فصلنامه علمی راهبرد سیاسی
انتشارات دانشگاه راهبردی

تحول تهدیدهای بیوتروریستی در عصر هوش مصنوعی مولد با تأکید بر الزامات راهبردی امنیت زیستی و چالش‌های مسئولیت کیفری

محدثه قوامی پور سرشکه[1] امیررضا محمودی[2] قاسم قاسمی بیورزنی[3] جمال بیگی[4]

دوره ۱۰، شماره ۲، پیاپی ۳۷
تابستان ۱۴۰۵

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۵/۰۴/۲۰
تاریخ پذیرش:
۱۴۰۵/۰۶/۲۰
صص: ۴۲۲-۳۹۱

شاپا چاپی: ۴۵۶۵-۲۵۸۸
الکترونیکی: ۰۳۸۱-۲۷۱۷

چکیده

همگرایی هوش مصنوعی مولد و زیست‌فناوری، ماهیت تهدیدهای بیوتروریستی و شیوه‌های مقابله با آن‌ها را دگرگون کرده است. این پژوهش با روش توصیفی – تحلیلی و با استفاده از منابع کتابخانه‌ای، اسناد بین‌المللی و مقررات کیفری، کارکرد دوگانه هوش مصنوعی مولد را در حوزه امنیت زیستی بررسی می‌کند. یافته‌ها نشان می‌دهد مدل‌های زبانی بزرگ، ابزارهای طراحی زیستی و سامانه‌های عامل‌محور از یک‌سو می‌توانند در دیده‌بانی ژنومیک، پایش محیطی، غربالگری توالی‌های زیستی، حفاظت از داده‌های ژنتیکی و تقویت سازوکارهای عدم اشاعه به کار گرفته شوند و از سوی دیگر، دسترسی به دانش تخصصی، شناسایی آسیب‌پذیری‌ها، طراحی محاسباتی و حملات سایبری – زیستی را تسهیل کنند. این سامانه‌ها جایگزین دانش تخصصی و زیرساخت آزمایشگاهی نمی شوند، اما می‌توانند موانع اطلاعاتی و فنی ارتکاب را کاهش دهند. مقابله با این مخاطرات مستلزم پایش هوشمند، حفاظت از زیرساخت‌ها و داده‌های زیستی، نظارت انسانی و همکاری بین‌المللی است. در حقوق کیفری نیز مسئولیت باید بر مبنای نقش، میزان کنترل، سطح آگاهی، قابلیت پیش‌بینی خطر و نقض تکالیف مراقبتی توزیع شود. در حقوق ایران، حملات زیستی گسترده، در صورت احراز عناصر قانونی و معنوی، با افساد فی‌الارض انطباق روشن‌تری نسبت به محاربه دارند.

کلیدواژه‌ها: هوش مصنوعی مولد، بیوتروریسم، امنیت زیستی، تهدیدهای نوپدید، راهبردهای پیشگیری، مسئولیت کیفری.

۱. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران mohadeseh.ghavamipour@iau.ac.ir
۲. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران (نویسنده مسئول) dr.mahmoudi@iau.ac.ir
۳. گروه معارف اسلامی، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران g.ghasemi4146@iau.ac.ir
۴. گروه جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران jamal_beigi@iau.ac.ir

مقدمه

پیشرفت زیست‌فناوری محاسباتی و گسترش سامانه‌های مولد، مرز میان پردازش داده‌های زیستی و فعالیت‌های آزمایشگاهی را دگرگون کرده است. تحلیل داده‌های ژنومیک، پیش‌بینی ساختار پروتئین‌ها، تولید توالی‌های جدید و سازمان‌دهی دانش تخصصی، فرصت‌هایی مهم برای شناخت بیماری‌ها، طراحی دارو و پایش همه‌گیری‌ها فراهم می‌کند. در مقابل، همین ظرفیت‌ها ممکن است برای شناسایی آسیب‌پذیری‌های زیستی، تسهیل دسترسی به اطلاعات تخصصی و تضعیف سازوکارهای غربالگری مورد سوءاستفاده قرار گیرند. ازاین‌رو، این فناوری‌ها در حوزه امنیت زیستی ماهیتی دوگانه دارند.

بیوتروریسم در مفهوم سنتی به استفاده عمدی از عوامل بیماری‌زا یا سموم زیستی برای ایجاد بیماری، مرگ، هراس عمومی یا اخلال اجتماعی اشاره دارد. با گسترش داده‌های توالی دیجیتال، آزمایشگاه‌های ابری و ابزارهای زیست‌محاسباتی، برخی مراحل شناسایی، تحلیل و بازطراحی عوامل زیستی می‌توانند پیش از ورود به محیط آزمایشگاه، در بسترهای دیجیتال انجام شوند. در نتیجه، ارزیابی تهدیدهای زیستی دیگر نباید تنها بر دسترسی فیزیکی به عوامل بیماری‌زا متمرکز باشد، بلکه نحوه دسترسی به داده‌ها، مدل‌های محاسباتی و زیرساخت‌های پردازشی را نیز باید دربر گیرد.

مدل‌های زبانی بزرگ می‌توانند منابع علمی پراکنده را گردآوری و سازمان‌دهی کنند؛ ابزارهای طراحی زیستی ظرفیت تحلیل توالی‌های ژنتیکی را افزایش می‌دهند؛ و سامانه‌های عامل‌محور بخش‌هایی از برنامه‌ریزی و اجرای وظایف را خودکار می‌سازند. البته این قابلیت‌ها به‌تنهایی برای ساخت یا انتشار موفق یک عامل زیستی کافی نیستند و تحقق حمله همچنان به دانش عملی، مواد، تجهیزات و مهارت آزمایشگاهی وابسته است. بااین‌حال، کاهش موانع اطلاعاتی و نزدیک‌شدن طراحی محاسباتی به اجرای آزمایشگاهی می‌تواند سطح خطر را افزایش دهد.

این فناوری‌ها در حوزه دفاع نیز کاربرد دارند. تحلیل داده‌های ژنومیک و اپیدمیولوژیک، پایش محیط، ارزیابی سفارش‌های سنتز DNA و پردازش گزارش‌های مرتبط با تعهدات بین‌المللی می‌تواند به شناسایی زودهنگام تهدیدها کمک کند. در عین حال، خطاهای الگوریتمی، غیرشفاف‌بودن تصمیم‌ها و پردازش گسترده داده‌های ژنتیکی ممکن است حریم خصوصی، آزادی پژوهش و حق اعتراض به تصمیم‌های خودکار را با مخاطره روبه‌رو سازد.

پیوند میان فناوری‌های مولد و بیوتروریسم، حقوق کیفری را نیز با مسئله انتساب مسئولیت مواجه کرده است. نظام‌های کیفری بر رفتار ارادی انسان و احراز علم، قصد یا تقصیر استوارند، درحالی‌که سامانه‌های خودکار ممکن است در تحلیل و تصمیم‌گیری نقش مؤثری داشته باشند، بدون آنکه دارای اراده یا اهلیت جنایی مستقل باشند. بنابراین، مسئله اصلی اعطای شخصیت کیفری به سامانه نیست، بلکه تعیین شرایط انتساب نتیجه به توسعه‌دهنده، ارائه‌دهنده، مدیر، اپراتور، کاربر نهایی یا شخص حقوقی است.

پراکندگی دانش و کنترل میان این بازیگران ممکن است به شکاف پاسخ‌گویی منجر شود. در مقابل، توسعه بی‌ضابطه مسئولیت کیفری نیز می‌تواند اشخاص فاقد علم، قصد، تقصیر یا نقش مؤثر را در معرض مجازات قرار دهد. در حقوق ایران، این مسئله باید بر اساس قانون مجازات اسلامی، قواعد مباشرت و تسبیب، مسئولیت اشخاص حقوقی و مقررات جرایم رایانه‌ای بررسی شود. در حملات گسترده نیز امکان انطباق رفتار با افساد فی‌الارض موضوع ماده ۲۸۶ مطرح است؛ مشروط بر آنکه تمام عناصر قانونی و معنوی جرم اثبات شود.

پرسش اصلی پژوهش آن است که کارکرد دوگانه فناوری‌های مولد در بیوتروریسم چه تأثیری بر معیارهای انتساب مسئولیت کیفری دارد. فرضیه پژوهش این است که مسئولیت کیفری مستقل برای خود سامانه با مبانی حقوق کیفری سازگار نیست و مسئولیت باید بر اساس نقش، آگاهی، میزان کنترل، قابلیت پیش‌بینی خطر و نقض تکالیف مراقبتی میان اشخاص دخیل توزیع شود.

این پژوهش با روش توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای، اسناد بین‌المللی و مقررات کیفری، ابتدا ظرفیت‌ها و مخاطرات این فناوری‌ها را بررسی کرده و سپس چالش‌های حریم خصوصی و انتساب مسئولیت کیفری را در حقوق بین‌المللی و حقوق ایران تحلیل می‌کند.

۱-تعریف بیوتروریسم در عصر دیجیتال و گذار به الگوهای داده‌محور

بیوتروریسم به استفاده عمدی از عوامل زیستی بیماری‌زا، از جمله میکروارگانیسم‌ها و سموم بیولوژیک، با هدف ایجاد بیماری، مرگ، اختلال اجتماعی یا گسترش ناامنی اطلاق می‌شود. در این نوع رفتار، عامل زیستی به‌عنوان وسیله ارتکاب عمل تروریستی به کار گرفته می‌شود و به همین اعتبار، در زمره سلاح‌های بیولوژیک قرار می‌گیرد. گسترش تهدیدهای تروریستی نیز ضرورت توجه جدی

به امکان استفاده از عوامل میکروبی برای ایجاد رعب و واردکردن خسارت گسترده را افزایش داده است (زارع بیدکی و بلالی مود، ۱۳۹٤، ۱۸۲).

اهمیت این پدیده تنها به آثار جسمانی عوامل زیستی محدود نیست. حملات بیوتروریستی می‌توانند حق بر حیات، سلامت و امنیت اشخاص را مستقیماً تهدید کنند و در مقیاس گسترده‌تر، سلامت عمومی و امنیت ملی و بین‌المللی را با مخاطره مواجه سازند. ازاین‌رو، بیوتروریسم را باید یکی از تهدیدهای مهم علیه جوامع انسانی دانست (جلالی و اقلر، ۱٤۰۳، ۲۰۵۷).

پیشرفت علوم زیستی و امکان سوءاستفاده از نتایج پژوهش‌های علمی، ظرفیت بهره‌گیری مجرمانه از برخی عوامل میکروبی را افزایش داده است. هزینه نسبتاً پایین، امکان تهیه برخی مواد و تجهیزات، قابلیت انتشار، دشواری تشخیص اولیه و توان ایجاد هراس عمومی، از جمله عواملی هستند که می‌توانند استفاده از عوامل زیستی را برای برخی گروه‌های تروریستی جذاب سازند. در چنین وضعیتی، امنیت ملی و سلامت عمومی به‌طور هم‌زمان در معرض تهدید قرار می‌گیرند (زرقانی و همکاران، ۱۳۹۷، ۱۳).

تحولات اخیر در زیست‌فناوری محاسباتی، ابعاد این تهدید را گسترده‌تر کرده است. بیوتروریسم دیگر صرفاً به دسترسی فیزیکی به عامل بیماری‌زا یا فعالیت در محیط آزمایشگاهی وابسته نیست، بلکه داده‌های زیستی، مدل‌های محاسباتی و زیرساخت‌های دیجیتال نیز می‌توانند در فرایند طراحی، تحلیل یا بازطراحی عوامل زیستی نقش داشته باشند.(de Lima et al., 2024, p. 2)

در این چارچوب، اطلاعات توالی دیجیتال[1] می‌تواند نیاز به دسترسی مستقیم به برخی نمونه‌های فیزیکی را کاهش دهد و بخشی از فرایند شناسایی، مدل‌سازی یا بازطراحی عوامل زیستی را به محیط‌های محاسباتی منتقل کند. به همین دلیل، تهدیدهای زیستی آینده صرفاً ماهیتی آزمایشگاهی نخواهند داشت، بلکه از پیوند دو حوزه زیستی و محاسباتی شکل خواهند گرفت (Annett et al., 2025, 1). این تحول، شناسایی منشأ تهدید، کنترل دسترسی و پیشگیری از سوءاستفاده را دشوارتر

۱ اطلاعات توالی دیجیتال (Digital Sequence Information یا DSI) به فایل‌ها و داده‌های رایانه‌ای مربوط به ساختار ژنتیکی موجودات زنده گفته می شود؛ برای مثال، اطلاعات مربوط به ترتیب DNA یا RNA یک ویروس، باکتری، گیاه یا حیوان. پژوهشگران می‌توانند این اطلاعات را بدون انتقال نمونه فیزیکی، در رایانه ذخیره کنند، برای دیگران بفرستند و مورد بررسی یا مقایسه قرار دهند

می‌کند و بر پیچیدگی بیوتروریســـم معاصـــر می‌افزاید (هلالی و همکاران، ۱٤۰٤، ص. ۱۵۵). بر این اساس، تعریف بیوتروریسم در عصر دیجیتال نباید به انتشار فیزیکی عوامل بیماری‌زا محدود بماند. این تعریف باید رفتارهای مقدماتی و تسهیل‌کننده‌ای مانند دسترسی غیرمجاز به داده‌های زیستی، پردازش و بازطراحی اطلاعات ژنتیکی و استفاده مجرمانه از زیرساخت‌های محاسباتی را نیز در بر گیرد.

