فصلنامه علمی و حقوقی قانون یار
LICENSE NUMBER: 78864 ARTICLE COD:Y8SH33A52285 ISSN-P: 2538-3701

تأثیر هوش مصنوعی بر حق حریم خصوصی از منظر حقوق بشر

(تاریخ دریافت ۱۴۰۴/۰۲/۱۵، تاریخ تصویب ۱۴۰۴/۰۳/۰۳)

ابوذر گودرز قلعه نوئی

دانشجوی دکترای حقوق بین الملل عمومی دانشگاه آزاد اسلامی واحد کرمانشاه

دکتر فرامرز امجدیان [۱]

استادیارحقوق بین الملل ،عضوهیئت علمی تمام وقت، دانشگاه آزاد اسلامی واحد کرمانشاه

چکیده

با گسترش فزاینده فناوری‌های نوین، به‌ویژه هوش مصنوعی، مناسبات سنتی بشر با مفاهیم بنیادین حقوقی همچون حریم خصوصی دستخوش تحولات جدی شده است. هوش مصنوعی با قابلیت پردازش بی‌سابقه داده‌ها، شناسایی الگوها و پیش‌بینی رفتار انسان‌ها، در حوزه‌های مختلفی از جمله امنیت، سلامت، تبلیغات و حکمرانی به‌کار گرفته می‌شود. با این حال، همین ظرفیت‌ها نگرانی‌های عمیقی را در زمینه حفاظت از داده‌های شخصی و تحدید آزادی‌های فردی ایجاد کرده‌اند؛ مسائلی که مستقیماً با حقوق بشر، به‌ویژه حق بر حریم خصوصی، پیوند می‌خورند. این مقاله می کوشد با تکیه بر اسناد بین‌المللی حقوق بشر و رویه‌های نهادهای ذی‌ربط، تأثیرات چندوجهی هوش مصنوعی بر حریم خصوصی را تحلیل کند. پرسش اصلی آن است که آیا نظام حقوق بشر بین‌الملل، با چارچوب‌ها و ابزارهای فعلی خود، توانسته پاسخ مناسبی به چالش‌های نوظهور ناشی از فناوری‌های مبتنی بر هوش مصنوعی ارائه دهد یا خیر. در این مسیر، ضمن بررسی نمونه‌های کاربردی، تلاش می‌شود خلأهای موجود در تنظیم گری حقوقی شناسایی و راهکارهایی برای تقویت صیانت از حریم خصوصی در عصر دیجیتال ارائه گردد. یافته‌های این پژوهش نشان می‌دهد که اگرچه برخی اسناد و سیاست‌های

---

[۱] نویسنده مسئول

بین‌المللی گام‌هایی اولیه در جهت حفاظت از حریم خصوصی برداشته‌اند، اما برای مقابله مؤثر با پیچیدگی‌های هوش مصنوعی، نیاز به بازاندیشی در مفاهیم، تقویت مکانیزم‌های نظارتی، و توسعه چارچوب‌های الزام‌آور جهانی به‌شدت احساس می‌شود.

واژگان کلیدی: هوش مصنوعی؛ حریم خصوصی؛ حقوق بشر؛ داده‌های شخصی؛ تنظیم‌گری فناوری؛ حقوق بین‌الملل؛ اخلاق دیجیتال؛ نظارت الگوریتمی؛ اسناد بین‌المللی؛ عدالت اطلاعاتی

مقدمه

در دهه‌های اخیر، فناوری‌های نوین، به‌ویژه هوش مصنوعی[۱]، به یکی از تعیین‌کننده‌ترین عوامل در شکل‌دهی آینده جوامع انسانی بدل شده‌اند. هوش مصنوعی، با قابلیت‌های بی‌سابقه در تحلیل داده‌های کلان، یادگیری ماشین، و تصمیم‌گیری شبه‌انسانی، در عرصه‌هایی چون بهداشت، امنیت، آموزش، قضاوت، و حتی حاکمیت، نقش فزاینده‌ای ایفا می‌کند. در کنار مزایای غیرقابل انکار این فناوری، نگرانی‌هایی بنیادین در خصوص پیامدهای آن بر حقوق و آزادی‌های اساسی بشر، به‌ویژه حق بر حریم خصوصی، پدید آمده است. این حق، که به عنوان یکی از ارکان کرامت انسانی در اسناد بین‌المللی چون اعلامیه جهانی حقوق بشر (ماده ۱۲) و میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۷) به رسمیت شناخته شده، اکنون در معرض تهدیداتی قرار دارد که ماهیتی جدید و پیچیده دارند.

هوش مصنوعی با استفاده از الگوریتم‌های پیشرفته، قادر است داده‌های کاربران را بدون رضایت آگاهانه تحلیل کرده، رفتارهای فردی را پیش‌بینی نموده، و حتی در بسیاری از موارد، تصمیماتی با پیامدهای اجتماعی و حقوقی اتخاذ نماید. در چنین شرایطی، مرزهای سنتی میان فضای خصوصی و عمومی به شدت دچار تزلزل شده و مفهوم «رضایت» به‌عنوان یکی از ارکان بنیادین حفاظت از داده‌ها، در عمل، تضعیف شده است. افزون بر این، قابلیت‌های نظارتی حکومت‌ها و شرکت‌های بزرگ فناوری، به مدد هوش مصنوعی، به سطحی رسیده‌اند که بدون دخالت مستقیم انسانی، قادر به رهگیری، ارزیابی و قضاوت درباره کنش‌های افراد هستند. این پدیده به‌طور جدی سوالاتی را درباره توازن میان منافع عمومی و حقوق فردی، و نیز حدود مشروع مداخلات فناورانه در زندگی خصوصی انسان‌ها، مطرح می‌سازد.

[۱] Artificial Intelligence

اهمیت و ضرورت پرداختن به این موضوع، نه‌تنها به‌خاطر وسعت و عمق تحولات فناورانه، بلکه به دلیل تأثیرات بالقوه و بالفعل آن بر نظم حقوقی بین‌المللی و اصول بنیادین حقوق بشر است. اگرچه بسیاری از کشورها اقدام به تدوین مقررات مرتبط با حفاظت از داده‌ها کرده‌اند، اما هنوز یک چارچوب جهانی الزام‌آور برای نظارت بر توسعه و استفاده از هوش مصنوعی از منظر حقوق بشر وجود ندارد. در نتیجه، این مقاله می‌کوشد به خلأهای قانونی موجود در زمینه حفاظت از حریم خصوصی در عصر هوش مصنوعی بپردازد و راهکارهایی برای مواجهه با این چالش نوظهور ارائه دهد.

