



بررسی تاثیر هوش مصنوعی بر پیشگیری و مقابله با تهدیدات ترور بیولوژیکی

اسراء بشیرنژاد مطلق

۱- دانشجوی دکترای حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد علوم تحقیقات، گروه حقوق، تهران، ایران

a.bashirnejhad.2025@gmail.com

چکیده

در چند دهه اخیر، پیشرفت‌های چشم‌گیر در حوزه تکنولوژی و ظهور فناوری‌های نوین، به‌ویژه هوش مصنوعی، منجر به تغییرات بنیادی در عرصه‌های مختلف علمی، صنعتی و امنیتی شده است. یکی از این عرصه‌ها که هوش مصنوعی می‌تواند نقش قابل توجهی در آن ایفا کند، مسائل مرتبط با امنیت زیستی و مقابله با تهدیدات تروریسم بیولوژیکی است. این نوع تهدیدها، به دلیل ماهیت پیچیده، پنهان و گسترده‌ی آسیب‌های احتمالی که می‌توانند به همراه داشته باشند، از جمله چالش‌های جدی پیش روی جوامع بشری محسوب می‌شوند. در چنین شرایطی، بهره‌گیری از فناوری‌های نوین مانند هوش مصنوعی برای شناسایی، پیشگیری و مقابله با این تهدیدات، ضرورت دوچندانی یافته است. هوش مصنوعی با توانمندی‌های منحصربه‌فرد خویش در تحلیل حجم بالایی از داده‌ها، پردازش سریع اطلاعات، و توانایی پیش‌بینی الگوهای ناشناخته، قادر است نقش مؤثری در پایش تهدیدات مرتبط با عوامل بیولوژیکی ایفا کند. بنابراین سوال این است که چگونه هوش مصنوعی می‌تواند به عنوان ابزار مؤثر در پیشگیری و مقابله با تهدیدات ترور بیولوژیکی ایفای نقش کند؟ روش تحقیق در این مقاله توصیفی - تحلیلی است و یافته‌ها نشان دهنده آن است که استفاده صحیح از ظرفیت‌های هوش مصنوعی در شناسایی تهدیدات زیستی، پیش‌بینی الگوهای خطرناک، و ارائه راهکارهای مناسب برای مقابله، نه تنها به افزایش امنیت زیستی کمک می‌کند، بلکه با تدوین قوانین حقوقی شفاف در حفاظت از حریم خصوصی افراد نیز همسو خواهد بود.

کلمات کلیدی: هوش مصنوعی، ترور بیولوژیک، تهدیدات، پیشگیری، مقابله.



۱. مقدمه

هوش مصنوعی* به عنوان یکی از فناوری‌های پیشرفته و تحول‌زا، توانسته است در بسیاری از حوزه‌ها نقش مهمی ایفا کند و تأثیرات چشمگیری بر روندهای امنیتی و مدیریتی بگذارد. یکی از حوزه‌هایی که هوش مصنوعی می‌تواند به طور قابل توجهی مفید واقع شود، پیشگیری و مقابله با تهدیدات ترور بیولوژیکی است که از جدی‌ترین چالش‌های امنیت جهانی شناخته می‌شود. تهدیدات ناشی از ترور بیولوژیکی که از طریق استفاده غیرقانونی از عوامل بیولوژیکی، مانند ویروس‌ها و باکتری‌های خطرناک، به منظور آسیب رساندن به جوامع انسانی به وقوع می‌پیوندند، رو به افزایش هستند و مقابله صحیح و به موقع با این نوع تهدیدات نیازمند بهره‌گیری از فناوری‌های نوین است. در همین راستا، هوش مصنوعی با ارائه قابلیت‌های پیشرفته در تحلیل داده‌ها، پیش‌بینی رفتارها و اتوماسیون فرآیندها، فرصت‌های جدیدی برای مدیریت این نوع مخاطرات فراهم کرده است.

در ابتدا باید تأکید کرد که ویژگی‌های خاص هوش مصنوعی در تحلیل داده‌های پیچیده و حجیم، آن را به ابزاری قدرتمند در شناسایی تهدیدات بیولوژیکی تبدیل کرده است. سیستم‌های مبتنی بر هوش مصنوعی قادرند عوامل مرتبط با یک حمله احتمالی را، از ترکیبات ژنتیکی مواد بررسی‌شده تا روند انتشار بیماری‌ها در جامعه، سریع‌تر و دقیق‌تر تحلیل کنند. این توانایی‌ها زمینه‌ساز شناسایی زودهنگام منابع احتمالی خطرات بیولوژیکی می‌شود و اجازه می‌دهد اقدامات پیشگیرانه قبل از وقوع بحران اجرا شوند. افزون بر این، هوش مصنوعی می‌تواند با استفاده از الگوریتم‌های پیشرفته خود، روندهای گسترش عوامل بیولوژیکی را پیش‌بینی کرده و از این طریق به نهادهای امنیتی و سلامت عمومی کمک کند تا برنامه‌های مداخله‌ای مؤثر تدوین کنند. (فتیحی زاده، ۱۴۰۴: ۱۱)

