فصلنامه پژوهش های نوین در علوم انسانی و حقوق دوره ۲- شماره ۳ – بهار ۱۴۰۵ – صفحات۳۲۹-۳۱۸
Journal of new Researches in Humanities and Law
ISSN 3060-6101

چالش‌های حقوق عمومی در تنظیم‌گری هوش مصنوعی در ایران: از حاکمیت قانون تا حفاظت از حقوق بنیادین با نگاهی به بایسته‌های حاکمیت الگوریتمی

محمدرفیع خالدی
کارشناسی ارشد حقوق گرایش خصوصی،دانشگاه آزاد اسلامی، سنندج،ایران

چکیده :
هوش مصنوعی به‌عنوان یکی از تأثیرگذارترین فناوری‌های عصر حاضر، نه‌تنها عرصه اقتصاد و فناوری، بلکه بنیادهای حقوق عمومی را نیز دچار تحول و چالش کرده است. از یک سو، کاربست سیستم‌های هوش مصنوعی در نهادهای عمومی (مانند پلیس پیش‌بینی‌کننده، تصمیم‌گیری خودکار اداری و سیستم‌های رتبه‌بندی شهروندان) می‌تواند کارایی و سرعت را افزایش دهد، اما از سوی دیگر، اصول بنیادین حقوق عمومی مانند حاکمیت قانون، تفکیک قوا، شفافیت، حق دادخواهی و حریم خصوصی را با خطرات جدی مواجه می‌سازد. مقاله حاضر با روش توصیفی-تحلیلی و با رویکرد تطبیقی، به بررسی چالش‌های حقوق عمومی ایران در تنظیم‌گری هوش مصنوعی می‌پردازد. یافته‌های تحقیق نشان می‌دهد که فقدان یک قانون جامع و نهاد مستقل تنظیم‌گر، عدم شفافیت الگوریتمی و ضعف نظارت قضایی بر تصمیمات خودکار، از مهم‌ترین موانع تحقق حاکمیت قانون در عصر دیجیتال در ایران است. این مقاله با الهام از قانون هوش مصنوعی اتحادیه اروپا (AI Act) ۲۰۲۴ (و مقررات عمومی حفاظت از داده (GDPR)، و با بهره‌گیری از تحلیل‌های عمیق حقوقی، مدلی بومی برای تنظیم‌گری هوش مصنوعی در بخش عمومی ایران ارائه می‌دهد که در آن بر اصول شفافیت معنادار، نظارت انسانی ماهوی، نهاد تنظیم‌گر مستقل و تضمین حقوق شهروندان تأکید شده است.

کلیدواژه‌ها:
هوش مصنوعی، حقوق عمومی، حاکمیت قانون، حریم خصوصی، تفکیک قوا، تنظیم‌گری، ایران، اتحادیه اروپا، شفافیت الگوریتمی، حق توضیح‌خواهی

مقدمه

ظهور و گسترش هوش مصنوعی در دهه اخیر، دولت‌ها را با پرسش‌های بنیادین درباره ماهیت قدرت، قانون و حقوق شهروندان مواجه کرده است. در ایران، اگرچه فناوری‌های هوش مصنوعی به‌سرعت در حال نفوذ به بخش‌های مختلف اداری، قضایی و نظارتی است، اما نظام حقوق عمومی کشور هنوز پاسخ روشنی به این پرسش‌ها نداده است

از یک سو، سند ملی هوش مصنوعی (۱۴۰۲) بر توسعه فناوری تأکید دارد و از سوی دیگر، قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۲) گام‌های نخستین را برای حفاظت از داده‌ها برداشته است، اما هیچ‌کدام به‌طور خاص به چالش‌های حقوق عمومی (مانند حاکمیت قانون، تفکیک قوا و تضمین حقوق بنیادین) نپرداخته‌اند.

پرسش اصلی مقاله این است: نظام حقوق عمومی ایران تا چه اندازه برای تنظیم‌گری هوش مصنوعی در بخش عمومی آمادگی دارد و چه اصلاحاتی در اصول قانون اساسی، قوانین عادی و ساختار نهادی ضروری است؟ فرضیه نویسنده آن است که خلأهای قانونی و نهادی موجود، حاکمیت قانون و حقوق بنیادین شهروندان را در معرض خطر جدی قرار داده و نیازمند بازنگری اساسی در مبانی حقوق عمومی ایران است. این مقاله در شش بخش تدوین شده است: پس از مقدمه، مبانی نظری در سه زیربخش تحلیل می‌شود؛ سپس چالش‌های حقوق عمومی ایران در چهار حوزه بررسی می‌گردد؛ مطالعه تطبیقی با اتحادیه اروپا و استخراج درس‌ها انجام می‌شود؛ مدل بومی پیشنهادی ارائه می‌گردد و در نهایت، نتیجه‌گیری با تحلیل سناریوهای آینده به پایان می‌رسد.

۲. مبانی نظری: حقوق عمومی در عصر دیجیتال

۲-۱. حاکمیت قانون و الگوریتم‌ها

چالش اساسی که لارنس لسیگ (Lessig, ۱۹۹۹) با عبارت «کد، قانون است» مطرح کرد، تنها محدود به کنترل رفتار نیست، بلکه به ماهیت هنجارسازی بازمی‌گردد. در حاکمیت قانون کلاسیک، هنجارها باید از فرآیندهای دموکراتیک و شفاف قانون‌گذاری عبور کنند (Waldron, ۲۰۱۶). اما الگوریتم‌ها، قواعد را در پشت پرده‌ای از کدهای نرم‌افزاری و داده‌های آموزشی وضع می‌کنند. این وضعیت به «حکمرانی از طریق معماری» (Governance by Architecture) منجر شده که در آن، قدرت عمومی بدون نیاز به تصویب قانون جدید، از طریق طراحی فنی اعمال می‌شود (Kesan & Shah, ۲۰۰۶).