۲-فناوری‌های مولد در زیست‌فناوری؛ ظرفیت‌ها، مخاطرات و پیامدهای حقوقی

سامانه‌های مولد به گروهی از فناوری‌های نوین گفته می‌شود که با تکیه بر مدل‌های زبانی بزرگ و داده‌های آموزشـی گسـترده، قادر به تولید محتوایی مانند متن، تصـویر و کد هسـتند. توانایی پردازش حجم گسـترده‌ای از اطلاعات و تولید پاسـخ‌های منسـجم موجب شـده اسـت که این سـامانه‌ها در حوزه‌های علمی، آموزشـــی، مدیریتی و تجاری به کار گرفته شـــوند. با وجود این، تولید اطلاعات نادرســـت، بازتولید ســـوگیری‌های موجود در داده‌های آموزشـــی، نقض حریم خصـــوصـــی و امکان سوءاستفاده از جمله مخاطراتی است که ضرورت نظارت انسانی و تدوین ضوابط اخلاقی و حقوقی را آ شکار می سازد (سازگار نژاد و همکاران، ۱٤۰۳، ص. ۱). کاربرد این فناوری‌ها در علوم زی ستی، بخشی از پژوهش‌های زیست‌فناورانه را از فعالیتی صرفاً آزمایشگاهی به فرایندی داده‌محور تبدیل کرده ا ست. در این الگو، داده‌های ژنومی در محیط‌های محا سباتی پردازش می شوند، ساختارهای زی ستی پیش‌بینی می‌گردند و توالی های جدید پیش از ورود به مرحله آزمایشـــگاهی مورد بررســـی قرار می‌گیرند مهم‌ترین ابزارهای مورد استفاده در این حوزه را می‌توان در سه گروه مدل‌های زبانی بزرگ، ابزارهای طراحی زیستی و سامانه‌های عامل‌محور بررسی کرد.(Annett et al., 2025, 1)

مدل‌های زبانی بزرگ می‌توانند حجم گســـترده‌ای از منابع علمی پراکنده را پردازش، خلاصـــه و سازمان‌دهی کنند و مطالب پیچیده زیست‌شناسی را در قالبی منسجم‌تر در اختیار کاربر قرار دهند. این قابلیت، فاصله اطلاعاتی میان متخصصان و کاربران کم‌تجربه را کاهش می‌دهد و دسترسی به اطلاعات مربوط به عوامل بیماری‌زا، پژوهش‌های ویروس‌شناسی و فرایندهای آزمایشگاهی را آسان‌تر می‌سازد .(Radcliffe, 2025, p. 765) در صـورت فقدان محدودیت‌های ایمنی، همین توانایی ممکن اسـت اطلاعات تخصصی پراکنده را به توضیحاتی ساختاریافته و قابل‌استفاده تبدیل کند و زمینه سوءاستفاده از آن‌ها را فراهم سازد .(Adamson & Allen, 2025, p. 14) مخاطره اصلی مدل‌های زبانی الزاماً در

تولید دانش علمی کاملاً جدید نیســت، بلکه در گردآوری و تبدیل دانش پراکنده به اطلاعاتی ســریع، منسجم و متناسب با نیاز کاربر نهفته است. با وجود این، دسترسی به اطلاعات نظری به‌تنهایی برای اجرای یک حمله زیستی کافی نیست؛ زیرا تحقق چنین اقدامی همچنان به مواد، تجهیزات، مهارت‌های آزمایشگاهی و زیرساخت فیزیکی نیاز دارد.

در کنار مدل‌های زبانی، ابزارهای طراحی زیستی یا ها برای تحلیل، پیش‌بینی و تولید ساختارها و توالی‌های زیستی توسعه یافته‌اند. سامانه‌هایی مانند Evo 2 بر مجموعه گسترده‌ای از داده‌های ژنومی، شــامل بیش از ۱۲۸ هزار ژنوم، آموزش دیده‌اند و می‌توانند توالی‌هایی پیشــنهاد کنند که برخی از آن‌ها نمونه کاملاً مشابهی در طبیعت ندارند (Adamson & Allen, 2025, p. 26). این ابزارها در طراحی دارو، مهندسی پروتئین، شناخت بیماری‌ها و توسعه روش‌های درمانی کاربرد دارند؛ اما ممکن است برای بررسی ساختارهای زیستی خطرناک نیز مورد سوءاستفاده قرار گیرند. البته تولید یک توالی جدید به‌تنهایی به معنای ایجاد عامل ســمی، بیماری‌زا یا قابل‌اســتفاده در شــرایط واقعی نیســت و بروز چنین ویژگی‌هایی به عوامل متعدد زیستی و آزمایشگاهی وابسته است. یکی از مخاطرات مطرح‌شده در این زمینه، روش موسوم به «طراحی با نویز» است. در این روش، ممکن است توالی‌هایی ایجاد شوند که برخی ویژگی‌های عملکردی خود را حفظ می‌کنند، اما شــباهت ظاهری کمتری به توالی‌های خطرناک شناخته‌شده دارند. چنین وضعیتی می‌تواند شناسایی آن‌ها را برای سامانه‌های غربالگری مبتنی بر تطبیق توالی دشوارتر سازد (Annett et al., 2025, 2). ازاین‌رو، غربالگری مؤثر نباید تنها بر شباهت ظاهری توالی‌ها متکی باشد و لازم است ساختار، عملکرد و سطح خطر احتمالی آن‌ها نیز بررسی شود.

ســامانه‌های عامل‌محور یا گروه دیگری از ابزارهای نوین‌اند که می‌توانند مجموعه‌ای از وظایف را برنامه‌ریزی، اجرا و بر اساس نتایج اصلاح کنند. اتصال این سامانه‌ها به آزمایشگاه‌های ابری، تجهیزات روباتیک و ابزارهای خودکار، امکان مدیریت بخشــی از فعالیت‌های آزمایشــگاهی از راه دور را فراهم می‌کند. البته میزان استقلال آن‌ها به سطح دسترسی به تجهیزات، داده‌ها، مجوزهای نرم‌افزاری و نظارت انسانی وابسته است و مدل‌های عمومی، بدون اتصال به زیرساخت‌های خارجی، توان اداره مستقل آزمایشگاه را ندارند.

1 Agentic AI

در همین زمینه، از «عامل‌های خفته» به‌عنوان یکی از سناریوهای امنیتی یاد شده است. این اصطلاح به مدل‌هایی اشاره دارد که در مرحله آموزش و ارزیابی، رفتاری سازگار با ضوابط ایمنی نشان می‌دهند، اما در شرایط یا در برابر محرک‌های خاص، رفتارهای پنهان و زیان‌بار بروز می‌دهند خطر چنین سامانه‌هایی در صورت اتصال به تجهیزات زیستی خودکار افزایش می‌یابد؛ هرچند اجرای مستقل فرایندهای منتهی به تولید عوامل زیستی خطرناک، در شرایط کنونی بیشتر یک سناریوی آینده‌نگرانه است تا قابلیتی تثبیت‌شده.

همچنین گزارش شده است که برخی ابزارهای پیشرفته می‌توانند ضعف‌های احتمالی پروتکل‌های غربالگری مراکز سنتز DNA را شناسایی کنند یا راهبردهایی برای مواجهه با این محدودیت‌ها پیشنهاد دهند (Adamson & Allen, 2025, p. 3; Radcliffe, 2025, p767). بااین‌حال، تولید یک پیشنهاد محاسباتی نباید معادل عبور موفق از تدابیر امنیتی تلقی شود؛ زیرا نتیجه عملی به کیفیت سامانه غربالگری، میزان دسترسی کاربر به اطلاعات فنی و امکان اجرای پیشنهادها بستگی دارد. مجموع این قابلیت‌ها نشان می‌دهد که فناوری‌های مولد در امنیت زیستی ماهیتی دوگانه دارند. یک سامانه ممکن است برای تحلیل داده‌های ژنومیک، تشخیص تغییرات مشکوک، پایش بیماری‌ها و شناسایی زودهنگام تهدیدهای زیستی به کار رود و در عین حال، برای شناخت ضعف سازوکارهای دفاعی یا تسهیل دسترسی به اطلاعات حساس مورد سوءاستفاده قرار گیرد (Annett et al., 2025,2). بنابراین، آثار این فناوری‌ها به نوع ابزار، هدف کاربر، سطح دسترسی و وجود یا فقدان سازوکارهای نظارتی وابسته است.

این دوگانگی از منظر حقوق کیفری نیز اهمیت دارد. در صورت استفاده مجرمانه از یک سامانه، ممکن است توسعه‌دهنده، شرکت ارائه‌دهنده، مالک زیرساخت، مدیر آزمایشگاه و کاربر نهایی در مراحل متفاوتی از فرایند دخالت داشته باشند. افزون بر این، غیرشفاف‌بودن عملکرد برخی الگوریتم‌ها می‌تواند اثبات علم، قصد و میزان کنترل هریک از اشخاص را دشوار سازد (Coco, 2026, p. 232). ازاین‌رو، مسئله اصلی تنها شناسایی قابلیت فنی ابزار نیست، بلکه باید مشخص شود مسئولیت ناشی از طراحی، ارائه و استفاده از آن بر چه مبنایی میان بازیگران مختلف توزیع می‌شود.

1 Sleeper Agents

۳-هوش مصنوعی به‌مثابه ابزار دفاع و پیشگیری: ظرفیت‌ها و فرصت‌ها

هوش مصنوعی مولد، با وجود مخاطرات امنیتی نا شی از کاربرد دوگانه، ظرفیت‌های قابل‌توجهی برای تقویت تاب‌آوری زیستی، حفاظت از داده‌های ژنومیک و نو سازی سازوکارهای نظارت و عدم اشاعه فراهم می‌آورد. اهمیت این فناوری در آن است که می‌تواند الگوی مقابله با تهدیدهای زیستی را از واکنش‌های عمدتاً پسینی، به سمت شناسایی زودهنگام، ارزیابی مستمر خطر و «پیش‌بینی پیش‌دستانه» سوق دهد

بااین‌حال، بهره‌گیری دفاعی از هوش مصنوعی نباید به معنای اعتماد کامل به تصمیم‌های خودکار تلقی شود. اعتبار داده‌های ورودی، احتمال خطاهای مثبت و منفی کاذب، سوگیری الگوریتمی، نبود شفافیت و امکان نقض حریم خصوصی، ضرورت نظارت انسانی و ایجاد سازوکارهای حقوقی پاسخ‌گویی را آشکار می‌سازد. در این چارچوب، مهم‌ترین ظرفیت‌های دفاعی هوش مصنوعی در چهار حوزه دیده‌بانی ژنومیک، نظارت بر تعهدات بین‌المللی، امنیت سایبری زیستی و غربالگری هوشمند قابل بررسی است.