۲-مفهوم‌شناسی و چارچوب نظری

۲-۱-تعریف و انواع هوش مصنوعی

هوش مصنوعی به مجموعه‌ای از فناوری‌ها و الگوریتم‌ها اطلاق می‌شود که به سیستم‌های ماشینی امکان می‌دهد وظایفی را انجام دهند که معمولاً به هوش انسانی نیاز دارند. این وظایف شامل یادگیری، استدلال، حل مسئله، درک زبان طبیعی، و در موارد پیشرفته‌تر، تصمیم‌گیری مستقل است. هرچند تعریف دقیقی که مورد اجماع همه صاحب‌نظران باشد هنوز وجود ندارد، اما تعریفی کاربردی آن است که هوش مصنوعی توانایی سیستم‌های کامپیوتری در تقلید و بازتولید رفتارهای شناختی انسان‌هاست.

هوش مصنوعی از منظر عملی به دو دسته کلی تقسیم می‌شود:

۱-هوش مصنوعی محدود[۱]:که برای انجام یک وظیفه خاص طراحی شده است، مانند دستیارهای صوتی، الگوریتم‌های پیشنهاد محتوا، یا سامانه‌های شناسایی چهره.

[۱] Narrow AI

۲-هوش مصنوعی عمومی[۱]: که توانایی درک، یادگیری و تطبیق با محیط‌های مختلف را همانند انسان داراست، و هنوز در مرحله تحقیقاتی و نظری قرار دارد.

با توجه به سرعت رشد این فناوری، مرز میان این دو دسته در حال کمرنگ شدن است. امروزه، بسیاری از سیستم‌های یادگیری ماشین[۲] و یادگیری عمیق[۳] در قالب هوش مصنوعی محدود فعالیت می‌کنند اما آثار اجتماعی و حقوقی عمیقی از خود بر جای می‌گذارند.

۲-۲- مفهوم حق حریم خصوصی در حقوق بشر

حق بر حریم خصوصی یکی از حقوق بنیادین بشر است که به معنای برخورداری از فضایی امن و آزاد برای زندگی فردی، خانوادگی، و ارتباطات بدون نظارت یا مداخله بی‌دلیل دولت یا دیگر اشخاص است. این حق، که با مفاهیمی چون آزادی اندیشه، کرامت انسانی و امنیت اطلاعات در پیوند است، در هسته نظام‌های حقوق بشری جای دارد. در اعلامیه جهانی حقوق بشر (۱۹۴۸)، ماده ۱۲ مقرر می‌دارد که "هیچ کس نباید در زندگی خصوصی، خانوادگی، مسکونی یا مکاتبات خود مورد دخالت خودسرانه قرار گیرد." همچنین در میثاق بین‌المللی حقوق مدنی و سیاسی[۴] ماده ۱۷ تأکید می‌کند که این حق باید از سوی قانون تضمین شود. حق حریم خصوصی، گرچه ابتدا بیشتر بر مسائل خانوادگی و مکاتبات تمرکز داشت، اما امروزه با گسترش فضای دیجیتال، به حوزه‌های جدیدی مانند داده‌های الکترونیکی، ارتباطات آنلاین، و رفتارهای دیجیتال گسترش یافته است.

برخورداری از حریم خصوصی، به افراد امکان می‌دهد که هویت شخصی و استقلال فردی خود را حفظ کنند. در واقع، بدون حریم خصوصی، دیگر حقوق بنیادین مانند آزادی بیان، آزادی اندیشه، و

---

۱ General AI
۲ Machine Learning
۳ Deep Learning
۴ ICCPR

آزادی تجمع نیز در معرض تهدید قرار می‌گیرند. به همین دلیل، حفاظت مؤثر از این حق در عصر فناوری‌های پیشرفته از اهمیتی دوچندان برخوردار است.

۳-۲- رابطه هوش مصنوعی و داده‌های شخصی

در قلب عملکرد بسیاری از سامانه‌های هوش مصنوعی، داده‌های شخصی انسان‌ها قرار دارد. این داده‌ها شامل اطلاعات رفتاری، بیومتریک، ارتباطات، موقعیت جغرافیایی، ترجیحات فردی، و حتی حالات روانی می‌شود. الگوریتم‌های هوش مصنوعی از طریق تجزیه و تحلیل این اطلاعات، الگوهایی را کشف می‌کنند که به آن‌ها توانایی پیش‌بینی رفتار و تصمیم‌گیری مستقل می‌دهد. این فرایند، در عین کارایی بالا، مخاطرات جدی برای حریم خصوصی به‌همراه دارد. نخست آنکه در بسیاری موارد، کاربران از میزان داده‌هایی که از آن‌ها جمع‌آوری می‌شود، آگاه نیستند یا رضایت واقعی و آگاهانه‌ای ارائه نمی‌دهند. دوم آنکه استفاده از داده‌ها در حوزه‌هایی چون پلیس پیش‌بینی‌گر، رتبه‌بندی اعتباری، یا تبلیغات هدفمند، می‌تواند به تصمیماتی منجر شود که اثرات عمیقی بر زندگی اشخاص دارند، بدون آنکه خود افراد در این تصمیم‌گیری‌ها نقشی داشته باشند. همچنین، مسأله تبعیض الگوریتمی[۱] نیز در این زمینه مطرح است. اگر داده‌هایی که به الگوریتم آموزش داده می‌شوند دارای سوگیری باشند، هوش مصنوعی نیز به بازتولید و حتی تشدید آن‌ها خواهد پرداخت. این موضوع ممکن است نه‌تنها حریم خصوصی، بلکه اصل برابری و کرامت انسانی را نیز به مخاطره اندازد.