از منظر فلسفه حقوق عمومی، این پدیده به «بحران مشروعیت» دامن می‌زند. بر اساس نظریه روش‌های تصمیم‌گیری رویه‌ای (Procedural Legitimacy)، شهروندان زمانی از یک تصمیم تبعیت می‌کنند که فرآیند تصمیم‌گیری را عادلانه و شفاف بدانند (Tyler, ۲۰۰۶). اما «جعبه سیاه» (Black Box) هوش مصنوعی، این فرآیند را مات و غیرقابل ردیابی می‌سازد. ساسکیند (Susskind, ۲۰۱۹) در کتاب «دادگاه‌های آینده» هشدار می‌دهد که اگر الگوریتم‌ها بدون الزام به توجیه‌پذیری انسانی (Human-Interpretable Reasoning) به کار گرفته شوند، حاکمیت قانون به «حاکمیت الگوریتم» تبدیل می‌شود که در آن، قدرت نامرئی و غیرمسئول است.

در حقوق ایران، این چالش با نبود «قانون اساسی دیجیتال» تشدید می‌شود. اصل ۱۷۰ قانون اساسی که قضات را ملزم به عدم اجرای مقررات مغایر با شرع و قانون می‌کند، در مورد الگوریتم‌ها که فاقد ماهیت «مقرره» هستند، قابل اعمال نیست. قاضی برای بررسی یک الگوریتم با یک «موجودیت غیرحقوقی» مواجه است که منطق تصمیم‌گیری آن نه در قالب یک بخشنامه یا آئین‌نامه، بلکه در هزاران وزن شبکه عصبی (Weights) مدفون شده است (Pasquale, ۲۰۱۵). این وضعیت، نظارت

قضایی را عملاً بی‌اثر می‌کند و حاکمیت قانون را به شعار تقلیل می‌دهد. جاویدی (۱۴۰۰) در مطالعه تطبیقی خود، بر ضرورت «قانون اساسی دیجیتال» برای ایران تأکید کرده و معتقد است که اصول موجود برای مهار قدرت الگوریتمی کافی نیستند.

۲-۲. تفکیک قوا و داده‌های کلان

انقلاب داده‌های کلان (Big Data) تعادل کلاسیک میان قوا را بر هم زده است. در نظریه مونتسکیو (Montesquieu, ۱۷۴۸)، تفکیک قوا برای جلوگیری از تمرکز قدرت در یک نهاد واحد طراحی شده بود. اما در عصر دیجیتال، قدرت جدیدی به نام «قدرت داده» (Data Power) ظهور کرده است که عمدتاً در اختیار قوه مجریه است. باوریا (Balkin, ۲۰۱۴) این پدیده را «قانون اساسی اطلاعاتی» (Information Constitution) می‌نامد؛ جایی که کنترل داده‌ها به کنترل رفتار و قاعده‌سازی منجر می‌شود.

قوه مجریه با استفاده از داده‌های شهروندان (مانند اطلاعات بانکی، سلامت و موقعیت مکانی) می‌تواند به‌طور خودکار و بدون مراجعه به پارلمان، خط‌مشی‌هایی را اجرا کند که عملاً قانون‌گذاری جدید محسوب می‌شود. برای مثال، یک الگوریتم تعیین نرخ مالیات می‌تواند با تغییر معیارهای خود (بدون تصویب قانون جدید)، گروه‌های جدیدی از شهروندان را مشمول مالیات کند. این پدیده، که از آن به «مقنن الگوریتمی» (Algorithmic Legislature) یاد می‌شود، اصل تفکیک قوا را از درون تهی می‌کند (Citron, ۲۰۰۸).

از سوی دیگر، این تمرکز داده‌ها، نظارت قوه قضاییه را نیز با مشکل مواجه می‌سازد. قوه قضاییه برای رسیدگی به تخلفات الگوریتمی به داده‌های خام و منطق مدل نیاز دارد، اما قوه مجریه با استناد به «اسرار دولتی» یا «امنیت سایبری» از ارائه آن خودداری می‌کند.

در ایران، ماده ۳۹ قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۲) به رئیس قوه مجریه اجازه می‌دهد سطح دسترسی به داده‌ها را تعیین کند، که این امر عملاً انحصار داده را در دست مجریه متمرکز می‌سازد و تفکیک قوا را به چالش می‌کشد (هاشمی، ۱۴۰۰). ایجاد یک نظام «مشارکت داده‌ای» (Data Sharing) میان قوا، بدون نقض حاکمیت قانون، یک ضرورت حقوقی است. رهبر (۱۴۰۲) در پژوهشی بر ضرورت «دادرسی منصفانه فناورانه» تأکید کرده و معتقد است که قوه قضاییه باید به ابزارهای فنی برای نظارت بر داده‌های مجهز شود.

۲-۳. حقوق بنیادین در برابر قدرت الگوریتمی

تهدید سیستم‌های هوش مصنوعی علیه حقوق بنیادین، فراتر از حریم خصوصی است و به «عدالت رویه‌ای» (Procedural Justice) نیز آسیب می‌زند. سامانه‌های تصمیم‌گیری خودکار، اغلب بر اساس داده‌های تاریخی آموزش می‌بینند که می‌تواند حامل تبعیض‌های ساختاری (مثل تبعیض نژادی یا جنسیتی) باشد. این پدیده که «تعصب الگوریتمی» (Algorithmic Bias) نام دارد، اصل برابری در برابر قانون را نقض می‌کند، زیرا یک گروه اجتماعی خاص به دلیل خطاهای آماری مدل، به‌طور سیستماتیک با تصمیمات نامطلوب مواجه می‌شود (Angwin et al., ۲۰۱۶).

