

مسئولیت حقوقی هوش مصنوعی و نظارت الگوریتمی با حاکمیت داده و دیپلماسی اقتصادی در نظم چندقطبی

سامان مرادی پور

دانشجوی دکتری تخصصی حقوق خصوصی، دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران.

Saman7500@gmail.com

چکیده

ظهور سریع هوش مصنوعی به‌عنوان یک فناوری عمومی و شکل‌گیری نظم جهانی چندقطبی، چالش‌های بی‌سابقه‌ای را در حوزه مسئولیت حقوقی، نظارت الگوریتمی، حاکمیت داده و دیپلماسی اقتصادی پدید آورده است. این مقاله با رویکردی بین‌رشته‌ای و بهره‌گیری از روش تحلیل محتوای کیفی، به بررسی تعامل پیچیده میان این چهار حوزه در فضای ژئوپلیتیک معاصر می‌پردازد. یافته‌های پژوهش نشان می‌دهد که نظام‌های حقوقی سنتی مبتنی بر تقصیر و مسئولیت محصول، در مواجهه با ویژگی‌های خاص سیستم‌های هوش مصنوعی از جمله کدیری، پیچیدگی و خودمختاری ناکارآمد هستند. سه مدل رگولاتوری متمایز در سطح جهانی شکل گرفته است: رویکرد حقوق محور اتحادیه اروپا، رویکرد نوآوری محور ایالات متحده و رویکرد کنترل دولتی چین. هم‌زمان، حاکمیت داده به ابزاری کلیدی در رقابت ژئوپلیتیک تبدیل شده و دیپلماسی اقتصادی به عرصه‌ای برای تعارض و همکاری میان قدرت‌های بزرگ بدل گشته است. مقاله استدلال می‌کند که فقدان هماهنگی بین‌المللی در زمینه مسئولیت هوش مصنوعی، خطر ایجاد خلأهای مسئولیت‌پذیری و تضعیف اعتماد عمومی را به همراه دارد و پیشنهاد می‌کند که نهادهای چندجانبه مانند گفتگوی جهانی هوش مصنوعی سازمان ملل متحد می‌توانند بستری برای همگرایی تدریجی فراهم آورند.

کلیدواژه‌ها: مسئولیت حقوقی هوش مصنوعی، نظارت الگوریتمی، حاکمیت داده، دیپلماسی اقتصادی، نظم چندقطبی

مقدمه

هوش مصنوعی در دهه گذشته از یک حوزه پژوهشی تخصصی به نیروی محوری در بازساخت اقتصاد جهانی، روابط بین‌الملل و ساختارهای قدرت تبدیل شده است. این فناوری نه تنها شیوه تولید، توزیع و مصرف را دگرگون ساخته، بلکه پرسش‌های بنیادینی را درباره مسئولیت حقوقی، مشروعیت نظارتی و عدالت توزیعی برانگیخته است. آنچه این تحول را پیچیده‌تر می‌سازد، هم‌زمانی آن با شکل‌گیری نظم جهانی چندقطبی است؛ نظامی که در آن قدرت‌های بزرگ رقابت فزاینده‌ای برای تعیین قواعد بازی در حوزه فناوری‌های نوظهور دارند (Gundani, ۲۰۲۵).

فناوری هوش مصنوعی امروز در مرکز منازعه راهبردی جهانی قرار گرفته و visions رقیب از حکمرانی، نوآوری و ارزش‌ها در حال شکل‌گیری است. تکه‌تکه شدن حکمرانی منجر به شکاف‌هایی در مسئولیت‌پذیری برای سوگیری الگوریتمی، خطرات حریم خصوصی و گسترش کاربردهای مضر از جمله اطلاعات نادرست و تبعیض شده است (TDGI, ۲۰۲۵). این وضعیت یک پارادوکس حکمرانی ایجاد کرده است: دولت‌ها چگونه می‌توانند کنترل حاکمیتی بر سیستم‌های هوش مصنوعی اعمال کنند در حالی که در یک اکوسیستم جهانی به‌هم‌پیوسته که مستلزم همکاری فراملی است، فعالیت می‌کنند؟ (Springer, ۲۰۲۴).

هدف این مقاله بررسی تعامل میان چهار حوزه به‌هم‌پیوسته است: مسئولیت حقوقی هوش مصنوعی، نظارت الگوریتمی، حاکمیت داده و دیپلماسی اقتصادی در چارچوب نظم چندقطبی. پرسش اصلی پژوهش این است که چگونه می‌توان یک چارچوب منسجم برای مسئولیت‌پذیری هوش مصنوعی طراحی کرد که هم‌زمان با الزامات حاکمیت داده، پویایی‌های ژئوپلیتیک و ضرورت‌های همکاری بین‌المللی سازگار باشد. برای پاسخ به این پرسش، مقاله در پنج بخش سازماندهی شده است. بخش دوم به مرور ادبیات و مبانی نظری می‌پردازد. بخش سوم روش‌شناسی پژوهش را تشریح می‌کند. بخش چهارم یافته‌های پژوهش را در قالب چهار محور اصلی ارائه می‌دهد. بخش پنجم به بحث و تفسیر یافته‌ها اختصاص دارد و نهایتاً نتیجه‌گیری و پیشنهادها را سیاستی ارائه می‌شود.

