

مسئولیت بین المللی دولت ها در قبال تصمیمات اتخاذ شده توسط سامانه های هوش مصنوعی خودمختار در فضای سایبری

(تاریخ دریافت ۱۴۰۵/۰۲/۱۲، تاریخ تصویب ۱۴۰۵/۰۳/۱۲)

مهدی کلانتری

چکیده

گسترش روزافزون سامانه های هوش مصنوعی خودمختار در فضای سایبری، چالش های نوینی را در حوزه حقوق بین الملل و به ویژه در نظام مسئولیت بین المللی دولت ها ایجاد کرده است. مسئله اصلی این پژوهش آن است که آیا قواعد سنتی مسئولیت بین المللی، به ویژه اصول انتساب رفتار و نقض تعهدات بین المللی، توان پاسخگویی به پیامدهای ناشی از تصمیمات مستقل این سامانه ها را دارند یا خیر. پژوهش حاضر با رویکردی تحلیلی و توصیفی، ضمن بررسی نظریه های کلاسیک مسئولیت بین المللی دولت ها مانند انتساب ارگانیک، کنترل مؤثر و کنترل کلی، به ارزیابی ظرفیت و محدودیت آن ها در مواجهه با فناوری های نوین پرداخته است. نتایج پژوهش بیانگر آن است که نظام مسئولیت بین المللی در حال حرکت به سوی یک الگوی ترکیبی است که در آن، علاوه بر انتساب مستقیم، مفاهیمی مانند کنترل ساختاری، مدیریت ریسک و بهره برداری از فناوری های پرخطر نیز در تعیین مسئولیت دولت ها نقش آفرین هستند. بر این اساس، حقوق بین الملل نیازمند بازتفسیر تدریجی و توسعه هنجاری است تا بتواند با تحولات ناشی از هوش مصنوعی در فضای سایبری همگام شود و از بروز خلأهای حقوقی در سطح بین المللی جلوگیری نماید.

واژگان کلیدی: مسئولیت بین المللی دولت ها، هوش مصنوعی خودمختار، فضای سایبری،

انتساب رفتار، حکمرانی الگوریتمی، کنترل مؤثر



مقدمه

تحولات شگرف فناوری اطلاعات و ارتباطات در دهه‌های اخیر، فضای سایبری را به یکی از مهم‌ترین عرصه‌های تعامل، رقابت و حتی تقابل دولت‌ها تبدیل کرده است. گسترش وابستگی جوامع به زیرساخت‌های دیجیتال، توسعه فناوری‌های کلان‌داده، یادگیری ماشین و هوش مصنوعی موجب شده است که بسیاری از فعالیت‌های راهبردی دولت‌ها در حوزه‌های امنیتی، نظامی، اقتصادی و اطلاعاتی به سامانه‌های هوشمند متکی شوند. در این میان، ظهور سامانه‌های هوش مصنوعی خودمختار که قادرند بدون مداخله مستقیم انسان و بر اساس الگوریتم‌های پیچیده، داده‌ها را تحلیل کرده و تصمیمات عملیاتی اتخاذ کنند، ابعاد جدیدی از چالش‌های حقوقی را در عرصه بین‌المللی پدید آورده است. کاربرد روزافزون این سامانه‌ها در عملیات سایبری، از جمله شناسایی تهدیدات، دفاع خودکار از شبکه‌ها، جمع‌آوری اطلاعات، پاسخ به حملات سایبری و حتی اجرای اقدامات تهاجمی، موجب شده است که مرز میان تصمیم انسانی و تصمیم ماشینی به تدریج کمرنگ شود. در چنین شرایطی، این پرسش بنیادین مطرح می‌شود که در صورت ارتکاب یک عمل متخلفانه بین‌المللی توسط سامانه‌های هوش مصنوعی خودمختار، مسئولیت ناشی از آن بر عهده چه شخص یا نهادی خواهد بود و آیا قواعد سنتی مسئولیت بین‌المللی دولت‌ها توان پاسخگویی به این وضعیت نوظهور را دارند یا خیر. نظام مسئولیت بین‌المللی دولت‌ها که بر مبنای انتساب رفتار و نقض تعهدات بین‌المللی شکل گرفته است، عمدتاً در زمانی توسعه یافته که تمامی تصمیمات و اقدامات مؤثر در روابط بین‌الملل مستقیماً توسط اشخاص انسانی اتخاذ می‌شد. با این حال، هوش مصنوعی خودمختار به دلیل برخورداری از قابلیت یادگیری، تحلیل مستقل داده‌ها و اتخاذ تصمیمات غیرقابل پیش‌بینی، چالش‌های مهمی را در زمینه انتساب رفتار، احراز عنصر تقصیر، تعیین حدود کنترل دولت و شناسایی رابطه سببیت میان رفتار دولت و نتایج حاصل از عملکرد سامانه ایجاد کرده است. از این رو، بسیاری از مفاهیم سنتی حقوق بین‌الملل با پرسش‌هایی مواجه شده‌اند که پاسخ به آن‌ها نیازمند بازاندیشی نظری و تفسیری است. اهمیت این موضوع زمانی دوچندان می‌شود که



اقدامات سایبری مبتنی بر هوش مصنوعی می‌توانند آثار فرامرزی گسترده‌ای بر امنیت ملی، زیرساخت‌های حیاتی، حریم داده‌ها و حقوق بنیادین اشخاص در کشورهای مختلف برجای گذارند. افزون بر این، ماهیت فراملی فضای سایبری و دشواری شناسایی منشأ حملات، فرایند انتساب رفتار به دولت‌ها را پیچیده‌تر ساخته و زمینه بروز اختلافات حقوقی و سیاسی گسترده‌ای را فراهم آورده است. در نتیجه، تداوم توسعه فناوری‌های خودمختار بدون تبیین دقیق چارچوب‌های مسئولیت بین‌المللی، می‌تواند به ایجاد خلأهای حقوقی و کاهش کارآمدی نظام حقوق بین‌الملل در حفظ نظم و امنیت بین‌المللی منجر شود. پژوهش حاضر درصدد است با بهره‌گیری از مبانی حقوق بین‌الملل عمومی، قواعد مسئولیت بین‌المللی دولت‌ها، اسناد و رویه‌های موجود در حوزه حقوق سایبری و نظریه‌های نوین مرتبط با حکمرانی هوش مصنوعی، امکان انتساب تصمیمات اتخاذشده توسط سامانه‌های هوش مصنوعی خودمختار به دولت‌ها و آثار حقوقی ناشی از آن را مورد بررسی قرار دهد. هدف اصلی این پژوهش آن است که ضمن تحلیل ظرفیت‌ها و محدودیت‌های قواعد موجود، راهکارهایی برای انطباق نظام مسئولیت بین‌المللی با واقعیت‌های فناورانه نوظهور ارائه کند و به توسعه ادبیات حقوقی در یکی از مهم‌ترین چالش‌های حقوق بین‌الملل معاصر یاری رساند.

