Journal of Islamic Human Rights
Volum 1, Consecutive Number 1, 2024
Journal Homepage: https://islamichumanrights.ir/

Human Rights Considerations of Using Artificial Intelligence in the Fight Against Terrorist Crimes

Peyman Namamian[1], Mehrdad Teymouri[2*]

1. Associate Professor, Department of Law, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran.

2. Assistant Professor, Department of Criminal Law and Criminology, Tabriz Branch, Islamic Azad University, Tabriz, Iran. dr.mehrdad.teymouri@iau.ac.ir

Abstract

The use of predictive artificial intelligence in combating terrorist crimes often has a detrimental impact on human rights and creates suspicions of "pre-crime" punishment and surveillance. However, the regular use of new capabilities may increase the ability of governments to protect citizens' right to life, while improving adherence to principles that protect other human rights, such as transparency, proportionality, and freedom from unfair discrimination. This same regulatory framework can also help protect against the broader misuse of related technologies. The research method of this article is theoretical and library data collection tool, and the data analysis method is descriptive-analytical; Based on the findings and results of the research, it indicates that most countries focus on preventing terrorist attacks instead of reacting to terrorist attacks. Therefore, prediction is effective in fighting terrorist crimes. AI allows higher volumes of data to be analyzed and may perceive patterns in this data that, for reasons of volume and dimension, would otherwise be beyond the capacity of human interpretation. The effect of this is that traditional methods of investigation that depart from known suspects may be supplemented by methods that analyze the activity of a large portion of the entire population to identify previously unknown threats.

Keywords: Artificial Intelligence, Terrorist Crimes, Police, Human Dignity, Human Rights

- Namamian, P., Teymouri, M. (2024). Human Rights Considerations of Using Artificial Intelligence in the Fight Against Terrorist Crimes, *Journal of Islamic Human Rights*, 2(1), 1-18.

مجله حقوق بشر اسلامی
دورۀ اول ـ شمارۀ اول ـ ۱۴۰۳
صفحات ۱-۱۸ (مقاله پژوهشی)
تاریخ: دریافت ۱۴۰۳/۰۶/۳۰ـ پذیرش ۱۴۰۳/۰۹/۲۷ ـ انتشار ۱۴۰۳/۱۰/۱

ملاحظات حقوق بشری استفاده از هوش مصنوعی در مبارزه با جرایم تروریستی

پیمان نمامیان[۱]، مهرداد تیموری[۲*]

۱. دانشیار، گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران.
۲. استادیار، گروه حقوق جزا و جرم شناسی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران.
dr.mehrdad.teymouri@iau.ac.ir

چکیده

استفاده از هوش مصنوعی پیش‌بینی‌کننده در مقابله با جرایم تروریستی معمولاً تأثیر مخربی بر حقوق بشر دارد و شبهاتی از مجازات و نظارت «قبل از جنایت» ایجاد می‌کند. با این حال، استفاده منظم از قابلیت‌های جدید ممکن است توانایی‌های دولت‌ها را برای حمایت از حقوق شهروندان برای زندگی افزایش دهد و درعین‌حال پایبندی به اصولی را که برای حمایت از سایر حقوق بشر ازجمله شفافیت، تناسب و آزادی از تبعیض ناعادلانه است، بهبود بخشد. همین چارچوب نظارتی همچنین می‌تواند به محافظت در برابر سوءاستفاده گسترده‌تر از فناوری‌های مرتبط کمک کند. روش پژوهش این مقاله از نوع نظری و ابزار جمع‌آوری داده کتابخانه‌ای بوده و روش تجزیه و تحلیل داده به صورت توصیفی ـ تحلیلی می‌باشد؛ که براساس یافته‌ها و نتایج پژوهش حاکی از این است که بیشتر کشورها به جای واکنش به حملات تروریستی، بر پیشگیری از حملات تروریستی تمرکز می‌کنند. به این ترتیب، پیش‌بینی در مبارزه با جرایم تروریستی مؤثر است. هوش مصنوعی اجازه می‌دهد تا حجم بالاتری از داده‌ها تجزیه و تحلیل شود و ممکن است الگوهایی را در این داده‌ها درک کند که به دلایل حجم و ابعاد، در غیر این صورت فراتر از ظرفیت تفسیر انسانی است. تأثیر این امر این است که روش‌های سنتی تحقیقات که از مظنونین شناخته شده خارج می‌شوند، ممکن است با روش‌هایی تکمیل شوند که فعالیت بخش وسیعی از کل جمعیت را برای شناسایی تهدیدهای ناشناخته قبلی تجزیه و تحلیل می‌کنند.

کلیدواژه: هوش مصنوعی، جرایم تروریستی، پلیس، کرامت انسانی، حقوق بشر

- نمامیان، پیمان؛ تیموری، مهرداد. (۱۴۰۳). ملاحظات حقوق بشری استفاده از هوش مصنوعی در مبارزه با جرایم تروریستی، مجله حقوق بشر اسلامی، ۲(۱)، صفحات ۱-۱۸.

مقدمه

نقض حریم خصوصی مرتبط با تجزیه و تحلیل خودکار انواع خاصی از داده‌های عمومی در اصل اشتباه نیست، اما تجزیه و تحلیل باید در چارچوب قانونی و سیاستی قوی انجام شود که براساس نتایج آن، محدودیت‌های معقولی را برای مداخلات ایجاد کند. در آینده، دسترسی گسترده‌تر به جنبه‌های کمتر مزاحم داده‌های عمومی، تنظیم مستقیم نحوه استفاده از آن داده‌ها «ازجمله نظارت بر فعالیت‌های بازیگران بخش خصوصی» و تحمیل تدابیر فنی و نظارتی ممکن است هم عملکرد عملیاتی و هم انطباق با قانون حقوق بشر مهم است که هرگونه چنین اقداماتی به‌گونه‌ای انجام شود که به تأثیر آن بر سایر حقوق مانند آزادی بیان و آزادی تشکل و اجتماع حساس باشد.

