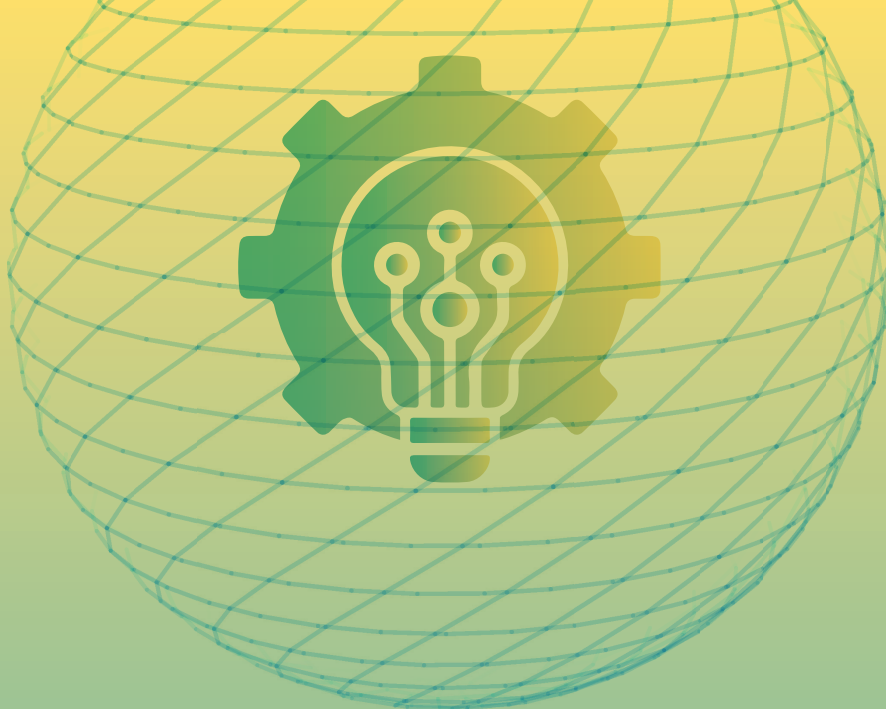


ده رند راهبردی فناوری های نوین در سال ۲۰۲۶ (بر اساس گزارش Gartner)

تاریخ انتشار: آذر ۱۴۰۴





پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

ده روند راهبردی فناوری‌های نوین در سال ۲۰۲۶ (براساس گزارش Gartner)

تاریخ انتشار: آذر ۱۴۰۴



پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

سازمان الکلیه

عنوان گزارش: ده روند راهبردی فناوری‌های نوین در سال ۲۰۲۶ (بر اساس گزارش Gartner)

تهیه کنندگان: عاطفه فرازمنند، لیلا حاجی رجبی

گروه پژوهشی: برنامه‌ریزی تحول دیجیتال

تاریخ نشر: آذر ۱۴۰۴

حقوق معنوی این اثر متعلق به پژوهشگاه ارتباطات و فناوری اطلاعات است و استفاده از آن با ذکر مأخذ بلامانع است.



پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

فهرست مطالب

مقدمه.....	۷
۱. سکوهای توسعه‌ی بومی مبتنی بر هوش مصنوعی.....	۹
۲. سکوهای ابررایانه‌ای هوش مصنوعی.....	۱۰
۳. محاسبات محرمانه.....	۱۰
۴. سامانه‌های چندعاملی.....	۱۰
۵. مدل‌های زبانی خاص هر حوزه.....	۱۱
۶. هوش مصنوعی فیزیکی.....	۱۱
۷. پیش دستی در امنیت سایبری.....	۱۲
۸. خاستگاه دیجیتال.....	۱۲
۹. سکوهای امنیت هوش مصنوعی.....	۱۲
۱۰. Geopatration.....	۱۳
جمع‌بندی.....	۱۴
درس‌آموخته‌ها.....	۱۵



پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

مقدمه

در تازه‌ترین سمپوزیوم جهانی گارتنر، این مؤسسه ده روند راهبردی فناوری را معرفی کرده‌است که انتظار می‌رود تا سال ۲۰۳۰ دستورکار فناوری‌های سازمانی را دگرگون کنند (شکل ۱). این روندها جزئی یا گذرا نیستند؛ بلکه روندهایی هستند که مدل‌های کسب‌وکار، معماری‌های فناوری و شیوه‌های اجرایی سازمان‌ها را در دنیایی که ترکیبی از هوش مصنوعی، ریسک و زیرساخت است، بازآرایی خواهند کرد.

به‌گفته‌ی گارتنر، از سال ۲۰۲۶ به بعد، اختلال فناورانه شتاب خواهد گرفت و توجه به هوش مصنوعی دیگر یک انتخاب اختیاری نیست، بلکه یک ضرورت راهبردی خواهد بود. رهبران فناوری دیگر نمی‌توانند نوآوری را به‌عنوان یک موضوع جانبی در نظر بگیرند؛ بلکه باید با سرعت عمل کنند، راهبرد دیجیتال را با الزامات کسب‌وکار هم‌راستا سازند و نوآوری‌ها را در چارچوبی ایمن، مقاوم و قابل مقیاس پیاده‌سازی کنند. در ادامه، به تحلیل و بررسی این فناوری‌ها پرداخته شده است.

این گزارش ۱۰ روند را معرفی می‌کند که رفتار سازمان‌ها را در سه محور اصلی تغییر خواهد داد:

- ساخت زیرساخت دیجیتال منعطف
- خلق ارزش از طریق فناوری‌های ترکیبی
- حفظ امنیت، اعتماد و حاکمیت داده

چشم‌انداز گارتنر، ده روند راهبردی را در سه خوشه‌ی اصلی (پیشگام، معمار، ترکیب‌کننده) تحت سه نقش ساختاری سازمانی دسته‌بندی می‌کند:

۱. خوشه‌ی معماری زیرساخت هوش‌محور: این بخش بیانگر مرحله‌ی بنیادین تحول است:

جایی که زیرساخت توسعه، قدرت محاسباتی و امنیت داده‌ها برای زیست‌بوم هوش مصنوعی آینده طراحی می‌شوند.

این سه روند به منزله‌ی «سنگ‌بنای فنی» دنیای جدید محسوب می‌شوند:

- **AI-Native Development Platforms:** تحول در فرایند مهندسی نرم‌افزار با استفاده از قابلیت‌های ذاتی هوش مصنوعی در فرایند طراحی و تولید.
- **AI Supercomputing Platforms:** شکل‌گیری زیرساخت‌های ابرمحاسباتی ویژه‌ی آموزش و اجرای مدل‌های عظیم.

- **Confidential Computing**: محور امنیت و حاکمیت داده در محیط‌های پردازش اشتراکی با رمزنگاری در زمان اجرا.
معمار فناوری باید در این مرحله تمرکز را بر نقشه‌ی داده، قدرت محاسبه و امنیت پایه قرار دهد.

۲. **خوشه‌ی ترکیب کننده: این خوشه به مرحله‌ی بلوغ ترکیبی هوش مصنوعی اشاره دارد، یعنی جایی که چندین عامل و مدل هوشمند به‌طور هم‌زمان و هماهنگ با یکدیگر وظایف پیچیده را انجام می‌دهند.**

- **Multiagent Systems**: استفاده از مجموعه‌ای از عامل‌های تخصصی که هماهنگ با یکدیگر وظایف پیچیده را انجام می‌دهند.
- **Domain-Specific Language Models (DSLMs)**: حرکت از مدل‌های عمومی به سمت مدل‌های تخصصی هر صنعت، به‌ویژه در حوزه‌های سلامت، حقوق، انرژی و دولت.
- **Physical AI**: ادغام هوشمندی در جهان فیزیکی از طریق ربات‌ها، پهبادهای و دستگاه‌های متصل (IoT هوش افزا).
در این مرحله، تأکید بر سازگاری بین‌الگویی، تعامل انسان-ماشین و هوشمندسازی محیط‌های واقعی است.