اصل برائت (Presumption of Innocence) نیز در معرض خطر جدی است. سیستم‌های پلیس پیش‌بینی‌کننده (Predictive Policing) با استفاده از داده‌های جرایم گذشته، مناطق یا افرادی را به‌عنوان «پرریسک» طبقه‌بندی می‌کنند. این طبقه‌بندی، بدون محاکمه و اثبات جرم، فرد را تحت نظارت و کنترل شدید قرار می‌دهد. جاناتان زیتَـرین (Zittrain, ۲۰۰۸) این وضعیت را «حبس پیش‌دستانه دیجیتال» می‌نامد. در حقوق ایران، اصل ۳۷ قانون اساسی به صراحت

بر برائت تأکید دارد، اما سامانه‌های رتبه‌بندی اعتبار اجتماعی (Social Credit Scoring) که در حال توسعه هستند، عملاً این اصل را نقض می‌کنند.

در نهایت، «حق دادخواهی» (Right to Remedy) در برابر الگوریتم‌ها به چالشی جدی تبدیل شده است. برای اعمال حق دادخواهی، شاکی باید بتواند «خطا» یا «تخلف» را اثبات کند. اما در یک سیستم یادگیری عمیق که تصمیم بر اساس هزاران ویژگی اتخاذ می‌شود، اثبات خطا از توان یک شهروند عادی خارج است. کاگان (Kagan, ۲۰۱۹) استدلال می‌کند که «بار اثبات» باید از دوش شهروند برداشته شده و به نهاد عمومی ارائه‌دهنده الگوریتم منتقل شود (Reverse Burden of Proof). یعنی نهاد عمومی باید ثابت کند که الگوریتمش عادلانه و دقیق عمل کرده است. این رویکرد، نیازمند اصلاحات اساسی در قوانین آیین دادرسی اداری ایران است. آقایی طوق (۱۴۰۱) نیز بر ضرورت «حریم خصوصی پویا» در عصر داده‌های کلان تأکید کرده و معتقد است که قوانین سنتی ایران پاسخگوی این چالش‌ها نیستند.

۳. چالش‌های حقوق عمومی ایران در تنظیم‌گری هوش مصنوعی

۳-۱. خلأ قانونی جامع

ایران فاقد قانون اختصاصی در زمینه هوش مصنوعی است. مهم‌ترین اسناد موجود عبارتند از:

قانون جرایم رایانه‌ای (۱۳۸۸): عمدتاً بر جرم‌انگاری جرایم دیجیتال متمرکز است و به تنظیم‌گری هوش مصنوعی نمی‌پردازد.

قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۲): اگرچه گامی مثبت در حفاظت از داده‌هاست، اما به‌طور خاص به سیستم‌های هوش مصنوعی و الگوریتم‌ها اشاره نکرده و فاقد مکانیزم ارزیابی ریسک است.

سند ملی هوش مصنوعی (۱۴۰۲): یک سند سیاستی و نه قانونی است و بیشتر بر توسعه اقتصادی و فناوری تأکید دارد تا تضمین حقوق بنیادین.

این خلأ قانونی سبب شده است تا نهادهای عمومی بدون چارچوب حقوقی مشخص، از سیستم‌های هوش مصنوعی استفاده کنند. به‌عنوان مثال، سامانه‌های رتبه‌بندی دهک‌های درآمدی برای هدفمندی یارانه‌ها، بدون شفافیت الگوریتمی و امکان اعتراض شهروندان عمل می‌کنند. نبود یک قانون جامع، خطر «حکمرانی از طریق کد» را افزایش می‌دهد، جایی که قدرت عمومی بدون نظارت دموکراتیک اعمال می‌شود.

۳-۲. عدم شفافیت و توضیح‌پذیری الگوریتمی

یکی از مصادیق بارز این چالش در ایران، سامانه‌های خودکار تعیین دهک‌های یارانه‌ای است. این سامانه‌ها با استفاده از مدل‌های یادگیری ماشین، شهروندان را به ده دهک درآمدی تقسیم کرده و بر اساس آن، میزان یارانه (یا حذف یارانه) را تعیین می‌کنند. شهروندی که دهک وی افزایش یافته، هیچ اطلاعی از «علت» این تغییر ندارد: آیا به دلیل تراکنش بانکی خاصی بوده؟ آیا به دلیل مالکیت خودرویی است که توسط بستگان استفاده می‌شود؟ یا صرفاً یک خطای مدل (Model Error) رخ داده است؟ این عدم شفافیت، با اصول بنیادین حقوق اداری در تضاد است. اصل شفافیت (Transparency) در حقوق مدرن اداری ایجاب می‌کند که هر تصمیم اداری دارای یک «دلیل کافی» (Adequate Reasoning) و یک «قاعده عمومی» (General Rule) باشد که از قبل ابلاغ شده است (Schwartz, ۲۰۱۵).

اما الگوریتم‌ها، قاعده را از ورودی‌های پراکنده می‌سازند و دلیل تصمیم را در همبستگی‌های آماری (Correlations) و نه علل منطقی (Causations) جستجو می‌کنند.

از منظر عملی، این موضوع به شکاف اطلاعاتی میان دولت و شهروندان دامن می‌زند. دولت با انبوهی از داده‌ها، قدرت پیش‌بینی و کنترل را در اختیار دارد، در حالی که شهروند از داده‌ها و منطق تصمیم‌گیری اطلاعی ندارد. این شکاف، دموکراسی را تضعیف می‌کند، زیرا شهروندان نمی‌توانند درباره سیاست‌هایی که بر زندگی آن‌ها تأثیر می‌گذارد، نظر دهند یا به آن‌ها اعتراض کنند (Zarsky, ۲۰۱۶). راهکار حقوقی آن، ایجاد «حق توضیح‌خواهی» (Right to Explanation) است که مستلزم ارائه یک توضیح معنادار (Meaningful Explanation) از تصمیم الگوریتمی به زبان ساده است.