٤-۲-اسناد بین‌المللی مرتبط

حقوق بشر در سطح بین‌المللی بر پایه اسناد کلیدی استوار است که در آن‌ها به صراحت به حق حریم خصوصی اشاره شده است. مهم‌ترین این اسناد عبارت‌اند از:

[۱] Algorithmic Bias

۱-اعلامیه جهانی حقوق بشر[۱]-ماده ۱۲

۲-میثاق بین‌المللی حقوق مدنی و سیاسی[۲]-ماده ۱۷

۳-کنوانسیون اروپایی حقوق بشر[۳]-ماده ۸

۴-کنوانسیون شماره ۱۰۸ شورای اروپا درباره حفاظت از افراد در ارتباط با پردازش خودکار داده‌های شخصی

۵-قانون عمومی حفاظت از داده‌های اتحادیه اروپا[۴]

۶-اصول راهنمای سازمان ملل درباره کسب‌وکار و حقوق بشر

هرچند برخی از این اسناد به دوره‌ای تعلق دارند که هنوز فناوری‌های نوین ظهور نیافته بودند، اما تفسیرهای به‌روز نهادهای حقوق بشری نشان می‌دهد که این اسناد ظرفیت گسترش مفهومی برای پوشش تحولات جدید را دارند. برای مثال، کمیته حقوق بشر سازمان ملل در تفسیر عمومی شماره ۱۶ بر لزوم حفاظت از حریم خصوصی در برابر فناوری‌های نوظهور تأکید کرده است. با این حال، خلأهایی نیز وجود دارد: بسیاری از کشورها هنوز مقررات مشخصی درباره الگوریتم‌ها و تصمیم‌گیری خودکار ندارند. همچنین، نبود یک رژیم بین‌المللی الزام‌آور برای نظارت بر توسعه و استفاده از هوش مصنوعی، موجب شده که اعمال محدودیت‌های مؤثر بر نقض حریم خصوصی دشوار باشد.

[۱] UDHR
[۲] ICCPR
[۳] ECHR
[۴] GDPR

در مجموع، این بخش نشان می‌دهد که تعامل هوش مصنوعی با حق حریم خصوصی، ترکیبی پیچیده از فرصت‌ها و تهدیدهاست؛ تعاملی که تنها از طریق تحلیل مفهومی دقیق، شناخت ابعاد حقوقی و بین‌المللی، و بازنگری در ابزارهای موجود حقوق بشر می‌توان برای آن راهکارهایی پایدار یافت.

۳-چالش‌های هوش مصنوعی برای حریم خصوصی

۳-۱-جمع‌آوری و تحلیل داده‌های بزرگ توسط الگوریتم‌ها

یکی از ویژگی‌های برجسته هوش مصنوعی، توانایی آن در جمع‌آوری، پردازش و تحلیل حجم عظیمی از داده‌ها است. این داده‌ها شامل اطلاعات شخصی، رفتاری، مکانی و حتی بیومتریک افراد می‌شود. الگوریتم‌های یادگیری ماشین با تحلیل این داده‌ها، الگوهایی را کشف می‌کنند که می‌توانند برای پیش‌بینی رفتارها، تصمیم‌گیری‌های خودکار و حتی تأثیرگذاری بر انتخاب‌های فردی مورد استفاده قرار گیرند. این فرآیند، هرچند از نظر فنی پیشرفته و کارآمد است، اما نگرانی‌های جدی در خصوص حریم خصوصی افراد ایجاد می‌کند. بسیاری از کاربران از میزان و نوع داده‌هایی که از آن‌ها جمع‌آوری می‌شود، آگاه نیستند و رضایت آگاهانه‌ای برای استفاده از این اطلاعات نداده‌اند. علاوه بر این، استفاده از داده‌های حساس بدون شفافیت و کنترل مناسب، می‌تواند منجر به نقض حقوق بنیادین افراد شود. طبق گزارش‌های منتشر شده، استفاده از هوش مصنوعی در تحلیل داده‌های بزرگ، به‌ویژه در حوزه‌های تجاری و امنیتی، بدون رعایت اصول اخلاقی و حقوقی، خطرات جدی برای حریم خصوصی افراد به‌همراه دارد.

۳-۲-نظارت دولتی و کنترل اجتماعی

دولت‌ها در سراسر جهان به‌طور فزاینده‌ای از فناوری‌های هوش مصنوعی برای نظارت بر شهروندان استفاده می‌کنند. این نظارت می‌تواند شامل پایش فعالیت‌های آنلاین، تحلیل رفتارهای اجتماعی، و

حتی پیش‌بینی اقدامات آینده افراد باشد. در برخی موارد، این فناوری‌ها برای کنترل اجتماعی و سرکوب مخالفت‌ها به‌کار گرفته می‌شوند.

برای مثال، استفاده از سامانه‌های شناسایی چهره در فضاهای عمومی، بدون رضایت افراد، می‌تواند منجر به نقض حریم خصوصی و آزادی‌های مدنی شود. همچنین، تحلیل داده‌های مکالمات و پیام‌های شخصی توسط الگوریتم‌های هوش مصنوعی، بدون نظارت و شفافیت کافی، خطرات جدی برای حقوق بشر به‌همراه دارد.

گزارش‌ها حاکی از آن است که گسترش نظارت مبتنی بر هوش مصنوعی، به‌ویژه در کشورهایی با نظام‌های غیر دموکراتیک، منجر به تقویت ابزارهای سرکوب و تضعیف آزادی‌های اساسی شده است.

۳-۳-استفاده از هوش مصنوعی در امنیت، پلیس پیش‌بینی‌گر، شناسایی چهره

کاربرد هوش مصنوعی در حوزه‌های امنیتی، به‌ویژه در پلیس پیش‌بینی‌گر و سامانه‌های شناسایی چهره، نگرانی‌های متعددی را در خصوص حریم خصوصی و تبعیض ایجاد کرده است. پلیس پیش‌بینی‌گر با تحلیل داده‌های گذشته، مناطقی را که احتمال وقوع جرم در آن‌ها بیشتر است، شناسایی می‌کند. اما این رویکرد می‌تواند منجر به تقویت تبعیض‌های موجود و هدف‌گیری ناعادلانه برخی جوامع شود.

سامانه‌های شناسایی چهره نیز، با جمع‌آوری و تحلیل تصاویر افراد در فضاهای عمومی، می‌توانند بدون رضایت آن‌ها، اطلاعات حساس را ذخیره و استفاده کنند. این فناوری‌ها، در صورت عدم نظارت و تنظیم‌گری مناسب، می‌توانند به ابزارهایی برای نقض حریم خصوصی و آزادی‌های فردی تبدیل شوند.

مطالعات نشان داده‌اند که استفاده از هوش مصنوعی در حوزه‌های امنیتی، بدون در نظر گرفتن اصول حقوق بشر و عدالت، می‌تواند منجر به نقض حقوق افراد و تضعیف اعتماد عمومی به نهادهای امنیتی شود.