سیاست ضد تروریستی بین حفظ امنیت یک جمعیت و احترام به حقوق فردی برای حفظ حریم خصوصی و آزادی‌هایی مانند آزادی بیان، انجمن و مذهب تعادل ایجاد می‌کند (Brokenshire, 2013: 1). تحولات جدید فناوری می‌تواند اجرای این سیاست‌ها را با وادار کردن مقامات به بررسی مجدد نحوه مبارزه با جرایم تروریستی به چالش بکشد. اقدامات انجام می‌شود (Cornish, 2010: 888). هوش مصنوعی یکی از این فناوری‌ها است. این مقاله توضیح می‌دهد که چگونه هوش مصنوعی می‌تواند از نظر تئوری به عملیات ضد تروریستی کمک کند و همچنین برخی از مناطقی که قبلاً از آن استفاده می‌شود. برخی از مشکلات استفاده فعلی از هوش مصنوعی برای این اهداف را ارائه می‌کند و محدودیت‌های عملی و پیامدهای حقوق بشر را بررسی می‌کند. همچنین فرصت‌ها و خطرات ناشی از افزایش استفاده از هوش مصنوعی را به‌عنوان بخشی از فعالیت‌های ضد جرایم تروریستی توسط دولت‌ها در نظر می‌گیرد. این موضوع نشان می‌دهد که استفاده از هوش مصنوعی در مبارزه با جرایم تروریستی ذاتاً اشتباه نیست و برخی از شرایط لازم برای استفاده مشروع از هوش مصنوعی را به‌عنوان بخشی از رویکرد پیش‌بینی‌کننده برای مقابله با جرایم تروریستی از سوی کشورهای لیبرال دموکرات پیشنهاد می‌کند. استفاده از هوش مصنوعی در مبارزه با جرایم تروریستی بر ایجاد پیش‌بینی‌های دقیق متمرکز است که به هدایت منابع برای مقابله با جرایم تروریستی کمک می‌کند. هوش مصنوعی پیش‌بینی‌کننده همچنین ممکن است نفوذ غیرضروری به اکثریت جمعیت را به حداقل برساند و تعصبات انسانی را در تصمیم‌گیری کاهش دهد. در عصری که جمع‌آوری،

ذخیره و تجزیه و تحلیل داده‌های افشاگرانه در مقیاس بزرگ در مورد فعالیت‌ها و انجمن‌های فردی افراد آسان‌تر می‌شود، روش‌های پیش‌بینی ممکن است به‌طور فزاینده‌ای اهمیت پیدا کنند، جایی که بتوانند به‌طور دقیق توجه را به مناطق یا افرادی که احتمالاً تهدیدکننده هستند، هدایت کنند؛ و کاهش تعداد شهروندانی که تحت نظارت تهاجمی‌تر هستند. خطرات شناخته شده‌ای در ارتباط با هوش مصنوعی وجود دارد. الگوریتم‌ها می‌توانند سوگیری‌های ذاتی یا آموخته‌شده خود را نشان دهند (Osoba and Welser, 2017: 1)، ممکن است در محیط‌های متخاصم آسیب‌پذیر باشند و ذاتاً توسط داده‌هایی که به آنها دسترسی دارند محدود می‌شوند. سیستم‌های تجزیه و تحلیل خودکار که ذاتاً برای انسان غیرقابل درک هستند. فقدان تدابیر کافی در مورد استفاده از هوش مصنوعی و مخازن وسیع داده‌هایی که بر آن تکیه می‌کند، می‌تواند نه‌تنها منجر به سوءاستفاده از آن توسط دولت‌های استبدادی به منظور تحمیل تمامیت‌خواهانه شود. کنترل بر شهروندان خود، بلکه به نقض بیش از حد حقوقی مانند حریم خصوصی و آزادی بیان یا تشکل در کشورهای دموکراتیک.

مفهوم استفاده از فناوری‌های پیش‌بینی دقیق مبتنی بر هوش مصنوعی برای مقاصد ضد جرایم تروریستی، حدس و گمان است اما امکان‌پذیر است. در نظر گرفتن احتمالات و هزینه‌های چنین رویکردی و چگونگی تنظیم این حوزه نوپا از قبل مفید است (Monaco, 2017: 25). لذا یکی از اقداماتی که می‌توان از هوش مصنوعی برای دفع تروریسم استفاده کرد، «پیش‌بینی رفتار افراد» از طریق ارائه داده‌ها به نرم‌افزارهای هوش مصنوعی است تا با تحلیل اطلاعات افراد که برگرفته از فضای مجازی و حقیقی است، بتواند رفتارهای احتمالی آنها در راستای اعمال تروریستی را پیش‌بینی نماید و از پیشروی بیشتر آن جلوگیری کند. همچنان که کنترل ارتباط‌گیری‌ها و کشف روابط شاخه‌های شبکه تروریستی در فضاهای ارتباطی مجازی است که می‌تواند نقشه تروریست‌ها در اعمال جنایی خنثی کرد.

۱. نقش فناوری‌ها و تحولات فنی در مقابله با جرایم تروریستی

دو راه برای مقابله با جرایم تروریستی وجود دارد. یکی بازدارندگی است: از طریق حفاظت از زیرساخت‌ها، اعمال بررسی‌های امنیتی و وعده مجازات. مورد دیگر سلب

توانایی انجام حملات است: با دستگیری تروریست‌ها قبل از به ثمر نشستن توطئه‌های آنها، مقابله با عضوگیری و رادیکالیزه کردن تروریست‌های آینده و ایجاد محدودیت برای حرکت و آزادی افراد. بسیاری از این روش‌ها دارای ویژگی‌های مشترک هستند. به‌طور خاص، آنها مطالباتی را برای منابع کمیاب مطرح می‌کنند و تا حدودی حقوق افرادی را که به آنها اعمال می‌شود، زیر پا می‌گذارند. نقض بیش از حد یا خودسرانه حقوق، به اصول لیبرال دموکراسی خیانت می‌کند و با انجام این کار، پیروزی را به تروریست‌ها واگذار می‌کند (Richardson, 2006: 250). ازاین‌رو، براساس عمل‌گرایی و همچنین اصل، مبارزه با جرایم تروریستی مؤثر را می‌توان به‌عنوان یک مشکل بهینه‌سازی توصیف کرد که هدف آن بهینه‌سازی است. تأمین امنیت برای اکثریت شهروندان با حداقل نقض حقوق و آزادی‌ها. برای رسیدن به این نقطه بهینه، پیشگیری مؤثر از جرایم تروریستی از روش‌هایی بهره می‌برد که شناخت موقعیت حملات یا رفتارهای مرتبط با آنها را بهبود می‌بخشد. پیش‌بینی در به‌کارگیری اقدامات پیشگیرانه اجازه می‌دهد تا تأثیر آن را بر کل جمعیت به حداقل برساند. برای مثال، پیش‌بینی مؤثر ممکن است این تأثیر را داشته باشد که فقط تروریست‌های خشن با زور یا محدودیت‌های اجباری مواجه می‌شوند، در حالی که اقدامات آشتی‌جویانه به سمت افراد آسیب‌پذیر در برابر افراط‌گرایی هدایت می‌شود. در مورد بازدارندگی از طریق حفاظت فیزیکی، پیش‌بینی می‌تواند به‌عنوان وسیله‌ای برای بهبود تخصیص منابع به مکان‌هایی که احتمالاً هدف هستند، عمل کند.