بخش اول: نظریه‌های مسئولیت بین‌المللی دولت‌ها

بند اول: نظریه کلاسیک مسئولیت مبتنی بر نقض تعهد

بر اساس نظریه کلاسیک مسئولیت بین‌المللی دولت‌ها مبتنی بر «عمل متخلفانه بین‌المللی»، تحقق مسئولیت منوط به اجتماع دو رکن اساسی است: نخست، انتساب رفتار به دولت و دوم، نقض یک تعهد بین‌المللی لازم‌الاجرا. این رویکرد که ریشه در رویه قضایی دیوان بین‌المللی دادگستری و همچنین در پیش‌نویس مواد کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت‌ها (ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts, ۲۰۰۱) دارد، یکی از منسجم‌ترین چارچوب‌های



نظری در حقوق بین‌الملل معاصر به شمار می‌رود. در این نظریه، مسئولیت بین‌المللی ماهیتی اساساً عینی و دولت‌محور دارد. بدین معنا که تمرکز اصلی بر رفتار منتسب به دولت و انطباق یا عدم انطباق آن با تعهدات بین‌المللی است، نه بر عنصر ذهنی یا روانی عامل. برخلاف برخی نظام‌های حقوق داخلی که مسئولیت مدنی یا کیفری را بر پایه تقصیر یا سوءنیت استوار می‌سازند، در حقوق بین‌الملل تحقق مسئولیت دولت‌ها نیازی به اثبات تقصیر ندارد و صرف وقوع فعل متخلفانه کافی است. این ویژگی، نظام مسئولیت بین‌المللی را به یک نظام «ناقص‌محور» و مبتنی بر نقض تعهد تبدیل کرده است. دیوان بین‌المللی دادگستری در آرای متعددی، از جمله در قضایای مربوط به دیوار حائل در سرزمین‌های اشغالی و نیز پرونده‌های مرتبط با فعالیت‌های نظامی و حمایت از گروه‌های غیردولتی، بر این اصل تأکید کرده است که عنصر کلیدی در احراز مسئولیت، انتساب رفتار به دولت و نقض تعهدات بین‌المللی است. در همین راستا، پیش‌نویس مواد کمیسیون حقوق بین‌الملل نیز نظامی ساختارمند برای تعیین شرایط انتساب، از جمله رفتار ارکان دولت، اشخاص تحت کنترل دولت و همچنین موارد پذیرش یا تصدیق رفتار، ارائه می‌دهد. اهمیت این نظریه در آن است که توانسته چارچوبی نسبتاً منسجم و قابل پیش‌بینی برای تنظیم روابط میان دولت‌ها فراهم آورد و از پراکندگی و ابهام در حوزه مسئولیت بین‌المللی جلوگیری کند. با این حال، این چارچوب در بستر تحولات نوین فناوری، به‌ویژه ظهور سامانه‌های هوش مصنوعی خودمختار، با چالش‌های جدی مواجه شده است. زیرا در این موارد، تعیین رابطه مستقیم میان اراده دولت و رفتار متخلفانه با پیچیدگی‌های فنی و مفهومی همراه است که می‌تواند کارآمدی معیارهای سنتی انتساب را تحت تأثیر قرار دهد.

بند دوم: نظریه مسئولیت مبتنی بر خطر

بر اساس نظریه مسئولیت مبتنی بر خطر^۱، مبنای تحقق مسئولیت بین‌المللی دولت‌ها از تمرکز صرف بر تقصیر یا انتساب مستقیم فراتر رفته و بر «ایجاد، کنترل یا بهره‌برداری از یک وضعیت

^۱ Risk-Based Responsibility



خطرناک قابل پیش‌بینی» استوار می‌شود. در این رویکرد، اصل بنیادین آن است که هرگاه دولت با علم به احتمال بروز خسارت فرامرزی، اقدام به توسعه، به کارگیری یا اجازه فعالیت در حوزه‌ای پرخطر نماید، ممکن است مسئول پیامدهای ناشی از آن شناخته شود. حتی اگر نتوان رفتار زیان‌بار را به‌طور مستقیم به اراده یا دستور مشخص دولت منتسب کرد، این نظریه به‌ویژه در پاسخ به نارسایی‌های نظام سنتی مسئولیت بین‌المللی شکل گرفته است. نظامی که عمدتاً بر انتساب مستقیم رفتار به دولت و اثبات نقض تعهدات مشخص متمرکز است. در حالی که در حوزه‌های نوین فناوری، از جمله انرژی هسته‌ای، فعالیت‌های فضایی، و به‌ویژه فناوری‌های دیجیتال و سایبری، زنجیره‌یت و کنترل به‌قدری پیچیده است که انتساب مستقیم همواره امکان‌پذیر نیست. از این رو، نظریه مبتنی بر خطر تلاش می‌کند با جایگزینی معیار «قابلیت پیش‌بینی و ایجاد خطر قابل توجه»، خلأهای موجود را جبران نماید. در فضای سایبری، به کارگیری سامانه‌های هوش مصنوعی خودمختار نمونه بارز فعالیت‌های پرخطر نوین محسوب می‌شود. این سامانه‌ها به دلیل توانایی تصمیم‌گیری مستقل، یادگیری مداوم و تعامل پیچیده با محیط دیجیتال، می‌توانند پیامدهایی فراتر از کنترل مستقیم انسانی ایجاد کنند. بنابراین، حتی در مواردی که رفتار مشخص و زیان‌بار قابل انتساب مستقیم به دولت نباشد، صرف طراحی، استقرار یا بهره‌برداری آگاهانه از چنین سامانه‌هایی ممکن است مبنای مسئولیت بین‌المللی قرار گیرد. از منظر هنجاری، این نظریه با اصولی همچون احتیاط^۱ و الزام به مراقبت مقتضی^۲ هم‌پوشانی دارد و در برخی حوزه‌های حقوق بین‌الملل محیط زیست و حقوق فعالیت‌های خطرناک نیز مورد پذیرش نسبی قرار گرفته است. توسعه آن در حوزه فضای سایبری و هوش مصنوعی همچنان محل بحث است، زیرا معیارهای تعیین خطر قابل پیش‌بینی و حدود مسئولیت دولت‌ها در این حوزه به‌طور دقیق تبیین نشده است. از این منظر، نظریه مبتنی بر خطر می‌تواند مکملی برای نظام سنتی مسئولیت بین‌المللی باشد، نه جایگزینی کامل برای آن.