مبانی نظری و مرور ادبیات

چارچوب مفهومی مسئولیت حقوقی هوش مصنوعی

مسئولیت حقوقی در زمینه هوش مصنوعی را می‌توان در سه سطح متمایز تحلیل کرد: مسئولیت مدنی (شامل مسئولیت مبتنی بر تقصیر و مسئولیت محصول)، مسئولیت کیفری و مسئولیت اداری-نظارتی. رویکرد سنتی حقوقی که بر مفاهیمی مانند تقصیر، رابطه سببیت و خسارت قابل جبران استوار است، در مواجهه با سیستم‌های هوش مصنوعی با چالش‌های اساسی روبه‌رو می‌شود (Parliament European, ۲۰۲۵a).

ویژگی‌های خاص سیستم‌های هوش مصنوعی — از جمله کدیری الگوریتمی (دشواری درک فرآیندهای تصمیم‌گیری)، پیچیدگی شبکه‌ای (تعاملات غیرقابل پیش‌بینی میان اجزا) و خودمختاری نسبی (توانایی عمل بدون مداخله مستقیم انسانی) — مفاهیم

سنتی تقصیر و رابطه سببیت را با بحران مواجه می‌سازد. کمیسیون اروپا در پاسخ به این چالش‌ها، پیشنهاد یک دستورالعمل مسئولیت هوش مصنوعی را ارائه کرد که هدف آن مدرن‌سازی قواعد مسئولیت مبتنی بر تقصیر با در نظر گرفتن ویژگی‌های منحصر به فرد هوش مصنوعی بود (Parliament European, ۲۰۲۵b). با این حال، این پیشنهاد در فوریه ۲۰۲۵ به دلیل عدم توافق میان نهادهای قانون‌گذاری اتحادیه اروپا پس گرفته شد (al et Tujjar, ۲۰۲۶).

نظریه‌های حکمرانی الگوریتمی

حکمرانی الگوریتمی به مجموعه‌ای از سازوکارها، نهادها و رویه‌هایی اشاره دارد که هدف آن‌ها هدایت، نظارت و پاسخگو ساختن سیستم‌های الگوریتمی است. در ادبیات علمی، سه رویکرد نظری اصلی در این زمینه قابل شناسایی است:

رویکرد حقوق‌محور که بر حقوق بنیادین، شفافیت و پاسخگویی تأکید دارد و در چارچوب آن، قانون هوش مصنوعی اتحادیه اروپا به‌عنوان پیشروترین نمونه جهانی شناخته می‌شود. این رویکرد سیستمی مبتنی بر ریسک ایجاد کرده که سیستم‌های هوش مصنوعی را به چهار سطح ریسک غیرقابل قبول (ممنوع)، پرخطر (با الزامات سختگیرانه)، ریسک محدود (با الزامات شفافیت) و ریسک حداقل (بدون الزام) طبقه‌بندی می‌کند (Commission European, ۲۰۲۴).

رویکرد بازارمحور که در ایالات متحده دنبال می‌شود و اولویت را به نوآوری و رقابت‌پذیری اقتصادی می‌دهد. در ژانویه ۲۰۲۵، دولت ترامپ با امضای یک فرمان اجرایی، حفاظت‌های قبلی را لغو کرد تا توسعه بدون محدودیت هوش مصنوعی را در اولویت قرار دهد (CACM, ۲۰۲۶). این رویکرد بر این فرض استوار است که مقررات سختگیرانه می‌تواند موقعیت رهبری فناوری آمریکا را تضعیف کند.

رویکرد دولتی-هدایتی که در چین اتخاذ شده و ترکیبی از توسعه سریع تجاری با کنترل دولتی دقیق است. چین سیستم ثبت اجباری الگوریتم‌های مولد را پیاده‌سازی کرده و بیش از ۳۵۰ الگوریتم هوش مصنوعی مولد را ثبت کرده است. همچنین تمام محتوای تولیدشده توسط هوش مصنوعی باید برچسب‌گذاری شود (CACM, ۲۰۲۶).

حاکمیت داده به‌عنوان ابزار ژئوپلیتیک

حاکمیت داده به توانایی دولت‌ها و نهادها برای کنترل، مدیریت و حکمرانی بر جریان‌های داده اشاره دارد. در نظم چندقطبی معاصر، حاکمیت داده از یک مفهوم صرفاً فنی به ابزاری محوری در رقابت ژئوپلیتیک تبدیل شده است. استراتژی اتحادیه اروپا برای اتحادیه داده، که در نوامبر ۲۰۲۵ منتشر شد، صراحتاً بر ضرورت حفاظت از حاکمیت داده اروپا تأکید می‌کند و اقدامات کلیدی از جمله دستورالعمل‌هایی برای ارزیابی رفتار منصفانه با داده‌های اروپایی در خارج از کشور و جعبه‌ابزاری برای مقابله با بومی‌سازی غیرموجه داده را پیشنهاد می‌کند (Commission European, ۲۰۲۵a).