۳. **خوشه‌ی پیشگام امنیت و اعتماد دیجیتال: آخرین بخش، نمایانگر آینده‌ی حکمرانی فناوری است؛ جایی که محور تحول به‌طور عمده بر اعتماد، منشأ داده، شفافیت، حاکمیت و تاب‌آوری ژئوپلیتیکی متمرکز است.**

- **Preemptive Cybersecurity**: گذار از امنیت واکنشی به امنیت پیش‌دستانه بر پایه تحلیل پیش‌بینیگر و هوش مصنوعی.
- **Digital Provenance**: رهگیری منشأ و اصالت داده‌ها و محتوای زنجیره‌تأمین دیجیتال.
- **AI Security Platforms**: معماری‌های امنیتی ویژه‌ی مدیریت و نظارت بر مدل‌ها، API ها و زنجیره ارزش هوش مصنوعی.
- **Geopatriation**: انتقال بارهای کاری و داده‌ها به محیط‌های ابری منطقه‌ای یا حاکمیتی برای کاهش وابستگی ژئوپلیتیکی.

این بخش نشان می‌دهد که امنیت، انطباق و حاکمیت داده از سطح عملیاتی به سطح راهبردی و ژئوپلیتیکی ارتقاء یافته‌اند. در برداشت گارتر، این سه خوشه بیانگر سه موج تحول دیجیتال در عصر هوش مصنوعی بومی هستند.

ماهیت تغییر	نقش انسانی متناظر	نقش کلیدی در تحول
ساخت و پایه‌گذاری واقعیت هوش‌محور	معمار سیستم‌ها	معمار
ترکیب و هم‌افزایی عامل‌ها و مدل‌ها	تحلیلگر و طراح هوشمند	ترکیب کننده
محافظت و حاکمیت بر اکوسیستم جهانی دیجیتال	رهبر راهبردی و اعتمادآفرین	پیشگام

گارتنر با این نقشه نشان می‌دهد که تحول فناورانه از "نوآوری فنی" به "سیاست‌گذاری هوشمند داده و هوش مصنوعی" تغییر یافته است. مدیران ارشد فناوری باید هم‌زمان سه نقش معمار، ترکیب‌گر و پیشگام را ایفا کنند تا اکوسیستم خود را مقیاس‌پذیر، امن و حاکم‌پذیر سازند.



شکل ۱. روندهای برتر فناوری از نظر گارتنر

۱. سکوهای توسعه‌ی بومی مبتنی بر هوش مصنوعی^۱

این دسته از سکوها، قابلیت‌های هوش مصنوعی مولد را به‌صورت درونی و یکپارچه در سراسر چرخه حیات توسعه نرم‌افزار اعمال می‌کنند. نتیجه چنین رویکردی، تولید نرم‌افزار با حجم کدنویسی کمتر، سطح انتزاع بالاتر و سرعت توسعه بیشتر است.

گارتنر پیش‌بینی می‌کند این رویکرد به سنگ‌بنای نسل آینده سامانه‌های کسب‌وکار تبدیل شود؛ به این معنا که مدیران فناوری اطلاعات ناگزیر از بازاندیشی در شیوه‌های مرسوم مهندسی نرم‌افزار خواهند بود.

اگر در سازمان خود هنوز به هوش مصنوعی صرفاً به‌عنوان یک افزونه در فرآیند توسعه می‌نگرید و نه یک تحول در سطح سکو و معماری، خطر عقب‌ماندن از رقبا برای شما بسیار جدی است.

