
بسم الله
الرحمن الرحيم

پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC

فن‌نگار

گاهنامه اطلاع‌رسانی و تخصصی پژوهشگاه ارتباطات و فناوری اطلاعات

صاحب امتیاز: پژوهشگاه ارتباطات و فناوری اطلاعات

- مدیر مسئول: سید محمد حسین‌پور
- سردبیر: الهام عدالتی
- دبیر علمی: اعظم صادق‌زاده
- دبیران فنی: محمدهادی بکائی و الهام رأفتی
- دبیر تحریریه: احسان سرشت
- طراح گرافیک: فاطمه محمدی
- عکس: هادی هادیان
- مدیر اجرایی: فرزانه فرزانیان
- همکاران این نشریه: محمدشهرام معین، مژگان فرهودی
طلا تفضلی، ساسان کرمی‌زاده، افسانه معدنی

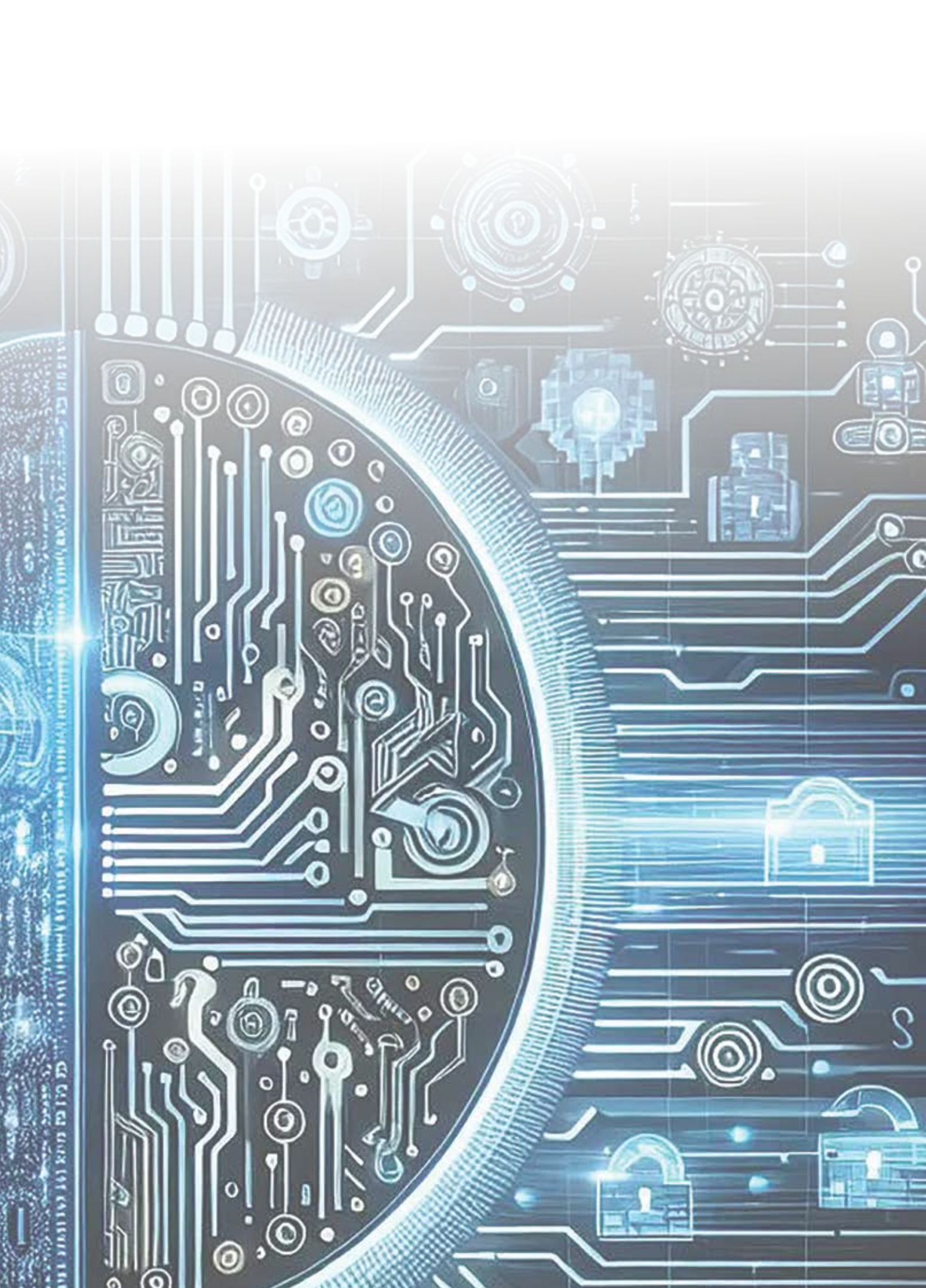
- **نشانی:** انتهای کارگر شمالی، روبه‌روی سازمان انرژی اتمی، پژوهشگاه ارتباطات و فناوری اطلاعات
تلفن: ۸۴۹۷۷۱۷۵

www.itrc.ac.ir

- فایل PDF و FLASH نشریه در سایت پژوهشگاه ارتباطات و فناوری اطلاعات، منوی بخش نشریه الکترونیک موجود است.
- نشریه در انتخاب ویرایش و تلخیص مطالب آزاد است.
- کلیه مطالب براساس سیاست‌گذاری و اهداف تحریریه منعکس خواهد شد.
- برای ارسال مطالب اعم از مقالات پژوهشی، تحقیقی، گزارشی و ... می‌تواند از سامانه اداری یا واحد ستادی مربوطه، شماره نمابر ۸۸۶۳۰۳۵۱ و یا نشانی ایمیل Info@itrc.ac.ir استفاده نمایید.

فهرست مطالب

پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC



سخن نخست

توسعه و به‌کارگیری فناوری‌های نوین در جهت رفع چالش‌های ملی، از جمله ناترازی انرژی کشور

سال گذشته، پژوهشگاه با تلاش و همت شما، مسیر پویایی را در توسعه علم و فناوری طی کرد. از همه شما که با تعهد و تخصص خود در پیشبرد اهداف پژوهشگاه سهم داشته‌اید، صمیمانه قدردانی می‌کنم. در این میان، یاد همکارانی را که دیگر در میان ما نیستند، گرامی می‌داریم. جای خالی آنان در جمع ما حس می‌شود، اما نقش و یادشان همیشه در مسیر پیشرفت پژوهشگاه زنده خواهد ماند.

در سال جدید که به "سرمایه گذرای برای تولید" توسط مقام معظم رهبری نامگذاری شده است، مسئولیت ما در مسیر توسعه ارتباطات و فناوری اطلاعات بیش از پیش اهمیت دارد. اعتماد وزیر محترم ارتباطات و فناوری اطلاعات به پژوهشگاه، ما را بر آن می‌دارد که نقشی کلیدی‌تر در آینده فناوری کشور در این سال ایفا کنیم. یکی از مهم‌ترین اولویت‌های ما در این راه، توسعه و به‌کارگیری فناوری‌های نوین در تحول دیجیتال، هوشمندسازی و رفع چالش‌های ملی، از جمله ناترازی انرژی است. فناوری‌های ارتباطی و هوش مصنوعی می‌توانند نقشی اساسی در مدیریت بهینه منابع، افزایش بهره‌وری و ایجاد زیرساخت‌های هوشمند ایفا کنند.

بی‌تردید، تحقق این اهداف تنها با هم‌افزایی ظرفیت‌های علمی و صنعتی کشور امکان‌پذیر خواهد بود. پژوهشگاه در سال جدید، با گسترش همکاری‌های مؤثر با

دانشـگاه‌ها، شـرکت‌های دانش‌بنیـان و صنایـع مرتبـط، بـه دنبـال آن اسـت کـه پلـی میـان دانـش و اجـرا باشـد و از ظرفیـت نخبـگان کشـور در مسـیر توسـعه فناوری‌هـای راهبـردی بهـره گیـرد. تعامـل سـازنده بـا بخش‌هـای مختلـف علمـی و صنعتـی، فرصتـی ارزشـمند بـرای ارتقـای تـوان پژوهشـگاه و تحقـق مأموریت‌هـای ملـی آن خواهـد بـود.

بـا امیـد بـه سـالی سرشـار از موفقیـت، پیشـرفت و دسـتاوردهای ارزشـمند، نـوروز و مـاه مبـارک رمضـان را بـه شـما و خانـواده محترمتـان تبریـک می‌گویـم و از درگاه خداونـد متعـال، سـلامتی، شـادکامی و توفیـق روزافـزون برایتـان آرزومنـدم.

تحلیل

هوش مصنوعی:
فرزند خلف یا ناخلف، سالم یا معلول

نویسنده: دکتر محمدشهرام معین

هوش مصنوعی از دهه ۵۰ میلادی با هدف ساختن رایانه یا سامانه ای که مانند انسان فکر و عمل کند مطرح شد. دو زمستان را در سال‌های دهه ۷۰ و ۹۰ میلادی تجربه کرد و از اواسط دهه ۲۰۰۰ میلادی با سرمایه گذاری هنگفت صورت گرفته در حوزه‌های زیرساخت پردازشی و الگوریتمی و نیز با افزایش چشمگیر حجم داده‌های قابل دسترس برای آموزش مدل‌های پیچیده با لایه‌های عمیق وارد مرحله جدیدی از پیشرفت چشمگیر و روزافزون شد. به شکلی که به هدف اولیه خود روزبه‌روز نزدیک و نزدیکتر می‌شود و حتی انتظار می‌رود با هوش مصنوعی فوق‌العاده یا همان ASR از توان انسان هم در سال‌های آتی فراتر رود. ظهور روزمره ابزارهای جدید در حوزه‌های مختلف هوش مصنوعی به‌ویژه مدل‌های زبانی بزرگ و هوش مصنوعی مولد در سه سال اخیر از ChatGPT گرفته تا DeepSeek مؤید این دیدگاه است. این ابزارها با کاربردهای عمومی و خاص و کاربرانی از طیف‌های گسترده تخصصی و غیرتخصصی و سنتی از محبوبیت چشمگیری برخوردار شده‌اند. همچنین کاربرد هوش مصنوعی در حوزه‌های مختلف مانند صنعت، بانکداری، پزشکی، کشاورزی و ... در دنیا افزایشی است.

در ایران نیز هوش مصنوعی از اوایل دهه ۶۰ شمسی با نقش‌آفرینی اساتیدی چون شادروان پروفسور کارو لوکس و شادروان پروفسور کامبیز بدیع در پژوهش‌های دانشگاهی مطرح شد و این روند ادامه داشت به شکلی که از نظر تولید مقالات علمی، ایران رتبه خوبی در دنیا و اول را در منطقه کسب کرده است. با این وجود کاربست نتایج این تحقیقات در ابعاد ملی و نیز استفاده از هوش مصنوعی در حوزه‌های مختلف کاربردی به شکلی که دولت و مردم از آن به شکل مناسبی بهره‌مند شوند، متأسفانه با آن شیب افزایش نیافته است. معاونت علمی، فناوری و اقتصاد دانش‌بنیان در سال ۱۳۹۸ اقدام به تدوین سند فناوری هوش مصنوعی به منظور تصویب آن در شورایعالی انقلاب فرهنگی نمود.

محتوای این سند مانند دیگر اسناد فناوری همچون نانو، فاقد مؤلفه‌های غیرفناورانه بود. اولین اقدام جدی در راستای عملیاتی نمودن هوش مصنوعی در ابعاد ملی در «مرکز نوآوری و توسعه هوش مصنوعی» در «پژوهشگاه ارتباطات و فناوری اطلاعات» با در نظر گرفتن تمام

جنبه‌های فنی، قانونی، کسب و کاری و راهبردی آن، طی سال‌های ۱۳۹۹ و ۱۴۰۰ و در قالب پروژه «تدوین نقشه راه توسعه ملی هوش مصنوعی» انجام شد. نتیجه این پروژه، که با سفارش معاونت نوآوری و فناوری وزارت ارتباطات و فناوری اطلاعات اجرا گردید، نقشه راه ملی‌ای با تمام مؤلفه‌های لازم از چشم‌انداز گرفته تا اقدام، پروژه و فعالیت بود که در آن نگاشت نهادی نیز ارائه شده بود.

بعد از فرمایشات مقام معظم رهبری در خصوص جایگاه هوش مصنوعی در حکمرانی کشور در آبان ۱۴۰۰، فعالیت‌ها برای عملیاتی نمودن هوش مصنوعی افزایش یافت. یکی از این فعالیت‌ها، بازبینی سند فناوری هوش مصنوعی در شورایعالی انقلاب فرهنگی بود که در آن نمایندگان نهادها و سازمان‌های مختلف منجمله وزارت ارتباطات و فناوری اطلاعات مشارکت داشتند و با سرعت کم نهایتاً در خرداد ۱۴۰۳ به تصویب شورا رسید. این سند با وجود نقدهای زیادی که بر آن وارد شده، می‌تواند به عنوان سند بالادستی مورد استناد قرار گیرد. فعالیت دیگر صورت گرفته تأسیس سازمان ملی هوش مصنوعی در تیر ۱۴۰۳ بود. این سازمان نیز به دلیل ابهام جایگاه آن در زیست بوم هوش مصنوعی و نقش آفرینی ضعیفش (که می‌تواند ناشی از عدم تصویب اساسنامه آن در هیئت دولت تاکنون باشد) نتوانسته تاکنون تأثیر قابل توجهی در توسعه هوش مصنوعی در کشور داشته باشد. البته اقداماتی در حوزه‌های مختلفی مانند صنعت، کشاورزی، پزشکی و بانکداری آغاز شده و ادامه هم دارد ولی با آنچه باید باشد فاصله دارد. لذا اینک با مشکلاتی در کاربست هوش مصنوعی در کشور مواجهیم که مهمترین آنها عبارتند از: نامشخص بودن متولی کار، عدم دسترسی به زیرساخت پردازشی و داده‌های کافی و مناسب، کمبود نیروی انسانی متخصص، تفرق کارها، فعالیت‌های نمایشی بدون بازده و عمدتا خسارت بار، ورود افراد نامطلع و سودجو در عرصه کار و عدم هم‌افزایی بین بازیگران. به این موارد ناشناس بودن کاربردهای مفید این فناوری در بین مردم و بعضاً تأکید صرف بر تهدیدات و مخاطرات آن را اضافه کنید. همه این موضوعات باعث شده تا ریسک پرورش یک فرزند ناخلف و نا به راه به نام هوش مصنوعی بسیار افزایش یافته و به جای داشتن یک فرزند سالم و شاداب، انتظار داشتن یک فرزند معلول و نامتقارن را داشته باشیم.

شایسته است که روند معیوب فعلی با مشخص شدن متولی توسعه متعادل، متوازن و چابک هوش مصنوعی و ایفای نقش دلسوزانه آن به همراه وفاق و همدلی بین تمام بازیگران، هر چه سریعتر تصحیح شود تا جایگاه هر بازیگر با توجه به تخصص، ظرفیت و مأموریت آن مشخص گردد و به جای فعالیت‌های موازی بدون بازده و بعضا مزاحم توسط سودجویان، دلسوزان در بخش‌های دولتی و خصوصی آستین بالا بزنند و نقش‌آفرینی کنند. در غیر اینصورت به جای یک فرزند سالم، شاداب و مفید شاهد تربیت یک فرزند ناخلف، افسرده و مضر به نام هوش مصنوعی خواهیم بود که حتی ممکن است به مرگ آن به معنی عدم کاربستش بیانجامد. با توجه به جایگاه ویژه پژوهشگاه ارتباطات و فناوری اطلاعات در زیست‌بوم هوش مصنوعی، توان علمی و نیز فعالیت‌های صورت گرفته در آن از چند دهه قبل تاکنون به‌ویژه تدوین سند نقشه راه توسعه ملی هوش مصنوعی، این پژوهشگاه آماده ایفای نقش کلیدی در این راستا می‌باشد.

دستاوردهای مرکز هوش مصنوعی پژوهشگاه در یک نگاه

محورها	انجام شده	در حال اجرا
طراحی و توسعه زیرساخت‌های لازم برای توسعه زیست‌بوم هوش مصنوعی	• طراحی و راه‌اندازی ابررایانه سیمرغ	• اقدام به راه‌اندازی مرکز پردازش فوق سریع و تولید داده‌های برچسب‌خورده فارسی در حوزه‌های مختلف مانند تشخیص ادعا، تحلیل احساسات، اخبار جعلی و غیره
طراحی و پیاده‌سازی سامانه‌های مورد نیاز برای توسعه کاربردهای هوش مصنوعی	• طراحی و پیاده‌سازی سامانه‌های تشخیص محتوای جعلی • تحلیل داده‌های ترافیکی شبکه ملی اطلاعات • سامانه ذکاوت برای ذائقه‌سنجی کاربران	• سامانه تحلیل اپلیکیشن‌های بازارگاه‌ها (تابان) • سامانه تخمین سطح زیرکشت محصولات کشاورزی با استفاده از هوش مصنوعی • مدیریت ترافیک شبکه‌های ارتباطی و نرم‌افزار شبکه LTE با هوش مصنوعی و قابلیت خودسازماندهی
آزمایشگاه ارزیابی محصولات و خدمات هوش مصنوعی		• طراحی و راه‌اندازی آزمایشگاه ارزیابی محصولات و خدمات حوزه هوش مصنوعی و دریافت مرجعیت مربوطه از سازمان فناوری اطلاعات • تدوین استانداردهای ملی • تاسیس دبیرخانه کمیته متناظر با IEC JTC1/Iso/SC42 • با عنوان هوش مصنوعی توسط سازمان ملی استاندارد در پژوهشگاه ارتباطات و فناوری • تغییر عضویت کمیته SC ۴۲ از O به P
تدوین برنامه‌ها و اسناد راهبردی توسعه پایدار زیست‌بوم هوش مصنوعی	• پیش‌نویس سند ملی توسعه هوش مصنوعی • انتشار کتابچه‌های کاربردی در حوزه‌های مختلف • تدوین مدل بلوغ هوش مصنوعی شرکت‌های ارتباطی • تدوین نظام فنی و اجرایی توسعه کاربردهای هوش مصنوعی	• تدوین پیش‌نویس لایحه هوش مصنوعی • تدوین چارچوب استانداردهای ملی و برنامه‌هایی نظیر مقابله با تهدیدات سایبری با رویکرد هوش مصنوعی و مدیریت و حکمرانی داده • مشارکت در تدوین برنامه عملیاتی سند نقشه راه هوش مصنوعی • تعریف و تدوین دوره‌های سطح ۱ برای مربیان فنی و حرفه‌ای سازمان فنی حرفه‌ای کشور
ترویج و فرهنگ‌سازی کاربردهای هوش مصنوعی	• رویدادهای تخصصی نظیر هم‌اندیشی درباره الزامات قانونی هوش مصنوعی، کشاورزی هوشمند، تحلیل متن فارسی در شبکه‌های اجتماعی، حکمرانی هوش مصنوعی • وبینارهای تخصصی • دوره‌های آموزشی مانند مدرسه تابستانه هوش مصنوعی • چاپ کتاب‌ها و مقالات علمی مرتبط	• برگزاری رویدادهای تخصصی • برگزاری وبینارهای تخصصی • برگزاری دوره‌های آموزشی هوش مصنوعی • چاپ کتاب‌ها و مقالات علمی مرتبط
ایجاد شبکه ارتباطی و تعاملات گسترده برای توسعه هوش مصنوعی در کشور	• ایجاد شبکه ارتباطی و تعاملات گسترده با بازیگران کلیدی این حوزه • تعامل با سازمان ملی هوش مصنوعی، شورای عالی انقلاب فرهنگی، معاونت علمی و فناوری ریاست جمهوری • تعامل با سازمان ملی هوش مصنوعی و ... در خصوص تدوین سند نقشه راه توسعه هوش مصنوعی • تعامل با معاونت حقوقی ریاست جمهوری و مرکز پژوهش‌های مجلس در خصوص تدوین لایحه هوش مصنوعی و ...	• تعامل با بازیگران کلیدی حوزه هوش مصنوعی در موضوعات مختلف

مصاحبه

افزایش دقت هوش مصنوعی ایرانی در آزمایشگاه‌های تخصصی

رئیس پژوهشگاه ارتباطات لیلا محمدی گفت راه‌اندازی آزمایشگاه مرجع هوش مصنوعی و همکاری دانشگاه‌ها و شرکت‌های دانش‌بنیان، ارزیابی و استانداردسازی این حوزه را توسعه می‌دهد.

به گزارش روابط عمومی پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) به نقل از خبرگزاری فارس، چند روز پیش در خبرها آمد که الزامات و شاخص‌های ارزیابی مدل‌های زبانی بزرگ فارسی تدوین خواهد شد؛ این پروژه با هدف ارزیابی مدل‌های زبانی بزرگ فارسی، شناسایی نقاط ضعف، کاهش سوگیری و ارتقای امنیت و انطباق اخلاقی اجرا می‌شود. تدوین دستورالعمل جامع و معیارهای دقیق، سازگاری مدل‌ها با نیازهای بومی را بهبود داده و در توسعه توانمندی‌های ملی نقش کلیدی دارد. رئیس پژوهشگاه ارتباطات و فناوری اطلاعات لیلا محمدی در تشریح جزئیات پروژه راهبردی «تدوین الزامات و شاخص‌های ارزیابی مدل‌های زبانی بزرگ فارسی» گفت: ارزیابی مدل‌های زبانی بزرگ با شاخص‌های متعددی انجام می‌شود که به بررسی عملکرد، دقت، پوشش دانش تخصصی، همسویی با ارزش‌های اخلاقی و قانونی، ایمنی در برابر کارکردهای نامطلوب و سایر معیارهای کلیدی می‌پردازد.

شاخص‌های ارزیابی مدل‌های زبانی

رئیس پژوهشگاه ارتباطات و فناوری اطلاعات در ادامه به برخی از مهم‌ترین شاخص‌های این ارزیابی اشاره و اظهار کرد: یکی از این شاخص‌ها، دقت و صحت است که میزان انطباق پاسخ‌های مدل با داده‌های واقعی و معتبر متناسب با فرهنگ بومی را می‌سنجد. وی یکی دیگر از این شاخص‌ها را شاخص روایی دانسته و تاکید کرد: بررسی پیوستگی معنایی و دستوری متون فارسی تولیدشده در این ارزیابی دیده شده است؛ همچنین پوشش دانش تخصصی شاخص دیگری است که به ارزیابی میزان آشنایی مدل با اصطلاحات و مفاهیم تخصصی در حوزه‌هایی مانند پزشکی، حقوق و مالی می‌پردازد. محمدی استدلال و تحلیل را شاخص بعدی عنوان کرده و در توضیح آن گفت: این شاخص توانایی مدل در انجام استدلال منطقی و تحلیل داده‌های پیچیده را بررسی می‌کند. وی افزود: بی‌طرفی و کاهش سوگیری، شاخص بعدی است که میزان سوگیری‌های احتمالی در پاسخ‌ها و بررسی عدالت در خروجی‌ها را ارزیابی می‌کند. رییس پژوهشگاه ارتباطات و فناوری اطلاعات با بیان اینکه شاخص قابلیت توضیح‌پذیری، توانایی مدل در ارائه پاسخ‌هایی که منطق آن‌ها قابل تبیین و درک باشد را بررسی می‌کند، گفت: کارایی و بهینه‌بودن شاخص دیگری است که به ارزیابی سرعت پاسخ‌دهی مدل و میزان مصرف منابع محاسباتی می‌پردازد. وی پایداری

و تطبیق‌پذیری را شاخص دیگری دانسته و اظهار کرد: این شاخص به بررسی مقاومت مدل در برابر ورودی‌های مخرب و قابلیت تطبیق با داده‌های جدید می‌پردازد.

چالش‌های ارزیابی مدل‌های زبانی

رئیس پژوهشگاه ارتباطات و فناوری اطلاعات در خصوص چالش‌های ارزیابی مدل‌های زبانی گفت: با وجود اهمیت ارزیابی مدل‌های زبانی، چالش‌هایی در این مسیر وجود دارد که از جمله آن‌ها می‌توان به کمبود دادگان باکیفیت و متنوع برای آموزش و ارزیابی مدل‌ها، دشواری در تعریف سوگیری‌های زبانی و فرهنگی در مدل‌های زبانی، نیاز به هماهنگی با نهادهای مختلف علمی و صنعتی، مقیاس‌پذیری و بهینه‌سازی فرآیند ارزیابی برای مدل‌های حجیم و لزوم در نظر گرفتن جنبه‌های اخلاقی و امنیتی در طراحی معیارهای ارزیابی اشاره کرد.

همکاری دانشگاه‌ها و شرکت‌های فناوری در ارزیابی مدل‌های زبانی

محمدی ادامه داد: در این راستا، دانشگاه‌ها، شرکت‌های فناوری و استارتاپ‌های حوزه هوش مصنوعی به‌عنوان بخش‌های همکار در فرآیند ارزیابی مدل‌های زبانی بزرگ مشارکت دارند.

وی در خصوص اهداف ارزیابی مدل‌های زبانی بومی نیز تأکید کرد: ارزیابی مدل‌های زبانی بزرگ با هدف کمک به بومی‌سازی و بهینه‌سازی مدل‌های زبانی برای زبان فارسی، شناسایی نقاط ضعف مدل‌ها و بهبود کیفیت خروجی‌ها، کاهش سوگیری‌ها و خطاهای ناخواسته در مدل‌های زبانی، افزایش ایمنی، قابلیت اعتماد و انطباق با ارزش‌های فرهنگی و فراهم‌سازی چارچوبی برای مقایسه عادلانه و استانداردسازی مدل‌های بومی دنبال می‌شود.

مراحل ارزیابی مدل‌های زبانی

وی در پاسخ به این سوال که ارزیابی مدل‌های زبانی معمولاً در چند مرحله انجام می‌شود، گفت: مرحله اول ارزیابی کمی است که از معیارهای آماری مانند Perplexity و Rouge برای سنجش کیفیت مدل استفاده می‌شود.محمدی ادامه داد: مرحله دوم ارزیابی کیفی است که به بررسی خروجی مدل‌ها توسط کارشناسان زبانی و فرهنگی می‌پردازد. رئیس پژوهشگاه ارتباطات و فناوری اطلاعات چهارمین مرحله ارزیابی را تست در سناریوهای واقعی دانسته و گفت: ارزیابی عملکرد مدل‌ها در کاربردهای عملی مانند چت‌بات‌ها و سیستم‌های ترجمه در این بخش صورت می‌گیرد. وی افزود: مقایسه با مدل‌های مرجع آخرین مرحله است که به سنجش عملکرد مدل‌های بومی در برابر مدل‌های بین‌المللی مانند GPT یا Gemini می‌پردازد.

ایجاد آزمایشگاه ارزیابی مدل‌های زبانی بزرگ

رئیس پژوهشگاه ارتباطات و فناوری اطلاعات ادامه داد: این فعالیت‌ها در چارچوب آزمایشگاه مرجع ارزیابی محصولات و خدمات پایه هوش مصنوعی انجام شده است. این آزمایشگاه که در پژوهشگاه ارتباطات و فناوری اطلاعات مستقر است، شبکه‌ای از آزمایشگاه‌های ارزیابی در حوزه‌های مختلف را توسعه داده و از توانمندی آزمایشگاه‌های دانشگاهی و ظرفیت شرکت‌های دانش‌بنیان در فرآیند ارزیابی و تدوین معیارهای سنجش استفاده می‌کند.

محمدی گفت: این شبکه علاوه بر مدل‌های زبانی بزرگ، ارزیابی سایر فناوری‌های هوش مصنوعی مانند سامانه‌های بازشناسی چهره، تشخیص پلاک خودرو، سامانه‌های نویسه‌خوان نوری (OCR) و سایر خدمات پایه هوش مصنوعی را نیز پوشش خواهد داد.

وی در پایان خاطرنشان کرد: اقدامات انجام‌شده در راستای افزایش اعتبار، شفافیت و کیفیت محصولات هوش مصنوعی بومی بوده و بستری برای توسعه و بهبود فناوری‌های هوش مصنوعی در کشور فراهم خواهد کرد.

راه‌اندازی آزمایشگاه مرجع ارزیابی محصولات و خدمات پایه هوش مصنوعی

به همت پژوهشگاه ارتباطات و فناوری اطلاعات انجام شد

رئیس آزمایشگاه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات از راه‌اندازی آزمایشگاه مرجع ارزیابی محصولات و خدمات پایه هوش مصنوعی در کشور خبر داد.

به گزارش روابط عمومی پژوهشگاه ارتباطات و فناوری اطلاعات مژگان فرهودی، درمصاحبه ای در خصوص ضرورت راه‌اندازی آزمایشگاه مرجع ارزیابی محصولات و خدمات پایه، اظهار داشت: در دنیای امروز هوش مصنوعی به حوزه‌های بسیاری مانند سلامت و پزشکی، کشاورزی، هوافضا، تسلیحات نظامی، بانکداری و آموزش وارد شده است. برخی از محصولات و خدمات ارائه شده در این حوزه‌ها، دارای کارکردهای عادی و روزمره و برخی دیگر دارای کارکردهای حیاتی و مهم هستند؛ لذا ضرورت وجود آزمایشگاه ملی هوش مصنوعی به‌عنوان یک نهاد ارزیاب و صحه‌گذاری که بتواند مطابق با شاخص‌ها و معیارهای مرسوم و با نگاه به اهداف و اولویت‌های کشور، محصولات و خدمات هوش مصنوعی را مورد بررسی و ارزیابی قرار دهد از اهمیت بالایی برخوردار است.