۳-۱-دیده‌بانی ژنومیک و پایش هوشمند محیطی

استفاده از مدل‌های یادگیری عمیق، ظرفیت‌های جدیدی در پایش ژنومیک و زیست‌محیطی ایجاد کرده است. این سامانه‌ها می‌توانند با تحلیل حجم گسترده‌ای از توالی‌های ژنتیکی، الگوهای غیرمعمول یا ناسازگار با برخی روندهای شناخته‌شده تکامل طبیعی را شناسایی کنند. بی‌نظمی در الگوی استفاده از کدون ها، وجود توالی های پروموتر غیرمتعارف و معماری های ژنتیکی نامعمول، از جمله شاخص‌هایی هستند که ممکن است احتمال مهندسی‌شدن یک ارگانیسم را مطرح سازند البته شناسایی این شاخص‌ها به‌تنهایی برای اثبات منشأ مصنوعی یک عامل زیستی کفایت نمی‌کند؛ زیرا برخی تغییرات مشابه ممکن است در نتیجه فرایندهای طبیعی، خطاهای توالی‌یابی یا تفاوت‌های پایگاه‌های داده نیز ایجاد شوند. ازاین‌رو، خروجی سامانه هوشمند باید به‌عنوان «نشانه خطر» و مبنایی برای بررسی های تکمیلی آزمایشگاهی و اپیدمیولوژیک تلقی شود، نه دلیل قطعی بر وقوع حمله بیوتروریستی. پایش هوشمند فاضلاب نیز که در جریان همه‌گیری کووید-۱۹ مورد توجه گسترده قرار گرفت، با ادغام الگوریتم‌های هوش مصنوعی می‌تواند به ابزاری داده‌محور برای شناسایی زودهنگام افزایش غیرعادی عوامل بیماری‌زا در سطح جامعه تبدیل شود. مزیت این روش آن است که بدون اتکا

به شناسایی و آزمایش تک‌تک بیماران، تصویری جمعی از وضعیت انتشار عوامل زیستی ارائه می‌کند و می‌تواند در تشخیص کانون‌های اولیه بیماری یا الگوهای غیرمتعارف شیوع مؤثر باشد (Annett et al., 2025,2; Angeles, 2026, 1)

۳-۲-هوش مصنوعی در خدمت کنوانسیون سلاح‌های بیولوژیک

کنوانسیون منع توسعه، تولید و ذخیره‌سازی سلاح‌های باکتریولوژیک (بیولوژیک) و سمی و انهدام آن‌ها، مصوب ۱۹۷۲، مهم‌ترین سند بین‌المللی در زمینه ممنوعیت جنگ‌افزارهای زیستی به شمار می‌رود (پورسعید و همکاران،۱٤۰۳: ص.٤۰۵). به موجب ماده ۲ این کنوانسیون، دولت‌های عضو موظف‌اند عوامل بیولوژیک، سموم، تجهیزات و وسایل مرتبط موجود در قلمرو یا تحت صلاحیت و کنترل خود را نابود کنند یا به مقاصد صلح‌آمیز اختصاص دهند. ماده ۳ نیز انتقال مستقیم یا غیرمستقیم این عوامل و تجهیزات و همچنین کمک، تشویق یا ترغیب دولت‌ها، سازمان‌ها و اشخاص برای تولید یا دستیابی به آن‌ها را ممنوع کرده است. با وجود این تعهدات، فقدان نظام جامع و الزام‌آور بازرسی و راستی‌آزمایی، از مهم‌ترین کاستی‌های کنوانسیون است و پیگیری موارد احتمالی عدم پایبندی دولت‌ها را دشوار می‌سازد (Thiermann et al., 2020, p.474).

کنوانسیون منع سلاح‌های بیولوژیک و سمی، برخلاف برخی رژیم‌های منع اشاعه، از سازوکار جامع و الزام‌آور بازرسی میدانی برخوردار نیست. در چنین شرایطی، هوش مصنوعی می‌تواند از طریق «تحلیل برون‌مکانی» ظرفیت تحلیل اطلاعات و شناسایی نشانه‌های خطر را تقویت کند

ابزارهای پردازش زبان طبیعی می‌توانند گزارش‌های اقدامات اعتماد ساز را استخراج، طبقه‌بندی و استانداردسازی کنند و تفاوت‌ها، خلأها یا ناسازگاری‌های احتمالی میان گزارش‌های ارائه‌شده در دوره‌های مختلف را نشان دهند(Angeles, 2026; p.2) این فناوری می‌تواند بار پردازش انسانی را کاهش دهد و موارد نیازمند بررسی بیشتر را اولویت‌بندی کند؛ اما تشخیص الگوریتمی یک ناسازگاری، لزوماً به معنای نقض تعهدات کنوانسیونی نیست و باید در پرتو زمینه علمی، اقتصادی و امنیتی هر کشور ارزیابی شود.

تحلیل پیش‌بینانه همچنین می‌تواند با ترکیب داده‌های مربوط به تجارت کالاهای حساس، بودجه‌های پژوهشی، انتشار مقالات، ثبت اختراعات و توسعه زیرساخت‌های زیستی، الگوهای غیرعادی در فعالیت‌های دارای کاربرد دوگانه را شناسایی کند افزون بر این، تحلیل تصاویر ماهواره‌ای،

داده‌های زنجیره تأمین و حسابرسی‌های دیجیتال ممکن است در شناسایی توسعه غیرمتعارف تأسیسات یا انحراف تجهیزات حساس از مقاصد اعلام‌شده مفید واقع شود (Annett et al., 2026;p.3)

باوجوداین، کاربرد هوش مصنوعی در نظارت بین‌المللی با محدودیت‌های حقوقی و سیاسی مهمی مواجه است. ابهام در منشأ و کیفیت داده‌ها، محرمانگی اطلاعات تجاری و پژوهشی، احتمال سوءتفسیر فعالیت‌های مشروع و نابرابری دولت‌ها در دسترسی به فناوری‌های تحلیلی، ممکن است مشروعیت و قابلیت استناد به نتایج را تضعیف کند. ازاین‌رو، هوش مصنوعی باید ابزار پشتیبان تصمیم‌گیری و اعتمادسازی باشد، نه جایگزین ارزیابی کارشناسی، گفت‌وگوی دیپلماتیک یا سازوکارهای راستی‌آزمایی مورد توافق دولت‌ها.

۳-۳- امنیت سایبری زیستی و حفاظت از حریم خصوصی داده‌های ژنتیکی

با دیجیتالی شدن تحقیقات زیستی، داده‌های ژنتیکی و زیرساخت‌های بیوانفورماتیک به بخشی از دارایی‌های حیاتی علمی و امنیتی تبدیل شده‌اند. دسترسی غیرمجاز، تخریب یا دستکاری این داده‌ها می‌تواند افزون بر نقض حریم خصوصی اشخاص، بر اعتبار نتایج پژوهشی، ایمنی فرایندهای آزمایشگاهی و امنیت زیستی اثر بگذارد. هوش مصنوعی می‌تواند با تحلیل مستمر رفتار کاربران و جریان داده‌ها، الگوهای غیرعادی را شناسایی کرده و نقاط آسیب‌پذیر در خط لوله‌های بیوانفورماتیک را آشکار سازد (Daniel, 2023, p3)

این سامانه‌ها ممکن است در تشخیص دسترسی‌های نامتعارف، تغییرات غیرمجاز در پایگاه‌های ژنومی یا انحراف در فرایندهای پردازش داده مؤثر باشند. بااین‌حال، خود ابزارهای هوش مصنوعی نیز می‌توانند به سطح جدیدی از آسیب‌پذیری تبدیل شوند؛ برای نمونه، دستکاری داده‌های آموزشی، حملات خصمانه به مدل یا اعطای دسترسی بیش از حد به سامانه‌های خودکار ممکن است کارکرد دفاعی آن‌ها را مختل کند. بنابراین، امنیت سایبری زیستی مستلزم حفاظت هم‌زمان از داده، مدل، نرم‌افزار و تجهیزات متصل است.

برای تقویت حریم خصوصی، استفاده از رمزنگاری هم‌ریخت[1] پیشنهاد شده است. این فناوری امکان انجام برخی محاسبات بر داده‌های رمزگذاری‌شده را بدون افشای محتوای خام آن‌ها فراهم

1 Homomorphic Encryption

می‌کند و از این طریق می‌تواند احتمال مشاهده مستقیم توالی‌های ژنتیکی توسط پردازشگران یا ارائه‌دهندگان خدمات را کاهش دهد (Tek Leaders, 2026)

بااین‌حال، رمزنگاری هم‌ریخت به‌تنهایی تمام مخاطرات حفاظت از داده را برطرف نمی‌کند و باید در کنار کنترل دسترسی، ثبت رویدادها، تفکیک وظایف، ناشناس‌سازی یا مستعارسازی داده‌ها و ارزیابی اثرات مربوط به حریم خصوصی به کار رود. همچنین، استانداردهای داده‌ای آماده برای پردازش هوش مصنوعی می‌توانند کیفیت، قابلیت ردیابی و سازگاری داده‌ها را افزایش دهند اما ا ستاندارد سازی نباید به تمرکز بی ضابطه داده‌های ژنتیکی یا ت سهیل د ستر سی‌های ثانویه و خارج از هدف اولیه منجر شود.

از منظر حقوقی، داده‌های ژنتیکی به دلیل قابلیت افشای اطلاعات مربوط به هویت، سلامت، خویشاوندان و استعدادهای زیستی اشخاص، واجد حساسیتی فراتر از بسیاری از داده‌های شخصی متعارف‌اند. ازاین‌رو، بهره‌برداری دفاعی از این داده‌ها باید بر پایه مجوز قانونی روشن، هدف مشخص، دسترسی محدود و نظارت مستقل صورت گیرد.

۳-٤- غربالگری هوشمند و همکاری بین‌المللی در مواجهه با مدل‌های متن‌باز

بخ شی از پروتکل‌های متعارف غربالگری در مراکز سنتز DNA بر تطبیق سفارش‌ها با فهر ست توالی‌ها یا عوامل زیستی خطرناک شناخته شده ا ستوار ا ست. چنین رویکردی ممکن ا ست در برابر توالی‌های جدید، تغییریافته یا طراحی‌شده به کمک هوش مصنوعی، کارایی محدودی داشته باشد؛ زیرا یک توالی می‌تواند از نظر ظاهری با موارد موجود در فهرست‌های خطر تفاوت داشته باشد، اما همچنان واجد عملکرد زیستی زیان‌بار باشد (Adamson & Allen, 2025, p. 4)

راهکار مکمل، حرکت از غربالگری صرفاً مبتنی بر فهر ست سیاه به سمت «ارزیابی عملکردی» است. در این روش، مدل‌های یادگیری ماشین علاوه بر شباهت توالی، ساختار احتمالی، نقش عملکردی، میزان بیماری‌زایی یا سمیت بالقوه و زمینه سفارش را نیز ارزیابی می‌کنند (Adamson & Allen, 2025, p. 28)این رویکرد می‌تواند احتمال شناسایی توالی‌های جدید را افزایش دهد، اما همچنان با خطر خطا، ابهام علمی و طبقه‌بندی نادرست پژوهش‌های مشروع مواجه است.

ازاین‌رو، تصمیم به رد سفارش، گزارش کاربر یا ارجاع موضوع به مراجع امنیتی نباید صرفاً بر خروجی یک مدل غیر شفاف مبتنی با شد. وجود امکان بازبینی ان سانی، معیارهای از پیش اعلام شده،

ثبت دلایل تصمیم و سازوکار اعتراض یا ارزیابی مجدد، برای جلوگیری از مداخله نامتناسب در آزادی پژوهش و فعالیت‌های مشروع زیست‌فناورانه ضروری است.

گسترش مدل‌های متن‌باز نیز مسئله را پیچیده‌تر می‌کند. انتشار آزاد مدل‌ها می‌تواند پژوهش، شفافیت و نوآوری را تقویت کند؛ اما ممکن است اعمال کنترل‌های ایمنی و محدودیت‌های دسترسی را دشوارتر سازد. پاسخ مؤثر به این وضعیت، صرفاً در ممنوعیت یا محدودسازی عمومی مدل‌های متن‌باز خلاصه نمی‌شود، بلکه مستلزم ارزیابی سطح خطر، کنترل دسترسی به قابلیت‌های حساس، تدوین استانداردهای مشترک و همکاری فرامرزی است در این زمینه، همکاری میان دولت‌های دارای ظرفیت بالای هوش مصنوعی و زیست‌فناوری ، برای تدوین هنجارهای مشترک و توسعه ظرفیت‌های اطلاعات زیستی» اهمیت دارد. این همکاری می‌تواند شامل تبادل شاخص‌های خطر، هماهنگ‌سازی معیارهای غربالگری و پایش فعالیت‌های مشکوک در فضای سایبری و بازارهای غیرقانونی آنلاین باشد (Goldsmith, 2026)

بااین‌حال، پایش فضای سایبری و دارک‌وب باید با تضمین‌های حقوقی مربوط به صلاحیت، حریم خصوصی، آزادی بیان و اعتبار ادله دیجیتال همراه باشد. توسعه همکاری اطلاعاتی بدون تعیین حدود روشن جمع‌آوری، اشتراک‌گذاری و نگهداری داده‌ها ممکن است خود به گسترش نظارت فراگیر و نقض حقوق اشخاص منجر شوددر مجموع، هوش مصنوعی می‌تواند در مراحل شناسایی، پیش‌بینی، حفاظت از داده، غربالگری و همکاری بین‌المللی، ظرفیت دفاعی دولت‌ها را در برابر بیوتروریسم افزایش دهد. بااین‌حال، کارآمدی این ابزارها به کیفیت داده، امکان توضیح تصمیم‌ها، نظارت انسانی و وجود چارچوب حقوقی شفاف وابسته است. بنابراین، دفاع هوشمند در برابر بیوتروریسم باید بر الگویی استوار شود که در آن امنیت زیستی و حقوق بنیادین، به‌ویژه حریم خصوصی و آزادی پژوهش، نه اهداف متعارض، بلکه اجزای مکمل یک نظام پیشگیری مشروع و پاسخ‌گو محسوب شوند.