در سطح بین‌المللی، توافقنامه‌های تجارت دیجیتال به عرصه اصلی تعارض و همکاری در حوزه حاکمیت داده تبدیل شده‌اند. مطالعه‌ای در مؤسسه اقتصاد بین‌المللی کره نشان می‌دهد که توافقنامه‌های تجارت دیجیتال در سه مدل متمایز آمریکایی، اروپایی و چینی شکل گرفته‌اند که هر یک رویکرد متفاوتی به جریان‌های فرامرزی داده، ممنوعیت بومی‌سازی داده و حفاظت از کد منبع دارند (Kang, ۲۰۲۵). مدل آمریکایی (مانند USMCA) معمولاً مقررات استاندارد بالا و باز در زمینه جریان‌های

فرامرزی داده را در فصل اختصاصی تجارت دیجیتال قرار می‌دهد، در حالی که مدل اروپایی این موضوعات را در چارچوب خدمات ادغام می‌کند و مدل چینی (مانند RCEP) رویکرد محافظه‌کارانه‌تری اتخاذ می‌کند.

روش‌شناسی پژوهش

این پژوهش از روش تحلیل محتوای کیفی با رویکرد تطبیقی بهره می‌گیرد. داده‌های پژوهش از سه دسته منابع گردآوری شده‌اند: نخست، اسناد حقوقی و سیاست‌گذاری رسمی شامل قانون هوش مصنوعی اتحادیه اروپا، دستورالعمل پیشنهادی مسئولیت هوش مصنوعی، قانون پاسخگویی الگوریتمی ایالات متحده و مقررات چین در زمینه هوش مصنوعی؛ دوم، گزارش‌های نهادهای بین‌المللی شامل سازمان ملل متحد، صندوق بین‌المللی پول، سازمان همکاری اقتصادی و توسعه و بانک جهانی؛ و سوم، مقالات علمی داوری‌شده منتشرشده در بازه زمانی ۲۰۲۰ تا ۲۰۲۶.

تحلیل داده‌ها در سه مرحله انجام شده است. در مرحله نخست، اسناد و متون گردآوری‌شده کدگذاری باز شدند و مفاهیم کلیدی استخراج گردید. در مرحله دوم، مفاهیم در قالب مقوله‌های اصلی سازماندهی شدند که عبارتند از: مدل‌های مسئولیت حقوقی، سازوکارهای نظارت الگوریتمی، رژیم‌های حاکمیت داده و استراتژی‌های دیپلماسی اقتصادی. در مرحله سوم، روابط میان مقوله‌ها در چارچوب نظم چندقطبی تحلیل و تفسیر شد.

حجم نمونه شامل ۲۸ منبع علمی و رسمی است که تمامی آن‌ها در بازه زمانی پنج سال اخیر (۲۰۲۰-۲۰۲۶) منتشر شده‌اند. معیارهای انتخاب منابع شامل اعتبار ناشر، به‌روز بودن، ارتباط مستقیم با موضوع پژوهش و تنوع جغرافیایی (پوشش اروپا، آمریکای شمالی، آسیا و سازمان‌های بین‌المللی) بوده است.

یافته‌های پژوهش

مسئولیت حقوقی هوش مصنوعی: از تقصیر تا بیمه دولتی

تحلیل اسناد حقوقی نشان می‌دهد که نظام‌های سنتی مسئولیت در مواجهه با هوش مصنوعی با سه چالش اساسی روبه‌رو هستند. نخست، چالش اثبات تقصیر: در سیستم‌هایی که تصمیم‌گیری به‌صورت توزیع‌شده میان توسعه‌دهنده، مستقرکننده و خود سیستم انجام می‌شود، انتساب تقصیر به یک عامل مشخص دشوار است (Parliament European, ۲۰۲۵b). دوم، چالش رابطه سببیت: ویژگی کدری الگوریتمی اثبات رابطه علت و معلولی میان رفتار سیستم و خسارت وارده را پیچیده می‌سازد. سوم، چالش جبران خسارت: حجم و ماهیت خسارات ناشی از هوش مصنوعی می‌تواند فراتر از ظرفیت سیستم‌های سنتی بیمه و جبران خسارت باشد.

در پاسخ به این چالش‌ها، مدل‌های نوآورانه‌ای در ادبیات علمی پیشنهاد شده است. Tran (۲۰۲۵) یک طرح جبران خسارت بدون تقصیر با پشتیبانی دولتی را پیشنهاد می‌کند که بر اساس مدل برنامه جبران آسیب واکسن طراحی شده است. این رویکرد

استدلال می‌کند که از آنجا که دولت در حکمرانی جعبه‌های شنی نظارتی نقش فعال دارد، به‌عنوان یک عامل هم‌مسئول شناخته می‌شود و بنابراین مسئولیت مشترک در موارد بروز خسارت توجیه‌پذیر است. چارچوب پیشنهادی Tran مزایای متعددی دارد: کاهش موانع برای شرکت‌های کوچک و متوسط، غلبه بر چالش‌های انتساب ناشی از سیستم‌های کدر، و تقویت اعتماد عمومی به رژیم‌های نظارتی آزمایشی.

در سطح اتحادیه اروپا، دستورالعمل مسئولیت هوش مصنوعی که در سال ۲۰۲۲ پیشنهاد شده بود، در فوریه ۲۰۲۵ پس گرفته شد. کمیته بازار داخلی و حمایت از مصرف‌کنندگان پارلمان اروپا در ماه مه ۲۰۲۵ توصیه کرد که این دستورالعمل رد شود، با این استدلال که الزامات سختگیرانه‌تر موجود در قانون هوش مصنوعی و دستورالعمل بازنگری‌شده مسئولیت محصول، نیاز به یک رژیم مسئولیت جداگانه را منتفی می‌سازد (CIL, ۲۰۲۵). با این حال، منتقدان استدلال می‌کنند که این تصمیم خلأهایی را در زمینه مسئولیت برای سیستم‌های هوش مصنوعی پرخطر باقی می‌گذارد (al et Tuijjar, ۲۰۲۶).