۲. سکوهای ابررایانه‌ای هوش مصنوعی^۱

با رشد تصاعدی حجم مجموعه داده‌ها و افزایش ابعاد و پیچیدگی مدل‌های هوش مصنوعی، تکیه بر ماشین‌های مجازی متعارف در ابرهای عمومی دیگر پاسخ‌گو نخواهد بود. گارتنر این نسل جدید معماری‌های زیرساختی را «سکوهای ابررایانه‌ای هوش مصنوعی» می‌نامد؛ بسترهای محاسباتی با کارایی بسیار بالا که برای اجرای مدل‌های فوق‌مقیاس و بارهای کاری تحلیلی سنگین بهینه شده‌اند. در عمل، سازمان‌ها ناچارند میان سه گزینه راهبردی تصمیم بگیرند: سرمایه‌گذاری برای ساخت و تملک چنین زیرساختی، اجاره توان محاسباتی از ارائه‌دهندگان تخصصی، و یا ورود به مدل‌های مشارکتی برای بهره‌برداری مشترک از ظرفیت پردازشی در سطح اگزااسکیل یا نزدیک به آن. در این مقیاس، موضوعاتی نظیر حاکمیت، ساختار هزینه و مدیریت مصرف انرژی از مسائل صرفاً فنی فراتر رفته و به دغدغه‌هایی راهبردی برای مدیران ارشد تبدیل می‌شوند.

۳. محاسبات محرمانه^۲

با مهاجرت داده‌ها و مدل‌های حساس به محیط‌های ابری اشتراکی، هیبریدی یا بسترهایی که به‌طور کامل قابل اعتماد نیستند، حفاظت از داده‌ها در زمانی که «در حال پردازش» هستند، به موضوعی حیاتی تبدیل شده است. در رویکرد محاسبات محرمانه، داده نه‌تنها در زمان ذخیره‌سازی و انتقال، بلکه هنگام پردازش نیز در وضعیت رمزنگاری شده باقی می‌ماند و تنها در محیط‌های محاسباتی ایزوله و قابل اعتماد قابل استفاده است.

گارتنر، محاسبات محرمانه را یکی از روندهای بنیادی در امنیت هوش مصنوعی و تحلیل داده‌ها می‌داند و تأکید می‌کند که رهبران فناوری باید به‌طور صریح به پرسش‌های زیر پاسخ دهند: آیا زیرساخت‌های فعلی خود را بالقوه در معرض نفوذ و دستکاری در نظر می‌گیرید؟ آیا معماری شما برای کار در محیط‌های چندابری و چندقانون‌گذاری طراحی شده و برای پیاده‌سازی اصول «بی‌اعتمادی صفر»^۳ آمادگی دارد؟

۴. سامانه‌های چندعاملی^۴

هوش مصنوعی در حال عبور از مرحله تکیه بر «یک مدل منفرد» است. گارتنر پیش‌بینی می‌کند که سامانه‌هایی متشکل از چندین عامل^۵ هوش مصنوعی همکاری‌کننده، که برای انجام کارهای پیچیده با

1. AI Supercomputing Platforms
2. Confidential Computing
3. Zero Trust
4. Multiagent Systems
5. Agents

یکدیگر تعامل و تقسیم کار می‌کنند، به سطح استفاده سازمانی برسند. پیام کلیدی این است که دیگر نباید «بات»ها را ابزارهایی منفرد و جزیره‌ای تلقی کرد؛ بلکه باید آن‌ها را موتورهای هماهنگی، تصمیم‌سازی و ترکیب انواع مختلف هوش دانست. بر این اساس، سازمان‌ها لازم است در نقشه راه خود لایه‌های هماهنگی میان عامل‌ها، سازوکارهای حکمرانی و کنترل رفتار عامل‌ها، و معماری‌های ترکیب‌پذیر برای اجزای مختلف هوش مصنوعی را به‌طور مشخص طراحی و پیاده‌سازی کنند.