٤- مخاطرات و نقش تسهیل‌گر هوش مصنوعی در ارتکاب بیوتروریسم

هم‌گرایی هوش مصنوعی مولد و زیست‌فناوری، مرزهای بیوتروریسم کلاسیک را جابه‌جا کرده و در کنار عوامل بیماری‌زای موجود در طبیعت، امکان تحلیل، اصلاح یا طراحی محاسباتی ساختارهای

زیستی را نیز در کانون ارزیابی‌های امنیتی قرار داده است (de Lima et al., 2024, p. 2) اهمیت این تحول در آن است که هوش مصنوعی می‌تواند برخی موانع اطلاعاتی و فنی را کاهش دهد و سرعت جست‌وجو، طراحی و ارزیابی گزینه‌های زیستی را افزایش دهد.

بااین‌حال، باید میان قابلیت‌های محاسباتی، امکان آزمایشگاهی و توانایی عملیاتی برای تولید و انتشار یک عامل زیستی تفکیک کرد. تولید یک توالی یا پیشنهاد محاسباتی، به‌تنهایی به معنای ساخت یک سلاح زیستی مؤثر نیست؛ زیرا عملیاتی شدن آن همچنان به دانش تخصصی، تجهیزات، مواد، آزمایش‌های تجربی و توانایی کنترل فرایندهای زیستی وابسته است. در این چارچوب، سه دسته از مخاطرات نوین بیش از سایر موارد در کانون توجه قرار دارند.

٤-١- طراحی عوامل مقاوم و امکان عبور از لایه‌های دفاعی

ابزارهای طراحی زیستی و مدل‌های پیش‌بینی ساختار، ظرفیت تحلیل توالی‌های ژنتیکی و ساختارهای پروتئینی را گسترش داده‌اند (Adamson & Allen, 2025, p. 2). این سامانه‌ها در اصل برای اهداف مشروعی مانند شناخت بیماری‌ها، طراحی دارو و مهندسی پروتئین توسعه یافته‌اند؛ اما خروجی آن‌ها ممکن است در ترکیب با سایر ابزارها و دانش تخصصی، برای بررسی تغییرات مؤثر بر بیماری‌زایی، قابلیت انتقال یا مقاومت عوامل زیستی مورد سوءاستفاده قرار گیرد. یکی از سناریوهای مورد توجه، طراحی عوامل دارای قابلیت «گریز ایمنی» است؛ یعنی عواملی که تغییرات آن‌ها ممکن است اثربخشی پاسخ ایمنی یا تدابیر درمانی موجود را کاهش دهد. افزون بر این، طراحی عامل با دوره نهفتگی طولانی‌تر یا نشانه‌های اولیه غیراختصاصی می‌تواند شناسایی زودهنگام آن را دشوار سازد. بااین‌حال، تحقق هم‌زمان این ویژگی‌ها از نظر زیستی پیچیده است و نباید صرف برخورداری از یک مدل محاسباتی را معادل توانایی قطعی برای تولید چنین عاملی دانست.

بی‌نظمی در الگوی کدون‌ها، پروموترهای نامتعارف و معماری‌های ژنتیکی غیرمعمول، عموماً از جمله شاخص‌هایی هستند که ممکن است برای شناسایی منشأ مهندسی‌شده یک توالی مورد استفاده قرار گیرند. در مقابل، عامل تهدید ممکن است بکوشد با تقلید از الگوهای طبیعی یا ایجاد تغییرات ظاهری، شناسایی مهندسی شدن توالی را دشوار کند (Annett et al., 2025 p.3). بنابراین، مسئله اصلی نه استفاده مستقیم از «بی‌نظمی کدونی» برای پنهان سازی از سیستم ایمنی، بلکه امکان کاهش قابلیت شناسایی منشأ مصنوعی یا ویژگی خطرناک توالی است.

نمونه دیگری که در ادبیات مخاطرات هوش مصنوعی مورد توجه قرار گرفته، استفاده معکوس از مدل‌های طراحی مولکولی است. در یک آزمایش شناخته شده، تغییر تابع هدف یک سامانه طراحی دارو موجب شد مدل در زمانی کوتاه هزاران ساختار مولکولی بالقوه سمی، از جمله ترکیباتی با شباهت یا سمیت پیش‌بینی‌شده در محدوده عوامل عصبی، پیشنهاد کند (de Lima et al., 2024, p. 5)این آزمایش به طراحی «پاتوژن مقاوم» مربوط نبود، بلکه نشان داد ابزارهای طراحی دارو می‌توانند با تغییر معیارهای بهینه‌سازی در جهت جست‌وجوی مولکول‌های سمی به کار گرفته شوند. افزون بر این، تولید محاسباتی یک فهرست از مولکول‌ها، به معنای امکان سنتز، پایداری یا کاربرد عملی همه آن‌ها نیست.

٤-٢-آگروتروریسم و هدف‌گیری امنیت غذایی و منابع ملی

آگروتروریسم یا تروریسم کشاورزی، به استفاده عمدی از عوامل زیستی علیه گیاهان، دام‌ها، محصولات کشاورزی یا زنجیره تأمین غذا با هدف ایجاد خسارت اقتصادی، اختلال اجتماعی یا فشار سیاسی اطلاق می‌شود و می‌توان آن را یکی از اشکال بیوتروریسم دانست (Ehsanpour & Hashempour, 2018, p. 155)

هوش مصنوعی می‌تواند با تحلیل داده‌های ژنومی، اقلیمی و کشاورزی، آسیب‌پذیری‌های گونه‌های گیاهی و دامی را شناسایی کند. این قابلیت در کاربرد مشروع، به اصلاح نژاد، کنترل بیماری و افزایش امنیت غذایی کمک می‌کند؛ اما در صورت سوءاستفاده، ممکن است برای شناسایی نقاط ضعف محصولات راهبردی یا تعیین شرایط مساعد گسترش یک عامل بیماری‌زا به کار رود

باوجوداین، تعبیر «فوق‌کشنده‌کردن حملات» از نظر علمی دقیق نیست. تأثیر یک عامل زیستی بر محصولات یا دام‌ها به عوامل متعددی مانند شرایط اقلیمی، تنوع ژنتیکی، شیوه کشت، مقاومت زیستی، امکان انتشار و تدابیر قرنطینه‌ای بستگی دارد. هوش مصنوعی می‌تواند تحلیل این متغیرها را تسهیل کند، اما نتیجه حمله را قطعی یا کاملاً قابل‌کنترل نمی‌سازد.

در سناریوهای شدیدتر، امکان طراحی یا انتخاب میکروارگانیسم‌هایی مطرح شده است که به‌صورت هدفمند به محصولات، دام‌ها، منابع آب یا بخش‌هایی از زنجیره تأمین غذا آسیب وارد کنند. گسترش چنین حملاتی ممکن است به کاهش تولید، افزایش قیمت مواد غذایی، اختلال اقتصادی و بی‌ثباتی اجتماعی منجر شود (de Lima et al., 2024, p. 8) بااین‌حال، ادعای ایجاد «گرسنگی

جمعی» باید به‌عنوان یکی از پیامدهای احتمالی در حملات گسترده و موفق بیان شود، نه نتیجه اجتناب‌ناپذیر هر حمله آگروتروریستی.

در حقوق ایران، حمله گسترده به منابع کشاورزی، دامی، آب یا امنیت غذایی ممکن است، در صورت تحقق تمام شرایط قانونی، با عنوان افساد فی‌الارض موضوع ماده ۲۸٦ قانون مجازات اسلامی انطباق یابد (هلالی و همکاران، ١٤٠٤، ص. ۱۵۵) بااین‌حال، صرف استفاده از عامل زیستی یا هوش مصنوعی برای تحقق این عنوان کافی نیست. رفتار باید به‌صورت گسترده ارتکاب یافته و موجب اخلال شدید در نظم عمومی، ناامنی یا ورود خسارت عمده شود و عنصر معنوی مقرر در قانون نیز احراز گردد. بنابراین، مجازات اعدام نتیجه خودکار هر حمله آگروتروریستی نیست، بلکه منوط به اثبات دقیق تمامی عناصر قانونی افساد فی‌الارض است.

٤-۳-حملات سایبری ـ زیستی و مخاطرات آزمایشگاه‌های ابری

امنیت سایبری زیستی[1] حوزه‌ای میان‌رشته‌ای است که از هم‌گرایی زیست‌فناوری، سامانه‌های اطلاعاتی، تجهیزات آزمایشگاهی متصل و داده‌های ژنتیکی پدید آمده است (Daniel, 2023) دیجیتالی شدن توالی‌های ژنتیکی و اتصال تجهیزات آزمایشگاهی به شبکه، در کنار مزایای پژوهشی، سطح جدیدی از مخاطرات سایبری را ایجاد می‌کند.

در این چارچوب، مسئله دقیق‌تر آن است که مهاجمان انسانی می‌توانند با بهره‌گیری از ابزارهای هوش مصنوعی برای شناسایی آسیب‌پذیری‌ها، خودکارسازی حمله یا تحلیل داده‌های سرقت‌شده، به پایگاه‌های ژنتیکی و سامانه‌های آزمایشگاهی نفوذ کنند. خودِ هوش مصنوعی، بدون عامل انسانی، مجوز دسترسی و اتصال به ابزارهای خارجی، مستقلاً «نفوذ» نمی‌کند.

دسترسی غیرمجاز به آزمایشگاه‌های ابری ممکن است به سرقت اطلاعات، تغییر داده‌های طراحی، دست‌کاری دستورهای ارسالی به تجهیزات یا اختلال در روند اجرای آزمایش منجر شود در سناریوهای شدید، دست‌کاری فایل‌های توالی یا فرایند سفارش و سنتز DNA می‌تواند موجب تولید محصولی متفاوت از آنچه پژوهشگر قصد داشته است شود. بااین‌حال، تولید مخفیانه یک پاتوژن عملیاتی مستلزم عبور از کنترل‌های متعدد فنی، انسانی و زیستی است و نباید به‌عنوان نتیجه ساده و فوری هر نفوذ سایبری توصیف شود.

1 Cyberbiosecurity

نشـت داده‌های ژنتیکی و زیسـت‌سـنجی نیز مخاطرات مهمی برای حریم خصـوصـی، تبعیض، جا سو سی علمی و امنیت ملی ایجاد می‌کند. در برخی منابع، احتمال ا ستفاده از داده‌های ژنتیکی برای طراحی عوامل زیسـتی با اثر متفاوت بر جمعیت‌های انسـانی مطرح شـده اسـت (de Lima et al., 2024, p. 4)بااین‌حال، امکان طراحی «سـلاح زیسـتی قوم‌هدف» همچنان از نظر علمی بسـیار محل تردید ا ست؛ زیرا تفاوت‌های ژنتیکی درون هر جمعیت معمولاً گسترده ا ست و مرز ژنتیکی رو شن و یکنواختی میان گروه‌های قومی وجود ندارد. ازاین‌رو، این مو ضوع باید به‌عنوان سناریوی امنیتی مورد مناقشه و بلندمدت مطرح شود، نه قابلیتی عملیاتی و اثبات‌شده.

در مجموع، نقش هوش مصـنوعی در تهدیدهای زیسـتی را نباید به طراحی مسـتقیم یک عامل بیماری‌زا محدود کرد. این فناوری می‌تواند در مراحل گوناگون، از گردآوری دانش و شـناسـایی آسـیب‌پذیری‌ها تا طراحی محاسـباتی، حملات سـایبری، پنهان‌سـازی منشـأ و انتخاب هدف، نقش تسـهیل‌کننده داشـته باشـد. بااین‌حال، ارزیابی حقوقی و امنیتی این مخاطرات باید میان امکان نظری، قابلیت آزمایشگاهی و توانایی عملیاتی تمایز گذارد تا از اغراق فناورانه و توسعه ناموجه دامنه مسئولیت کیفری جلوگیری شود.

