعه داشته باشد. به عنوان مثال، در صنایع حساس مانند بهداشت، تأمین و توزیع، حفظ حریم خصوصی می‌تواند به بهبود اعتماد مردم به سیستم‌های هوش مصنوعی کمک کند. برای حفظ حریم خصوصی، نیاز به نظارت و کنترل مناسب بر روی تکنولوژی‌های هوش مصنوعی و استفاده از آنها وجود دارد. که شامل استفاده از فناوری‌های مانیتورینگ و روش‌های ارزیابی برای اطمینان از پیروی از مقررات حریم خصوصی است. برای حفظ حریم خصوصی در هوش مصنوعی، می‌توان استفاده از استانداردها، راهنمایی‌ها و اصول بهینه‌سازی موردی از سوی سازمان‌های مختلف را در نظر گرفت. این استانداردها می‌توانند از توسعه و اجرای تکنولوژی‌های هوش مصنوعی با رویکردهای مناسب حمایت کنند. به طور کلی، حفظ حریم خصوصی در تکنولوژی‌های هوش مصنوعی نیازمند یک ترکیب مناسب از قوانین، فناوری، نظارت و مسئولیت‌پذیری است که به منظور تضمین احترام به حقوق اساسی کاربران و جامعه عمومی، لازم است.

## منابع


۱. انصاری، مهدی. (۱۳۹۰). نظریهٔ نقض کارآمد قرارداد از مکتب تحلیل اقتصادی حقوق. فصلنامهٔ حقوق، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی، ۴۱(۱).

۲. بنافی، فرشته. (۱۴۰۲). حفاظت از حقّ حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی. پژوهش حقوق خصوصی، ۱۲(۴۵)، ۱۴۹-۱۷۶.

۳. تخشید، زهرا. (۱۴۰۰). مقدمه‌ای بر چالش‌های هوش مصنوعی در حوزه مسئولیت مدنی. حقوق خصوصی، ۱۸(۱)، ۲۲۷-۲۵۰.

۴. جعفری، علی، رهبرپور، محمدرضا. (۱۳۹۶). مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه. پژوهش حقوق خصوصی، ۵(۱۸)، ۴۳-۷۴.

۵. دهقان‌پور فراشاه، سبحان، رهبر، نوید. (۱۴۰۰). بررسی خطرهای تهدیدکنندهٔ حریم خصوصی و الزامات حقوقی حمایت از آن در استفاده از وسایل نقلیهٔ خودران. مطالعات حقوق خصوصی، ۵۱(۴)، ۶۹۵-۷۱۵.

۶. رهبری، ابراهیم، شعبانپور، علی. (۱۴۰۱). چالش‌های کاربرد هوش مصنوعی به‌عنوان قاضی در دادرسی‌های حقوقی. فصلنامه تحقیقات حقوقی، ۲۵(ویژه‌نامه حقوق و فناوری)، ۴۱۹-۴۴۴.

۷. عباسی، عاطفه. (۱۳۹۹). گستره حریم خصوصی بیمار در فضای مجازی. حقوق پزشکی، ۱۴(۵۴)، ۱۱۵-۱۳۰. مولائی، یوسف، حاجی‌پور، مرتضی. (۱۳۹۷). اساسی‌سازی حقوق خصوصی. پژوهش حقوق عمومی، ۲۰(۶۱)، ۲۰۹-۲۳۴.

۸. براهویی، قاسم. (۱۳۹۹). بررسی حق حریم خصوصی با تکیه بر منشور حقوق شهروندی و قانون اساسی جمهوری اسلامی ایران. پایان‌نامه کارشناسی ارشد حقوق، دانشگاه تهران.

۹. طباطبایی پور، فاطمه سادات. (۱۴۰۲). حفاظت از حق بر حریم خصوصی در کاربرد سیستم‌های هوش مصنوعی. پایان‌نامه کارشناسی ارشد حقوق، دانشگاه شهید بهشتی.

۱۰. جمشیدی، سمیه. (۱۳۹۷). حریم خصوصی؛ قلمرو، مصادیق و تحلیل مبانی فقهی آن از منظر فقه امامیه. انتشارات استاد شهریار.

۱۱. کاسترن، کانی جی. (۱۴۰۲). حقوق حریم خصوصی با نگاهی به حقوق آمریکا. ترجمه دکتر سید احسان حسینی، انتشارات خرسندی، ۱۸-۱۹.

۱۲. رودینی، مهدی، میرلاشاری، مرجان، کباری، محبوبه سادات. (۱۴۰۲). حریم قانونی در هوش مصنوعی: راهکارهای بهداشتی برای نگه‌داری از اطلاعات در عصر جدید. هجدهمین کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک، شیروان، ۱-۸.

۱۳. گلی زاده، امین. (۱۳۹۶). قلمرو حریم خصوصی در قانون مجازات اسلامی مصوب ۱۳۹۲. دومین کنفرانس ملی حقوق، الهیات و علوم سیاسی، شیراز.

14. Bertino, E., Shawn M., Alina N., & Christine U. (2019). Redefining Data Transparency: A Multidimensional Approach. IEEE, 52(1), 16-26.
15. Bill Text. (2019). California Consumer Privacy Act of. Leginfo.legislature.ca.gov..
16. Gogol, A., & Kessler, M. (2021). AI, Privacy, and the Law: Navigating the Ethical Landscape. Journal of Privacy and Data Protection, 9(4), 102-120.
17. Chakraborty, S., & Sharma, R. (2020). Legal and Ethical Challenges in AI Privacy Protection. International Journal of Artificial Intelligence & Law, 28(2), 245-263.
18. Goodman, Bryce, & Flaxman, Seth. (2017). EU Regulations on Algorithmic Decision-Making and a "Right to Explanation". AI Magazine, 38(3),
19. Kaplan, Andreas, & Haenlein, Michael. (2019). Siri, Siri, in My Hand: Who's the Fairest in the Land? Business Horizons, 62.15-25.
20. Kuner, C., & Mantelero, A. (2022). Data Privacy in the Age of Artificial Intelligence: A Global Perspective. European Data Protection Law Review, 8(1), 34-50.
21. Mohanty, S., Cormican, K., & Dhanapathi, CH. (2022). More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. IEEE Transactions on Knowledge and Data Engineering.
22. Zeng, Y., & Zheng, S. (2023). AI Privacy and Ethics: A Comparative Study of Legal Frameworks. AI & Society, 38(2), 263-278.