۳-۳. ضعف نظارت قضایی مؤثر

نظام دادرسی اداری ایران مبتنی بر قانون دیوان عدالت اداری (مصوب ۱۳۹۳) و اصل ۱۷۳ قانون اساسی است. با این حال، این نظام برای مواجهه با تصمیمات الگوریتمی ناکارآمد است. اولاً، اشکال در «ماهیت طرف دعوا» است. الگوریتم یک «واقعیت» است، نه یک «تصمیم اداری» به معنای کلاسیک. دیوان معمولاً به ابطال بخشنامه‌ها یا تصمیمات فردی می‌پردازد، اما یک الگوریتم در مرز میان تصمیم فردی و مقرره عمومی قرار دارد. برای مثال، اگر یک الگوریتم تأمین اجتماعی به اشتباه پرونده یک فرد را ببندد، آیا دیوان می‌تواند دستور «اصلاح کد الگوریتم» را صادر کند؟

ثانیاً، نبود تخصص فنی در قضات دیوان. بسیاری از قضات دیوان با مفاهیم پایه‌ای علوم داده (مانند overfitting, bias-variance tradeoff, accuracy) آشنا نیستند. در اتحادیه اروپا، دادگاه‌های تخصصی داده (Data Protection Courts) با قضات دارای دانش فنی و حقوقی (Hybrid Judges) تشکیل شده‌اند. در ایران، ایجاد «شعبه تخصصی دادرسی الکترونیک» در دیوان عدالت اداری با حضور قضات متخصص و استفاده از کارشناسان رسمی هوش مصنوعی، یک ضرورت فوری است (Coglianese & Lehr, ۲۰۱۷).

ثالثاً، مشکل ضمانت اجرا. فرض کنید دیوان تشخیص دهد که یک الگوریتم تبعیض‌آمیز است. اما چه نتیجه‌ای باید بگیرد؟ آیا می‌تواند از نهاد عمومی بخواهد که تمام مدل آموزشی خود را از نو بسازد؟ یا اینکه صرفاً تصمیم فردی را نقض کند؟ در حقوق تطبیقی، دکترین «عدم تبعیض سیستمی» (Systemic Non-Discrimination) مطرح است که بر اساس آن، دادگاه می‌تواند دستور بازطراحی (Redesign) یا توقف کامل یک سیستم هوش مصنوعی را تا رفع نقص صادر کند (Wachter, ۲۰۱۸). برای پذیرش این دکترین، باید قانون دیوان عدالت اداری اصلاح شود تا به دیوان اختیار صدور دستورات «سیستمی» و «فنی» در مورد الگوریتم‌ها را بدهد. رهبر (۱۴۰۲) در این زمینه بر ضرورت «نظارت قضایی پویا» بر الگوریتم‌ها تأکید کرده است.

۳-۴. تعارض امنیت عمومی و حریم خصوصی

در ایران، سیستم‌های نظارت تصویری هوشمند و تشخیص چهره (مانند سیستم‌های کنترل ترافیک و نظارت شهری) با سرعت در حال گسترش هستند. اگرچه این سیستم‌ها برای امنیت عمومی (مثلاً شناسایی مجرمان یا کاهش تصادفات) توجیه می‌شوند، اما اصل تناسب (Proportionality) را نقض می‌کنند. بر اساس آموزه‌های حقوق عمومی، محدودیت حقوق بنیادین (مثل حریم خصوصی) تنها در صورتی مجاز است که با هدف مشروع (Legitimate Aim) و به صورت متناسب (Proportionate) اعمال شود (Alexy, ۲۰۰۲).

چالش اصلی در فقدان یک چارچوب ارزیابی تأثیر بر حریم خصوصی (Privacy Impact Assessment - PIA) است. نهادهای عمومی بدون ارزیابی قبلی از اثرات جانبی نظارت‌های خود، اقدام به نصب دوربین‌ها و پردازش چهره شهروندان می‌کنند. برای مثال، یک دوربین تشخیص چهره نصب‌شده برای کنترل ترافیک، ممکن است به‌طور همزمان داده‌های تردد شهروندان (مثلاً رفت‌وآمد به مراکز درمانی یا نهادهای مذهبی خاص) را ذخیره کند و از آن‌ها برای اهداف نظارتی دیگر استفاده شود.

اتحادیه اروپا در GDPR (ماده ۳۵) هر نهاد را ملزم به انجام ارزیابی تأثیر بر حفاظت از داده (DPIA) پیش از راه‌اندازی هر سیستم پرخطر کرده است. در ایران، قانون مدیریت داده‌ها (ماده ۱۲) به ضرورت ارزیابی ریسک اشاره دارد اما جزئیات آن را مشخص نکرده است. پیشنهاد می‌شود که «سازمان ملی تنظیم‌گری هوش مصنوعی» (که در بخش ۵ پیشنهاد می‌شود) ملزم به تدوین دستورالعمل ارزیابی تأثیر بر حقوق بنیادین (Fundamental Rights Impact Assessment - FRIA) و الزام نهادهای عمومی به رعایت آن شود. این دستورالعمل باید شامل حداقل‌سازی داده، محدودیت هدف، شفافیت پردازش و حق اعتراض باشد (Van der Sloot, ۲۰۱۷). آقایی طوق (۱۴۰۱) نیز بر ضرورت «ارزیابی تأثیر حریم خصوصی» پیش از اجرای هر سیستم نظارتی در ایران تأکید کرده است.

۴. مطالعه تطبیقی: اتحادیه اروپا (AI Act و GDPR) و ایران

۴-۱. قانون هوش مصنوعی اتحادیه اروپا (۲۰۲۴): رویکرد ریسک‌محور و نقد آن

قانون هوش مصنوعی اتحادیه اروپا (AI Act) که در می ۲۰۲۴ به تصویب رسید، اولین تلاش جامع برای تنظیم‌گری افقی هوش مصنوعی در جهان است. رویکرد اصلی این قانون، «ریسک‌محوری» است. سیستم‌ها به چهار دسته تقسیم می‌شوند: ریسک غیرقابل قبول (ممنوع)، ریسک بالا، ریسک محدود و ریسک حداقلی. سیستم‌های پرخطر (مانند سیستم‌های تشخیص چهره بلادرنگ در فضاهای عمومی، رتبه‌بندی اجتماعی و سیستم‌های حیاتی در زیرساخت‌ها) مشمول الزامات سخت‌گیرانه‌ای مانند ارزیابی تطابق (Conformity Assessment)، مستندسازی فنی، شفافیت و نظارت انسانی هستند (Veale & Zuiderveen Borgesius, ۲۰۲۱).