۵- چالش‌های حریم خصوصی و امنیت داده‌های زیستی

دیجیتالی‌شدن تحقیقات زیستی و گسترش بیوانفورماتیک، حفاظت از داده‌های ژنومیک و زیست‌سنجی را به یکی از حوزه‌های نوظهور امنیت سـایبری تبدیل کرده اسـت .(Tek Leaders, 2026, p. 132) این داده‌ها به دلیل قابلیت اسـتفاده در شـناسـایی اشـخاص، پیش‌بینی برخی ویژگی‌های سـلامت، پزشـکی شخصی‌سازی‌شده و تحقیقات زیستی، از ارزش علمی، اقتصادی و امنیتی بالایی برخوردارند و ممکن است هدف حملات سایبری، جاسوسی علمی و بهره‌برداری‌های غیرمجاز قرار گیرند (Daniel, 2023)

اهمیت حمایت از داده‌های زیستی صرفاً از محرمانه‌بودن آن‌ها نا شی نمی شود. داده ژنتیکی می‌تواند اطلاعاتی درباره و ضعیت سلامت، ا ستعداد ابتلا به برخی بیماری‌ها، روابط خوی شاوندی و ویژگی‌های وراثتی فرد آشکار سازد و آثار افشای آن ممکن است به بستگان زیستی وی نیز تسری یابد. افزون بر این، ترکیب داده‌های زیستی با اطلاعات هویتی، مکانی، درمانی و رفتاری می‌تواند امکان بازشناسایی اشخاص و استنتاج اطلاعاتی را فراهم کند که هنگام جمع‌آوری اولیه داده‌ها موردنظر نبوده است.

۵-۱ .ماهیت منحصربه‌فرد داده‌های زیستی و دشواری تغییر آن‌ها

برخلاف گذرواژه، شماره کارت بانکی یا برخی شناسه‌های دیجیتال که پس از سرقت یا افشا قابل تغییر و بازنشانی‌اند، بسیاری از ویژگی‌های زیستی، از جمله توالیDNA ، اثر انگشت و ویژگی‌های اصلی چهره، ماهیتی نسبتاً پایدار دارند .ازاین‌رو، افشای این اطلاعات ممکن است آثاری بلندمدت ایجاد کند؛ زیرا شخص نمی‌تواند ژنوم یا ویژگی‌های زیست‌سنجی خود را به‌آسانی تغییر دهد.

بااین‌حال، تعبیر «غیرقابل تغییر بودن» نباید به‌صورت مطلق به کار رود. داده زیست‌سنجی ثبت‌شده در یک سامانه، مانند الگوی عددی استخراج شده از تصویر چهره یا اثر انگشت، ممکن است قابل ابطال یا جایگزینی فنی باشد؛ اما ویژگی زیستی مبنای آن عموماً پایدار باقی می‌ماند. داده ژنومیک نیز با وجود ثبات نسبی، ممکن است از نظر کیفیت نمونه، تفسیر علمی و میزان اطلاعات قابل استخراج در طول زمان تغییر کند. نشست داده های زیستی می‌تواند زمینه هویت‌رابایی مبتنی بر اطلاعات زیست سنجی، تبعیض ژنتیکی در حوزه اشتغال یا بیمه، افشای ناخواسته وضعیت سلامت و کاهش کنترل فرد بر نحوه استفاده از اطلاعات شخصی خود را فراهم سازد .(Tek Leaders, 2026, p. 4)متمایز داده ژنتیکی آن است که افشای اطلاعات یک فرد ممکن است به استنتاج اطلاعاتی درباره والدین، فرزندان و سایر خویشاوندان او نیز منجر شود؛ بنابراین رضایت یک شخص برای پردازش داده‌های ژنومیک، لزوماً تمامی آثار خانوادگی آن را پوشش نمی‌دهد.

در برخی ارزیابی‌های امنیتی، احتمال استفاده از داده‌های ژنتیکی برای طراحی عوامل زیستی با اثرگذاری متفاوت بر برخی جمعیت‌ها مطرح شده است(de Lima et al., 2024, p.7) بااین‌حال، ایده سلاح بیولوژیک «قوم‌هدف» یا «نژادهدف» از نظر علمی با محدودیت‌های جدی مواجه است؛ زیرا تنوع ژنتیکی درون گروه‌های جمعیتی بسیار گسترده است و مرز ژنتیکی روشن و یکنواختی میان گروه های قومی یا نژادی وجود ندارد. ازاین‌رو، این موضوع باید به‌عنوان سناریویی امنیتی، مناقشه‌برانگیز و بلندمدت بررسی شود، نه قابلیتی عملیاتی و اثبات‌شده.

حتی با فرض فقدان امکان طراحی سلاح قوم‌هدف، دسترسی غیرمجاز به پایگاه‌های ژنتیکی همچنان می‌تواند برای شناسایی آسیب‌پذیری‌های سلامت، هدف‌گذاری اشخاص معین، باج‌گیری، تبعیض یا جاسوسی زیستی مورد استفاده قرار گیرد. بنابراین، ضرورت حمایت حقوقی از این داده‌ها به تحقق سناریوهای بسیار شدید بیوتروریستی وابسته نیست.

۵-۲- الزامات حقوقی حکمرانی داده‌های زیستی

راهکارهای فنی زمانی اثربخش‌اند که در چارچوب حکمرانی حقوقی منسجم به کار گرفته شوند. حمایت از داده‌های زیستی مستلزم تعیین روشن مبنای قانونی جمع‌آوری و پردازش، هدف استفاده، دوره نگهداری، اشخاص مجاز به دسترسی و شرایط انتقال داخلی و فرامرزی داده‌هاست. رضایت نیز باید آگاهانه، مشخص و قابل بازنگری باشد و نمی‌توان رضایت کلی برای پژوهش را مجوز نامحدود استفاده‌های امنیتی، تجاری یا کیفری دانست.

مؤسسات نگهدارنده داده‌های ژنومیک باید اصل حداقل دسترسی، تفکیک داده‌های هویتی از داده‌های پژوهشی، ثبت سوابق دسترسی، ارزیابی اثرات حریم خصوصی و اعلام رخدادهای امنیتی را رعایت کنند. افزون بر این، استفاده از داده‌های زیستی در تصمیم‌های کیفری یا امنیتی باید تحت نظارت انسانی و قضایی قرار گیرد و اشخاص از حق اطلاع، اصلاح داده نادرست و اعتراض به تصمیم‌های مبتنی بر پردازش خودکار برخوردار باشند. در مجموع، امنیت داده‌های زیستی صرفاً مسئله حفاظت از یک پایگاه اطلاعاتی نیست، بلکه به صیانت از هویت، سلامت، کرامت و خودمختاری فرد ارتباط دارد. یادگیری فدرال، حریم خصوصی تفاضلی، بلاک‌چین و رمزنگاری هم‌ریخت می‌توانند بخشی از معماری حفاظتی باشند، اما هیچ‌یک جایگزین قواعد حقوقی مربوط به ضرورت، تناسب، محدودیت هدف، پاسخ‌گویی و نظارت مستقل نخواهند بود.

٦- چالش‌های انتساب مسئولیت کیفری و شکاف پاسخ‌گویی

ظهور سامانه‌های هوش مصنوعی مولد و عامل‌های هوشمند که می‌توانند با درجات متفاوتی از خودمختاری، چند مرحله از فرایند تحلیل، طراحی و تصمیم‌گیری زیستی را اجرا کنند، الگوهای سنتی انتساب مسئولیت کیفری را با نوعی «شکاف پاسخ‌گویی» مواجه ساخته است (Coco, 2026, p. 232). منشأ این چالش آن است که چارچوب‌های موجود حقوق کیفری، اساساً انسان‌محورند و مسئولیت را بر رفتار ارادی، قابلیت سرزنش و برخورداری مرتکب از علم و قصد استوار می‌کنند. در مقابل، الگوریتم‌های خودمختار، با وجود توانایی پردازش داده و انتخاب میان گزینه‌های مختلف، فاقد آگاهی خودبنیاد، اراده آزاد و قصد انسانی در معنای متعارف حقوقی‌اند (Coco, 2026, p. 233)

ازاین‌رو، مسئله اصلی آن نیست که آیا می‌توان خود سامانه هوش مصنوعی را مرتکب مستقل جرم دانست، بلکه باید مشخص شود خروجی زیان‌بار آن، تحت چه شرایطی به توسعه‌دهنده، ارائه‌دهنده، بهره‌بردار، فرمانده، اپراتور یا سایر اشخاص دخیل قابل انتساب است. پراکندگی کنترل و تصمیم‌گیری میان این بازیگران ممکن است موجب شود هیچ‌یک از آنان به‌تنهایی واجد تمام عناصر لازم برای مسئولیت کیفری شناخته نشوند، درحالی‌که نتیجه مجرمانه از عملکرد مجموع آنان پدید آمده است.

٦-١- بحران رکن روانی و چالش فنی جعبه سیاه

اثبات رکن معنوی جرم در پرونده‌های مرتبط با هوش مصنوعی ممکن است با چالش فنی موسوم به «جعبه سیاه» مواجه شود. بسیاری از الگوریتم‌های یادگیری عمیق از چنان پیچیدگی‌ای برخوردارند که باز سازی کامل فرایند منتهی به یک خروجی مشخص، مانند انتخاب یا پیشنهاد یک توالی ژنتیکی خطرناک، حتی برای طراحان انسانی نیز دشوار است

بااین‌حال، دشواری توضیح عملکرد درونی مدل، به‌خودی‌خود به معنای فقدان قصد یا علم در همه بازیگران انسانی نیست. هرگاه کاربر، سامانه را آگاهانه برای طراحی، بهینه سازی یا تسهیل یک عامل زیستی خطرناک به کار گرفته باشد، قصد و علم او می‌تواند از دستورهای صادرشده، داده‌های ورودی، هدف اعلام‌شده، نحوه استفاده از خروجی و سایر قرائن خارجی احراز شود؛ حتی اگر مسیر محاسباتی داخلی الگوریتم به‌طور کامل قابل توضیح نباشد.

چالش اصلی در مواردی پدید می‌آید که نتیجه زیان‌بار، هدف مستقیم هیچ‌یک از بازیگران نبوده و از تعامل غیرقابل‌پیش‌بینی میان معماری مدل، داده‌های آموزشی، محیط استقرار و تصمیم‌های خودکار ناشی شده باشد. در چنین وضعیتی، انتساب قصد یا علم به شخص انسانی دشوارتر است، مگر آنکه اثبات شود فرد سامانه را برای هدف مجرمانه پیکربندی کرده، خطر مشخصی را آگاهانه پذیرفته یا با وجود پیش‌بینی‌پذیری نتیجه، از اتخاذ تدابیر لازم خودداری کرده است (Coco, 2026, p. 236)

در ادبیات مربوط، از وضعیتی که در آن رفتار مخرب سامانه به تصمیم یا خطای انسانی مستقیم و قابل شناسایی قابل ردیابی نیست، با عنوان «جرم سخت هوش مصنوعی» یاد شده است (Coco, 2026, p. 232). بااین‌حال، این اصطلاح بیش از آنکه بیانگر فقدان مطلق عامل انسانی باشد، نشان‌دهنده دشواری اثبات نقش، کنترل و حالت ذهنی اشخاص دخیل است. حتی در چنین مواردی

باید بررسی شود که آیا تقصیر در طراحی، آموزش، آزمون، استقرار، نظارت یا توقف سامانه وجود داشته است یا خیر

۶-۲- چالش تعدد عوامل

پیچیدگی زنجیره طراحی و استقرار هوش مصنوعی، انتساب مسئولیت را با مسئله «تعدد عوامل» روبه‌رو می‌کند توسعه و بهره‌برداری از یک سامانه زیستی هوشمند ممکن است حاصل مشارکت برنامه‌نویسان، مهندسان داده، متخصصان زیست‌شناسی، شرکت‌های فناوری، تأمین‌کنندگان زیرساخت، مدیران، فرماندهان و اپراتورها باشد که هریک فقط بر بخشی از فرایند کنترل دارند

در چنین ساختاری، ممکن است توسعه‌دهنده از هدف نهایی کاربر آگاه نباشد، اپراتور بر معماری یا داده‌های آموزشی تسلط نداشته باشد و مدیر نیز تصمیم فنی معینی اتخاذ نکرده باشد. این پراکندگی دانش و کنترل، شناسایی شخصی واحد به‌عنوان مسئول نهایی را دشوار می‌کند؛ به‌ویژه هنگامی که سامانه در محیطی متفاوت از شرایط آموزش و آزمایش خود عمل کرده و رفتاری غیرمنتظره بروز داده باشد (Coco, 2026, p. 234)

بااین‌حال، تعدد عوامل نباید به مصونیت جمعی بینجامد. ارزیابی مسئولیت باید به‌صورت نقش‌محور انجام شود و درباره هر بازیگر، میزان کنترل، آگاهی، قابلیت پیش‌بینی خطر، تکلیف قانونی یا حرفه‌ای و تأثیر رفتار او بر وقوع نتیجه بررسی شود. ممکن است مسئولیت اشخاص مختلف از حیث مباشرت، معاونت، تقصیر غیرعمدی یا مسئولیت شخص حقوقی متفاوت باشد.