٤-۳-خطرات تبعیض الگوریتمی و نقض اصل برابری

الگوریتم‌های هوش مصنوعی، در صورتی که بر اساس داده‌های مغرضانه یا ناقص آموزش ببینند، می‌توانند تبعیض‌های موجود در جامعه را بازتولید و حتی تشدید کنند. این تبعیض‌ها می‌توانند بر اساس نژاد، جنسیت، مذهب، یا سایر ویژگی‌های فردی باشند.

برای مثال، در فرآیندهای استخدام، الگوریتم‌هایی که بر اساس داده‌های تاریخی آموزش دیده‌اند، ممکن است به‌طور ناعادلانه‌ای افراد را بر اساس جنسیت یا نژاد رد یا قبول کنند. همچنین، در حوزه‌های مالی و اعتباری، استفاده از الگوریتم‌های مغرضانه می‌تواند منجر به تبعیض در اعطای وام یا خدمات مالی شود.

این تبعیض‌های الگوریتمی، نه‌تنها اصل برابری را نقض می‌کنند، بلکه می‌توانند اعتماد عمومی به فناوری‌های هوش مصنوعی را نیز تضعیف کنند. بنابراین، ضروری است که در طراحی و پیاده‌سازی این الگوریتم‌ها، اصول عدالت، شفافیت و پاسخ‌گویی رعایت شود.

در مجموع، چالش‌های مطرح‌شده نشان می‌دهند که استفاده از هوش مصنوعی بدون نظارت و تنظیم‌گری مناسب، می‌تواند منجر به نقض حریم خصوصی، تبعیض و تضعیف حقوق بشر شود. بنابراین، ضروری است که چارچوب‌های حقوقی و اخلاقی مناسبی برای استفاده از این فناوری‌ها تدوین و اجرا شود.

٤-واکنش نظام حقوق بشر بین‌الملل

٤-١-مواضع نهادهای حقوق بشری (کمیته حقوق بشر، شورای حقوق بشر سازمان ملل و ...)

در پاسخ به تهدیدات جدیدی که فناوری‌های هوش مصنوعی برای حریم خصوصی و حقوق بشر به‌وجود آورده‌اند، نهادهای بین‌المللی حقوق بشری به‌ویژه کمیته حقوق بشر و شورای حقوق بشر سازمان ملل، مواضع مهمی اتخاذ کرده‌اند. این نهادها تلاش کرده‌اند تا با تفسیر و توسعه اصول حقوق بشر، به چالش‌های ناشی از گسترش استفاده از هوش مصنوعی و نظارت دیجیتال پاسخ دهند.

کمیته حقوق بشر سازمان ملل در تفسیر عمومی شماره ۳۶ (۲۰۱۸) خود بر لزوم حفظ حریم خصوصی در دنیای دیجیتال تأکید کرده است. این تفسیر تأکید دارد که تمامی اشکال نظارت، جمع‌آوری و پردازش داده‌ها باید مطابق با اصول حقوقی همچون ضرورت، تناسب و شفافیت انجام شوند. کمیته همچنین به کشورها توصیه کرده است که از پیاده‌سازی فناوری‌هایی که می‌توانند به نقض حقوق بشر منجر شوند، خودداری کنند.

شورای حقوق بشر سازمان ملل نیز در چندین قطعنامه، از جمله قطعنامه ۲۷/۴۶ (۲۰۲۱) که به بررسی اثرات حقوق بشر ناشی از استفاده از هوش مصنوعی می‌پردازد، از کشورهای عضو خواسته است که مراقب تهدیداتی باشند که هوش مصنوعی برای حقوق خصوصی، آزادی‌های فردی، و برابری ایجاد می‌کند. شورا به‌ویژه از نقض حریم خصوصی از طریق فناوری‌های نظارتی مانند شناسایی چهره، هشدار داده و خواستار تنظیم مقررات سخت‌گیرانه‌تری در این زمینه شده است.

همچنین، در سطح گزارشگران ویژه حقوق بشر، گزارش‌های متعددی به تحلیل چالش‌های جدید ناشی از گسترش فناوری‌ها در زمینه‌های مختلف مانند حریم خصوصی، آزادی بیان، و نظارت دولتی

پرداخته است. این گزارش‌ها بیشتر بر لزوم برخورد با موارد سوءاستفاده از داده‌ها و ایجاد شفافیت در پردازش آن‌ها تأکید دارند.

۲-٤-ارزیابی کنش دولت‌ها در تراز با اسناد حقوق بشری

در سطح جهانی، دولت‌ها واکنش‌های متفاوتی به چالش‌های مرتبط با هوش مصنوعی نشان داده‌اند. برخی کشورها به‌ویژه در اروپا و برخی کشورهای آسیایی، به سرعت تلاش کرده‌اند تا مقرراتی برای نظارت و محدود کردن استفاده از هوش مصنوعی وضع کنند، در حالی که کشورهای دیگر به دلیل محدودیت‌های سیاسی و قانونی، واکنش‌های کندتری داشته‌اند.

در اتحادیه اروپا، به‌ویژه پس از تصویب قانون حفاظت از داده‌های عمومی[۱]، توجه ویژه‌ای به حفاظت از حریم خصوصی و داده‌های شخصی شده است. مقررات AI اتحادیه اروپا (۲۰۲۱)، که در حال بررسی است، قرار است معیارهای جدیدی برای استفاده از هوش مصنوعی در اروپا معرفی کند و از جمله تاکید دارد بر محدود کردن کاربردهایی چون شناسایی چهره در فضاهای عمومی.

در آمریکا، دولت‌ها به‌طور کلی به شفافیت و نظارت دقیق‌تر بر هوش مصنوعی توجه زیادی ندارند. با این حال، برخی ایالت‌ها مانند کالیفرنیا با تصویب قوانینی مانند قانون شفافیت نظارتی[۲] تلاش کرده‌اند که حقوق حریم خصوصی شهروندان را در برابر فناوری‌های نوین حفظ کنند.