وی افزود: ارزیابی‌های انجام شده در این آزمایشگاه همچنین می‌تواند با شناسایی نقاط قوت و ضعف محصول یا خدمت موردنظر به فرایند توسعه آن کمک کند. از طرفی این آزمایشگاه جهت حل چالش‌های حوزه هوش مصنوعی محصولات و خدمات بومی در کشور به عنوان حلقه واسط میان صنعت و پژوهشگران داخلی عمل کرده تا از این طریق بتواند ضمن شناسایی افراد توانمند و خبره در این حوزه و با بهره‌گیری از ایده‌های خلاق آنها در یک فضای رقابتی سالم به حل مسائل و چالش‌های واقعی محصولات و خدمات هوش مصنوعی در کشور بپردازد.

رئیس آزمایشگاه هوش مصنوعی با بیان اینکه خدمات این آزمایشگاه به دو دسته کلان تقسیم می‌شوند، گفت: خدمات اصلی این آزمایشگاه، ارزیابی و سطح‌بندی محصولات و خدمات پایه هوش مصنوعی در حوزه‌های

کاربـردی مختلـف از جملـه امنیـت، کشـاورزی، سـلامت و غیـره باهـدف تأییـد نمونـه و ارائـه گواهـی بـه آن‌هـا، ارزیابـی و رتبه‌بنـدی ابزارهـا، مدل‌هـا، الگوریتم‌هـای هـوش مصنوعـی باهـدف تقویـت زیرسـاخت‌های فنـی و رفـع چالش‌هـای حـوزه هـوش مصنوعـی محصـولات و خدمـات بومـی و همچنیـن کمـک بـه توسـعه‌دهندگان در مسـیر فراینـد توسـعه محصـولات و خدمـات هـوش مصنوعـی بـا انجـام ارزیابی‌هـای مربوطـه و ارائـه گزارش‌هـا ارزیابـی و شناسـایی نقـاط ضعـف و قـوت آن‌هـا اسـت.

دکتـر مژگان فرهـودی تأکیـد کـرد: بخـش دیگـر خدمـات آزمایشـگاه، خدمـات جانبـی اسـت کـه مربـوط بـه تعریـف و حـل مسـائل و چالش‌هـای حـوزه دادگان و مدل‌هـای هـوش مصنوعـی از طریـق بسـتر جمع‌سـپاری، ارائـه API خدمـات مختلـف هـوش مصنوعـی توسـعه داده شـده در آزمایشـگاه، آزادسـازی مسـتندات و دادگان تولیـد شـده در آزمایشـگاه باهـدف ارتقـای حـوزه پژوهشـی و توسـعه‌ای حـوزه هـوش مصنوعـی در کشـور اسـت.

وی گفـت: خدمـات ایـن آزمایشـگاه در راسـتای صحه‌گـذاری و پیشـرفت سـطح فنـی محصـولات و خدمـات هـوش مصنوعـی ارائـه می‌شـود. ایـن آزمایشـگاه در کنـار مقولـه رگولاتـوری نقـش اساسـی در اسـتقرار هـوش مصنوعـی اعتمادپذیـر در کشـور دارد.

رئیـس آزمایشـگاه هـوش مصنوعـی پژوهشـگاه ارتباطـات و فنـاوری اطلاعـات دربـاره هـوش مصنوعـی اعتمادپذیـر افـزود: هـوش مصنوعـی اعتمادپذیـر مفهومـی بنیادیـن و اساسـی در حـوزه هـوش مصنوعـی بـوده کـه اسـاس به‌کارگیـری هـوش مصنوعـی در سـطح عمومـی در کشورهاسـت. امـروزه کشـورهای پیشـرفته در هـوش مصنوعـی تحقیقـات گسـترده‌ای را انجـام می‌دهنـد. ایـن مفهـوم بـا در نظـر گرفتـن معیارهایـی نظیـر مسـئولیت‌پذیری، حریـم خصوصـی، امنیـت، منصفانـه بـودن و غیـره سـعی در کاهـش مخاطـرات و ریسـک به‌کارگیـری هـوش مصنوعـی در سـطح عمومـی دارد. بنیـان آزمایشـگاه ارزیابـی محصـولات و خدمـات هـوش مصنوعـی نیـز بـر اسـاس هـوش مصنوعـی اعتمادپذیـر اسـت.

فرهـودی دربـاره نحـوه تعامـل آزمایشـگاه بـا مراکـز آزمایشـگاهی فعال کشـور در هـوش مصنوعی تأکیـد کـرد: آزمایشـگاه مرجـع ارزیابـی محصـولات و خدمـات هـوش مصنوعـی در پژوهشـگاه ارتباطـات و فنـاوری اطلاعـات کـه بـا همـکاری سـازمان فنـاوری اطلاعـات راه‌انـدازی شـده اسـت، قصـد دارد به‌منظـور توسـعه شـبکه آزمایشـگاهی خـود از ظرفیت‌هـای موجـود در داخـل کشـور اسـتفاده کنـد و بدیـن منظـور آمـاده همـکاری بـا تمامـی دانشـگاه‌ها، مؤسسـات پژوهشـی، شـرکت‌های خصوصـی و دولتـی فعـال در حـوزه ارزیابـی محصـولات و خدمـات هـوش مصنوعـی اسـت.

وی گفـت: در اولیـن گام طـی فراخوانـی کـه بـه‌زودی اعـلام می‌شـود از تمامـی آزمایشـگاه‌های دانشـگاهی، خصوصـی و دولتـی کـه می‌تواننـد نقـش مؤثـری در گسـترش ایـن شـبکه آزمایشـگاهی داشـته باشـند، دعـوت بـه همـکاری خواهـد شـد. بعـد از بررسـی رزومـه و احـراز صلاحیـت مراکـز آزمایشـگاهی، گواهـی رسـمی فعالیـت در حـوزه ارزیابـی محصـولات و خدمـات هـوش مصنوعـی از طـرف سـازمان فنـاوری اطلاعـات بـه ایـن آزمایشـگاه‌ها اعطـا شـده و ایـن مراکـز به‌عنـوان همـکار و بال‌هـای اجرایـی آزمایشـگاه تحت نظـارت آزمایشـگاه مرجـع بـه فعالیـت و ارائـه خدمـات ارزیابـی خواهنـد پرداخـت.

گفت‌وگو

معرفی برنامه پژوهشگاه ارتباطات و فناوری اطلاعات در حوزه هوش مصنوعی

تأمین زیرساخت‌های هوش مصنوعی از فعالیت‌های کلیدی پژوهشگاه ICT است

گفت‌وگوی رئیس مرکز نوآوری و توسعه هوش مصنوعی با ماهنامه پیوست

در حالی که هوش مصنوعی به یکی از مهم‌ترین حوزه‌های فناوری در جهان تبدیل شده است، نقش نهادهای نظارتی در تضمین کیفیت و استانداردسازی محصولات این حوزه بیش از پیش اهمیت یافته است. در کشور متولی‌های مختلفی فعالیت‌های این حوزه را پیگیری می‌کنند. مرکز نوآوری و توسعه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات، قدیمی‌ترین نهاد حاکمیتی کشور در حوزه هوش مصنوعی است که از سال ۱۳۹۹ آغاز به کار کرده است.

به گزارش روابط عمومی پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)؛ محمد هادی بکایی، رئیس مرکز توسعه هوش مصنوعی پژوهشگاه ارتباطات، به بررسی مأموریت‌ها، چالش‌ها و انتظارات از حاکمیت در این حوزه پرداخت.

مسئولیت‌های مرکز توسعه و نوآوری هوش مصنوعی چه تفاوتی با سایر مراکز هوش مصنوعی دارد؟

مسئولیت‌های مرکز نوآوری و توسعه هوش مصنوعی در مقایسه با سایر مراکز هوش مصنوعی، از چند جهت متمایز است. این مرکز مأموریت‌های گسترده‌ای دارد که شامل توسعه زیرساخت‌ها و منابع هوش مصنوعی، پیشبرد کاربردهای نوین این فناوری، توسعه علمی و پژوهشی در حوزه هوش مصنوعی، استقرار مرجعیت رگولاتوری و حقوقی، گسترش تعاملات بین‌المللی و ترویج نوآوری در این حوزه می‌شود. علاوه بر این، مرکز به‌عنوان مشاوری کلیدی در اجرایی‌سازی تحول دیجیتال با محوریت هوش مصنوعی در نهادهای حاکمیتی عمل می‌کند.

یکی از اصلی‌ترین وظایف این مرکز، ارزیابی و آزمایش محصولات هوش مصنوعی است. مرکز توسعه و نوآوری هوش مصنوعی به‌عنوان مرجعی معتبر در کشور، مسئولیت ارزیابی محصولات هوش مصنوعی را بر عهده دارد. آزمایشگاه مرجع این مرکز، فرآیند ارزیابی محصولات را با استفاده

از مجموعه داده‌های تخصصی و مدل‌های مرتبط با هر حوزه انجام می‌دهد. این ارزیابی‌ها بر اساس معیارهای دقیق و متناسب با کاربردهای مشخص تعریف شده‌اند. هدف اصلی از ایجاد این آزمایشگاه، بررسی و ارزیابی محصولات توسعه‌یافته در حوزه هوش مصنوعی است تا در صورت نیاز به استفاده در سطح کلان، مشخص شود کدام محصول برای کدام شرکت یا کاربرد خاص، کارآمدتر است. این فرآیند نه‌تنها به بهبود کیفیت محصولات کمک می‌کند، بلکه باعث انتخاب و استفاده بهینه از آن‌ها را نیز تسهیل می‌شود. به‌عنوان یک نهاد حاکمیتی این مرکز تمرکز خود را بر نظارت و ارزیابی و ایجاد بنچمارک‌های استاندارد قرار داده و از ورود مستقیم به توسعه محصولات خودداری می‌کند.

انتظارات از حاکمیت در این بخش شامل چه مواردی است؟

در مرحله اول، تمرکز اصلی بر حمایت از بخش خصوصی و تسهیل فرآیند توسعه محصولات هوش مصنوعی است. این حمایت‌ها شامل ارائه دادگان (دیتاست‌های) استاندارد، توسعه بنچمارک‌های معتبر و ایجاد زیرساخت‌های لازم برای ارزیابی محصولات است. شرکت‌ها با استفاده از این ابزارها می‌توانند کیفیت محصولات خود را در تراز جهانی ارزیابی کنند، نقاط قوت و ضعف خود را شناسایی نمایند و در جهت بهبود و تقویت محصولات خود گام بردارند.

این نقش بر عهده آزمایشگاه هوش مصنوعی مرکز است؟

در این مرحله، نقش آزمایشگاه مرجع هوش مصنوعی بیشتر تسهیل‌گرانه و حمایتی است. این مرکز با توسعه دادگان استاندارد و بنچمارک‌ها در حوزه‌های مختلف، به شرکت‌ها کمک می‌کند تا محصولات خود را با دقت بیشتری آزمایش و بهبود دهند. این رویکرد نه‌تنها به رشد و توسعه بخش خصوصی کمک می‌کند، بلکه کیفیت محصولات هوش مصنوعی را در سطح ملی ارتقا می‌دهد. حمایت حاکمیت در این زمینه می‌تواند شامل تأمین منابع مالی، کاهش هزینه‌های ارزیابی، و ایجاد بسترهای قانونی و فنی لازم باشد.

در کنار این حمایت‌ها، موضوع امنیت و کیفیت دادگان هم اهمیت زیادی دارد. به‌ویژه در کاربردهای حساس مانند تشخیص چهره، هرگونه خطا می‌تواند تبعات جدی به همراه داشته باشد. بنابراین، دادگان مورد استفاده در ارزیابی‌ها باید از نظر امنیتی قابل‌اعتماد و از نظر کیفیت تضمین‌شده باشند. این امر نیازمند همکاری نزدیک بین حاکمیت، بخش خصوصی و مراکز تحقیقاتی است.

پس از شکل‌گیری یک زیست‌بوم پایدار هوش مصنوعی در کشور، نقش نظارتی حاکمیت پررنگ‌تر می‌شود. در این مرحله، حاکمیت می‌تواند با تعیین استانداردها و قوانین لازم، اطمینان حاصل کند که محصولات هوش مصنوعی از نظر امنیتی و کیفیتی در سطح مطلوبی قرار دارند. این نظارت باید به‌گونه‌ای باشد که هم از منافع عمومی محافظت کند و هم مانع رشد و نوآوری در بخش خصوصی نشود.

یعنی حاکمیت وارد امور اجرائی می‌شود؟

به‌طور خلاصه، انتظارات از حاکمیت در این حوزه شامل حمایت از بخش خصوصی در مراحل اولیه توسعه، تسهیل دسترسی به دادگان

و زیرساخت‌های لازم و در نهایت نظارت بر کیفیت و امنیت محصولات پس از شکل‌گیری زیست‌بوم پایدار هوش مصنوعی است. این رویکرد متوازن به رشد پایدار و ایمن فناوری هوش مصنوعی در کشور کمک خواهد کرد.

سند ملی هوش مصنوعی که از طرف پژوهشگاه تهیه شد، به نظر شما چه نقاط قوت و ضعف‌هایی داشت؟

سند هوش مصنوعی که توسط پژوهشگاه ارتباطات و فناوری اطلاعات تهیه شده است، نقاط قوت و ضعف‌هایی دارد که به‌طور خلاصه به آن‌ها می‌پردازیم. این سند که در سال ۱۴۰۰ تدوین و در سال ۱۴۰۲ به‌روزرسانی شد، هر چند در سطح ملی تصویب نهایی نشد اما بخش‌های قابل‌توجهی از آن در سند ملی هوش مصنوعی مصوب شورای عالی انقلاب فرهنگی و همچنین در تدوین برنامه ملی هوش مصنوعی مورد استفاده قرار گرفته است. یکی از نقاط قوت این سند، ایجاد چارچوبی روشن برای هماهنگی و هم‌افزایی بین نهادهای مختلف در حوزه هوش مصنوعی است. این سند با نگاشت نهادی دقیق، نقش‌ها و مسئولیت‌های هر بخش را مشخص کرده و زمینه را برای همکاری‌های بین‌سازمانی فراهم می‌کند.

از جمله اقدامات مثبت مبتنی بر این سند، تهیه لایحه هوش مصنوعی با رویکرد تسهیل‌گری و تدوین نظام‌نامه‌های فنی و استانداردسازی در این حوزه است. پژوهشگاه به‌عنوان متولی استانداردسازی هوش مصنوعی از سوی سازمان ملی استاندارد شناخته شده و نقش دبیرخانه کمیته زیرمجموعه هوش مصنوعی ایزو در ایران را نیز بر عهده دارد. این موقعیت به ایران این امکان را می‌دهد تا در تدوین استانداردهای بین‌المللی مشارکت فعال داشته باشد و از تحمیل استانداردهای خارجی که لزوماً با نیازهای ملی همخوانی ندارند جلوگیری کند.

شما قبلا گفته بودید سند باید در حین اجرا اصلاح شود.

یکی از نقاط ضعف این سند و در کل سند ملی هوش مصنوعی، کندی در اجرای برخی از اقدامات پیش‌بینی‌شده است. اگرچه گام‌های ابتدایی بر اساس این اسناد برداشته شده، اما بسیاری از برنامه‌ها هنوز به‌طور کامل عملیاتی نشده‌اند. این موضوع می‌تواند به دلیل چالش‌های ساختاری، کمبود منابع یا نیاز به هماهنگی بیشتر بین نهادهای مرتبط باشد.

در برنامه هفتم توسعه نیز وزارت ارتباطات به‌عنوان

متولی تأمین زیرساخت‌های لازم برای توسعه اقتصاد دیجیتال و هوش مصنوعی تعیین شده است. پژوهشگاه در این راستا اقدامات عملیاتی را آغاز کرده و نقش فعالی ایفا می‌کند. با این حال، برای تحقق کامل اهداف سند، نیاز به تسریع در اجرای برنامه‌ها و رفع موانع پیش‌رو وجود دارد. به‌طور کلی، سند ملی هوش مصنوعی چارچوب مناسبی برای توسعه این فناوری در کشور فراهم کرده است، اما موفقیت کامل آن منوط به اجرای به‌موقع و هماهنگ برنامه‌ها و رفع چالش‌های موجود است.

برنامه ملی هوش مصنوعی در چه مرحله‌ای است؟

برنامه ملی هوش مصنوعی در حال حاضر در مراحل پایانی تدوین و تصویب قرار دارد. برای درک بهتر وضعیت این برنامه، ابتدا لازم است تفاوت بین سند ملی هوش مصنوعی و برنامه ملی هوش مصنوعی را توضیح دهیم. سند ملی هوش مصنوعی به کلیات این حوزه از جمله چشم‌انداز، اهداف کلان، و اقدامات استراتژیک می‌پردازد. در حالی که برنامه ملی هوش مصنوعی بر اساس اهداف تعیین‌شده در سند ملی، اقدامات عملیاتی، نگاشت نهادی را انجام داده و مسئولیت‌های هر سازمان را به‌طور دقیق مشخص می‌کند. به عبارت دیگر، برنامه ملی نقشه راه اجرایی برای تحقق اهداف سند ملی است.

در این راستا، سازمان‌های مختلفی برنامه‌های خود را برای توسعه هوش مصنوعی ارائه داده‌اند. از میان این برنامه‌ها، اسناد تهیه‌شده توسط سازمان ملی هوش مصنوعی و مرکز نوآوری و توسعه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات به‌عنوان کامل‌ترین و جامع‌ترین برنامه‌ها شناخته شده‌اند. این اسناد با در نظر گرفتن نیازهای ملی و تجربیات بین‌المللی، چارچوب مناسبی برای توسعه هوش مصنوعی در کشور فراهم کرده‌اند.

در ادامه، با برگزاری جلسات متعدد و با حضور دستگاه‌های ذی‌ربط، برنامه‌های ارائه‌شده توسط سازمان‌های مختلف با یکدیگر ادغام شده‌اند. این ادغام با هدف پوشش نقاط قوت و رفع نقاط ضعف هر برنامه انجام شده است تا در نهایت یک برنامه ملی منسجم و کارآمد تهیه شود. این فرآیند مشارکتی باعث شده است که برنامه ملی هوش مصنوعی از نظر جامعیت و عملیاتی بودن به سطح مطلوبی برسد.

این برنامه در حال اجرا است؟

در حال حاضر، این برنامه مراحل نهایی تصویب خود را طی می‌کند. امیدواریم ظرف هفته‌های

آینده و قبل از پایان سال این فرآیند به نتیجه برسد و برنامه ملی هوش مصنوعی به‌طور رسمی تصویب و ابلاغ شود. با تصویب این برنامه، کشور جهت مشخصی برای توسعه هوش مصنوعی پیدا خواهد کرد و منابع لازم نیز به‌طور مناسب تخصیص خواهد یافت. این اتفاق می‌تواند نقطه عطفی در پیشبرد اهداف ملی در حوزه هوش مصنوعی و تبدیل ایران به یکی از بازیگران اصلی این فناوری در سطح منطقه و جهان باشد.

آیا طرح هوش مصنوعی مجلس هم در راستای رویکرد اجرایی مثل سند تدوین شده است؟

طرح هوش مصنوعی که در مجلس تدوین می‌شود بیشتر بر تعیین جایگاه هریک از مراکز متمرکز است. این طرح که در مرکز پژوهش‌های مجلس در دست تدوین است و با تمرکز بر تعیین جایگاه سازمان ملی هوش مصنوعی و وظایف دستگاه‌های مرتبط مانند وزارت ارتباطات، وزارت امور خارجه و معاونت علمی ریاست جمهوری، با چالش‌های متعددی روبه‌رو است. به عنوان یک طرح که قرار است به قانون تبدیل شود، ایرادات متعددی به آن وارد شده که هم‌اکنون در حال جمع‌بندی و بازنگری است.

تأخیر در اجرای پروژه به دلیل نبود رگولاتوری است یا نبود زیرساخت مانع شده است؟

تأخیر در اجرای پروژه‌های حوزه هوش مصنوعی را می‌توان به دو عامل اصلی نسبت داد؛ نبود زیرساخت‌های اساسی و چالش‌های مرتبط با رگولاتوری و هماهنگی بین‌دستگاهی. این دو موضوع در کنار هم باعث شده‌اند که پیشرفت در این حوزه به‌طور کامل محقق نشود.

در مورد زیرساخت‌ها، باید گفت که دسترسی به داده‌های باکیفیت، منابع محاسباتی قدرتمند، و شبکه‌های ارتباطی پیشرفته از ضروریات توسعه هوش مصنوعی هستند. بدون این زیرساخت‌ها، حتی با وجود برنامه‌ریزی‌های دقیق، اجرای پروژه‌ها با دشواری مواجه می‌شود. وزارت ارتباطات و فناوری اطلاعات به‌عنوان یکی از بازیگران اصلی در این حوزه، تلاش کرده است تا با پروژه‌هایی مانند ایجاد ابر دولت، قطب‌های مراکز داده و سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات بخشی از این نیازها را برطرف کند؛ با این حال، هنوز جای کار بیشتری وجود دارد و تأمین کامل زیرساخت‌ها نیازمند همکاری و سرمایه‌گذاری بیشتر است.

از سوی دیگر، چالش‌های رگولاتوری و هماهنگی بین‌دستگاهی نیز نقش مهمی در این تأخیرها داشته‌اند. اختلافات و عدم انسجام بین نهادهای مرتبط باعث تأخیر در تخصیص بودجه و تعیین نقش‌های مشخص برای هر نهاد شده است. این موضوع به ویژه در حوزه‌هایی که نیازمند همکاری چندین سازمان هستند، مانند استانداردسازی و رگولاتوری، مشهود است. برای مثال، تدوین قوانین و مقرراتی که بتواند به‌طور هماهنگ نیازهای بخش‌های مختلف را پوشش دهد، هنوز به نتیجه نهایی نرسیده است.

وزارت ارتباطات می‌تواند این نقش را داشته باشد؟

وزارت ارتباطات و فناوری اطلاعات به‌عنوان یکی از نهادهای کلیدی در توسعه زیست‌بوم هوش مصنوعی، نقش مهمی در پیشبرد این حوزه ایفا می‌کند. این وزارتخانه با تمرکز بر پروژه‌های زیرساختی و تسهیل‌گری، تلاش کرده تا بستر

لازم برای رشد هوش مصنوعی را فراهم کند. با این حال، موفقیت کامل این تلاش‌ها منوط به همکاری و هماهنگی بیشتر بین سایر نهادهای مرتبط است. بدون تعریف دقیق نقش‌ها و مسئولیت‌ها، و همچنین تخصیص به‌موقع بودجه‌های موردنیاز، پیشرفت در این حوزه کند خواهد بود.

برای رفع این چالش‌ها، نیاز به اقدامات عملی داریم. اولاً، هر نهاد باید مسئولیت‌های خود را به‌طور شفاف بداند و از موازی‌کاری جلوگیری شود. ثانیاً، ایجاد مکانیزم‌های هماهنگی مؤثر بین نهادهای مختلف برای تسریع در تصمیم‌گیری و اجرای پروژه‌ها ضروری است. ثالثاً، سرمایه‌گذاری بیشتر در زیرساخت‌های اساسی مانند داده‌های باکیفیت، منابع محاسباتی، و شبکه‌های ارتباطی باید در اولویت قرار گیرد. و در نهایت، تدوین و تصویب سریع‌تر قوانین و مقرراتی که بتواند به‌طور جامع نیازهای حوزه هوش مصنوعی را پوشش دهد، از اهمیت بالایی برخوردار است.

در نهایت، برای دستیابی به پیشرفت قابل‌توجه در حوزه هوش مصنوعی، هم‌زمانی تأمین زیرساخت‌ها و بهبود هماهنگی بین‌دستگاهی ضروری است. این دو عامل در کنار هم می‌توانند زمینه را برای اجرای موفقیت‌آمیز پروژه‌های هوش مصنوعی فراهم کنند.

تأمین زیرساخت در چه بخش‌هایی بر عهده وزارت ارتباطات است؟

تأمین زیرساخت‌های لازم برای توسعه هوش مصنوعی یکی از مسئولیت‌های کلیدی ما و وزارت ارتباطات است. این زیرساخت‌ها شامل چند بخش اصلی می‌شود که هر کدام از اهمیت بالایی برخوردارند. یکی از محورهای کلیدی، تأمین زیرساخت‌های پردازشی سریع و ایجاد دیتاسنترهای مستقل است. این دیتاسنترها به‌عنوان پایه‌ای برای استقلال فناورانه در حوزه هوش مصنوعی عمل می‌کنند و باید با برنامه‌ریزی دقیق و مؤثر تقویت شوند. بدون این زیرساخت‌ها، حتی پیشرفته‌ترین الگوریتم‌ها و مدل‌های هوش مصنوعی نیز نمی‌توانند به‌طور کامل به کار گرفته شوند.

اما این زیرساخت‌ها بیشتر سخت‌افزاری است که تهیه آن‌ها چالش‌های خاص خود را دارد.

یکی از چالش‌های مهمی که در بسیاری از اسناد و برنامه‌ها نادیده گرفته شده، فقدان برنامه‌ریزی برای ورود به حوزه طراحی و ساخت تراشه‌ها (چیپ‌ست‌ها) است. با وجود اسنادی مانند سند ابررسانه و سند نیمه‌هادی‌ها، حوزه هوش مصنوعی نیازمند یک مسیر مشخص برای ورود به این صنعت حیاتی است. این مسیر باید شامل برنامه‌ریزی برای خرید ادوات مرتبط با لیتوگرافی و در بلندمدت توسعه توانمندی‌های داخلی در طراحی و ساخت تراشه‌ها باشد. بدون این اقدامات، وابستگی به واردات همچنان باقی می‌ماند و استقلال فناورانه در این حوزه تحقق نخواهد یافت.

البته ساخت تراشه نیاز به فناوری‌های پیشرفته‌ای دارد و این مسیر چالش‌های خاص خود را دارد. اما تجربه‌های مشابه در حوزه‌هایی مانند صنعت هسته‌ای نشان داده که دستیابی به توانمندی‌های تولید مستقل، حتی در سطوح اولیه، می‌تواند زمینه‌ساز پیشرفت‌های بزرگ‌تر و باز شدن درهای جدید در صنایع مختلف باشد.

بنابرایـن، برنامه‌ریـزی بـرای دسـتیابی بـه فناوری‌هـای عمیـق و اسـتقلال در تولیـد زیرسـاخت‌های هـوش مصنوعـی، بایـد بخشـی از اسـتراتژی کلان کشـور باشـد. در ایـن مسـیر، بایـد از ظرفیـت دانشـگاه‌ها و مراکـز تحقیقاتـی بـه نحـو احسـن اسـتفاده شـود.

ما در حال حاضر در حوزه میکروالکترونیک افراد برجسته‌ای داریم که در سطح بین‌المللی صاحب‌نظر هستند. به عنوان مثال، دانشگاه شریف چندین استاد هیئت علمی دارد که در این حوزه جزو نخبگان جهانی محسوب می‌شوند. اما با شرایط فعلی، نمی‌توان خوش‌بین بود که بدون تغییرات اساسی در تأمین منابع، به موفقیت قابل‌توجهی دست پیدا کنیم. کشورهایی مانند مالزی، کره جنوبی و حتی روسیه در حال ورود و تقویت جایگاه خود در این صنعت هستند و ما نیز باید با برنامه‌ریزی دقیق به این مسیر ورود کنیم. با همکاری این کشورها و استفاده از رویکرد فبلس (Fabless manufacturing)، می‌توانیم به تولید نمونه‌های اولیه برسیم و گام‌های اولیه را برای کاهش وابستگی برداریم.

اگر هدف ما دستیابی به استقلال فناورانه در این حوزه است، باید ابتدا به تأمین زیرساخت‌های اساسی بپردازیم. حتی اگر بخواهیم در لایه‌های بالاتر و نرم‌افزاری فعالیت کنیم و برای مثال مدل‌های پایه (Foundation Models) را توسعه دهیم، به زیرساخت‌های قدرتمندی نیاز داریم. بدون تأمین این منابع، حتی در صورت خرید فناوری‌های پیشرفته نیز وابستگی ما به واردات و تحریم‌ها باقی خواهد ماند. برای رسیدن به لایه‌های عمیق‌تر فناوری، باید برنامه‌ریزی کنیم تا علاوه بر درک تکنولوژی، به مرحله ساخت و تولید نیز ورود کنیم.

در نهایت، تأمین زیرساخت‌های لازم برای توسعه هوش مصنوعی نیازمند همکاری بین‌دستگاهی، برنامه‌ریزی بلندمدت، و سرمایه‌گذاری هدفمند است. این اقدامات نه‌تنها به رشد فناوری هوش مصنوعی کمک می‌کند، بلکه زمینه را برای دستیابی به استقلال فناورانه و کاهش وابستگی به خارج فراهم می‌کند.

پژوهشگاه در این موضوع چه نقشی را ایفا می‌کند؟

پژوهشگاه ارتباطات و فناوری اطلاعات به‌عنوان بازوی تحقیق و توسعه وزارت ارتباطات، نقش کلیدی در توسعه زیرساخت‌های حوزه هوش مصنوعی ایفا می‌کند. یکی از اصلی‌ترین وظایف پژوهشگاه، طراحی و نظارت بر زیرساخت‌های فناوری اطلاعات و ارتباطات است که برای توسعه هوش مصنوعی ضروری هستند. این شامل مطالعات مکان‌یابی قطب‌های مراکز داده، تأمین تجهیزات مرتبط، و ایجاد بسترهای لازم برای حمایت مالی دولت از پروژه‌های زیرساختی است.