همچنین باید میان مشارکت در توسعه یک فناوری عمومی دارای کاربرد دوگانه و مشارکت در یک طرح مجرمانه مشخص تفکیک کرد. صرف طراحی یا انتشار ابزاری که قابلیت استفاده مشروع و نامشروع دارد، بدون احراز علم، قصد، تقصیر یا نقض تکلیف قانونی معین، نباید به مسئولیت کیفری منجر شود.

۶-۳-الگوهای انتساب مسئولیت بر اساس اساسنامه رم

الگوهای مسئولیت مقرر در اساسنامه رم تنها زمانی قابل اعمال‌اند که رفتار زیستی موردنظر واجد عناصر یکی از جرایم داخل در صلاحیت دیوان کیفری بین‌المللی، مانند نسل‌زدایی، جنایت علیه بشریت یا جنایت جنگی باشد. هر حمله بیوتروریستی یا زیستی صرفاً به دلیل شدت یا ماهیت فناورانه آن، الزاماً در صلاحیت دیوان قرار نمی‌گیرد.

الف) ارتکاب جرم با استفاده از هوش مصنوعی به‌عنوان ابزار

بر اساس بند ۳(الف) ماده ۲۵ اساسنامه رم، شخص ممکن است جرم را به‌تنهایی، مشترکاً یا از طریق شخص دیگری ارتکاب دهد. در ادبیات مرتبط پیشنهاد شده است که هوش مصنوعی به‌عنوان «ابزار فاقد مسئولیت» در اختیار طراح یا اپراتور تحلیل شود؛ برای مثال، شخصی سامانه را آگاهانه برای هدف‌گیری یک جمعیت معین یا طراحی یک عامل زیستی به کار گیرد (Coco, 2026, p. 241)

بااین‌حال، از نظر اصطلاحی، عنوان «ارتکاب از طریق دیگری» در اساسنامه رم ناظر به ارتکاب جرم از طریق « شخص دیگر» است. ازآنجاکه سامانه هوش مصنوعی در حقوق موجود شخص محسوب نمی‌شود، دقیق‌تر آن است که در این فرض، از ارتکاب مستقیم جرم با استفاده از یک ابزار فناورانه سخن گفته شود. هوش مصنوعی در چنین حالتی وسیله اجرای تصمیم مجرمانه است و مسئولیت متوجه شخصی خواهد بود که با علم و قصد لازم، آن را در خدمت طرح مجرمانه قرار داده است.

تنها در صورتی می‌توان از مباشرت معنوی به معنای دقیق سخن گفت که مرتکب، شخص انسانی دیگری را که فاقد مسئولیت یا تحت سلطه اوست، برای اجرای جرم به کار گیرد. بنابراین، نباید مفهوم «عامل بی‌گناه» بدون تعدیل به خود سامانه هوش مصنوعی تسری داده شود.

ب) مسئولیت فرماندهان و سایر مافوق‌ها

ماده ۲۸ اساسنامه رم، مسئولیت فرماندهان نظامی و سایر مافوق‌ها را در قبال جرایم ارتکابی نیروها یا زیردستان انسانیِ تحت فرماندهی و کنترل مؤثر آنان مقرر می‌کند. تحقق این مسئولیت مستلزم آن است که فرمانده یا مافوق از ارتکاب یا شرف ارتکاب جرم آگاه بوده یا، حسب مورد، باید آگاه می‌بود و با وجود برخورداری از کنترل مؤثر، اقدامات ضروری و معقول را برای پیشگیری، سرکوب یا گزارش جرم انجام نداده باشد

بنابراین، نمی‌توان مسئولیت مافوق را مستقیماً به «جرم سامانه هوش مصنوعی تحت نظارت فرمانده» تسری داد؛ زیرا الگوریتم، نیروی نظامی یا زیردست انسانی محسوب نمی‌شود (Coco, 2026, p. 253)

بااین‌حال، اگر نیروها یا اپراتورهای انسانی تحت کنترل مؤثر فرمانده، از هوش مصنوعی برای ارتکاب جرم استفاده کنند، ماده ۲۸ قابل اعمال خواهد بود. در این فرض، سامانه هوش مصنوعی

بخشی از ابزار یا ساختار عملیاتی نیروهای انسانی است و مسئولیت فرمانده از رفتار زیردستان و قصور او در نظارت ناشی می‌شود، نه از رابطه حقوقی مستقیم میان فرمانده و الگوریتم.

٦-٤-بازاندیشی در معیار تقصیر و حدود مسئولیت کیفری

خودمختاری نسبی و پیش‌بینی‌ناپذیری برخی سامانه‌های هوش مصنوعی، اتکای صرف به قصد مستقیم را برای پاسخ‌گویی به همه زیان‌های ناشی از آن‌ها ناکافی ساخته است. ازاین‌رو، شماری از پژوهشگران پیشنهاد کرده‌اند که در کنار مسئولیت عمدی، امکان انتساب مسئولیت بر مبنای بی‌پروایی و بی‌احتیاطی یا بی‌مبالاتی نیز مورد توجه قرار گیرد.(Pagallo, 2013, p. 84)

بر این اساس، هرگاه توسعه‌دهنده، ارائه‌دهنده یا بهره‌بردار از وجود خطری جدی و ناموجه آگاه باشد، اما با وجود امکان پیشگیری، سامانه طراحی زیستی را در محیطی حساس به کار گیرد، ممکن است به دلیل پذیرش آگاهانه خطر یا نقض تکلیف مراقبت مسئول شناخته شود (Bashayreh et al., 2021, p. 175). تشخیص این مسئولیت به عواملی مانند میزان آگاهی شخص، شدت و احتمال وقوع خطر، استانداردهای حرفه‌ای، امکان اتخاذ تدابیر پیشگیرانه و وجود رابطه سببیت میان قصور و نتیجه زیان‌بار بستگی دارد.

رعایت دقت لازم در این حوزه می‌تواند شامل ارزیابی خطر پیش از استقرار، انجام آزمون‌های ایمنی، محدودکردن دسترسی به قابلیت‌های حساس، ثبت فعالیت‌های سامانه، نظارت انسانی، پیش‌بینی سازوکار توقف اضطراری و گزارش رخدادهای امنیتی باشد. نقض این الزامات تنها زمانی می‌تواند مبنای مسئولیت کیفری قرار گیرد که تکلیف قانونی یا حرفه‌ای مشخصی وجود داشته باشد و میان کوتاهی شخص و نتیجه مجرمانه، رابطه استناد قابل اثباتی برقرار شود.(King et al., 2019, p. 102)

در کنار مسئولیت مبتنی بر تقصیر، پیشنهاد اعمال مسئولیت مطلق نسبت به برخی فعالیت‌های فوق‌خطرناک سایبری ـــ زیستی نیز مطرح شده است؛ مسئولیتی که در آن اثبات قصد یا تقصیر ضرورت ندارد .(Wagner, 2021, p. 12) پذیرش چنین الگویی در قلمرو حقوق کیفری با اصولی مانند شخصی‌بودن مسئولیت، لزوم تقصیر و تناسب جرم و مجازات تعارض دارد. به‌ویژه در جرایم شدیدی مانند بیوتروریسم، جنایت علیه بشریت و نسل‌زدایی، نمی‌توان مسئولیت مطلق را جایگزین اثبات علم، قصد یا سایر اشکال معتبر رکن روانی کرد.

حتی در صـــورت پذیرش محدود این رویکرد، مناســـب‌تر اســـت قلمرو آن به تخلفات ایمنی و تنظیم‌گرانه اختصـــاص یابد؛ مانند عرضـــه ســـامانه بدون انجام ارزیابی خطر الزامی، نقض تکالیف گزارش‌دهی، فقدان کنترل دسترسی یا رعایت‌نکردن استانداردهای اجباری. در جرایم شدید، همچنان باید قصد، علم، پذیرش آگاهانه خطر یا درجه‌ای از تقصیر کیفری متناسب با ماهیت جرم احراز شود.

بر این مبنا، راه‌حل شکاف پاسخ‌گویی نه اعطای شخصیت کیفری به سامانه و نه حذف رکن روانی از جرایم شدید است. الگوی مناسب‌تر، توزیع مسئولیت بر اساس نقش هر شخص، میزان کنترل او، سطح آگاهی، قابلیت پیش‌بینی خطر و نقض تکالیف مراقبتی است (Bashayreh et al., 2021, p. 182). این الگو از یک سو مانع پنهان شدن اشخاص مسئول در پس پیچیدگی‌های فنی می شود و از سـوی دیگر، توسـعه‌دهندگان و ارائه‌دهندگان را بدون اثبات نقش مؤثر یا تقصـیر، مسـئول تمام نتایج پیش‌بینی‌نشده سامانه نمی‌داند.

۷-مبانی انتساب مسئولیت کیفری در حقوق ایران

نظام حقوق کیفری ایران، مسئولیت را بر رفتار قابل انتساب به شخص و احراز علم، اراده، قصد یا تقصیر او استوار می‌سازد. بر همین اساس، در جرایم زیستی مرتبط با سامانه‌های هوشمند، باید نقش و میزان کنترل هریک از طراحان، ارائه‌دهندگان، مدیران و کاربران در وقوع نتیجه مجرمانه به‌طور جداگانه بررسی شود.

۷-۱-شرایط عمومی مسئولیت کیفری

مطابق ماده ۱۴۰ قانون مجازات اسلامی مصوب ۱۳۹۲، تحقق مسئولیت کیفری در حدود، قصاص و تعزیرات منوط به آن اســت که مرتکب هنگام ارتکاب رفتار، عاقل، بالغ و مختار باشــد مســئولیت کیفری بر شخصی تحمیل می شود که افزون بر انتساب رفتار زیان‌بار به او، از قابلیت درک و انتخاب برخوردار باشد و بتوان وی را به سبب رفتار ارتکابی سرزنش کرد

در جرایم بیوتروریستی نیز میزان آگاهی و اختیار مرتکب در ارزیابی مسئولیت او اهمیت اساسی دارد. شخصی که با شناخت ماهیت عامل زیستی و پیامدهای انتشار آن، آگاهانه در طراحی یا اجرای حمله مشارکت می‌کند، نسبت به فردی که بدون اطلاع کافی یا تحت اجبار در بخشی از فرایند دخالت داشته است، از قابلیت سرزنش بیشتری برخوردار خواهد بود در جرایم عمدی، وجود شرایط ماده

۱٤۰ به‌تنهایی کافی نیســـت و رکن معنوی جرم نیز باید احراز شـــود. مطابق ماده ۱٤٤ قانون مجازات اسلامی، در جرایم مقید، مرتکب باید علاوه بر قصد انجام رفتار، قصد تحقق نتیجه مجرمانه یا علم به وقوع آن را داشته باشد. بنابراین، در مواردی که انتشار عامل زیستی به مرگ، بیماری گسترده یا اخلال در سلامت عمومی منجر می‌شود، مسئولیت عمدی تنها زمانی قابل انتساب است که علم یا قصد لازم نسبت به نتیجه نیز اثبات شود

۷-۲-مباشرت، تسبیب و رابطه استناد

در حملات زیســـتی، به دلیل دوره نهفتگی عوامل بیماری‌زا، دخالت متغیرهای محیطی و فاصـــله زمانی میان رفتار و نتیجه، اثبات رابطه سببیت با دشواری همراه است ازاین‌رو، احراز رابطه استناد میان رفتار مرتکب و نتیجه زیان‌بار، یکی از مهم‌ترین شرایط تحمیل مسئولیت کیفری است. این رابطه باید با استفاده از شواهد علمی، پزشکی، اپیدمیولوژیک و قرائن عقلی اثبات شود و صرف احتمال یا تسامح عرفی برای انتساب نتیجه کافی نیست (صادقی و میرزایی، ۱۳۹۸، صص. ۱٦۷).