^۱ Precautionary Principle

^۲ Due Diligence



بند سوم: نظریه مسئولیت عینی و تضمینی در حقوق بین‌الملل

بر اساس نظریه مسئولیت عینی و تضمینی^۱، دولت‌ها در برخی حوزه‌های خاص حقوق بین‌الملل ممکن است بدون نیاز به اثبات تقصیر، سوءنیت یا حتی در مواردی بدون لزوم احراز دقیق انتساب رفتار، مسئول پیامدهای زیان‌بار ناشی از فعالیت‌های خود شناخته شوند. این رویکرد در واقع شکل توسعه‌یافته‌ای از مسئولیت است که بر نتیجه تمرکز دارد نه بر رفتار یا وضعیت ذهنی عامل. در این چارچوب، صرف تحقق خسارت و وجود ارتباط منطقی میان فعالیت دولت و زیان وارده می‌تواند برای احراز مسئولیت کافی تلقی شود. ریشه‌های این نظریه را می‌توان در برخی رژیم‌های خاص حقوق بین‌الملل مشاهده کرد. به‌ویژه در حوزه‌هایی که فعالیت‌ها ذاتاً خطرناک یا با احتمال بالای ایجاد خسارت فرامرزی همراه هستند، مانند فعالیت‌های فضایی، استفاده از انرژی هسته‌ای، یا برخی رژیم‌های مسئولیت در حقوق محیط زیست بین‌المللی. در این حوزه‌ها، به دلیل ماهیت پرریسک فعالیت، نظام حقوقی به سمت پذیرش مسئولیت سخت‌گیرانه‌تر حرکت کرده است تا از یک‌سو جبران خسارت قربانیان تضمین شود و از سوی دیگر، دولت‌ها به رعایت استانداردهای ایمنی و احتیاطی ملزم گردند. ویژگی مهم این نظریه آن است که بار اثبات را به شکل قابل توجهی بر دوش دولت یا عامل فعالیت قرار می‌دهد و از ورود به مباحث پیچیده‌ای مانند قصد، تقصیر یا حتی کنترل مستقیم تا حدی فاصله می‌گیرد. در نتیجه، این رویکرد از منظر حمایت از زیان‌دیدگان و افزایش کارآمدی نظام جبران خسارت، مزیت قابل توجهی دارد. با این حال، از منظر سنتی حقوق بین‌الملل، پذیرش گسترده آن با چالش‌هایی همراه بوده است، زیرا ممکن است با اصل حاکمیت دولت‌ها و منطق مبتنی بر انتساب در تعارض نسبی قرار گیرد. در حوزه فناوری‌های نوین، به‌ویژه سامانه‌های هوش مصنوعی خودمختار در فضای سایبری، نظریه مسئولیت عینی اهمیت ویژه‌ای پیدا می‌کند. زیرا این سامانه‌ها به دلیل پیچیدگی الگوریتمی، یادگیری مستقل و رفتارهای غیرقابل پیش‌بینی، می‌توانند خساراتی ایجاد کنند که انتساب دقیق آن به یک تصمیم

^۱ Objective or Strict Liability



انسانی یا اراده مشخص دشوار است. در چنین شرایطی، اتکای صرف بر معیارهای سنتی مسئولیت ممکن است به ایجاد خلأ جبران منجر شود. بنابراین، توسعه رویکردهای عینی یا تضمینی می‌تواند به عنوان یک راه‌حل مکمل برای تضمین پاسخگویی دولت‌ها در قبال پیامدهای ناشی از این فناوری‌ها مطرح گردد. گسترش این نظریه در حقوق بین‌الملل معاصر نیازمند دقت هنجاری بالاست، زیرا اعمال مسئولیت مطلق می‌تواند پیامدهایی همچون افزایش بار حقوقی دولت‌ها و ایجاد موانع در توسعه فناوری را به همراه داشته باشد. از این رو، بسیاری از حقوق‌دانان پیشنهاد می‌کنند که مسئولیت عینی در این حوزه‌ها به صورت محدود، هدفمند و مبتنی بر معیارهای مشخص خطر و پیش‌بینی‌پذیری اعمال شود تا تعادل میان توسعه فناوری و حمایت از حقوق بین‌الملل حفظ گردد.

بخش دوم: نظریه‌های انتساب رفتار و کنترل

بند اول: نظریه انتساب ارگانیک^۱

بر اساس نظریه انتساب ارگانیک، رفتار ارکان دولت به طور مستقیم و بدون نیاز به احراز شرایط اضافی به خود دولت منتسب می‌شود. این نظریه یکی از بنیادی‌ترین و کلاسیک‌ترین مبانی مسئولیت بین‌المللی دولت‌ها را تشکیل می‌دهد و در ماده ۴ پیش‌نویس مواد کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت‌ها (ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts, ۲۰۰۱) به صورت صریح تثبیت شده است. مطابق این ماده، اعمال هر یک از ارکان دولت، اعم از قوه مقننه، مجریه، قضاییه یا هر شخص یا نهادی که به موجب حقوق داخلی واجد وصف «ارگان دولتی» باشد، به دولت قابل انتساب است. حتی اگر آن ارگان در چارچوب اختیارات خود عمل نکرده یا از حدود صلاحیت خود فراتر رفته باشد. منطق بنیادین این نظریه بر وحدت شخصیت حقوقی دولت استوار است. دولت به عنوان یک شخص حقوقی واحد در حقوق بین‌الملل، از طریق ارکان و