در برخی کشورهای اسلامی نیز، حقوق حریم خصوصی در برخی سیستم‌های حقوقی به‌ویژه در زمینه حفاظت از داده‌ها، تحت تأثیر تفسیرهای دینی قرار دارد. برای مثال، در برخی کشورهای خاورمیانه، محدودیت‌های قانونی برای جمع‌آوری و پردازش داده‌ها به‌ویژه در حوزه‌های مرتبط با دین و اعتقادات مذهبی مشاهده می‌شود. در عین حال، چالش‌های نوظهور در این کشورها مربوط به مدیریت

[۱] GDPR
[۲] California Consumer Privacy Act

نظارت‌های دیجیتال، برخورد با گروه‌های مخالف سیاسی و استفاده از فناوری‌های نوین در حوزه‌های امنیتی است.

از این رو، برخی کشورها نه‌تنها مقرراتی برای هوش مصنوعی وضع نکرده‌اند بلکه بر اساس شرایط سیاسی و اجتماعی خود، ممکن است استفاده از این فناوری‌ها را به ابزارهایی برای نظارت اجتماعی تبدیل کنند که مغایر با استانداردهای بین‌المللی حقوق بشر باشد.

۳-٤-تحلیل تطبیقی مقررات منطقه‌ای (اروپا، آمریکا، کشورهای اسلامی)

تحلیل مقررات منطقه‌ای نشان می‌دهد که کشورهای مختلف، بر اساس چارچوب‌های قانونی و فرهنگی خود، برخوردهای متفاوتی با تهدیدات هوش مصنوعی دارند.

۱-اروپا:اروپا پیشرو در تدوین مقررات برای هوش مصنوعی و حفظ حریم خصوصی بوده است. مهم‌ترین نمونه این رویکرد، قانون GDPR است که از سال ۲۰۱۸ در کشورهای اتحادیه اروپا اجرایی شده است و به‌طور ویژه بر حفظ داده‌های شخصی و حق حریم خصوصی تأکید دارد. علاوه بر آن، اتحادیه اروپا در تلاش است تا اولین مقررات جامع هوش مصنوعی را وضع کند که شامل استانداردهایی برای استفاده از فناوری‌های نوین مانند شناسایی چهره و هوش مصنوعی در تصمیم‌گیری‌های خودکار می‌شود.

۲-آمریکا:در آمریکا، مقررات موجود بیشتر پراکنده و در سطح ایالتی هستند. دولت فدرال همچنان اقدامی جامع برای تنظیم استفاده از هوش مصنوعی در مقیاس ملی نداشته است. اگرچه برخی ایالت‌ها مانند کالیفرنیا قوانینی در زمینه حفاظت از داده‌ها دارند، اما از آن‌جا که آمریکا به‌طور کلی به‌دنبال نظارت دقیق بر فناوری‌های نوین نیست، لزوم استانداردسازی این قوانین و تجدید نظر در سیاست‌های ملی به شدت احساس می‌شود.

۳-کشورهای اسلامی:در کشورهای اسلامی، نظارت دیجیتال و جمع‌آوری داده‌ها به‌ویژه در کشورهای با سیستم‌های سیاسی بسته، موضوعات پیچیده‌ای هستند. در حالی که برخی کشورها مانند امارات متحده عربی به تنظیم قوانین برای حفاظت از داده‌های شخصی پرداخته‌اند، در برخی دیگر از کشورها، به‌ویژه در حوزه‌های امنیتی و نظارت اجتماعی، استفاده از هوش مصنوعی در ابعاد مختلف بدون نظارت دقیق و کافی ادامه دارد.

٤-٤-نقد کارآمدی ابزارهای موجود و خلأهای قانونی

با وجود تلاش‌های گسترده‌ای که در سطح بین‌المللی و ملی برای تنظیم استفاده از هوش مصنوعی صورت گرفته است، ابزارهای موجود همچنان با چالش‌های جدی مواجه‌اند. یکی از بزرگ‌ترین خلأهای قانونی، عدم تطابق سرعت پیشرفت فناوری‌ها با توسعه قوانین و مقررات است. قوانین موجود در بسیاری از کشورها، که عمدتاً مربوط به دهه‌ها پیش هستند، نمی‌توانند به‌طور کامل تهدیدات نوین هوش مصنوعی را پوشش دهند.

از سوی دیگر، حتی در کشورهایی که تلاش کرده‌اند مقررات دقیقی وضع کنند، همچنان خلأهای جدی در زمینه اجرای این قوانین وجود دارد. بسیاری از قوانین حفاظت از داده‌ها، علی‌رغم پیشرفت‌های قانونی، همچنان نتوانسته‌اند به‌طور مؤثر از داده‌های حساس و حریم خصوصی شهروندان در برابر سوءاستفاده‌های هوش مصنوعی محافظت کنند. برخی از منتقدان نیز بر این باورند که بسیاری از مقررات موجود، مانندGDPR ، نیاز به اصلاح و به‌روز رسانی دارند تا با چالش‌های جدید هوش مصنوعی تطابق پیدا کنند. در این راستا، پیشنهادهایی همچون ایجاد چارچوب‌های قانونی جهانی برای هوش مصنوعی و تقویت همکاری‌های بین‌المللی به‌منظور اجرای مؤثر قوانین و مقررات به طور فراگیر مطرح شده است. در مجموع، این بخش نشان می‌دهد که در حالی که برخی کشورها و نهادهای بین‌المللی تلاش‌های قابل توجهی برای مدیریت تهدیدات هوش مصنوعی انجام داده‌اند، هنوز بسیاری

از خلأهای قانونی و چالش‌های اجرایی وجود دارند که نیازمند توجه جدی و اصلاحات گسترده در سطح جهانی هستند.

۵- راهکارها و سیاست‌گذاری مطلوب

۱-۵-طراحی مقررات الزام‌آور برای هوش مصنوعی

برای مقابله با چالش‌های ناشی از استفاده گسترده و بی‌ضابطه از فناوری‌های هوش مصنوعی، نیاز به طراحی مقررات الزام‌آور و شفاف در سطح بین‌المللی و ملی احساس می‌شود. این مقررات باید به گونه‌ای تدوین شوند که نه‌تنها از حریم خصوصی افراد محافظت کنند، بلکه از توسعه و به‌کارگیری فناوری‌های هوش مصنوعی در جهت منافع عمومی و در راستای حقوق بشر حمایت نمایند.