به‌عنوان مثال، ابررایانه سیمرغ، که یکی از بزرگ‌ترین و پیشرفته‌ترین پروژه‌های کشور در حوزه پردازش‌های سریع است، با نظارت و مدیریت پژوهشگاه توسعه یافته است. این پروژه نشان‌دهنده توانمندی پژوهشگاه در طراحی و اجرای پروژه‌های پیچیده و زیرساختی است. پژوهشگاه با استفاده از تجربه و تخصص خود، توانسته است در ترمیم و تقویت زیرساخت‌های مرتبط با مراکز داده و پردازش‌های سریع نقش مؤثری ایفا کند.

در حوزه‌هایی مانند میکروالکترونیک، ممکن است نقش پژوهشگاه کمرنگ‌تر به نظر برسد، چرا که این حوزه نیازمند تخصص‌های بسیار پیشرفته و مشارکت بخش‌های تخصصی دیگر است. با این حال، پژوهشگاه می‌تواند به‌عنوان هماهنگ‌کننده و تسهیل‌گر، بین نهادهای مختلف ارتباط برقرار کند و از ظرفیت‌های موجود در دانشگاه‌ها و مراکز تحقیقاتی بهره‌برداری نماید. برای مثال، پژوهشگاه می‌تواند با همکاری دانشگاه‌های برتر کشور، مانند دانشگاه شریف که دارای اساتید برجسته در حوزه میکروالکترونیک هستند، پروژه‌های مشترکی را تعریف و اجرا کند.

برای تحقق این اهداف، تأمین منابع مالی کافی در سطح ملی ضروری است. این موضوع نیازمند یک ناظر مرکزی است که بتواند تمامی این اقدامات را منسجم کند و از پراکندگی جلوگیری کند. به نظر می‌رسد وجود یک سازمان ملی با نقش نظارتی و سیاست‌گذاری می‌تواند راه‌حل مناسبی باشد. این سازمان باید مسئولیت انسجام‌بخشی به تلاش‌ها، تأمین

منابع مالی، و راهبری زیست‌بوم هوش مصنوعی را بر عهده بگیرد. پژوهشگاه می‌تواند به‌عنوان بازوی فنی و تحقیقاتی این سازمان، در طراحی و اجرای پروژه‌ها نقش فعالی ایفا کند.

در نهایت، پژوهشگاه ارتباطات و فناوری اطلاعات با استفاده از توانمندی‌های خود در حوزه تحقیق و توسعه، می‌تواند به‌عنوان یکی از بازیگران اصلی در توسعه زیرساخت‌های هوش مصنوعی عمل کند. این نقش نه‌تنها شامل طراحی و نظارت بر پروژه‌های زیرساختی است، بلکه هماهنگی بین نهادهای مختلف و استفاده از ظرفیت‌های داخلی را نیز در بر می‌گیرد. با حمایت‌های لازم و همکاری بین‌دستگاهی، پژوهشگاه می‌تواند به‌عنوان موتور محرکه توسعه هوش مصنوعی در کشور عمل کند.

آیا تعدد مراکز در حوزه هوش مصنوعی در ساختار حاکمیتی نیاز است؟

سوال بسیار مهمی است. وقتی صحبت از تعدد مراکز در سطح حاکمیتی در حوزه هوش مصنوعی می‌شود، باید به این نکته توجه کنیم که این مراکز نقش‌های کلیدی در سیاست‌گذاری، نظارت، و هدایت این حوزه دارند. در حال حاضر، نهادهای مختلفی مانند شورای عالی انقلاب فرهنگی، شورای عالی فضای مجازی، معاونت علمی و فناوری ریاست جمهوری، و وزارت ارتباطات و فناوری اطلاعات هر کدام به نوعی درگیر موضوع هوش مصنوعی هستند. این تعدد مراکز حاکمیتی هم نقاط قوت دارد و هم نقاط ضعف.

از یک طرف، وجود نهادهای مختلف می‌تواند به تخصصی‌تر شدن فعالیت‌ها در حوزه‌های مختلف هوش مصنوعی کمک کند. برای مثال، یک نهاد ممکن است روی سیاست‌گذاری‌های کلان و تنظیم مقررات تمرکز کند، در حالی که نهاد دیگر بر روی توسعه زیرساخت‌ها یا حمایت از نوآوری‌ها متمرکز شود. این تقسیم وظایف می‌تواند به پیشرفت سریع‌تر در هر حوزه منجر شود.

اما از طرف دیگر، اگر این نهادها هم‌پوشانی زیادی در وظایف داشته باشند یا بدون هماهنگی فعالیت کنند، می‌توانند باعث موازی‌کاری، پراکندگی منابع، و کندی در پیشرفت‌ها شوند. متأسفانه، تا حدودی این اتفاق در حال حاضر نیز رخ داده است. نهادهای مختلف گاهی اوقات سیاست‌ها و برنامه‌های مشابهی را دنبال می‌کنند یا درگیر رقابت‌های داخلی می‌شوند که این موضوع به جای پیشرفت، باعث هدررفت منابع و زمان می‌شود.

در اینجا نقش یک سازمان ملی هوش مصنوعی که تحت نظر ریاست جمهوری فعالیت کند، بسیار حیاتی است. این سازمان باید به‌عنوان ناظر و راهبر اصلی حوزه هوش مصنوعی عمل کند. وظیفه این سازمان تعیین چارچوب‌ها، سیاست‌ها، و اولویت‌های ملی است تا از موازی‌کاری جلوگیری شود و منابع به‌طور بهینه تخصیص یابند. این سازمان باید اطمینان حاصل کند که هر نهاد در حوزه تخصصی خود فعالیت می‌کند و هماهنگی لازم بین نهادهای مختلف وجود دارد.

به‌علاوه، این سازمان می‌تواند به‌عنوان نماینده حاکمیت، نقش هماهنگ‌کننده بین نهادهای مختلف را ایفا کند و از ایجاد رقابت‌های بی‌ثمر جلوگیری کند. برای مثال، می‌تواند با تعریف پروژه‌های کلان و تقسیم وظایف بین نهادها، مانع هدررفت منابع شود و هم‌زمان از تخصص هر نهاد به بهترین شکل استفاده کند.

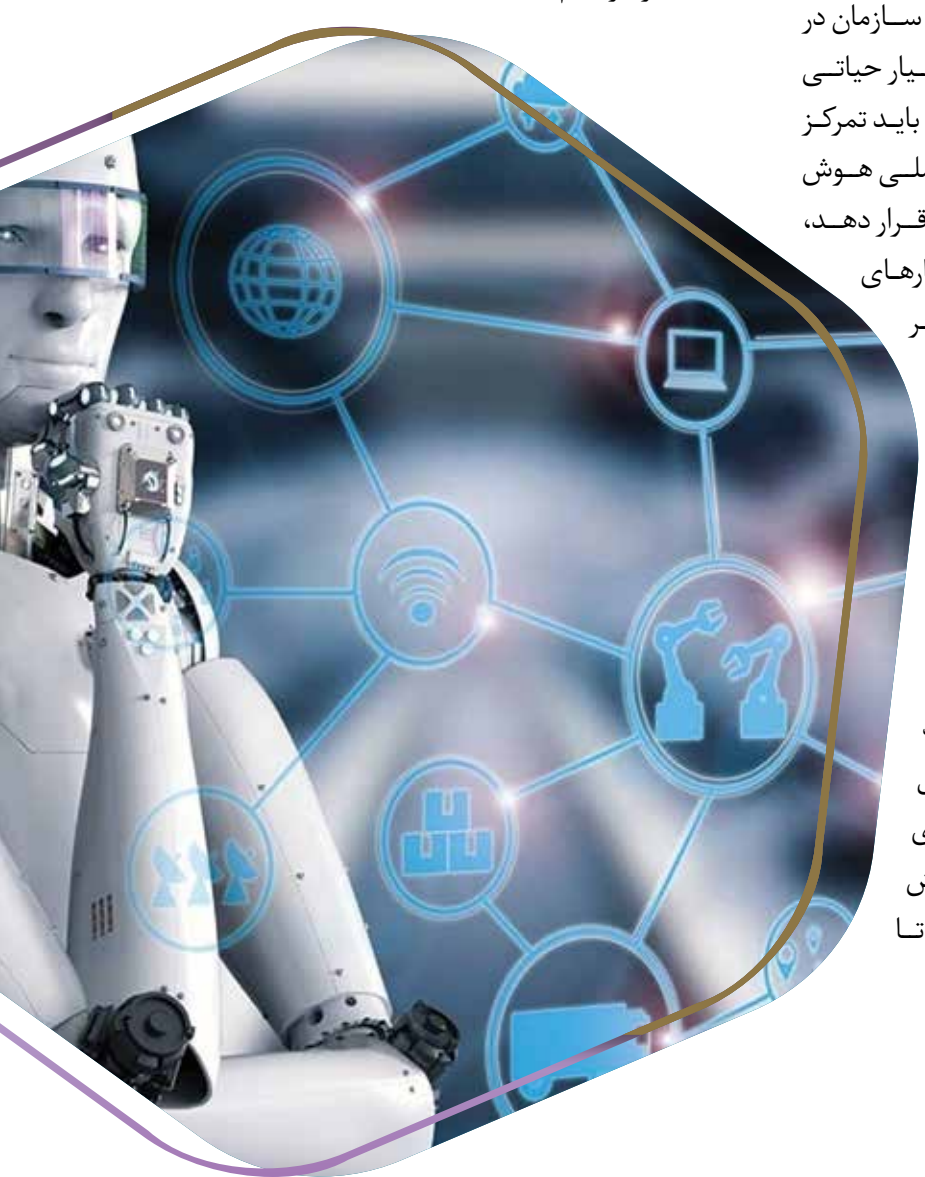
در نهایت، تعدد مراکز حاکمیتی در حوزه هوش مصنوعی می‌تواند مفید باشد، اما تنها در صورتی که تحت نظارت و هدایت یک سازمان ملی منسجم و قدرتمند قرار گیرند. این سازمان باید اطمینان حاصل کند که هر نهاد در حوزه تخصصی خود فعالیت می‌کند و هماهنگی لازم بین نهادهای مختلف وجود دارد. در غیر این صورت، تعدد مراکز می‌تواند به جای پیشرفت، باعث کندی و پراکندگی شود.

در میان تعدد متولیان این حوزه در کشور جایگاه سازمان ملی هوش مصنوعی چگونه تعریف می‌شود؟

سازمان ملی هوش مصنوعی باید به‌عنوان نهاد راهبر و هماهنگ‌کننده در حوزه هوش مصنوعی عمل کند. جایگاه این سازمان در میان تعدد متولیان این حوزه، بسیار حیاتی است. سازمان ملی هوش مصنوعی باید تمرکز خود را بر نظارت بر اجرای سند ملی هوش مصنوعی و برنامه‌های کلان مرتبط قرار دهد، نه اینکه وارد کارهای اجرایی شود. کارهای اجرایی باید به بخش‌های تخصصی‌تر مانند شرکت‌ها، دانشگاه‌ها، و مراکز تحقیقاتی سپرده شود، چرا که این نهادها توانایی و انعطاف بیشتری برای انجام پروژه‌های عملیاتی دارند.

وظیفه اصلی سازمان ملی هوش مصنوعی، تسهیل‌گری و حمایت از این نهادها است. این سازمان باید با ایجاد بسترهای لازم، مانند تسهیل دسترسی به داده‌ها، زیرساخت‌های محاسباتی، و منابع مالی، به بخش خصوصی و دانشگاه‌ها کمک کند تا بتوانند به‌طور مؤثر در حوزه هوش مصنوعی فعالیت کنند. همچنین، سازمان ملی هوش مصنوعی باید با تدوین استانداردها و قوانین مناسب، از ایجاد رقابت‌های ناسالم جلوگیری کند و اطمینان حاصل کند که تمامی بازیگران در چارچوب مشخصی فعالیت می‌کنند.

یکی از مهم‌ترین نقش‌های سازمان ملی هوش مصنوعی، نظارت دقیق بر اجرای سند ملی هوش مصنوعی و برنامه‌های مرتبط است. این سازمان باید اطمینان حاصل کند که اهداف کلان تعیین‌شده در سند ملی به‌طور کامل و دقیق اجرایی می‌شوند. این نظارت باید به‌گونه‌ای باشد که از موازی‌کاری جلوگیری کند و هماهنگی لازم بین نهادهای مختلف را فراهم کند.




گزارش رصدی

هوش مصنوعی مولد: چالش‌ها، فرصت‌ها، امنیت و حریم خصوصی

برگرفته از کارگاه هوش مصنوعی مولد اتحادیه جهانی مخابرات

تهیه‌کنندگان: ساسان کرمی‌زاده، طلا تفضلی و افسانه معدنی

چکیده

با در نظر گرفتن هوش مصنوعی به عنوان یکی از مهمترین و پیشروترین فناوری‌های حوزه فناوری اطلاعات، اتحادیه جهانی مخابرات[1] در ۱۹ فوریه ۲۰۲۴ کارگاهی با موضوع هوش مصنوعی مولد با حضور پژوهشگرانی از کشورهای آمریکا، ژاپن، آلمان، انگلیس، فرانسه، چین، اسکاتلند و کره جنوبی برگزار نموده و در آن به طور خاص به چالش‌های امنیتی حول موضوع هوش مصنوعی مولد پرداخته شد. موضوعات مطرح شده در این نشست به طور کلی به مباحثی عمومی در مورد هوش مصنوعی از جمله چرخه حیات‌هوش مصنوعی و ذی‌نفعان آن و به طور ویژه به مخاطرات امنیتی مربوط به این فناوری مربوط می‌شود. همچنین الزامات موجود در نهاد استانداردهای اتحادیه اروپا، کمیته فنی ایمن‌سازی هوش مصنوعی اتحادیه اروپا[2] و مرکز امنیت سایبری ملی بریتانیا[3] نیز مورد بررسی قرار گرفته است. در انتها و در بخش نتیجه‌گیری، مواردی به عنوان خلاصه این نشست ارائه شده است.

مقدمه

هوش مصنوعی مولد محتوا را در قالب‌های مختلف از جمله متن، تصاویر، صوت، انیمیشن، مدل‌های سه بعدی و موارد دیگر در پاسخ به درخواست‌های کاربران تولید می‌کند. چنین تطبیق پذیری با ارائه فرصت‌های امیدوارکننده و همچنین معرفی چالش‌های منحصر به فرد که نیاز به توجه دقیق دارد، تأثیری دوگانه بر امنیت دارد. از یک سو، هوش مصنوعی مولد پتانسیل افزایش قابلیت‌های امنیتی را دارد. از سوی دیگر، مهاجمان را با افزایش مقیاس-پذیری و پیچیدگی آن‌ها توانمند می‌کند. خطرات امنیتی کلیدی شامل جعل عمیق[4] "یک تکنیک نرم‌افزاری مبتنی بر هوش‌مصنوعی است که در محتوای صوتی و تصویری دست می‌برد و آن را به‌دلخواه تغییر می‌دهد " و نقض حق چاپ است. علاوه بر این، هوش مصنوعی مولد تهدیدی برای حریم خصوصی داده‌ها، از جمله نقض داده‌ها، ناشناس‌سازی ناکافی، اشتراک‌گذاری غیرمجاز داده، سوگیری‌ها، عدم رضایت و شفافیت و حفظ ناکافی داده‌ها است. لذا اقدامات جامع امنیتی و حفظ حریم خصوصی برای رفع موثر این نگرانی‌ها ضروری است. در این نشست که در ژنو برگزار شد، افراد از کشورهای مختلف در این نشست شرکت کرده بودند. اهداف کارگاه که توسط کمیته راهبری برای کارهای آینده در

1. International Telecommunication Union
2. European Union
3. National Cyber Security Centre is an organization of the United Kingdom Government

4. Deep fakes

گروه مطالعاتی ۱۷ در نظر گرفته شده عبارتند از: شناسایی و ارائه یک نمای کلی جامع از مزایا و همچنین چالش‌های امنیتی و حفظ حریم خصوصی مرتبط با برنامه‌های کاربردی مبتنی بر هوش مصنوعی، شناسایی کنترل های فنی و سازمانی امنیتی و حریم خصوصی برای کاهش تهدیدات شناسایی شده، تسهیل تبادل فعالیت‌های جاری در سازمان‌های توسعه استاندارد مربوطه و سایر سازمان‌ها در رسیدگی به امنیت و حریم خصوصی برای برنامه‌های کاربردی مبتنی بر هوش مصنوعی

مزایا و چالش‌های مربوط به امنیت و حریم خصوصی

هوش مصنوعی مولد با ارائه فرصت‌های امیدوارکننده و همچنین معرفی چالش‌های منحصربه فردی که نیازمند توجه دقیق است، تأثیری دوگانه بر امنیت دارد. ازیک طرف، هوش مصنوعی مولد پتانسیل افزایش قابلیت‌های امنیتی را دارد. از طرف دیگر، مهاجمان را با افزایش مقیاس‌پذیری و پیچیدگی آن‌ها توانمند می‌کند. در این بخش به بررسی پویایی دوگانه هوش مصنوعی مولد پرداخته شده و چالش‌ها، خطرات و تهدیدات امنیتی و حریم‌خصوصی پیرامون هوش مصنوعی نشان داده شده است. لازم به ذکر است در این نشست پژوهشگرانی از کشورهای کره، آلمان، اسکاتلند، امریکا و فرانسه حضور داشتند.

ذینفعان سیستم هوش مصنوعی

هنگام در نظر گرفتن چرخه عمر یک سیستم هوش مصنوعی، ذی‌نفعان زیر در برنامه‌ریزی، طراحی، توسعه، استقرار، بهره‌برداری و نگهداری یک سیستم هوش مصنوعی نقش دارند. که در ادامه به آن‌ها اشاره شده است.

- مدیریت سازمان:
مدیریت سازمان یک ذینفع محسوب می‌شود زیرا استراتژی‌های سیستم هوش مصنوعی، اهداف، منابع، ارزش‌ها، روش‌های ارزیابی می‌بایست با اهداف تجاری آن سازمان هماهنگ باشند.
- معماران مدل هوش مصنوعی: زیرا در معماری مدل هوش مصنوعی نیاز است که الگوریتم‌ها، طراحی و مدل‌ها تنظیم، دقیق و مقیاس‌پذیری و تفسیرپذیری مدل اولویت‌بندی شوند.
- اپراتورهای خدمت دهنده هوش مصنوعی: زیرا این اپراتورها باید خدمات هوش مصنوعی را مدیریت و سیستم‌های هوش مصنوعی را نظارت، به روز رسانی، نگهداری و ایمن کنند.

تهدیدات امنیتی هوش مصنوعی مولد

در این بخش تمرکز بر انواع تهدیدات هوش مصنوعی مولد است. تهدیدات امنیتی شامل استفاده از داده‌های نادرست، سوءاستفاده از مدل‌های هوش مصنوعی، آسیب‌پذیری‌های امنیتی در سیستم‌های هوش مصنوعی، ناامنی در استقرار و استفاده، و تغییرات غیرمنتظره در عملکرد مدل‌ها می‌شود. برای مقابله با این تهدیدات، استانداردهای امنیتی مناسب از جمله رمزگذاری، احراز هویت، مانیتورینگ فعالیت‌ها و آموزش کاربران باید اجرا شود و استفاده از روش‌های بازبینی و آزمون امنیتی نیز توصیه می‌شود. تهدیدات امنیتی و خطرات مرتبط می‌توانند بر تمام مراحل چرخه حیات هوش

جدول ۱. تهدیدات امنیتی با توجه به مراحل چرخه عمر هوش مصنوعی

تهدیدات امنیتی	برنامه‌ریزی	آماده سازی داده‌ها	طراحی مدل	آموزش/توسعه مدل	استقرار مدل	عملیات/نظارت و نگهداری
سوگیری[1] الگوریتمی			×	×		
آسیب کد امنیتی				×		
ناهماهنگ بودن داده‌های آموزش		×		×		
مسموم کردن دادهای آموزش		×		×	×	
حمله دور زدن[2] (فرار) (دستکاری ورودی)		×		×	×	
استنتاج عضویت[3]		×		×		
استخراج مدل[4]				×	×	
وارونگی مدل[5]		×		×		
ضعف الگوریتم هوش مصنوعی در ورودی پایگاه داده			×	×	×	
الگوریتم غیرقابل تفسیر[6]				×		
حمله مهاجمان				×		
داده‌های آلوده یا تحریف شده				×	×	×

مصنوعی تأثیرگذار باشند. در جدول ۱ مخاطرات امنیتی مرتبط با هر یک از مراحل چرخه عمر هوش مصنوعی نشان داده شده است.

الزامات امنیتی

مدیریت خطرات در طول چرخه عمر هوش مصنوعی نیازمند اجرای تدابیر امنیتی و بهره‌گیری از راهکارهای مناسب است. برخی از الزامات اصلی در این زمینه عبارتند از: توسعه و اجرای استانداردها و راه‌حل‌های امنیتی در طول تمام مراحل چرخه عمر هوش مصنوعی، آموزش و آگاهی کاربران درباره خطرات امنیتی مرتبط با هوش مصنوعی و رفتارهای امنیتی ضروری، ارزیابی مداوم و مدیریت خطرات امنیتی مرتبط با هوش مصنوعی، رصد فعالیت‌ها و پاسخ به حوادث در طول چرخه عمر هوش مصنوعی، استفاده از ابزارهای امنیتی مناسب برای شناسایی و مدیریت خطرات امنیتی، و همکاری و هماهنگی بین تیم‌های مختلف برای اجرای موثر استراتژی‌های امنیتی و مدیریت خطرات امنیتی در طول چرخه عمر هوش مصنوعی. با رعایت این الزامات و اجرای تدابیر مناسب، می‌توان خطرات امنیتی مرتبط با چرخه عمر هوش مصنوعی را کاهش داد و امنیت اطلاعات و سیستم‌های مرتبط با آن‌ها را تضمین کرد. جزئیات بیشتر مربوط به این الزامات امنیتی در جدول ۲ ارائه شده است.

1. Algorithm bias
2. Evasion attack
3. Membership inference
4. Model Extraction
5. Model Inversion
6. Algorithm unexplainability

جدول۲. الزامات امنیتی

مرحله چرخه عمر سیستم هوش مصنوعی	الزمات امنیتی
برنامه‌ریزی	• شناسایی و تجزیه و تحلیل تهدیدات امنیتی بالقوه ای • ارایه راهکار برای مقابله و شناسایی تهدیدات
آماده‌سازی داده‌ها	• بررسی عادی یا غیرعادی بودن داده‌ها • آمادگی در برابر تهدیدات امنیتی • حفاظت از مجموعه داده‌های آموزشی در برابر دسترسی، اصلاح یا تخریب غیرمجاز • تهیه مجموعه داده‌های مناسب برای آموزش و ارزیابی؛ (مثل تمیز کردن، قالب‌بندی و عادی‌سازی مجموعه داده‌ها)
طراحی مدل	• بررسی فرآیند مدیریت ریسک را با در نظر گرفتن کل چرخه حیات سیستم‌های هوش مصنوعی که شامل شناسایی ریسک، تجزیه و تحلیل ریسک، ارزیابی ریسک و درمان ریسک • بررسی و شناسایی تهدیدات امنیتی و آسیب‌پذیری‌های ذاتی سیستم هوش مصنوعی
آموزش/توسعه مدل	• بررسی تهدیدات امنیتی و آسیب‌پذیری‌های موجود در کتابخانه‌های منبع باز • آموزش تکنیک‌های لازم به توسعه‌دهندگان جهت کاهش حملات • بررسی ثبات عملیاتی کتابخانه‌های منبع باز موجود در سیستم هوش مصنوعی • استفاده از محیط‌های امن برای آموزش داده‌ها
توسعه	• اجرای فرآیند مدیریت ریسک در مرحله استقرار و عملیات سیستم هوش
عملیات / نظارت و نگهداری	• ارایه راهنما برای استفاده صحیح از خدمات هوش مصنوعی • نظارت مداوم بر مجموعه داده‌ها و مدل‌های یادگیری

حفاظت از داده‌ها برای هوش مصنوعی

نحوه تعامل افراد با هوش مصنوعی، بسته به زمینه و هدف تعامل آن‌ها می‌تواند تأثیرات متفاوتی داشته باشد. به طور کلی، سه مسیر اصلی وجود دارد که از طریق آن افراد و سازمان ها به هوش مصنوعی دسترسی پیدا می کنند:

۱. دسترسی کاربران (مانند کارمندان، شهروندان و غیره) به پلتفرم‌های هوش مصنوعی در دسترس عموم همانند BARD، ChatGPT، و غیره. این موضوع، خطر سرقت داده‌ها را برای سازمان‌ها به همراه دارد.

۲. کارمندان یا دانش آموزانی که از هوش مصنوعی ارائه شده توسط سازمان ها یا مؤسسات آموزشی آن‌ها از طریق برنامه های کاربردی یا وب سایت های شرکتی استفاده می کنند. برای این موضوع در حالی که هنوز خطرات استخراج داده را به همراه دارد، می‌توان یک چارچوب امنیتی قرار داد که رعایت گردد.

۳. سازمان‌هایی که مدل‌ها یا برنامه‌های کاربردی هوش مصنوعی خود را برای استفاده داخلی توسعه می‌دهند. در این مورد نیز ممکن است داده ها توسط دیگران قابل دسترسی باشد. زیرا سوالاتی در مورد داده های مورد استفاده برای آموزش و اشتراک گذاری بالقوه آن داده ها مطرح می شود.

خطرات امنیتی هوش مصنوعی مولد

این قسمت در مورد ملاحظات مختلف مربوط به خطرات امنیتی مرتبط با هوش مصنوعی مولد است. این موارد شامل مسائلی مانند دسترسی به خدمات، مراجع صدور مجوز، تهدیدات امنیتی احتمالی، حفظ حریم خصوصی، شفافیت، رعایت قوانین و حقوق بشر است. برخی از چالش‌های خاص ذکر شده در این خصوص شامل چالش‌های حریم خصوصی مرتبط با داده‌های ارائه شده، چارچوب‌های قانونی کنترل داده‌ها و مکانیسم‌های نظارتی است. همچنین در این قسمت به چالش‌های قانونی مرتبط با هوش مصنوعی، مانند حقوق شرکت‌های هوش مصنوعی برای استفاده از داده‌های آموزشی و اصالت محتوای تولید شده توسط هوش مصنوعی اشاره شده است. در این بخش همچنین چالش‌های نظارتی، شامل قوانین در اتحادیه اروپا و ایالات متحده در خصوص حاکمیت هوش مصنوعی نیز بحث شده است.

مرکز امنیت سایبری ملی بریتانیا

مرکز امنیت سایبری ملی بریتانیا، در کارگاهی چالش‌ها و فرصت‌های هوش مصنوعی را چنین عنوان کرده است؛ چالش‌ها شامل عجله در پیاده‌سازی سیستم‌های هوش مصنوعی، ایجاد سیستم‌های خطرناک به‌طور ناخواسته، عدم حفاظت از داده‌ها در فرآیند توسعه سیستم، آسیب‌پذیری در برابر حملات هوش مصنوعی و عدم وجود کنترل‌های مورد انتظار مشابه سیستم‌های معمولی است. بنابراین، با وجود قابلیت‌های چشم‌گیر هوش مصنوعی مولد، اعتماد عمومی به آن کم است. هرچندفرصت‌هایی نیز در این حوزه وجود دارد، از جمله استفاده مدافعان از هوش مصنوعی مولد برای مقابله با حملاتی که مهاجمان از آن استفاده می‌کنند شامل خودکارسازی وظایفی که در حال حاضر وقت مدافعان را می‌گیرد و

تجزیه و تحلیل کارآمد داده‌های بلادرنگ بدون صرف وقت زیاد است.

کنترل و حریم خصوصی

این بخش بر شناسایی کنترل‌هایی برای کاهش نگرانی‌های امنیتی و حفظ حریم خصوصی در مورد هوش مصنوعی مولد تمرکز می‌کند و دیدگاه‌های جدیدی را درباره نحوه تنظیم کنترل‌های موثر برای حفظ امنیت و حفظ حریم خصوصی به اشتراک می‌گذارد. لازم به ذکر است در این نشست پژوهشگرانی از کشورهای چین، امریکا، افریقای جنوبی، کره جنوبی، هلند تحقیقات خود را ارایه دادند.

بررسی در حکمرانی هوش مصنوعی مولد

این بخش به حکمرانی هوش مصنوعی مولد در طول چرخه عمر آن و کنترل‌ها و ریسک‌های مرتبط تمرکز دارد. همچنین دربرگیرنده مسائل امنیتی، خطرات مرتبط با محتوای تولید شده، خطرات ساخت مدل و مسائل حقوق مالکیت معنوی است.ضمناً به موضوعات مربوط به حقوق مالکیت فکری، که ممکن است در حفاظت از داده‌های آموزشی نقض شود، پرداخته شده است. این نشست به امنیت در طول چرخه عمر ارائه خدمات یا عملکرد سیستم، از جمله آموزش، راه‌اندازی سرویس، تولید محتوا و توزیع محتوا می‌پردازد. همچنین به جای تمرکز صرفاً بر آموزش مدل یا تولید محتوا، تأکید بر اجرای کنترل‌ها در طول کل چرخه عمر قرار دارد. این کنترل‌ها باید در طول چرخه عمر اعمال شوند، به‌ویژه برای داده‌های آموزشی که نیازمند ارزیابی منابع داده برای فیلتر کردن، برچسب‌گذاری و بازرسی هستند. استانداردهای موجود برای مقابله با این مسائل باید مورد مشاوره قرار گیرند. برای حفاظت از اطلاعات شخصی، الزامات نظارتی در مناطق مختلف باید تدوین گردد . درباره بخش مدل، باید گفت ایجاد و استفاده از استانداردها برای ارزیابی مدل، امری بسیار حیاتی است. معیارها می‌توانند با استفاده از روش‌های مختلفی مانند ایجاد پرسش‌های ریسک بر اساس پایگاه دانش ریسک به صورت دستی یا استفاده از مدل دیگری برای تولید آن‌ها ساخته شوند و مدل‌ها با استفاده از پرسش‌ها ارزیابی شوند. به‌علاوه، تعبیه امنیت در مدل‌ها امری ضروری است

کـه از طریـق روش‌هـای مختلفـی ماننـد معرفـی عمـدی نمونه‌هـای مجـازی متنـوع بـه داده‌هـای آموزشـی بـرای تقویـت آن انجـام می‌شـود. ایـن تنهـا بـرای اهـداف آموزشـی اسـت و در نهایـت یـک رویکـرد مـدل سـنتی ممکـن اسـت بـرای پـردازش پرسـش‌های ریسـک مناسـب باشـد.