^۱ Organic Attribution



نهادهای خود در عرصه بین‌المللی عمل می‌کند و بنابراین، تفکیک میان رفتار ارگان و دولت از منظر مسئولیت بین‌المللی پذیرفته نیست. این رویکرد موجب ایجاد شفافیت، پیش‌بینی‌پذیری و انسجام در نظام مسئولیت بین‌المللی شده و از پیچیدگی‌های مربوط به تفکیک مسئولیت اشخاص داخلی دولت جلوگیری می‌کند. در پرتو تحولات فناوری و ظهور سامانه‌های هوش مصنوعی خودمختار، کارایی و کفایت این نظریه با چالش‌های جدی مواجه شده است. نخست آنکه، سامانه‌های هوش مصنوعی ذاتاً فاقد شخصیت حقوقی دولتی هستند و به‌طور معمول در زمره ارکان رسمی دولت قرار نمی‌گیرند. حتی در مواردی که دولت‌ها از این سامانه‌ها در فرآیندهای تصمیم‌گیری یا اجرای عملیات سایبری استفاده می‌کنند، این سامانه‌ها معمولاً به‌عنوان ابزار یا فناوری تلقی می‌شوند، نه به‌عنوان «ارگان» به معنای حقوقی آن. دوم آنکه، شرط اساسی برای اعمال نظریه انتساب ارگانیک، وجود رابطه ساختاری و حقوقی میان نهاد مورد نظر و دولت است. در حالی که بسیاری از سامانه‌های هوش مصنوعی خودمختار توسط شرکت‌های خصوصی توسعه یافته و صرفاً در اختیار یا مورد بهره‌برداری دولت قرار می‌گیرند، نه به‌عنوان بخشی از ساختار رسمی دولت. بنابراین، در اغلب موارد، این سامانه‌ها نمی‌توانند به‌طور مستقیم ذیل مفهوم ارگان دولتی قرار گیرند، مگر آنکه در سطح نهادی و حقوقی به‌صورت کامل در ساختار دولت ادغام شده باشند. با وجود این محدودیت‌ها، نظریه انتساب ارگانیک همچنان در تحلیل برخی سناریوهای خاص مرتبط با هوش مصنوعی قابل استفاده است. برای مثال، در صورتی که یک سامانه هوش مصنوعی به‌طور کامل در یک نهاد دولتی ادغام شده باشد و به‌عنوان ابزار تصمیم‌گیری رسمی آن نهاد عمل کند، می‌توان رفتار آن را به‌طور غیرمستقیم به ارگان دولتی منتسب دانست. در چنین حالتی، مسئولیت نه به خود سامانه، بلکه به نهاد انسانی یا ساختار دولتی که آن را به کار گرفته است، بازمی‌گردد. نظریه انتساب ارگانیک همچنان ستون فقرات نظام سنتی مسئولیت بین‌المللی دولت‌ها را تشکیل می‌دهد، اما در مواجهه با فناوری‌های نوینی مانند سامانه‌های هوش مصنوعی خودمختار، با محدودیت‌های مفهومی و ساختاری مواجه است. این وضعیت نشان می‌دهد که برای پاسخگویی به چالش‌های نوظهور در فضای سایبری، لازم است این نظریه در کنار سایر نظریه‌های انتساب، به‌ویژه نظریه



کنترل مؤثر و کنترل کلی، به صورت ترکیبی و تکمیلی مورد استفاده قرار گیرد تا بتوان شکاف‌های موجود در نظام مسئولیت بین‌المللی را تا حد امکان کاهش داد.

بند دوم: نظریه کنترل مؤثر^۱

بر اساس نظریه کنترل مؤثر، انتساب رفتار به دولت منوط به احراز میزان مشخصی از کنترل واقعی و عملی دولت بر عامل یا عملیات مورد نظر است. این نظریه یکی از معیارهای کلیدی در حقوق بین‌الملل معاصر برای تعیین حدود مسئولیت دولت‌ها به شمار می‌رود و در رویه دیوان بین‌المللی دادگستری، به‌ویژه در قضایای مشهور مرتبط با فعالیت گروه‌های غیردولتی، مورد تأکید قرار گرفته است. مطابق این رویکرد، صرف حمایت، تأمین مالی یا حتی هدایت کلی یک عامل غیردولتی برای انتساب رفتار به دولت کافی نیست، بلکه باید ثابت شود که دولت در زمان وقوع عمل متخلفانه، کنترل مؤثر و عملیاتی بر آن رفتار خاص داشته است. منطق این نظریه بر تفکیک میان «حمایت کلی» و «کنترل عملیاتی مستقیم» استوار است. به عبارت دیگر، حقوق بین‌الملل میان وضعیت‌هایی که دولت صرفاً بستر یا امکانات انجام عمل را فراهم می‌کند با مواردی که در آن دولت به‌طور واقعی در هدایت و اجرای عملیات نقش دارد، تمایز قائل می‌شود. این تمایز با هدف جلوگیری از توسعه بی‌ضابطه مسئولیت دولت‌ها و حفظ اصل حاکمیت و استقلال دولت‌ها طراحی شده است. در بستر تحولات فناوری و به‌ویژه ظهور سامانه‌های هوش مصنوعی خودمختار، اعمال این نظریه با چالش‌های جدی مواجه شده است. یکی از مهم‌ترین پرسش‌ها این است که آیا مفهوم «کنترل مؤثر» که اساساً برای رفتار انسان‌ها و گروه‌های سازمان‌یافته طراحی شده، قابلیت انطباق با سامانه‌های الگوریتمی پیچیده و خودآموز را دارد یا خیر. این سامانه‌ها، به‌ویژه در حوزه فضای سایبری، بر اساس یادگیری ماشینی، پردازش کلان‌داده و تحلیل مستقل محیط عمل می‌کنند و در بسیاری موارد، رفتار آن‌ها قابل پیش‌بینی دقیق یا هدایت لحظه‌ای توسط انسان نیست. مسئله اصلی در تطبیق نظریه

^۱ Effective Control Test



کنترل مؤثر با هوش مصنوعی، تعیین حدود «کنترل واقعی» دولت بر فرآیندهای تصمیم‌گیری الگوریتمی است. در حالی که دولت‌ها ممکن است در مرحله طراحی، آموزش یا استقرار این سامانه‌ها نقش مستقیم داشته باشند، اما پس از فعال‌سازی، تصمیمات عملیاتی ممکن است به گونه‌ای اتخاذ شود که از کنترل مستقیم انسانی خارج گردد. این وضعیت موجب ایجاد شکاف میان کنترل اولیه و رفتار نهایی سامانه می‌شود. شکافی که در نظریه سنتی کنترل مؤثر به صراحت پیش‌بینی نشده است. با وجود این چالش‌ها، برخی حقوقدانان معتقدند که می‌توان مفهوم کنترل مؤثر را به صورت پویا تفسیر کرد و آن را از کنترل لحظه‌ای به کنترل ساختاری و طراحی محور توسعه داد. بر این اساس، اگر دولت در طراحی معماری سیستم، تعیین اهداف، محدودسازی الگوریتم‌ها و نظارت بر عملکرد کلی سامانه نقش تعیین‌کننده داشته باشد، می‌توان وجود نوعی کنترل مؤثر غیرمستقیم را پذیرفت. در مقابل، دیدگاه‌های محدودتر بر این باورند که فقدان امکان مداخله مستقیم در تصمیمات لحظه‌ای سامانه‌های خودمختار، مانع از اعمال کامل این نظریه در حوزه هوش مصنوعی است. نظریه کنترل مؤثر اگرچه همچنان یکی از ابزارهای اصلی برای تحلیل انتساب رفتار در حقوق بین‌الملل محسوب می‌شود، اما در مواجهه با سامانه‌های هوش مصنوعی خودمختار نیازمند بازتفسیر و توسعه مفهومی است تا بتواند پاسخگوی پیچیدگی‌های فنی و عملی فضای سایبری معاصر باشد.