هرگاه شخص مستقیماً عامل زیستی را منتشر کند یا سامانه‌ای را آگاهانه برای اجرای حمله به کار گیرد، ممکن است رفتار به‌عنوان مباشرت به او منتسب شود. استفاده از تجهیزات خودکار یا ابزارهای محاسباتی نیز مانع تحقق مباشرت انسانی نیست؛ زیرا ابزار فاقد اراده مستقل حقوقی است و رفتار به شخصی منتسب می‌شود که آن را آگاهانه هدایت کرده است.

در صورت دخالت هم‌زمان مباشر و مسبب، اصل بر مسئولیت مباشر است، مگر آنکه نقش سبب چنان مؤثر باشد که نتیجه عرفاً و حقوقاً به او مستند شود. این وضعیت در فقه و حقوق با قاعده «سبب اقوی از مباشر» تحلیل می شود (عباسی و فروغی، ۱٤۰۰، ص. ۸۱). برای مثال، اگر پزشکی با علم به آلودگی یک دارو، پرســـتاری ناآگاه را مأمور تزریق آن کند، نتیجه بیش از آنکه به پرســـتار فاقد علم منتسب باشد، به رفتار پزشک مستند خواهد بوددر فرض تعدد اسباب نیز نمی‌توان صرفاً بر تقدم یا تأخر زمانی تکیه کرد. هرچند در برخی تحلیل‌ها مسئولیت سبب مؤخر در وجود مطرح شده است معیار اصلی باید میزان تأثیر هر عامل و استناد نتیجه به رفتار او باشد. ممکن است سبب متأخر، حلقه نهایی وقوع زیان باشـــد، اما در مواردی نیز ســـبب مقدم نقش اصـــلی را در ایجاد خطر داشـــته باشـــد. بنابراین، دادگاه باید ســـهم واقعی هر عامل، قابلیت پیش‌بینی نتیجه و رابطه رفتار او با زیان نهایی را جداگانه بررسی کند.

۷-۳- مسئولیت طراح، اپراتور و ارائه‌دهنده ابزار

در حملات سایبری ـ زیستی، مسئولیت اشخاص بر اساس نقشی که در طراحی، هدایت یا تسهیل حمله داشته‌اند تعیین می‌شود. طراح نرم‌افزار یا سامانه صرفاً به دلیل تولید یک ابزار دارای کاربرد دوگانه، مسئول هر استفاده مجرمانه از آن نیست. مسئولیت او زمانی مطرح می‌شود که با علم به هدف مجرمانه، سامانه را برای اجرای حمله معین طراحی یا تغییر داده، محدودیت‌های ایمنی را حذف کرده یا امکانات لازم را در اختیار مرتکب قرار داده باشد.

اپراتور یا کاربری که با اطلاع از ماهیت عمل و پیامدهای آن، سامانه را برای آلوده‌سازی منابع آب، انتشار عامل بیماری‌زا یا اخلال در زیر ساخت‌های زیستی هدایت می‌کند، حسب نوع دخالت ممکن است مباشر، شریک یا مسبب جرم شناخته شود. در جرایم مقید، افزون بر قصد هدایت سامانه، باید قصد نتیجه یا علم به تحقق آن نیز احراز شود (کرامت میرشکارلو و خالقی، ۱۴۰۳، ص. ۷).

ارائه‌دهندگان ابزارهای فنی نیز در شرایطی ممکن است مسئولیت کیفری مستقلی داشته باشند. ماده ۷۵۳ قانون مجازات اسلامی، که ناظر به ابزارهای ارتکاب جرایم رایانه‌ای است، تولید، انتشار، توزیع یا در دسترس قراردادن نرم‌افزارها و وسایلی را که منحصراً برای ارتکاب جرایم رایانه‌ای طراحی شده‌اند، جرم‌انگاری کرده است. بنابراین، اگر ابزاری به‌طور اختصاصی برای نفوذ به سامانه‌های آزمایشگاهی یا زیرساخت‌های زیستی تهیه یا عرضه شود، امکان اعمال این ماده وجود دارد (یکرنگی و مرسی، ۱۳۹۹، ص. ۳۱۱). بااین‌حال، درباره ابزارهای عمومی و دارای استفاده مشروع، صرف امکان سوءاستفاده برای تحقق جرم کافی نیست.

۷-۴- مسئولیت کیفری اشخاص حقوقی

مواد ۲۰ و ۱۴۳ قانون مجازات اسلامی، امکان مسئولیت کیفری اشخاص حقوقی را پذیرفته‌اند. این موضوع در جرایم زیستی اهمیت ویژه‌ای دارد؛ زیرا فعالیت‌های آزمایشگاهی، دارویی و زیست‌فناورانه معمولاً در قالب شرکت‌ها، مؤسسات پژوهشی یا مراکز درمانی انجام می‌شوند

مطابق ماده ۱۴۳، شخص حقوقی زمانی مسئول است که نماینده قانونی آن، به نام یا در راستای منافع شخص حقوقی مرتکب جرم شود. بنابراین، صرف وقوع جرم در محیط یک شرکت یا استفاده از تجهیزات آن برای انتساب مسئولیت کافی نیست و باید رابطه رفتار مرتکب با نمایندگی، فعالیت یا منافع شخص حقوقی احراز شود (مرادی و دیگران، ۱۴۰۰، ص. ۱۵۱).

وجود نظام مؤثر نظارت داخلی، کنترل دسترسی، ثبت فعالیت‌ها و ارزیابی خطر می‌تواند در تشخیص تقصیر سازمانی و تعیین واکنش کیفری مؤثر باشد. بااین‌حال، صرف برخورداری از سازوکارهای نظارتی، مسئولیت شخص حقوقی را به‌طور خودکار منتفی نمی‌کند. دادگاه باید واقعی و مؤثربودن این تدابیر و نقش آن‌ها در پیشگیری از جرم را بررسی کند. این اقدامات ممکن است، حسب شرایط قانونی، در تعیین یا تخفیف مجازات و بهره‌مندی از برخی نهادهای ارفاقی مؤثر باشند (یکرنگی و زمانی، ۱٤۰۳، صص. ۵۱۵ و ۵۳۳).

مجازات‌هایی مانند انحلال یا مصادره کل اموال نیز در همه موارد قابل اعمال نیستند و تحقق آن‌ها به شرایط خاص قانونی وابسته است. بنابراین، ضعف نظارت یا وقوع جرم توسط یکی از کارکنان، بدون احراز شرایط مقرر، نباید به‌طور خودکار به شدیدترین مجازات شخص حقوقی منجر شود.

۷-۵- .افساد فی‌الارض و تمایز آن از محاربه

ماده ۲۸٦ قانون مجازات اسلامی یکی از مهم‌ترین مستندهای قانونی برای رسیدگی به حملات زیستی گسترده است. این ماده، پخش گسترده مواد سمی، میکروبی و خطرناک را در صورتی که موجب اخلال شدید در نظم عمومی، ناامنی یا ورود خسارت عمده به تمامیت جسمانی اشخاص یا اموال عمومی و خصوصی شود، در قلمرو افساد فی‌الارض قرار می‌دهد

تحقق این جرم به صرف انتشار یک عامل زیستی وابسته نیست. رفتار باید از گستردگی لازم برخوردار باشد و آثار شدید مقرر در قانون را ایجاد کند. مفاهیمی مانند «گسترده»، « شدید» و «عمده» باید با توجه به شمار قربانیان، دامنه جغرافیایی، مدت استمرار خطر، میزان خسارت و آثار واردشده بر سلامت و امنیت عمومی احراز شوند (احمدزاده و دیگران، ۱٤۰۳، صص. ۱۷۹). افزون بر این، قصد ایجاد اخلال گسترده یا علم مرتکب به مؤثربودن رفتار خود نیز باید اثبات شود.

افساد فی‌الارض با محاربه تفاوت دارد. مطابق ماده ۲۷۹ قانون مجازات اسلامی، محاربه مستلزم کشیدن سلاح با قصد تعرض به جان، مال یا ناموس مردم یا ارعاب آنان، به‌گونه‌ای است که موجب ناامنی در محیط شود. ازاین‌رو، در حملات زیستی پنهانی که بدون کشیدن سلاح به معنای قانونی انجام می شوند، انطباق رفتار با محاربه محل تردید است. در مقابل، ماده ۲۸٦ به‌طور صریح به پخش مواد سمی و میکروبی اشاره کرده و مبنای روشن‌تری برای رسیدگی به حملات زیستی گسترده فراهم می‌کند (احمدزاده و دیگران، ۱٤۰۳، ص. ۱۷٦).

معاونت در افساد فی‌الارض نیز به‌طور خودکار موجب اعمال مجازات مباشر اصلی نمی‌شود. شخصی که مواد، داده یا تجهیزات لازم را فراهم می‌کند، باید بر اساس قواعد معاونت و با توجه به علم، قصد و میزان دخالت خود مسئول شناخته شود. تنها در صورتی می‌توان مجازات شدیدتری بر او تحمیل کرد که رفتار وی مستقلاً واجد عناصر افساد فی‌الارض باشد یا عنوان مجرمانه دیگری، مانند سردستگی گروه مجرمانه سازمان‌یافته، درباره او تحقق یابد (حاجی‌ده‌آبادی، ۱۴۰۱، ۲۴).

بر این اساس، مسئولیت کیفری در حملات بیوتروریستی باید با احراز جداگانه شرایط عمومی مسئولیت، رکن معنوی، رابطه استناد و نقش هر شخص تعیین شود. شدت نتیجه یا پیچیدگی فناوری نباید جایگزین اثبات عناصر قانونی جرم شود.

نتیجه‌گیری

پیوند فناوری‌های مولد با زیست‌فناوری، ماهیت تهدیدهای زیستی را از الگویی صرفاً آزمایشگاهی به ساختاری ترکیبی و داده‌محور تغییر داده است. در این وضعیت، داده‌های ژنومیک، مدل‌های زبانی، ابزارهای طراحی زیستی، آزمایشگاه‌های ابری و سامانه‌های عامل‌محور می‌توانند در مراحل مختلف تحلیل، طراحی، ارزیابی و اجرای فرایندهای زیستی نقش داشته باشند. بااین‌حال، توان محاسباتی به‌تنهایی معادل برخورداری از قابلیت عملیاتی برای تولید یا انتشار عامل زیستی نیست و تحقق یک حمله همچنان به دانش تخصصی، تجهیزات، مواد، زیرساخت و امکان کنترل فرایندهای آزمایشگاهی وابسته است. اهمیت این فناوری‌ها بیشتر در کاهش موانع اطلاعاتی، تسریع تحلیل و نزدیک‌کردن مراحل طراحی محاسباتی به اجرای فیزیکی نهفته است.

یافته‌های پژوهش نشان داد که کارکرد این فناوری‌ها در حوزه امنیت زیستی دوگانه است. همان ابزارهایی که می‌توانند برای پایش ژنومیک، شناسایی الگوهای غیرعادی، غربالگری سفارش‌های سنتز DNA، حفاظت از داده‌های زیستی و تقویت سازوکارهای عدم اشاعه به کار روند، ممکن است برای شناخت آسیب‌پذیری‌های سامانه‌های دفاعی، سازمان‌دهی دانش تخصصی یا تسهیل بخشی از اقدامات زیان‌بار نیز مورد سوءاستفاده قرار گیرند. بنابراین، ارزیابی حقوقی آن‌ها نباید بر ماهیت ذاتی ابزار استوار باشد، بلکه باید نوع کاربرد، سطح دسترسی، هدف کاربر، قابلیت‌های فعال‌شده و وجود یا فقدان سازوکارهای نظارتی را در نظر گیرد.

در حوزه حفاظت از داده‌ها نیز رو شن شد که افزایش ظرفیت تحلیل ژنومیک، مخاطراتی فراتر از نقض محرمانگی ایجاد می‌کند. داده‌های ژنتیکی می‌توانند اطلاعاتی درباره سلامت، خویشاوندان و ویژگی‌های وراثتی ا شخاص آ شکار سازند و آثار اف شای آن‌ها بلندمدت و گاه غیرقابل جبران با شد. راهکارهایی مانند یادگیری فدرال، حریم خصوصی تفاضلی، بلاک‌چین و رمزنگاری هم‌ریخت می‌توانند بخشی از مخاطرات را کاهش دهند، اما جایگزین قواعد حقوقی مربوط به رضایت، محدودیت هدف، کمینه سازی داده، کنترل د ستر سی، پا سخ‌گویی و نظارت م ستقل نی ستند. ازاین‌رو، امنیت زیستی باید هم‌زمان با صیانت از حریم خصوصی، آزادی پژوهش و حق اعتراض به تصمیم‌های خودکار دنبال شود.