اکوسیســتم هــوش مصنوعی و کنتــرل های امنیتــی حیاتی

در ایـن بخـش از نشسـت بـه موضـوع اکوسیسـتم هـوش مصنوعـی[1] و کنتـرل هـای امنیتـی حیاتـی پرداختـه شـد و همچنیـن بیـان شـد کـه فناوری‌های هـوش مصنوعـی، اسـتانداردهای فنـی و شـیوه‌های مـورد اسـتفاده، در حـال افزایـش و عملیاتـی شـدن هسـتند. بـا توجـه بـه اینکـه هـوش مصنوعـی امـروزه در همـه جـا کاربـرد پیـدا کـرده اسـت دارای

1. AI Ecosystem

چالش‌هایـی از قبیـل مسـائل حقوقـی متعـدد بـه ویـژه تخلفـات، حقـوق مالکیـت معنـوی، حقـوق بشـر، کشـف و تعـارض قانـون اسـت. بـرای درک ایـن چالش‌هـا نیـاز اسـت تـا آسـیب‌پذیری‌ها، تهدیـدات و حمـلات هـوش مصنوعـی و اینکـه چگونـه ممکـن اسـت ایـن حمـلات ازیکدیگرمتفـاوت باشـند را بایـد درک نمـود. بـه عـلاوه نیـاز اسـت تـا آگاهـی از محوریـت اسـتانداردهای امنیتـی در ایـن زمینـه وجـود داشـته باشـد.

انواع حملات به هوش مصنوعی مولد

در ایـن بخـش از نشسـت، در مـورد حملاتـی کـه بـه هـوش مصنوعـی مولـد می‌شـود پرداختـه شـد. می‌تـوان ایـن حمـلات را بصـورت زیـر دسـته بنـدی نمـود.

- بدافزاری که به دلخواه، دفاع را دور می‌زند
- داده‌هـای آموزشـی مسـموم - دسـتکاری ورودی / سر یع
- الگوریتم‌های هوش مصنوعی به خطر افتاده
- وارونگـی مـدل (زیـرا عوامـل تهدیـد خروجـی مـدل را بـرای اسـتنتاج دسـتکاری مـی کننـد)
- داده هـای آموزشـی حسـاس - خطـرات حفـظ حریـم خصوصـی
- حمـلات اکتشـافی، مـدل رفتـار، آسـیب پذیـری و حساسـیت سـرقت اطلاعات
- مدل DDoS
- سـرویس‌های ابـری نسـل سـوم هـوش مصنوعـی در معـرض خطر

حملاتـی کـه مدل‌هـای مولـد هـوش مصنوعـی، یادگیـری عمیـق و هـوش مصنوعـی را بـه خطـر مـی انـدازد عبارتنـد از:

- بدافـزار چنـد شـکلی و دگرگونـی در سـطحی دیگـر

- جعل عمیق[1]های کاملاً قوی - عدم وجود چک کننده های یکپارچگی خوب
- اخبار جعلی (اطلاعات دروغ و اطلاعات نادرست)
- الگوریتم‌ها/مدل‌های هوش مصنوعی به خطر افتاده
- اطمینان کامل از اطلاعات نادرست
- الگوریتم‌ها/مدل‌های هوش مصنوعی کامل آموزشی بر روی داده‌های مسموم

در ادامه در این بخش از نشست، در مورد کارهایی که برای دفاع سایبری، کنترل‌های تشخیص و پیشگیری می‌توان انجام داد موارد ذیل مطرح گردید:

- بهبود تشخیص بدافزار در ترافیک رمزگذاری شده
- بهبود احراز هویت مداوم
- آدرس راهنما بدافزار رمزگذاری شده
- بهبود تشخیص تهدید
- شناسایی و بیرون کردن مجرمان سایبری
- بهبود تشخیص و پیشگیری از نفوذ

هوش مصنوعی مولد برای تشخیص ناهنجاری/تهدید

- رفتار غیرمعمول کاربر/فرایند

تجزیه و تحلیل رفتاری امنیت سایبری

- ساخت مجموعه ای از داده‌های تهدید

توسعه مدل امن

- محفظه‌های امن، ماشین‌های مجازی و نمونه‌های مجازی، مدل‌های امن و آموزش داده‌ها

1. Deepfake

نظارت بر زمان واقعی و هوش مصنوعی حفظ حریم خصوصی

- راه حل‌های امنیت سایبری مبتنی بر هوش مصنوعی
- داده‌های مصنوعی، چالش‌های مربوط به حریم خصوصی

تسهیل تحقیقات فارنزیک دیجیتال

- کاهش زمان لازم برای حل و فصل پرونده‌های قضایی مربوط به جرایم سایبری
- بهبود مجازات‌های مرتبط با جرایم سایبری
- بهبود انتساب سایبری برای بازیگران تهدید دولت ملی
- تحلیلگران امنیت سایبری که می‌توانند تهدیدها را سریعتر و کارآمدتر شناسایی کرده و به آن‌ها پاسخ دهند.

استفاده ایمن از هوش مصنوعی مولد

اقدامات فنی برای استفاده ایمن از هوش مصنوعی مولد و همچنین جلوگیری از خطرات و مسائل امنیتی هنگام استفاده از هوش مصنوعی مولد عبارتند از:

- حریم خصوصی و محرمانه بودن داده ها
- مسائل امنیتی شخص ثالث
- بررسی آسیب پذیری رفتاری هوش مصنوعی
- مسائل حقوقی
- تکامل بازیگران تهدید (حمله کنندگان)
- مسائل مربوط به حق چاپ
- مسائل تعصب و تبعیض
- مسائل اعتماد و شهرت
- بررسی آسیب پذیری امنیتی نرم افزار
- مسائل مربوط به عملکرد، در دسترس بودن و هزینه
- مسائل اخلاقی و مقرراتی
- خطر امنیتی برتر مدل های زبان بزرگ[1] (LLM)
- تزریق سریع[2]
- مدیریت ناامن خروجی
- داده های آموزشی مسمومیت

1. Large language models
2. Prompt Injection

- مدل انکار خدمات
- آسیب پذیری زنجیره تأمین
- افشای اطلاعات حساس
- طراحی افزونه[3] ناامن
- عاملیت بیش از حد[4]
- اتکای بیش از حد
- مدل سرقت

کنترل‌های امنیت و حریم خصوصی هوش مصنوعی

در این بخش از نشست به انواع کنترل امنیت و حریم خصوصی هوش مصنوعی پرداخته شده که در ادامه آورده شده است:

- کنترل‌های امنیتی هوش مصنوعی برای محافظت از داده‌های شخصی
- کنترل‌های امنیتی هوش مصنوعی برای محدود کردن تأثیر رفتار مدل
- کنترل‌های اضافی برای محافظت از حقوق حریم خصوصی فردی:
  - اعتبارسنجی هدف (مثلاً تغییر هدف داده های شخصی)
  - داشتن رضایت
  - کنترل سوگیری ناخواسته
  - ارائه شفافیت/توضیح
  - دستیابی به دقت و به روز رسانی داده‌ها
  - ارایه ویژگی‌هایی برای تصحیح، دسترسی، پاک کردن

هوش مصنوعی مولد در مدیریت هویت و ردیابی محتوا

هوش مصنوعی بر روی همه جنبه‌های زندگی بشری تاثیر می‌گذارد. تا سال ۲۰۳۰ هوش

3. Plugin
4. Overreliance

مصنوعی زندگی بشری را مورد تاثیر قرار می‌دهد و امنیت و حریم خصوصی آن اهمیت بسزایی دارد. هوش مصنوعی کاربردهای متفاوتی دارد که در شکل ۱ نشان داده شده است.

شکل ۱. کاربردهای مختلف هوش مصنوعی

دولت‌ها در سراسر دنیا قوانین و مقرراتی را برای امنیت و حریم خصوصی در هوش مصنوعی تدوین نموده‌اند. هوش مصنوعی مولد ریسک‌های امنیتی متعددی دارد. مانند ریسک تولید اطلاعات نادرست[1] و احراز هویت. آیا محتوای تولید شده به صورت برخط توسط انسان تولید شده یا به صورت اتوماتیک توسط هوش مصنوعی. به منظور پاسخ به این سوال راهکارهای زیر پیشنهاد گردیده است:

- برچسب‌گذاری باید بر روی محتوای تولید شده انجام گیرد و امنیت به صورت برخط تامین شود تا کاربران بدانندکه محتوا توسط هوش مصنوعی تولید شده است تا تاثیر محتوای گمراه‌کننده بر روی جامعه کاهش یابد. به صورت بین‌المللی، به این مسئله به عنوان برچسب‌گذاری ارجاع می‌شود.
- باید روش‌هایی برای ردیابی محتواهای تولید شده توسط هوش مصنوعی وجود داشته باشد تا از انتشار محتوای گمراه‌کننده و منسوخ ممانعت بعمل آید و همچنین از حق نشر[2] و ابداع[3] محافظت شود.

همچنین به منظور کاهش ریسک انتشار محتوای گمراه‌کننده از طریق برچسب‌گذاری باید یک اجماع جهانی صورت گیرد. برچسب‌گذاری محتوای تولید شده توسط هوش مصنوعی باید مطابق با قوانین و مقررات مرتبط با تولیدکنندگان اطلاعات برخط به کمک هوش مصنوعی، اطلاعات تولید شده توسط هوش مصنوعی و مقالات تولید شده توسط هوش مصنوعی، تصاویر و ویدیوها صورت گیرد. مثلا، خروجی هوش مصنوعی مولد باید به گونه‌ای برچسب‌گذاری شود که توسط ماشین تولید شده باشد.

در اتحادیه اروپا برای استفاده از هوش مصنوعی قوانین و مقرراتی تدوین گردیده است. برخی از آن‌ها به شرح ذیل است:

- تولیدکنندگان سیستم‌های هوش مصنوعی، صدا، تصویر و ویدئو یا متن باید مطمئن باشند که خروجی سیستم هوش مصنوعی ساختار قابل خواندن توسط ماشین دارد و مشخص است که توسط هوش مصنوعی تولید گردیده است.
- تولیدکنندگان سیستم‌های هوش مصنوعی

1. misinformation

2. copyright
3. authorship

جدول ۳. معیارهای ردیابی پیاده‌سازی شده

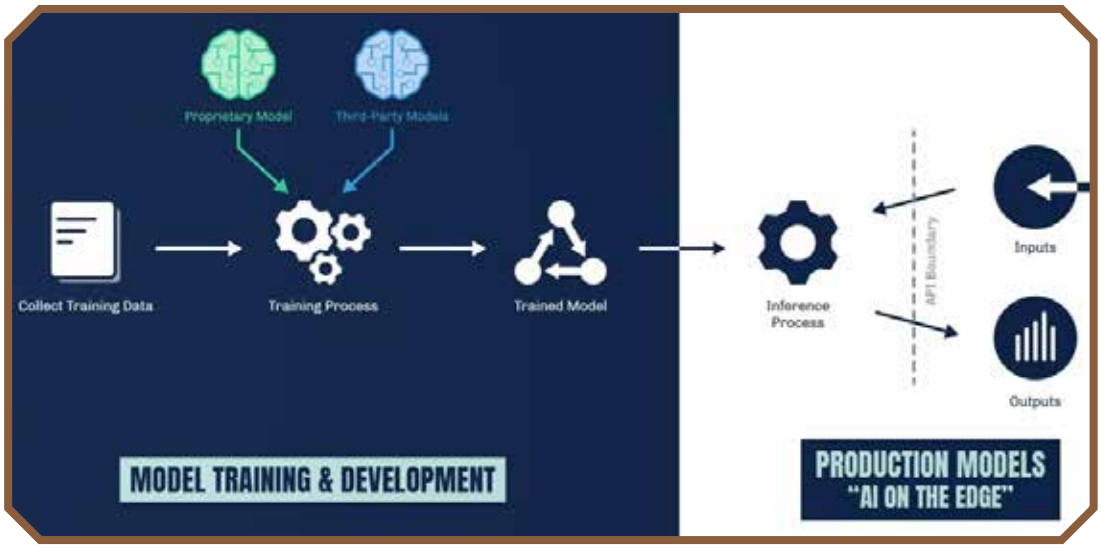
نوع فایل	الگوریتم	شناسایی محتوا	روش پیاده‌سازی
تصویر	Self-developed	نام مولد سرویس، شناسه محتوا	Transform domain watermark
ویدئو	Self-developed	نام مولد سرویس، شناسه محتوا	Transform domain watermark
صدا	Self-developed	نام مولد سرویس، شناسه محتوا	Frequency domain watermark

که محتوای تصویر، ویدیو و صدا را تولید می‌کنند، مشتمل بر محتوای جعلی، باید ذکر نمایند که محتواهایشان توسط ماشین تولید شده است.

کشور کانادا نیز اصولی را برای مسئولیت‌ها، قابلیت اعتماد و فناوری‌های هوش مصنوعی مولد تدوین نموده است. از قبیل اینکه همه طرف‌ها باید اطمینان یابند که خروجی سیستم‌های هوش مصنوعی که بر روی افراد یا گروه‌ها تاثیر می‌گذارد توسط آنها به عنوان ابزار هوش مصنوعی مولدعلامت‌گذاری شده است.

استانداردسازی باید انجام گیرد تا محتوای تولید شده توسط هوش مصنوعی شناسایی شود. این استاندارد سازی با در نظر گرفتن موارد ذیل باید صورت گیرد:

- برچسب‌گذاری محتوای تولید شده توسط هوش مصنوعی برای اعلان به کاربران وب که محتوا توسط هوش مصنوعی تولید شده است.



شکل ۲ ـ چرخه حیات هوش مصنوعی

- این کار موجب کاهش ریسک استفاده نادرست و سوء استفاده می‌گردد و از استفاده نادرست کاربران وب از محتوای تولید شده توسط هوش مصنوعی ممانعت بعمل می‌آورد.

- ایجاد مکانیزم ردیابی برای محتوای تولید شده توسط هوش مصنوعی به منظور کاهش یا حذف تاثیر منفی یا نادرست انتشار محتوای تولید شده بر جامعه:
  - ریسک انتشار محتوای گمراه‌کننده: ردیابی محتوای گمراه‌کننده تولید شده توسط هوش مصنوعی.
  - ریسک امنیت مالکیت معنوی: حفظ حریم خصوصی و سایر حقوق قانونی.
- محتوای تولید شده توسط هوش مصنوعی مولد باید برچسب‌گذاری گردد.

چین به منظور تایید هویت محتوای تولیدشده، استانداردهایی را مصوب نموده است.

در سال گذشته چین اولین مستند مربوط به مقررات بر روی هوش مصنوعی مولد را منتشر نمود (راهنمای هوش مصنوعی مولد در آموزش و تحقیق).

در این مستند بیان شده که تولیدکنندگان مدل‌ها و نرم‌افزارهای هوش مصنوعی مولد باید محتواهای تولید شده مانند تصاویر و ویدئوها را مطابق با تولیدات بر روی مدیریت ترکیب‌های داده سرویس‌های اطلاعاتی مبتنی بر اینترنت برچسب‌گذاری نمایند.

استانداردسازی بر روی هویت محتواهای تولید شده یک راهنما بر روی روش‌های شناسایی محتوای تولید شده توسط سرویس‌های هوش مصنوعی مولد منتشر گردیده تا محتوای تولید شده شناسایی گردد:

جدول ۴ ـ ریسک‌های هوش مصنوعی مولد و روش‌های مواجهه با آن

حملات به زنجیره تامین	مدیریت تقلب	هوش مصنوعی مولد	مورد مصرف هوش مصنوعی
حملات باج‌افزارها مسموم‌سازی داده مدل‌های در پشتی	استنتاج عبور حملات باج‌افزار	استنتاج مسموم‌سازی داده تزریق اعلان	رایج‌ترین انواع حملات
اسکن مدل محافظت برخط	پویش مدل محافظت برخط	اسکن مدل‌ها محافظت برخط	کنترل‌های کلیدی مورد نیاز

- علامت‌گذاری برای اعلان به کاربران و ممانعت از سوءاستفاده از محتوای تولیدشده
- نمایش پیوسته متن اعلان
- استفاده از ته‌نقش[1]
- افزودن متن اعلان به تصاویر و ویدئوها
- علامت ترکیب ماشین، انسان برای ممانعت از گیج شدن در زمان استفاده از سرویس‌های مشترک انسان و هوش مصنوعی

1. Watermark

پیاده‌سازی معیارهای ردیابی

زمانیکه تصاویر، ویدئو و صوت توسط هوش مصنوعی تولید می‌شود، واترمارک بر روی آن باید ثبت گردد. این واترمارک باید شامل حداقل نام ارائه‌دهنده سرویس و سایر محتواها باشد.

چین چهار استاندارد برای هوش مصنوعی مولدتدوین نموده است:

- نیازمندی‌های اولیه برای امنیت سرویس‌های هوش مصنوعی مولد
- روش‌های شناسایی محتوا برای سرویس‌های

هوش مصنوعی

- مشخصات ایمنی برای آموزش اولیه و بهینه‌سازی داده آموزشی در هوش مصنوعی مولد
- استانداردهای ایمنی برای جداسازی دستی در هوش مصنوعی مولد

استفاده ایمن از LLMها و سیستم‌های هوش مصنوعی مولد

فرصت‌های ایجاد شده توسط هوش مصنوعی و ریسک آن زیاد است. هوش مصنوعی می‌تواند تا ۱۵٫۷ تریلیون دلار در اقتصاد جهانی تا سال ۲۰۳۰ ایجاد نماید. امنیت تنها ریسکی است که باید در نظر گرفته شود. در طی سال ۲۰۲۲، ۳۰ درصد از حملات هوش مصنوعی موجب بالا رفتن مسمومیت داده آموزشی در هوش مصنوعی می‌شود.

حملات مهاجمین به هوش مصنوعی رو به رشد است به همین دلیل نیاز است تا مدل‌ها پویش شوند و امنیت آن‌ها تایید گردد.

مدل‌های هوش مصنوعی باید به گونه‌ای باشند که حملات به هوش مصنوعی را شناسایی نموده و به آن پاسخ دهند. همچنین عملیات امنیتی متعددی باید بر روی هوش مصنوعی انجام گیرد مانند کشف، ایمنی و اعتماد، مانیتورینگ حمله، پاسخگویی و آگاهی‌رسانی وضعیتی. هوش مصنوعی یک بردار حمله ناامن است. هیچ راهی برای ایمن‌سازی سیستم‌های هوش مصنوعی توسط فایروال، ابر و آنتی‌ویروس وجود ندارد. مدل هوش مصنوعی امکان عبور جانبی[1] از شبکه را فراهم می‌نماید. مدل‌های هوش مصنوعی باید پویش شوند تا امنیت و یکپارچگی آنها مورد بررسی قرار گیرد. چگونه شناسایی ریسک‌های هوش مصنوعی و روش‌های مواجهه با آن‌ها در جدول ۴ نشان داده شده است. نیاز است که ریسک‌های هر مدل شناسایی شوند و همچنین باید مدل‌ها اسکن و بر روی آن تست نفوذ انجام شود.

جمع‌بندی و پیشنهادات

در بخش پایانی این نشست فرصت‌های پیش رو برای استانداردهای آینده بررسی شده و توصیه‌هایی به گروه مطالعاتی ITU-T 17 برای کار آینده در این زمینه ارائه شد. همچنین در مواردی که هوش مصنوعی مولد برای امنیت استفاده می شود توضیحاتی از طرف اعضای نشست بیان شد که در ادامه به بعضی از این موارد اشاره میگردد:

- اتوماسیون دفاع سایبری
- هوش تهدید
- تولید و شناسایی کد ایمن
- شناسایی حملات سایبری
- شناسایی بدافزار
- افزایش اثربخشی فناوری های امنیت سایبری

به علاوه در مواردی که از هوش مصنوعی مولد برای حمله استفاده می شود اشاره شد.

- حملات مهندسی اجتماعی
- حملات فیشینگ
- هک خودکار
- تولید کد باج افزار
- تولید کد بدافزار

در انتها از بین اعضای شرکت کننده در موارد مختلف مرتبط با این نشست، سوالاتی مطرح شد که در ادامه این سوالات نیز آورده شده است.

- شکاف‌های استانداردسازی:

1. Lateral

۱. شکاف‌های فعلی استانداردهای بین المللی مربوط به امنیت و حریم خصوصی هوش مصنوعی مولد، هوش مصنوعی مولد برای امنیت چیست و چگونه می توان آن‌ها را برطرف کرد؟
۲. چگونه استانداردهای آینده می توانند قابلیت همکاری و سازگاری را در بین فناوری ها و پلت فرم های مختلف هوش مصنوعی مولد تضمین کنند؟

- ملاحظات اخلاقی:

۱. چگونگی استفاده از استانداردها و دستورالعمل‌های اخلاقی، برای هدایت توسعه و استفاده از فناوری‌های هوش مصنوعی مولد موثر است.

- استانداردهای جهانی و همکاری:

۱. همکاری بین‌المللی و تلاش‌های استانداردسازی چگونه می‌توانند باعث افزایش امنیت و حریم خصوصی فناوری‌های هوش‌مصنوعی‌مولدشود.

مواردی که در کارگاه هوش مصنوعی مولد اتحادیه جهانی مخابرات مطرح گردیده به طور خلاصه شامل موارد زیر است:

- شاغلین و کاربران هوش مصنوعی نیاز به راهنمایی دارند.
- هوش مصنوعی یک فناوری نوظهور است که بر اساس سابقه طولانی کمک رایانه به صنعت، فعالیت های اجتماعی، فعالیت های تجاری و اوقات فراغت شکل گرفته است.
- بسیاری از کارهایی که هوش مصنوعی انجام می دهد تکاملی است.
- بسیاری از کارهایی که هوش مصنوعی می تواند انجام دهد انقلابی است.
- سرعتی که هوش مصنوعی می تواند انقلابی شود، سریعتر از چیزی است که آمادگی لازم برای آن وجود داشته باشد.
- بسیاری از نگرانی‌های اجتماعی ریشه در ترس از ناشناخته‌ها و آزمایش نشده‌ها دارد.
- نهادهای استاندارد می‌توانند عقلانیت را به بحث هوش مصنوعی بیاورند.
- در مورد موضوعات هوش مصنوعی باید با منطق و به دور از احساسات روبرو شد.
- استانداردها باید فقط آنچه را که برای دستیابی به اهداف لازم است مشخص کند و رویکرد خاصی را برای اجرا تحمیل نکند.
- الزام باید شامل تمام اطلاعات لازم برای درک آن الزام باشد، چه به طور مستقیم یا با ارجاع به اسناد دیگر. خواننده استاندارد نباید نیازی به فرضیاتی در مورد اجرای هر الزامی داشته باشد.
- الزامات باید واضح و دقیق، بدون جزئیات غیر ضروری که ممکن است خواننده را سردرگم کند، بیان شود.
- در عناصر فردی نیازمندی‌ها باید به شیوه‌ای مناسب و خوانا گنجانده شوند.
- هیچ تناقضی بین الزامات مختلف در استاندارد و یا سایر استانداردهای مرتبط نباید وجود داشته باشد.
- باید ابزار روشن و واضحی وجود داشته باشد که نشان دهد یک پیاده سازی با الزامات مطابقت دارد.

مراجع

ITU Workshop on Generative AI: Challenges and Opportunities for Security and Privacy, Geneva, Switzerland, 19 February 2024

تحلیل وضعیت آمادگی کشور در حوزه هوش مصنوعی بر اساس سند آکسفورد ۲۰۲۴

الهام رافتی، هادی بکائی

مرکز نوآوری و توسعه هوش مصنوعی، پژوهشگاه ارتباطات و فناوری اطلاعات

مقدمه

هوش مصنوعی دیگر تنها یک فناوری نوظهور و دارای گستره محدودی از کاربردهای فناورانه مثل سایر فناوری‌های نوظهور مانند اینترنت اشیاء نیست، بلکه یکی از ارکان اصلی تحول اقتصادی-اجتماعی و فناورانه در سطوح ملی و جهانی است. آگاهی از وضعیت و میزان آمادگی کشور در زمینه توسعه و بکارگیری این فناوری نقش موثری در برنامه‌ریزی‌ها و اقدامات کشور ایفا می‌کند. سند آکسفورد ۲۰۲۴، که یکی از معتبرترین گزارش‌های بین‌المللی در ارزیابی وضعیت کشورها در این حوزه است، تصویری از جایگاه کشورهای مختلف از جمله جمهوری اسلامی ایران ارائه می‌دهد که در این گزارش مورد استفاده قرارگرفته و براساس آمار و شاخص‌های ارائه‌شده در آن، تحلیل‌های راهبردی متناسب با وضعیت کشور همراه با پیشنهاداتی برای بهبود سیاست‌گذاری موثر در این زمینه ارائه شده است.

وضعیت کلی ایران در هوش مصنوعی

سند آکسفورد ۲۰۲۴ یکی از معتبرترین گزارش‌های بین‌المللی است که وضعیت کشورها را در حوزه فناوری‌های نوین، از جمله هوش مصنوعی، کلان‌داده، زیرساخت‌های دیجیتال و سیاست‌گذاری فناوری ارزیابی می‌کند. این سند با استفاده از شاخص‌های کلیدی نظیر زیرساخت‌های فناوری اطلاعات، حکمرانی داده، میزان سرمایه‌گذاری در تحقیق و توسعه، پذیرش فناوری‌های نوین در صنعت، کیفیت آموزش در حوزه رشته‌های علوم، فناوری، مهندسی و ریاضیات امنیت سایبری و نوآوری دیجیتال، عملکرد کشورها را تحلیل و رتبه‌بندی می‌کند.

اهداف اصلی این سند عبارت‌اند از:

- تحلیل وضعیت کشورها در مسیر توسعه فناوری و دیجیتالی شدن
- شناسایی چالش‌های سیاست‌گذاری و ارائه راهکارهای بهبود
- مقایسه عملکرد کشورها در حوزه‌هایی مانند هوش مصنوعی، داده‌های باز، امنیت سایبری و حکمرانی فناوری
- کمک به تصمیم‌گیری دولت‌ها و نهادهای بین‌المللی برای توسعه فناوری‌های نوین

مؤسسه آکسفورد هر ساله گزارش رتبه بندی کشورها را در حوزه هوش مصنوعی منتشر می‌کند. هفتمین نسخه این گزارش در سال ۲۰۲۴ منتشر شده و به عنوان منبعی معتبر برای سیاست‌گذاران تبدیل شده و به عنوان معیار رسمی توسط دولت‌های ملی و سازمان‌های برجسته‌ای مانند یونسکو و گروه ۲۰ مورد استفاده قرار می‌گیرد.

جـدول زیـر جایـگاه ایـران را در حـوزه هـوش مصنوعـی طـی چهـار سـال متوالـی نشـان می‌دهـد. ایـن مقایسـه بیانگـر ایـن موضـوع اسـت کـه ایـران بـا کسـب امتیـاز ۴۳.۸۸ در رتبـه ۹۱ از میـان ۱۸۸ کشـور قـرار گرفتـه اسـت. ایـن رتبـه در مقایسـه بـا سـال ۲۰۲۳ (رتبـه ۹۴) بهبـود یافتـه، امـا نسـبت بـه سـال ۲۰۲۲ (رتبـه ۷۵) افـت چشـمگیری داشـته اسـت، کـه نشـان‌دهنده نوسـانات جایـگاه کشـور در ایـن حـوزه اسـت.

جدول ۱. رتبه ایران در شاخص آمادگی هوش مصنوعی دولت در سال‌های اخیر

سال	جایگاه ایران	تعداد کشورها	امتیاز ایران
۲۰۲۴	۹۱	۱۸۸	۴۳٫۸۸
۲۰۲۳	۹۴	۱۹۳	۴۲٫۰۷
۲۰۲۲	۷۵	۱۸۱	۴۵٫۳۰
۲۰۲۱	۷۲	۱۶۰	۴۶٫۲۳

ارزیابـی پیشـرفت کشـور در حـوزه هـوش مصنوعـی

تحـول دیجیتـال و پیشـرفت فناوری‌هـای هـوش مصنوعـی نقـش مهمـی در توسـعه اقتصـادی، اجتماعـی و صنعتـی کشـورها ایفـا می‌کنـد. ارزیابـی میـزان پیشـرفت کشـورها در ایـن حـوزه، نیازمنـد مجموعـه‌ای از شـاخص‌های مشـخص و قابـل اندازه‌گیـری اسـت کـه بتواننـد نقـاط قـوت و ضعـف هـر کشـور را تعییـن کننـد. ایـن شـاخص‌ها طیـف گسـترده‌ای از عوامـل مؤثـر بـر اکوسیسـتم هـوش مصنوعـی را شـامل می‌شـوند، از جملـه سیاسـت‌گذاری، زیرسـاخت‌های فنـاوری، سـرمایه‌گذاری، آمـوزش، تحقیـق و توسـعه، و دسترسـی بـه داده.