طبق اعلام شورای مهندسی و علوم فیزیک و تحقیقات «هدف فناوری‌های هوش مصنوعی بازتولید یا پیشی گرفتن از توانایی‌ها (در سیستم‌های محاسباتی) است که اگر انسان‌ها آنها را انجام دهند به «هوش» نیاز دارند. اینها عبارتند از: یادگیری و سازگاری. درک حسی و تعامل؛ استدلال و برنامه‌ریزی؛ بهینه‌سازی رویه‌ها و پارامترها؛ خودمختاری؛ خلاقیت؛ و استخراج دانش و آینده‌انگاری از داده‌های دیجیتالی بزرگ و متنوع.» (Engineering and Physical Science and Research Council, 2018: 1) امروزه بسیاری از نیروهای انتظامی کشورهای مختلف در حال بهره‌مندی از بهترین و جدیدترین فناوری‌های روز دنیا در عرصه کنترل و پیشگیری و همچنین حفظ حقوق شهروندی و حفظ امنیت داخلی در تمامی زیرمجموعه‌ها ازجمله امنیت مالی، جانی، غذایی، سلامت، بهداشتی و ... می‌باشند.

از اقداماتی که می‌تواند ریشه‌های فکری افراد تروریست را تحت تأثیر قرار داد و درنتیجه از اقدامات تروریستی از ابتدا جلوگیری کند، شناسایی و کنترل افراد از طریق جمع‌آوری هوشمند داده‌ها از فضای مجازی آنهاست تا با تحلیل این اطلاعات بتواند شاخه‌های فکری مرتبط با این اقدامات را شناسایی و در جهت اصلاح و تعدیل اندیشه آنان به صورت هوشمند اقدام نماید.

۲. جلوه‌های کاربست هوش مصنوعی در نیروهای پلیس

یکی از دامنه‌های استفاده از هوش مصنوعی در حوزه‌های مهم و کاربردی استفاده نیروی‌های نظامی ـ انتظامی از هوش مصنوعی در عرصه‌ها و حوزه‌های مختلف است بدین‌صورت که این فناوری ضمن شناسایی و کشف جرم، توانسته است الگوهای وقوع جرم و الگوهای پیشگیری از وقوع جرم را نیز ترسیم کند. همین‌طور افراد با زمینه‌های ذهنی و بیولوژیکی که نسبت به سایر افراد بیشتر امکان انجام اعمال مجرمانه را دارند و همچنین افرادی که می‌توانند بیشتر از بقیه کاندیدای قربانی شدن باشند را شناسایی کند و گام‌های بسیار مؤثری را در جهت مقابله با وقوع جرم و پیشگیری از وقوع جرم انجام دهد. همه این فرآیندها که با به‌کارگیری این فناوری انجام می‌شود، درنهایت منجر به افزایش امنیت و کاهش میزان جرم و جنایت در سطح کشور می‌شود و امنیت شهروندان را تأمین و حقوق شهروندی آنها را تضمین می‌کند. موضوع هوشمندی و استفاده از هوش مصنوعی در انتظام و امنیت، حوزه و بخش‌های وسیعی دارد که این حوزه شامل همه‌گونه ناهنجاری، قانون‌شکنی و عملیات مجرمانه از پایین‌ترین تا بالاترین حد است. امروزه هوش مصنوعی در پلیس امکان کشف جرایم مرتبط با پول‌شویی و سایر کلاه‌برداری‌های مشابه را فراهم می‌کند. علاوه بر استفاده از هوش مصنوعی در پلیس، هوش مصنوعی باید توسط سایر سازمان‌ها برای کشف جرم استفاده شود. می‌توان از آن برای شناسایی کالاهایی که به‌طور غیرقانونی حمل می‌شوند استفاده کرد. به‌کارگیری هوش مصنوعی در جرم‌شناسی در نحوه عملکرد پلیس و تصمیم‌گیری برای برنامه‌های حفظ امنیت کشور و مبارزه با تروریسم، ضروری و مهم خواهد بود. البته پیش‌بینی جرایم احتمالی و رفتارهای آتی مجرمان خطرناک، صرفاً در جهت پیشگیری از وقوع جرم خواهد بود و دستگیری و مجازات افراد، پیش از آنکه مرتکب جرمی شوند، براساس قوانین حقوق کیفری کشور مورد منع جدی

قرار گرفته است. همچنین استفاده از الگوریتم‌های پیش‌بینی رفتار افراد می‌تواند در تصمیم‌گیری مقامات قضایی نقش کارآمدی داشته باشد. این الگوریتم‌ها که براساس الگوهای ارزیابی خطر عمل می‌کنند، می‌توانند درجه خطرناکی فرد را اعتبارسنجی و ارزیابی کنند. هوش مصنوعی با پیش‌بینی رفتار مجرمان، می‌تواند در جهت اعمال کارهای ارفاقی مانند آزادی مشروط، تعلیق و غیره بسیار نقش کارآمدی ایفا کند. بهره‌مندی از هوش مصنوعی همچنین از قرارهای تأمین کیفری که بر مبنای درجه خطرناکی متهم و تضمین حضور او در دادرسی است، کاربرد خواهد داشت.

در حال حاضر بخش‌های جامعه ازجمله پلیس و بسیاری از ادارات پلیس هستند که از هوش مصنوعی برای کمک به پیش‌بینی و شناسایی افراد و مکان‌های مشکوک استفاده می‌کند. همان‌طورکه مراقبت‌های بهداشتی، بیمه، تجارت و حمل‌ونقل. استفاده می‌شود. در نیروهای نظامی ـ انتظامی، اصطلاح «هوش مصنوعی» ممکن است به معنای استفاده رو به رشد از فناوری‌های کاربردی بهترین باشد است. هوش مصنوعی در حال حاضر یک عامل مهم است. کاری که با افزایش کارایی و ارائه بینش از کلان داده‌ها، می‌تواند مزایای واقعی را برای پلیس در مقابله با جرایم و اجرای آن فراهم کند. همچنین می‌توان از هوش مصنوعی در زمینه قانون و پزشکی، کشاورزی و ارتباطات و نیروهای پلیس را مدرن کنیم (E. Joh, 2014: 6). البته نیروی‌های پلیس در حوزه‌های مختلفی وظایف امنیتی و انتظامی و پیشگیرانه و برخوردهای قاطع را بر عهده دارد. در بسیاری از حوزه‌ها ازجمله امنیت داخلی و خارجی امنیت داخلی طیف وسیعی از زیرمجموعه‌ها را شامل می‌شود که عبارت‌اند از: جانی، مالی، سرمایه‌گذاری گرفته تا حوزه غذایی و حوزه سلامت. به عبارتی با استفاده از هوش مصنوعی در این عرصه می‌تواند اقدامات بسیار مؤثری را در زمینه پیشگیری و کشف جرم و تعقیب مجرمان و مبارزه در جرایم تروریستی انجام داد.