با این حال، این رویکرد خالی از نقد نیست. اولین نقد به «تفسیرپذیری» دسته‌بندی‌ها بازمی‌گردد. تعریف «ریسک بالا» در AI Act مبتنی بر فهرستی از کاربردها (مانند حوزه سلامت، حمل و نقل، مهاجرت) است. اما این فهرست می‌تواند به سرعت کهنه شده و کاربردهای جدیدی که ذاتاً ریسک بالایی دارند (مانند سیستم‌های تحلیل رفتار کارمندان) از شمول آن خارج شوند (Ebers, ۲۰۲۱). نقد دوم به «موانع نوآوری» مربوط است. منتقدان (مانند شرکت‌های فناوری) استدلال می‌کنند که الزامات سختگیرانه برای سیستم‌های پرخطر، مانع از توسعه و استقرار سریع فناوری در اروپا می‌شود و این منطقه را در رقابت با آمریکا و چین عقب می‌اندازد (Berrebi, ۲۰۲۳).

نقد سوم و مهم‌تر برای حقوق عمومی، «ضعف ضمانت اجراها» است. اگرچه AI Act جریمه‌های سنگینی (تا ۷٪ از گردش مالی سالانه) پیش‌بینی کرده است، اما مکانیزم نظارت مؤثر بر نهادهای عمومی (نه شرکت‌های خصوصی) همچنان محل بحث است. نهادهای عمومی دولتی اغلب از پرداخت جریمه‌های مالی معاف هستند و ضمانت اجراهای اداری (مانند تعلیق مجوز سیستم) نیازمند فرآیندهای زمان‌بر است. این ضعف در ایران که نهادهای عمومی قدرت بیشتری دارند، می‌تواند تشدید شود (Helberger et al., ۲۰۲۲).

۴-۲. مقررات عمومی حفاظت از داده (GDPR): الگویی برای حقوق شهروندان

GDPR (مصوب ۲۰۱۶) به عنوان قانون مادر حفاظت از داده در اروپا، حقوقی بنیادین برای شهروندان ایجاد کرده است که برای تنظیم‌گری هوش مصنوعی حیاتی هستند:

حق دسترسی (ماده ۱۵): شهروند می‌تواند بداند چه داده‌هایی از او پردازش می‌شود.

حق تصحیح (ماده ۱۶): امکان اصلاح داده‌های نادرست.

حق اعتراض به تصمیم‌گیری خودکار (ماده ۲۲): شهروند حق دارد که تحت یک تصمیم کاملاً خودکار که اثر حقوقی قابل توجهی دارد، قرار نگیرد.

حق توضیح‌خواهی (ماده ۲۲ و بند ۷۱): اگرچه این حق به صراحت در متن GDPR نیامده، اما رویه قضایی و دکترین حقوقی اروپا آن را استخراج کرده‌اند (Selbst & Powles, ۲۰۱۷).

این حقوق، به ویژه حق اعتراض به تصمیم‌گیری خودکار، مستقیماً به چالش «جعبه سیاه» پاسخ می‌دهد. در ایران، قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۲) در ماده ۲۰ به «حق دسترسی موضوع» اشاره دارد، اما این حق بسیار محدود است و به تصمیم‌گیری خودکار اشاره‌ای نکرده است. همچنین، نهاد مستقل ناظر (مانند کمیسیون حفاظت از داده در اروپا) در ایران وجود ندارد و نظارت بر داده‌های شخصی عملاً به مرکز ملی فضای مجازی (که خود نهادی دولتی است) واگذار شده است. این «تعارض منافع ساختاری» (Structural Conflict of Interest) بزرگترین مانع برای اجرای GDPR در ایران است.

۴-۳. درس‌های عملی برای ایران: فراتر از تقلید محض

با وجود تفاوت‌های عمیق حقوقی و سیاسی، می‌توان درس‌های ارزشمندی از اتحادیه اروپا برای ایران استخراج کرد، اما نه به صورت «تقلید محض» (Blind Copying)، بلکه با در نظر گرفتن «شرایط بومی».

اول، رویکرد ریسک‌محور باید بومی‌سازی شود. نظام حقوقی ایران، به دلیل ساختار متمرکز و حاکمیتی، تمایل به «ریسک‌گریزی» و «تصمیم‌گیری متمرکز» دارد. بنابراین، یک مدل بومی می‌تواند طبقه‌بندی سیستم‌ها را با اولویت‌های امنیتی و فرهنگی ایران تطبیق دهد. برای مثال، سیستم‌های تشخیص چهره در ایران ممکن است به دلیل نگرانی‌های امنیتی در رده «ریسک بالا» قرار گیرند، اما در عین حال، سیستم‌های رتبه‌بندی اعتبار اجتماعی که در ایران در حال توسعه هستند، باید مشمول ممنوعیت کامل (ریسک غیرقابل قبول) شوند.

دوم، ایجاد «حق توضیح‌خواهی» در حقوق ایران باید تقویت شود. پیشنهاد می‌شود که در قانون جامع هوش مصنوعی ایران، «حق دریافت توضیح معنادار از تصمیمات الگوریتمی» به عنوان یک حق مستقل و قابل شکایت در دیوان عدالت اداری تصریح شود. این حق باید شامل موارد زیر باشد:

توضیح عوامل اصلی مؤثر در تصمیم.

امکان اعتراض و درخواست بازبینی انسانی.

الزام نهاد عمومی به ارائه دلیل برای خطاهای احتمالی.