براسـاس مـدل ارزیابـی، امتیـازات هر کشـور را بر اسـاس سـه محـور اصلـی "حاکمیـت"، "فنـاوری" و "داده و زیرسـاخت" محاسـبه کـرده اسـت. (ذیـل هـر

محـور تعـدادی بعـد وجـود دارد و ذیـل هـر بعـد نیـز تعـدادی شـاخص مـورد بررسـی قـرار گرفتـه اسـت. در مجمـوع ۴۰ شـاخص بعنـوان مرجـع امتیازبنـدی در موسسـه اکسـفورد مـورد بررسـی قـرار گرفتـه و کشـورها را امتیـاز بنـدی و رتبـه بنـدی نمـوده اسـت.

حاکمیـت: دولـت بایـد چشـم‌اندازی راهبـردی بـرای توسـعه و حکمرانـی بر هـوش مصنوعی داشـته باشـد. ایـن چشـم‌انداز بایـد بـا مقـررات مناسـب و توجـه بـه خطـرات اخلاقـی (حکمرانـی و اخـلاق) پشـتیبانی شـود. عـلاوه بـر ایـن، دولـت بایـد ظرفیت دیجیتـال داخلـی قـوی داشـته باشـد، از جملـه مهارت‌هـا و شـیوه‌هایی کـه بـه تطبیق‌پذیـری آن در مواجهـه بـا فناوری‌هـای جدیـد کمـک می‌کننـد.

فنـاوری: نهادهـای عمومـی بـرای تأمیـن نیازهـای خـود بـه ابزارهـای هـوش مصنوعـی، بـه عرضـه مناسـب از سـوی بخـش فنـاوری کشـور وابسـته هسـتند. ایـن بخـش بایـد بـه بلـوغ کافـی برسـد تـا بتوانـد پاسـخگوی نیازهـای دولـت باشـد. همچنیـن، بایـد ظرفیـت بـالای نوآوری داشـته باشـد و در محیطـی تجـاری فعالیـت کنـد کـه از کارآفرینـی و سـرمایه‌گذاری در تحقیـق و توسـعه حمایـت می‌کنـد. عـلاوه بـر ایـن، وجـود سـرمایه انسـانی توانمنـد، کـه توسـعه راه‌حل‌هـای پیشـرفته هـوش مصنوعـی را هدایـت کنـد، ضـروری اسـت تـا ایـن بخـش بتوانـد بـه نیازهـای در حـال تغییـر دولت‌هـا پاسـخ دهـد.

داده و زیرسـاخت: ابزارهـای هـوش مصنوعـی بـه داده‌هـای باکیفیـت (دسـترس‌پذیری داده) نیـاز دارنـد تـا از بـروز خطـا و سـوگیری جلوگیـری شـود. ایـن داده‌هـا بایـد نمایانگـر تمامـی شـهروندان یـک کشـور باشـند (نمایـه پذیـری داده). در نهایـت، ابزارهـای هـوش مصنوعـی بـدون زیرسـاخت‌های لازم بـرای توسـعه، اسـتقرار و ارائـه آن‌هـا بـه

شکل ۱. محورهای اصلی و ابعاد استفاده شده در ارزیابی آمادگی هوش مصنوعی دولت

شـهروندان، نمی‌تواننـد به‌طـور مؤثـر مـورد اسـتفاده قـرار گیرنـد.

شـکل ۱ محورهـای اصلـی ارزیابـی هـوش مصنوعـی و ابعـاد هـر محـور را نمایـش مـی دهـد.

جـداول زیـر، ارزیابـی پیشـرفت ابعـاد را بـا محوریت‌هـای حاکمیـت، فنـاوری و داده و زیرسـاخت در سـال ۲۰۲۳ و ۲۰۲۴ بـرای ایـران نشـان می‌دهـد:

جـداول زیـر، ارزیابـی پیشـرفت ابعـاد را بـا محوریت‌هـای حاکمیـت، فنـاوری و داده و زیرسـاخت در سـال ۲۰۲۳[1] و ۲۰۲۴[2] بـرای ایـران نشـان می‌دهـد:

جدول ۲. امتیازبندی شاخص‌های محور حاکمیت

محور حاکمیت					
امتیاز ۲۰۲۳= ۳۱٫۵۶			امتیاز ۲۰۲۴= ۲۶٫۵۴		
بعد	امتیاز ۲۰۲۳	امتیاز ۲۰۲۴	میزان پیشرفت	شاخص	منبع/مرجع
چشم‌انداز	۰	۰	۰	نقشه راه و استراتژی ملی هوش مصنوعی	Desk research (e.g. OECD AI Policy Observatory, UN IDIR AI policy portal)[3]
حاکمیت و اخلاق	۴۴٫۰۱	۳۸٫۱۹	-۵٫۸۲	قوانین حفاظت از داده‌ها و حریم خصوصی	Desk research (with support from the GovTech Maturity Index I-38 and IAPP Global Privacy Law and DPA Directory)[4]
				امنیت سایبری	Global Cybersecurity Index[5]
				کیفیت تنظیم مقررات	Worldwide Governance Indicators[6]
				اصول اخلاقی هوش مصنوعی	OECD AI Principles[7]
				مسئولیت‌پذیری	Worldwide Governance Indicators
ظرفیت دیجیتال	۵۳٫۴۰	۴۴٫۸۱	-۸٫۵۹	سرویس‌های آنلاین دولتی	UN E-Government Survey[8]
				زیرساخت‌های فناوری اطلاعات	GovTech Dataset[9]
				حمایت دولت از پذیرش هوش مصنوعی	World Economic Forum Executive Opinion Survey[10]
				توسعه مهارت‌های هوش مصنوعی در بخش دولتی	Global Index on Responsible AI[11]
سازگاری	۲۸٫۸۵	۲۳٫۱۷	-۵٫۶۸	اثربخشی دولت	Worldwide Governance Indicators
				پاسخگویی و واکنش دولت به تغییرات	World Economic Forum Executive Opinion Survey[12]
				داده‌های تدارکاتی	Global data barometer[13]

1.https://oxfordinsights.com/wp-content/uploads/2024/02/2023-Government-AI-Readiness-Index-Public-Indicator-Data.xlsx
2. https://oxfordinsights.com/wp-content/uploads/2024/12/2024-GAIRI-data.xlsx
3. https://oecd.ai/
4. https://datacatalog.worldbank.org/search/dataset/0037889/govtech-dataset
5. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
6. https://www.worldbank.org/en/publication/worldwide-governance-indicators
7. https://oecd.ai/en/ai-principles
8. https://publicadministration.desa.un.org/Research/UN-e-Government-Surveys
9. https://datacatalog.worldbank.org/search/dataset/0037889/govtech-dataset
10. https://initiatives.weforum.org/executive-opinion-survey/home
11. https://www.global-index.ai/
12. https://initiatives.weforum.org/executive-opinion-survey/home
13. https://globaldatabarometer.org/module/procurement/

جدول ۳. امتیازبندی شاخص‌های محور فناوری

محور فناوری					
امتیاز ۳۸٫۷۷=۲۰۲۳		امتیاز ۳۸٫۸۲=۲۰۲۴			
بعد	امتیاز ۲۰۲۳	امتیاز ۲۰۲۴	میزان پیشرفت	شاخص	منبع/مرجع
بلوغ	۲۳٫۶۵	۲۱٫۶۸	-۱٫۹۷	تعداد استارتاپ‌های میلیارد دلاری در هوش مصنوعی	CB Insights[1]
				تعداد استارتاپ‌های میلیارد دلاری غیر هوش مصنوعی	CB Insights
				ارزش تجارت در خدمات ICT (سرانه)	UNCTAD[2]
				ارزش تجارت در کالاهای ICT (سرانه)	UNCTAD
				هزینه نرم‌افزارهای کامپیوتری	Global Innovation Index[3]
ظرفیت نوآوری	۴۷٫۰۵	۴۷٫۶۴	۰٫۵۹	مدت زمان صرف‌شده برای رسیدگی به مقررات دولتی	World Bank World Development Indicators[4]
				دسترسی به سرمایه خطرپذیر (VC)	DealRoom[5]
				هزینه‌های تحقیق و توسعه (R&D)	UNESCO
				پذیرش هوش مصنوعی برای نوآوری	World Economic Forum Executive Opinion Survey
				مقالات تحقیقاتی هوش مصنوعی	Scimago[6]
سرمایه انسانی	۴۵٫۶۲	۴۷٫۱۲	۱٫۵	فارغ‌التحصیلان در رشته‌های STEM	UNESCO[7]
				فعالیت در گیت‌هاب	GitHub Innovation Graph data[8]
				فارغ‌التحصیلان زن در STEM	UNESCO
				کیفیت آموزش عالی در مهندسی و فناوری	QS World University Rankings[9]
				مهارت‌های ICT	Network Readiness[10]

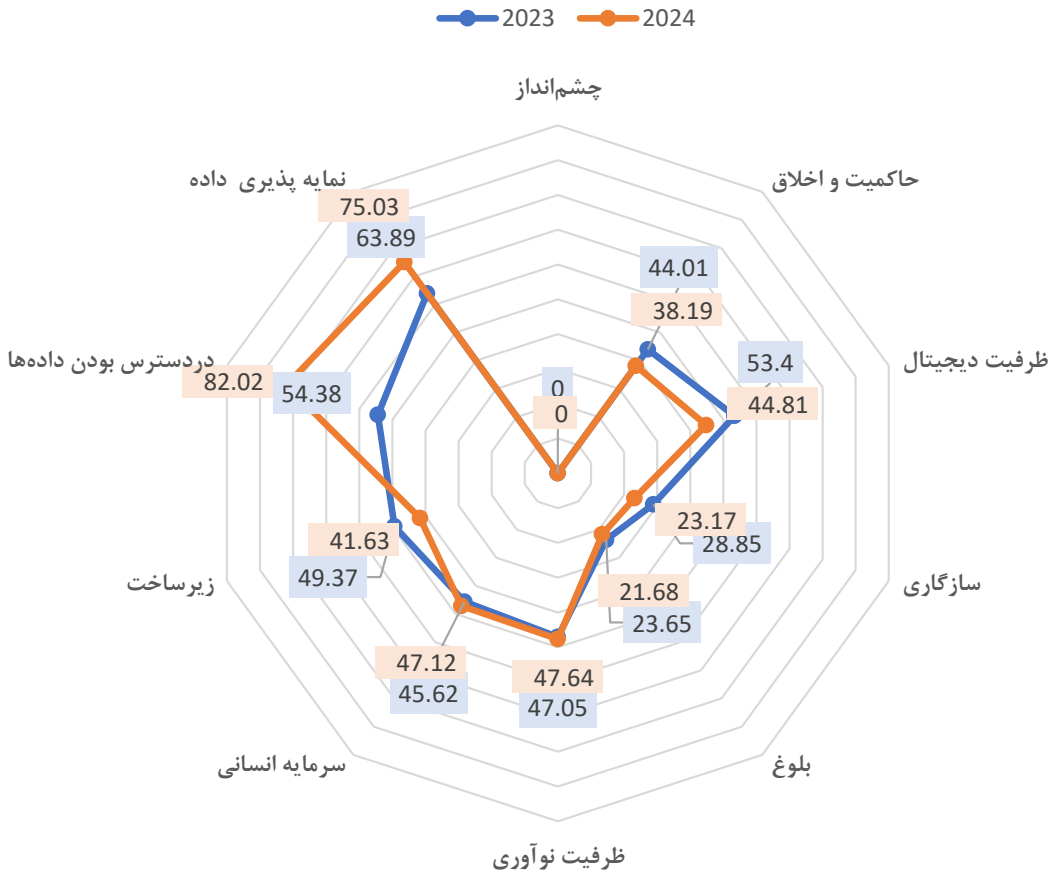
1. https://www.cbinsights.com/research-unicorn-companies
2. https://unctadstat.unctad.org/datacentre
3. https://www.wipo.int/en/web/global-innovation-index
4. https://databank.worldbank.org/source/world-development-indicators/Series/IC.GOV.DURS.ZS
5. https://dealroom.co/guides/global
6. https://www.scimagojr.com/countryrank.php?category=1702&year=2020
7. https://databrowser.uis.unesco.org/
8. https://github.com/github/innovationgraph/blob/main/docs/datasheet.md#schema-for-developerscsv
9. https://www.topuniversities.com/university-subject-rankings/engineering-technology
10. https://networkreadinessindex.org/

جدول ۳. امتیازبندی شاخص‌های محور داده و زیرساخت

داده و زیرساخت					
امتیاز ۲۰۲۳=۶۳٫۳۸		امتیاز ۲۰۲۴=۶۶٫۲۹			
بعد	امتیاز ۲۰۲۳	امتیاز ۲۰۲۴	میزان پیشرفت	شاخص	منبع/مرجع
زیرساخت	۴۹٫۳۷	۴۱٫۶۳	-۷٫۷۴	زیرساخت مخابراتی	UN-EGornment Communications Infrastructure[1]
				سوپرکامپیوترها	top500[2]
				کیفیت پهنای باند	EIU Inclusive Internet Index[3]
				زیرساختG۵	GSMAMobile Connectivity Index[4]
				سازگاری فناوری‌های کلیدی (AI, Big Data, VR, AR)	World Economic Forum Executive Opinion Survey
دردسترس بودن داده‌ها	۵۴٫۳۸	۸۲٫۰۲	۲۷٫۶۴	داده‌های باز	Global data barometer[5]
				حکمرانی داده	Desk research (with support from the GovTech Maturity Index I-34)
				اشتراک تلفن همراه	ITU[6]
				خانوارهای دارای دسترسی به اینترنت	ITU
				ظرفیت آماری	SPI GitHub Report
نمایه پذیری داده۷	۶۳٫۸۹	۷۵٫۰۳	۱۱٫۱۴	شکاف جنسیتی در دسترسی به اینترنت	GSMAMobile Connectivity Index
				مقرون‌به‌صرفه بودن دستگاه‌های همراه	EIU Inclusive Internet Index۸

1. https://publicadministration.un.org/egovkb/en-us/Data-Center
2. https://www.top500.org/lists/top500
3. https://impact.economist.com/projects/inclusive-internet-index/
4. https://www.mobileconnectivityindex.com/index.html#year=2019&dataSet=indexScore
5. https://globaldatabarometer.org/module/procurement/
6. https://datahub.itu.int/data/?i=178&u=per+100+people
7. data representativeness
8. https://impact.economist.com/projects/inclusive-internet-index/

شکل ۲ تغییرات امتیازهای هر بعد از سند را در سال ۲۰۲۳ - ۲۰۲۴ نمایش می دهد.



شکل ۲. مقایسه ابعاد شاخص آمادگی هوش مصنوعی دولت ایران در سال ۲۰۲۳_۲۰۲۴

بررسی تغییرات امتیازات ایران در سه محور کلیدی حکمرانی، تکنولوژی و داده و زیرساخت نشان‌دهنده روندهای متفاوتی در هر بخش است. در محور حاکمیت، کاهش امتیاز از ۳۱٫۵۶ در سال ۲۰۲۳ به ۲۶٫۵۴ در سال ۲۰۲۴ نشان‌دهنده افت قابل‌توجه در این حوزه است. کاهش امتیازات در ابعاد حاکمیت و اخلاق (۵٫۸۲-)، ظرفیت دیجیتال (۸٫۵۹-) و سازگاری (۵٫۶۸-) حاکی از ضعف در انتشار و اجرای سیاست‌های حاکمیتی مؤثر در زمینه هوش مصنوعی است. عدم بهبود در شاخص چشم‌انداز (امتیاز صفر در هر دو سال) نیز بیانگر نبود استراتژی مشخص و شفاف در سطح کلان است.

در محور تکنولوژی، امتیاز کلی تقریباً ثابت مانده و از ۳۸٫۷۷ در سال ۲۰۲۳ به ۳۸٫۸۲ در سال ۲۰۲۴ افزایش جزئی داشته است. پیشرفت در ظرفیت نوآوری (۰٫۵۹+) و سرمایه انسانی(۱٫۵+) از نقاط قوت این بخش محسوب می‌شود که نشان از توانمندی نسبی نیروی انسانی و بهبود در نوآوری‌های فناورانه دارد. بااین‌حال، کاهش امتیاز در بلوغ تکنولوژی (۱٫۹۷-) نشان می‌دهد که روند توسعه فناوری‌های مبتنی بر هوش مصنوعی و بلوغ اکوسیستم فناوری همچنان با چالش‌هایی مواجه است.

در محور
داده و زیرساخت، ایران
با افزایش امتیاز از ۶۳٫۳۸ در
سال ۲۰۲۳ به ۶۶٫۲۹ در سال ۲۰۲۴، بهبود
قابل‌توجهی را تجربه کرده است. این رشد عمدتاً
ناشی از افزایش چشمگیر در دسترس‌پذیری
داده‌ها (+۲۷٫۶۴) و نمایه‌پذیری داده‌ها
(+۱۱٫۱۴) است که نشان‌دهنده پیشرفت در
حوزه مدیریت داده و بهبود امکان پردازش و
تحلیل داده‌های کلان می‌باشد. بااین‌حال،
کاهش امتیاز در زیرساخت (-۷٫۷۴) حاکی از
ضعف در توسعه ظرفیت‌های پردازشی کشور
است که می‌تواند مانعی برای توسعه پایدار در
این حوزه باشد.

به‌طور کلی، افت محسوس در بخش
حاکمیت، ثبات نسبی در بخش تکنولوژی و
بهبود در محور داده و زیرساخت نشان می‌دهد
که درحالی‌که ایران در برخی زمینه‌ها مانند
مدیریت داده‌ها پیشرفت داشته، همچنان
در تدوین سیاست‌های حاکمیتی و تقویت
زیرساخت‌های فناوری نیازمند اصلاحات اساسی
است. اتخاذ رویکردی یکپارچه برای تقویت
حکمرانی، سرمایه‌گذاری در زیرساخت‌های
دیجیتال و حمایت از اکوسیستم نوآوری می‌تواند
زمینه‌ساز رشد پایدار در حوزه هوش مصنوعی
باشد.

یافته‌های کلیدی

- ایران براساس گزارش ۲۰۲۴ آمادگی هوش مصنوعی دولت، با کسب امتیاز ۴۳.۸۸ در رتبه ۹۱ از میان ۱۸۸ کشور قرار گرفته است. این رتبه در مقایسه با سال ۲۰۲۳ (رتبه ۹۴) بهبود یافته، اما نسبت به سال ۲۰۲۲ (رتبه ۷۵) افت چشمگیری داشته است، که نشان‌دهنده نوسانات جایگاه کشور در این حوزه است. در مقابل، کشورهای پیشرو مانند چین، آمریکا و اتحادیه اروپا با سرمایه‌گذاری‌های کلان، سیاست‌گذاری‌های منسجم و برنامه‌های حمایتی، فاصله خود را با ایران افزایش داده‌اند.
- ارزیابی شاخص‌های هوش مصنوعی ایران نشان‌دهنده افت محسوس در حوزه حاکمیت (کاهش امتیاز از 31.56 به 26.54) به دلیل ضعف در سیاست‌گذاری، ظرفیت دیجیتال و سازگاری است. در بخش تکنولوژی، امتیاز کلی تقریباً ثابت مانده، اما کاهش در بلوغ فناوری و پیشرفت جزئی در سرمایه انسانی و نوآوری مشاهده می‌شود. در مقابل، محور داده و زیرساخت با رشد قابل‌توجهی همراه بوده (افزایش از 63.38 به 66.29)، که عمدتاً ناشی از بهبود در دسترس‌پذیری و نمایه‌پذیری داده‌ها است، هرچند که ضعف در زیرساخت‌ها همچنان چالش‌برانگیز است. این روندها نشان می‌دهد که ایران برای پیشرفت در هوش مصنوعی نیازمند سیاست‌گذاری قوی‌تر در حاکمیت، توسعه زیرساخت‌های دیجیتال و حمایت از نوآوری است.
- ایران در حکمرانی هوش مصنوعی با چالش‌های متعددی مواجه است، از جمله عدم انتشار استراتژی

ملی، محدودیت در زیرساخت‌های داده و پـــردازش، و ضعـــف در وضع مقررات امنیت سایبری و حفاظـــت از داده. کمبود ســـرمایه‌گذاری در تحقیق و توســـعه، مهاجرت نخبگان ، و ضعف ارتباط میان دانشگاه و صنعـــت، توســـعه بومی این فناوری را کند کرده است. علاوه بر این، تحریم‌هـــای بین‌المللی دسترسی به فناوری‌های پیشرفته و همکاری‌هـــای علمی را محدود کـــرده و موجـــب عقب‌ماندگی در تعاملات فناورانه شده است.

- نگاشت نهادی و تقسیم کار ملی در راهبردهای ارائه شـــده تا کنون با ابهام و عدم مرزبندی دقیق مواجه است. با توجه به چندبعدی بودن راهبردهای پیشـــنهادی و تنوع حوزه‌های اجرایی، شناســـایی دقیق نهادهای متولی برای هر اقدام ضروری است. اجرای اثربخش سیاست‌های تعیین شده مستلزم تقسیم شفاف مسئولیت‌ها میان نهادهای دولتی، بخش خصوصی و مراکز علمی و تحقیقاتی است تا هر ســـازمان نقش مشخصی در پیشبرد اهداف ایفا کند.
- هر نهاد متولی باید به‌طور مستمر اقداماتی را برای به‌روزرســـانی داده‌ها، بهبـــود برنامه‌ریزی و ارتقای عملکرد سیاست‌ها انجام دهد. این امر شامل پایش مستمر شـــاخص‌ها، بهینه‌سازی تصمیم‌گیری‌های اجرایـــی و ایجاد زیرســـاخت‌های اطلاعاتی کارآمد است. بدون این ســـاختار مدیریتی و مکانیزم‌های نظارتی، اجرای سیاســـت‌ها بـــا چالش‌های جدی روبه‌رو شده و کارایی اقدامات کاهش خواهد یافت.
- نیـــاز به یک نقطـــه کانونی و متمرکـــز برای پایش عملکرد بخشـــها ی مختلـــف و انعکاس شـــاخص هـــای عملکرد در درگاه‌های مرجع جهانی برای اجتناب از ارزیابی های غلط وضعیت ایران ضروری است. ازاین‌رو، تعریف مسئولیت‌ها، به‌روزرســـانی مستمر داده‌ها و ایجاد هماهنگی بین بخش‌های مختلف باید به‌عنوان یک اولویت اساســـی در دستور کار سیاست‌گذاران قرار گیرد.
- یکی از مهم‌ترین دلایل پایین بودن شـــاخص‌های ایـــران در حـــوزه هـــوش مصنوعـــی، کمبـــود زیرســـاخت‌های پردازشـــی و فناوری است؛ عدم توسعه مراکز داده قوی، سرورهای پردازش پیشرفته و پهنای باند مناسب باعث شده که توانایی پردازش داده‌هـــای کلان محـــدود شـــود. همچنین، نبود سوپرکامپیوترهای پیشرفته و تجهیزات سخت‌افزاری کافی، اجرای پروژه‌های پیچیده هوش مصنوعی را دشـــوار کرده اســـت. علاوه بر این، سرمایه‌گذاری

ناکافی در تحقیق و توسعه از دیگر مشکلات عمده است؛ بخش دولتی و خصوصی حمایت لازم را از استارتاپ‌ها و شرکت‌های فناور ندارند و همین امر موجب کندی رشد فناوری در کشور شده است. تحریم‌های اقتصادی و محدودیت‌های بین‌المللی نیز ورود فناوری‌های جدید و دسترسی به منابع خارجی را دشوار کرده، از سوی دیگر، مهاجرت نخبگان و کمبود نیروی متخصص به دلیل نبود فرصت‌های شغلی و پژوهشی مناسب، یکی دیگر از چالش‌های اساسی کشور است، به‌طوری که بسیاری از فارغ‌التحصیلان این حوزه جذب کشورهای توسعه‌یافته می‌شوند.

جمع‌بندی و ارائه پیشنهاد

بررسی سند آکسفورد ۲۰۲۴ نشان می‌دهد که ایران در برخی شاخص‌های فناوری و هوش مصنوعی پیشرفت‌هایی داشته است، اما همچنان در بسیاری از شاخص‌های کلیدی با چالش‌های عمده روبه‌رو است. در مجموع، استعدادهای قابل‌توجهی در زمینه نیروی انسانی، تولید دانش علمی و برخی زیرساخت‌های ارتباطی در کشور وجود دارد، اما در حوزه‌هایی همچون سرمایه‌گذاری، سیاست‌گذاری منسجم، اجرای مقررات، پذیرش فناوری‌های نوین و حمایت از نوآوری در بخش خصوصی، چالش‌های جدی به چشم می‌خورد. بررسی جایگاه ایران در این سند، فاصله قابل‌توجه کشور با رهبران فناوری و نوآوری جهانی را نشان می‌دهد. این وضعیت عمدتاً ناشی از کمبود زیرساخت‌های فناوری، ضعف در حکمرانی داده، محدودیت‌های بین‌المللی و سرمایه‌گذاری ناکافی در تحقیق و توسعه است.

چالش‌های کلیدی

- سرمایه‌گذاری محدود در تحقیق و توسعه و حمایت ناکافی از استارتاپ‌های فناوری
- چالش‌های زیرساختی در حوزه مخابرات، پهنای باند و توسعه 5G
- ضعف در قوانین حفاظت از داده‌ها و حکمرانی دیجیتال
- عدم تدوین استراتژی ملی هوش مصنوعی و سیاست‌های حمایتی شفاف
- فرصت‌های بهبود:
- توسعه سیاست‌های حمایتی برای استارتاپ‌های هوش مصنوعی و نوآوری دیجیتال
- افزایش سرمایه‌گذاری در تحقیق و توسعه و جذب سرمایه‌گذاری خطرپذیر (VC)
- بهبود زیرساخت‌های دیجیتال و ارتباطات
- تدوین چارچوب‌های قانونی قوی‌تر برای امنیت سایبری و حکمرانی داده
- تقویت همکاری‌های بین‌المللی در حوزه فناوری و هوش مصنوعی

علاوه بر تقویت زیرساخت‌های فناوری و افزایش سرمایه‌گذاری در تحقیق و توسعه کشور نیازمند یک سیاست‌گذاری هوشمندانه و یکپارچه در حوزه فناوری و نوآوری است. برای تحقق این هدف، همکاری گسترده میان نهادهای دولتی، بخش خصوصی و دانشگاه‌ها ضروری است. همچنین، افزایش تعاملات بین‌المللی و ایجاد چارچوب‌های قانونی پایدار می‌تواند زمینه‌ساز رشد پایدار در حوزه هوش مصنوعی و فناوری‌های دیجیتال شود.

در نهایت، اگر هدف، کسب جایگاهی بهتر در مسیر تحولات فناوری جهانی باشد، انتشار و اجرای نقشه راه برای توسعه نوآوری، دیجیتالی‌سازی و بهره‌گیری از فناوری‌های نوین ضروری است. این امر نه‌تنها جایگاه کشور را در

رتبه‌بندی‌های جهانی بهبود می‌بخشد، بلکه زمینه‌ساز رشد اقتصادی، اشتغال‌زایی و افزایش رقابت‌پذیری در عرصه بین‌المللی خواهد شد.

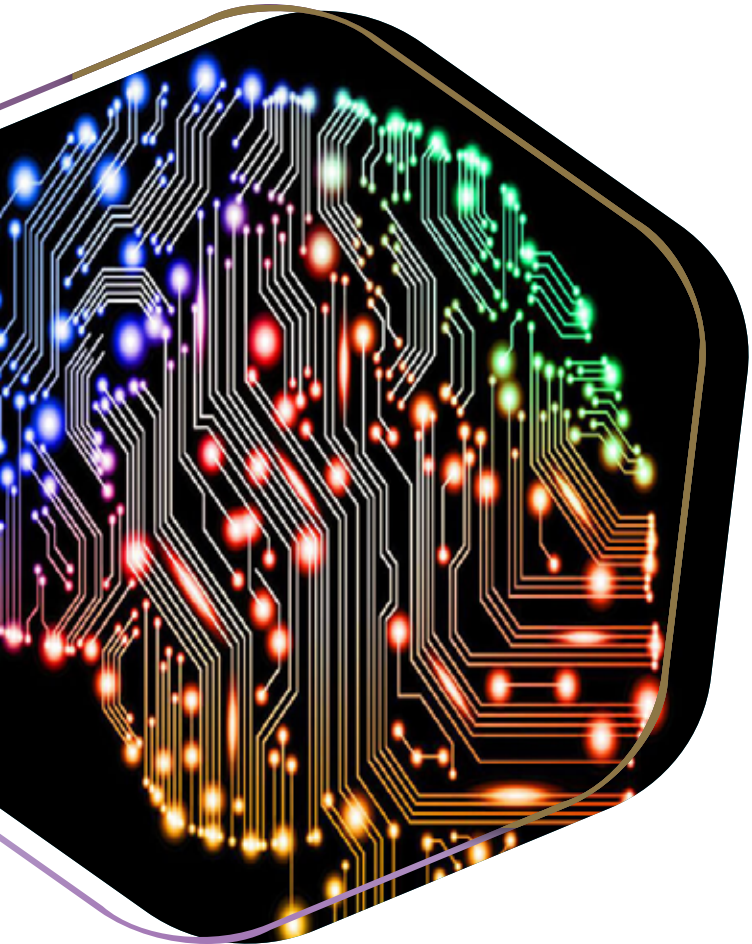
ارتقای جایگاه ایران در شاخص‌های هوش مصنوعی، نیازمند یک برنامه راهبردی ملی، اصلاحات سیاستی، افزایش سرمایه‌گذاری در تحقیق و توسعه، بهبود زیرساخت‌های دیجیتال و تعاملات گسترده علمی و فناوری با سایر کشورها است. بدون اتخاذ رویکردهای نوین و سیاست‌گذاری‌های منسجم، کاهش فاصله با کشورهای پیشرو در حوزه فناوری و هوش مصنوعی دشوار خواهد بود.