یک چارچوب قانونی جامع برای هوش مصنوعی باید شامل چندین بخش کلیدی باشد:

۱-مقررات حفاظت از داده‌ها: یکی از اساسی‌ترین ابعاد مقررات هوش مصنوعی باید به حفاظت از داده‌های شخصی و حساس افراد بپردازد. در این راستا، مقررات مشابه قانون حفاظت از داده‌های عمومی اتحادیه اروپا GDPR که تضمین‌کننده حریم خصوصی افراد در برابر فناوری‌های نوین است، می‌تواند به‌عنوان الگو مورد استفاده قرار گیرد.

۲-محدودیت‌ها در کاربرد فناوری‌های نظارتی: کشورها باید برای استفاده از فناوری‌هایی چون شناسایی چهره و ردیابی رفتارهای آنلاین، محدودیت‌های قانونی قائل شوند. این محدودیت‌ها باید مطابق با اصول حقوق بشر و در چارچوب نیازهای امنیتی و اجتماعی باشند.

۳-پاسخ‌گویی و نظارت: طراحی مقررات باید سازوکارهایی برای نظارت مستقل بر عملکرد الگوریتم‌ها و مدل‌های هوش مصنوعی ایجاد کند تا اطمینان حاصل شود که این فناوری‌ها به‌طور عادلانه و منصفانه به کار گرفته می‌شوند. مقررات الزام‌آور می‌توانند از برخوردهای خودسرانه و

غیرقانونی با داده‌ها و اطلاعات شخصی جلوگیری کرده و یک چارچوب حقوقی پایدار برای استفاده از هوش مصنوعی به‌وجود آورند.

۲-۵-شفافیت الگوریتمی و پاسخ‌گویی‌پذیری

یکی از اصلی‌ترین چالش‌ها در استفاده از هوش مصنوعی، عدم شفافیت در نحوه عملکرد الگوریتم‌ها و تصمیم‌گیری‌های خودکار است. این مسأله به‌ویژه زمانی حادتر می‌شود که این الگوریتم‌ها بر زندگی افراد تأثیرگذار باشند، مانند تصمیمات مربوط به اعتبار مالی، استخدام یا نظارت‌های امنیتی. برای این که هوش مصنوعی به ابزاری عادلانه و مسئول تبدیل شود، لازم است که سیستم‌های تصمیم‌گیری الگوریتمی شفاف و قابل‌فهم باشند.

شفافیت الگوریتمی به این معناست که سازمان‌ها و دولت‌ها باید به‌طور دقیق توضیح دهند که چگونه از داده‌ها استفاده می‌کنند، چه الگوریتم‌هایی در تصمیم‌گیری‌های خود به کار می‌برند و این الگوریتم‌ها بر اساس کدام اصول عمل می‌کنند. این شفافیت به افراد این امکان را می‌دهد که بفهمند چرا و چگونه تصمیمات به نفع یا ضررشان اتخاذ می‌شود.

پاسخ‌گویی‌پذیری به این معناست که در صورت بروز خطا یا تبعیض از سوی الگوریتم‌ها، باید امکان پیگیری و بررسی وجود داشته باشد. سازوکارهای قانونی باید تضمین کنند که افراد آسیب‌دیده از استفاده نادرست از هوش مصنوعی بتوانند به‌راحتی به مقامات ذی‌صلاح شکایت کنند و در صورت نیاز، اصلاحات صورت گیرد.

شفافیت و پاسخ‌گویی‌پذیری از دو جنبه مهم برخوردارند:

۱-اعتماد عمومی: برای اینکه افراد به فناوری‌های هوش مصنوعی اعتماد کنند، باید مطمئن شوند که این فناوری‌ها به‌طور شفاف و عادلانه عمل می‌کنند.

۲-پیشگیری از تبعیض و نقض حقوق: شفافیت در طراحی و عملکرد الگوریتم‌ها می‌تواند مانع از ایجاد تبعیض‌های ناعادلانه و نقض حقوق بشر شود. این موضوع در زمینه‌هایی چون استخدام، سلامت، و آموزش اهمیت بیشتری پیدا می‌کند.

برای تحقق شفافیت الگوریتمی، نهادهای حقوقی می‌توانند از سازوکارهای نظارتی مستقل برای ارزیابی و نظارت بر الگوریتم‌ها استفاده کنند.

۳-۵-حق بر کنترل داده و رضایت آگاهانه

یکی از اصول بنیادین در حقوق بشر، حق افراد بر کنترل داده‌های شخصی خود است. در دنیای دیجیتال، که حجم زیادی از اطلاعات افراد جمع‌آوری می‌شود، این حق بیش از پیش اهمیت پیدا کرده است. افراد باید قادر باشند که بدانند چه داده‌هایی از آن‌ها جمع‌آوری می‌شود، برای چه مقاصدی مورد استفاده قرار می‌گیرد و چه مدت زمانی نگهداری می‌شود.

رضایت آگاهانه به این معناست که افراد باید توانایی انتخاب و آگاهی کامل از پیامدهای تصمیمات خود داشته باشند. در زمینه هوش مصنوعی، این به‌معنای داشتن اختیار کامل برای موافقت یا مخالفت با جمع‌آوری و پردازش داده‌های شخصی است. باید اطمینان حاصل شود که افراد به‌طور کامل از نحوه استفاده از داده‌های خود آگاه هستند و این فرآیند بدون فشار یا گمراهی صورت می‌گیرد.

ایجاد سامانه‌های مدیریت داده که امکان دسترسی و اصلاح داده‌ها را به افراد بدهند، و همچنین سیستم‌های رضایت‌گیری دیجیتال که به وضوح هدف از جمع‌آوری داده‌ها و استفاده از آن‌ها را شرح دهند، می‌تواند به تحقق این حق کمک کند. افراد باید بتوانند در هر زمان به‌راحتی رضایت خود را پس بگیرند و داده‌های خود را حذف کنند.

حقوق مربوط به کنترل داده باید در قالب قوانین و مقرراتی چون GDPR به‌طور فراگیر پیاده‌سازی شوند و کشورها موظف به رعایت آن باشند.

٤-٥-نقش نهادهای بین‌المللی در تنظیم‌گری اخلاقی و حقوقی

در جهانی که فناوری‌های هوش مصنوعی به‌طور فزاینده‌ای بر جوامع مختلف تأثیر می‌گذارند، نهادهای بین‌المللی می‌توانند نقش محوری در تدوین و اجرای قوانین و مقررات مشترک ایفا کنند. این نهادها، با ارائه چارچوب‌های اخلاقی و حقوقی، می‌توانند به کشورهای مختلف کمک کنند تا به‌طور هماهنگ با چالش‌های هوش مصنوعی مقابله کنند و از حقوق بشر در برابر خطرات این فناوری‌ها محافظت کنند.