بند سوم: نظریه کنترل کلی و توسعه آن در حقوق بین‌الملل نوین

بر اساس نظریه کنترل کلی^۱، برای انتساب رفتار به دولت یا یک بازیگر حقوقی، نیازی به اثبات کنترل مستقیم و جزئی بر هر اقدام مشخص وجود ندارد، بلکه احراز نوعی «کنترل ساختاری، سازمانی و راهبردی» بر مجموعه عملیات یا نهاد کافی است. این نظریه در برخی رویه‌های حقوق بین‌الملل کیفری، به‌ویژه در آرای دادگاه‌های کیفری بین‌المللی برای یوگسلاوی سابق، توسعه یافته و به عنوان معیاری میان‌برد میان کنترل صرفاً حمایتی و کنترل مؤثر سخت‌گیرانه

^۱ Overall Control



مطرح شده است. در این چارچوب، اگر یک دولت در طراحی، سازمان‌دهی، تجهیز یا هدایت کلی یک ساختار عملیاتی نقش تعیین‌کننده داشته باشد، می‌توان رفتارهای منتسب به آن ساختار را به دولت مرتبط دانست، حتی اگر جزئیات عملیات توسط عوامل میانی یا مستقل انجام شود. منطق این نظریه بر این فرض استوار است که در ساختارهای پیچیده و چندلایه، تمرکز بر کنترل جزئی و لحظه‌ای عملاً غیرواقع‌بینانه است و ممکن است به فرار از مسئولیت در نظام‌های سازمان‌یافته منجر شود. بنابراین، معیار کنترل کلی تلاش می‌کند میان ضرورت حفظ مسئولیت‌پذیری و واقعیت پیچیدگی ساختارهای مدرن تعادل برقرار کند. در بستر حقوق بین‌الملل نوین و به‌ویژه در فضای سایبری، این نظریه قابلیت کاربرد قابل توجهی پیدا می‌کند. سامانه‌های هوش مصنوعی خودمختار معمولاً در یک چرخه پیچیده از طراحی، آموزش، استقرار و بهره‌برداری قرار دارند که در آن، دولت‌ها یا نهادهای وابسته به آن‌ها نقش اساسی در تعیین اهداف، معماری الگوریتمی و چارچوب عملکردی سامانه دارند. حتی اگر تصمیمات عملیاتی در سطح خرد توسط الگوریتم‌های یادگیرنده و بدون مداخله انسانی اتخاذ شود، همچنان می‌توان گفت که دولت از طریق کنترل کلی بر طراحی و کارکرد سامانه، در شکل‌گیری نتایج نهایی نقش دارد. توسعه این نظریه در حوزه هوش مصنوعی با چالش‌هایی نیز همراه است. از جمله اینکه مرز میان «کنترل کلی» و «استفاده صرف از فناوری» به‌روشنی قابل تعیین نیست و ممکن است تفسیر گسترده آن به گسترش بیش از حد مسئولیت دولت‌ها منجر شود. با وجود این، بسیاری از تحلیلگران حقوق بین‌الملل بر این باورند که نظریه کنترل کلی می‌تواند به عنوان یک ابزار تفسیری مهم، خلأهای موجود در نظریه کنترل مؤثر را در مواجهه با سامانه‌های پیچیده و خودمختار تا حدی جبران کند و زمینه را برای توسعه تدریجی قواعد مسئولیت در عصر فناوری‌های نوین فراهم سازد.



بخش سوم: نظریه‌های حکمرانی فناوری و هوش مصنوعی

بند اول: نظریه حکمرانی الگوریتمی^۱

بر اساس نظریه حکمرانی الگوریتمی، ساختارهای قدرت و فرآیندهای تصمیم‌گیری در دولت‌های معاصر به تدریج از الگوهای سنتی مبتنی بر تصمیم‌انسانی به سمت نظام‌های مبتنی بر داده و الگوریتم حرکت کرده‌اند. در این چارچوب، الگوریتم‌ها و سامانه‌های هوش مصنوعی نه صرفاً ابزارهای کمکی، بلکه به عنوان سازوکارهای فعال حکمرانی عمل می‌کنند که در حوزه‌های مختلفی از جمله امنیت، اقتصاد، مدیریت منابع، کنترل مرزها و حتی سیاست‌گذاری عمومی نقش ایفا می‌نمایند. بدین ترتیب، بخشی از اعمال حاکمیت دولت به سطح محاسباتی و خودکار منتقل شده و تصمیم‌گیری انسانی در بسیاری از موارد به مرحله طراحی، نظارت یا اصلاح محدود می‌شود. این تحول مفهومی، بنیان‌های سنتی حقوق عمومی و حقوق بین‌الملل را با چالش‌های اساسی مواجه ساخته است. در نظام کلاسیک حکمرانی، مسئولیت ناشی از تصمیمات دولتی به طور مستقیم به اراده و اقدام مقامات انسانی قابل انتساب بود. اما در الگوی حکمرانی الگوریتمی، تصمیمات نهایی ممکن است نتیجه پردازش پیچیده داده‌ها، یادگیری ماشین و تعاملات غیرخطی سامانه‌های هوش مصنوعی باشد که پیش‌بینی کامل آن‌ها برای انسان دشوار یا حتی ناممکن است. در نتیجه، مرز میان «تصمیم دولت» و «خروجی سیستم» به تدریج مبهم می‌شود. در این نظریه، دولت‌ها همچنان نقش محوری در طراحی، تنظیم و تعیین چارچوب‌های عملکرد الگوریتم‌ها دارند. به عبارت دیگر، حاکمیت از بین نرفته، بلکه «فناورانه» و «غیرمستقیم» شده است. دولت‌ها از طریق تعیین داده‌های ورودی، طراحی اهداف سیستم، انتخاب مدل‌های یادگیری و وضع محدودیت‌های عملکردی، به طور ساختاری در فرآیند حکمرانی مشارکت دارند. با این حال، استقلال نسبی سامانه‌های هوش مصنوعی در تولید خروجی‌ها موجب می‌شود که مسئولیت ناشی از خطاهای الگوریتمی به سادگی قابل

^۱ Algorithmic Governance



انتساب مستقیم به یک تصمیم انسانی خاص نباشد. از منظر حقوق بین الملل، این وضعیت پرسش‌های مهمی را درباره ماهیت مسئولیت دولت‌ها ایجاد می‌کند. اگر یک سامانه هوش مصنوعی در فضای سایبری تصمیمی اتخاذ کند که منجر به نقض تعهدات بین‌المللی یا ورود خسارت فرامرزی شود، این سؤال مطرح می‌شود که آیا مسئولیت ناشی از آن باید بر مبنای طراحی و کنترل سیستم به دولت منتسب گردد یا آنکه استقلال عملکردی الگوریتم‌ها می‌تواند نوعی گسست در زنجیره انتساب ایجاد کند. نظریه حکمرانی الگوریتمی نشان می‌دهد که فناوری نه تنها ابزار اجرای قدرت، بلکه به بخشی از ساختار خود قدرت تبدیل شده است. این امر مستلزم بازاندیشی در مفاهیم سنتی مسئولیت، حاکمیت و انتساب در حقوق بین‌الملل است تا بتوان میان واقعیت‌های نوین فناوری و چارچوب‌های حقوقی موجود تعادل برقرار کرد.