نظارت الگوریتمی و ممیزی هوش مصنوعی

نظارت الگوریتمی به‌عنوان مکانیزم کلیدی برای تضمین پاسخگویی سیستم‌های هوش مصنوعی شناخته می‌شود. ممیزی هوش مصنوعی، که به‌عنوان ارزیابی سیستماتیک یک سیستم، توسعه و رفتار آن نسبت به مجموعه‌ای از معیارهای از پیش تعیین‌شده تعریف می‌شود، می‌تواند اشکال مختلفی داشته باشد: ارزیابی ریسک پیش از استقرار، نظارت مستمر و آزمون انطباق (Cen & Alur, ۲۰۲۴).

پرسش محوری در ادبیات ممیزی الگوریتمی این است که چه سطحی از دسترسی به سیستم برای انجام یک ممیزی معنادار لازم است. Cen و Alur (۲۰۲۴) استدلال می‌کنند که حداقل دسترسی جعبه‌سیاه—یعنی دسترسی پرس‌وجو به مدل بدون افشای پیاده‌سازی داخلی آن—باید به میزان اعطا شود. آن‌ها **ДОВОД** می‌کنند که دسترسی جعبه‌سیاه تعادل مؤثری میان نگرانی‌های مربوط به فناوری اختصاصی، حریم خصوصی داده، استانداردسازی ممیزی و کارایی ممیزی برقرار می‌کند. با این حال، پژوهش‌های دیگر نشان می‌دهند که دسترسی جعبه‌سیاه برای ممیزی‌های دقیق کافی نیست. مطالعات انجام‌شده در کنفرانس ACM ۲۰۲۴ در زمینه انصاف، پاسخگویی و شفافیت استدلال می‌کنند که دسترسی جعبه‌سفید به کارکردهای داخلی سیستم (مانند وزن‌ها، فعال‌سازی‌ها و گرادین‌ها) به ممیز اجازه می‌دهد حملات قوی‌تری انجام دهد، مدل‌ها را عمیق‌تر تفسیر کند و تنظیم دقیق انجام دهد (MIT, ۲۰۲۴). جدول ۱ سطوح مختلف دسترسی ممیزی را نشان می‌دهد.

جدول ۱: سطوح دسترسی در ممیزی الگوریتمی

سطح دسترسی	آنچه قابل دسترسی است	انواع ممیزی ممکن	نمونه موردی
دسترسی فرآیندی	چارچوب‌ها، چک‌لیست‌ها، کارت‌های مدل، گزارش‌های فنی	ممیزی اسنادی	ممیزی الگوریتم AMS اتریش
دسترسی مدل (جعبه‌سیاه)	مدل پیش‌بین با داده مصنوعی	حملات خصمانه، انصاف خصمانه	ممیزی Diffusion Stable بلومبرگ

دسترسی ورودی	مدل پیش‌بین و داده‌های آموزشی	توضیحات جانشین، داده مصنوعی	ممیزی نرم‌افزار غربالگری پی‌متریکس
دسترسی نتیجه (جعبه خاکستری)	مدل، داده آموزشی و نتایج واقعی	تحلیل رانش مفهومی، حملات وارونگی	تحقیق ProPublica در مورد COMPAS
دسترسی جعبه سفید	کل معماری و اسناد	ممیزی‌های تجربی، مداخلات	ممیزی سیستم رفاه روتردام

منبع: اقتباس از Springer (۲۰۲۴)

حاکمیت داده در نظم چندقطبی

حاکمیت داده در نظم چندقطبی معاصر به عرصه‌ای برای تعارض و همکاری میان قدرت‌های بزرگ تبدیل شده است. تحلیل اسناد نشان می‌دهد که سه رویکرد متمایز در این حوزه شکل گرفته است: رویکرد حفاظت از حریم خصوصی و حقوق بنیادین اتحادیه اروپا، رویکرد جریان آزاد داده با تأکید بر رقابت اقتصادی ایالات متحده، و رویکرد کنترل دولتی و امنیت ملی چین (Kang, ۲۰۲۵).

اتحادیه اروپا در استراتژی اتحادیه داده خود، که در نوامبر ۲۰۲۵ منتشر شد، سه اولویت اصلی را تعیین کرده است: نیازهای داده برای نوآوری، گزارش‌دهی خودکار داده برای انطباق نظارتی و ابعاد بین‌المللی اقتصاد داده (European Commission, ۲۰۲۵b). این استراتژی صراحتاً بر حفاظت از حاکمیت داده اروپا تأکید دارد و ابزارهایی برای مقابله با بومی‌سازی غیرموجه داده و نشت داده پیشنهاد می‌کند.

در سطح فرآتلانتیک، چارچوب حریم خصوصی داده اتحادیه اروپا-آمریکا (DPF) به‌عنوان جانشین توافقنامه‌های Safe Harbour و Shield Privacy در سال ۲۰۲۳ معرفی شد. در سپتامبر ۲۰۲۵، دادگاه عمومی اتحادیه اروپا در پرونده Latombe علیه کمیسیون، اعتبار این چارچوب را تأیید کرد (Freshfields, ۲۰۲۵). این تصمیم ثبات را برای جریان‌های داده فرآتلانتیک بازگرداند، هرچند همچنان با چالش‌های حقوقی بالقوه در آینده روبه‌روست.