۳. کاربردها و سازوکارهای عملی در مقابله با جرایم تروریستی

در فرآیند مقابله با جرایم تروریستی برخط، هوش مصنوعی می‌تواند تأثیر عمیقی بر جامعه ما داشته باشد، از مراقبت‌های بهداشتی، کشاورزی و صنعت گرفته تا خدمات مالی و آموزش در حالی که این فناوری‌ها نویدبخش هستند، بدون خطر نیستند و برخی از آنها اضطراب و حتی ترس را القا می‌کنند. آنها می‌توانند برای اهداف مخرب مورد استفاده قرار

گیرند یا پیامدهای منفی ناخواسته داشته باشند. هوش مصنوعی این دوگانگی را شاید بیشتر از هر فناوری نوظهور امروزی تجسم می‌دهد. در حالی که می‌تواند در بسیاری از بخش‌ها پیشرفت کند، اما این پتانسیل را نیز دارد که مانع بهره‌مندی از حقوق بشر و آزادی‌های اساسی ـ به‌ویژه حقوق حریم خصوصی، آزادی اندیشه و بیان و عدم تبعیض شود؛ بنابراین، هرگونه اکتشاف در مورد استفاده از فناوری‌های مجهز به هوش مصنوعی باید همیشه با تلاش‌هایی برای جلوگیری از نقض بالقوه حقوق بشر همراه باشد. در این زمینه، بسیاری از سازمان‌های بین‌المللی و منطقه‌ای، مقامات ملی و سازمان‌های جامعه مدنی را مشاهده کرده‌ایم که بر روی طرح‌هایی با هدف ایجاد دستورالعمل‌های اخلاقی در مورد استفاده از هوش مصنوعی و همچنین ظهور چارچوب‌های اولیه قانونی کار می‌کنند.

در استراتژی جهانی مبارزه با جرایم تروریستی سازمان ملل متحد[۱]، کشورهای عضو تصمیم گرفتند با توجه به محرمانه بودن، احترام به حقوق بشر و با رعایت سایر تعهدات تحت قوانین بین‌المللی، با سازمان ملل همکاری کنند تا راه‌هایی را بررسی کنند. هماهنگ کردن تلاش‌ها در سطوح بین‌المللی و منطقه‌ای برای مبارزه با جرایم تروریستی در همه اشکال و مظاهر آن در اینترنت و استفاده از اینترنت به‌عنوان ابزاری برای مقابله با گسترش جرایم تروریستی. درعین‌حال، استراتژی تشخیص می‌دهد که کشورهای عضو ممکن است برای انجام این تعهدات به کمک نیاز داشته باشند. با توجه به تهدید جرایم تروریستی، نرخ رو به رشد دیجیتالی شدن و رشد جمعیت جوان، آسیب‌پذیر و آنلاین در جنوب آسیا و جنوب شرق آسیا، این گزارش راهنمایی‌هایی را به آژانس‌های مجری قانون و ضد جرایم تروریستی در جنوب آسیا و جنوب شرق آسیا در مورد پتانسیل ارائه می‌دهد. استفاده از هوش مصنوعی برای مقابله با جرایم تروریستی آنلاین و همچنین در مورد بسیاری از چالش‌های حقوق بشر، فنی و سیاسی که باید در نظر بگیرند و در صورت تمایل به انجام آن رسیدگی کنند.[۲]

تجزیه و تحلیل خودکار داده‌ها برای پشتیبانی از فعالیت‌های سرویس‌های اطلاعاتی و امنیتی، به‌ویژه از طریق تجسم داده‌ها استفاده می‌شود. الگوریتم‌ها مظنونان تروریستی را

---

۱. United Nations Global Counter-Terrorism Strategy (A/RES/60/288)

۲. https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence

اولویت‌بندی می‌کنند. (Anderson, 2017: 38) و به‌طور معمول خطر مسافران سفر هوایی را ارزیابی می‌کنند. (Elias, 2014: 1) اطلاعات را می‌توان به‌طور پیش‌فرض جمع‌آوری و ذخیره کرد بعداً با هدف آشکار کردن الگوها و پیوندهایی که شبکه‌های تروریستی یا فعالیت‌های مشکوک را افشا می‌کنند، تجزیه و تحلیل شود. (Akhgar et al, 2015: 4) رویکردهای یادگیری ماشینی امکان تفسیر و تجزیه و تحلیل الگوهای غیرقابل دسترس در مقادیر زیادی از داده‌ها را فراهم می‌کنند. (Van Puyvelde et al, 2017: 1398) این رویکردها ممکن است شامل فیلتر کردن، تجزیه و تحلیل روابط بین موجودات، یا ابزارهای پیچیده‌تر تشخیص تصویر یا صدا. سازمان‌های اطلاعاتی و سرویس‌های امنیتی تنها کسانی نیستند که ارزش پیش‌بینی داده‌ها را تشخیص داده و تلاش می‌کنند تا به آن پی ببرند. نتیجه واگذاری روش‌ها و قابلیت‌ها به مقامات غیرنظامی (مانند پلیس) بوده است. (Galdon Clavell, 2016: 91) تجزیه و تحلیل شبکه‌های اجتماعی باندهای شهری (Gunnell, 2016: 6)، سیستم هشدار در سطح شهر (Levine, 2017: 75)، پیش‌بینی محل وقوع جرم و کمک‌های تصمیم‌گیری بازداشت همگی نمونه‌هایی از پیش‌بینی هستند. ابزارهای مبتنی بر هوش مصنوعی که برای مبارزه با جرایم تروریستی قابل‌استفاده است و در حال حاضر توسط سازمان‌های مجری قانون استفاده می‌شود.

در مورد مبارزه با جرایم تروریستی، رویکردهای تحقیقی که قبل از وقوع حمله به کار می‌رود، به‌طور سنتی توسط سرویس‌های اطلاعاتی و امنیتی انجام می‌شود. به‌طورکلی، این رویکردها بر روی کار کردن از توطئه‌های نیمه کشف شده یا مظنونان شناخته شده به‌منظور یافتن سایر طرف‌های درگیر یا شناسایی پیوندهایی که عمیق‌تر به سازمان‌های تروریستی منجر می‌شوند تمرکز دارند. اعطای دسترسی به داده‌های مربوط به یک فرد خاص مشروط به داشتن آنهاست. پیوندی به یک یا چند تحقیق موجود متمایز از این و اخیراً با پیشرفت‌های هوش مصنوعی قابل‌قبول است، تجزیه و تحلیل فعالیت‌های معمول همه افراد برای پیش‌بینی رویدادهای تروریستی، یا شناسایی تروریست‌ها از طریق تشخیص آنچه در فعالیت یک زیرگروه خاص متمایز است، است. حجم وسیعی از اطلاعات دیجیتالی که اکنون توسط یک فرد معمولی تولید می‌شود به این معنی است که می‌توان بیشتر این فعالیت‌های معمول را از طریق تجزیه و تحلیل درک کرد. منابع شامل ابر داده‌های ارتباطات و سوابق اتصال به اینترنت است، اما به ردیابی مکان و فعالیت، خریدها و

فعالیت رسانه‌های اجتماعی نیز گسترش می‌یابد. بسیاری از این اطلاعات در دست سرویس‌های اطلاعاتی و امنیتی نیست، به این معنی که عواملی که در بهره‌برداری از آن دخالت دارند، متنوع هستند.