برای اجرای مؤثر راهبردهای پیشنهادی و دستیابی به اهداف تعیین‌شده در سند، ضروری است که نهادهای متولی و مسئول اجرای هر یک از این راهبردها به‌دقت شناسایی و بررسی شوند. علاوه بر این، هر نهاد متولی باید به‌طور مستمر اقداماتی را برای برنامه‌ریزی، به‌روزرسانی داده‌ها و بهبود فرآیندهای اجرایی انجام دهد تا ضمن افزایش هماهنگی میان بخش‌های مختلف، امکان ارزیابی مستمر و اصلاح سیاست‌ها بر اساس تغییرات فناوری و نیازهای کشور فراهم شود.

موفقیت در بهبود جایگاه ایران در حوزه هوش مصنوعی، تنها زمانی امکان‌پذیر خواهد بود که مسئولیت‌های اجرایی به‌طور شفاف میان نهادهای دولتی، بخش خصوصی و مراکز علمی و تحقیقاتی تقسیم شود و هر سازمان نقش مشخصی در پیشبرد اهداف ایفا کند.

ازاین‌رو، انجام یک مطالعه جامع برای تحلیل ظرفیت اجرایی نهادهای مرتبط، تدوین نقشه راه عملیاتی و ایجاد هماهنگی بین دستگاه‌های ذی‌ربط ضروری است. این امر مستلزم اجرای یک فعالیت تحقیقاتی مستقل است تا مدل اجرایی مناسبی برای تحقق راهبردهای پیشنهاد شده در سند تدوین شود و از اتلاف منابع جلوگیری گردد. بدون چنین بررسی دقیقی، اجرای سیاست‌ها و راهبردهای کلان، با چالش‌های جدی مواجه خواهد شد و اثربخشی اقدامات کاهش می‌یابد.

همچنین برای ارتقای جایگاه ایران در حوزه هوش مصنوعی، لازم است شاخص‌های کلیدی بر اساس برآورد هزینه‌ها، تأثیرگذاری بر رتبه‌بندی و مقایسه عملکرد با سایر کشورها اولویت‌بندی شوند. این رویکرد به تخصیص کارآمد منابع، شناسایی حوزه‌های با بیشترین بازدهی سرمایه‌گذاری و تسریع پیشرفت در بخش‌های حیاتی کمک خواهد کرد. به‌کارگیری چنین مدلی می‌تواند سیاست‌گذاری را هدفمندتر ساخته، بهره‌وری سرمایه‌گذاری‌ها را افزایش داده و رقابت‌پذیری ایران را در عرصه بین‌المللی تقویت کند.



نقش وزارت ارتباطات و فناوری اطلاعات در ایجاد و توسعه اپراتور هوش مصنوعی

مژگان فرهودی

مرکز نوآوری و توسعه هوش مصنوعی، پژوهشگاه ارتباطات و فناوری اطلاعات

مقدمه

اپراتور هوش مصنوعی[1] به نهاد، سازمان یا شرکتی اطلاق می‌شود که مجموعه‌ای از خدمات و زیرساخت‌های مربوط به هوش مصنوعی را به‌صورت یکپارچه و مقیاس‌پذیر به کاربران و سازمان‌ها ارائه می‌دهد. این خدمات اغلب شامل سه لایه اصلی زیرساخت (IaaS)، سکو (PaaS)، و نرم‌افزار (SaaS) هستند که به توسعه‌دهندگان، محققان، و سازمان‌ها این امکان را می‌دهند تا از ظرفیت‌های هوش مصنوعی بهره‌برداری کنند، بدون اینکه نیاز به ساخت، نگهداری، یا مدیریت این زیرساخت‌ها و خدمات به‌صورت مستقل داشته باشند. اپراتورهای هوش مصنوعی معمولاً به‌عنوان ارائه‌دهندگان AIaaS)هوش مصنوعی به عنوان خدمت) شناخته می‌شوند، که به‌طور خاص شامل پردازش ابری، سکوهای توسعه و آموزش مدل‌های هوش مصنوعی، سرویس‌های تحلیل داده، یادگیری ماشین، بینایی کامپیوتری، پردازش زبان طبیعی، و سایر کارکردهای مشابه می‌شوند.

این اپراتورها می‌توانند زیرساخت‌های پردازشی مانند رایانش ابری، GPUها و منابع مقیاس‌پذیر را فراهم کرده و همچنین سکوها و ابزارهای توسعه لازم برای ساخت، آموزش و استقرار مدل‌های هوش مصنوعی را در اختیار کاربران قرار دهند. به‌طور کلی، اپراتورهای هوش مصنوعی نقش کلیدی در تسهیل و تسریع فرآیندهای تحقیقاتی، توسعه و پیاده‌سازی هوش مصنوعی دارند و با فراهم‌آوردن سرویس‌های مقیاس‌پذیر و دسترسی به زیرساخت‌های پیشرفته، به سازمان‌ها کمک می‌کنند تا از هوش مصنوعی در محصولات و خدمات خود بهره ببرند.

هدف از این گزارش، استانداردسازی تعریف‌های اولیه در راستای ایجاد یک فهم مشترک از موضوع و سپس تبیین جایگاه وزارت ارتباطات و پژوهشگاه در راستای ایجاد این اپراتورها در زیست‌بوم هوش مصنوعی کشور می باشد.

واژگان و اصطلاحات

اپراتور هوش مصنوعی: شرکت یا نهادی است که خدمات هوش مصنوعی در لایه‌های مختلف را در فضای ابری ارائه می‌دهد (AIaaS)

هوش مصنوعی به عنوان یک خدمت: مدلی از ارائه خدمات ابری است که در آن سازمان‌ها، شرکت‌ها و اشخاص می‌توانند بدون نیاز به توسعه یا مدیریت زیرساخت‌ها و الگوریتم‌های پیچیده، از قابلیت‌های هوش مصنوعی آماده (در لایه‌های مختلف زیرساخت،

1. AI Operator

سکوی توسعه و نرم‌افزار) مانند پردازش زبان طبیعی، تشخیص تصویر، و یادگیری ماشین بهره‌مند شوند.

سکو/پلتفورم هوش مصنوعی: یک بستر نرم‌افزاری است که ابزارها، فریم‌ورک‌ها و زیرساخت‌های لازم برای توسعه، آموزش، استقرار و مدیریت مدل‌های هوش مصنوعی را به‌صورت یکپارچه ارائه می‌دهد.

زیرساخت به عنوان یک خدمت[1]: ارائه زیرساخت‌های موردنیاز برای پردازش و اجرای مدل‌های هوش مصنوعی، شامل سرورها، ذخیره‌سازی، و شبکه، به‌صورت مقیاس‌پذیر و مدیریت‌شده در فضای ابری.

سکوی توسعه به عنوان یک خدمت[2]: ارائه ابزارها و محیط‌های توسعه برای ساخت، آموزش، و استقرار مدل‌های هوش مصنوعی در فضای ابری

نرم‌افزار به عنوان یک سرویس[3]: ارائه نرم‌افزارها، الگوریتم‌ها و مدل‌های مبتنی بر هوش مصنوعی در حوزه‌های مختلف در فضای ابری

دلیل نیاز به اپراتور هوش مصنوعی در کشو ر

وجود اپراتور هوش مصنوعی در کشور به دلایل زیر از اهمیت بالایی برخوردار است:

۱. توسعه زیست‌بوم هوش مصنوعی بومی: ایران به دلیل ساختارهای فرهنگی، زبانی، و اقتصادی خاص خود نیاز به خدمات هوش مصنوعی بومی دارد که توسط اپراتورهای داخلی طراحی و ارائه شوند. این خدمات باید نیازهای خاص کاربران ایرانی را پاسخ دهند و استقلال فناوری را تضمین کنند.

۲. حاکمیت داده و امنیت ملی: در نبود اپراتورهای داخلی، وابستگی به سرویس‌های خارجی می‌تواند امنیت داده‌های حساس کشور را به خطر بیندازد. اپراتور هوش مصنوعی به مدیریت امن داده‌های ملی و حاکمیت بر آن کمک می‌کند.

۳. کاهش وابستگی به فناوری‌های خارجی: ایجاد اپراتورهای هوش مصنوعی می‌تواند جایگزینی برای وابستگی به پلتفرم‌ها و زیرساخت‌های بین‌المللی باشد، به‌ویژه در شرایط تحریم‌ها که دسترسی به این فناوری‌ها محدود است.

۴. تسهیل دسترسی کسب‌وکارها به فناوری هوش مصنوعی: بسیاری از کسب‌وکارهای کوچک و متوسط در ایران توانایی راه‌اندازی زیرساخت‌های پیچیده هوش مصنوعی را ندارند. اپراتور هوش مصنوعی می‌تواند با ارائه خدمات زیرساختی و پلتفرمی این نیازها را رفع کند و راه را برای رشد فناوری در صنایع مختلف هموار سازد.

۵. ایجاد یکپارچگی و استانداردسازی: وجود اپراتور هوش مصنوعی به تنظیم استانداردهای بومی برای جمع‌آوری، پردازش و تحلیل داده‌ها کمک می‌کند و می‌تواند از پراکندگی در توسعه فناوری جلوگیری کند.

۶. تحریک رشد اقتصادی و نوآوری: اپراتورهای هوش مصنوعی می‌توانند بستر لازم برای توسعه نوآوری‌ها و استارتاپ‌های حوزه هوش مصنوعی را فراهم کنند و در نهایت محرکی برای رشد اقتصادی کشور باشند.

۷. رقابت‌پذیری جهانی: اگر ایران بخواهد در میدان رقابت جهانی در حوزه هوش مصنوعی

1. IaaS (Infrastructure as a Service)
2. PaaS (Platform as a Service)
3. SaaS (Software as a Service)

نقش مؤثری داشته باشد، وجود اپراتورهایی که بتوانند خدمات پیشرفته و بومی ارائه دهند، ضروری است.

۸. تقویت صنعت‌های دیجیتال: اپراتورهای هوش مصنوعی می‌توانند زیرساخت‌های لازم برای توسعه صنایع دیجیتال مانند تجارت الکترونیک، تبلیغات دیجیتال، رسانه‌های اجتماعی، وفناوری‌های مالی را فراهم کنند.

در نهایت، اپراتور هوش مصنوعی می‌تواند به‌عنوان ستون فقرات تحول دیجیتال در کشور عمل کند و نقشی کلیدی در توسعه پایدار فناوری و اقتصاد ایران ایفا کند.

مدل‌های اجرایی برای توسعه اپراتور هوش مصنوعی در کشور

نحوه اجرایی شدن اپراتور هوش مصنوعی را می‌توان از دو زاویه اصلی بررسی کرد. هر زاویه، رویکرد متفاوتی در طراحی و مدیریت این اپراتورها ارائه می‌دهد که هر یک مزایا و چالش‌های خاص خود را دارند.

- **رویکرد اول: اپراتور یکپارچه با مدیریت مرکزی**

در این مدل، یک نهاد یا شرکت واحد مسئولیت تمامی لایه‌های AIaaS (هوش مصنوعی به‌عنوان سرویس) را بر عهده دارد. این نهاد به‌صورت متمرکز خدمات زیرساخت، ابزارهای هوش مصنوعی، و سرویس‌های کاربردی را توسعه داده و مدیریت می‌کند.

ویژگی‌های این رویکرد عبارتند از:

- تمرکز کامل بر ارائه خدمات: تمام مراحل از طراحی زیرساخت تا توسعه سرویس‌ها توسط یک نهاد واحد انجام می‌شود.
- یکپارچگی در مدیریت: مدیریت متمرکز موجب می‌شود که هماهنگی بین بخش‌های مختلف ساده‌تر باشد و تصمیم‌گیری‌ها سریع‌تر انجام شوند.
- چالش‌ها: در این مدل، بار مالی و اجرایی بر عهده یک نهاد است که ممکن است در مواجهه با گستردگی نیازها و مقیاس کشور، مشکلاتی ایجاد کند.

- **رویکرد دوم: اپراتور به‌عنوان هاب هماهنگی**

در این رویکرد، اپراتور هوش مصنوعی نقش هماهنگ‌کننده و مدیریت‌کننده را ایفا می‌کند و ارائه‌دهندگان سرویس‌های مختلف از شرکت‌ها و نهادهای متعدد وارد عمل می‌شوند.

ویژگی‌های این مدل شامل موارد زیر است:

- انعطاف‌پذیری بیشتر: مسئولیت ارائه سرویس‌ها به شرکت‌های مختلف سپرده می‌شود که می‌توانند هر یک تخصص خود را در یک حوزه مشخص ارائه دهند.
- تنوع در ارائه خدمات: حضور چندین ارائه‌دهنده سرویس موجب تنوع و کیفیت بهتر خدمات می‌شود.
- چالش‌ها: این مدل نیازمند مدیریت پیچیده‌تر برای هماهنگی بین ارائه‌دهندگان مختلف و حفظ استانداردهای یکپارچه است.

- **مدل ترکیبی: اپراتورهای متعدد برای حوزه‌های مختلف**

نگاه دیگر این است که به جای تمرکز بر یک اپراتور واحد، اپراتورهای متعددی برای حوزه‌های مختلف هوش مصنوعی ایجاد شوند. هر اپراتور می‌تواند با تمرکز بر یک حوزه خاص (مانند بینایی ماشین، پردازش زبان طبیعی، سلامت، حمل‌ونقل هوشمند و...) به ارائه خدمات بپردازد.

این اپراتورها نیز می‌توانند به یکی از دو روش زیر عمل کنند:

۱. مدل یکپارچه: در آن هر اپراتور مسئولیت کامل ارائه خدمات در حوزه خود را بر عهده دارد.

۲. مدل هاب هماهنگی: در آن اپراتور تنها نقش مدیریت و هماهنگی را داشته و ارائه‌دهندگان مختلف در آن حوزه فعالیت می‌کنند.

- **مدل بهینه**

انتخاب مدل مناسب برای ایجاد اپراتور هوش مصنوعی به عوامل متعددی از جمله ظرفیت‌های موجود، نیازهای بازار، چالش‌های اجرایی و اولویت‌های ملی بستگی دارد.

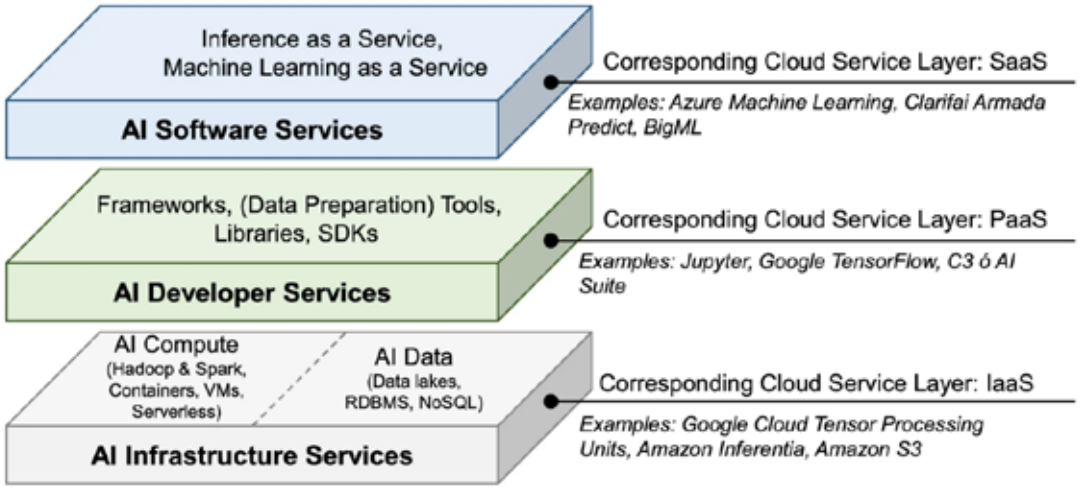
- مدل یکپارچه می‌تواند در مراحل ابتدایی و برای ایجاد استانداردهای اولیه کارآمد باشد.
- مدل هاب هماهنگی برای گسترش سریع خدمات و بهره‌گیری از ظرفیت‌های متنوع مناسب‌تر است.
- ایجاد اپراتورهای متعدد برای حوزه‌های خاص نیز می‌تواند به توزیع بار اجرایی کمک کرده و توسعه متوازن فناوری هوش مصنوعی در کشور را تسهیل کند.

لایه‌های مختلف خدمات در هوش مصنوعی به عنوان یک خدمت

شکل ۱، یک نمای کلی از لایه‌های مختلف در هوش مصنوعی به عنوان یک خدمت را نشان می‌دهد. این مدل شامل سه لایه اصلی است که عبارتند از:

- خدمات زیرساخت هوش مصنوعی که به لایه IaaS معروف است و در آن توان محاسباتی خام، ذخیره‌سازی داده‌ها و ظرفیت شبکه برای ساخت و آموزش الگوریتم‌های هوش مصنوعی در اختیار متقاضیان قرار می‌گیرد. به عبارتی این لایه پایه‌ای‌ترین سطح معماری را تشکیل می‌دهد و شامل منابع پردازشی مانند GPU/TPU، ذخیره‌سازی مقیاس‌پذیر، و سرویس‌های ابری، شبکه‌های ارتباطی برای انتقال داده (CDN)، پایگاه‌داده کلان مانند MongoDB است. این بخش به اپراتور امکان می‌دهد تا قابلیت‌های مقیاس‌پذیر و امن را برای اجرای مدل‌ها و پردازش داده‌ها فراهم کند.

- خدمات توسعه‌دهنده هوش مصنوعی که به لایه PaaS معروف است و در آن ابزارهایی برای کمک به توسعه‌دهندگان در پیاده‌سازی و استفاده از قابلیت‌های هوش مصنوعی ارائه می‌گردد. این بخش واسطی میان زیرساخت و سرویس‌های هوش مصنوعی است و ابزارهایی مانند فریم‌ورک‌های یادگیری ماشین، رابط‌های



شکل ۱. لایه‌های مختلف خدمات در هوش مصنوعی به عنوان یک خدمت

برنامه‌نویسی کاربردی (API)، و سکوهای توسعه مدل مانند تنسورفلو، ابزارهای توسعه و آموزش مدل مانند google colab را ارائه می‌دهد. این لایه به توسعه‌دهندگان کمک می‌کند تا مدل‌ها را ایجاد، آموزش و مدیریت کنند.

- خدمات نرم‌افزار هوش مصنوعی که به لایه SaaS معروف است و در آن برنامه‌ها و ابزارهای آماده برای استفاده مانند ابزارهای تحلیل داده‌ها، پردازش زبان طبیعی (NLP)، بینایی کامپیوتری، سیستم‌های توصیه‌گر، سرویس‌های صوتی، چت‌بات‌ها و غیره به کاربران ارائه می‌شود. این سرویس‌ها معمولاً به‌صورت آماده یا قابل‌پیکربندی در اختیار توسعه‌دهندگان و کسب‌وکارها قرار می‌گیرند.

لازم به ذکر است چند نمونه از مدل‌های مطرح AIaaS از گوگل، آمازون و مایکروسافت در گزارش پیوست آمده است.

ذی نفعان اپراتور هوش مصنوعی

در ادامه ذی‌نفعان و بازیگران اپراتور هوش مصنوعی به همراه شرح مختصری برای هر کدام آمده است:

- دولت و نهادهای دولتی: مسئول تنظیم سیاست‌ها، قوانین و مقررات مربوط به استفاده از هوش مصنوعی و ایجاد بسترهای قانونی برای توسعه آن هستند. همچنین، نقش مهمی در استانداردسازی، و نظارت بر کیفیت و عملکرد محصولات و خدمات هوش مصنوعی را به‌عهده دارند.
- شرکت‌ها و سازمان‌های بخش خصوصی: شامل اپراتورهای هوش مصنوعی که خدمات زیرساخت، سکو و سرویس‌های هوش مصنوعی را ارائه می‌دهند. این بخش همچنین شامل شرکت‌های فناوری، استارتاپ‌ها و مشاوران است که در پیاده‌سازی و توسعه راه‌حل‌های مبتنی بر هوش مصنوعی فعال هستند.
- سازمان‌های تحقیقاتی و دانشگاه‌ها: مراکز پژوهشی که در زمینه توسعه الگوریتم‌ها و مدل‌های جدید هوش مصنوعی کار می‌کنند و از طریق آموزش نیروی انسانی متخصص، به پیشرفت این حوزه کمک می‌کنند. همچنین، آزمایشگاه‌های تحقیقاتی در زمینه‌های خاص نیز در این گروه قرار دارند.
- کاربران نهایی و صنایع مختلف: کسب‌وکارهایی که از هوش مصنوعی برای بهبود عملیات و خدمات خود استفاده می‌کنند، به ویژه در صنایع مختلف مانند سلامت، حمل‌ونقل و تولید. این بخش همچنین شامل استارتاپ‌ها و بخش‌های دولتی است که از هوش مصنوعی در خدمات عمومی بهره می‌برند.
- مصرف‌کنندگان: افراد و کاربران نهایی که از محصولات و خدمات مبتنی بر هوش مصنوعی در زندگی روزمره خود استفاده می‌کنند، مانند دستیارهای صوتی، خودروهای خودران و سیستم‌های شناسایی.
- ارائه‌دهندگان زیرساخت‌های فناوری: شامل شرکت‌هایی که سخت‌افزار و نرم‌افزارهای لازم برای پردازش و ذخیره‌سازی داده‌های مرتبط با هوش مصنوعی را فراهم می‌کنند، همچنین اپراتورهای شبکه که بسترهای ارتباطی برای پردازش داده‌ها را ارائه می‌دهند.
- نهادهای مالی و سرمایه‌گذاری: صندوق‌های سرمایه‌گذاری، بانک‌ها و سایر نهادهای مالی که منابع مالی لازم را برای پروژه‌ها و استارتاپ‌های هوش مصنوعی تأمین می‌کنند تا این پروژه‌ها به مرحله اجرایی برسند.
- نهادهای اخلاقی و حقوقی: شامل

سازمان‌هایی که بر رعایت اصول اخلاقی در استفاده از هوش مصنوعی نظارت می‌کنند و همچنین مشاوران حقوقی که به مسائل مربوط به حریم خصوصی، مالکیت داده‌ها و حقوق افراد در این زمینه می‌پردازند.

نمونه‌هایی از اپراتور هوش مصنوعی در دیگر کشورها

اپراتورهای هوش مصنوعی بیشتر در کشورهای پیشرفته یا در حال توسعه که سرمایه‌گذاری بالایی در زمینه هوش مصنوعی داشته‌اند، فعالیت می‌کنند. نمونه‌هایی از این کشورها عبارتند از:

۱. ایالات متحده: شرکت‌هایی مانند Google (Cloud AI)، Microsoft (Azure AI)، و Amazon (AWS AI) خدمات گسترده‌ای به عنوان اپراتور هوش مصنوعی ارائه می‌دهند. دولت آمریکا از طریق DARPA و سایر نهادها نیز به ایجاد زیرساخت‌های AI پرداخته است.

۲. چین: شرکت‌هایی مثل Baidu, Tencent و Alibaba نقش کلیدی در ارائه خدمات هوش مصنوعی دارند. دولت چین نیز سرمایه‌گذاری کلانی در ایجاد زیرساخت‌های AI داشته است.

۳. اتحادیه اروپا: کشورهای آلمان، فرانسه، و هلند از پیشگامان AI در اروپا هستند. برنامه‌هایی مانند GAIA-X برای ایجاد زیرساخت‌های مشترک داده و هوش مصنوعی در اروپا طراحی شده است.

۴. کانادا: موسساتی مانند Vector Institute و MILA نقش کلیدی در توسعه هوش مصنوعی دارند. دولت کانادا از طریق برنامه‌های ملی AI به توسعه این حوزه کمک می‌کند.

۵. هند: شرکت‌های فناوری مانند Infosys, TCS, و Wipro در حال ارائه خدمات AI هستند. دولت هند برنامه ملی AI (NITI Aayog) را برای ایجاد زیرساخت‌های هوش مصنوعی طراحی کرده است.

۶. سنگاپور: به دلیل اندازه کوچک و فناوری‌محور بودن، سنگاپور یکی از پیشروان هوش مصنوعی در آسیا است. پروژه‌هایی مانند AI Singapore برای تسهیل دسترسی به داده‌ها و زیرساخت‌ها طراحی شده است.

۷. امارات متحده عربی: با راه‌اندازی وزارت هوش مصنوعی و پروژه‌هایی مانند AI Lab Initiative، امارات به دنبال تبدیل شدن به یکی از مراکز جهانی هوش مصنوعی است.

۸. استرالیا: نهادهایی مانند CSIRO و برنامه‌های دولت استرالیا در زمینه AI از توسعه زیرساخت‌های اپراتوری حمایت می‌کنند.

۹. ژاپن و کره جنوبی: شرکت‌هایی مانند SoftBank, Fujitsu در ژاپن و Samsung, LG در کره جنوبی نقش مهمی در توسعه زیرساخت‌های هوش مصنوعی دارند.

وضعیت موجود اپراتور هوش مصنوعی در کشور

وضعیت اپراتورهای هوش مصنوعی در ایران در حال حاضر در مرحله ابتدایی و توسعه است، با این حال گام‌هایی به سمت ایجاد زیرساخت‌های لازم و بسترهای مناسب برداشته شده است. به عنوان مثال شرکت‌هایی مانند پارت، اهورا و آرمان رایان شریف، پلتفرم‌هایی را برای پردازش و تحلیل دادگان و سایر خدمات مرتبط ارائه می‌دهند و یا شرکت‌هایی مانند گرین‌وب و هماکلاد نیز به ارائه زیرساخت‌هایی پردازشی برای توسعه محصولات و خدمات هوش مصنوعی می‌پردازند. اما علیرغم تلاش‌های شرکت‌ها،

برای گسترش دامنه خدمات و هماهنگی با سایر بخش‌ها نیاز به توجه بیشتری و فعالیت‌های متمرکزتری در کشور وجود دارد.

نقش دولت و وزارت ارتباطات در ایجاد و توسعه اپراتور هوش مصنوعی

نقش دولت (و به تبع آن وزارت ارتباطات) در توسعه و ایجاد اپراتور یا سکوی هوش مصنوعی و ارتباط با سایر ذی‌نفعان در چند حوزه کلیدی ذکر می‌شود:

- تنظیم چارچوب‌های قانونی و سیاستی: دولت و وزارت ارتباطات مسئول تدوین قوانین و مقررات مرتبط با توسعه و بهره‌برداری از هوش مصنوعی در کشور هستند. این قوانین باید به‌گونه‌ای طراحی شوند که هم از نوآوری در این حوزه حمایت کنند و هم حریم خصوصی و حقوق کاربران را تضمین کنند.
- ایجاد زیرساخت‌های فناورانه و استاندارد: دولت باید زیرساخت‌های لازم برای توسعه سکوهای هوش مصنوعی را فراهم کند، از جمله تأمین بسترهای نرم‌افزاری و سخت‌افزاری مناسب، استانداردسازی فرآیندهای هوش مصنوعی و ایجاد محیط‌های آزمایشگاهی برای ارزیابی و تست مدل‌ها و الگوریتم‌ها.
- تسهیل همکاری و هماهنگی میان ذی‌نفعان: وزارت ارتباطات باید زمینه همکاری میان بخش‌های دولتی، خصوصی، دانشگاه‌ها و مراکز تحقیقاتی را تسهیل کند. این همکاری‌ها می‌توانند شامل پروژه‌های مشترک تحقیقاتی، به‌اشتراک‌گذاری داده‌ها و منابع، و طراحی چارچوب‌های مشترک برای توسعه و ارزیابی محصولات هوش مصنوعی باشند.
- حمایت از نوآوری و توسعه بازار: دولت نقش حمایت‌کننده از شرکت‌های نوپا و استارتاپ‌ها در حوزه هوش مصنوعی را ایفا می‌کند. این حمایت می‌تواند شامل ارائه تسهیلات مالی، مشاوره فنی، یا ایجاد بستری مناسب برای جذب سرمایه‌گذاران داخلی و خارجی باشد.
- ایجاد نهادهای نظارتی و ارزیابی: دولت باید نهادهایی برای نظارت و ارزیابی محصولات و خدمات هوش مصنوعی ایجاد کند تا از انطباق آن‌ها با استانداردها و قوانین موجود اطمینان حاصل شود. این نهادها به تضمین کیفیت و قابلیت اطمینان فناوری‌های هوش مصنوعی کمک خواهند کرد.
- آموزش و توانمندسازی منابع انسانی: دولت باید برنامه‌های آموزشی برای پرورش نیروی انسانی متخصص در زمینه هوش مصنوعی داشته باشد و با همکاری دانشگاه‌ها و مؤسسات آموزشی، نیروی کار متخصص را در این حوزه تربیت کند.

با این رویکرد، دولت و وزارت ارتباطات می‌توانند به عنوان تسهیل‌کننده و تنظیم‌کننده اصلی در توسعه اپراتورها و سکوهای هوش مصنوعی عمل کنند و زمینه‌های لازم برای همکاری مؤثر میان سایر ذی‌نفعان را فراهم آورند. این ارتباط و همکاری در نهایت به رشد سریع‌تر و پایدارتر صنعت هوش مصنوعی کشور کمک خواهد کرد.