بند دوم: نظریه انسان در حلقه تصمیم^۱

بر اساس نظریه «انسان در حلقه تصمیم»، مشروعیت و مسئولیت‌پذیری سامانه‌های هوش مصنوعی، به وجود نوعی نظارت و مداخله انسانی در چرخه تصمیم‌گیری وابسته است. این نظریه بر این اصل استوار است که حتی در پیشرفته‌ترین سامانه‌های خودمختار، باید انسان در یکی از مراحل کلیدی فرآیند تصمیم‌سازی حضور داشته باشد. خواه در مرحله طراحی و برنامه‌ریزی، خواه در مرحله تأیید نهایی یا امکان مداخله اضطراری. هدف اصلی این رویکرد، حفظ کنترل انسانی بر فناوری و جلوگیری از رهاسازی کامل تصمیمات حساس به الگوریتم‌های غیرانسانی است. در چارچوب حقوقی، این نظریه تلاش می‌کند پیوند میان تصمیمات فناورانه و مسئولیت حقوقی را حفظ کند. بدین معنا که هرگاه یک سامانه هوش مصنوعی اقدام به تولید خروجی زیان‌بار یا ناقض تعهدات بین‌المللی نماید، بتوان آن را به انسانی منتسب کرد که در طراحی، نظارت یا بهره‌برداری از آن نقش داشته است. از این منظر، نظریه «انسان در حلقه تصمیم» به عنوان ابزاری برای جلوگیری از گسست مسئولیت در عصر

^۱ Human-in-the-Loop Theory



خود کارسازی عمل می‌کند و مانع از شکل‌گیری خلأ حقوقی در مواجهه با فناوری‌های نوین می‌شود. در عمل و به‌ویژه در سامانه‌های هوش مصنوعی خودمختار در فضای سایبری، کارایی این نظریه با چالش‌های جدی مواجه است. بسیاری از سامانه‌های پیشرفته به گونه‌ای طراحی شده‌اند که فرآیند تصمیم‌گیری آن‌ها در لحظه و بر اساس تحلیل داده‌های پویا انجام می‌شود، به گونه‌ای که مداخله انسانی یا بسیار محدود است یا عملاً پس از وقوع تصمیم صورت می‌گیرد. در چنین شرایطی، «حضور انسان در حلقه ممکن است به یک حضور صوری یا صرفاً تأییدی تبدیل شود، بدون آنکه تأثیر واقعی بر ماهیت تصمیم داشته باشد. از منظر حقوق بین‌الملل، این وضعیت پرسش مهمی را مطرح می‌سازد: آیا صرف وجود یک لایه نظارت انسانی کافی است تا مسئولیت کامل تصمیمات به دولت یا عامل انسانی منتسب شود، یا آنکه باید میزان واقعی و مؤثر کنترل انسانی مورد ارزیابی قرار گیرد؟ پاسخ به این پرسش، نقش تعیین‌کننده‌ای در تبیین حدود مسئولیت دولت‌ها در قبال عملکرد سامانه‌های هوش مصنوعی خودمختار دارد و نشان می‌دهد که نظریه انسان در حلقه تصمیم اگرچه از نظر هنجاری جذاب است، اما در مواجهه با فناوری‌های بسیار پیشرفته نیازمند بازتعریف و تکمیل مفهومی است.

بند سوم: نظریه استقلال فناورانه و شکاف مسئولیت^۱

بر اساس نظریه «استقلال فناورانه و شکاف مسئولیت»، توسعه سامانه‌های هوش مصنوعی خودمختار موجب شکل‌گیری فاصله‌ای فزاینده میان اراده انسانی و نتایج عملی تصمیمات الگوریتمی شده است. این نظریه بر این فرض استوار است که هرچه سطح استقلال عملکردی سامانه‌های هوش مصنوعی افزایش یابد، توانایی انسان یا دولت در پیش‌بینی، کنترل و هدایت مستقیم نتایج کاهش می‌یابد و در نتیجه، زنجیره سنتی انتساب در حقوق بین‌الملل دچار گسست یا ابهام می‌شود. در نظام‌های کلاسیک حقوق بین‌الملل، مسئولیت دولت‌ها بر یک رابطه نسبتاً خطی میان اراده دولت، رفتار قابل انتساب و نتیجه زیان‌بار استوار است. اما در فضای

^۱ Technological Autonomy Gap



سایبری و به‌ویژه در سامانه‌های یادگیرنده و خودمختار، این رابطه به‌صورت غیرخطی و پیچیده درآمده است. الگوریتم‌های پیشرفته قادرند بر اساس داده‌های ورودی، تجربه‌های قبلی و تعاملات محیطی، تصمیماتی اتخاذ کنند که حتی برای طراحان اولیه سیستم نیز قابل پیش‌بینی دقیق نیست. در نتیجه، فاصله‌ای میان کنترل اولیه انسانی و خروجی نهایی سیستم شکل می‌گیرد که در ادبیات نظری از آن به عنوان شکاف مسئولیت یاد می‌شود. این شکاف پیامدهای مهمی برای حقوق بین‌الملل دارد. نخست آنکه، معیارهای سنتی انتساب رفتار، مانند کنترل مؤثر یا کنترل کلی، ممکن است در بسیاری از موارد نتوانند رابطه حقوقی کافی میان دولت و رفتار زیان‌بار را به‌طور دقیق تبیین کنند. دوم آنکه، افزایش استقلال فناوریانه می‌تواند منجر به وضعیت‌هایی شود که در آن، هیچ عامل انسانی به‌طور مستقیم مسئول تصمیم نهایی نیست، در حالی که پیامدهای آن در سطح بین‌المللی قابل توجه و گاه فرامرزی است. نظریه شکاف مسئولیت نه تنها یک تحلیل فنی، بلکه یک چالش هنجاری برای نظام حقوق بین‌الملل محسوب می‌شود. این نظریه نشان می‌دهد که ادامه اتکای صرف بر مفاهیم سنتی انتساب و کنترل، ممکن است به ناکارآمدی نظام مسئولیت بین‌المللی در مواجهه با فناوری‌های نوین منجر شود. در نتیجه، ضرورت بازاندیشی در مفاهیم بنیادین مسئولیت، از جمله رابطه علیت حقوقی، سطح کنترل قابل قبول و معیارهای پیش‌بینی‌پذیری رفتار، بیش از پیش احساس می‌شود. نظریه استقلال فناوریانه و شکاف مسئولیت بر این نکته تأکید دارد که حقوق بین‌الملل در حال ورود به مرحله‌ای است که در آن، باید میان واقعیت‌های پیچیده فناوری و ساختارهای سنتی حقوقی تعادل جدیدی برقرار شود. این امر مستلزم توسعه رویکردهای ترکیبی، انعطاف‌پذیر و آینده‌نگر در تفسیر قواعد مسئولیت بین‌المللی دولت‌ها است تا از یک‌سو خلأهای حقوقی ناشی از فناوری‌های خودمختار جبران شود و از سوی دیگر، اصول بنیادین حقوق بین‌الملل حفظ گردد.