انتظار اینکه هوش مصنوعی راه‌حل‌های فوری برای سؤالات پیچیده ارائه دهد، واقع‌بینانه نیست. به‌طور خلاصه، نمونه‌های متعددی از هوش مصنوعی وجود دارد که جرایم تروریستی یا جنبه‌هایی از جرایم تروریستی را پیش‌بینی می‌کند. اغلب، توانایی توسعه ابزارهای هوش مصنوعی برای این منظور در اختیار کسانی است که به داده‌ها دسترسی دارند یا به واسطه خدماتی که ارائه می‌دهند، نگهبان آن هستند. در جایی که هوش مصنوعی پیش‌بینی‌کننده برای نیروهای پلیس و سایر مقامات (مانند سازمان‌های مجری مرز) مفید است، توسعه آن اغلب به صنعت نرم‌افزار واگذار می‌شود. با فرض ادامه روند دیجیتالی شدن و بهبود عملکرد هوش مصنوعی، در آینده زمینه بیشتری برای به دست آوردن پیش‌بینی‌های دقیق درباره جرایم تروریستی از هوش مصنوعی وجود خواهد داشت و احتمالاً جذب آن برای استفاده ضد جرایم تروریستی افزایش می‌یابد.

٤. هوش مصنوعی و ملاحظات حقوق بشری آن

هوش مصنوعی می‌تواند برای شناخت آینده جرایم تروریستی براساس فراداده‌های ارتباطی، اطلاعات تراکنش‌های مالی، الگوهای سفر و فعالیت‌های مرور اینترنت و همچنین اطلاعات در دسترس عموم مانند فعالیت رسانه‌های اجتماعی استفاده شود. پتانسیل جلوگیری از حملات تروریستی ممکن است انگیزه‌ای برای افزایش استفاده از این فناوری باشد. برای مثال، در سال ۲۰۱۷، یک بررسی بهبود عملیاتی بریتانیا که پس از چهار حمله تروریستی تکمیل شد، خواستار تغییر گامی در توانایی «بهره‌برداری از داده‌ها برای شناسایی فعالیت‌های نگران‌کننده» با توجه به هر دو موضوع مورد علاقه که قبلاً برای امنیت شناخته شده بود، شد. خدمات و آنهایی که برای آنها ناشناخته است. تعدادی از چالش‌ها در رابطه با استفاده از هوش مصنوعی پیش‌بینی‌کننده در مقابله با جرایم تروریستی وجود دارد یا در حال بروز است. کاربرد آن باید به دو نوع نگرانی پاسخ دهد: ملاحظات حقوق بشر؛ و مفاهیم عملی.

در سال ۲۰۱۴، گزارش دفتر کمیساریای عالی حقوق بشر سازمان ملل[۱] در مورد حق حفظ حریم خصوصی در عصر دیجیتال مشاهده کرد که نمونه‌هایی از نظارت دیجیتالی آشکار و پنهان در حوزه‌های قضایی در سراسر جهان، با توده‌های دولتی، افزایش یافته است. نظارت به‌عنوان یک عادت خطرناک به جای یک اقدام استثنایی ظاهر می‌شود. پیشرفت‌های اخیر در تجزیه و تحلیل ویدیو و پردازش زبان طبیعی نشان می‌دهد که فناوری‌های آینده احتمالاً این امر را با هزینه‌های بالقوه پایین‌تر امکان‌پذیر می‌کنند.

هوش مصنوعی به‌طور گسترده‌ای به‌عنوان فناوری شناخته می‌شود که ممکن است مزایای بزرگی را به همراه داشته باشد و در عین حال خطرات قابل توجهی را به همراه داشته باشد، با سازمان‌های متعددی که منابعی را برای کاوش در این موارد اختصاص می‌دهند. یکی از گزارش‌های اخیر و چند نویسنده در مورد استفاده مخرب هوش مصنوعی، تأثیر آن را بر آزادی سیاسی، ازجمله سناریوی آینده احتمالی یک سیستم پیش‌بینی‌کننده «اختلال مدنی» که برای جلوگیری از تهدیدها قبل از به ثمر نشستن آنها طراحی شده است. در مورد استفاده از این فناوری‌ها، چه توسط سرویس‌های اطلاعاتی و امنیتی، چه مجریان قانون یا بخش خصوصی، خط‌خطی باید ترسیم شود.

برخی از حقوق و آزادی‌های مورد بحث در اعلامیه جهانی حقوق بشر تشریح شده و در معاهداتی مانند میثاق بین‌المللی حقوق مدنی و سیاسی[۲] ادغام شده است. این سند از حقوق حریم خصوصی، آزادی اندیشه و مذهب، بیان و انجمن حمایت می‌کند. قطعنامه مجمع عمومی سازمان ملل متحد در مورد حق حفظ حریم خصوصی در عصر دیجیتال[۳] این قطعنامه وظیفه دولت‌ها را می‌گذارد که اطمینان حاصل کنند که فعالیت‌های آنها با قوانین بین‌المللی مطابقت دارد، اما تفاسیر متفاوت از مفاهیمی مانند دخالت «خودسرانه» یا حتی «غیرقانونی» در حریم خصوصی افراد به این معنی است که این قطعنامه به‌عنوان یک هنجار الزام‌آور نسبتاً ضعیف است. معاهدات منطقه‌ای حمایت از حقوق به تقویت این امر در برخی زمینه‌ها کمک می‌کند، به‌ویژه در مواردی که صلاحیت دادگاه‌های فراملی را