مهم‌ترین چالش حقوق کیفری در این حوزه، تعیین نحوه انتساب نتیجه زیان‌بار به بازیگران انسانی و اشخاص حقوقی است. سامانه‌های هوشمند در چارچوب حقوق موجود فاقد اراده، آگاهی خودبنیاد و اهلیت جنایی‌اند و نمی‌توانند م ستقلاً مرتکب جرم شناخته شوند. در نتیجه، راه‌حل منا سب اعطای شخصیت کیفری به سامانه نیست، بلکه باید مسئولیت اشخاصی بررسی شود که در طراحی، آموزش، عرضه، استقرار، نظارت یا استفاده از آن نقش داشته‌اند.

با توجه به پراکندگی دانش و کنترل میان توسعه‌دهنده، ارائه‌دهنده زیرساخت، مدیر، اپراتور و کاربر نهایی، انت ساب م سئولیت نباید به صورت کلی و جمعی انجام گیرد. ارزیابی م سئولیت باید نق شمحور با شد و درباره هر شخص، میزان کنترل، سطح آگاهی، قابلیت پیش‌بینی خطر، وجود تکلیف قانونی یا حرفه‌ای، نحوه مداخله و رابطه اس تناد میان رفتار و نتیجه بررسی شود. صرف طراحی یا ارائه یک فناوری دارای کاربرد دوگانه، بدون احراز علم، ق صد، تق صیر یا نقش مؤثر، نمی‌تواند مبنای م سئولیت کیفری باشد. در مقابل، پیچیدگی فنی نیز نباید به ابزاری برای فرار اشخاص مسئول از پاسخ‌گویی تبدیل شود.

در حقوق ایران، مواد ۱٤۰، ۱٤٤ و قانون مجازات اسلامی، همراه با قواعد مباشرت، تسبیب، معاونت و مسئولیت اشخاص حقوقی، ظرفیت اولیه برای تحلیل این پرونده‌ها را فراهم می‌کنند. در جرایم عمدی، اثبات قصد رفتار و حسب مورد قصد نتیجه یا علم به وقوع آن ضروری است. در موارد غیرعمدی نیز مسئولیت به احراز تقصیر، وجود تکلیف مراقبتی و رابطه سببیت وابسته خواهد بود. اگر شخص آگاهانه سامانه را برای ارتکاب حمله زیستی به کار گیرد، می‌توان رفتار را مستقیماً به او

منتسب کرد؛ اما درباره طراحان و ارائه‌دهندگان، صرف امکان سوءاستفاده کافی نیست و باید مشارکت آگاهانه، تسهیل هدفمند یا نقض تکلیف مشخص اثبات شود.

در حملات گسترده زیستی، ماده ۲۸۶ قانون مجازات اسلامی به دلیل تصریح به پخش مواد سمی و میکروبی، ظرفیت بیشتری برای انطباق با افساد فی‌الارض دارد؛ بااین‌حال، اعمال این عنوان منوط به احراز گستردگی رفتار، اخلال شدید، خسارت عمده و عنصر معنوی مقرر در قانون است. محاربه نیز به دلیل وابستگی به مفهوم کشیدن سلاح، در حملات پنهانی زیستی با دشواری بیشتری در انطباق روبه‌رو است. بنابراین، شدت نتیجه یا ماهیت فناورانه رفتار نباید جایگزین تفسیر مضیق مقررات کیفری و اثبات دقیق عناصر جرم شود.

برآیند پژوهش آن است که الگوی مطلوب برای مواجهه کیفری با بیوتروریسم مبتنی بر فناوری‌های مولد، الگویی چندسطحی و مبتنی بر مسئولیت تفکیک‌شده است. در این الگو، مسئولیت کیفری شدید باید همچنان به اثبات علم، قصد یا تقصیر متناسب وابسته باشد؛ درحالی‌که تخلفات ایمنی و تنظیم‌گرانه، مانند فقدان ارزیابی خطر، رعایت‌نکردن استانداردهای دسترسی، نقض تکالیف گزارش‌دهی یا نبود سازوکار توقف اضطراری، می‌توانند موضوع مسئولیت‌های مستقل و متناسب قرار گیرند.

از منظر سیاست جنایی، تدوین استانداردهای اجباری ارزیابی خطر، ثبت و نگهداری سوابق تصمیم‌گیری، کنترل دسترسی به قابلیت‌های حساس، نظارت انسانی مؤثر، گزارش رخدادهای امنیتی و تعیین حدود مسئولیت اشخاص حقوقی ضروری است. همچنین، همکاری بین‌المللی در زمینه غربالگری توالی‌ها، حفاظت از داده‌های ژنومیک و تقویت سازوکارهای اعتمادسازی باید توسعه یابد. در نهایت، پاسخ حقوقی کارآمد باید از یک سو مانع سوءاستفاده از پیچیدگی‌های فنی برای گریز از مسئولیت شود و از سوی دیگر، از توسعه ناموجه مسئولیت کیفری و محدودسازی بی‌ضابطه پژوهش‌های مشروع جلوگیری کند.

فهرست منابع

احمدزاده، رسول؛ موسوی مجاب، سیددرید؛ صابر، محمود. (۱٤۰۳). اخلالِ افساد فی‌الارض محور در نظام اقتصادی کشور. مجلس و راهبرد، ۳۱(۱۲۰)، ۱۷۹-۲۰٤.

پورسعید، فرزانه؛ جلالی، محمود؛ راعی، مسعود. (۱٤۰۳). چالش‌های کارکردی نظام ممنوعیت جنگ‌افزارهای بیولوژیکی. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ٥٤(۱)، ٤۰٥-٤۲۷.

جلالی، محمود؛ آقالر، علی اصغر. (۱٤۰۲). توسل به بیوتروریسم از منظر حقوق بین‌الملل. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ٥۳(٤)، ۲۰٥۷-۲۰۷۹.

حاجی‌ده‌آبادی، احمد. (۱٤۰۱). درنگی پیرامون معاونت در افساد فی‌الارض موضوع ماده ۲۸٦. فصلنامه دین و قانون، ۱۰(۳٥)، ۱-۲٥.

زارع بیدکی، مجید؛ بلالی مود، مهدی. (۱۳۹٤). بیوتروریسم و جنگ‌افزارهای بیولوژیک، از گذشته تا به امروز: یک مطالعه مروری کلاسیک. مجله علمی دانشگاه علوم پزشکی بیرجند، ۲۲(۳)، ۱۸۲-۱۸۸.

زرقانی، سید هادی؛ نسیمی، زهرا؛ خوارزمی، امید علی. (۱۳۹۷). بیوتروریسم و تأثیر آن بر امنیت شهروندان. جغرافیای اجتماعی شهری، ٥(۲)، ۱۷-۳۰.

سازگارنژاد، احمدرضا؛ احمدی، امیرمحمد؛ عابدین زاده، زهرا؛ فاطمی، فاطمه سادات؛ رکن الدینی، فاطمه؛ میرزایی، محمدرضا؛ نظیف کار، محمد؛ خواجه پور، بهاره؛ فاطمی، حسین؛ میرعمادی، سید ایمان. (۱٤۰۲). هوش مصنوعی مولد: دیدگاه‌های چندرشته‌ای پیرامون فرصت‌ها، چالش‌ها و پیامدها در پژوهش، عمل و سیاستگذاری. سیاست علم و فناوری، ۱۷(۰)، ۱-۱۰۰.

شاهسواری، مریم؛ موسوی، سیده مرضیه. (۱٤۰۱). تهدیدات زیستی بیوتروریسم و نقش پدافند غیرعامل در مواجهه با آن. مجموعه مقالات همایش ملی جنگ بیولوژیک: ماهیت، ابعاد، پیامدها و راهکارها، دامغان.

صادقی، محمدهادی؛ میرزایی، محمد. (۱۳۹۸). ماهیت رابطه استناد و معیار احراز آن. مطالعات فقه و حقوق اسلامی، ۱۱(۲۱)، ۱٦۷-۱۹٤.

عباسی، مراد؛ فروغی، فضل‌الله. (۱٤۰۰). بازاندیشی مقایسه ای دو نظریه سبب مقدم در تأثیر و سبب اقوی از مباشر. مطالعات حقوقی معاصر، ۱۲(۲٤)، ۸۱-۱۰٤.

کرامت میرشکارلو، یاسین؛ خالقی، ابوالفتح. (۱٤۰۳). مسئولیت کیفری ارتکاب ترور سایبری با فناوری هوش مصنوعی در حقوق کیفری بین الملل. اولین کنفرانس ملی پژوهش های نوظهور در مدیریت و حقوق با رویکرد شعار سال.

مرادی، محمد؛ صادقی، آزاده؛ هادی‌تبار، اسماعیل. (۱٤۰۰). مطالعه تطبیقی مسئولیت کیفری اشخاص حقوقی در ایران و شورای اروپا. پژوهشنامه حقوق تطبیقی، ۵(۱)، ۱۵۱-۱۷۲.

هلالی، مهدی؛ خالقی، ابوالفتح؛ فتحی، مرتضی. (۱٤۰٤). سیاست جنایی ایران و مصر در مقابله با بیوتروریسم. آموزه‌های حقوق کیفری کشورهای اسلامی، ۱۰، ۱۵۵-۱۸٤.

یکرنگی، محمد؛ زمانی بابگهری، زینب. (۱٤۰۳). مطالعه تطبیقی تأثیر سازوکارهای نظارتی و کنترلی مؤثر بر مسئولیت کیفری شخص حقوقی. مطالعات حقوق کیفری و جرم‌شناسی، ٥٤(۲)، ۵۱۵-۵۳۳.

یکرنگی، محمد؛ مرسی، هادی. (۱۳۹۹). تحلیل جرم‌انگاری تولید و پخش نرم‌افزار و ابزارهای الکترونیکی صرفاً مجرمانه. دیدگاه‌های حقوق قضایی، (۹۲)، ۳۱۱-۳۳۲.

Adamson, G., & Allen, G. C. (2025). Opportunities to strengthen U.S. biosecurity from AI-enabled bioterrorism: What policymakers should know. Center for Strategic and International Studies (CSIS).

Angeles, K. (2026). How would an AI verification system work in the Biological Weapons Convention? Georgetown Security Studies Review.

Annett, E., DiEuliis, D., & Giordano, J. (2025). Artificial intelligence: A double-edged sword in support and subversion of the Biological Weapons Convention Part One: Framing the issues. Strategic Insights, Institute for National Strategic Studies, National Defense University.

Annett, E., Giordano, J., & Melley, B. (2026, February 20). VIEWPOINT: How AI can help enforce the Biological Weapons Convention. National Defense Magazine.

Bashayreh, M. H., et al. (2021). Artificial intelligence and legal liability: towards an international approach of proportional liability based on risk sharing. Information & Communications Technology Law, 30(2), 169–192.

Coco, A. (2026). Modes of liability for AI-enabled crimes in international criminal law. International Law Studies, 107, 228–255.

Daniel, C. (2023, July 15). Biosecurity: The imperative role of AI in cyberbiosecurity. Medium.

de Lima, R. C., Sinclair, L., Megger, R., Maciel, M. A. G., Vasconcelos, P. F. C., & Quaresma, J. A. S. (2024). Artificial intelligence challenges in the face of biological threats: Emerging catastrophic risks for public health. Frontiers in Artificial Intelligence, 7, Article 1382356. https://doi.org/10.3389/frai.2024.1382356

de Vries, B. (2026, February 10). Biological weapons: Why strengthening the BWC matters now. Lieber Institute at West Point.

Ehsanpour, S. R., & Hashempour, N. (2018). Agroterrorism; Iranian criminal policy. International Journal of Multicultural and Multireligious Understanding, 5(6), 155–161.

Goldsmith, J. (2026, May 20). Establishing US-China cooperation on open-source AI-biosecurity risks. Pacific Forum.

King, T. C., et al. (2019). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 26, 89–120.

Pagallo, U. (2013). The Laws of Robots: Crimes, Contracts, and Torts. Springer Science & Business Media.

Radcliffe, J. (2025). Assessing the accelerated threat of bioterrorism in the age of AI. William & Mary Environmental Law and Policy Review, 49(3), 761-785.

Tek Leaders. (2026). Biological data privacy: The next frontier in cybersecurity challenges.

Thiermann, H., Kehe, K., & Zoller, L. (2020). Chemical and Biological Weapons and Their Regulation. In Regulatory Toxicology (pp. 473-500). Springer.

Wagner, G. (2021). Liability for Artificial Intelligence: A Proposal of the European Parliament. SSRN Electronic Journal