نقش آزمایشگاه‌های ارزیابی در اپراتورهای هوش مصنوعی

نقش و جایگاه آزمایشگاه هوش مصنوعی در یک اپراتور هوش مصنوعی می‌تواند بسیار حیاتی و مؤثر باشد. این آزمایشگاه‌ها به عنوان نهادهای تحقیقاتی و ارزیاب، نقشی اساسی در

ایجـاد، توسـعه و تسـت سیسـتم‌ها و مدل‌هـای هـوش مصنوعـی و اطمینـان از عملکـرد صحیـح و مؤثـر آنهـا ایفـا می‌کننـد. آزمایشـگاه‌های ارزیابـی بـا ارزیابـی دقیـق و جامـع مدل‌هـا و داده‌هـا، بـه توسـعه‌دهندگان کمـک می‌کننـد تـا سیسـتم‌های هـوش مصنوعـی بـا کیفیـت بـالا و مطابـق بـا نیازهـای کاربـران و مقـررات موجـود تولیـد کننـد. از ایـن رو، آزمایشـگاه‌های ارزیابـی می‌تواننـد بـه عنـوان ارگان‌هـای حیاتـی در اکوسیسـتم هـوش مصنوعـی در نظـر گرفتـه شـوند. در ادامـه، نقش‌ها و جایـگاه آزمایشـگاه(های) ارزیابـی در اپراتـور هـوش مصنوعـی بـه تفصیـل توضیـح داده می‌شـود:

۱. طراحی شیوه‌نامه‌های ارزیابی: آزمایشگاه‌های ارزیابی مسئول تدوین شیوه‌نامه‌ها و استانداردهای ارزیابی محصولات و خدمات هوش مصنوعی هستند. این شیوه‌نامه‌ها باید مشخص کنند که چگونه می‌توان مدل‌ها و سیستم‌های هوش مصنوعی را در محیط‌های مختلف ارزیابی کرد تا از صحت عملکرد آن‌ها اطمینان حاصل شود.

۲. ارزیابی کیفیت داده‌ها: برای ارزیابی مؤثر سیستم‌های هوش مصنوعی، باید داده‌های استفاده‌شده از نظر کیفیت و دقت بررسی شوند. آزمایشگاه‌های ارزیابی این وظیفه را بر عهده دارند تا اطمینان حاصل کنند که داده‌ها بدون نقص و به درستی برچسب‌گذاری شده‌اند.

۳. برگزاری آزمایش‌های عملیاتی: آزمایشگاه‌های ارزیابی باید سیستم‌های هوش مصنوعی را در شرایط واقعی یا شبیه به آن ارزیابی کنند. این آزمایش‌ها می‌توانند شامل تست‌های عملکردی، تست‌های تطابق با نیازهای کاربر و حتی بررسی تأثیرات اجتماعی و اخلاقی سیستم‌های هوش مصنوعی باشند.

۴. گزارش‌دهی و تحلیل نتایج: یکی از وظایف مهم آزمایشگاه‌های ارزیابی، گزارش‌دهی دقیق و شفاف نتایج ارزیابی‌ها است. این گزارش‌ها باید نه تنها به کاربران و ذینفعان اطلاعات مفیدی ارائه دهند، بلکه باید شامل پیشنهادات و بهبودهایی برای توسعه مدل‌ها باشند.

۵. تضمین تطابق با استانداردها و مقررات: آزمایشگاه‌های ارزیابی باید اطمینان حاصل کنند که سیستم‌های هوش مصنوعی با استانداردهای بین‌المللی و مقررات قانونی در حوزه‌های مختلف تطابق دارند. این شامل رعایت مسائل مربوط به حریم خصوصی، امنیت، و اخلاقیات می‌شود.

۶. توسعه بنچمارک‌ها و شاخص‌های مقایسه‌ای: آزمایشگاه‌های ارزیابی می‌توانند بنچمارک‌ها (معیارهای مقایسه‌ای) برای ارزیابی مدل‌ها و سیستم‌های هوش مصنوعی در حوزه‌های مختلف ایجاد کنند. این بنچمارک‌ها می‌توانند به کاربران کمک کنند تا مدل‌ها را از نظر عملکرد مقایسه کنند.

۷. آموزش و توانمندسازی متخصصان ارزیابی: آزمایشگاه‌های ارزیابی می‌توانند نقش مهمی در آموزش و توانمندسازی

متخصصان ارزیابی ایفا کنند. این آموزش‌ها باید شامل مفاهیم ارزیابی، تحلیل داده‌ها، و پیاده‌سازی شیوه‌نامه‌های ارزیابی باشد.

نقش و جایگاه پژوهشگاه در راستای تحقق اپراتور هوش مصنوعی و اقدامات انجام شده

پژوهشگاه در راستای تحقق اپراتور هوش مصنوعی نقش حیاتی در طراحی و توسعه زیرساخت‌ها، استانداردها و زیرساخت‌های ارزیابی ایفا می‌کنند. در این راستا، اقدامات متعددی انجام شده است که در ادامه توضیح داده می‌شود:

- توسعه مراکز داده در کشور
- توسعه زیرساخت‌های پردازشی سریع نظیر ابررایانه سیمرغ
- حمایت از پژوهش و نیروی انسانی متخصص از طریق حمایت از پایان‌نامه‌های تحصیلات تکمیلی و ظرفیت سربازهای نخبه در زمینه هوش مصنوعی به‌منظور توسعه دانش بومی و حل چالش‌های ملی و همچنین
- طراحی و راه‌اندازی آزمایشگاه مرجع ارزیابی محصولات و خدمات پایه هوش مصنوعی و شروع شکل‌دهی شبکه آزمایشگاهی در کشور در حوزه‌های مختلف هوش مصنوعی
- تشکیل دبیرخانه استاندارد ISO شاخه JTC1/ SC42 در حوزه هوش مصنوعی

ارائه راهکار کلان درخصوص ایجاد و توسعه اپراتور هوش مصنوعی

برای ایجاد و توسعه اپراتور هوش مصنوعی در کشور، نیاز به یک راهکار کلان و جامع است که شامل مراحل طراحی، استقرار، توسعه و بهبود مستمر اپراتور باشد. این راهکار باید به نیازهای بومی کشور، چالش‌های خاص، و همچنین توانمندی‌های موجود توجه داشته باشد. در ادامه یک راهکار کلان برای ایجاد و توسعه اپراتور هوش مصنوعی پیشنهاد شده است:

۱. طراحی معماری کلان اپراتور هوش مصنوعی
۲. تدوین استانداردها و چارچوب‌های ارزیابی
۳. حمایت از نوآوری و پژوهش‌های بومی
۴. ایجاد زیرساخت داده و بسترهای جمع‌آوری داده‌های بومی
۵. توسعه برنامه‌های آموزشی و مهارت‌سازی
۶. ایجاد اکوسیستم قانون‌گذاری و نظارت
۷. حمایت مالی و سرمایه‌گذاری

جمع‌بندی

با توجه به مطالب گفته شده، ایجاد و یا توسعه اپراتور(های) هوش مصنوعی در کشور نیازمند همکاری میان دولت، بخش خصوصی، دانشگاه‌ها، و نهادهای تحقیقاتی است. این اپراتور باید به‌عنوان یک چارچوب مشترک و زیرساخت بومی برای توسعه، ارزیابی، و استقرار مدل‌های هوش مصنوعی عمل کند. در این راستا، استانداردسازی و آزمایشگاه‌های ارزیابی از اهمیت ویژه‌ای برخوردارند که می‌توانند موجب اعتمادسازی و تضمین کیفیت در استفاده از فناوری‌های هوش مصنوعی شوند.


گزارش ویژه

دستیابی به عمق هوش مصنوعی
لایه زیرساخت

تهیه شده توسط
مرکز نوآوری و توسعه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات
برگرفته از نشست «تبیین لایه‌های عمیق هوش مصنوعی در لایه زیرساخت»

پیشگفتار

هوش مصنوعی در سال‌های اخیر به یکی از محورهای اساسی توسعه علمی و فناورانه در جهان تبدیل شده و کشورهای پیشرو، با سرمایه‌گذاری‌های کلان در این حوزه، به‌دنبال کسب مزیت‌های راهبردی در ابعاد مختلف اقتصادی، نظامی، اجتماعی و فرهنگی هستند. این فناوری به دلیل برخورداری از لایه‌های پیچیده و عمیق، صرفاً محدود به بهره‌برداری از ابزارها و الگوریتم‌های موجود نیست؛ بلکه دستیابی به تسلط کامل بر آن مستلزم توسعه زیرساخت‌های بومی، تولید داده‌های باکیفیت و متنوع، طراحی مدل‌های پیشرفته و به‌کارگیری مناسب آن در کاربردهای گوناگون است. رهبر معظم انقلاب اسلامی در نخستین دیدار اعضای هیئت دولت چهاردهم، با تأکید بر این موضوع، هشدار دادند که بهره‌بردار بودن از این فناوری کافی نیست و اگر در لایه‌های عمیق آن مسلط نشویم، ممکن است در آینده با محدودیت‌های بین‌المللی و موانعی مشابه آنچه در فناوری هسته‌ای رخ داد، مواجه شویم.

از این منظر، چالش اصلی کشور نه صرفاً در استفاده از ابزارهای موجود، بلکه در دستیابی به توانمندی‌های اساسی برای تولید و مدیریت این فناوری است. لایه‌های عمیق هوش مصنوعی، شامل زیرساخت‌های پردازشی پیشرفته، دسترسی به داده‌های بومی در ابعاد کلان، الگوریتم‌ها و مدل‌های بومی‌سازی‌شده و همچنین کاربردهای استراتژیک و بومی این فناوری است. تمرکز بر این لایه‌ها، علاوه بر ایجاد ظرفیت‌های فناورانه داخلی، می‌تواند به شکل‌گیری زنجیره ارزش هوش مصنوعی در کشور منجر شود و از وابستگی به فناوری‌های خارجی جلوگیری کند.

در این راستا، پژوهشگاه ارتباطات و فناوری اطلاعات با درک این ضرورت، سلسله نشست‌هایی با محوریت تبیین لایه‌های عمیق هوش مصنوعی برنامه‌ریزی کرده است. هدف از این نشست‌ها، بررسی و تحلیل این فناوری از چهار منظر کلیدی زیرساخت، داده، مدل و کاربرد بوده تا نقشه راهی برای توسعه پایدار هوش مصنوعی در کشور ترسیم شود. امید است با استمرار این مباحثات علمی و فنی، کشور بتواند گام‌های موثری در خودکفایی و پیشتازی در این عرصه حیاتی بردارد.

مقدمه

این گزارش به عنوان اولین گزارش از سلسله‌گزارش‌های دستیابی به عمق هوش مصنوعی و با هدف تبیین مفهوم لایه‌های عمیق هوش مصنوعی و دستیابی به آن پیرو فرمایش مقام معظم رهبری تدوین شده است.

عمق هوش مصنوعی و دستیابی به آن، موضوعی است که نیاز به تبیین و شفافیت دارد؛ لذا این نشست‌ها با تبیین مفهوم لایه‌های عمیق هوش مصنوعی به بررسی نیازمندی‌ها، اقدامات، همکاری‌ها و نقش حاکمیت، دانشگاه‌ها، بخش خصوصی و به طور کلی زیست‌بوم هوش مصنوعی در دستیابی به این لایه‌ها می‌پردازد.

گزارش حاضر مستخرج از دو نشست تخصصی در لایه زیرساخت‌ها و سخت‌افزارهای پردازشی است که در تاریخ‌های ۱۰ مهر و ۱۳ آبان سال ۱۴۰۳ در پژوهشگاه ارتباطات و فناوری اطلاعات برگزار شده است.

در این دو نشست که با حضور اساتید و خبرگان هوش مصنوعی شاغل در بخش خصوصی، دانشگاه‌ها و بدنه حکمرانی کشور برگزار شد، ابتدا زیرساخت‌های سخت‌افزاری هوش مصنوعی معرفی و تشریح و سپس مصادیق عمق هوش مصنوعی در لایه زیرساخت معرفی گردید. در ادامه در خصوص چالش‌ها، برنامه‌ها و اهداف کشور برای دستیابی به این مصادیق بحث و تبادل نظر صورت گرفت. آن‌چه در ادامه می‌خوانید مروری است بر این مباحث و تدقیق آن‌ها.

مفهوم عمق هوش مصنوعی

در فرهنگ‌نامه‌های فارسی یکی از معانی که برای کلمه عمق آورده شده است. فاصله سطح تا انتهای چیزی است. پس در اولین گام اگر از عمق هوش مصنوعی صحبت می‌کنیم، باید بپذیریم هوش مصنوعی، چیزی است که جنبه‌ای سطحی دارد و جنبه‌ای عمیق.

سطح هوش مصنوعی آن‌چیزی است که نمود خارجی دارد و عمق آن، چیزی که سبب نمود سطح هوش مصنوعی شده است و عیان نیست. برای درک آن باید دانشی تخصصی در مواردی پیدا کرد که سبب شده است جنبه بیرونی و سطحی هوش مصنوعی نمایان گردد.

با این تفاسیر می‌توان برای جنبه عمیق هوش مصنوعی، لایه‌های متعددی را متصور شد؛ چرا که جنبه نمادین و آنچه که همگان از هوش مصنوعی می‌بینند، نتیجه اجرای عملیات و وظایف مختلفی است که در برخی موارد تحت عنوان زیرساخت‌های هوش مصنوعی از آن‌ها یاد می‌شود و به این ترتیب می‌توان گفت لایه‌های عمیق یا لایه‌های زیرساختی هوش مصنوعی؛ شکل ۱ برخی از لایه‌های زیرساختی هوش مصنوعی را نمایش می‌دهد.

مواردی نظیر فلسفه و مبانی هوش مصنوعی نیز جزو مصادیق عمق هوش مصنوعی است؛ اما وقتی صحبت از دستیابی به لایه‌هایی می‌شود که کشور را از بهره‌بردار بودن به

شکل ۱. لایه‌های هوش مصنوعی

قدرت منطقه‌ای و جهانی تبدیل می‌کند، دستیابی به دانش و فناوری است الگوی فعلی و آینده نزدیک هوش مصنوعی را هدایت می‌کند.

سلسله‌نشست‌های دستیابی به عمق هوش مصنوعی در مرحله نخست، در چهار لایه نمایش داده‌شده در شکل ۱ برنامه‌ریزی شده است.

همه این لایه‌ها دارای مصداق در عمق هوش مصنوعی نیستند اما به طور خاص در لایه زیرساخت و سخت‌افزارهای پردازشی و لایه مدل‌ها و الگوریتم‌های هوش مصنوعی، مصادیقی برای عمق هوش مصنوعی و دستیابی به آن وجود دارد. لایه داده به عنوان یکی از اصلی‌ترین و مهم‌ترین الزامات و نیازمندی‌ها، نه تنها در دستیابی به عمق هوش مصنوعی که در توسعه کاربردی آن نیز مؤثر است. این نشست‌ها ممکن است در موضوعاتی به غیر از این ۴ لایه نیز ادامه یابد.

زیرساخت‌های سخت‌افزاری هوش مصنوعی

وقتی صحبت از زیرساخت‌های سخت‌افزاری هوش مصنوعی می‌شود، بسیاری فکر می‌کنند که منظور فقط واحدهای پردازش گرافیکی (GPUs) است. شاید بتوان گفت که GPUها معروف‌ترین سخت‌افزار مورد نیاز برای توسعه مدل‌های هوش مصنوعی است، اما زیرساخت‌های سخت‌افزاری هوش مصنوعی شامل طیف وسیعی از تجهیزات می‌شود.

در یک دسته بندی کلی می‌توان تجهیزات و زیرساخت‌های سخت‌افزاری هوش مصنوعی را در دو دسته زیرساخت‌های فعال و غیر فعال تقسیم‌بندی کرد.

زیرساخت‌های غیر فعال عبارتند از: ساختمان و محل فیزیکی، منابع و تجهیزات تأمین برق، تجهیزات خنک‌کنندگی، تجهیزات اعلان و اطفای حریق، کابل‌های ارتباطی.

در این دسته از زیرساخت‌ها، تأمین برق و خنک‌کنندگی از موضوعات بسیار چالشی است که شرکت‌های بزرگ دنیا سرمایه‌گذاری بسیاری برای کاهش مصرف برق و بهبود تجهیزات خنک‌کنندگی انجام می‌دهد. خنک‌کنندگی بر پایه مایع از جدیدترین و به‌روزترین فناوری‌های این حوزه است.

زیرساخت‌های فعال هوش مصنوعی عبارتند از: تجهیزات پردازشی، تجهیزات ذخیره‌سازی، تجهیزات شبکه و تجهیزات امنیت اطلاعات. تجهیزات پردازشی امروزه به عنوان اصلی‌ترین سخت‌افزارهای هوش مصنوعی و ابزار قدرت، برتری و تمایز در حوزه هوش مصنوعی شناخته می‌شود. این تجهیزات که انواع مختلفی دارند که GPUها و TPUها از معروف‌ترین آن‌ها هستند و دستیابی به ساخت این تراشه‌های هوش مصنوعی که مبتنی بر نیمه‌هادی‌ها هستند یکی از مصادیق دستیابی به اعماق هوش مصنوعی است.

چرا تولید و ساخت تراشه‌ها مهم است؟

الگوی فعلی توسعه هوش مصنوعی به شدت به منابع محاسباتی بستگی دارد. **برای حفظ پیشتازی خود در هوش مصنوعی، ایالات متحده باید به توسعه پیشرفته‌ترین نیمه‌هادی‌های هوش مصنوعی جهان و ساخت پیشرفته‌ترین زیرساخت‌های محاسباتی اختصاصی هوش مصنوعی خود ادامه دهد.** این یکی از بندهای یادداشت پیشبرد رهبری ایالات متحده در هوش مصنوعی است که در اکتبر ۲۰۲۴ توسط جو بایدن ابلاغ شده است.

تجهیزات پردازشی و محاسباتی قلب هوش مصنوعی است، بزرگترین و دقیق‌ترین مدل‌ها و الگوریتم‌های هوش مصنوعی و به طور کلی‌تر تمام تلاش‌ها در هوش مصنوعی بدون وجود واحدهای مناسب پردازشی ابتر خواهد ماند؛ کمااینکه یکی از مهم‌ترین علل زمستان هوش مصنوعی در دهه ۷۰ میلادی نبود همین سخت‌افزارها بود.

آمریکا قصد رهبری هوش مصنوعی در جهان را دارد و این موضوع را به صورت عینی در اسناد خود منتشر می‌کند و زیرساخت‌های محاسباتی را یکی از مهم‌ترین ابزارهای خود برای رسیدن به این هدف می‌داند. تحریم چین و ایجاد محدودیت‌های دستیابی به مدل‌های جدید و قوی GPUها در بیش از ۴۰ کشور جهان، بیانگر اهمیت این تراشه‌ها و نسل‌های آینده آن‌ها در رهبری هوش مصنوعی و پیشبرد اهداف امنیت ملی است.

گزارش‌ها پیش‌بینی می‌کنند که صنعت نیمه هادی تا پایان دهه به ۱ تریلیون دلار افزایش یابد. سرمایه‌گذاری‌های هنگفت بر روی تولید تراشه‌های هوش مصنوعی توسط کشورهای گوناگون که در جدول ۱ نمایش داده شده است. نیز بیانگر همین موضوع است.

جدول ۱. سرمایه‌گذاری در حوزه تراشه‌ها

نام کشور	میزان سرمایه‌گذاری
کره جنوبی	۴۷۰ میلیون دلار
مالزی	۱۰۷ میلیون دلار
چین	۴۷.۵ میلیون دلار
ژاپن	۶۵ میلیون دلار

اتحادیه اروپا نیز پروژه‌ای بلند مدت را از حدود بیش از ۱۰ سال پیش در حوزه طراحی تراشه‌های هوش مصنوعی آغاز کرده است. این اتحادیه در انتهای سال ۲۰۲۳ قانونی تحت عنوان **قانون تراشه اتحادیه اروپا** با محوریت رهبری فناوری توسط این اتحادیه منتشر کرده است. پیش‌بینی این اتحادیه بر سرمایه‌گذاری حدود ۴۳ میلیارد یورویی تا سال ۲۰۳۰ است.

هند نیز رونمایی از تراشه بومی خود را برای سال ۲۰۲۵ پیش‌بینی کرده است.

آنچه مشخص است این است که اتکای به خود و تولید تراشه‌های بومی به یکی از راهبردهای مهم و موضوعات امنیت ملی بسیاری از کشورها تبدیل شده است.

چرا ساخت تراشه‌ها برای ایران مهم است؟

اهمیت راهبردی صنعت نیمه‌هادی‌ها و تولید تراشه‌های هوش مصنوعی به طور خلاصه در بخش قبلی بیان شد، این موضوع برای ایران به دو دلیل از اهمیت بیشتری برخوردار است.

۱. تحریم

تحریم یکی از مهم‌ترین چالش‌های ایران است. با توجه به سیاست‌های تحریمی ایالات متحده آمریکا در حوزه تراشه‌های هوش مصنوعی و روابط سیاسی میان ایران و آمریکا، بدون شک ایران یکی از کشورهای هدف تحریم در دستیابی به این تراشه‌ها هستند. احتمال تشدید این تحریم‌ها در آینده بیشتر است. حتی در صورتی که آمریکا در سایر حوزه‌ها موضع تحریمی خود نسبت به ایران را تغییر دهد، با توجه به برنامه‌ریزی رهبری هوش مصنوعی ایالات متحده آمریکا، پیش‌بینی می‌شود محدودیت‌ها و تحریم دستیابی به تراشه‌ها برای ایران هم‌چنان به قوت خود باقی بماند. این یعنی حتی مصرف‌کننده بودن ایران در هوش مصنوعی نیز با چالش جدی رو به رو است.

۲. برنامه‌ریزی‌های راهبردی ایران

ایران در افق ۱۴۱۲ باید حداقل جزو ۱۰ کشور برتر در حوزه هوش مصنوعی در جهان باشد. این چشم‌انداز هوش مصنوعی ایران است با تمرکز بر دستیابی به لایه‌های عمیق هوش مصنوعی.

برای هر کنشی در هوش مصنوعی باید زیرساخت‌های پردازشی و سخت‌افزاری آن به اندازه کافی وجود داشته باشد و بدون داشتن زیرساخت پزدازشی کنشگری معنا ندارد. همانطور که گفته شد ایران برای تبدیل به یک مصرف کننده در حوزه هوش مصنوعی با چالش روبه‌رو است؛ حال آنکه ایران می‌خواهد در این عرصه بازیگری تعیین کننده و مؤثر باشد.

با توجه به رویکردهای کشورهای مختلف در جهان و برای رسیدن به اهداف تعیین شده برای کشور، بدون شک دستیابی به دانش و فناوری توسعه تراشه‌های هوش مصنوعی یکی از اصلی‌ترین الزامات و نیازمندی‌ها است.

چالش‌های ایران در لایه زیرساخت

در حوزه زیرساخت‌های سخت‌افزاری هوش مصنوعی کشور با چالش‌های جدی رو به است. که در ادامه به برخی از آن‌ها اشاره خواهد شد.

۱. فقدان نگاه راهبردی

باید پذیرفت هوش مصنوعی و حوزه سخت‌افزارهای آن یک موضوع اقتدارآفرین، بنیادی و مرتبط با امنیت ملی است و علی رغم اهداف بزرگ برای هوش مصنوعی در کشور، نگاه راهبردی و متناسب با آنچه گفته شد، فعلا در کشور وجود ندارد و غالب نگاه‌ها و برنامه‌ریزی ها سطحی و در حوزه کاربردی است. در تمام دنیا در حوزه زیرساخت پردازشی حاکمیت نقش اصلی و سرمایه‌گذار اصلی است و در ایران نیز حاکمیت باید این نگاه و نقش را بپذیرد.

۲. تحریم

موضوع تحریم سبب شده تا دستیابی به تراشه‌ها و تجهیزات سخت‌افزاری هوش مصنوعی برای کشور مشکل‌ساز شود. تحریم سبب شده بهای تمام شده هر تجهیز برای کشور حدود دوبرابر شده و علاوه بر این به دلیل خرید از واسطه‌ها چالش‌هایی نظیر عدم دریافت گواهی رسمی برای بهره‌مندی از امکانات ارائه شده توسط شرکت تولید کننده وجود دارد.

۳. ناترازی انرژی

توسعه تراشه‌ها و یا ایجاد مراکز پردازش سریع هوش مصنوعی نیاز به انرژی قابل توجه و البته پایدار دارد. کشور در زمینه انرژی به خصوص برق دچار ناترازی و مشکلات عدیده‌ای است.

۴. محدودیت بودجه

سرمایه‌گذاری در حوزه زیرساخت چه جهت تجهیز و خریداری سخت‌افزارها و چه در جهت تولید تراشه‌های هوش مصنوعی نیازمند منابع مالی بسیار زیادی است و کشور با محدودیت بودجه رو به رو است.

۵. سرعت اینترنت

دسترسی به شبکه‌های ارتباطی و اینترنت پایدار و با سرعت بالا نیز یکی دیگر نیازمندی‌های حوزه زیرساخت‌های پردازشی است که کشور در این موضوع نیز با چالش روبه‌رو است.

۶. عقب‌ماندگی فناوری

تولید تراشه نیاز به فناوری و دانش در حوزه‌های گوناگونی دارد. از منظر دانشی کشور در وضعیت نسبتاً مناسبی قرار دارد اما در حوزه فناوری و صنعت ساخت فناوری کشور دچار عقب‌ماندگی جدی است.

برنامه‌های پیشنهادی در لایه زیرساخت

۱. برنامه کوتاه مدت

بدون شک به عنوان یک برنامه کوتاه مدت و به جهت توسعه و توانمندسازی زیست‌بوم هوش مصنوعی کشور، نیاز است تا زیرساخت‌های پردازشی و مراکز پردازش سریع هوش مصنوعی در کشور راه‌اندازی و تجهیز گردند.

برای این منظور باید ابتدا یک برنامه‌ریزی بر اساس میزان نیاز کشور صورت گرفته، سپس معماری فنی این مراکز پردازشی تعیین شده و بعد واردات تجهیزات و سخت‌افزارهای مورد نیاز صورت گیرد.

نگرانی قابل توجه در این زمینه موازی‌کاری، خریداری تراشه‌ها و تجهیزات سخت‌افزاری بدون نگاه کارشناسی و به اصطلاح پول‌پاشی است.

بهتر است با توجه به قیمت بالای این تجهیزات و تحریم‌های موجود، خریداری تجهیزات بر اساس یک معماری مشترک و حتی الامکان توسط یک نهاد یا زیرنظر یک نهاد حاکمیتی در کشور اتفاق بیفتد. البته بخش خصوصی می‌تواند با توجه به نیازمندی‌های خود نسبت به خریداری و واردات تجهیزات اقدام کند و مبحث بیان شده جهت هماهنگی و استفاده بهینه از منابع مالی کشور است؛ چون همانطور که گفته شد کشور دچار محدودیت بودجه است باید از خرید هیجان زده تجهیزات در مقیاس کلان جلوگیری شود.

۲. برنامه بلند مدت

همانطور که گفته شد ساخت تراشه‌های هوش مصنوعی یکی از مصادیق دستیابی به عمق هوش مصنوعی است و با توجه به اهداف و برنامه‌ریزی‌های کلان کشور باید به این عرصه ورود کرد.

از طرفی عقب‌ماندگی کشور در فناوری و تولید این تراشه‌ها، محدودیت‌های بودجه و تحریم از جمله مهم‌ترین موانع پیشروی کشور در این حوزه است.

به عنوان برنامه بلند مدت کشور باید برای تولید و ساخت این تراشه‌ها اقدام کرد اما حتی‌الامکان باید از راه‌هایی استفاده شود که مسیر دستیابی کشور به این فناوری کوتاه‌تر شود.

استفاده از رویکرد تولید بدون‌ساخت و همکاری با کشورهایی که شرکای تجاری یا راهبردی ما هستند و یا محدودیت‌های کمتری برای همکاری با آن‌ها وجود دارد یکی از رویکردهای ممکن و البته اجرایی است که باید برای آن برنامه‌ریزی و اقدامات لازم صورت گیرد.

پرداختن به مباحث جدید در حوزه پردازش و محاسبات نظیر محاسبات کوانتومی و پردازش نورومورفیک و سرمایه‌گذاری در توسعه پردازشگرهای آن‌ها نیز رویکرد دیگری است که حتما باید به آن پرداخت شود.

برای موفقیت در این حوزه باید سرمایه‌گذاری به شکل بلندمدت، راهبردی و پیوسته و به میزان زیاد صورت گیرد.

دکتر امین نظارات

مدیرعامل و بنیان گذار شرکت رایانش سریع هزاره ایرانیان

حوزه پردازش سریع و زیرساخت‌های پردازشی به مانند خودکفایی گندم برای کشور مهم و حیاتی است. سرمایه‌گذاری در حوزه زیرساخت‌های پردازشی، تولید تراشه‌های خاص برای هوش مصنوعی و دیگر فناوری‌های نوین با رویکرد Fabless و توسعه نرم‌افزارها و پلتفرم‌های هوش مصنوعی به‌منظور ارتقای قابلیت‌های محاسباتی و پردازشی در داخل کشور از جمله اقداماتی است که در لایه زیرساخت باید انجام شود.

دکتر احسان آریانیان

رئیس پژوهشکده فناوری اطلاعات پژوهشگاه ارتباطات و فناوری اطلاعات

با توجه به سابقه کشور در طراحی ابررایانه‌هایی نظیر سیمرغ، علی‌رغم تحریم‌ها و سایر چالش‌های بین المللی موجود، دستیابی به توان‌های پردازشی پیش‌بینی شده در اسناد بالادستی ممکن ولی پیچیده است و نیاز به تأمین مالی قابل توجهی دارد. مسئله مهم خودباوری و امید است و مشارکت بخش خصوصی و شرکت‌های دانش‌بنیان را نیز نباید از یاد برد.