۱. Office of the United Nations High Commissioner for Human Rights (OHCHR)

۲. International Covenant on Civil and Political Rights (ICCPR)

۳. The right to privacy in the digital age: resolution/adopted by the General Assembly 15 September 2021.

تضمین می‌کند.[۱] جدای از حوزه‌هایی که تحت صلاحیت دادگاه‌های دارای اختیارات فراملی قرار دارند، کنترل‌هایی در برابر سوء استفاده از هوش مصنوعی و مخازن وسیع داده‌هایی که بر آن تکیه می‌کند در سطح ایالتی وجود دارد. در سراسر جهان در مورد استفاده قابل قبول از هوش مصنوعی، هم از نظر روش و هم هدف، تنوع زیادی وجود دارد. به‌عنوان مثال، گزارش شده است که چین از فناوری تشخیص چهره و تجزیه و تحلیل رفتاری ویدیویی در مقیاسی بی‌سابقه استفاده می‌کند، برای اهداف مختلفی که شامل شناسایی جایوکرها و دستگیری مجرمان تحت تعقیب در رویدادهای عمومی است. جمع‌آوری و نگهداری انبوه داده‌های داخلی به تنهایی که استفاده از هوش مصنوعی پیش‌بینی‌کننده احتمالاً مشروط به برخی از اشکال آن است، همچنان یک نقطه بحث داغ است. به‌عنوان مثال، در دادگاه اروپایی حقوق بشر[۲] پرونده‌های معلق مختلفی وجود دارد که ادعا می‌کند کشورهایی ازجمله آلمان، سوئد و بریتانیا از طریق شنود، نگهداری و استفاده از داده‌های انبوه، کنوانسیون اروپایی حقوق بشر[۳] را نقض می‌کنند. ایالت‌ها همچنین در احکام دیوان دادگستری اتحادیه اروپا[۴] از اختیارات نگهداری داده‌ها سلب شده‌اند. برای مثال، در دسامبر ۲۰۱۶، دادگاه دیوان عدالت اداری علیه قانون حفظ داده‌ها و اختیارات تحقیقی بریتانیا در سال ۲۰۱۴ حکم داد و بیان کرد که این قانون نتوانست حقوق اساسی تضمین شده توسط منشور اتحادیه اروپا را برآورده کند.[۵] چالش‌های قانونی برای قانون جایگزین ـ قانون اختیارات تحقیق ۲۰۱۶ ـ در حال حاضر در جریان است و اعتراضات اولیه توسط دادگاه عالی داخلی تأیید شده است که منجر به اصلاح این قانون شده است.

---

۱. ر.ک. به: کنوانسیون اروپایی حقوق بشر، که در سال ۱۹۵۳ به تصویب رسید، کنوانسیون آمریکایی حقوق بشر، که در سال ۱۹۷۸به تصویب رسید و منشور آفریقایی در مورد انسان و مردم حقوق، در سال ۱۹۸۶ به تصویب رسید.

۲. European Court of Human Rights (ECHR)

۳. European Convention on Human Rights

۴. Court of Justice of the European Union (CJEU)

۵. Court of Justice of the European Union (2016), Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland) v. Tom Watson and Others, Judgement of the Court (Grand Chamber), 21 December 2016 In Joined Cases C-203/15 and C-698/15, https://eur-lex.europa.eu/legal-content/EN/SUM/?uri=CELEX%3A62015CJ0203

قدرت دسترسی، جمع‌آوری و ذخیره داده‌های شهروندان ناشی از عصر اطلاعات می‌تواند نشان‌دهنده تغییر در روابط بین دولت‌ها و شهروندان باشد و خواستار تجدید نظر در اقدامات طراحی‌شده نه‌تنها از حریم خصوصی، بلکه از دیگر آزادی‌های حیاتی برای عملکرد دموکراتیک است. پیشرفت‌های بعدی عصر دیجیتال، مانند توانایی خودکارسازی بخش‌های بزرگی از تجزیه و تحلیل آن داده‌ها، این الزام را تکرار می‌کند. در استفاده و محدود کردن این اختیارات، باید بتوان بین دولت‌های دموکراتیک و اقتدارگرا تمایز قائل شد.

هوش مصنوعی پیش‌بینی‌کننده بر تجزیه و تحلیل داده‌های متعلق به عموم مردم برای تشخیص رفتارهای مشکوک از عادی یا تشخیص روندهایی که ممکن است به پیش‌بینی حملات کمک کند، تکیه می‌کند. اکثریت قریب به اتفاق داده‌های مورد تجزیه و تحلیل توسط افرادی تولید می‌شود که مورد علاقه سرویس‌های اطلاعاتی نیستند.

به همین دلیل، یکی از حوزه‌های خاص نگرانی مرتبط با فناوری هوش مصنوعی پیش‌بینی‌کننده این است که یک اقدام نظارتی است که برای کل جمعیت اعمال می‌شود و این امر آن را بی‌تمایز و درنتیجه ذاتاً نامتناسب می‌کند. این همچنین یکی از کانون‌های اعتراض به برنامه‌های جمع‌آوری و تحلیل داده‌های انبوه ایالت‌ها بوده است. درحالی‌که چنین برنامه‌هایی مستقیماً با استفاده از هوش مصنوعی مرتبط نیستند، استفاده از هوش مصنوعی پیش‌بینی‌کننده برای مقابله با جرایم تروریستی احتمالاً بر توانایی جمع‌آوری و تجزیه و تحلیل داده‌ها به صورت انبوه متکی است. حتی جمع‌آوری و تجزیه و تحلیل داده‌های به ظاهر غیر حساس هنوز هم می‌تواند تداخل قابل توجهی در حریم خصوصی ایجاد کند. قطعنامه ۱۶۷/۶۸ مجمع عمومی سازمان ملل متحد در مورد حق حریم خصوصی در عصر دیجیتال، «جمع‌آوری غیرقانونی یا خودسرانه داده‌های شخصی» را به‌عنوان یک اقدام بسیار مداخله‌جویانه توصیف می‌کند که می‌تواند «حق حفظ حریم خصوصی و آزادی بیان» را نقض کند و ممکن است در تضاد با اصول باشد. از یک جامعه دموکراتیک.[1] این به دلیل شناخت طولانی‌مدت است که اطلاعات شخصی مهم را می‌توان از این نوع داده‌ها استنباط کرد و اینکه تجمیع و تجزیه و تحلیل داده‌ها تجاوز به حریم

۱. مجمع عمومی سازمان ملل متحد (۲۰۱۴)، قطعنامه تصویب شده توسط مجمع عمومی در ۱۸ دسامبر ۲۰۱۳، ۱۶۷/۶۸. حق حفظ حریم خصوصی در عصر دیجیتال.

خصوصی است؛ بنابراین، حتی اگر داده‌های مربوطه از منابع باز جمع‌آوری شده باشند، بحث همچنان پابرجاست. برخی از قوانین حقوق بین‌الملل دستورالعمل‌هایی برای ارزیابی اینکه آیا هرگونه نقض حریم خصوصی داده‌ها قابل توجیه است یا خیر، ارائه می‌دهد. حق حفظ حریم خصوصی داده‌ها به‌طور خاص تحت ماده ۸ منشور اتحادیه اروپا محافظت می‌شود و همچنین به‌طورکلی در ماده ۸ کنوانسیون اروپایی حقوق بشر تحت پوشش حق حفظ حریم خصوصی است. به همین دلیل، دیوان دادگستری[۱] و دادگاه حقوق بشر اروپا[۲] هر دو احکام مربوطه را صادر کرده‌اند. برای هر دو نهاد، مداخله باید یک معیار سه‌گانه را برآورده کند، یعنی تحقق یک هدف مشروع که در چارچوب قانونی انجام شود و شرایط ضرورت و تناسب را برآورده کند. ضرورت در این زمینه به این معناست که اقدام مناسب است، زیرا دارای علت و معلولی است. ارتباط با هدف سیاست و اینکه با توجه به گزینه‌های جایگزین، حقوقی بیش از حد لازم را محدود نمی‌کند؛ که براساس هدف مورد نظر محدود یا مشمول تمایز است؛ که تابع دستورالعمل‌های دقیق و عینی است؛ و اینکه تدابیر کافی و مؤثر در برابر سوء استفاده وجود دارد.