از منظر حقوقی، استفاده از فناوری‌های هوش مصنوعی در مدیریت ترور بیولوژیکی باید تحت قوانین مشخص و شفاف انجام گیرد. هرچند هوش مصنوعی منافع بسیاری در این زمینه دارد، اما نگرانی‌هایی نیز وجود دارد که نیازمند نظارت دقیق حقوقی هستند. برای مثال، جمع‌آوری داده‌های حساس مرتبط با سلامت عمومی برای استفاده در تحلیل الگوریتم‌ها ممکن است مسائل مربوط به حریم خصوصی افراد را تحت تأثیر قرار دهد. بنابراین قانون‌گذاری شفاف که بتواند هم امکان بهره‌گیری کامل از ظرفیت‌های هوش مصنوعی را فراهم کند و هم مانعی برای نقض حقوق بنیادی افراد نباشد، ضروری است. علاوه بر آن، تعیین مسئولیت قانونی در برابر خطاهای احتمالی سیستم‌های مبتنی بر هوش مصنوعی نیز یکی دیگر از موضوعات حقوقی مهم است که باید مورد توجه قرار گیرد. همچنین باید گفت که استفاده گسترده از هوش مصنوعی در ایجاد سیستم‌های پیشگیری و مدیریت بحران مربوط به ترور بیولوژیکی نیازمند همکاری چندجانبه بین‌المللی است. ترور بیولوژیکی اغلب فراتر از مرزهای ملی عمل می‌کند و آسیب‌های آن دامنه‌ای جهانی دارند؛ بنابراین هرگونه تلاش مؤثر برای مقابله با این تهدیدها نیازمند تعامل بین دولت‌ها، نهادهای بین‌المللی و متخصصان حوزه حقوق، پزشکی، فناوری اطلاعات و امنیت است. مقررات بین‌المللی مانند کنوانسیون سلاح‌های بیولوژیکی نقش مهمی در هدایت این همکاری‌ها ایفا می‌کنند، اما با توجه به سرعت پیشرفت فناوری‌هایی نظیر هوش مصنوعی، بازنگری و بروزرسانی مداوم چنین مقرراتی اجتناب‌ناپذیر خواهد بود.

در نهایت مسئله دیگری که باید مدنظر گرفت، اخلاقیات مرتبط با استفاده از هوش مصنوعی در حوزه امنیت زیستی است. هوش مصنوعی دارای قدرت ایجاد تغییرات اساسی در نحوه اداره بحران‌ها و مدیریت تهدیدات است؛ اما این موضوع نیازمند هدایت مناسب اخلاقی است تا از سوءاستفاده احتمالی از فناوری جلوگیری شود. برای نمونه، امکان توسعه الگوریتم‌هایی توسط گروه‌های غیرقانونی برای شناسایی نقاط ضعف سیستم‌های امنیت زیستی یا حتی تسریع انتشار عوامل بیولوژیکی خود نشان‌دهنده ضرورت ایجاد چارچوب‌های اخلاقی محکم در این زمینه است. بر این مبنا مقاله حاضر به دنبال پاسخ به

* - Artificial intelligence



این سوال است که چگونه هوش مصنوعی می تواند به عنوان ابزار موثر در پیشگیری و مقابله با تهدیدات ترور بیولوژیکی ایفای نقش کند؟

۲. ادبیات تحقیق

مفهوم و ماهیت تهدیدات ترور بیولوژیکی نشانگر یکی از پیچیده ترین و حساس ترین مسائل امنیتی در عرصه بین المللی و داخلی است. این نوع تهدید به دلیل ماهیت خاص خود، ابعاد گسترده ای از خطرات برای انسان ها، حیوانات و محیط زیست ایجاد می کند و چالش های حقوقی، علمی و اخلاقی قابل توجهی به همراه دارد.

ترور بیولوژیکی به طور کلی به استفاده عمدی از عوامل زیستی نظیر ویروس ها، باکتری ها، توکسین ها یا فرآیندهای اصلاح شده ژنتیکی اشاره دارد که با اهداف سیاسی، مذهبی یا اقتصادی طراحی می شود. این فعل می تواند خسارات جدی و حتی برگشتناپذیری بر سلامت عمومی و ساختارهای اجتماعی وارد کند (دریایی، ۱۳۹۴: ۴۶). رویکرد بین المللی نسبت به این مسئله در اسناد معتبر نظیر کنوانسیون سلاح های بیولوژیکی ۱۹۷۲ و پروتکل ژنو ۱۹۲۵ به وضوح مشخص شده است. بر اساس این اسناد، تولید، انباشت یا استفاده از سلاح های بیولوژیکی به عنوان عملی غیرقانونی و جرمی بین المللی شناخته می شود. اصول بنیادینی همچون ممنوعیت استفاده از سلاح های زیستی* به صورتی محکم و غیرقابل تفسیر در حقوق بین الملل تاکید شده است. (اسکندری صدیقی، ۱۳۹۸: ۸-۹)