دکتر بهنام رهنما

مدیرعامل و بنیان گذار هلدینگ مدیس

برای رقابت مؤثر در سطح جهانی، ضروری است که به لایه زیرساخت وارد شویم. سیاست‌گذاری جامع در بخش انرژی، ورود به فناوری Fabless یا خرید نسل‌های قدیمی‌تر تراشه‌ها، دورنگاه به طراحی و ساخت تراشه، غافل نشدن از موضوعات رباتیک و اینترنت اشیا و موضوع رگولاتوری از جمله مهم‌ترین مواردی است که در حوزه زیرساخت‌های هوش مصنوعی باید در کشور به آن پرداخته شود.

دکتر دارا رحمتی

عضو هیات علمی دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی

با افزایش سرمایه‌گذاری و بهره‌گیری از ظرفیت‌های داخلی، می‌توان در بلندمدت به تولید داخلی چیپ‌ست‌ها و حتی GPU دست یافت و به سمت استقلال فناورانه حرکت کرد. تأسیس و تقویت سیاست‌های حاکمیتی برای سرعت بخشیدن به فرآیندهای زیرساختی هوش مصنوعی و هماهنگی میان ارگان‌های مختلف و ایجاد همکاری مؤثر و هدفمند میان حاکمیت، مراکز علمی و بخش خصوصی برای پیشبرد پروژه‌های زیرساختی هوش مصنوعی و رفع چالش‌های موجود از جمله اقدامات مؤثر است.

دکتر سید مهدی حاتمیان

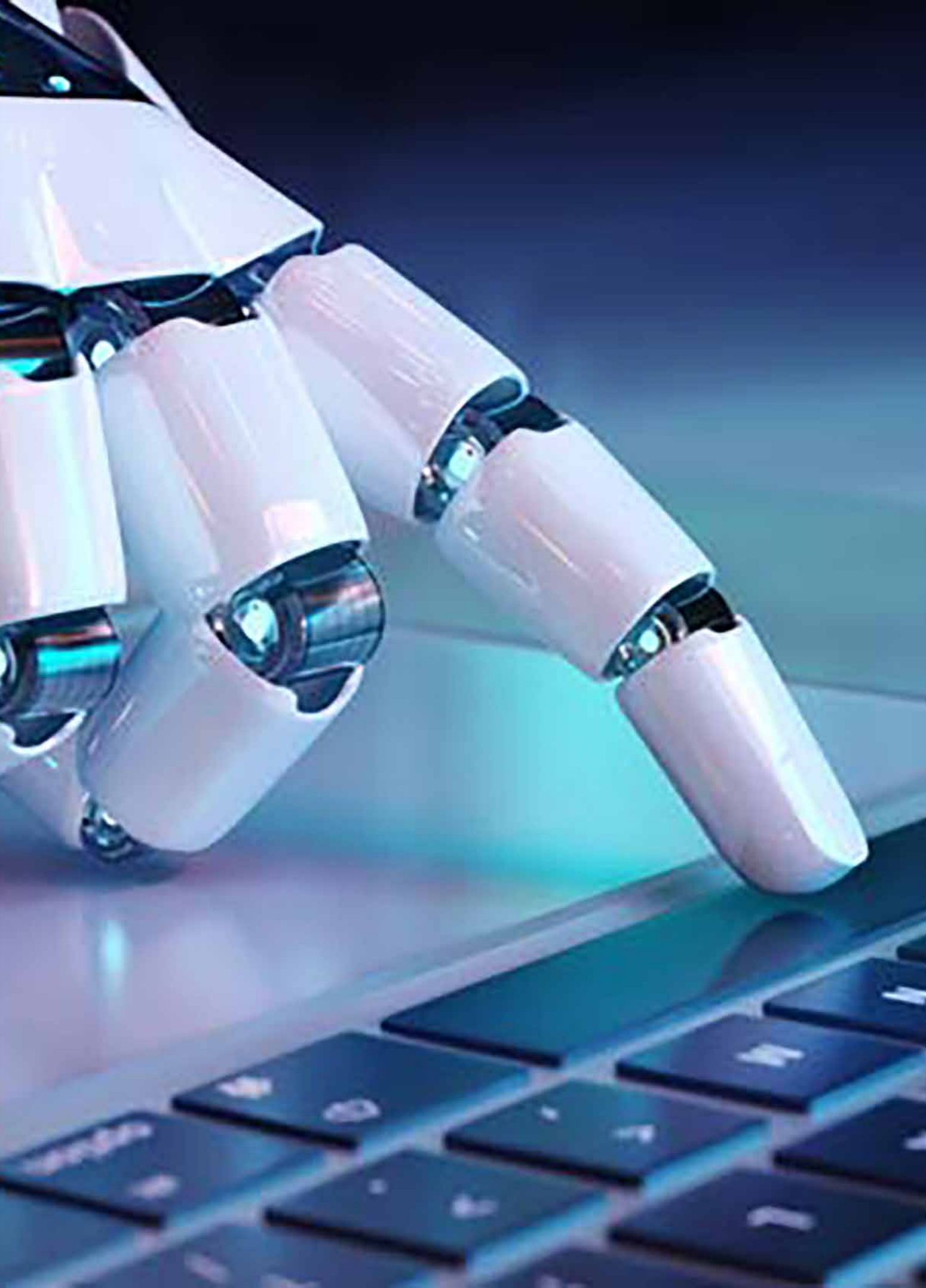
مدیرکل تأمین منابع و سرمایه‌گذاری وزارت ارتباطات و فناوری اطلاعات

در حوزه هوش مصنوعی و زیرساخت‌های آن باید یک هم‌افزایی و مشارکت چندجانبه میان دانشگاه، بخش خصوصی و حاکمیت شکل گیرد. حاکمیت باید نقش حامی را در این حوزه برقرار کند و با ارائه طرح‌های حمایتی و تشویقی بخش خصوصی را برای حضور پررنگ در این عرصه ترغیب کند.

دکتر مهدی مشیری

معاون تحقیق و توسعه زیرساخت های ارتباطی شرکت ارتباطات زیرساخت

تولید تراشه زمان‌بر و هزینه‌بر است اما مهم نیز هست. کشور باید علاوه بر نگاه بلند مدت به این موضوع توسعه و ایجاد زیرساخت‌های پردازشی جدید در کشور برای پشتیبانی از پروژه‌های هوش مصنوعی، دسترسی به منابع محاسباتی قوی، توسعه زیرساخت‌های انرژی، و ایجاد ارتباطات فوق‌سریع را در کنار رگولاتوری هوش مصنوعی مد نظر قرار دهد.



دستیابی به عمق هوش مصنوعی
لایه داده

تهیه شده توسط
مرکز نوآوری و توسعه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات
برگرفته از نشست «تبیین لایه‌های عمیق هوش مصنوعی در لایه داده»

مقدمه

گزارش حاضر به عنوان دومین گزارش از سلسله‌گزارش‌های دستیابی به عمق هوش مصنوعی و با هدف تبیین مفهوم لایه‌های عمیق هوش مصنوعی و دستیابی به آن پیرو فرمایش مقام معظم رهبری تدوین شده است.

گزارش حاضر مستخرج از نشست تخصصی در لایه داده است که در تاریخ ۱۹ آذر سال ۱۴۰۳ در پژوهشگاه ارتباطات و فناوری اطلاعات برگزار شده است. این نشست نیز به مانند نشست‌های لایه زیرساخت با حضور خبرگان حوزه داده از بخش خصوصی، دانشگاه‌ها و بنده حکمرانی کشور برگزار شد.

داده از اهمیت بسیار بالایی در هوش مصنوعی برخوردار است و می‌توان گفت ستون فقرات و پیشران اصلی هوش مصنوعی است. داده به عنوان مصداقی از عمق هوش مصنوعی مطرح نیست اما تصور هوش مصنوعی بدون داده نیز ممکن نیست. در این گزارش جایگاه داده در دستیابی به عمق هوش مصنوعی و چالش‌های اصلی کشور در حوزه هوش مصنوعی مستخرج از مباحث مطرح شده در نشست ۱۹ آذر ماه ۱۴۰۳ بررسی خواهد شد.

اهمیت داده در دستیابی به عمق هوش مصنوعی

برخی داده را به عنوان طلای دیجیتال و موتور محرک زیست‌بوم هوش مصنوعی معرفی می‌کنند. برخی دیگر داده را اصلی‌ترین دارایی سازمان‌ها و صنایع در عصر صنعتی چهارم قلمداد می‌کنند.

برخی بر لزوم جمع‌آوری داده تمرکز دارند و برخی دیگر بر اهمیت افزایش کیفیت دادگان. هر آنچه هست در الگوی فعلی هوش مصنوعی، داده نقشی کلیدی دارد و بدون داده نمی‌توان توسعه سامانه‌های هوش مصنوعی را متصور شد.

داده در بعد فردی یک دارایی شخصی و دسترسی غیر مجاز و بدون اجازه به آن مصداق نقض حریم خصوصی است، در بعد سازمانی یک دارایی استراتژیک و مزیت رقابتی و در سطح ملی یک مصداق عینی و بارز از امنیت ملی است که نیاز به محافظت دارد.

در بین لایه‌های هوش مصنوعی داده لایه دوم است و پیش‌نیازی برای لایه مدل. دقیقاً همین نقش اهمیت داده را بالا می‌برد. در اینکه یکی از مصادیق لایه‌های عمیق هوش مصنوعی توسعه مدل‌های بنیادین است شکی نیست و این مدل‌ها بدون تکیه بر دادگان مرتبط، معتبر و به تعداد زیاد در عمل توسعه نخواهند یافت.

پس دسترسی به دادگان باکیفیت و معتبر پیش‌نیازی برای توسعه مدل‌های بنیادین هوش مصنوعی ملی و بومی است.

اما این دسترسی به سهولت اتفاق نمی‌افتد و کشور با چالش‌های جدی در این زمینه رو به است. برخی از مهم‌ترین این چالش‌ها در شکل ۱ نمایش داده شده است.

در این گزارش سعی می‌شود مروری کلی بر چالش‌های مطرح شده در شکل ۱ صورت گیرد و اهمیت هر یک از آن‌ها به صورت خلاصه بیان شده و برنامه‌های برای هر یک ارائه گردد.

شکل ۱. چالش‌های اساسی داده در کشور

حکمرانی داده

اینکه داده ها چگونه ذخیره شوند، چگونه در دسترس افراد مناسب قرار گیرند، چگونه کیفیت آنها کنترل شود، با چه ابزارهایی آنها را تحلیل کنیم و مسائلی از این دست؛ باعث به وجود آمدن شاخه جدیدی در علم داده با نام «حکمرانی داده »شده است. در یک کلام حکمرانی داده می‌خواهد چارچوبی برای اداره و مدیریت دادگان جمع‌آوری شده در اختیار ما قرار دهد.

برای حکمرانی یا حاکمیت داده تعاریف مختلفی ارائه شده است. هم‌چنین مؤسسات مختلف ابعاد گوناگونی برای آن در نظر گرفته‌اند. با در نظر گرفتن ابعاد گوناگون حاکمیت داده می‌توان تعریفی کامل برای آن ارائه کرد. حکمرانی داده در واقع چارچوبی برای مدیریت تمامی ابعاد ذکر شده است.

یکی از چارچوب‌های معروف متعلق به داما است که ابعاد آن در شکل ۲ نمایش داده شده است.

حکمرانی داده مزایای متعددی دارد که برخی از آن‌ها عبارتند از:

- ایجاد درک مشترک از داده
- ارتقای کیفیت داده‌ها
- بهبود مدیریت داده
- بهبود امنیت داده‌ها با استقرار نقش‌ها و مسئولیت‌های مرتبط

حکمرانی داده یک انتخاب نیست بلکه یک ضرورت است. این حکمرانی در سطح سازمانی و ملی مفهوم می‌یابد. ابتدا نیاز است تا در نگاهی کلان حکمرانی داده در سطح ملی تعریف شده و سپس هر سازمان نیز برای بهره‌برداری و مدیریت دادگان خود نظام حکمرانی داده سازمانی را مستقر کند.

حکمرانی داده در ایران

«پیش‌نویس سند نظام حکمرانی داده کشور که از مجموعه اسناد ذیل سند راهبردی در فضای مجازی است، در نشست کمیسیون عالی تنظیم مقررات کشور با حضور اعضای کمیسیون و نمایندگان دستگاه های مرتبط بررسی شد». این آخرین وضعیت حکمرانی داده کشور است، پروژه‌ای که در بهمن ۱۴۰۱ در وزارت ارتباطات و فناوری اطلاعات و سازمان فناوری اطلاعات آغاز شد و منجر به تدوین سندی در ۱۰ فصل و افق در نظر گرفته شده برای سال ۱۴۱۰ شد. در افق مذکور کشور باید زیست بوم داده یکپارچه، هماهنگ و کارآمد به منظور حکمرانی، اقتدارآفرینی، مدیریت و بهره‌برداری شفاف و امن از داده‌ها برای ایجاد ارزش در راستای منافع ملی به کمک به روزترین ابزارها، استانداردها و رویه‌ها ایجاد کند.

در پیش‌نویس این سند شفاف‌سازی رکن مهمی است که در نظر گرفته شده است. اینکه هر نهادی تا چه حد و در چه زمینه‌هایی می‌تواند ورود پیدا کند. زمینه اختیارات داده‌ای آن‌ها را مشخص می‌کند و از تخلف و استفاده مجرمانه از داده‌ها جلوگیری شود. این تنظیم‌گری باید زودتر اعلام شود چون با انجام برخی از فعالیت‌ها در این زمینه پس از اعلام سیاست‌گذاری‌ها فعالیت برخی از نهادها و کسب‌وکارها ممکن است قانون‌شکنی تلقی شود.

به دلیل هزینه‌های بالا برای تبادل داده و نبود سکویی جامع برای جمع‌آوری و نگهداری داده در سازمان‌ها، پراکندگی داده‌هایی که انواع مختلفی نیز دارند باعث شده سازمان‌ها هنوز سیلو وار عمل کنند و حتی تمایلی به تبادل داده بین بخش‌های داخلی خودشان نداشته باشند.

سند حکمرانی داده باید برای ادامه حرکت در مسیر تحول دیجیتال و هوش مصنوعی، از طرف دولت این اطمینان را حاصل کند که کیفیت، صحت و یکپارچگی داده‌ها برای کسب و کارها فراهم شود. با بررسی قوانین حکمرانی داده در دنیا و نیز چالش‌های داخل کشور سعی شده تنظیم‌گری بومی صورت بگیرد.

همانطور که گفته شد نکته مهم این است که این سند هر چه سریع‌تر نهایی و ابلاغ گردد چرا که ممکن است بسیاری از کسب و کارها اقدام به استفاده از داده‌هایی برای توسعه مدل‌های هوش مصنوعی خود کنند و بعد از ابلاغ سند با مشکل مواجه شوند. علاوه بر این بسیاری از سازمان‌های دولتی در حال حاضر اقدام به تدوین سند حکمرانی داده خود کرده و یا برای آن برنامه‌ریزی دارند و بهتر است ابتدا در قالب سندی ملی وضعیت دادگان در سطح کلان مشخص شده و در ادامه این سازمان‌ها با در نظر گرفتن سند مذکور به عنوان سند بالادستی نسبت به تدوین سند سازمان خود اقدام نمایند.

داده‌های باز و در دسترس قرار گرفتن داده‌ها

یکی از مهم‌ترین اقداماتی که در راه توسعه مدل‌های هوش مصنوعی و بهره‌برداری از دادگان به منظور خلق ارزش باید صورت گیرد، اقدام به در دسترس قرار دادن داده‌ها است. دادگان دارایی ارزشمندی هستند اما به تنهایی کاربردی ندارند و برای اینکه به مرحله استفاده در فرآیند تصمیم‌گیری و در اصطلاح تصمیم‌گیری داده مبنا برسند، باید در اختیار توسعه‌دهندگان و دانشمندان علوم داده قرار بگیرند.

البته این مهم به این معنا نیست که دادگان بدون خط مشی خاص و در نظر گرفتن ملاحضات مرتبط با امنیت، حریم خصوصی و ... و در اختیار تمامی اشخاص قرار گیرند، بلکه باید تمامی این ملاحظات در نظر گرفته شده که حکمرانی داده این موارد را نیز پوشش می‌دهند؛ اما نباید دادگان را در صندوقچه‌هایی متروکه نگه داشت.

در ایران سامانه ملی کاتالوگ و مجموعه داده‌های باز و کاربردی کشور تحت نظارت سازمان فناوری اطلاعات ایران طراحی و پیاده‌سازی گردیده است. این سامانه به‌عنوان یکی از اجزای اصلی نظام مرجع داده‌های باز مطرح بوده با هدف اصلی ایجاد یک زیرساخت مشترک برای به اشتراک‌گذاری مجموعه داده‌های تولید شده توسط دستگاه‌های متولی اطلاعات در کشور راه‌اندازی شده است. البته به دلیل نبود سازوکارهای به اشتراک‌گذاری داده به خصوص در بدنه حاکمیت کشور، در حال حاضر این سامانه کاربرد مدنظر را نداشته و از اهداف خود فاصله دارد. علاوه بر این معمولاً دادگانی که در این سامانه منتشر می‌شود به صورت یک رکورد یا یک شی منتشر شده و با عنوان ذخیره‌سازی آن‌ها یعنی دیتاست سنخیتی ندارند. به عبارت دیگر حجم قابل توجهی از دیتاست‌های موجود در سامانه اصلا دیتاست یا مجموعه دادگان نیستند بلکه تنها یک رکورد هستند که می‌تواند شامل یک عکس، یک فایل صفحه گسترده و ... باشد.

مسئله دیگر عدم وجود اهتمام جدی از سوی سازمان‌ها برای آزادرسانی دادگان در این سامانه است به نحوی که نوعی رفع تکلیف و سرسری انجام دادن کار مشهود است؛ کما اینکه بسیاری از دستگاه‌ها همین ظاهر را هم حفظ نکرده و اصلا در میان سازمان‌های سامانه اثری از آن‌ها نیست.

چالش‌های دیگر، کاربرمحور نبودن و نبود چرخه‌ای منظم برای فرآیند استفاده از داده‌های باز است.

به هر حال صرف وجود این سامانه مغتنم است اما به واقع کافی نیست. وظیفه نهادهای بالادستی است که تمامی دستگاه‌های متولی را ملزم به ارائه مجموعه دادگان واقعی، باکیفیت، معتبر و جدید خود در این سامانه کنند؛ هرچند به دلیل چالش فرهنگی این الزام هم شاید راه به جایی نبرد.

قوانین و مقررات مرتبط با داده

قانون دوام یا قانون مدیریت داده و اطلاعات ملی مرتبط ترین قانون در حوزه داده در ایران است. البته این قانون بیشتر از جنس تعیین وظایف و تکالیف است و کمتر به جزئیات، الزامات و اقتضاعات حوزه داده می‌پردازد. بدون شک نیاز است تا در برخی از موارد، قانون یا مجموعه‌ای از قوانین با ذکر جزئیات، تکالیف روشن و ضمانت اجرایی تدوین گردد که در ادامه برخی از آن‌ها ذکر می‌گردد.

۱. مالکیت معنوی

وقتی گفته می‌شود داده یک دارایی است که از جنس ناملموس نیز دسته‌بندی می‌شود نیاز است تا به موضوع مالکیت معنوی در خصوص آن پرداخته شود.

باید مشخص شود که مالکیت یک داده به هنگام تولید آن برای کیست؟ پس از جمع‌آوری چطور؟ بعد تغییر، نرمال‌سازی و پاکسازی آن چطور؟ وقتی داده‌ها در یک مدل هوش مصنوعی به کار گرفته می‌شوند، مالکیت آن‌ها با کیست؟ چه الزاماتی در خصوص رعایت این مالکیت وجود دارد؟ و در خصوص تخطی یا دستبرد به دادگان باید چه مجازات‌هایی برای آن در نظر گرفته شود؟ این‌ها سؤالاتی هستند که پاسخ به آن‌ها نه تنها سبب سهولت اشتراک‌گذاری دادگان بلکه سبب افزایش اعتماد نسبت به سامانه‌های داده مبنا و هوش مصنوعی خواهد شد.

۲. ارزش‌گذاری و حسابرسی داده

ارزش ریالی یک داده بر چه اساسی مشخص می‌شود؟ در صورت خرید و فروش داده چگونه می‌توان صورت‌های مالی معتبر صادر کرد به نوعی که به تخلفات مالی منجر نشود؟

باید قانون و خط‌مشی مشخصی در خصوص قیمت‌گذاری داده وجود داشته باشد تا بتوان به سوالات فوق پاسخ داد. علاوه بر این یکی از کسب و کارهای موجود در حوزه داده، بازارگاه‌های داده هستند، اگر ساز و کار قیمت‌گذاری داده مشخص نگردد امکان راه‌اندازی و توسعه این بازارگاه‌ها نیز ممکن نخواهد بود. هم‌چنین نیاز است تا روشی برای حسابرسی دادگان وجود داشته باشد تا بتوان در صورت‌های مالی شرکت‌ها میزان دارایی‌ها،هزینه‌کرد یا سود حاصل از داده‌ها را ارزیابی یا صحت‌سنجی کرد.

۳. حریم خصوصی دادگان

یکی از مهم‌ترین مباحث در حوزه قوانین مرتبط با داده، حریم خصوصی دادگان است. باید برای حریم خصوصی قانون وضع کرد، زیرا نبود قانون در این زمینه سبب سوءاستفاده و وقوع جرایم سایبری در حوزه داده شده و علاوه بر این نبود این قوانین سبب سلب اعتماد و عدم تمایل جهت به اشتراک‌گذاری دادگان برای توسعه مدل‌های هوش مصنوعی می‌شود.

کیفیت داده

در علوم داده و توسعه مدل‌های تحلیلی مبتنی بر داده، بیشترین زمان و انرژی صرف پاکسازی دادگان می‌شود. دادگان با کیفیت و البته در حجم زیاد لازمه توسعه مدل‌های هوش مصنوعی با دقت و عملکرد مناسب است و دلایل زیر برای این موضوع قابل ذکر هستند:

دقت و صحت نتایج: کیفیت دادگان به طور مستقیم بر دقت نتایج مدل‌های هوش مصنوعی تأثیر می‌گذارد. مدل‌هایی که بر اساس داده‌های با کیفیت پایین آموزش دیده‌اند، معمولاً عملکرد ضعیفی دارند و نمی‌توانند نتایج دقیقی ارائه دهند.

جلوگیری از سوگیری: اگر داده‌ها ناقص، غیرنماینده یا دارای سوگیری باشند، این سوگیری‌ها می‌توانند به مدل منتقل شوند و منجر به نتایج نادرست و غیرمنصفانه در زمینه‌های مختلف شوند. کیفیت‌سنجی به شناسایی و کاهش این سوگیری‌ها کمک می‌کند.

بهبود تعمیم‌پذیری: ارزیابی و بهبود کیفیت داده‌ها می‌تواند به تعمیم‌پذیری مدل‌ها کمک کند. مدل‌های آموزش‌دیده با داده‌های با کیفیت، قابلیت بیشتری برای تعمیم به داده‌های جدید و ناشناخته دارند.

افزایش کارایی مدل: به کمک کیفیت‌سنجی می‌توان مشخص کرد که کدام داده‌ها برای آموزش مهم‌تر و مؤثرتر هستند و در نتیجه می‌توان بر روی داده‌های کلیدی تمرکز کرد و کارایی مدل را افزایش داد.

کاهش هزینه‌ها: شناسایی اشکالات و نواقص در داده‌ها در مراحل اولیه می‌تواند هزینه‌های بالاتر در مراحل بعدی توسعه و پیاده‌سازی مدل را کاهش دهد.

قابلیت الفاظ و تفسیر نتایج: مدل‌هایی که بر اساس داده‌های با کیفیت طراحی شده‌اند، نتایج و پیش‌بینی‌های بهتری ارائه می‌دهند که این امر در تفسیر و تصمیم‌گیری‌های مبتنی بر هوش مصنوعی بسیار اهمیت دارد.

تضمین انطباق با مقررات: در بسیاری از صنایع، استانداردها و مقرراتی وجود دارند که بر کیفیت داده‌ها تأکید دارند. با اجرای روش‌های کیفیت‌سنجی می‌توان اطمینان حاصل شود که داده‌های مورد استفاده با این مقررات مطابقت دارند.

روش‌های کیفیت‌سنجی دادگان نه تنها برای کارایی و دقت بالای مدل‌های هوش مصنوعی ضروری است، بلکه به عنوان یک گام حیاتی در چرخه حیات توسعه این مدل‌ها شناخته می‌شود و باید به‌کار گرفته شوند.

راهبردهای کلان پیشنهادی برای لایه داده کشور

علاوه بر تدوین و ابلاغ سند حکمرانی داده، در اینجا برخی از مهم‌ترین راهبردها در لایه داده برای کشور پیشنهاد می‌شود.

ایجاد زیرساخت‌های داده‌محور

- سرمایه‌گذاری در مراکز ذخیره‌سازی و پردازش داده‌های بزرگ
- استفاده از فناوری‌های پیشرفته مانند ذخیره‌سازی ابری و ذخیره‌سازی توزیع‌شده در سطح کلان
- ایجاد یکپارچگی بین پایگاه‌های داده سازمان‌ها و نهادهای مختلف
- توسعه شبکه ملی اطلاعات در مدیریت داده‌ها

بهبود کیفیت داده‌ها

- تعریف قالب‌ها و استانداردهای مشخص برای ذخیره‌سازی و اشتراک‌گذاری داده‌ها
- استفاده از ابزارهای خودکار برای پاک‌سازی و بهبود کیفیت داده‌ها
- ایجاد پروتکل‌های جمع‌آوری داده برای کاهش خطاها و داده‌های ناقص

تضمین امنیت و حریم خصوصی داده‌ها

- استفاده از روش‌های رمزنگاری پیشرفته برای ایمن‌سازی داده‌ها
- ایجاد مکانیزم‌های مقابله با حملات سایبری که داده‌ها را هدف قرار می‌دهند.
- تدوین سیاست‌های شفاف درباره جمع‌آوری و استفاده از داده‌های شخصی

تقویت همکاری در استفاده از داده‌ها

- ایجاد پلتفرم‌های اشتراک‌گذاری داده میان سازمان‌ها و شرکت‌ها و تقویت سامانه کاتالوگ
- تدوین مدل‌های تجاری برای تسهیل دسترسی به داده‌ها
- مشارکت در پروژه‌های بین‌المللی برای بهره‌برداری از داده‌های مشترک

توسعه قوانین و مقررات مدیریت داده

- تدوین مقررات مالکیت، اشتراک‌گذاری، حریم خصوصی و استفاده از داده‌ها
- ایجاد چارچوب‌های حقوقی برای ارزش‌گذاری و تجارت داده
- تعریف مسئولیت‌ها برای بازیگران مختلف در زیست‌بوم داده

آموزش و فرهنگ‌سازی

- آموزش متخصصان داده در زمینه مدیریت و تحلیل داده
- افزایش آگاهی عمومی و توسعه دوره‌های آموزشی برای ارتقای سواد داده در سطوح مختلف
- تشویق سازمان‌ها به مدیریت مسئولانه داده‌ها و ایجاد تفکر و فرهنگ داده‌محور

توسعه مدل‌های اقتصادی پایدار

- ایجاد برنامه‌هایی برای ارزش‌گذاری داده قیمت‌گذاری آن‌ها
- تشویق سرمایه‌گذاری خصوصی و عمومی در حوزه داده

دکتر مسعود مظلوم

بنیان گذار مرکز نوآوری علم داده و هوش مصنوعی و محقق هوش مصنوعی دانشگاه آمستردام

داده‌ها را باید شهروند درجه یک در نظر گرفت، بدون ایجاد ذهنیت داده‌محور و در نظر گرفتن داده‌ها به‌عنوان یک محصول کلیدی، تحول دیجیتال و توسعه هوش مصنوعی اتفاق نخواهد افتاد. اهمیت تغییر نگرش سازمان‌ها برای کسب درآمد از داده‌ها و خلق ارزش در راستای اهداف کسب‌وکار موضوعی مهم و راهبردی است.

برای خلق ارزش از داده‌ها، در ابتدا باید حکمرانی داده را مصوب و اجرایی کرد و در نتیجه آن داده‌های مرتبط و باکیفیت ایجاد شده و با تدوین و اجرایی نمودن استراتژی هوش مصنوعی خلق ارزش محقق خواهد شد. توسعه سامانه‌های یکپارچه‌سازی داده و کاتالوگ داده نیز به طی کردن این مسیر کمک می‌کند.

دکتر محمدرضا رسولی

عضو هیئت علمی دانشگاه علم و صنعت و مدیر پروژه تدوین سند حکمرانی داده کشور

تنظیم سند حکمرانی داده تحت قانون دوام یک گام اساسی است و مسیر را برای سازمان و کسب‌وکارها شفاف می‌کند. با این اقدام پایگاه اصلی داده کشور تشکیل می‌شود و با سیاست‌گذاری از رهاشدن برخی مسائل و سواستفاده از داده جلوگیری می‌شود. از طرفی برخی از محدودیت‌های بیش از حد سخت‌گیرانه که تا کنون مانع از توسعه‌های فناورانه در کشور شده‌اند، به شکل اصولی رفع می‌شود. در مورد انواع داده‌ها، علاوه‌بر داده‌هایی با دسترسی آزاد، بخش دیگری از داده‌ها هستند که می‌توانند با سطوح مختلف دسترسی در سازمان رده‌بندی شوند. این سند زیست‌بوم جامع از داده‌های بومی کشور ایجاد کرده و با نظر بخش خصوصی قوانین مالکیت معنوی و ملاحظات اخلاقی متناسب با فناوری‌هایی مثل هوش مصنوعی در آن دیده شده است.

پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC