

نقش هوش مصنوعی در تقویت تاب آوری نظام سلامت در برابر تهدیدات ترور بیولوژیکی (تطبیقی بر حقوق ایران و اتحادیه اروپا)

حسین اسماعیلی^۱

تاریخ دریافت: ۱۴۰۵/۰۳/۰۱ تاریخ چاپ: ۱۴۰۵/۰۶/۳۰

چکیده

ترور بیولوژیکی به عنوان یکی از تهدیدات پیچیده و فرامرزی معاصر، می تواند با ایجاد بیماری، مرگ، هراس عمومی و اختلال در نظم اجتماعی، امنیت ملی و سلامت عمومی را به طور جدی متأثر سازد. در چنین شرایطی، تاب آوری نظام سلامت به عنوان توانایی پیشگیری، آمادگی، شناسایی، پاسخ دهی و بازبایی در برابر بحران های زیستی اهمیت ویژه ای می یابد. پرسش اصلی این پژوهش آن است که هوش مصنوعی چگونه می تواند در تقویت تاب آوری نظام سلامت در برابر تهدیدات ترور بیولوژیکی نقش آفرینی کند و نظام های حقوقی ایران و اتحادیه اروپا چه ظرفیت ها و چالش هایی در تنظیم حقوقی این نقش دارند؟ پژوهش حاضر با رویکردی تحلیلی - تطبیقی، به بررسی نقش هوش مصنوعی در تقویت تاب آوری نظام سلامت در برابر ترور بیولوژیکی و نیز ظرفیت ها و چالش های حقوقی ایران و اتحادیه اروپا در تنظیم این نقش می پردازد. یافته های پژوهش نشان می دهد هوش مصنوعی می تواند از طریق پایش هوشمند داده ها، هشدار زودهنگام، تشخیص سریع، پیش بینی مسیر انتشار بیماری، مدیریت منابع درمانی، تسريع در توسعه دارو و واکسن و مقابله با اطلاعات نادرست، ظرفیت پاسخ نظام سلامت را به طور چشمگیری افزایش دهد. با این حال، بهره گیری مؤثر از این فناوری مستلزم وجود چارچوب های حقوقی شفاف، پاسخ گو و مبتنی بر نظارت انسانی است تا از خطراتی مانند نقض حریم خصوصی، تبعیض الگوریتمی، مسئولیت مبهم، و سوءاستفاده امنیتی جلوگیری شود. بررسی تطبیقی نشان می دهد که اتحادیه اروپا با اتکا به مقرراتی چون حفاظت از داده ها، مقررات هوش مصنوعی و سازوکارهای امنیت سایبری و مدیریت بحران فرامرزی، از نظام حقوقی منسجم تری برخوردار است؛ در حالی که حقوق ایران اگرچه از ظرفیت هایی در قانون اساسی، قوانین سلامت عمومی، پدافند غیرعامل و جرائم رایانه ای برخوردار است، اما همچنان با پراکندگی مقررات، فقدان قانون جامع حفاظت از داده های سلامت و نبود چارچوب اختصاصی برای هوش مصنوعی مواجه است. نتیجه آنکه تحقق بهره برداری مشروع و مؤثر از هوش مصنوعی در مقابله با ترور بیولوژیکی، نیازمند حرکت به سوی حکمرانی حقوق بنیاد، ریسک محور و آینده نگر در حوزه سلامت است.

واژگان کلیدی

ترور بیولوژیکی، هوش مصنوعی، تاب آوری نظام سلامت، حقوق سلامت، حفاظت از داده، اتحادیه اروپا، ایران

۱. کارشناس ارشد رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تاکستان، قزوین، ایران.

۱. مقدمه

ترور بیولوژیکی^۱ یا بیوتروریسم در جهان معاصر، دیگر صرفاً یک تهدید محدود و سنتی علیه سلامت انسان‌ها تلقی نمی‌شود، بلکه پدیده‌ای پیچیده، پنهان و چندبعدی است که می‌تواند با استفاده عمدی از عوامل زیستی مانند ویروس‌ها، باکتری‌ها، سموم زیستی یا سایر عوامل بیماری‌زا، مرگ، بیماری، هراس عمومی، اختلال در نظم اجتماعی و تضعیف امنیت ملی را به دنبال داشته باشد. ویژگی متمایز این نوع تهدید در آن است که برخلاف بسیاری از تهدیدات کلاسیک، غالباً نامرئی، دیرآشکار، فرامرزی و دارای آثار زنجیره‌ای است؛ به گونه‌ای که پیامدهای آن تنها به حوزه سلامت عمومی^۲ محدود نمی‌شود، بلکه می‌تواند اقتصاد، امنیت ملی، اعتماد عمومی، انسجام اجتماعی و کارآمدی نهادهای حاکمیتی را نیز تحت تأثیر قرار دهد (بیافرین، ۱۳۹۹). از این رو، مواجهه با بیوتروریسم نیازمند رویکردی صرفاً درمان‌محور نیست، بلکه مستلزم شکل‌گیری نظامی هوشمند، پیش‌نگر، هماهنگ و تاب‌آور در حوزه سلامت است. در چنین شرایطی، تاب‌آوری نظام سلامت به‌عنوان یکی از مؤلفه‌های اساسی امنیت ملی و سلامت عمومی اهمیت ویژه‌ای پیدا می‌کند. تاب‌آوری نظام سلامت به معنای توانایی این نظام در پیشگیری، آمادگی، شناسایی، پاسخ‌دهی، کنترل و بازیابی در برابر بحران‌ها و تهدیدات شدید، از جمله حملات بیولوژیکی است (اسکندری صدیقی، ۱۳۹۸). تجربه جهانی همه‌گیری کووید-۱۹ نشان داد که حتی نظام‌های سلامت پیشرفته نیز در برابر بحران‌های زیستی گسترده ممکن است با چالش‌هایی چون کمبود منابع درمانی، ضعف در هشدار سریع، اختلال در زنجیره تأمین، ناهماهنگی نهادی، فرسایش اعتماد عمومی و ناتوانی در مدیریت داده‌های گسترده مواجه شوند. افزون بر این، پیشرفت شتابان زیست‌فناوری، مهندسی ژنتیک و دسترسی گسترده‌تر به دانش و امکانات آزمایشگاهی، احتمال سوءاستفاده از عوامل زیستی را افزایش داده و ضرورت بازاندیشی در شیوه‌های سنتی مقابله با تهدیدات زیستی را آشکار ساخته است.

در این میان، هوش مصنوعی می‌تواند به‌عنوان یکی از ابزارهای کلیدی حکمرانی نوین سلامت^۳، نقش قابل توجهی در تقویت تاب‌آوری نظام سلامت ایفا کند. این فناوری از طریق تحلیل سریع و هوشمند داده‌ها، پیش‌بینی الگوهای شیوع، شناسایی زود هنگام ناهنجاری‌های اپیدمیولوژیک، ردیابی روند انتشار بیماری، مدیریت منابع درمانی، پشتیبانی از تصمیم‌گیری مدیران سلامت و حتی تسریع در فرآیند کشف دارو و تولید واکسن، می‌تواند ظرفیت نظام سلامت را برای مقابله با تهدیدات بیولوژیکی افزایش دهد (عباس نژادورزی و همکاران، ۱۴۰۳). در واقع، مقابله مؤثر با بیوتروریسم در عصر داده، بدون بهره‌گیری از سامانه‌های هوشمند پایش، هشدار سریع، تحلیل کلان‌داده‌ها و تصمیم‌سازی الگوریتمی دشوار به نظر می‌رسد. با این حال، استفاده از هوش مصنوعی در چنین حوزه حساسی، صرفاً یک مسئله فنی یا مدیریتی نیست، بلکه با پرسش‌های بنیادین حقوقی و اخلاقی همراه است (کاکویی، ۱۴۰۰)؛ پرسش‌هایی که به حریم خصوصی، حفاظت از داده‌های سلامت، امنیت سایبری، مسئولیت مدنی ناشی از تصمیمات الگوریتمی، تبعیض الگوریتمی، شفافیت، نظارت انسانی و تعارض احتمالی میان ضرورت‌های امنیت ملی و حقوق بنیادین شهروندان مربوط می‌شود.

بر همین اساس، پرسش اصلی این پژوهش آن است که هوش مصنوعی چگونه می‌تواند در تقویت تاب‌آوری نظام سلامت در برابر تهدیدات ترور بیولوژیکی نقش آفرینی کند و نظام‌های حقوقی ایران و اتحادیه اروپا چه ظرفیت‌ها و چالش‌هایی در تنظیم حقوقی این نقش دارند؟ پاسخ به این پرسش از آن جهت اهمیت دارد که بهره‌گیری از هوش مصنوعی در مقابله با بیوتروریسم، تنها زمانی می‌تواند مشروع، مؤثر و پایدار باشد که در چارچوبی حقوقی، شفاف، پاسخ‌گو و مبتنی بر موازنه میان امنیت و آزادی‌های بنیادین شهروندان سامان یابد. بنابراین، تحلیل حقوقی این موضوع باید همزمان دو بُعد را در نظر گیرد: نخست، ظرفیت‌های فناورانه هوش

۱- Biological terror

۲- Public health

۳- New health governance

مصنوعی در افزایش آمادگی و پاسخ نظام سلامت؛ و دوم، الزامات حقوقی لازم برای جلوگیری از سوءاستفاده، نقض حریم خصوصی، تصمیم‌گیری غیرشفاف و تمرکز بیش از حد قدرت در وضعیت‌های اضطراری زیستی. فرضیه پژوهش حاضر بر این مبنا استوار است که هوش مصنوعی می‌تواند از طریق پایش هوشمند داده‌های سلامت، پیش‌بینی شیوع، تشخیص زودهنگام حملات زیستی و بهینه‌سازی پاسخ درمانی، تاب‌آوری نظام سلامت را در برابر تهدیدات بیولوژیکی افزایش دهد؛ اما میزان موفقیت و مشروعیت این نقش‌آفرینی به کیفیت چارچوب‌های حقوقی و نهادی هر نظام حقوقی وابسته است. بر این اساس، به نظر می‌رسد اتحادیه اروپا به دلیل برخورداری از مقررات نسبتاً جامع در زمینه حفاظت از داده‌ها، امنیت سایبری، مدیریت بحران‌های سلامت فرامرزی و تنظیم‌گری هوش مصنوعی، ظرفیت حقوقی بیشتری برای بهره‌گیری مسئولانه از هوش مصنوعی در مقابله با تهدیدات زیستی دارد. در مقابل، در حقوق ایران، نبود قانون جامع و منسجم در زمینه حفاظت از داده‌های سلامت، فقدان مقررات خاص درباره هوش مصنوعی، پراکندگی مقررات مربوط به امنیت زیستی و ضعف سازوکارهای نظارت الگوریتمی، از جمله موانع اصلی استفاده مؤثر، ایمن و مشروع از این فناوری در مقابله با بیوتروریسم محسوب می‌شود.

از این رو، بررسی تطبیقی حقوق ایران و اتحادیه اروپا می‌تواند نشان دهد که هر یک از این نظام‌های حقوقی تا چه اندازه برای بهره‌گیری ایمن و قانونمند از هوش مصنوعی در حوزه مقابله با تهدیدات بیولوژیکی آمادگی دارند. اهمیت و ضرورت چنین پژوهشی در آن است که از یک سو، خطر تهدیدات زیستی نوین در پرتو تحولات فناورانه و تجربه همه‌گیری‌های جهانی افزایش یافته و از سوی دیگر، داده و فناوری به عناصر تعیین‌کننده در مدیریت بحران‌های سلامت تبدیل شده‌اند. در نتیجه، فقدان چارچوب حقوقی مناسب می‌تواند نه تنها کارایی هوش مصنوعی را کاهش دهد، بلکه خود به منشأ تهدیدات جدیدی برای حقوق شهروندان، اعتماد عمومی و امنیت ملی تبدیل شود. بنابراین، پژوهش حاضر می‌کوشد با رویکردی تحلیلی و تطبیقی، ضمن تبیین نقش هوش مصنوعی در تقویت تاب‌آوری نظام سلامت در برابر بیوتروریسم، ظرفیت‌ها و خلأهای حقوقی ایران و اتحادیه اروپا را بررسی کرده و ضرورت حرکت به سوی تنظیم‌گری جامع، مسئولانه و آینده‌نگر در این حوزه را برجسته سازد.

۲. چارچوب مفهومی

ترور بیولوژیکی به معنای استفاده عمدی از عوامل زیستی یا سموم برای ایجاد بیماری، مرگ یا اختلال گسترده در جامعه است؛ تهدیدی که ماهیت آن با پنهان‌کاری، ابهام و قدرت سرایت بالا گره خورده است. این نوع ترور معمولاً به گونه‌ای عمل می‌کند که انتشار آن در مراحل اولیه به سادگی قابل مشاهده نیست و همین پنهان‌بودن، شناسایی سریع منشأ حادثه را دشوار می‌سازد (فتحی زاده، ۱۴۰۴). یکی از مهم‌ترین پیچیدگی‌های آن این است که در بسیاری از موارد، تشخیص اینکه یک بیماری منشأ طبیعی دارد یا نتیجه اقدام عمدی است، به آسانی ممکن نیست. افزون بر این، در جهان به‌هم پیوسته امروز، عوامل بیولوژیکی می‌توانند با سرعتی زیاد و حتی در مقیاس فرامرزی گسترش یابند و پیامدهای آنها تنها به حوزه سلامت محدود نماند، بلکه ابعاد روانی، اجتماعی، اقتصادی و امنیتی گسترده‌ای نیز ایجاد کند. به همین دلیل، مقابله با چنین تهدیدی صرفاً وظیفه نظام درمانی نیست، بلکه نیازمند واکنشی هماهنگ میان نظام سلامت، نهادهای امنیتی، دستگاه‌های اجرایی و سازوکارهای مدیریت بحران است. (غلامی، ۱۳۹۹)

در برابر چنین تهدیدی، مفهوم تاب‌آوری نظام سلامت^۱ اهمیت بنیادی پیدا می‌کند. تاب‌آوری نظام سلامت به توانایی این نظام برای پیشگیری از بحران، آمادگی پیشینی، تشخیص و هشدار سریع، پاسخ مؤثر و هماهنگ، حفظ تداوم خدمات ضروری و در نهایت بازیابی و بازسازی پس از بحران اشاره دارد. به بیان دیگر، یک نظام سلامت تاب‌آور فقط در لحظه وقوع بحران واکنش نشان نمی‌دهد، بلکه از پیش برای مواجهه با آن آماده می‌شود، ظرفیت‌های نظارتی و تشخیصی خود را تقویت می‌کند، زنجیره خدمات حیاتی را حفظ می‌کند و پس از عبور از بحران نیز می‌تواند خود را بازسازی کند و به وضعیت پایدار بازگردد (مولائی فرد و مسعودی فرد، ۱۴۰۴). در زمینه تهدیدات بیولوژیکی، این تاب‌آوری زمانی معنا و کارکرد واقعی پیدا می‌کند که نظام سلامت بتواند

^۱ - Health system resilience

در کوتاه‌ترین زمان ممکن منشأ تهدید را شناسایی کند، مسیرهای انتشار را مهار سازد، از گسترش بیشتر آسیب جلوگیری کند، خدمات درمانی و مراقبتی ضروری را بدون اختلال جدی ادامه دهد و هم‌زمان اعتماد عمومی را از طریق اطلاع‌رسانی مؤثر و مدیریت اجتماعی بحران حفظ کند.

در این میان، هوش مصنوعی^۱ به‌عنوان یکی از ابزارهای نوین و تحول‌آفرین در حوزه سلامت، می‌تواند نقش مهمی در تقویت این تاب‌آوری ایفا کند. هوش مصنوعی در سلامت به مجموعه سامانه‌ها و فناوری‌هایی گفته می‌شود که با تکیه بر داده‌ها و الگوریتم‌ها قادرند وظایفی مانند تشخیص بیماری، پیش‌بینی شیوع، اولویت‌بندی بیماران، تحلیل تصاویر پزشکی، طراحی دارو و پشتیبانی از تصمیم‌گیری بالینی را انجام دهند. اهمیت این فناوری در آن است که می‌تواند سرعت و دقت تحلیل را افزایش دهد، الگوهای پنهان در داده‌های گسترده را آشکار سازد و به تصمیم‌گیران کمک کند تا در شرایط بحرانی واکنش سریع‌تر و دقیق‌تری داشته باشند (فتحی زاده، ۱۴۰۴). از این منظر، هوش مصنوعی تنها یک ابزار فنی نیست، بلکه می‌تواند به بخشی از ظرفیت راهبردی نظام سلامت برای شناسایی زود هنگام تهدیدات، مدیریت بهتر منابع، کاهش خطا، بهبود هماهنگی میان بخش‌ها و ارتقای توان پاسخ در شرایط پیچیده تبدیل شود. بنابراین، پیوند میان مفهوم ترور بیولوژیکی، تاب‌آوری نظام سلامت و کاربردهای هوش مصنوعی نشان می‌دهد که مواجهه مؤثر با تهدیدات زیستی در دنیای امروز، نیازمند نگاهی تلفیقی، آینده‌نگر و چندبخشی است؛ نگاهی که در آن سلامت، امنیت و فناوری در کنار یکدیگر قرار می‌گیرند تا از جامعه در برابر بحران‌های پیچیده و پرمخاطره محافظت شود.

۳. کاربردهای هوش مصنوعی در مقابله با ترور بیولوژیکی

هوش مصنوعی می‌تواند در مقابله با ترور بیولوژیکی نقشی چندلایه و راهبردی ایفا کند، زیرا ماهیت این نوع تهدید با سرعت انتشار، پنهان‌بودن منشأ، دشواری تشخیص اولیه و پیامدهای گسترده اجتماعی همراه است. در چنین شرایطی، اتکا به روش‌های سنتی پایش و تصمیم‌گیری کافی نیست و نظام سلامت نیازمند ابزارهایی است که بتوانند حجم عظیمی از داده‌ها را در زمان کوتاه تحلیل کنند، نشانه‌های غیرعادی را تشخیص دهند و امکان واکنش سریع و هماهنگ را فراهم سازند. از این منظر، هوش مصنوعی نه تنها یک فناوری کمکی، بلکه بخشی از زیرساخت تاب‌آوری سلامت در برابر تهدیدات زیستی محسوب می‌شود. (González, 2023)

یکی از مهم‌ترین کاربردهای هوش مصنوعی در این حوزه، پایش مستمر و هشدار زود هنگام است. در حملات بیولوژیکی، فاصله زمانی میان انتشار عامل بیماری‌زا و شناسایی رسمی بحران می‌تواند تعیین‌کننده میزان خسارت باشد. سامانه‌های هوشمند قادرند داده‌های متنوعی مانند مراجعات بیمارستانی، نسخه‌های دارویی، علائم ثبت‌شده در مراکز درمانی، نتایج آزمایشگاهی، داده‌های جغرافیایی، گزارش‌های دامپزشکی و محیط‌زیستی، داده‌های شبکه‌های اجتماعی و حتی الگوهای جست‌وجوی اینترنتی را به‌صورت هم‌زمان تحلیل کنند (Adamson, 2025). این داده‌ها اگر به‌تنبه‌ای بررسی شوند ممکن است نشانه روشنی از بحران ارائه ندهند، اما هوش مصنوعی می‌تواند با ترکیب آنها، الگوهای غیرعادی را شناسایی کند؛ برای مثال افزایش ناگهانی یک علامت خاص در چند منطقه، رشد غیرمنتظره مصرف برخی داروها یا هم‌زمانی گزارش‌های انسانی، دامی و محیطی می‌تواند به‌عنوان نشانه‌ای از یک تهدید زیستی تلقی شود. چنین قابلیت‌هایی امکان صدور هشدار سریع را فراهم می‌کند و به مسئولان فرصت می‌دهد پیش از گسترش وسیع بحران، اقدامات کنترلی را آغاز کنند.

کاربرد مهم دیگر هوش مصنوعی، کمک به تشخیص سریع و افتراقی بیماری است. در یک حمله بیولوژیکی، تشخیص عامل بیماری‌زا اهمیت حیاتی دارد، زیرا نوع عامل، مسیر انتقال، شدت بیماری، روش درمان و اقدامات کنترلی را تعیین می‌کند. سامانه‌های هوشمند می‌توانند نتایج آزمایشگاهی را با سرعت بیشتری تحلیل کنند، الگوهای علائم بیماران را با داده‌های پیشین مقایسه نمایند و احتمال ارتباط موارد مختلف بیماری را ارزیابی کنند. افزون بر این، هوش مصنوعی می‌تواند به پزشکان کمک کند تا میان شیوع طبیعی یک بیماری و احتمال وقوع یک اقدام عمدی تمایز قائل شوند. البته این تمایز صرفاً بر پایه داده‌های پزشکی انجام نمی‌شود،

^۱ - Artificial intelligence

بلکه نیازمند تلفیق اطلاعات اپیدمیولوژیک، جغرافیایی، زمانی و گاه امنیتی است (Egan, 2023). بنابراین نقش هوش مصنوعی در این بخش، جایگزینی پزشک یا کارشناس نیست، بلکه تقویت تصمیم‌گیری انسانی از طریق تحلیل سریع‌تر و دقیق‌تر شواهد است. پیش‌بینی مسیر انتشار نیز از دیگر ظرفیت‌های مهم هوش مصنوعی در مقابله با تهدیدات بیولوژیکی است. عوامل زیستی^۱ می‌توانند تحت تأثیر متغیرهایی مانند تراکم جمعیت، الگوهای رفت‌وآمد، شبکه حمل‌ونقل، شرایط اقلیمی، رفتارهای اجتماعی و میزان تماس افراد گسترش پیدا کنند. مدل‌های هوش مصنوعی می‌توانند این داده‌ها را تحلیل کرده و مسیرهای احتمالی انتشار را شبیه‌سازی کنند. نتیجه چنین تحلیلی برای سیاست‌گذاران بسیار ارزشمند است، زیرا به آنها کمک می‌کند قرنطینه را به‌صورت هدفمند اعمال کنند، منابع درمانی را پیش از تشدید بحران به مناطق پرخطر منتقل سازند، محدودیت‌های رفت‌وآمد را دقیق‌تر طراحی کنند و از اقدامات بیش‌ازحد یا ناکافی جلوگیری نمایند. اهمیت این مسئله در آن است که تصمیم‌های نادرست در بحران‌های زیستی می‌تواند هم به گسترش بیماری منجر شود و هم هزینه‌های اجتماعی و اقتصادی سنگینی ایجاد کند (غلامی، ۱۳۹۹). بنابراین هوش مصنوعی می‌تواند به ایجاد تعادل میان کنترل مؤثر بحران و حفظ کارکردهای ضروری جامعه کمک کند.

در حوزه مدیریت منابع درمانی^۲ نیز هوش مصنوعی نقش تعیین‌کننده‌ای دارد. بحران‌های بیولوژیکی معمولاً با فشار شدید بر بیمارستان‌ها، آزمایشگاه‌ها، مراکز درمانی و زنجیره تأمین تجهیزات پزشکی همراه هستند. کمبود تخت بیمارستانی، تخت مراقبت ویژه، تجهیزات حفاظت فردی، دارو، واکسن، دستگاه‌های تنفسی و نیروی انسانی می‌تواند پاسخ نظام سلامت را به‌شدت کاهش دهد. سامانه‌های هوشمند می‌توانند با تحلیل روند بیماری و پیش‌بینی نیازهای آینده، به برنامه‌ریزی دقیق‌تر کمک کنند. برای نمونه، می‌توانند نیاز احتمالی به تخت‌های ICU را در مناطق مختلف برآورد کنند، توزیع دارو و واکسن را بر اساس سطح خطر و نیاز واقعی بهینه سازند، زنجیره تأمین تجهیزات پزشکی را مدیریت کنند و از ائتلاف منابع جلوگیری نمایند (صادقی و اسلامی، ۱۴۰۴). همچنین در شرایطی که منابع محدود است، هوش مصنوعی می‌تواند در اولویت‌بندی بیماران بر پایه معیارهای شفاف، علمی و عادلانه به تصمیم‌گیران کمک کند؛ هرچند چنین کاربردی باید حتماً تحت نظارت انسانی، اصول اخلاق پزشکی و چارچوب‌های قانونی انجام شود.

هوش مصنوعی در توسعه دارو و واکسن نیز ظرفیت چشمگیری دارد. در مواجهه با عوامل بیماری‌زای نوظهور یا دستکاری‌شده، سرعت در شناخت ساختار عامل زیستی و یافتن راهکار درمانی اهمیت بالایی دارد. الگوریتم‌های هوشمند می‌توانند ساختار ژنتیکی یا مولکولی عوامل بیماری‌زا را تحلیل کنند، تعامل آنها با بدن انسان را مدل‌سازی نمایند و ترکیبات دارویی بالقوه مؤثر را پیش‌بینی کنند. همچنین این فناوری می‌تواند روند طراحی واکسن را تسریع کند، گزینه‌های مناسب‌تر را برای آزمایش‌های بعدی پیشنهاد دهد و طراحی آزمایش‌های بالینی را بهینه سازد. مزیت اصلی هوش مصنوعی در این حوزه، کاهش زمان و هزینه پژوهش است؛ زیرا می‌تواند از میان حجم عظیمی از ترکیبات و داده‌ها، گزینه‌های امیدبخش‌تر را برای بررسی انسانی و آزمایشگاهی انتخاب کند. با این حال، استفاده از هوش مصنوعی در تولید دارو و واکسن باید با ارزیابی‌های دقیق ایمنی، اثربخشی و نظارت علمی همراه باشد، زیرا تصمیم‌نهایی در این حوزه نمی‌تواند صرفاً بر خروجی الگوریتم‌ها متکی باشد. (صادقی و همکاران، ۱۴۰۴)

بعد دیگر مقابله با ترور بیولوژیکی، مدیریت فضای اطلاعاتی و مقابله با اطلاعات نادرست است. در بحران‌های زیستی، ترس عمومی، ابهام، کمبود اطلاعات معتبر و سرعت انتشار اخبار می‌تواند زمینه‌ساز گسترش شایعات و روایت‌های نادرست شود. این مسئله ممکن است اعتماد عمومی را تضعیف کند، همکاری مردم با توصیه‌های بهداشتی را کاهش دهد و حتی باعث رفتارهای پرخطر مانند هجوم به مراکز درمانی، مصرف خودسرانه دارو یا بی‌اعتنایی به هشدارهای رسمی شود. سامانه‌های هوش مصنوعی می‌توانند جریان‌های اطلاعاتی را رصد کنند، الگوهای انتشار شایعات را شناسایی نمایند و به نهادهای مسئول کمک کنند تا

^۱ - Biological factors

^۲ - Management of medical resources

پاسخ‌های دقیق، سریع و متناسب ارائه دهند. البته این کاربرد بسیار حساس است و باید با رعایت آزادی بیان، شفافیت، حریم خصوصی و نظارت قانونی همراه باشد (کرامت میرشکارلو، ۱۴۰۳). هدف از مقابله با اطلاعات نادرست نباید کنترل ناموجه افکار عمومی باشد، بلکه باید حفظ سلامت جامعه، افزایش آگاهی عمومی و تقویت اعتماد اجتماعی از طریق اطلاع‌رسانی درست و مسئولانه باشد.

در مجموع، کاربردهای هوش مصنوعی در مقابله با ترور بیولوژیکی از مرحله پیش از بحران تا هنگام پاسخ و پس از آن را دربرمی‌گیرد. این فناوری می‌تواند در پایش و هشدار زودهنگام، تشخیص سریع، پیش‌بینی انتشار، مدیریت منابع، توسعه دارو و واکسن و کنترل پیامدهای اطلاعاتی بحران نقش‌آفرینی کند. با این حال، اثربخشی هوش مصنوعی وابسته به کیفیت داده‌ها، یکپارچگی سامانه‌های سلامت، همکاری میان نهادهای مختلف، رعایت اصول اخلاقی، حفاظت از حریم خصوصی و وجود نظارت انسانی است. بنابراین هوش مصنوعی زمانی می‌تواند به ابزاری مؤثر در برابر تهدیدات بیولوژیکی تبدیل شود که نه به‌صورت منفرد، بلکه در چارچوب یک نظام سلامت تاب‌آور، شفاف، قانون‌مند و هماهنگ به کار گرفته شود.

۴. وضعیت حقوقی در اتحادیه اروپا

اتحادیه اروپا در سال‌های اخیر یکی از پیشرفته‌ترین چارچوب‌های حقوقی جهان را در حوزه حکمرانی داده، سلامت عمومی، امنیت سایبری، زیرساخت‌های حیاتی و هوش مصنوعی ایجاد کرده است. اهمیت این چارچوب زمانی بیشتر می‌شود که موضوعاتی مانند داده‌های سلامت، سامانه‌های هوش مصنوعی پزشکی، پایش بیماری‌های واگیردار، تهدیدات بیولوژیکی، آزمایشگاه‌های زیستی و امنیت بیمارستان‌ها مطرح باشد. در چنین حوزه‌هایی، مسئله صرفاً فنی یا پزشکی نیست، بلکه با حقوق بنیادین اشخاص، امنیت عمومی، حاکمیت داده، اعتماد اجتماعی و مسئولیت دولت‌ها نیز ارتباط مستقیم دارد (Gronvall, 2012). رویکرد اتحادیه اروپا معمولاً بر چند اصل اساسی استوار است: حفاظت از حقوق بنیادین، پیشگیری از خطر، شفافیت، پاسخگویی، نظارت انسانی، امنیت داده‌ها و همکاری فرامرزی. به همین دلیل، مقررات اروپایی تلاش می‌کنند میان نوآوری فناورانه و کنترل مخاطرات تعادل برقرار کنند. این موضوع به‌ویژه در زمینه هوش مصنوعی سلامت و مقابله با تهدیدات بیولوژیکی اهمیت دارد؛ زیرا استفاده از داده‌های عظیم سلامت و ابزارهای تحلیلی پیشرفته می‌تواند به تشخیص سریع بیماری‌ها، پیش‌بینی شیوع‌ها و مدیریت بحران کمک کند، اما در عین حال ممکن است خطراتی مانند نقض حریم خصوصی، تبعیض الگوریتمی، سوءاستفاده امنیتی، نشت داده یا تصمیم‌گیری غیرشفاف را نیز به همراه داشته باشد.