بخش چهارم: تحلیل و تطبیق نظریه‌ها با مسئولیت بین‌المللی دولت‌ها در فضای سایبری

ترکیب نظریه‌های کلاسیک مسئولیت بین‌المللی دولت‌ها با نظریه‌های نوین حکمرانی فناوری نشان می‌دهد که نظام حقوق بین‌الملل در مواجهه با سامانه‌های هوش مصنوعی خودمختار در مرحله گذار مفهومی قرار دارد. از یک سو، چارچوب‌های سنتی همچنان بر اصول انتساب، کنترل و نقض تعهد استوار هستند و از سوی دیگر، واقعیت‌های فناوری‌های نوین، این اصول را با چالش‌های بنیادین مواجه ساخته‌اند. در سطح نخست، نظریه‌های کلاسیک مانند نظریه انتساب ارگانیکی و کنترل مؤثر، همچنان مبنای اصلی تشخیص مسئولیت دولت‌ها محسوب می‌شوند. با این حال، این نظریه‌ها در مواجهه با سامانه‌های خودمختار که دارای قابلیت تصمیم‌گیری مستقل هستند، با محدودیت‌های جدی مواجه‌اند. زیرا عنصر «اراده انسانی قابل شناسایی» در بسیاری از موارد تضعیف می‌شود. این امر موجب می‌شود که فرآیند انتساب رفتار در فضای سایبری پیچیده‌تر و غیرخطی‌تر از الگوهای سنتی باشد. در سطح دوم، نظریه‌های مبتنی بر خطر و مسئولیت عینی، تلاش می‌کنند این خلأ را از طریق تمرکز بر «نتیجه» به جای «رفتار» جبران نمایند. در این چارچوب، دولت‌ها حتی در صورت عدم کنترل مستقیم بر تصمیمات سامانه‌های هوش مصنوعی، ممکن است به دلیل ایجاد یا بهره‌برداری از یک وضعیت پرخطر، مسئول شناخته شوند. این رویکرد به‌ویژه در فضای سایبری که پیامدهای فرامرزی و غیرقابل پیش‌بینی دارد، اهمیت مضاعف پیدا می‌کند. در سطح سوم، نظریه‌های حکمرانی الگوریتمی و شکاف مسئولیت فناورانه نشان می‌دهند که حقوق بین‌الملل باید با یک واقعیت جدید مواجه شود: تصمیم‌گیری حقوقی در بسیاری از موارد دیگر محصول اراده مستقیم انسانی نیست، بلکه نتیجه تعامل پیچیده میان انسان، داده و ماشین است. این امر موجب می‌شود که مفهوم سنتی «کنترل» نیازمند بازتعریف در قالب کنترل ساختاری، طراحی محور یا نظارت پسینی باشد. تطبیق این نظریه‌ها بیانگر آن است که نظام مسئولیت بین‌المللی دولت‌ها نمی‌تواند صرفاً بر قواعد کلاسیک اتکا کند، بلکه نیازمند توسعه تفسیری و هنجاری است تا بتواند با پدیده‌های نوینی



مانند هوش مصنوعی خودمختار سازگار شود. این تحول نه به معنای کنارگذاری قواعد سنتی، بلکه به معنای تکامل تدریجی آن‌ها در پاسخ به واقعیت‌های فناوری معاصر است.

نتیجه‌گیری

پژوهش حاضر با هدف تحلیل مسئولیت بین‌المللی دولت‌ها در قبال تصمیمات اتخاذشده توسط سامانه‌های هوش مصنوعی خودمختار در فضای سایبری، نشان داد که نظام حقوق بین‌الملل با یک تحول ساختاری و مفهومی مواجه است که در آن، مبانی سنتی مسئولیت به‌تنهایی پاسخگوی پیچیدگی‌های فناوری‌های نوین نیست. در چارچوب سنتی حقوق بین‌الملل، مسئولیت دولت‌ها بر دو رکن اساسی «انتساب رفتار» و «نقض تعهد بین‌المللی» استوار است. این ساختار که در پیش‌نویس مواد کمیسیون حقوق بین‌الملل نیز تثبیت شده، مبتنی بر فرض وجود یک رابطه نسبتاً مستقیم میان اراده انسانی و نتیجه متخلفانه است. با این حال، ورود سامانه‌های هوش مصنوعی خودمختار به عرصه تصمیم‌گیری سایبری این رابطه خطی را دچار گسست کرده و الگوهای جدیدی از کنش حقوقی را ایجاد نموده است. یافته‌های پژوهش نشان می‌دهد که نظریه‌های کلاسیک انتساب، از جمله انتساب ارگانیکی، کنترل مؤثر و کنترل کلی، همچنان نقش بنیادین در تحلیل مسئولیت دارند، اما در مواجهه با سامانه‌های یادگیرنده و خودمختار، با محدودیت‌های تفسیری و عملی روبه‌رو می‌شوند. این محدودیت‌ها ناشی از آن است که در بسیاری از موارد، تصمیم‌نهایی سامانه‌های هوش مصنوعی نتیجه فرآیندهای پیچیده محاسباتی و داده‌محور است که امکان پیش‌بینی دقیق یا کنترل لحظه‌ای انسانی بر آن وجود ندارد. در نتیجه، مفهوم سنتی «کنترل مستقیم» در برخی سناریوهای سایبری کارایی کامل خود را از دست می‌دهد. نظریه‌های نوین مانند مسئولیت مبتنی بر خطر، مسئولیت عینی و حکمرانی الگوریتمی، تلاش می‌کنند این خلأ را از طریق تمرکز بر نتیجه و ریسک قابل پیش‌بینی جبران نمایند. این نظریه‌ها نشان می‌دهند که مسئولیت دولت‌ها می‌تواند نه صرفاً بر مبنای انتساب مستقیم رفتار، بلکه بر اساس نقش آن‌ها در طراحی، استقرار، بهره‌برداری و مدیریت سامانه‌های