یک وجه مهم دیگر در تحلیل تهدیدات ترور بیولوژیکی، تمایز آن با بیوتروریسم داخلی است. در حقوق کیفری داخلی، چنین اعمالی علاوه بر اینکه جرائم سنگینی علیه امنیت ملی تلقی می شوند، می توانند به دلیل وسعت تاثیرگذاری شان زیر مجموعه جرائم علیه بشریت نیز قرار گیرند. این مسئله هنگامی بارزتر می شود که حملات بیولوژیکی موجب انتشار بیماری های اپیدمیک گسترده گردد که نه تنها جان انسان ها بلکه بنیان های جوامع را تهدید می کند (فتحی زاده، ۱۴۰۴: ۳۲). همچنین لازم به ذکر است که ترور بیولوژیکی علاوه بر ابعاد حقوقی و کیفری، جنبه هایی علمی و فنی نیز دارد. پیچیدگی فناوری مورد استفاده برای ایجاد عوامل بیولوژیکی خطرناک و قابلیت اصلاح ژنتیکی آن ها موجب شده تا مقابله با این تهدیدات نیازمند توسعه ای ابزارهای پیشرفته جهت تشخیص، پیشگیری و مقابله باشد. این امر همکاری میان رشته ای گسترده ای بین دولت ها، سازمان های علمی و نهادهای پزشکی را ضروری کرده است.

به طور کلی، ترور بیولوژیکی را باید یکی از چالش های نوظهور در قرن جدید دانست که برای مواجهه با آن، هم افزایی بین کشورها و تقویت ظرفیت های قانونی و اجرایی ضروری است. علاوه بر تنظیم قوانین سختگیرانه، ایجاد سیستم های نظارتی مؤثر و تشویق به اشتراک دانش جهانی در زمینه علوم زیستی، از گام های کلیدی برای کاهش احتمال وقوع چنین وقایعی محسوب می شود. تنظیم فرآیندهای عملیاتی استاندارد جهت پاسخگویی سریع در زمان بروز بحران، اهمیت ویژه ای داشته و در سیاستگذاری های امنیت داخلی و بین المللی باید مورد توجه قرار گیرد.

۳. مسئولیت های حقوقی و بین المللی (پیوندی میان هوش مصنوعی و ترور بیولوژیک)

یکی از موضوعات پیچیده و حساس در دنیای امروز، پیوند عمیق میان فناوری های پیشرفته و چالش های حقوقی و اخلاقی نوظهور است. توسعه بی امن هوش مصنوعی و فناوری های مرتبط با آن، زمینه ساز بروز تحولات بزرگی در علوم مختلف شده و در کنار فرصت هایی که فراهم کرده، مخاطراتی نیز به همراه داشته است. از جمله این مخاطرات می توان به سوءاستفاده احتمالی از ابزارهای هوش مصنوعی برای برنامه ریزی و اجرای اقدامات غیرقانونی اشاره کرد، چالشی که مرزهای اخلاقی، قانونی، و بین المللی را به طرز بی سابقه ای به آزمون می کشد. در این میان، اتصال بین هوش مصنوعی و تهدیدات مبتنی بر ترور بیولوژیک نشان دهنده وضعیتی بحرانی است که نیازمند بررسی دقیق و جدی توسط کارشناسان حوزه های مختلف، از علوم فناوری گرفته تا حقوق بین الملل، است. این ارتباط نه تنها پرسش های جدید و دشواری را در زمینه مسئولیت های حقوقی افراد و نهادهای مرتبط مطرح می سازد، بلکه همکاری های جهانی و نظارت قانونی دقیق تری را

* - non-use of biological weapons



برای جلوگیری از تهدیدهای احتمالی طلب می‌کند. در چنین بستری، تحلیل ابعاد حقوقی، بین‌المللی و داخلی این موضوع اهمیتی ویژه یافته و نقشی کلیدی در شکل‌دهی به سیاست‌ها و اقدامات آینده دارد.

۱-۳- بعد بین‌المللی

تحلیل حقوقی و بررسی مسئولیت‌های بین‌المللی در رابطه با استفاده از هوش مصنوعی در بستر حقوق بین‌الملل، ابعاد متعددی دارد. در این حوزه، تعامل مفاهیم حقوقی نظیر مسئولیت دولت‌ها و حاکمیت نظارتی بین‌المللی با تکنولوژی‌های پیشرفته و پیچیده، چالش‌های جدیدی را مطرح کرده است. یکی از مهم‌ترین موضوعات، نظارت بر کاربردهای مخرب هوش مصنوعی به خصوص در زمینه‌های بیولوژیکی و زیستی است. این مسئله از منظر حقوق بین‌الملل عمومی و همچنین حقوق کیفری بین‌المللی قابل تحلیل است.