نهادهای سازمان ملل متحد، کمیسیون اروپا و سازمان توسعه و همکاری اقتصادی[1] از جمله نهادهایی هستند که در تدوین استانداردهای بین‌المللی برای هوش مصنوعی نقش دارند. این نهادها باید:

۱-ایجاد اصول اخلاقی جهانی: تدوین اصول اخلاقی مشترک برای هوش مصنوعی که کشورهای عضو موظف به رعایت آن باشند، به‌ویژه در زمینه‌هایی چون حفظ حریم خصوصی، جلوگیری از تبعیض، و شفافیت در فرآیندهای تصمیم‌گیری.

۲-همکاری بین‌المللی در زمینه نظارت و تنظیم‌گری: تقویت همکاری‌ها بین کشورهای مختلف برای نظارت بر استفاده از هوش مصنوعی و ایجاد ساختارهای مشترک برای مقابله با چالش‌های فناوری‌های نوین.

۳-آموزش و آگاهی‌بخشی: نهادهای بین‌المللی باید به کشورهای مختلف کمک کنند تا ظرفیت‌های خود را برای تنظیم‌گری و استفاده مسئولانه از هوش مصنوعی افزایش دهند. این موضوع از طریق

[1] OECD

آموزش، برگزاری کارگاه‌های آموزشی، و توسعه منابع آگاه‌سازی عمومی امکان‌پذیر است. نهادهای بین‌المللی همچنین باید در راستای تنظیم سیاست‌های جهانی، از برقراری معاهدات بین‌المللی و مقررات جهانی برای هوش مصنوعی حمایت کنند.

نتیجه‌گیری

در این مقاله، به بررسی تأثیر هوش مصنوعی بر حریم خصوصی از منظر حقوق بشر پرداخته شد.این تحلیل شامل مفهوم‌شناسی هوش مصنوعی، چالش‌های آن برای حقوق بشر، واکنش نهادهای بین‌المللی و دولت‌ها، و ارائه راهکارهای مناسب برای تنظیم‌گری و سیاست‌گذاری بود. هدف این تحقیق، بررسی نحوه تعامل هوش مصنوعی با حریم خصوصی و حقوق بشر در دنیای دیجیتال و همچنین تحلیل راهکارهایی برای ایجاد یک تعادل میان پیشرفت‌های فناوری و حفظ حقوق انسانی بوده است.

الف-جمع‌بندی یافته‌ها

یکی از اصلی‌ترین یافته‌های این تحقیق، پیچیدگی و چندوجهی بودن چالش‌های هوش مصنوعی برای حریم خصوصی است. فناوری‌های هوش مصنوعی می‌توانند به‌طور گسترده‌ای داده‌های شخصی را جمع‌آوری و پردازش کنند، به‌ویژه در زمینه‌هایی چون شناسایی چهره، نظارت اجتماعی، و پیش‌بینی رفتارهای فردی. این امر موجب نگرانی‌هایی درباره نقض حریم خصوصی و آزادی‌های فردی شده است. علاوه بر این، استفاده از هوش مصنوعی در بخش‌هایی مانند پلیس پیش‌بینی‌گر، تحلیل داده‌های بزرگ، و نظارت اجتماعی می‌تواند تبعات منفی‌ای چون تبعیض الگوریتمی، نقض حقوق بشر و عدم شفافیت در فرآیندهای تصمیم‌گیری به همراه داشته باشد.

در واکنش به این تهدیدات، نهادهای بین‌المللی نظیر کمیته حقوق بشر سازمان ملل، شورای حقوق بشر، و اتحادیه اروپا اقدامات مختلفی را برای تضمین احترام به حقوق بشر در دنیای دیجیتال پیشنهاد داده‌اند. این اقدامات، اگرچه در برخی موارد مؤثر بوده‌اند، اما هنوز نواقصی در کارآمدی آن‌ها وجود

دارد و به‌ویژه در زمینه‌هایی چون نظارت و تنظیم‌گری بین‌المللی هوش مصنوعی، خلأهایی وجود دارد.

ب-پاسخ به پرسش‌های تحقیق

پاسخ به پرسش‌های تحقیق نشان می‌دهد که:

۱-هوش مصنوعی و حریم خصوصی ارتباط پیچیده‌ای دارند که نیازمند راهکارهای حقوقی و اخلاقی خاص است. از یک سو، استفاده از هوش مصنوعی می‌تواند به بهره‌برداری غیرمجاز از داده‌های شخصی منجر شود و از سوی دیگر، می‌تواند با پیشرفت‌های مثبت در زمینه‌های بهداشتی، آموزشی و امنیتی، زندگی افراد را بهبود بخشد

۲-تهدیدات اصلی برای حریم خصوصی ناشی از هوش مصنوعی شامل جمع‌آوری و پردازش داده‌های شخصی بدون رضایت آگاهانه، نظارت‌های اجتماعی بدون محدودیت، و تبعیض‌های الگوریتمی هستند. این تهدیدات می‌توانند اصول اساسی حقوق بشر، از جمله حق بر حریم خصوصی، آزادی‌های فردی، و برابری را نقض کنند.

۳-واکنش نظام حقوق بشر بین‌الملل و دولت‌ها نشان‌دهنده تلاش‌های متعددی برای ایجاد تعادل میان استفاده از هوش مصنوعی و احترام به حقوق بشر است، اما هنوز هم چالش‌های اساسی در زمینه تدوین قوانین و مقررات جامع وجود دارد.

۴-پاسخ‌های عملی برای مقابله با چالش‌ها شامل طراحی مقررات الزام‌آور برای هوش مصنوعی، ایجاد شفافیت در الگوریتم‌ها، ضمانت‌های قوی برای کنترل داده‌ها، و نقش مؤثر نهادهای بین‌المللی در تنظیم‌گری اخلاقی و حقوقی است.