در قاره آفریقا، اتحادیه آفریقا در دسامبر ۲۰۲۵ فرآیند اعتبارسنجی چارچوب‌های حاکمیت داده را آغاز کرد تا بازار دیجیتال واحد آفریقا را تا سال ۲۰۳۰ تسریع کند. چارچوب جریان‌های داده فرامرزی، مکانیزم‌های اعتماد مشارکتی را پیشنهاد می‌کند که امکان حرکت امن و یکپارچه داده میان کشورهای عضو را فراهم می‌سازد (AU, ۲۰۲۵).

دیپلماسی اقتصادی و رقابت ژئوپلیتیک در حکمرانی هوش مصنوعی

حکمرانی هوش مصنوعی به یکی از محورهای اصلی دیپلماسی اقتصادی در نظم چندقطبی تبدیل شده است. تحلیل مواضع قدرت‌های بزرگ نشان می‌دهد که رقابت برای تعیین قواعد بازی در این حوزه شدت یافته است.

چین در نشست رهبران APEC در نوامبر ۲۰۲۵، پیشنهاد ایجاد یک سازمان همکاری جهانی هوش مصنوعی را مطرح کرد که هدف آن تعیین قواعد حکمرانی و تقویت همکاری بین‌المللی است. رئیس‌جمهور شی جین پینگ، هوش مصنوعی را "کالای عمومی برای جامعه بین‌المللی" توصیف کرد و بر ضرورت تضمین بهره‌مندی همه کشورها و مناطق از این فناوری تأکید کرد (Newsmax, ۲۰۲۵). این پیشنهاد در حالی مطرح شد که ایالات متحده تلاش‌ها برای تنظیم هوش مصنوعی در نهادهای بین‌المللی را رد کرده است.

در سطح سازمان ملل متحد، گفتگوی جهانی حکمرانی هوش مصنوعی در سپتامبر ۲۰۲۵ در نیویورک راه‌اندازی شد. آنتونیو گوترش، دبیرکل سازمان ملل متحد، این رویداد را "سنگ‌بنای یک اکوسیستم جهانی هوش مصنوعی" توصیف کرد که بر سه ستون بنیادین استوار است: سیاست، علم و ظرفیت‌سازی (UN, ۲۰۲۵). پنل علمی مستقل بین‌المللی هوش مصنوعی، متشکل از ۴۰ کارشناس از مناطق و رشته‌های مختلف، به‌عنوان "سیستم هشدار اولیه جهانی" عمل خواهد کرد.

در چارچوب گروه ۲۰، کارگروه هوش مصنوعی در سپتامبر ۲۰۲۵ سندی را منتشر کرد که بر توسعه اخلاقی و امن هوش مصنوعی با تکیه بر حاکمیت داده قوی تأکید دارد (G۲۰, ۲۰۲۵). هم‌زمان، بریکس پلاس در بیانیه مشترک خود در آوریل ۲۰۲۵، بر ضرورت حکمرانی بین‌المللی فراگیر برای هوش مصنوعی و توجه ویژه به نیازهای کشورهای جنوب جهانی تأکید کرد (CIL, ۲۰۲۵).

بحث و تفسیر

تعارض مدل‌های حکمرانی و پیامدهای آن

یافته‌های این پژوهش نشان می‌دهد که جهان در آستانه شکل‌گیری سه مدل متمایز حکمرانی هوش مصنوعی است که هر یک مبتنی بر ارزش‌ها، اولویت‌ها و ساختارهای نهادی متفاوتی هستند. مدل اروپایی که بر حقوق بنیادین، شفافیت و پاسخگویی استوار است، مدل آمریکایی که نوآوری و رهبری فناوری را در اولویت قرار می‌دهد و مدل چینی که کنترل دولتی را با توسعه تجاری ترکیب می‌کند (CACM, ۲۰۲۶).

این واگرایی پیامدهای مهمی برای مسئولیت حقوقی و نظارت الگوریتمی دارد. شرکت‌های جهانی هوش مصنوعی ناچارند سه کتاب قواعد متفاوت را هم‌زمان دنبال کنند که این امر هزینه‌های انطباق را افزایش می‌دهد و ممکن است نوآوری را کند کند. گزارش شاخص هوش مصنوعی ۲۰۲۵ نشان می‌دهد که این رویکرد چندقطبی به رگولاتوری، بیشتر به یک "فدرالیسم جهانی" شباهت دارد تا یک رژیم واحد (ISIA Istituto, ۲۰۲۴). برخی از شرکت‌های فناوری آمریکایی به دلیل عدم قطعیت نظارتی، عرضه برخی محصولات هوش مصنوعی در اروپا را متوقف کرده‌اند (CTILS, ۲۰۲۶).

خلأ مسئولیت‌پذیری و ضرورت نوآوری نهادی

یافته‌های پژوهش حاکی از آن است که نظام‌های سنتی مسئولیت حقوقی برای مواجهه با چالش‌های هوش مصنوعی ناکافی هستند. لغو دستورالعمل مسئولیت هوش مصنوعی اتحادیه اروپا در فوریه ۲۰۲۵، اگرچه با استدلال وجود مقررات کافی در قانون هوش مصنوعی و دستورالعمل مسئولیت محصول توجیه شد، اما خلأهایی را در زمینه جبران خسارت برای قربانیان سیستم‌های هوش مصنوعی باقی می‌گذارد (Parliament European, ۲۰۲۵a).