۴-۱- مقررات عمومی حفاظت از داده‌ها^۱

مقررات عمومی حفاظت از داده‌ها مهم‌ترین چارچوب حقوقی اتحادیه اروپا در حوزه حفاظت از داده‌های شخصی به‌شمار می‌رود. این مقررات با هدف تقویت کنترل افراد بر داده‌های خود، افزایش شفافیت در پردازش اطلاعات و ایجاد مسئولیت‌پذیری برای نهادهای دولتی و خصوصی تدوین شده است. در این نظام حقوقی، داده‌های مربوط به سلامت در زمره داده‌های حساس قرار دارند و به همین دلیل، پردازش آن‌ها به‌طور اصولی ممنوع است؛ مگر آنکه یکی از مبانی قانونی مشخص وجود داشته باشد. از جمله مهم‌ترین استثنای پیش‌بینی شده در مقررات عمومی حفاظت از داده‌ها می‌توان به رضایت صریح فرد، ضرورت پردازش برای ارائه خدمات پزشکی و درمانی، حفظ سلامت عمومی، حمایت از منافع حیاتی اشخاص، و نیز استفاده از داده‌ها برای پژوهش‌های علمی با رعایت تضمین‌های مناسب اشاره کرد. این مقررات همچنین اصول بنیادینی مانند قانونی بودن، شفافیت، محدودیت هدف، حداقل‌سازی داده، دقت، محدودیت نگهداری، محرمانگی و پاسخگویی را بر همه پردازشگران داده تحمیل می‌کند. از این رو، مقررات عمومی حفاظت از داده‌ها نه تنها یک مقرر حفاظتی، بلکه ابزاری مهم برای تنظیم مرز میان نوآوری داده‌محور و صیانت از حقوق بنیادین افراد است. (González, 2023)

^۱- General Data Protection Regulation

۴-۲- مقررات هوش مصنوعی اتحادیه اروپا

اتحادیه اروپا با تصویب مقررات هوش مصنوعی، رویکردی مبتنی بر ریسک را در تنظیم این فناوری در پیش گرفته است. بر اساس این رویکرد، سامانه‌های هوش مصنوعی بر حسب میزان خطر برای حقوق، امنیت و سلامت افراد دسته‌بندی می‌شوند. برخی از کاربردهای هوش مصنوعی، به‌ویژه در حوزه سلامت، مدیریت بحران، تصمیم‌گیری‌های حساس و زیرساخت‌های حیاتی، ممکن است در رده سامانه‌های پرخطر قرار گیرند و بنابراین مشمول الزامات سخت‌گیرانه‌تری شوند. در مورد سامانه‌های پرخطر، الزامات متعددی مطرح است؛ از جمله مدیریت ریسک، کیفیت و نمایندگی مناسب داده‌های آموزشی، ثبت و مستندسازی عملکرد سامانه، شفافیت در برابر کاربران، نظارت انسانی مؤثر، دقت و استحکام فنی، امنیت سایبری و ارزیابی انطباق پیش از عرضه به بازار (Egan, 2023). این چارچوب به‌ویژه در حوزه سلامت اهمیت دارد، زیرا تصمیم‌های مبتنی بر هوش مصنوعی می‌توانند مستقیماً بر جان و حقوق بیماران اثر بگذارند. در نتیجه، مقررات هوش مصنوعی اتحادیه اروپا می‌کوشد میان بهره‌برداری از ظرفیت‌های نوآورانه و پیشگیری از آسیب‌های احتمالی تعادل برقرار کند.

۴-۳- مقررات تهدیدات جدی سلامت فرامرزی^۱

اتحادیه اروپا برای مقابله با تهدیدات جدی سلامت فرامرزی، چارچوبی حقوقی و نهادی طراحی کرده است که هدف آن هماهنگی میان کشورهای عضو در مواجهه با بحران‌های بهداشتی است. این مقررات بر همکاری، تبادل سریع اطلاعات، هشدار زودهنگام، ارزیابی مشترک خطر و اتخاذ اقدامات هماهنگ تأکید دارد. در واقع، این نظام حقوقی می‌پذیرد که تهدیدات سلامت، مانند همه‌گیری‌ها یا حملات زیستی، معمولاً از مرزهای ملی فراتر می‌روند و صرفاً با اقدام یک کشور قابل کنترل نیستند. اهمیت این مقررات در حوزه تهدیدات بیولوژیکی بسیار بالاست، زیرا شیوع عوامل بیماری‌زا یا حملات زیستی می‌تواند به سرعت چندین کشور را تحت تأثیر قرار دهد (دریایی، ۱۳۹۴). از این رو، اتحادیه اروپا با ایجاد سازوکارهای هماهنگ، تلاش کرده است ظرفیت واکنش جمعی را افزایش دهد و از پراکندگی تصمیم‌گیری جلوگیری کند. این رویکرد، یک مدل حقوقی برای مدیریت بحران‌های زیستی در سطح فراملی به شمار می‌آید.

۴-۴- مرکز اروپایی پیشگیری و کنترل بیماری‌ها^۲

مرکز اروپایی پیشگیری و کنترل بیماری‌ها یکی از نهادهای کلیدی اتحادیه اروپا در حوزه سلامت عمومی است. مأموریت اصلی این مرکز، پایش بیماری‌های واگیر، تحلیل داده‌های اپیدمیولوژیک، ارزیابی خطر و ارائه توصیه‌های علمی و سیاستی به دولت‌های عضو است. این نهاد نقشی اساسی در تقویت آمادگی اروپا برای مواجهه با تهدیدات بهداشتی ایفا می‌کند. در سال‌های اخیر، استفاده از ابزارهای تحلیلی پیشرفته و سامانه‌های داده‌محور در فعالیت‌های مرکز اروپایی پیشگیری و کنترل بیماری‌ها اهمیت بیشتری یافته است. بهره‌گیری از فناوری‌های نوین، از جمله تحلیل‌های مبتنی بر هوش مصنوعی، می‌تواند به این نهاد در شناسایی الگوهای بیماری، پیش‌بینی روند شیوع و افزایش سرعت واکنش کمک کند (Adamson, 2025). از این منظر، مرکز اروپایی پیشگیری و کنترل بیماری‌ها نمونه‌ای مهم از کاربرد نهادی فناوری در تقویت تاب آوری سلامت عمومی و ارتقای ظرفیت تصمیم‌گیری علمی در سطح اتحادیه اروپا است.

۴-۵- امنیت سایبری^۳ و زیرساخت‌های حیاتی

اتحادیه اروپا در سال‌های اخیر توجه ویژه‌ای به امنیت سایبری و حفاظت از زیرساخت‌های حیاتی نشان داده است. نهادهای اروپایی با تصویب مقررات و دستورالعمل‌های مختلف، تلاش کرده‌اند سطح آمادگی و تاب‌آوری شبکه‌ها و سامانه‌های اطلاعاتی را افزایش دهند. در این چارچوب، بیمارستان‌ها، آزمایشگاه‌ها، مراکز داده سلامت و سامانه‌های پایش بیماری در شمار زیرساخت‌های حیاتی یا

1- Serious cross-border health threats

2- European Centre for Disease Prevention and Control

3- Cybersecurity

مهم قرار می‌گیرند و ملزم به رعایت استانداردهای امنیتی سخت‌گیرانه هستند. اهمیت این موضوع از آن جهت است که اختلال یا حمله سایبری به این زیرساخت‌ها می‌تواند پیامدهای مستقیم و جدی برای سلامت عمومی داشته باشد. برای مثال، از کار افتادن سامانه‌های بیمارستانی، دستکاری داده‌های آزمایشگاهی یا نفوذ به شبکه‌های مراقبت سلامت می‌تواند فرآیند درمان و پاسخ اضطراری را مختل کند (González, 2023). به همین دلیل، اتحادیه اروپا امنیت سایبری را صرفاً یک مسئله فنی نمی‌داند، بلکه آن را بخشی از امنیت عمومی، سلامت جمعی و حکمرانی مسئولانه داده و فناوری تلقی می‌کند.

۵. وضعیت حقوقی در ایران

در ایران، موضوعاتی مانند سلامت عمومی، امنیت زیستی، پدافند غیرعامل، جرائم رایانه‌ای، مسئولیت مدنی، اسرار پزشکی و مدیریت بحران در قوانین و مقررات مختلف مورد توجه قرار گرفته‌اند. با این حال، این مقررات به صورت پراکنده تنظیم شده‌اند و هنوز چارچوبی جامع و منسجم برای مواجهه با پیوند میان هوش مصنوعی، داده‌های سلامت و تهدیدات بیولوژیکی یا بیوتروریستی وجود ندارد. اهمیت این مسئله از آن جهت است که تهدیدات نوین زیستی دیگر صرفاً به عوامل طبیعی یا حملات فیزیکی محدود نیستند. امروزه داده‌های سلامت، سامانه‌های آزمایشگاهی، پایگاه‌های اطلاعات ژنتیکی، تجهیزات پزشکی متصل، الگوریتم‌های پیش‌بینی بیماری و سامانه‌های هوش مصنوعی می‌توانند هم ابزار تقویت سلامت عمومی باشند و هم در صورت سوءاستفاده، منشأ خطرات جدی شوند. بنابراین، نظام حقوقی باید بتواند هم از نوآوری و کارآمدی فناوری حمایت کند و هم از حریم خصوصی، امنیت ملی، سلامت عمومی و حقوق شهروندان حفاظت نماید. در وضعیت فعلی، حقوق ایران دارای ظرفیت‌هایی برای پاسخ به بخشی از این مسائل است، اما این ظرفیت‌ها بیشتر از طریق قواعد عمومی و مقررات پراکنده قابل استفاده‌اند. به همین دلیل، برای مدیریت حقوقی هوش مصنوعی در حوزه سلامت و امنیت زیستی، نیاز به قانون‌گذاری تخصصی، هماهنگی نهادی، استانداردسازی داده‌ها، نظام ارزیابی ریسک و سازوکارهای نظارتی مستقل وجود دارد.

۵-۱- قانون اساسی^۱

قانون اساسی جمهوری اسلامی ایران می‌تواند یکی از مهم‌ترین مبانی حقوقی برای تنظیم‌گری در حوزه سلامت، داده‌های زیستی، هوش مصنوعی و امنیت عمومی باشد. اصول مرتبط با کرامت انسانی، حق برخورداری از تأمین اجتماعی و خدمات بهداشتی و درمانی، حمایت از حقوق مردم و تکلیف دولت به حفظ امنیت عمومی، همگی ظرفیت‌هایی هستند که می‌توانند مبنای مداخله قانون‌گذار و دولت در این حوزه قرار گیرند. از منظر حقوق اساسی، استفاده از فناوری‌هایی مانند هوش مصنوعی در حوزه سلامت باید به گونه‌ای باشد که با کرامت انسانی، عدالت در دسترسی به خدمات درمانی، حفظ حریم خصوصی و حمایت از جان و سلامت افراد سازگار باشد (رنجبر، ۱۳۹۹). بنابراین، هرگونه پردازش داده‌های سلامت یا تصمیم‌گیری خودکار در زمینه پزشکی و بهداشت عمومی باید در چارچوب حقوق بنیادین اشخاص تفسیر شود. قانون اساسی از این جهت می‌تواند نقش‌مبنایی در تدوین قوانین آتی درباره داده‌های سلامت، امنیت زیستی و فناوری‌های نوین داشته باشد.

۵-۲- قوانین سلامت عمومی^۲

قوانین و مقررات مربوط به سلامت عمومی، بهداشت، کنترل بیماری‌های واگیر، وظایف وزارت بهداشت و مدیریت بحران از دیگر ظرفیت‌های مهم حقوق ایران محسوب می‌شوند. این مقررات می‌توانند در شناسایی، پیشگیری، کنترل و پاسخ به تهدیدات زیستی مورد استفاده قرار گیرند (صادقی و همکاران، ۱۴۰۴). برای نمونه، اختیارات وزارت بهداشت در زمینه پایش بیماری‌ها، اعلام وضعیت‌های بهداشتی، مداخله در شرایط اضطراری و هماهنگی با سایر نهادها، می‌تواند پایه‌ای برای مدیریت بحران‌های زیستی باشد. با این حال، این قوانین عمدتاً برای شرایط کلاسیک سلامت عمومی طراحی شده‌اند و معمولاً به‌طور مستقیم به موضوعاتی مانند

^۱- Constitution

^۲- Public health laws

داده‌های بزرگ سلامت، الگوریتم‌های پیش‌بینی شیوع، سامانه‌های هوشمند پایش بیماری و تصمیم‌گیری خودکار نمی‌پردازند. بنابراین، اگرچه قوانین سلامت عمومی ظرفیت اولیه دارند، اما برای پاسخ‌گویی به چالش‌های ناشی از فناوری‌های نوین نیازمند تکمیل، بازنگری و به‌روزرسانی هستند.

۵-۳- پدافند غیرعامل^۱

پدافند غیرعامل یکی از حوزه‌هایی است که می‌تواند در مواجهه با تهدیدات بیولوژیکی و حفاظت از زیرساخت‌های سلامت نقش مهمی ایفا کند. رویکرد پدافند غیرعامل بر کاهش آسیب‌پذیری، افزایش تاب‌آوری، استمرار خدمات حیاتی و پیشگیری از اختلال در زیرساخت‌های مهم تمرکز دارد. از این منظر، بیمارستان‌ها، آزمایشگاه‌های مرجع، سامانه‌های اطلاعات سلامت، بانک‌های زیستی و مراکز تشخیص بیماری می‌توانند در زمره زیرساخت‌های حساس قرار گیرند (جعفری هزارانی، ۱۴۰۴). در حوزه تهدیدات زیستی، پدافند غیرعامل می‌تواند به طراحی سازوکارهای آمادگی، سناریو نویسی بحران، حفاظت از زنجیره تأمین دارو و تجهیزات پزشکی، امنیت آزمایشگاه‌ها و تداوم خدمات درمانی کمک کند. همچنین، با توجه به پیوند روزافزون سلامت با سامانه‌های دیجیتال، پدافند غیرعامل باید امنیت سایبری سامانه‌های سلامت و حفاظت از داده‌های حساس را نیز در بر گیرد. بنابراین، ظرفیت پدافند غیرعامل تنها به دفاع فیزیکی محدود نیست، بلکه می‌تواند مبنایی برای حکمرانی ریسک در حوزه سلامت و زیست‌امنیت باشد.

۵-۴- قانون جرائم رایانه‌ای^۲

قانون جرائم رایانه‌ای یکی دیگر از ظرفیت‌های موجود در حقوق ایران است که می‌تواند در مقابله با حملات سایبری علیه سامانه‌های سلامت مورد استفاده قرار گیرد. سامانه‌های بیمارستانی، پرونده‌های الکترونیک سلامت، پایگاه‌های داده آزمایشگاهی و سامانه‌های پایش بیماری‌ها، همگی ممکن است هدف حملاتی مانند دسترسی غیرمجاز، تخریب داده، اختلال در خدمات، سرقت اطلاعات یا دستکاری داده‌های پزشکی قرار گیرند. در چنین مواردی، قانون جرائم رایانه‌ای می‌تواند مبنای تعقیب کیفری مرتکبان و حمایت از امنیت سامانه‌های سلامت باشد. با این حال، این قانون نیز به‌صورت خاص برای حوزه سلامت و داده‌های حساس پزشکی طراحی نشده است. در نتیجه، لازم است در کنار استفاده از ظرفیت‌های موجود، مقررات تخصصی‌تری برای حفاظت از زیرساخت‌های دیجیتال سلامت و تعیین تکالیف امنیتی نهادهای درمانی و پژوهشی تدوین شود. (صادقی و اسلامی، ۱۴۰۴)

۵-۵- قواعد مسئولیت مدنی و کیفری

قواعد عمومی مسئولیت مدنی و کیفری نیز می‌توانند در مواردی که به اشخاص در نتیجه خطا، تقصیر، بی‌احتیاطی یا سوءاستفاده از فناوری زیان وارد می‌شود، مورد استناد قرار گیرند. برای مثال، اگر استفاده از یک سامانه هوش مصنوعی در تشخیص بیماری منجر به خطای جدی و ورود زیان به بیمار شود، یا اگر افشای داده‌های سلامت موجب آسیب مادی یا معنوی به فرد گردد، امکان طرح مسئولیت بر اساس قواعد عمومی وجود دارد. با این حال، در حوزه هوش مصنوعی و سامانه‌های پیچیده، تعیین مسئولیت دشوارتر می‌شود. زیرا ممکن است زیان ناشی از خطای طراح الگوریتم، نقص داده‌های آموزشی، عملکرد نادرست کاربر، ضعف نظارت انسانی یا ترکیبی از این عوامل باشد (عباس نژادورزی و همکاران، ۱۴۰۳). قواعد سنتی مسئولیت مدنی و کیفری همیشه توان پاسخ‌گویی دقیق به این وضعیت‌ها را ندارند. بنابراین، اگرچه این قواعد ظرفیت حمایتی دارند، اما برای مواجهه با مسئولیت ناشی از فناوری‌های نوین، نیاز به قواعد اختصاصی و شفاف‌تر احساس می‌شود.

۶. تطبیق حقوق ایران و اتحادیه اروپا

مقایسه حقوق ایران و اتحادیه اروپا در زمینه سلامت دیجیتال، داده‌های سلامت، هوش مصنوعی و امنیت زیستی نشان می‌دهد که تفاوت اصلی میان این دو نظام حقوقی در میزان انسجام، تخصصی‌بودن و الزام‌آوری مقررات است. اتحادیه اروپا طی سال‌های اخیر

^۱ - Passive defense

^۲ - Computer Crimes Act

تلاش کرده است با تصویب و اجرای مقررات فراگیر، نظامی هماهنگ و چندلایه برای حمایت از داده‌های شخصی، تنظیم فناوری‌های نوین، مدیریت تهدیدات سلامت و تضمین امنیت سایبری ایجاد کند. در مقابل، حقوق ایران اگرچه در برخی حوزه‌ها دارای قواعد پراکنده و اصول کلی است، اما هنوز از یک چارچوب جامع، منسجم و اختصاصی در زمینه حکمرانی داده‌های سلامت، هوش مصنوعی پزشکی و امنیت سایبری سلامت برخوردار نیست. این تفاوت موجب می‌شود که در اتحادیه اروپا، مواجهه با فناوری‌های نوین سلامت بیشتر مبتنی بر پیش‌بینی، ارزیابی خطر، پاسخگویی و نظارت نهادی باشد، در حالی که در ایران، بسیاری از مسائل همچنان از طریق قواعد عمومی مسئولیت مدنی، مقررات پراکنده اداری، اصول کلی حریم خصوصی یا دستورالعمل‌های بخشی مدیریت می‌شود.

در حوزه حفاظت از داده‌های سلامت، اتحادیه اروپا به واسطه مقررات عمومی حفاظت از داده‌ها یکی از پیشرفته‌ترین نظام‌های حقوقی جهان را ایجاد کرده است. در این نظام، داده‌های مربوط به سلامت از جمله داده‌های حساس محسوب می‌شوند و پردازش آن‌ها اصولاً ممنوع است، مگر در موارد استثنایی و با رعایت شرایط سخت‌گیرانه مانند رضایت صریح فرد، ضرورت درمان، منافع عمومی در حوزه سلامت یا اهداف پژوهشی با تضمین‌های کافی. حفاظت از داده‌ها اصولی مانند شفافیت، محدودیت هدف، حداقل‌گرایی داده، صحت، محدودیت نگهداری، امنیت، پاسخگویی و حق دسترسی، اصلاح، حذف و اعتراض را به رسمیت می‌شناسد. این اصول باعث می‌شوند بیمار یا شهروند در برابر نهادهای درمانی، شرکت‌های فناوری، بیمه‌ها و دولت از حقوق مشخص و قابل مطالبه برخوردار باشد (González, 2023). در ایران، هرچند اصل حریم خصوصی در قانون اساسی، برخی مواد قانون مجازات اسلامی، قانون جرایم رایانه‌ای، قانون تجارت الکترونیکی و مقررات مرتبط با اسرار پزشکی قابل استناد است، اما قانون جامع و مستقلی که به‌طور خاص از داده‌های سلامت و داده‌های پزشکی دیجیتال حمایت کند وجود ندارد (فتحی زاده، ۱۴۰۴). همین امر سبب می‌شود مرزهای مجاز پردازش، اشتراک‌گذاری، ذخیره‌سازی، انتقال و استفاده ثانویه از داده‌های سلامت، به‌ویژه در بیمارستان‌های هوشمند، سامانه‌های نسخه‌نویسی الکترونیک، پرونده الکترونیک سلامت و پژوهش‌های مبتنی بر کلان‌داده، به روشنی مشخص نباشد.

در زمینه تنظیم هوش مصنوعی نیز اتحادیه اروپا رویکردی ریسک‌محور و الزام‌آور^۱ اتخاذ کرده است. بر اساس این رویکرد، همه کاربردهای هوش مصنوعی یکسان تلقی نمی‌شوند، بلکه بر حسب میزان خطری که برای سلامت، ایمنی، کرامت انسانی، حقوق بنیادین و منافع عمومی ایجاد می‌کنند، در سطوح مختلف قرار می‌گیرند. کاربردهای هوش مصنوعی در حوزه پزشکی، تشخیص بیماری، تصمیم‌گیری درمانی، تجهیزات پزشکی هوشمند و مدیریت خدمات سلامت غالباً در دسته سامانه‌های پرخطر قرار می‌گیرند و بنابراین مشمول الزامات جدی مانند ارزیابی ریسک، کیفیت داده‌ها، مستندسازی، شفافیت، نظارت انسانی، امنیت، دقت، قابلیت ردیابی و پاسخگویی می‌شوند. اهمیت این رویکرد در آن است که پیش از بروز زیان، سازوکارهای پیشگیرانه و نظارتی فعال می‌شوند (صادقی و همکاران، ۱۴۰۴). در ایران، هنوز قانون خاص و جامعی درباره هوش مصنوعی وجود ندارد و کاربردهای آن در سلامت عمدتاً از طریق قواعد عمومی، مقررات پزشکی، مسئولیت مدنی، نظامات صنفی و سیاست‌های کلی فناوری اطلاعات قابل تحلیل است. این وضعیت، در برابر کاربردهای پیچیده‌ای مانند الگوریتم‌های تشخیص سرطان، سامانه‌های اولویت‌بندی بیماران، ابزارهای پیش‌بینی اپیدمی، ربات‌های جراحی یا سامانه‌های تصمیم‌یار بالینی، خلأهای مهمی ایجاد می‌کند؛ زیرا روشن نیست در صورت خطای الگوریتم، تبعیض داده‌ای، تصمیم غیرشفاف یا آسیب ناشی از توصیه هوش مصنوعی، مسئولیت دقیقاً متوجه پزشک، بیمارستان، طراح نرم‌افزار، تولیدکننده داده، ارائه‌دهنده زیرساخت یا نهاد ناظر خواهد بود.

از حیث مدیریت تهدیدات سلامت فرامرزی، اتحادیه اروپا تجربه قابل توجهی در ایجاد سازوکارهای هماهنگ منطقه‌ای دارد. بحران‌هایی مانند همه‌گیری کووید - ۱۹ نشان دادند که تهدیدات سلامت محدود به مرزهای ملی نیستند و مقابله مؤثر با آن‌ها نیازمند

^۱- A risk-based and mandatory approach

تبادل سریع داده، هماهنگی میان دولت‌ها، نظام هشدار سریع، خرید مشترک تجهیزات و واکسن، استانداردهای مشترک نظارتی و همکاری نهادهای علمی و اجرایی است. اتحادیه اروپا از طریق نهادهایی مانند مرکز اروپایی پیشگیری و کنترل بیماری‌ها و سازوکارهای مشترک مدیریت بحران، تلاش کرده است واکنش دولت‌های عضو را هماهنگ کند (Adamson, 2025). در ایران، مدیریت تهدیدات سلامت بیشتر ماهیتی ملی و بخشی دارد و عمدتاً توسط وزارت بهداشت، درمان و آموزش پزشکی و دیگر نهادهای داخلی انجام می‌شود. هرچند ایران در سطح بین‌المللی می‌تواند با سازمان جهانی بهداشت و سایر سازوکارهای منطقه‌ای همکاری کند، اما از نظر حقوق داخلی، نظامی جامع و شفاف برای حکمرانی داده‌های سلامت در شرایط بحران، تبادل داده میان دستگاه‌ها، محدودیت‌های حقوق فردی، نظارت قضایی یا پارلمانی و تضمین‌های مربوط به عدم سوءاستفاده از داده‌های اضطراری به اندازه نظام اتحادیه اروپا توسعه نیافته است.

در حوزه امنیت سایبری سلامت نیز تفاوت مهمی میان دو نظام دیده می‌شود. اتحادیه اروپا با توجه به حساسیت زیرساخت‌های سلامت، بیمارستان‌ها، سامانه‌های پرونده الکترونیک، تجهیزات پزشکی متصل و پایگاه‌های داده بیماران، مقررات نسبتاً توسعه‌یافته‌ای برای امنیت شبکه و اطلاعات ایجاد کرده است. در این نظام، ارائه‌دهندگان خدمات حیاتی و نهادهای فعال در حوزه سلامت موظف‌اند تدابیر فنی و سازمانی مناسب برای پیشگیری از حملات سایبری، نشت داده، باج‌افزارها، اختلال در خدمات درمانی و سوءاستفاده از اطلاعات بیماران اتخاذ کنند. امنیت سایبری در اینجا صرفاً یک موضوع فنی نیست، بلکه بخشی از حقوق بیمار، ایمنی سلامت عمومی و اعتماد عمومی به نظام درمان محسوب می‌شود. در ایران نیز مقرراتی درباره جرایم رایانه‌ای، امنیت فضای تبادل اطلاعات، پدافند غیرعامل، حفاظت از سامانه‌های حیاتی و الزامات کلی امنیت اطلاعات وجود دارد، اما مقررات اختصاصی و تفصیلی برای امنیت سایبری در بخش سلامت هنوز نیازمند تقویت است. با توجه به گسترش نسخه الکترونیک، سامانه‌های بیمه‌ای، تله‌مدیسن و بیمارستان‌های هوشمند، نبود استانداردهای الزام‌آور و تخصصی می‌تواند خطر افشای اطلاعات پزشکی، اختلال در درمان و کاهش اعتماد عمومی را افزایش دهد. (اسکندری صدیقی، ۱۳۹۸)

مسئولیت الگوریتمی^۱ یکی از مهم‌ترین محورهای مقایسه است. در اتحادیه اروپا، هرچند این حوزه همچنان در حال توسعه است، اما مسیر کلی به سمت شفاف‌تر شدن مسئولیت‌ها، قابلیت توضیح تصمیمات، مستندسازی عملکرد سامانه‌ها و تعیین نقش بازیگران مختلف حرکت می‌کند. وقتی یک سامانه هوش مصنوعی در تشخیص یا درمان نقش دارد، پرسش‌هایی مانند کیفیت داده‌های آموزشی، میزان خطای قابل قبول، امکان نظارت انسانی، اطلاع بیمار از استفاده از الگوریتم، قابلیت اعتراض به تصمیم و مسئولیت تولیدکننده یا استفاده‌کننده اهمیت پیدا می‌کند. حقوق اتحادیه اروپا تلاش می‌کند این پرسش‌ها را از طریق ترکیب قواعد حفاظت از داده، مقررات هوش مصنوعی، ایمنی محصول، مسئولیت مدنی و حقوق مصرف‌کننده پاسخ دهد (Egan, 2023). در ایران، مسئولیت ناشی از تصمیمات الگوریتمی عمدتاً باید بر پایه قواعد عمومی مسئولیت مدنی، تقصیر، رابطه سببیت، ضمان قهری، مسئولیت پزشکی یا مسئولیت مراکز درمانی تحلیل شود. این قواعد برای بسیاری از موارد سنتی کارآمدند، اما در مواجهه با سامانه‌های یادگیرنده، تصمیمات غیرقابل توضیح، دخالت چندین بازیگر و خطاهای ناشی از داده‌های آموزشی ناکافی، ممکن است پاسخ کافی و دقیق ارائه نکنند.

در زمینه شفافیت و نظارت نیز اتحادیه اروپا ساختار روشن‌تری دارد. در این نظام، نهادهای ناظر حفاظت از داده، مراجع ارزیابی انطباق، سازوکارهای گزارش‌دهی، ارزیابی اثرات بر حریم خصوصی و الزامات پاسخگویی نقش مهمی در کنترل قدرت دولت و شرکت‌های فناوری ایفا می‌کنند. اصل مهم این است که پردازش داده‌های سلامت یا استفاده از هوش مصنوعی نباید در فضایی مبهم و غیرقابل نظارت انجام شود. شهروند باید بداند چه داده‌ای از او جمع‌آوری می‌شود، برای چه هدفی استفاده می‌شود، چه کسی به آن دسترسی دارد، چه مدت نگهداری می‌شود و در صورت نقض حقوقش به کجا می‌تواند شکایت کند. در ایران، نیاز به نهادسازی

^۱- Algorithmic responsibility

جدی‌تر احساس می‌شود؛ به‌ویژه نهادی مستقل و تخصصی برای حفاظت از داده‌های شخصی و سلامت، نظارت بر سامانه‌های هوش مصنوعی پزشکی، رسیدگی به شکایات، تدوین استانداردها و اعمال ضمانت اجرا. بدون چنین نهادی، حتی اگر مقررات پراکنده وجود داشته باشد، اجرای مؤثر و اعتماد عمومی با چالش روبه‌رو خواهد شد. (مولائی فرد و مسعودی فر، ۱۴۰۴)

از منظر تعادل میان امنیت و حقوق فردی^۱، اتحادیه اروپا تلاش کرده است میان ضرورت‌های سلامت عمومی، امنیت سایبری و مدیریت بحران از یک سو و حقوق بنیادینی مانند حریم خصوصی، کرامت انسانی، آزادی، منع تبعیض و حق بر دادرسی مؤثر از سوی دیگر توازن برقرار کند. این توازن معمولاً بر پایه اصول ضرورت، تناسب، محدودیت زمانی، هدف مشخص، نظارت مستقل و امکان اعتراض تعریف می‌شود. برای مثال، اگر در شرایط همه‌گیری نیاز به جمع‌آوری یا تحلیل داده‌های شهروندان وجود داشته باشد، این اقدام باید ضروری، متناسب، محدود به هدف سلامت عمومی، همراه با تضمین‌های امنیتی و تحت نظارت انجام شود (González, 2023). در ایران نیز می‌توان چنین اصولی را از مبانی قانون اساسی، حقوق شهروندی، قواعد شرعی و اصول عمومی حقوق عمومی استنباط کرد، اما مشکل اصلی در تصریح، نظام‌مند کردن و تضمین اجرای آن‌هاست. به بیان دیگر، حقوق ایران ظرفیت نظری لازم برای حمایت از حریم خصوصی، کرامت انسانی و امنیت سلامت را دارد، اما برای تبدیل این ظرفیت به نظامی مؤثر، نیازمند قانون‌گذاری صریح، ضمانت اجرا، نهاد ناظر مستقل و استانداردهای عملیاتی است.

در مجموع، اتحادیه اروپا در مقایسه با ایران از نظامی منسجم‌تر، تخصصی‌تر و آینده‌نگرتر برخوردار است؛ نظامی که در آن حفاظت از داده، تنظیم هوش مصنوعی، امنیت سایبری و مدیریت بحران سلامت به صورت مرتبط و مکمل دیده می‌شوند. نقطه قوت رویکرد اروپایی در این است که فناوری را نه صرفاً به عنوان ابزار توسعه، بلکه به عنوان پدیده‌ای پرخطر و اثرگذار بر حقوق بنیادین انسان تنظیم می‌کند. در مقابل، حقوق ایران هنوز بیشتر در مرحله اتکا به قواعد عمومی و مقررات پراکنده قرار دارد. این وضعیت به معنای فقدان کامل حمایت حقوقی نیست، اما نشان‌دهنده نیاز جدی به تدوین قانون جامع حفاظت از داده‌های شخصی و سلامت، قانون یا چارچوب ملی تنظیم هوش مصنوعی، مقررات اختصاصی امنیت سایبری سلامت، نظام روشن مسئولیت الگوریتمی و ایجاد نهادهای تخصصی نظارتی است. اگر حقوق ایران بخواهد همگام با تحولات سلامت دیجیتال حرکت کند، باید از الگوی واکنشی و بخشی فاصله بگیرد و به سمت حکمرانی پیشگیرانه، شفاف، ریسک‌محور و حقوق‌بنیاد حرکت کند؛ الگویی که هم نوآوری و توسعه فناوری را ممکن سازد و هم از حقوق بیماران، اعتماد عمومی و امنیت سلامت جامعه صیانت کند.

۷. نتیجه‌گیری

برآیند مباحث نشان می‌دهد که مواجهه مؤثر با ترور بیولوژیکی در عصر فناوری، وابسته به توان نظام سلامت در پیوند دادن سه عنصر اساسی آمادگی نهادی، ظرفیت فناورانه و تضمین‌های حقوقی است. تهدیدات زیستی نوین به دلیل ماهیت پنهان، سرعت انتشار، دشواری انتساب و آثار گسترده بر سلامت، اقتصاد، امنیت و اعتماد عمومی، نظام‌های سلامت را ناگزیر می‌سازند از الگوهای واکنشی و سنتی فاصله بگیرند و به سمت حکمرانی پیش‌نگر، داده‌محور و هماهنگ حرکت کنند. در چنین الگویی، هوش مصنوعی می‌تواند با افزایش سرعت تشخیص، ارتقای دقت پیش‌بینی، بهینه‌سازی تخصیص منابع، پشتیبانی از تصمیم‌گیری و تقویت نظام هشدار سریع، ظرفیت تاب‌آوری سلامت را به‌طور چشمگیری افزایش دهد. با این حال، ارزش راهبردی این فناوری زمانی محقق می‌شود که در یک ساختار حقوقی و نهادی قابل اعتماد به کار گرفته شود؛ زیرا همان ابزاری که می‌تواند به شناسایی سریع تهدید و نجات جان انسان‌ها کمک کند، در صورت فقدان ضابطه، ممکن است به نقض حریم خصوصی، تبعیض، تمرکز قدرت، سوءاستفاده امنیتی، خطای غیرقابل توضیح و کاهش اعتماد عمومی منجر شود.

^۱- Individual rights

از منظر تطبیقی، تجربه اتحادیه اروپا نشان می‌دهد که بهره‌گیری مسئولانه از هوش مصنوعی در حوزه سلامت و امنیت زیستی، نیازمند مجموعه‌ای به هم پیوسته از قواعد است؛ قواعدی که هم از داده‌های حساس سلامت حمایت کند، هم سامانه‌های هوش مصنوعی را بر اساس میزان خطر تنظیم نماید، هم امنیت سایبری زیرساخت‌های درمانی و آزمایشگاهی را تضمین کند و هم سازوکارهای هماهنگ برای مدیریت بحران‌های سلامت فرامرزی فراهم سازد. در این نظام، تنظیم‌گری فناوری صرفاً پس از وقوع زیان فعال نمی‌شود، بلکه از مرحله طراحی، آموزش داده، ارزیابی ریسک، استقرار سامانه، نظارت انسانی و پاسخگویی حقوقی حضور دارد. همین ویژگی موجب می‌شود که نوآوری فناورانه در کنار اصولی مانند شفافیت، تناسب، پاسخگویی، امنیت، منع تبعیض و صیانت از حقوق بنیادین پیش برود. بنابراین، نقطه قوت رویکرد اروپایی نه فقط در وجود مقررات متعدد، بلکه در پیوند ساختاری میان سلامت عمومی، حفاظت از داده، امنیت سایبری و حقوق بشر است. در مقابل، حقوق ایران اگرچه از ظرفیت‌های مهمی در قانون اساسی، مقررات سلامت عمومی، پدافند غیرعامل، قانون جرایم رایانه‌ای و قواعد مسئولیت مدنی و کیفری برخوردار است، اما این ظرفیت‌ها هنوز به یک نظام منسجم و تخصصی برای حکمرانی هوش مصنوعی در حوزه سلامت و مقابله با تهدیدات زیستی تبدیل نشده‌اند. پراکندگی مقررات، نبود قانون جامع حفاظت از داده‌های سلامت، فقدان قواعد خاص درباره سامانه‌های هوش مصنوعی پزشکی، ابهام در مسئولیت ناشی از تصمیمات الگوریتمی، ضعف استانداردهای الزام‌آور امنیت سایبری سلامت و نبود نهاد مستقل ناظر، از مهم‌ترین چالش‌هایی است که می‌تواند کارآمدی و مشروعیت استفاده از هوش مصنوعی را در شرایط بحران زیستی تضعیف کند. این وضعیت به‌ویژه در شرایط اضطراری خطرناک‌تر می‌شود؛ زیرا بحران‌های زیستی معمولاً زمینه مداخله گسترده دولت، جمع‌آوری وسیع داده، محدودسازی برخی آزادی‌ها و تصمیم‌گیری سریع را فراهم می‌کنند و اگر این اقدامات با معیارهای روشن ضرورت، تناسب، محدودیت زمانی و نظارت مستقل همراه نباشد، احتمال آسیب به حقوق شهروندان افزایش می‌یابد.

بنابراین، نتیجه اساسی آن است که هوش مصنوعی به‌تنهایی نه تضمین‌کننده امنیت زیستی است و نه جایگزین حکمرانی کارآمد سلامت؛ بلکه ابزاری قدرتمند است که اثر آن به کیفیت داده‌ها، آمادگی نهادی، اعتماد اجتماعی، امنیت زیرساخت‌ها و چارچوب حقوقی وابسته است. برای استفاده مؤثر از این فناوری در برابر ترور بیولوژیکی، لازم است نظام حقوقی ایران از رویکرد پراکنده و پسینی فاصله گرفته و به سمت تنظیم‌گری جامع، ریسک‌محور و حقوق‌بنیاد حرکت کند. تدوین قانون جامع حفاظت از داده‌های شخصی و سلامت، ایجاد چارچوب ملی برای هوش مصنوعی با تأکید بر کاربردهای پرخطر پزشکی و امنیت زیستی، تعیین قواعد روشن مسئولیت الگوریتمی، الزام مراکز درمانی و آزمایشگاهی به رعایت استانداردهای امنیت سایبری، پیش‌بینی سازوکارهای ارزیابی اثرات حقوقی و اخلاقی، و ایجاد نهاد تخصصی و مستقل برای نظارت بر داده و هوش مصنوعی سلامت، از ضرورت‌های اصلی این مسیر است. در نهایت، مقابله با بیوتروریسم در جهان معاصر بیش از آنکه صرفاً مسئله‌ای پزشکی یا امنیتی باشد، مسئله‌ای مربوط به حکمرانی هوشمند، اعتماد عمومی و موازنه میان امنیت و آزادی است. نظام سلامت تاب‌آور نظامی است که بتواند پیش از بحران هشدار دهد، هنگام بحران سریع و هماهنگ عمل کند، پس از بحران بازسازی شود و در تمام این مراحل کرامت، حریم خصوصی و حقوق بنیادین شهروندان را حفظ نماید. از این رو، آینده موفق مقابله با تهدیدات بیولوژیکی در گرو آن است که فناوری‌های هوشمند نه در خلأ حقوقی و نه تحت منطق صرفاً امنیتی، بلکه در چارچوبی شفاف، پاسخگو، انسانی و قانونمند به کار گرفته شوند. چنین رویکردی می‌تواند هم توان کشور را در برابر حملات زیستی افزایش دهد و هم مانع آن شود که ابزارهای مقابله با بحران، خود به منشأ بحران‌های حقوقی، اجتماعی و اخلاقی تازه تبدیل شوند.

پیشنهادهای

با توجه به نتایج به‌دست آمده، پیشنهاد می‌شود نظام حقوقی ایران در گام نخست به سمت تدوین قانون جامع حفاظت از داده‌های شخصی، به‌ویژه داده‌های سلامت، حرکت کند. داده‌های پزشکی، ژنتیکی، آزمایشگاهی، اپیدمیولوژیک و اطلاعات مربوط به سوابق درمانی باید به‌عنوان داده‌های حساس شناسایی شوند و پردازش، ذخیره‌سازی، تبادل، انتقال و استفاده ثانویه از آن‌ها تنها بر اساس

مبانی قانونی روشن و با رعایت اصولی مانند رضایت آگاهانه، حداقل سازی داده، محدودیت هدف، امنیت، محرمانگی، شفافیت و پاسخگویی مجاز باشد. همچنین لازم است حقوق مشخصی برای شهروندان در برابر نهادهای درمانی، پژوهشی، بیمه‌ای و فناوریانه پیش‌بینی شود؛ از جمله حق دسترسی به داده، حق اصلاح، حق اعتراض به پردازش، حق اطلاع از موارد نقض امنیتی و حق شکایت نزد نهاد ناظر مستقل.

در کنار آن، تدوین چارچوب ملی تنظیم‌گری هوش مصنوعی در حوزه سلامت و امنیت زیستی ضروری است. این چارچوب باید مبتنی بر رویکرد ریسک‌محور باشد و کاربردهایی مانند تشخیص بیماری، پیش‌بینی شیوع، اولویت‌بندی بیماران، مدیریت منابع درمانی، تحلیل داده‌های اپیدمیولوژیک و سامانه‌های هشدار سریع زیستی را در زمره کاربردهای پرخطر قرار دهد. برای این سامانه‌ها باید الزاماتی مانند ارزیابی ریسک پیش از بهره‌برداری، کیفیت و اعتبارسنجی داده‌های آموزشی، مستندسازی عملکرد، قابلیت توضیح‌پذیری، نظارت انسانی، امکان اعتراض به تصمیمات الگوریتمی، امنیت سایبری، پایش مستمر و مسئولیت‌پذیری ارائه‌دهندگان و استفاده‌کنندگان پیش‌بینی شود. هدف از چنین تنظیم‌گری‌ای نباید محدود کردن نوآوری باشد، بلکه باید ایجاد اعتماد، کاهش خطر و هدایت فناوری در مسیر حمایت از سلامت عمومی و حقوق شهروندان باشد.

پیشنهاد دیگر، ایجاد نهاد مستقل و تخصصی برای نظارت بر داده‌های سلامت و کاربردهای هوش مصنوعی پزشکی است. این نهاد می‌تواند وظایفی مانند تدوین استانداردهای فنی و اخلاقی، صدور مجوز برای سامانه‌های پرخطر، ارزیابی اثرات حقوقی و اجتماعی فناوری‌ها، رسیدگی به شکایات شهروندان، نظارت بر مراکز درمانی و شرکت‌های فناوری، الزام به گزارش‌دهی رخدادهای امنیتی و انتشار گزارش‌های عمومی درباره وضعیت حکمرانی داده و هوش مصنوعی در سلامت را بر عهده داشته باشد. استقلال، تخصص‌گرایی و پاسخگویی چنین نهادی اهمیت زیادی دارد؛ زیرا بدون نظارت مؤثر، حتی بهترین قوانین نیز ممکن است در عمل به حمایت کافی از حقوق شهروندان و امنیت سلامت منجر نشوند.

همچنین لازم است امنیت سایبری زیرساخت‌های سلامت به‌صورت خاص و الزام‌آور تقویت شود. بیمارستان‌ها، آزمایشگاه‌ها، مراکز داده سلامت، سامانه‌های نسخه‌نویسی الکترونیک، پرونده الکترونیک سلامت، تجهیزات پزشکی متصل و بانک‌های زیستی باید به‌عنوان زیرساخت‌های حیاتی یا حساس شناسایی شوند و ملزم به رعایت استانداردهای امنیتی مشخص باشند. اقداماتی مانند رمزنگاری داده‌ها، کنترل دسترسی، ثبت و پایش رویدادها، آزمون نفوذ دوره‌ای، پشتیبان‌گیری امن، برنامه تداوم خدمت، آموزش کارکنان، مدیریت رخدادهای سایبری و گزارش فوری نشت داده باید به‌صورت قانونی الزام‌آور شود. در غیر این صورت، حمله سایبری یا دستکاری داده‌های سلامت می‌تواند در زمان بحران زیستی، توان پاسخ نظام سلامت را مختل کرده و اعتماد عمومی را به‌شدت کاهش دهد.

در حوزه مسئولیت حقوقی نیز پیشنهاد می‌شود قواعد ویژه‌ای برای مسئولیت ناشی از سامانه‌های هوش مصنوعی در سلامت تدوین شود. در این قواعد باید نقش و مسئولیت طراح الگوریتم، تولیدکننده نرم‌افزار، تأمین‌کننده داده، مرکز درمانی، پزشک، اپراتور سامانه و نهاد ناظر به‌روشنی تعیین گردد. همچنین باید مشخص شود در مواردی مانند خطای تشخیص، تبعیض الگوریتمی، نقص داده‌های آموزشی، تصمیم غیرقابل توضیح، افشای داده‌های سلامت یا آسیب ناشی از توصیه نادرست سامانه، زیان‌دیده چگونه می‌تواند جبران خسارت دریافت کند. پیش‌بینی بیمه مسئولیت حرفه‌ای برای ارائه‌دهندگان سامانه‌های هوش مصنوعی پزشکی و الزام به مستندسازی تصمیمات الگوریتمی می‌تواند در این زمینه نقش مهمی داشته باشد.

منابع

۱. اسکندری صدیقی، رضا. (۱۳۹۸). بیوتروریسم. چاپ اول، تهران: انتشارات پشتیبان.
۲. بیافرین، علی. (۱۳۹۹). تئوری ترور. چاپ اول، تهران: نشر معارف.
۳. جعفری هزارانی، نورالدین. (۱۴۰۳). تحلیل عملیات ترور اسماعیل هنیه در تهران: باگ های امنیتی و درس های اطلاعاتی. مقالات پیش چاپ سیولیکا، ۱-۳۰.
۴. دریایی، محمدرسول. (۱۳۹۴). بیوتروریسم در طب غربی. چاپ اول، تهران: موسسه فرهنگی آرمان رشد.
۵. رنجبر، قاسم. (۱۳۹۹). تحلیل سیاسی بیوتروریسم و بررسی نیاز به تدوین سند بین المللی. چاپ اول، تهران: دیادخت.
۶. صادقی، سالار. صمدی راد، بهرام. اسلامی، طاهّا. (۱۴۰۴). مطالعه تطبیقی سازوکارهای مقابله با بیوتروریسم علیه کودکان (با نگاهی تطبیقی بر کنوانسیون های بین المللی و کشورهای آمریکا، کانادا، استرالیا و آلمان). مجله تحقیق و توسعه در حقوق تطبیقی، شماره ۲۸، ۳۴۲-۳۷۷.
۷. صادقی، سالار. اسلامی، طاهّا. (۱۴۰۴). نقش میکروبیولوژی قانونی در کشف علمی جرایم (با نگاهی تطبیقی به رویکرد کشورهای آمریکا، انگلستان، آلمان و ایران). مجله کارآگاه، شماره ۷۱، ۸۵-۱۰۳.
۸. عباس نژادورزی، رمضان. رهی، مجید. عباس نژادورزی، سعید. (۱۴۰۳). هوش مصنوعی در امنیت سایبری: مفاهیم، کاربرد ها، چالش ها، الگوریتم ها و ابزارها. چاپ اول، تهران: انتشارات فناوری نوین.
۹. غلامی، بهادر. (۱۳۹۹). تأثیرات تهدیدات بیولوژیکی بر بودجه ریزی دفاعی و امنیتی: مطالعه موردی کووید-۱۹. مجله راهبرد، شماره ۹۷، ۶۸-۹۶.
۱۰. فتحی زاده، نورمحمد. (۱۴۰۴). پیشگیری از ترور با هوش مصنوعی. چاپ اول، تهران: هورین.
۱۱. کرامت میرشکارلو، یاسین. (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، ۱۱-۱.
۱۲. کاکویی، عیسی. (۱۴۰۰). ترور شخصیت. چاپ اول، تهران: به اندیش.
۱۳. مولائی فرد، محسن. مسعودی فر، هادی. (۱۴۰۴). تأثیر بیماری های فراگیر بر گسترش تروریسم. مجله تمدن حقوقی، شماره ۲۳، ۳۷-۶۴.

14. Adamson, Georgia. (2025). *Opportunities to Strengthen U.S. Biosecurity from AI-Enabled Bioterrorism: What Policymakers Should Know*. Washington, DC: Center for Strategic and International Studies.
15. Egan, Janet. (2023). *Biosecurity in the Age of AI: What's the Risk?*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School.
16. González, Gómez. (2023). *Artificial intelligence for healthcare and well-being during exceptional times: A recent landscape from a European perspective*. Luxembourg: Publications Office of the European Union.

17. Gronvall, Gigi Kwik. (2012). *Preparing for Bioterrorism: The Alfred P. Sloan Foundation's Leadership in Biosecurity*. Baltimore, MD: Center for Biosecurity of UPMC.

The Role of Artificial Intelligence in Strengthening the Resilience of the Health System against Bioterrorism Threats

Hossein Esmaili¹

Date of Receipt: 2018/00/00 Date of Issue: 2018/00/00

Abstract

Bioterrorism, as one of the complex and transboundary contemporary threats, can seriously affect national security and public health by causing disease, death, public fear, and disruption of social order. In such circumstances, the resilience of the health system, as the ability to prevent, prepare for, identify, respond to, and recover from biological crises, gains particular importance. The main question of this study is how artificial intelligence can play a role in strengthening the resilience of the health system against bioterrorism threats, and what capacities and challenges the legal systems of Iran and the European Union have in legally regulating this role. The present study, with an analytical-comparative approach, examines the role of artificial intelligence in strengthening the resilience of the health system against bioterrorism, as well as the legal capacities and challenges of Iran and the European Union in regulating this role. The findings of the study indicate that artificial intelligence can significantly enhance the response capacity of the health system through intelligent data monitoring, early warning, rapid diagnosis, prediction of disease transmission pathways, management of medical resources, acceleration of drug and vaccine development, and combating misinformation. However, the effective use of this technology requires clear, accountable legal frameworks based on human oversight in order to prevent risks such as violation of privacy, algorithmic discrimination, ambiguous liability, and security-related misuse. The comparative analysis shows that the European Union, relying on regulations such as data protection, artificial intelligence regulations, and cybersecurity and cross-border crisis management mechanisms, enjoys a more coherent legal system; whereas Iranian law, although possessing capacities in the Constitution, public health laws, passive defense, and computer crimes legislation, still faces fragmentation of regulations, the absence of a comprehensive law on health data protection, and the lack of a dedicated framework for artificial intelligence. The conclusion is that achieving the lawful and effective use of artificial intelligence in combating bioterrorism requires moving toward rights-based, risk-oriented, and forward-looking governance in the field of health.

Keywords

Bioterrorism, Artificial Intelligence, Health System Resilience, Health Law, Data Protection, European Union, Iran

¹ - Master of Science in Criminal Law and Criminology, Islamic Azad University, Takestan Branch, Qazvin, Iran.