در حقوق بین‌الملل عمومی، دولت‌ها بنا به اصول پذیرفته‌شده مسئولیت دارند تا اقدامات خود یا نهادهای تحت اختیارشان را کنترل کنند. ماده ۲ کنوانسیون سلاح‌های بیولوژیکی و اصول عرفی مرتبط با مسئولیت دولت‌ها تأکید دارد که نظارت کافی بر فناوری‌های حساس از جمله فناوری هوش مصنوعی امری ضروری است. عدم انجام چنین وظایفی می‌تواند موجب مسئولیت دولت‌ها در موارد نقض گردد. به عبارتی، اگر دولت‌ها در پایش کافی فناوری‌های هوش مصنوعی کوتاهی کرده و اجازه دهند این فناوری‌ها توسط شرکت‌ها یا نهادهای خصوصی برای اهداف مخرب مانند ترور بیولوژیکی به کار رود، طبق اصول عدم مداخله و ضرورت پیشگیری از تهدیدهای جهانی زیستی، مسئول تلقی می‌شوند (رنجبر، ۱۳۹۹: ۵۲). با توجه به تغییرات جهانی و ظهور فناوری‌های نوین، پیشنهادهایی برای اصلاح مقررات و تقویت نظام کنترل جمعی در این عرصه ارائه شده است. یکی از این راهکارها، پیشنهاد افزودن مفاهیمی نظیر «نظارت زیستی- هوش مصنوعی» یا «امنیت زیستی الگوریتمی» به کنوانسیون سلاح‌های بیولوژیکی است. این مفاهیم تمرکز بر الزام کشورهای عضو به نظارت دقیق بر الگوریتم‌های مرتبط با امنیت زیستی و سلامت حیاتی دارند. چنین اصلاحاتی می‌تواند سازوکاری جامع‌تر برای مقابله با سوء استفاده‌های فناورانه در سطح بین‌المللی ایجاد کند.

از سوی دیگر، حقوق کیفری بین‌المللی ابزار قدرتمندی برای پاسخگویی به سوء استفاده از هوش مصنوعی در ارتکاب جرایم بزرگ ارائه می‌دهد. صلاحیت دیوان کیفری بین‌المللی* نیز در این حوزه قابل بررسی است. براساس بند (ب) ماده ۸ اساسنامه رم که «استفاده از سلاح‌های ممنوعه» را جرم می‌شمارد، بهره‌گیری از هوش مصنوعی در طراحی ابزارهای حمله بیولوژیکی با تلفات گسترده می‌تواند جرم قلمداد شود. این امر نشان‌دهنده نقش حیاتی مقررات کیفری بین‌المللی در مواجهه با تهدیدات مدرن است. در برخی موارد شاید نقش توسعه‌دهندگان الگوریتم‌های هوش مصنوعی نیز مورد توجه قرار گیرد. اگر مشخص شود که این افراد یا نهادها آگاهانه ابزارهایی طراحی کرده‌اند که امکان استفاده برای مقاصد مجرمانه مانند تسهیل در حملات بیولوژیکی را فراهم آورده، ممکن است تحت عنوان معاونت یا مشارکت در جرم پاسخگو باشند (هاشمی، ۱۳۹۸: ۶۷). این موضوع ضرورت تعریف دقیق مسئولیت کیفری برای نقش‌آفرینان غیرمستقیم در زنجیره تولید فناوری‌های پیشرفته را آشکار می‌کند.

به طور کلی، توسعه و استفاده از فناوری‌های پیچیده مانند هوش مصنوعی مستلزم تنظیم چارچوب‌های حقوقی روشن و جامع است. چنین چارچوب‌هایی لازم است که نه تنها نقش دولت‌ها را در پیشگیری از سوء استفاده فناوری مدنظر قرار دهند، بلکه به تعاملات فنی نهادهای خصوصی و توسعه‌دهندگان فناوری نیز بپردازند. افزون بر این، ابزارهایی مانند تعهدات نظارتی بین‌المللی و ایجاد یک نظام پاسخگویی کیفری فراگیر می‌تواند تضمینی برای کاهش مخاطرات ناشی از سوء استفاده از این فناوری‌ها ارائه دهد. این موضوع نشان می‌دهد که حقوق بین‌الملل عمومی و کیفری هر دو قابلیت انطباق با شرایط جدید فناوری را دارند. هرچند تدوین مقررات جدید و ایجاد توافقات جمعی میان کشورها برای مواجهه مؤثرتر با

* - ICC



چالش‌ها اهمیت ویژه‌ای پیدا کرده است. بنابراین، ارتقای همکاری‌های جهانی و شفاف‌سازی مسئولیت‌ها می‌توانند گامی مؤثر در جهت حفاظت از امنیت زیستی و جلوگیری از تهدیدهای نوظهور باشد.

۲-۳- بعد داخلی

در نظام حقوقی فعلی ایران، «ترور بیولوژیک» به‌عنوان یک جرم مستقل تعریف نشده است؛ با این حال، امکان بررسی چنین اعمالی در قالب قوانین موجود وجود دارد. یکی از چارچوب‌هایی که می‌تواند به این موضوع مرتبط باشد، قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ است. در این قانون، استفاده از سامانه‌های هوش مصنوعی یا شبکه‌های رایانه‌ای برای انتشار یا کنترل عوامل بیولوژیکی شاید قابلیت انطباق داشته باشد، به‌خصوص در مواردی که این ابزارها بخشی از فرایند ارتکاب جرم باشند. این موضوع نشان‌دهنده نزدیکی مفاهیم فناوری مدرن و ترور بیولوژیک در بخش‌هایی از قوانین موجود است. از سوی دیگر، قانون مجازات اسلامی و به‌ویژه مواد ۵۰۸ و ۵۱۱ کتاب پنجم تعزیرات به همکاری با گروه‌های تروریستی و اقدامات علیه امنیت ملی اشاره دارند. هرچند این مواد به‌طور خاص به استفاده از عوامل بیولوژیک اشاره نمی‌کنند، اما جرم‌انگاری فعالیت‌هایی که تهدیدی علیه امنیت ملی محسوب شوند، می‌توانند با اعمال بیولوژیکی مرتبط باشند. این شمول نسبی قوانین عمومی ضدتروریستی در موارد مشابه، ظرفیت بالقوه‌ای برای برخورد با ترور بیولوژیک به‌وجود آورده است. (مرادی، ۱۴۰۳: ۸-۹)

همچنین قانون مقابله با تامین مالی تروریسم با تعریف نسبتاً گسترده‌ای از ترور، به بخش‌های مختلف اقدامات تروریستی اشاره دارد. با این حال در متن این قانون، هیچ اشاره مستقیمی به به‌کارگیری ابزارهای بیولوژیک نشده است (کرامت میرشکارلو، ۱۴۰۲: ۳). همین امر فضای خالی حقوقی قابل توجهی ایجاد کرده که می‌تواند به سوء استفاده از خلأهای قانونی منجر شود. بررسی دقیق‌تر محتویات این قانون نشان می‌دهد که علیرغم جامعیت نسبی در تعریف اصول کلی تروریسم، هنوز در برابر تهدیدهای نوین تروریستی، نقص‌هایی وجود دارد. قانون حفاظت در برابر اشعه و مواد پرتوزا مصوب سال ۱۳۶۸ نیز تا حدودی به حوزه‌های مرتبط با تهدیدات فناورانه می‌پردازد؛ اگرچه محوریت مواد این قانون بیشتر بر جنبه‌های پرتوایی متمرکز است و نسبت به تهدیدات ناشی از عوامل بیولوژیکی مستقیم نمی‌باشد (کرامت میرشکارلو، ۱۴۰۲: ۳). این قانون نیز اگرچه می‌تواند در برخی سناریوهای بسیار خاص کاربرد داشته باشد، اما آن‌طور که انتظار می‌رود جامعیت کافی برای مواجهه با ترور بیولوژیکی را ندارد.

با توجه به موارد مورد بررسی، عدم وجود تعریف مستقل از «ترور بیولوژیک» در قوانین کیفری ایران یکی از نقاط ضعف مهم در نظام حقوقی کشور تلقی می‌شود. در عصری که تهدیدات نوین مانند بهره‌گیری از عوامل بیولوژیک برای مقاصد تروریستی رو به گسترش هستند، جای خالی یک قانون مشخص و جامع در این زمینه احساس می‌شود. چنین خلأ قانونی نه‌تنها امکان واکنش پیشگیرانه و موثر را کاهش می‌دهد، بلکه زمینه‌ساز سوءاستفاده و ایجاد چالش‌های امنیتی جدید خواهد شد. اگرچه مواردی از سایر قوانین موجود قابلیت انطباق نسبی با اعمال مرتبط دارند، اما کافی نیستند تا ساختار حقوقی کشور بتواند با پیچیدگی‌های ترور بیولوژیکی در دنیای امروز همگام شود. ایجاد و تدوین یک چارچوب قانونی تخصصی و هدفمند برای جرم‌انگاری و مقابله مؤثر با «ترور بیولوژیک» ضرورتی حیاتی محسوب می‌شود که باید مورد توجه قانون‌گذار قرار گیرد.

۴- نقش و چالش‌های هوش مصنوعی در ترور و مقابله با ترور بیولوژیک

هوش مصنوعی در سال‌های اخیر نقشی کلیدی در پیشگیری، شناسایی و مقابله با تهدیدات زیستی و بیولوژیکی ایفا کرده است. با پیشرفت فناوری‌های یادگیری عمیق و تحلیل داده‌های پیچیده، استفاده از هوش مصنوعی در این حوزه به شکل چشم‌گیری افزایش یافته و توانسته نیازهای علمی و عملی زیادی را مرتفع سازد. یکی از جنبه‌های برجسته این فناوری در پیشگیری، توانایی تشخیص زودهنگام تهدیدات است. هوش مصنوعی می‌تواند از طریق تحلیل داده‌های نامتعارف در آزمایشگاه‌ها و سازمان‌های مرتبط، الگوهای غیرعادی را شناسایی کند و با پیش‌بینی حرکات و جهش احتمالی عوامل



بیماری‌زا، هشدارهای لازم را ارائه دهد. همچنین این فناوری امکان بهینه‌سازی سیستم‌های پایش مرزهای زیستی را فراهم می‌آورد، که به‌عنوان یک فناوری واکنش سریع در شناسایی تهدیدات محیطی اهمیت بالایی دارد.

در هنگام وقوع حمله زیستی یا شایع شدن یک بیماری جدید، هوش مصنوعی قادر است فرآیند مقابله و پاسخگویی سریع را به شدت تقویت کند. از طریق مدل‌سازی اپیدمیولوژیک، می‌توان گسترش احتمالی بیماری‌ها را شبیه‌سازی کرده و سرعت اقدام‌های اضطراری را افزایش داد. همچنین بهره‌گیری از هوش مصنوعی می‌تواند توزیع واکسن‌ها و داروها را بهینه نماید و زمان لازم برای دسترسی اقشار مختلف جامعه به این منابع حیاتی را کاهش دهد. در مدیریت داده‌های مرتبط با بیماران نیز، فناوری هوش مصنوعی می‌تواند تأثیر بسزایی داشته باشد؛ به‌ویژه در زمینه تجزیه و تحلیل اطلاعات، تعیین منشأ آلودگی، و حتی کمک به کاهش خطاهای انسانی در روند درمان و مدیریت بحران. (عباس نژادورزی و همکاران، ۱۴۰۳: ۹۱)

با وجود تمام مزایایی که این فناوری ارائه می‌دهد، خطرات بالقوه‌ای هم ممکن است از آن ناشی شود که توجه خاصی را می‌طلبد. یکی از موضوعات بسیار حساس در این زمینه، امکان سوءاستفاده از همین فناوری برای طراحی عوامل زیستی خطرناک است. با ظهور مدل‌های پیشرفته مولد زیستی که با استفاده از داده‌های ژنتیکی می‌توانند سموم یا ویروس‌های اصلاح‌شده تولید کنند، احتمال افزایش تهدیداتی وجود دارد که توسط گروه‌ها یا افراد غیرمسئول مورد بهره‌برداری قرار گیرد. قابلیت طراحی ساختارهای بیولوژیکی پیچیده در آزمایشگاه‌های مجازی، نقطه‌ای بحرانی است که باید با نهایت دقت و نظارت کنترل شود تا از هرگونه استفاده نادرست جلوگیری به عمل آید (کاکویی، ۱۴۰۰: ۷۹). در مجموع، اگر چه هوش مصنوعی پتانسیل عظیمی برای تحول در زمینه پیشگیری، کشف و مقابله با تهدیدات زیستی دارد، ولی بدون نظارت دقیق بر کاربردهای آن، می‌تواند خطرآفرین باشد. دستیابی به این توازن نیازمند همکاری بین‌المللی، وضع مقررات اخلاقی مشخص، و پایش مستمر فعالیت‌ها در این حوزه است. با اتخاذ تدابیر مناسب، هوش مصنوعی نه‌تنها به عنوان ابزار مهمی در خدمت سلامت جهانی قرار می‌گیرد بلکه می‌تواند از گسترش تهدیدات زیستی جلوگیری کرده و پایداری جوامع انسانی را تضمین نماید.

۵- تحلیلی پیشگیرانه

یک روش نهایی برای کاهش خطر بلایای بیولوژیکی وجود دارد که فراتر از برنامه‌ریزی برای واکنش و دفاع پیش می‌رود. این روش بر مدیریت بهینه فناوری‌های نوین تمرکز دارد؛ راهکاری که ممکن است تنها مسیر واقعی برای جلوگیری از وقوع حملات بیولوژیکی گسترده باشد. دولت‌ها ابزارهای متنوعی برای سامان‌دهی و نظارت بر پیشرفت‌های فناورانه در اختیار دارند. برای مثال، آن‌ها می‌توانند تأمین مالی آزمایش‌های خاص را متوقف کنند یا حتی برخی از این آزمایشات را به طور کامل ممنوع نمایند. از سوی دیگر، مقامات قادرند مجوزهای قانونی لازم برای انجام برخی فعالیت‌ها را الزامی کنند و نیز نظارت بیشتری بر اتوماسیون آزمایشگاه‌های آینده اعمال کنند. در کنار این اقدامات، ضروری است که دولتمردان اکوسیستم حمایتی برای تحقیق و توسعه زیستی فراهم آورند. به عنوان نمونه، می‌توان شرکت‌های فروشنده مواد زیستی نظیر اسیدهای نوکلئیک، سویه‌ها، معرف‌ها و تجهیزات موردنیاز علوم زیستی را موظف ساخت تا اصول «شناخت مشتری» را رعایت کنند. بر این اساس، شرکت‌ها باید هویت مشتریان و ماهیت فعالیت‌هایشان را تأیید کنند و اطمینان داشته باشند که کالاهای زیستی تنها به مراکز قانونی و شناخته‌شده ارسال می‌شوند. رویکرد مشابهی مدت‌هاست در مؤسسات مالی اعمال شده تا از جریان پول به سمت شبکه‌های مجرمانه جلوگیری شود (جعفری هزارانی، ۱۴۰۳: ۲۷). افزون بر این، سیاست‌گذاران باید چارچوب‌هایی هوشمند برای نظارت بر فعالیت‌های زیستی ممنوع طراحی کنند تا با شناسایی سریع‌تر چنین اقدامات خطرناکی از وقوع حملات پیشگیری شود.

هوش مصنوعی و مهندسی بیولوژیکی با وجود قابلیت‌های چشمگیرشان، چالش‌های بزرگی نیز به همراه دارند. از همین امروز باید دولت‌ها سیاست‌های خود در حوزه دفاع بیولوژیکی را با توجه به امکانات هوش مصنوعی تدوین کنند.