مدل‌های جایگزین مانند طرح جبران خسارت بدون تقصیر با پشتیبانی دولتی که توسط Tran (۲۰۲۵) پیشنهاد شده، می‌تواند راه‌حلی عملی برای این خلأ باشد. این مدل مزایای متعددی دارد: کاهش بار اثبات بر دوش قربانیان، توزیع عادلانه‌تر هزینه‌های جبران خسارت و ایجاد انگیزه برای نوآوری مسئولانه. با این حال، پیاده‌سازی چنین مدلی نیازمند زیرساخت‌های نهادی و مالی قابل توجهی است که ممکن است برای بسیاری از کشورها، به‌ویژه در جنوب جهانی، چالش‌برانگیز باشد.

حاکمیت داده به‌عنوان عرصه تعارض و همکاری

تحلیل رژیم‌های حاکمیت داده نشان می‌دهد که این حوزه به عرصه اصلی تعارض ژئوپلیتیک تبدیل شده است. اتحادیه اروپا با استراتژی اتحادیه داده خود در تلاش است تا حاکمیت داده را به‌عنوان یک اصل راهنما در روابط بین‌المللی تثبیت کند (Commission European, ۲۰۲۵a). در مقابل، ایالات متحده بر جریان آزاد داده به‌عنوان موتور رشد اقتصادی تأکید دارد و چین کنترل دولتی بر داده را به‌عنوان ابزاری برای امنیت ملی و ثبات سیاسی می‌نگرد.

این تعارض در سطح توافقنامه‌های تجارت دیجیتال آشکارتر است. توافقنامه‌های به سبک آمریکایی معمولاً ممنوعیت بومی‌سازی داده و جریان آزاد فرامرزی را در بر می‌گیرند، در حالی که توافقنامه‌های به سبک چینی استثنای گسترده‌ای برای اهداف سیاست عمومی مشروع و امنیت ملی پیش‌بینی می‌کنند (Kang, ۲۰۲۵). اتحادیه اروپا رویکرد میانه‌ای اتخاذ کرده که جریان داده را با رعایت کامل قوانین حفاظت از داده ترکیب می‌کند.

با این حال، نشانه‌هایی از همگرایی تدریجی نیز مشاهده می‌شود. تصویب چارچوب حریم خصوصی داده اتحادیه اروپا-آمریکا و تأیید اعتبار آن توسط دادگاه عمومی اتحادیه اروپا در سال ۲۰۲۵، گامی به سوی ثبات در جریان‌های داده فراتلانتیک محسوب می‌شود (Freshfields, ۲۰۲۵). همچنین، تصویب پیمان دیجیتال جهانی در سپتامبر ۲۰۲۴ به‌عنوان اولین توافق جهانی در زمینه حکمرانی هوش مصنوعی، نشان‌دهنده امکان همکاری بین‌المللی در این حوزه است (UN, ۲۰۲۴).

نقش نهادهای بین‌المللی در پر کردن خلأها

یافته‌ها نشان می‌دهد که نهادهای بین‌المللی در حال ایفای نقش فزاینده‌ای در حکمرانی هوش مصنوعی هستند. گفتگوی جهانی حکمرانی هوش مصنوعی سازمان ملل متحد، که در سپتامبر ۲۰۲۵ راه‌اندازی شد، به‌عنوان "اولین پلتفرم واقعاً جهانی

و فراگیر برای مشارکت جهانی در حکمرانی هوش مصنوعی" توصیف شده است (UN, ۲۰۲۵). این نهاد می‌تواند فضایی برای هماهنگی میان رژیم‌های مختلف حکمرانی و کاهش تکه‌تکه شدن فراهم آورد.

با این حال، چالش‌های قابل توجهی نیز وجود دارد. از سپتامبر ۲۰۲۴، ۱۱۸ کشور عضو هیچ‌یک از هفت ابتکار غیرسازمان ملل متحد با مسیرهای بین‌دولتی نبودند (UN, ۲۰۲۴). این آمار نشان‌دهنده شکاف عمیق در پوشش جهانی ابتکارات حکمرانی هوش مصنوعی است. سرمایه‌گذاری، ظرفیت و مدل‌های زبانی بزرگ به‌طور فزاینده‌ای در تعداد محدودی از کشورها و شرکت‌ها متمرکز شده است.

جنوب جهانی و ضرورت فراگیری

یکی از یافته‌های مهم این پژوهش، شکاف فزاینده میان شمال و جنوب جهانی در حوزه حکمرانی هوش مصنوعی است. کشورهای در حال توسعه با محدودیت‌های ساختاری در زمینه زیرساخت، مهارت و سرمایه روبه‌رو هستند که توانایی آن‌ها برای مشارکت مؤثر در حکمرانی جهانی هوش مصنوعی را محدود می‌کند (AI.OECD, ۲۰۲۵). با این حال، رویکردهای نوآورانه‌ای در حال شکل‌گیری است. استفاده از ابزارهای بدون کد برای حکمرانی محلی هوش مصنوعی، امکان می‌دهد که جوامع در حال توسعه بدون انتظار برای چارچوب‌های متمرکز، قوانین و محافظ‌های خود را تدوین کنند (AI.OECD, ۲۰۲۵). این رویکرد "نوآوری معکوس" می‌تواند الگویی برای سایر کشورهای جنوب جهانی باشد.