چارچوب‌های قانونی و حاکمیتی برای استفاده از داده‌های انبوه عمدتاً بر قدرت دسترسی به داده‌ها، با توصیف محدودی از نحوه استفاده از داده‌ها یا ملاحظات نتیجه‌ای در مورد نحوه حفاظت صحیح از آنها در برابر سوء استفاده متمرکز است. بدون ارائه جزئیات بیشتر در مورد استفاده از داده‌ها، اثبات ضرورت با پیوند دادن واضح حفظ داده‌ها به چیزی که می‌توان نشان داد که هدفی مشروع است، دشوار است. اگر هوش مصنوعی به میزان بیشتری مورد استفاده قرار گیرد، چارچوبی که تحت آن استفاده می‌شود باید مشارکت آن را در رسیدن به یک هدف مشروع ثابت کند ـ یا در غیر این صورت تضمین کند.

برخی از شرکت‌ها که با محدودیت‌های قانونی در جمع‌آوری و فروش داده‌ها کار می‌کنند، اطلاعات عمومی را به کالایی تبدیل کرده‌اند که همان شرکت‌ها می‌توانند آن را به سازمان‌های مجری قانون و امنیتی بفروشند. دولت‌ها ممکن است داده‌هایی را خریداری کنند که به حفظ امنیت آنها کمک می‌کند، اگر نتوانند از راه‌های دیگر، مانند شنود مخابراتی، آنها را به صورت قانونی به دست آورند (Cagle, 2016: 6). داده‌ها کالای

۱. Court of Justice of the European Union (CJEU)

۲. Homepage of the European Court of Human Rights (HECHR)

ارزشمندی هستند، به این معنی که تعهدات شرکت‌های خصوصی برای محافظت از حریم خصوصی مشتریان همیشه به اندازه آنها اصولی نیست. ممکن است به نظر برسد. درحالی‌که برخی از شرکت‌های فناوری صراحتاً دولت‌ها را از استفاده از داده‌های پلتفرم‌هایشان مسدود کرده‌اند، همین داده‌ها در دسترس شرکت‌های شخص ثالث باقی می‌مانند. ازاین‌رو، چنین مقرراتی عمدتاً از نظر ارزشی بلاغی هستند (Levin, 2016: 9). عمل‌گرایی در مورد دسترسی به بازارهای بزرگ باعث می‌شود که حریم خصوصی و آزادی کاربران بیشتر در معرض خطر باشند، از اصول اعلام شده خود صرف‌نظر کنند. در یک افراط، در کشورهایی که کنترل بیشتری از سوی دولت بر صنایع خصوصی وجود دارد، فرصت‌های نامحدودی برای دولت‌ها وجود دارد تا اطلاعات شخصی یا حساس در مورد موضوعات خود را جمع‌آوری و تجزیه و تحلیل کنند. درحالی‌که انعطاف‌پذیری نسبی در بخش خصوصی ممکن است فرصت‌هایی را فراهم کند، سپردن مسئولیت بیش از حد به دست شرکت‌های تجاری می‌تواند منجر به کسری فزاینده پاسخگویی شود. اگرچه برخی از شرکت‌های خصوصی برای شفاف‌سازی تلاش می‌کنند، اما این اقدامات جزئی هستند و به صلاحدید خودشان انجام می‌شوند.

عدم شفافیت ذاتی روش‌های استفاده از هوش مصنوعی پیش‌بینی‌کننده در مقابله با جرایم تروریستی، یا حتی در استفاده از داده‌های انبوه حفظ شده به‌طورکلی، ایجاد تضمین‌های قانونی جبران خسارت را دشوار می‌کند. مقررات حفاظت از داده‌های عمومی اتحادیه اروپا[1]، یکی از گسترده‌ترین رژیم‌های حفاظت از داده‌ها در جهان، تلاش می‌کند این را با تضمین حق جبران خسارت در مورد هر تصمیم کاملاً خودکاری که گرفته می‌شود، متعادل کند. با این حال، مشخص نیست که آیا این معیار را می‌توان با تصمیماتی که مستلزم سطح خودسرانه نظارت انسانی است برآورده کرد یا خیر. علاوه بر این، شامل یک معافیت برای سازمان‌های دولتی است.

شیوع کم جرایم تروریستی و تمایل تاکتیک‌های تروریستی به تکامل نسبتاً سریع، ساخت مدل‌های پیش‌بینی خوب را دشوار می‌کند. نقش‌های مختلف متعددی در جرایم تروریستی وجود دارد و راه‌های متعددی برای ایفای آن نقش‌ها وجود دارد. این بدان

۱. General Data Protection Regulation (GDPR)

معناست که فهرست کردن شاخص‌های قطعی دخالت یا طرد از جرایم تروریستی غیرممکن است (Borum, 2015: 80). در حالی که به نظر می‌رسد روندهای قابل‌تشخیصی در ویژگی‌های مشترک تروریست‌ها وجود دارد، تعداد اندک تروریست‌ها در جمعیت عمومی، ویژگی‌های گسترده‌ای را براساس پروفایل هیچ نشان می‌دهند.

ازآنجایی‌که استفاده از هوش مصنوعی پیش‌بینی‌کننده در مقابله با جرایم تروریستی در حال ظهور است، فقدان تلاش برای اطمینان از وجود و اجرای استانداردهای اعتبارسنجی ممکن است قابل درک باشد. اگر هوش مصنوعی پیش‌بینی‌کننده به‌طور گسترده‌تری در مقابله با جرایم تروریستی در آینده استفاده شود، ناتوانی در اثبات اعتبار مدل‌های پیش‌بینی می‌تواند شفافیت و اشتراک اطلاعات را تضعیف کند.