شرکت‌های تکنولوژی، پیش از ارائه مدل‌های بزرگ زبانی، شیوه‌های امنیتی متنوعی همچون خطوط قرمز طراحی کرده‌اند؛ سیستمی که جلوی عبور کاربران از محدودیت‌های تعیین‌شده را می‌گیرد. به عنوان مثال، ChatGPT-4 و Claude 3.5 Sonnet از پاسخ به پرسش‌هایی که مستقیماً نحوه تکامل ویروس‌ها برای تخریب منابع زیستی را مطرح می‌کنند، خودداری می‌کنند. اما چالش زمانی نمایان می‌شود که کاربران وارد روشی غیرمستقیم برای دریافت اطلاعات خطرناک شوند؛ در این حالت ممکن است مدل‌ها راهنمایی‌هایی ارائه دهند که قابل استفاده باشد. بدین ترتیب، نیاز به تدابیر حفاظتی بیشتری برای محدودسازی ارائه اطلاعات حساس وجود دارد، و نقش دولت‌ها در این میان بسیار کلیدی است. مدیریت خطرات فناوری‌های جدید کار آسانی نخواهد بود. البته برخی ابزارهای کنترل ممکن است سرعت تحقیقات مشروع را کاهش دهند، اما نظارت هوشمندانه اجتناب‌ناپذیر است. حقیقت این است که با وجود همه مزایای برجسته‌ای که هوش مصنوعی و مهندسی بیولوژیکی دارند، چالش‌ها و تهدیدهای بزرگی نیز همراه‌شان است؛ بنابراین جوامع و دولت‌ها باید با دیدگاهی دقیق و منطقی فواید فعلی و احتمالی این پیشرفت‌ها را مقابل مخاطرات بالقوه‌شان قرار دهند. یکی از بزنگاه‌های قرن بیستویکم این خواهد بود که آیا جهان می‌تواند با ظهور فناوری‌های نوین که وعده تغییرات بنیادین در تمدن بشری را ارائه می‌دهند کنار بیاید یا خیر. همانند انرژی هسته‌ای، این فناوری‌ها دستاورد پژوهش‌های انسانی هستند، اما همانگونه که در مورد فناوری هسته‌ای امکان بازگشت به عقب وجود ندارد، سیاست‌گذاری هوشمندانه می‌تواند مسیر بهره‌برداری مطلوب از این پیشرفت‌ها را تضمین کند. آینده نیازمند داوری روزانه مبتنی بر خرد، انعطاف‌پذیری و صبر خواهد بود تا اطمینان حاصل شود که از خطرات بزرگ جلوگیری شده و مسیر استفاده پایدار هموار گردد.

۴. نتیجه گیری

ترور بیولوژیک، معجونی پیچیده از زیست‌فناوری و هوش مصنوعی است که به‌طور بالقوه قادر است مرزهای میان مفاهیمی چون جرم جنگی، تروریسم و جنایت علیه بشریت را مخدوش سازد. این مفهوم که در دهه‌های اخیر با رشد حیرت‌آور فناوری‌های مدرن به یکی از تهدیدهای جدی تبدیل شده، نه تنها جوامع مدرن، بلکه نظام‌های حقوقی و قوانین سنتی را نیز به چالش کشیده است. ترکیب دانش ژنتیک با توانمندی‌های پردازشی هوش مصنوعی، امکان خلق ابزارهایی را فراهم کرده که می‌توانند از تنظیم دقیق رفتار سیستم‌های زیستی گرفته تا تولید عوامل بیماری‌زای مهندسی‌شده را در بر گیرند. همین گستردگی در ابعاد تهدیدآمیز، درک جدیدی از امنیت زیست محیطی و زیستی را ایجاد می‌کند. در این میان، نظام حقوقی ایران نیز از این تغییرات مصون نمانده است. بررسی قوانین موجود نشان می‌دهد که هنوز خلایق قابل توجهی در جرم‌انگاری رفتارهایی که در حیطه تهدیدهای زیستی تعریف می‌شوند، وجود دارد. گرچه در قوانین کیفری ایران تلاش‌هایی برای الحاق مفاهیمی چون جرایم زیست‌محیطی یا عملکردهای ضد امنیت عمومی دیده می‌شود، اما حوزه ترور بیولوژیک با توجه به پیچیدگی ماهیتی و نیاز به ابزارهای حقوقی تخصصی همچنان بدون پاسخ مانده است. به بیان دیگر، چارچوب تقنینی کنونی توانایی مقابله مؤثر با تهدیدهایی که نتیجه دستکاری عمدی در سیستم‌های زیستی هستند، ندارد. در سطح بین‌المللی نیز با وجود اسناد و معاهدات متعددی مانند کنوانسیون سلاح‌های بیولوژیک، ضعف در ضمانت اجرا و تصمیم‌گیری‌های قاطعانه مشهود است. این موضوع نشان می‌دهد که هنگام مواجهه با پدیده‌هایی همچون ترور بیولوژیک که ماهیتی فراملی دارد، کشورهای مختلف ناگزیر به تدوین و به‌روزرسانی نظام‌های حقوقی خود بر اساس استانداردهای مشترک جهانی خواهند بود. این ضرورت در دوران هوش مصنوعی و پیشرفت سریع فناوری بیش از گذشته احساس می‌شود، چرا که یک نرم‌افزار ساده می‌تواند به‌اندازه یک سلاح کشتار جمعی قدرت تخریب داشته باشد.