هم‌زمان، پیشنهاد چین برای ایجاد سازمان همکاری جهانی هوش مصنوعی و تأکید آن بر بهره‌مندی همه کشورها از این فناوری، نشان‌دهنده تلاش برای جلب حمایت جنوب جهانی است (Newsmax, ۲۰۲۵). اعلامیه شانگهای و قطعنامه اخیر سازمان ملل در زمینه ظرفیت‌سازی هوش مصنوعی نیز نشان‌دهنده توجه فزاینده به نیازهای کشورهای در حال توسعه است (Beijing Review, ۲۰۲۵).

جدول ۲: مقایسه مدل‌های حکمرانی هوش مصنوعی در سه قطب اصلی

بُعد	اتحادیه اروپا	ایالات متحده	چین
فلسفه حاکم	حقوق اول، نوآوری دوم	نوآوری اول، اصلاح بعد	توسعه سخت، کنترل دقیق
رویکرد نظارتی	مبتنی بر ریسک، جامع	بخشی، خودتنظیمی	دولتی-هدایتی، ثبت اجباری
تمرکز اصلی	حقوق بنیادین، شفافیت	رقابت‌پذیری، رهبری فناوری	امنیت ملی، ثبات اجتماعی
حاکمیت داده	حفاظت از حریم خصوصی، حاکمیت داده	جریان آزاد داده	کنترل دولتی، بومی‌سازی
مسئولیت حقوقی	مسئولیت مبتنی بر تقصیر + مسئولیت محصول	مسئولیت محصول، قوانین ایالتی	مسئولیت اداری، کنترل دولتی
نهاد کلیدی	دفتر هوش مصنوعی اتحادیه اروپا	FTC، وزارت دادگستری	اداره فضای سایبری چین

منبع: اقتباس از CACM (۲۰۲۶) و CTILS (۲۰۲۶)

نتیجه‌گیری

این پژوهش نشان داد که مسئولیت حقوقی هوش مصنوعی، نظارت الگوریتمی، حاکمیت داده و دیپلماسی اقتصادی در نظم چندقطبی معاصر به‌طور جدایی‌ناپذیری در هم تنیده‌اند. نظام‌های سنتی مسئولیت حقوقی برای مواجهه با ویژگی‌های خاص سیستم‌های هوش مصنوعی ناکافی هستند و خلأ مسئولیت‌پذیری ناشی از آن، اعتماد عمومی و مشروعیت نهادی را تهدید می‌کند. هم‌زمان، رقابت ژئوپلیتیک میان سه مدل متمایز حکمرانی—اروپایی، آمریکایی و چینی—خطر تکه‌تکه شدن بیشتر فضای جهانی حکمرانی هوش مصنوعی را به همراه دارد.

با این حال، نشانه‌هایی از همگرایی تدریجی نیز مشاهده می‌شود. تصویب پیمان دیجیتال جهانی، راه‌اندازی گفتگوی جهانی حکمرانی هوش مصنوعی و تأیید اعتبار چارچوب حریم خصوصی داده اتحادیه اروپا-آمریکا، همگی نشان‌دهنده امکان همکاری بین‌المللی در حوزه‌های حساس هستند. نهادهای بین‌المللی، به‌ویژه سازمان ملل متحد، می‌توانند نقشی محوری در تسهیل این همگرایی ایفا کنند.

بر اساس یافته‌های پژوهش، پیشنهادهای سیاستی زیر ارائه می‌شود:

نخست، ایجاد یک چارچوب بین‌المللی برای مسئولیت هوش مصنوعی که حداقل استانداردهای مشترک برای شفافیت، ممیزی و جبران خسارت را تعیین کند. این چارچوب می‌تواند بر اصول موجود در قانون هوش مصنوعی اتحادیه اروپا و پیمان دیجیتال جهانی سازمان ملل متحد بنا شود.

دوم، تقویت ظرفیت‌های ممیزی الگوریتمی در سطح جهانی از طریق ایجاد شبکه‌ای از نهادهای ممیزی مستقل که به سطوح مناسب دسترسی به سیستم‌های هوش مصنوعی مجهز باشند. دسترسی جعبه‌سیاه باید به‌عنوان حداقل استاندارد در نظر گرفته شود، با امکان ارتقا به سطوح بالاتر دسترسی در موارد پرخطر.

سوم، توسعه مدل‌های نوآورانه جبران خسارت، از جمله طرح‌های بیمه اجباری و صندوق‌های جبران خسارت با پشتیبانی دولتی، به‌ویژه برای سیستم‌های هوش مصنوعی پرخطر. این مدل‌ها باید به‌گونه‌ای طراحی شوند که برای کشورهای جنوب جهانی نیز قابل دسترس باشند.

چهارم، ترویج همگرایی در حاکمیت داده از طریق توافقنامه‌های تجارت دیجیتال که تعادل میان جریان آزاد داده و حفاظت از حریم خصوصی و امنیت ملی برقرار کنند. رویکرد اتحادیه اروپا می‌تواند الگویی برای این همگرایی باشد.