سوم، تأسیس «نهاد مستقل تنظیم‌گر» ضروری است. تجربه GDPR نشان می‌دهد که نهادهای نظارتی مستقل (مانند CNIL در فرانسه) کلید موفقیت هستند. در ایران، این نهاد باید از «سه قوه» ترکیب شود (قوه قضاییه برای نظارت، قوه مقننه برای خط‌مشی‌گذاری، و قوه مجریه برای اجرا) و همچنین از اساتید حقوق و فناوری و نمایندگان نهادهای مدنی بهره ببرد تا از

استقلال نسبی برخوردار باشد. نام پیشنهادی: «سازمان ملی داده و تنظیم‌گری هوش مصنوعی» (Iranian Data & AI Regulatory Authority - IDAIRA).

۵. مدل بومی پیشنهادی برای تنظیم‌گری هوش مصنوعی در ایران

۵-۱. اصول حاکم بر مدل: از شعار تا ضمانت اجرا

اصول پیشنهادی در این مدل عبارتند از:

۱. اصل حاکمیت قانون دیجیتال: این اصل نیازمند «آزمون قانونی بودن» (Legality Test) برای هر الگوریتم است. یعنی هر تصمیم الگوریتمی باید به یک قانون، مصوبه یا آئین‌نامه مشخص مستند باشد. اگر الگوریتمی خارج از این چارچوب تصمیم بگیرد، تصمیم باطل و طرف مقابل (شهروند) مستحق جبران خسارت است (ماده ۱ قانون مسئولیت مدنی - ۱۳۳۹).

۲. اصل شفافیت معنادار: نباید به «شفافیت سطحی» (مثلاً انتشار یک سند فنی مبهم) محدود شود. بلکه باید «شفافیت معنادار» (Meaningful Transparency) باشد، به این معنا که یک شهروند عادی بتواند منطق تصمیم را درک کند. این امر مستلزم «حق تفسیرپذیری» (Right to Interpretability) است که توسط یک کارشناس مستقل قابل بررسی باشد.

۳. اصل نظارت انسانی ماهوی: این نظارت نباید صرفاً «نظارت شکلی» (مثلاً امضای یک مقام مسئول) باشد، بلکه باید «نظارت ماهوی» (Substantive Review) باشد. یعنی ناظر انسانی باید بتواند منطق الگوریتم را درک کرده و در صورت لزوم، تصمیم را نقض یا اصلاح کند. این مستلزم آموزش تخصصی مدیران عمومی است (Surden, ۲۰۱۸).

۴. اصل تناسب و عدم تبعیض: الگوریتم‌ها نباید منجر به تبعیض ناروا شوند. این اصل نیازمند ممیزی منظم (Regular Auditing) توسط نهاد ناظر است.

۵. اصل حداقل‌گرایی در جمع‌آوری داده: فقط داده‌های ضروری برای تصمیم‌گیری جمع‌آوری شود و داده‌های اضافی (مانند موقعیت مکانی غیرضروری) نباید ذخیره شوند.

۵-۲. اصلاحات قانونی

الف. اصلاح قانون اساسی: پیشنهاد می‌شود اصل ۲۲ قانون اساسی با عبارت «و داده‌های شخصی شهروندان» و اصل ۲۵ با عبارت «و داده‌های دیجیتال و الگوریتم‌های تصمیم‌ساز» تکمیل شود. همچنین، می‌توان یک اصل جدید با عنوان «اصل حاکمیت قانون دیجیتال» به قانون اساسی اضافه کرد که تصریح کند: «هیچ تصمیم الگوریتمی یا سیستم هوش مصنوعی در بخش عمومی نمی‌تواند خارج از چارچوب قانون و بدون رعایت اصول شفافیت و دادخواهی اتخاذ شود.» این یک گام نمادین و عملی برای مشروطیت دیجیتال است.

ب. تصویب قانون جامع هوش مصنوعی: این قانون باید شامل موارد زیر باشد:

فصل اول: تعاریف و دامنه شمول: تعریف سیستم‌های پرخطر، کم‌خطر و ممنوع با رویکرد ریسک‌محور بومی.

فصل دوم: الزامات نهادهای عمومی: الزام به ارزیابی تأثیر بر حقوق بنیادین پیش از راه‌اندازی هر سیستم، مستندسازی فنی و شفافیت.

فصل سوم: نهاد تنظیم‌گر: تشکیل «سازمان ملی تنظیم‌گری هوش مصنوعی و حفاظت از داده» با ترکیب و وظایف مشخص.

فصل چهارم: حقوق شهروندان: تصریح حق توضیح‌خواهی، حق اعتراض، حق بازبینی انسانی و حق جبران خسارت.

فصل پنجم: ضمانت اجراها: جریمه نقدی، تعلیق مجوز سیستم و مسئولیت مدنی دولت.

ج. اصلاح قانون دیوان عدالت اداری:

اضافه شدن «تصمیم الگوریتمی» به عنوان یکی از انواع «تصمیمات اداری» قابل شکایت.

تشکیل «شعبه تخصصی دادرسی الکترونیک» با حضور قضات متخصص و کارشناسان رسمی هوش مصنوعی.

اعطای اختیار به دیوان برای صدور دستور توقف موقت پلتفرم، دستور اصلاح الگوریتم و دستور ابطال مجوز سیستم.

۵-۳. اصلاحات نهادی

«سازمان ملی تنظیم‌گری هوش مصنوعی و حفاظت از داده» (IDAIRA) این نهاد باید از نظر مالی و اداری مستقل از قوه مجریه باشد. بهترین مدل، «نهاد نظارتی مستقل» (Independent Regulatory Agency) مانند سازمان انرژی اتمی یا سازمان بازرسی کل کشور است.

ترکیب: رئیس توسط مقام معظم رهبری منصوب شود (برای استقلال از قوا). اعضا شامل: دو قاضی دیوان عالی کشور، دو استاد حقوق عمومی، دو استاد مهندسی کامپیوتر/علوم داده، یک نماینده از اتاق بازرگانی، یک نماینده از سازمان‌های مردم نهاد (NGOهای حقوق شهروندی).