پیشرفت فناوری‌ها و پردازشگرهای مقرون به صرفه علاوه بر تسهیل پیشرفت علمی، امکان سوءاستفاده از قدرت هوش مصنوعی برای طراحی عوامل بیماری‌زا یا حملات بیولوژیک هدفمند را نیز قابل تصور ساخته است. تفاوت اساسی این نسل از تهدیدها با مفاهیم سنتی تروریسم در این است که حملات زیستی می‌توانند بدون بر جای گذاشتن ردپایی فیزیکی



انجام شوند، یا حتی اثراشان تا مدت‌ها پس از وقوع آشکار نشود. این امر تلاش برای شناسایی عوامل و واکنش سریع نسبت به چنین حملاتی را دشوارتر می‌کند. از این‌رو، بازبینی جامع‌تر قوانین ملی با تمرکز بر ادغام ظرفیت‌های علمی و حقوقی اهمیت اساسی دارد. استقرار سیاست جنایی خاص و ساخت‌یافته که بتواند هم افراد متخلف را شناسایی کند و هم بستر پیشگیری را فراهم آورد، ضروری به نظر می‌رسد. افزون بر این، تقویت همکاری‌های منطقه‌ای و جهانی می‌تواند به‌عنوان گامی موثر در مهار خطرات ناشی از سوءاستفاده از روش‌ها و ابزارهای نوین تکنولوژیک مورد توجه قرار گیرد. در نهایت، عصری که در آن فناوری با سرعتی بی‌سابقه در حال تحول است، نیازمند نظام حقوقی‌ای است که نه صرفاً واکنشی بلکه فعالانه عمل کند. این نظام باید ضمن دفاع از امنیت جسمانی و اخلاقیات انسانی، بتواند خط قرمزی واضح میان استفاده صلح‌آمیز از فناوری‌ها و سوءاستفاده مجرمانه از آنها ترسیم کند. تنها با چنین رویکرد جامعی است که می‌توان مقابل تهدیدهایی نظیر ترور بیولوژیک ایستادگی کرد؛ تهدیدهایی که نه‌تنها امنیت جوامع حاضر بلکه حق حیات نسل‌های آینده را نیز به خطر می‌اندازند.

پیشنهادهای

- اضافه کردن فصل جداگانه تحت عنوان «جرایم مرتبط با ترور بیولوژیک و فناوری‌های پیشرفته» به قانون مجازات اسلامی.
- طراحی و اجرای نظام مجوزدهی و نظارت بر سامانه‌های هوش مصنوعی زیستی تحت نظارت شورای عالی امنیت ملی.
- تعیین مسئولیت کیفری مضاعف برای شرکت‌های فناوری داخلی در صورت صادرات ابزارهای هوش مصنوعی با قابلیت استفاده دوگانه.
- ایجاد چارچوب همکاری بین‌المللی با سازمان‌هایی نظیر سازمان بهداشت جهانی^{*}، کنوانسیون سلاح‌های بیولوژیک[†] و اینترپل در زمینه مقابله با تهدیدات زیستی.
- تصویب «منشور امنیت زیستی و حقوق بشر» به منظور حفظ توازن میان امنیت ملی و آزادی‌های فردی و تضمین حقوق شهروندان در برابر تهدیدات زیستی.

* - WHO

† - BWC



منابع

۱. اسکندری صدیقی، ر. (۱۳۹۸)، "بیوتروریسم"، تهران: انتشارات پشتیبان.
۲. بیافرین، ع. (۱۳۹۹)، "تئوری ترور"، تهران: نشر معارف.
۳. جعفری هزارانی، ن. (۱۴۰۳)، "تحلیل عملیات ترور اسماعیل هنیه در تهران: باگ های امنیتی و درس های اطلاعاتی"، مقالات پیش چاپ سیویلیکا، ۱-۳۰.
۴. دریایی، م.ر. (۱۳۹۴)، "بیوتروریسم در طب غربی"، تهران: موسسه فرهنگی آرمان رشد.
۵. رنجبر، ق. (۱۳۹۹)، "تحلیل سیاسی بیوتروریسم و بررسی نیاز به تدوین سند بین المللی"، تهران: دیبادخت.
۶. عباس نژادورزی، ر. رهی، م. عباس نژادورزی، س. (۱۴۰۳)، "هوش مصنوعی در امنیت سایبری: مفاهیم، کاربرد ها، چالش ها، الگوریتم ها و ابزارها"، تهران: انتشارات فناوری نوین.
۷. فتحی زاده، ن.م. (۱۴۰۴)، "پیشگیری از ترور با هوش مصنوعی"، تهران: هورین.
۸. کرامت میرشکارلو، ی. (۱۴۰۳)، "مسئولیت کیفری ارتکاب ترور سایبری با فناوری هوش مصنوعی در حقوق کیفری بین الملل"، تهران: اولین کنفرانس ملی پژوهش های نوظهور در مدیریت و حقوق با رویکرد شعار سال، ۱-۱۱.
۹. کاکویی، ع. (۱۴۰۰)، "ترور شخصیت"، تهران: به اندیش.
۱۰. مرادی، ع. (۱۴۰۳)، "موانع و چالش های تعقیب و مجازات عاملان ترور دانشمندان هسته ای"، تهران: ششمین کنفرانس بین المللی مطالعات نوین در علوم انسانی، علوم تربیتی، حقوق و مطالعات اجتماعی، ۱-۳۰.
۱۱. هاشمی، ر. (۱۳۹۸)، "سیاست کیفری ایران در قبال بیوتروریسم"، پایان نامه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه علم و فرهنگ.