پنجم، تقویت مشارکت کشورهای جنوب جهانی در حکمرانی هوش مصنوعی از طریق ظرفیت‌سازی، انتقال فناوری و تأمین مالی. گفتگوی جهانی هوش مصنوعی سازمان ملل متحد باید به‌عنوان بستری برای تضمین حضور مؤثر این کشورها در فرآیندهای تصمیم‌گیری عمل کند.

در نهایت، این پژوهش استدلال می‌کند که حکمرانی مؤثر هوش مصنوعی در نظم چندقطبی مستلزم ترکیبی از انعطاف‌پذیری نهادی، همکاری بین‌المللی و تعهد به ارزش‌های بنیادین است. بدون چنین رویکردی، خطر آن وجود دارد که رقابت ژئوپلیتیک، فضای لازم برای همکاری سازنده در زمینه مسئولیت‌پذیری هوش مصنوعی را از بین ببرد.

منابع

۱. Beijing Review. (۲۰۲۵). The Global South in global AI governance. Beijing Review. <https://french.beijingreview.com.cn>
۲. Cen, S. H., & Alur, R. (۲۰۲۴). From transparency to accountability and back: A discussion of access and evidence in AI auditing. In Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '۲۴). ACM. <https://doi.org/10.1145/3689904.3694711>
۳. CIL. (۲۰۲۵). Artificial intelligence & technology in international law news update. Centre for International Law, National University of Singapore. <https://cil.nus.edu.sg>
۴. Communications of the ACM. (۲۰۲۶). Three rulebooks, one race: AI regulation in the U.S., EU, and China. Communications of the ACM. <https://cacm.acm.org>
۵. CTILS. (۲۰۲۶). ۲۰۲۵ global AI regulation review. CTILS. <https://www.ctils.com>
۶. European Commission. (۲۰۲۴). AI Act enters into force. European Commission. <https://commission.europa.eu>
۷. European Commission. (۲۰۲۵a). Data Union in a nutshell. European Commission. <https://digital-strategy.ec.europa.eu>
۸. European Commission. (۲۰۲۵b). Study - The next data frontier: Generative AI, regulatory compliance and international dimensions. European Commission. <https://digital-strategy.ec.europa.eu>
۹. European Parliament. (۲۰۲۵a). Parliamentary question E-۰۰۲۶۵۴/۲۴. European Parliament. <https://www.europarl.europa.eu>
۱۰. European Parliament. (۲۰۲۵b). Answer given by Mr McGrath on behalf of the European Commission. European Parliament. <https://www.europarl.europa.eu>
۱۱. Freshfields. (۲۰۲۵). EU-US Data Privacy Framework survives its first judicial challenge. Freshfields. <https://www.freshfields.com>
۱۲. G۲۰. (۲۰۲۵). G۲۰ AI Task Force chair's summary. G۲۰. <https://news.cgtn.com>
۱۳. Gundani, T. (۲۰۲۵). Toward a new multilateralism for AI: Insights from the IMF Annual Meetings ۲۰۲۵. Regulatory Studies Center, George Washington University. <https://regulatorystudies.columbian.gwu.edu>
۱۴. Istituto ISIA. (۲۰۲۴). AI Index Report ۲۰۲۵: Regulatory implications. Istituto ISIA. <https://www.istitutoisia.it>
۱۵. Kang, M. (۲۰۲۵). Digital trade rules in the age of AI: Global regulatory trends and Korea's strategic direction. Korea Institute for International Economic Policy. <https://www.kiep.go.kr>
۱۶. MIT. (۲۰۲۴). Black-box access is insufficient for rigorous AI audits. MIT. <https://dspace.mit.edu>
۱۷. Newsmax. (۲۰۲۵). China's Xi uses APEC to challenge US on AI, trade. Newsmax. <https://www.newsmax.com>

۱۸. [OECD.AI](https://oecd.ai). (۲۰۲۵). From risk to resilience: No-code AI governance in the Global South. [OECD.AI](https://oecd.ai). <https://oecd.ai>
۱۹. Springer. (۲۰۲۴). Addressing the regulatory gap: Moving towards an EU AI audit ecosystem beyond the AI Act by including civil society. AI and Ethics. <https://link.springer.com>
۲۰. TDGI. (۲۰۲۵). The geopolitics of AI: Three models of digital sovereignty. TDGI. <https://tdgi.org>
۲۱. Tran, H.-C. (۲۰۲۵). Who foots the bill? State-backed no-fault compensation for experimental harms in artificial intelligence regulatory sandboxes. Proceedings of the AAAI ACM Conference on AI, Ethics, and Society, ۸(۳), ۲۵۰۸-۲۵۲۱. <https://doi.org/10.11609/aies.v8i3.36734>
۲۲. Tujjar, Ientile, & Toppetti. (۲۰۲۶). After the AI Liability Directive: Civil liability for healthcare AI and the limits of EU risk regulation. Private Law Theory. <https://www.private-law-theory.org>
۲۳. United Nations. (۲۰۲۴). Global Digital Compact. United Nations. <https://www.un.org>
۲۴. United Nations. (۲۰۲۵). Secretary-General: Global Dialogue on Artificial Intelligence offers platform to build safe systems. United Nations. <https://india.un.org>
۲۵. African Union. (۲۰۲۵). AU commences validation of data governance frameworks to accelerate digital single market by ۲۰۳۰. African Union. <https://aucapps.au.int>