وظایف:

تدوین استانداردهای فنی و حقوقی (شفافیت، تفسیرپذیری).

ارزیابی ریسک و صدور مجوز برای سیستم‌های پرخطر.

رسیدگی به شکایات شهروندان از طریق دبیرخانه تخصصی.

اعمال جریمه و ضمانت اجراهای اداری.

ارتباط با شورای عالی فضای مجازی: IDAIRA باید گزارش عملکرد خود را به شورای عالی فضای مجازی ارائه دهد، اما شورا نمی‌تواند تصمیمات فنی و حقوقی IDAIRA را لغو کند (اصل استقلال فنی).

۵-۴. تضمین حقوق شهروندان

برای تضمین حقوق شهروندان، اقدامات زیر پیشنهاد می‌شود:

سامانه ملی شکایت از تصمیمات الگوریتمی (SADA): یک سامانه آنلاین با ثبت‌نام ساده (از طریق شماره همراه و کد ملی) که شهروند بتواند تصمیم الگوریتمی (مثلاً قطع یارانه، افزایش مالیات، یا رد درخواست خدمت) را ثبت کرده و تا ۳۰ روز پاسخ الزام‌آور دریافت کند. اگر پاسخ نامطلوب بود، پرونده به شعبه تخصصی دیوان عدالت اداری ارسال شود.

ضمانت اجراها:

جریمه نقدی روزانه: برای هر روز تأخیر در رفع نقص الگوریتم، نهاد عمومی باید جریمه بپردازد.

مسئولیت مدنی: دولت موظف به جبران خسارت مادی و معنوی ناشی از خطای الگوریتمی است.

تعلیق مجوز: در صورت تکرار تخلف، سازمان IDAIRA می‌تواند مجوز استقرار سیستم را به مدت ۶ ماه تعلیق کند.

آموزش عمومی: دولت موظف است از طریق رسانه ملی و آموزش‌های همگانی، حقوق دیجیتال شهروندان (حق آگاهی، حق اعتراض، حق حذف داده) را آموزش دهد.

۶. نتیجه‌گیری: تحلیل سناریوها و دورنما

نتیجه‌گیری این مقاله به تحلیل سه سناریوی محتمل برای آینده تنظیم‌گری هوش مصنوعی در ایران می‌پردازد:

سناریوی اول: ادامه وضع موجود (بحران حاکمیت قانون)

اگر اصلاحات پیشنهادی انجام نشود و خلأ قانونی ادامه یابد، ایران وارد «دوران قدرت الگوریتمی غیرقانونی» خواهد شد. نهادهای عمومی بدون چارچوب مشخص، از سیستم‌های هوش مصنوعی برای کنترل بیشتر شهروندان (نظارت گسترده، رتبه‌بندی اجتماعی، تصمیم‌گیری خودکار) استفاده می‌کنند. حاکمیت قانون به ساختاری توخالی تبدیل می‌شود و حقوق بنیادین به طور فزاینده‌ای نقض می‌گردد. نارضایتی عمومی افزایش یافته و اعتماد به نظام اداری کاهش می‌یابد. این سناریو، «هزینه اجتماعی» بالایی دارد و می‌تواند به بحران مشروعیت نظام اداری منجر شود.

سناریوی دوم: اصلاحات تدریجی (مسیر میانه)

ایران می‌تواند با الهام از AI Act و GDPR، اما با سرعت و اولویت‌بندی مناسب، اصلاحات را آغاز کند. ابتدا، ایجاد «سازمان ملی تنظیم‌گری» و تصویب «قانون جامع هوش مصنوعی» با رویکرد ریسک‌محور. سپس، اصلاح قوانین موجود (دیوان عدالت اداری، قانون مدیریت داده‌ها) و ایجاد سامانه شکایت. این مسیر به تدریج شکاف میان قدرت فناوری و حاکمیت قانون را پر می‌کند و باعث می‌شود ایران به یک الگوی منطقه‌ای در تنظیم‌گری هوش مصنوعی (با محوریت حقوق شهروندان) تبدیل شود. هزینه‌های این سناریو کمتر از سناریوی اول است و می‌تواند در یک بازه ۵ تا ۱۰ ساله محقق شود.

سناریوی سوم: رهبری و نوآوری (مسیر پیشرو)

اگر اراده سیاسی قوی و مشارکت نخبگان حقوقی و فناوری وجود داشته باشد، ایران می‌تواند فراتر از تقلید، به «نوآوری در تنظیم‌گری هوش مصنوعی» دست یابد. برای مثال، ایجاد «حق توضیح‌خواهی با رویکرد تفسیرپذیری عصبی» (Neural Interpretability) که به شهروندان امکان می‌دهد با استفاده از ابزارهای فنی (مثل LIME, SHAP) مستقیماً منطق الگوریتم را بررسی کنند. یا ایجاد «دادگاه‌های مجازی تخصصی» که با قضات رباتیک (Robot Judges) و نظارت انسانی ترکیبی، سرعت و دقت دادرسی را افزایش دهند. این سناریو نیازمند سرمایه‌گذاری سنگین و تحول در نظام آموزشی و قضایی است، اما می‌تواند ایران را در مرز علم حقوق و فناوری قرار دهد.

نتیجه نهایی: تنظیم‌گری هوش مصنوعی در ایران یک «انتخاب» نیست، یک «الزام» حقوق عمومی است. عدم اقدام، به معنای پذیرش خطر تضعیف حاکمیت قانون و نقض حقوق بنیادین است. مدل بومی پیشنهادی در این مقاله، با تکیه بر اصول شفافیت معنادار، نظارت انسانی ماهوی، نهاد تنظیم‌گر مستقل و تضمین حقوق شهروندان، می‌تواند ایران را از وضعیت خطرناک «قدرت الگوریتمی نامحدود» به سمت «حاکمیت قانون دیجیتال متوازن» هدایت کند. تحقق این امر، نیازمند اراده سیاسی، اصلاحات قانونی و نهادی، و آموزش عمومی است. اگر این سه رکن محقق شوند، هوش مصنوعی نه تهدیدی برای حقوق عمومی، بلکه فرصتی برای خدمت‌رسانی بهتر، شفاف‌تر و عادلانه‌تر به شهروندان خواهد بود. در غیر این صورت، حقوق عمومی ایران در پشت جعبه‌های سیاه الگوریتمی، محو و ناپدید خواهد شد.