ج-ارائه پیشنهادهای کاربردی و مسیرهای آینده تحقیق

با توجه به یافته‌های این تحقیق، پیشنهادات زیر می‌تواند به بهبود وضعیت موجود و حفاظت بهتر از حریم خصوصی در مواجهه با هوش مصنوعی کمک کند:

۱-طراحی مقررات جامع و الزام‌آور برای هوش مصنوعی: تدوین مقررات شفاف و جامع برای استفاده از هوش مصنوعی که به‌طور خاص بر حفاظت از حریم خصوصی و جلوگیری از سوءاستفاده از داده‌های شخصی تمرکز دارد، امری ضروری است. کشورها و نهادهای بین‌المللی باید در این راستا همکاری کنند و قوانینی نظیر GDPR را به‌عنوان الگویی برای تنظیم استفاده از هوش مصنوعی پیاده‌سازی نمایند.

۲-ایجاد شفافیت الگوریتمی و سیستم‌های نظارتی مستقل: سازمان‌ها و دولت‌ها باید به‌طور شفاف توضیح دهند که چگونه از داده‌های شخصی استفاده می‌کنند و الگوریتم‌ها به چه نحوی تصمیم‌گیری می‌کنند. این شفافیت می‌تواند به‌طور قابل‌توجهی از نگرانی‌های عمومی در زمینه نقض حقوق بشر جلوگیری کند. همچنین، نظارت مستقل بر عملکرد الگوریتم‌ها برای اطمینان از عدم تبعیض و برخورد منصفانه با افراد، از جمله اقداماتی است که باید مدنظر قرار گیرد.

۳-تقویت حقوق افراد برای کنترل داده‌های خود و رضایت آگاهانه: افراد باید از حق کنترل داده‌های شخصی خود برخوردار باشند و این اختیار را داشته باشند که رضایت آگاهانه خود را برای پردازش داده‌ها اعطا کنند. همچنین، باید سازوکارهای قانونی برای جلوگیری از دسترسی غیرمجاز به داده‌ها و بازنگری در استفاده از آن‌ها وجود داشته باشد.

۴-نقش مؤثر نهادهای بین‌المللی در تنظیم‌گری جهانی هوش مصنوعی: نهادهای بین‌المللی باید در زمینه تنظیم‌گری اخلاقی و حقوقی هوش مصنوعی نقش پیشرو ایفا کنند. این نهادها می‌توانند با تدوین

اصول و استانداردهای جهانی و ایجاد سازوکارهای نظارتی مشترک، از توسعه هوش مصنوعی در راستای حفظ حقوق بشر و حریم خصوصی حمایت کنند.

در مسیر آینده تحقیق، توجه به توسعه مدل‌های هوش مصنوعی به‌صورت مسئولانه و اخلاقی و تأثیر آن‌ها بر دیگر ابعاد حقوق بشر، از جمله حق بر برابری و عدالت، می‌تواند محوری برای پژوهش‌های آینده باشد. به‌ویژه در زمینه‌های تطبیقی و تحلیل‌های حقوقی بین‌المللی، بررسی چگونگی تطابق قوانین ملی با الزامات جهانی و تجربه‌های مختلف کشورها در تنظیم‌گری هوش مصنوعی، می‌تواند به غنای مباحث حقوق بشر در دنیای دیجیتال کمک کند.

در مجموع، با تدوین سیاست‌ها و مقررات دقیق و با همکاری بین‌المللی، می‌توان از هوش مصنوعی به‌عنوان ابزاری مفید و مسئولانه استفاده کرده و هم‌زمان از تهدیدات آن برای حریم خصوصی و حقوق بشر جلوگیری کرد.

منابع و مآخذ

۱.European Union General Data Protection Regulation (GDPR)

Official website of the EU: https://gdpr.eu/

۲.United Nations Human Rights Office (OHCHR) UN Human Rights Committee, General Comment No. ۱۶ on Article ۱۷ of the International Covenant on Civil and Political Rights (ICCPR)

۳.Cohen, J. E. (۲۰۱۹). “The Regulatory State in the Age of Artificial Intelligence”

Journal of Technology in Society, ۳۳(۲), ۲۹-۴۵.

۴.Tufekci, Z. (۲۰۱۵). “Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency” Journal of Information Technology and Politics, ۱۲(۴), ۴۰۰-۴۱۵.

۵.Binns, R. (۲۰۱۸). “Fairness in Machine Learning: Lessons from Political Philosophy” Proceedings of the ۲۰۱۸ CHI Conference on Human Factors in Computing Systems.

۶.Privacy International (۲۰۱۸). “The Role of Artificial Intelligence in Human Rights and Privacy” Privacy International Report.

۷.The Council of Europe Convention ۱۰۸ for the Protection of Individuals with regard to Automatic Processing of Personal Data (۱۹۸۱) Council of

Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/۱۰۸

۸.O'Flaherty, M. (۲۰۱۶). "The Right to Privacy in the Digital Age: Global Perspectives" Cambridge University Press.

۹.Zeng, Z., et al. (۲۰۲۰). "Artificial Intelligence in the Eyes of Human Rights Law"

Harvard International Law Journal, ۶۱(۲), ۱۵۰-۱۷۵.

۱۰.Floridi, L. (۲۰۱۴). "The Fourth Revolution: How the Infosphere is Reshaping Human Reality" Oxford University Press.

- **منابع قانونی**

۱.Universal Declaration of Human Rights (UDHR) United Nations General Assembly Resolution ۲۱۷ A (III), ۱۹۴۸.

۲.International Covenant on Civil and Political Rights (ICCPR) United Nations, ۱۹۶۶.

۳.The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data OECD, ۲۰۱۳.

- **کتاب‌ها**

۱.Privacy in the Age of Big Data: Recognizing the Harmful Effects of Data Collection, Analytics, and Algorithms" Theresa A. Pardo.

۲.“The Fourth Industrial Revolution” Klaus Schwab.

۳.“Artificial Intelligence: A Guide for Thinking Humans” Melanie Mitchell.

۴.“The Ethics of Artificial Intelligence and Robotics” Vincent C. Müller.

۵.“Privacy and Big Data: The Players, Regulators, and Stakeholders” Terence Craig وMary E. Ludloff.

۶.“Artificial Intelligence and Human Rights: The Legal and Ethical Challenges” Chris Reed.

۷.“Digital Privacy: Theory, Technologies, and Practices” Alessandro Acquisti, Curtis Taylor وLiad Wagman.

۸.“Big Data, Big Brother? Privacy and Public Safety in the Age of Surveillance” David Lyon.

۹.“The Right to Privacy” Jeffrey Rosen.

۱۰.“Law and the Regulation of Technology” Roger Brownsword وKaren Yeung.