نتیجه‌گیری

ساختارهای فعلی که استفاده از هوش مصنوعی پیش‌بینی‌کننده را در مقابله با جرایم تروریستی تنظیم می‌کنند، بعید به نظر می‌رسند که در برابر سوءاستفاده محافظت کنند یا بتوانند سودمندترین استفاده از این فناوری‌ها را، هم از نظر عملکرد عملیاتی و هم از نظر رعایت اصول حقوق بشر، ممکن کنند. پیگیری تلاش‌های هماهنگ‌تر برای استفاده از هوش مصنوعی پیش‌بینی‌کننده در عملیات‌های ضد جرایم تروریستی نیازمند تعهد از نظر تحقیق و آزمایش است تا مدل‌هایی آماده استفاده ایجاد شود. اگر فناوری‌های هوش مصنوعی برای پیش‌بینی جرایم تروریستی به بلوغ برسد، دسترسی بیشتر به داده‌ها و تمرکز بیشتر ـ تحت پادمان‌های سخت‌گیرانه ـ می‌تواند راهی برای میانجی‌گری نقض حریم خصوصی برای اهداف متناسب ارائه دهد. در حال حاضر، مقررات خاص استفاده از هوش مصنوعی به منظور شناخت مداخله یا خطر جرایم تروریستی جزئی یا به‌طور کامل وجود ندارد. در مواردی که محدودیت وجود دارد، اغلب بر دسترسی به داده‌ها تمرکز می‌کنند و نه بر نحوه استفاده از داده‌ها. به‌طور متناقض، محدود کردن دسترسی می‌تواند توانایی توسعه مدل‌های خوب را که در غیر این صورت می‌توانند انطباق با شرایط تناسب و عدم تبعیض را بهبود بخشند، محدود کند. دسترسی متمرکزتر با مقررات بهتر می‌تواند منصفانه‌تر از دسترسی تصادفی به صلاحدید هر بازیگر یا آژانسی باشد که بتواند آن را به دست آورد.

توسعه و استفاده از قابلیت‌های پیش‌بینی می‌تواند توجیه معتبری برای دسترسی و استفاده گسترده‌تر از داده‌های عمومی باشد، مشروط بر اینکه مدل‌ها قبل از استفاده کاملاً اعتبارسنجی شوند، مراحل اولیه تجزیه و تحلیل به‌طور خودکار انجام شود و اقدامات فنی کنترل در آنها انجام شود. مکانی برای جلوگیری از سوءاستفاده دسترسی مستمر به هر داده برای اهداف مقابله با جرایم تروریستی باید مشروط به توانایی استخراج ارزش پیش‌بینی کافی از آن داده‌های خاص باشد ـ به این معنی که تناسب دسترسی مستقیماً با تحقق یک هدف مشروع مرتبط است. دولت‌ها هنگام پیگیری اهداف حیاتی مانند امنیت عمومی از ابزارهای فناوری جدید در اختیار خود استفاده خواهند کرد. این واقعیت که هوش مصنوعی تهاجم به حریم خصوصی را در مقیاس بسیار آسان‌تر می‌کند به این معنی است که استفاده از آن فناوری‌ها همچنان یک نگرانی سیاست عمومی است. این بدان معنا نیست که استفاده از هوش مصنوعی برای پیش‌بینی جرایم تروریستی توسط دموکراسی‌های لیبرال باید خارج از محدودیت باشد. درواقع، قابلیت‌های پیش‌بینی خوب مبتنی بر تجزیه و تحلیل خودکار داده‌های کمتر مزاحم می‌تواند بخشی از محدودیت‌های معقول در استفاده نامتناسب از اقداماتی باشد که تهدیدات بیشتری برای حریم خصوصی و سایر آزادی‌های مرتبط ایجاد می‌کند. یک فرآیند تصمیم‌گیری، با عملکرد قابل اندازه‌گیری، با توجه به اینکه چه کسی باید تحت نظارت مداخله‌جویانه‌تر قرار گیرد، ممکن است برای محدود کردن استفاده از نظارت فنی فعال در جایی که محدودیت‌های عملی احتمالاً از بین می‌رود، کلیدی باشد. اینکه دولت‌ها تا چه اندازه قدرت‌هایی را که فناوری جدید برای آنها به ارمغان می‌آورد، مدیریت می‌کنند، نشان‌دهنده میزان تثبیت نهادهای آنها و قدرت تعهد آنها به حمایت از حقوق شهروندان به‌طورکلی خواهد بود.

References

- Akhgar, B., Saathoff, G. B., Arabnia, H., Hill, R., Staniforth, A. and Bayerl, P. (2015), Application of Big Data for National Security, Oxford: Butterworth-Heinemann.

- Anderson, D. (2017), Attacks in London and Manchester March–June 2017, independent assessment of M15 and police internal reviews, December 2017, para 2.38.

- Borum, R. (2015), 'Assessing Risk for Terrorism Involvement', Journal of Threat Assessment and Management, 2(2): 63-87.

- Brokenshire, J. (2013), 'National Security and Civil Liberties – Getting the balance right', speech delivered at National Security Summit at Queen Elizabeth Conference Centre, 3 July 2013, https://www.gov.uk/government/speeches/national-security-and-civil-liberties-getting-thebalance-right

- Cagle, M. (2016), 'Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color', ACLU Northern California website, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillanceproduct-marketed-target

- Cornish, P. (2010), 'Technology, Strategy and Counterterrorism', International Affairs, 86(4), p. 888, https://www.jstor.org/stable/40865000

- E. Joh, Elizabeth (2014), Artificial Intelligence and Policing: First Questions, Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35, 35.

- Elias, B. (2014), Risk-Based Approaches to Airline Passenger Screening, Congressional Research Service Report, 31 March 2014, https://www.hsdl.org/?view&did=752251 (accessed 1 Oct. 2018); and US Department of Homeland Security (2013), Passenger Name Record (PNR) Privacy Policy, 21 June 2013.

- Engineering and Physical Sciences Research Council (2018), 'Research Areas: Artificial Intelligence Technologies', Engineering and Physical Sciences Research Council Website, https://epsrc.ukri.org/research/ourportfolio/researchareas/ait/

- Galdon Clavell, G. (2016), 'Policing, Big Data and the Commodification of Security', in van der Sloot, B., Broeders, D. and Schrijvers, E. (eds) (2016), Exploring the Boundaries of Big Data, Netherlands Scientific Council for Government Policy (WRR) Report, Amsterdam: Amsterdam University Press, p. 91.

- Gunnell, D., Hillier, J. and Blakeborough, L. (2016), 'Social Network Analysis of an Urban Street Gang using Police Intelligence Data', Home Office Research Report 89, January 2016,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/491578/horr89.pdf

- Levin, S. (2016), 'Twitter blocks government 'spy centers' from accessing user data', Guardian, 15 December 2016, https://www.theguardian.com/technology/2016/dec/15/twitter-dataminr-user-data-aclu

- Levine, E. S., Tisch, J., Tasso, A. and Joy, M. (2017), 'The New York City Police Department's Domain Awareness System', Interfaces 47(1), pp. 70-84.

- Monaco, L (2017) ‘Preventing the Next Attack; A Strategy for the War on Terrorism’ Foreign Affairs 96(6), pp. 23-29.

- Osoba, O. and Welser, W. (2017), An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, CA: RAND Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1744/RAND_RR1744.pdf

- Richardson, L. (2006) What Terrorists Want: Understanding the Enemy, Containing the Threat, New York: Random House, p. 250.

- Van Puyvelde et al. (2017), ‘Beyond the Buzzword: big data and national security decision-making’, p. 1398.