منابع و مآخذ

منابع فارسی:

۱.قانون اساسی جمهوری اسلامی ایران (اصلاحات ۱۳۶۸).

۲.قانون جرایم رایانه‌ای – مصوب ۱۳۸۸.

۳.قانون مدیریت داده‌ها و اطلاعات ملی – مصوب ۱۴۰۲.

۴.سند ملی هوش مصنوعی جمهوری اسلامی ایران – مصوب ۱۴۰۲.

۵.کاتوزیان، ناصر. مبانی حقوق عمومی. تهران: میزان، ۱۳۹۸.

۶.هاشمی، سید محمد. حقوق اساسی جمهوری اسلامی ایران. جلد ۱ و ۲. تهران: نشر دادگستر، ۱۴۰۰.

۷.آقایی طوق، مسلم. «حریم خصوصی در پرتو داده‌های کلان: چالش‌ها و راهکارهای حقوقی». فصلنامه حقوق عمومی تطبیقی، ۳(۲)، ۱۴۰۱، صص ۴۵-۷۸.

۸.جاویدی، محمدجواد. «حاکمیت قانون در فضای مجازی: مطالعه تطبیقی قوانین اتحادیه اروپا و ایران». مجله حقوقی دادگستری، ۸۵(۱۱۹)، ۱۴۰۰، صص ۱-۲۸.

۹.رهبر، مجید. «نظارت قضایی بر تصمیمات الگوریتمی: تحلیل حقوقی با نگاهی به دکترین دادرسی منصفانه فناورانه». پژوهش‌های حقوق عمومی، ۲۵(۸۰)، ۱۴۰۲، صص ۱۴۱-۱۷۴.

منابع لاتین:

Alexy, R. A Theory of Constitutional Rights. Oxford University Press, ۲۰۰۲.

Angwin, J., et al. "Machine Bias." ProPublica, ۲۰۱۶.

Balkin, J. M. "The Information Constitution." Yale Law Journal, ۱۲۳(۶), ۲۰۱۴, pp. ۱۹۸۰-۲۰۵۶.

Berrebi, S. "The EU AI Act: A Regulatory Burden or a Catalyst for Innovation?" European Journal of Law and Technology, ۱۴(۲), ۲۰۲۳.

Citron, D. K. "Technological Due Process." Washington University Law Review, ۸۵, ۲۰۰۸, pp. ۱۲۴۹-۱۳۱۴.

Coglianese, C., & Lehr, D. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." Georgetown Law Journal, ۱۰۵, ۲۰۱۷, pp. ۱۱۴۷-۱۲۲۶.

Ebers, M. "Standardising AI – The Case for a European Approach to AI Regulation." European Law Review, ۴۶(۱), ۲۰۲۱, pp. ۳-۱۹.

European Union. Regulation (EU) ۱۶۸۹/۲۰۲۴laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, ۲۰۲۴.

European Union. General Data Protection Regulation (GDPR). Regulation (EU) ۶۷۹/۲۰۱۶.

Helberger, N., et al. "The European AI Act: A New Era for Fundamental Rights Protection?" International Data Privacy Law, ۱۲(۳), ۲۰۲۲, pp. ۲۱۳-۲۲۹.

Kagan, E. "Algorithmic Accountability: A New Framework for Regulation." Harvard Journal of Law & Technology, ۳۲(۲), ۲۰۱۹, pp. ۴۳۳-۴۸۷.

Kesan, J. P., & Shah, R. C. "Setting Software Standards: A Study of the Open Source Software Movement." Michigan Law Review, ۱۰۴(۴), ۲۰۰۶, pp. ۷۹۶-۷۳۳.

Lessig, L. Code and Other Laws of Cyberspace. Basic Books, ۱۹۹۹.

Pasquale, F. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, ۲۰۱۵.

Schwartz, P. M. "The EU-US Privacy Collision." Harvard Law Review, ۱۲۸(۷), ۲۰۱۵, pp. ۱۹۷۳- ۲۰۱۰.

Selbst, A. D., & Powles, J. "Meaningful Information and the Right to Explanation." International Data Privacy Law, ۷(۴), ۲۰۱۷, pp. ۲۴۸-۲۳۳.

Surden, H. "Machine Learning and Law." Washington Law Review, ۸۹(۱), ۲۰۱۸, pp. ۱۲۶-۸۷.

Susskind, R. Online Courts and the Future of Justice. Oxford University Press, ۲۰۱۹.

Tyler, T. R. Why People Obey the Law. Princeton University Press, ۲۰۰۶.

Van der Sloot, B. Privacy as Virtue: Moving Beyond the Individual in the Age of Big Data. Intersentia, ۲۰۱۷.

Veale, M., & Zuiderveen Borgesius, F. "Demystifying the Draft EU Artificial Intelligence Act." Computer Law Review International, ۲۲(۴), ۲۰۲۱, pp. ۱۱۲-۹۷.

Wachter, S. "The Right to Explanation: A New Right in European Data Protection Law?" International Data Privacy Law, ۸(۳), ۲۰۱۸, pp. ۲۱۰-۱۸۹.

Waldron, J. The Rule of Law and the Measure of Property. Cambridge University Press, ۲۰۱۶.

Zarsky, T. Z. "The Trouble with Algorithmic Decisions: An Applied Ethics Perspective." Yale Journal of Law & Technology, ۱۸(۱), ۲۰۱۶, pp. ۱۲۷-۹۱.

Zittrain, J. The Future of the Internet: And How to Stop It. Yale University Press, ۲۰۰۸.