بر خطر نیز شکل گیرد. با این حال، توسعه بی ضابطه این رویکردها نیز می‌تواند به گسترش بیش از حد مسئولیت و تضعیف اصل قطعیت حقوقی منجر شود. تحلیل نظریه‌هایی مانند «انسان در حلقه تصمیم» و «شکاف مسئولیت فناورانه» بیانگر آن است که حضور انسان در فرآیندهای تصمیم‌گیری الگوریتمی، در بسیاری از موارد به سطحی صوری یا پسینی تنزل یافته و نمی‌تواند به‌طور کامل زنجیره انتساب را تضمین کند. این وضعیت نشان‌دهنده ظهور یک شکاف ساختاری میان فناوری و حقوق است که در آن، ابزارهای سنتی تحلیل حقوقی قادر به پوشش کامل پیچیدگی‌های فناوری‌های خودمختار نیستند. پژوهش به این نتیجه می‌رسد که نظام مسئولیت بین‌المللی دولت‌ها در حال گذار از یک الگوی تک‌بعدی مبتنی بر انتساب مستقیم به سوی یک الگوی چندلایه و ترکیبی است. در این الگو، مفاهیمی همچون کنترل ساختاری، مدیریت ریسک، نظارت پیشینی و پسینی، و مسئولیت ناشی از بهره‌برداری از فناوری‌های پرخطر نقش مکمل در کنار قواعد سنتی ایفا می‌کنند. بنابراین، آینده حقوق بین‌الملل در حوزه مسئولیت دولت‌ها نه در کنارگذاری اصول کلاسیک، بلکه در بازتفسیر تدریجی و انطباق‌پذیر آن‌ها با واقعیت‌های فناوری‌های نوین سایبری و هوش مصنوعی قابل تصور است. این تحول، ضرورت توسعه رویکردهای میان‌رشته‌ای و تدوین استانداردهای نوین بین‌المللی را بیش از پیش آشکار می‌سازد.

• پیشنهادات

۱. بازتفسیر قواعد انتساب در حقوق بین‌الملل: پیشنهاد می‌شود کمیسیون حقوق بین‌الملل در تفسیر مواد مسئولیت دولت‌ها، مفهوم انتساب را به گونه‌ای توسعه دهد که شامل اشکال نوین کنترل ساختاری بر سامانه‌های هوش مصنوعی نیز باشد.
۲. تدوین رژیم خاص برای مسئولیت سایبری مبتنی بر هوش مصنوعی: با توجه به ویژگی‌های خاص فضای سایبری، لازم است یک چارچوب حقوقی ویژه برای مسئولیت ناشی از اقدامات خودکار و الگوریتمی تدوین شود.



۳. تقویت استانداردهای «مراقبت مقتضی» در استفاده از هوش مصنوعی: دولت‌ها باید به تعهدات سخت‌گیرانه‌تری در زمینه طراحی، نظارت و به‌کارگیری سامانه‌های هوش مصنوعی پایبند باشند تا از بروز خسارات فرامرزی جلوگیری شود.
۴. ایجاد نظام مشترک بین‌المللی نظارت بر هوش مصنوعی خودمختار: تشکیل نهادهای نظارتی بین‌المللی می‌تواند به کاهش شکاف مسئولیت و افزایش شفافیت در استفاده از فناوری‌های سایبری کمک کند.
۵. توسعه پژوهش‌های میان‌رشته‌ای: برای درک بهتر مسئولیت در عصر هوش مصنوعی، لازم است مطالعات حقوقی با علوم کامپیوتر، امنیت سایبری و اخلاق فناوری تلفیق شوند تا چارچوب‌های جامع‌تری ایجاد گردد.



منابع و مآخذ

الف: منابع فارسی

۱. بیگدلی، محمدرضا. حقوق بین‌الملل عمومی. تهران: گنج دانش.
۲. بیگدلی، سمیرا. حقوق بین‌الملل در فضای سایبر. تهران: سمت، ۱۴۰۱.
۳. قائم‌مقامی، محمود. مسئولیت بین‌المللی دولت‌ها در حقوق بین‌الملل. تهران: جنگل.
۴. عباسعلی زارعی. حقوق بین‌الملل معاصر. تهران: میزان.
۵. محمدعلی موحد. حقوق بین‌الملل عمومی. تهران: نشر خرسندی.
۶. سید حسین صفایی. کلیات حقوق بین‌الملل عمومی. تهران: دانشگاه تهران.
۷. عبدالحسین شیروی. حقوق تجارت بین‌الملل. تهران: سمت.
۸. ناصر کاتوزیان. مقدمه علم حقوق (برای مباحث نظری مسئولیت). تهران: بهنشر.
۹. محمدجواد ظریف. اصول و مبانی حقوق بین‌الملل عمومی. تهران: اطلاعات.
۱۰. حسن حبیبی. حقوق بین‌الملل عمومی و سازمان‌های بین‌المللی. تهران: سمت.
۱۱. محمدرضا ظفری. بررسی مسئولیت بین‌المللی دولت‌ها در حقوق معاصر. فصلنامه پژوهش حقوق عمومی.
۱۲. علی‌اکبر داور. انتساب رفتار در حقوق بین‌الملل. مجله حقوقی دادگستر.
۱۳. فاطمه هاشمی. حقوق سایبری و چالش‌های حاکمیتی. فصلنامه مطالعات حقوق فناوری.
۱۴. رضا اسلامی. مسئولیت دولت‌ها در فضای مجازی. مجله حقوقی بین‌المللی.
۱۵. مهدی چمران. تحلیل حقوقی حملات سایبری در حقوق بین‌الملل. مجله سیاست خارجی.
۱۶. سارا احمدی. هوش مصنوعی و چالش‌های حقوقی نوین. فصلنامه حقوق فناوری اطلاعات.
۱۷. محمدرضا صادقی. انتساب رفتار در فضای سایبری. پژوهشنامه حقوق بین‌الملل.

ب: منابع لاتین

۱۸. Crawford, James. State Responsibility: The General Part. Cambridge University Press, ۲۰۱۳.
۱۹. Crawford, James; Pellet, Alain; Olleson, Simon. The Law of International Responsibility. Oxford University Press, ۲۰۱۰.
۲۰. Schmitt, Michael N. Tallinn Manual ۲.۰ on the International Law Applicable to Cyber Operations. Cambridge University Press, ۲۰۱۷.
۲۱. Delerue, François. Cyber Operations and International Law. Cambridge University Press, ۲۰۲۰.
۲۲. Schmitt, Michael N. Autonomous Cyber Capabilities and International Law. International Law Studies, ۲۰۲۰.
۲۳. Tsagourias, Nicholas; Buchan, Russell. Research Handbook on International Law and Cyberspace. Edward Elgar Publishing, ۲۰۲۱.
۲۴. Moynihan, Harriet. The Application of International Law to Cyberattacks. Chatham House Research Paper, ۲۰۱۹.
۲۵. Crootof, Rebecca. International Cybertorts: Expanding State Accountability in Cyberspace. Cornell Law Review, ۲۰۲۰.
۲۶. Schmitt, Michael N.; Shany, Yuval. An International Attribution Mechanism for Hostile Cyber Operations? International Law Studies, ۲۰۲۰.
۲۷. Daskal, Jennifer. The Un-Territoriality of Data. Yale Law Journal, ۲۰۱۸.