۵. مدل‌های زبانی خاص هر حوزه^۱

اگرچه مدل‌های زبانی بزرگ عمومی همچنان نقش مهمی در اکوسیستم هوش مصنوعی ایفا خواهند کرد، گارتنر روند غالب را حرکت به سمت مدل‌های زبانی اختصاصی هر حوزه می‌داند؛ برای مثال در حوزه‌های حقوقی، بالینی، مالی یا صنایع خاص.

برای سازمان‌ها، این تحول به معنای ضرورت سرمایه‌گذاری بر ایجاد، تنظیم یا میزبانی مدل‌هایی است که بر پایه داده‌های اختصاصی و دارای مالکیت همان حوزه آموزش دیده‌اند. تکیه صرف بر مدل‌های عمومی دیگر برای دستیابی به مزیت رقابتی، مدیریت ریسک، و بهره‌برداری ایمن و قابل اعتماد از هوش مصنوعی کافی نخواهد بود.

۶. هوش مصنوعی فیزیکی^۲

در این مرحله، هوشمندی از مرزهای صرفاً دیجیتال عبور کرده و وارد جهان فیزیکی می‌شود: ربات‌ها، پهپادها، تجهیزات هوشمند و سامانه‌های تعبیه‌شده‌ای که در تعامل مستقیم با محیط، ادراک می‌کنند، تصمیم می‌گیرند و عمل می‌کنند. گارتنر این حوزه را «هوش مصنوعی فیزیکی» می‌نامد؛ نقطه تلاقی دنیای دیجیتال با مکانیک. برای صنایعی که ماهیت آن‌ها بر عملیات فیزیکی استوار است - مانند تولید، لجستیک، انرژی یا زیرساخت - پرسش‌های کلیدی از این جنس مطرح هستند: در کدام نقاط زنجیره ارزش می‌توان هوش مصنوعی را در ماشین‌ها، محیط‌های کاری یا فرآیندهای میدانی تعبیه کرد؟ نقشه راه ما برای ارتقای سطح خودکارسازی، خودمختاری و آگاهی محیطی در ماشین‌ها چیست؟ پاسخ به این پرسش‌ها تعیین می‌کند که سازمان تا چه حد می‌تواند از مزایایی مانند کاهش هزینه، افزایش ایمنی، بهینه‌سازی مصرف منابع و خلق مدل‌های جدید کسب‌وکار مبتنی بر دارایی‌های فیزیکی بهره‌مند شود.

1. Domain-Specific Language Models - DSLMs

2. Physical AI

۷. پیش دستی^۱ در امنیت سایبری

در اغلب سازمان‌ها، الگوی رایج در امنیت سایبری همچنان واکنشی است؛ یعنی ابتدا حمله یا تهدید رخ می‌دهد و سپس فرآیند شناسایی، تحلیل و پاسخ آغاز می‌شود. گارتنر استدلال می‌کند که این رویکرد دیگر کفایت نمی‌کند و باید به سمت گردش کارهای پیش‌دستانه حرکت کرد؛ گردش کارهایی که با تکیه بر هوش مصنوعی، تحلیل پیش‌نگر و لایه‌های هماهنگ‌سازی، تهدیدها را پیش از وقوع شناسایی و خنثی کند؛ و یا دست‌کم اثر آن‌ها را به‌طور معناداری کاهش دهد.

سؤال کلیدی برای مدیران فناوری این است: آیا سازمان شما همچنان عمدتاً در موضع دفاع واکنشی قرار دارد، یا سامانه‌ها و فرآیندهایی طراحی کرده‌اید که تهدیدها را زودتر تشخیص می‌دهند، خود را با محیط و الگوهای جدید حمله تطبیق می‌دهند و تاب‌آوری کسب‌وکار را در برابر مخاطرات سایبری تقویت می‌کنند؟

۸. خاستگاه دیجیتال^۲

در دنیایی که حجم محتواهای مولد، زنجیره‌های تأمین داده‌ی پیچیده و اکوسیستم‌های وابسته به طرف‌های ثالث دائماً در حال گسترش است، ردیابی منبع، تاریخچه و اصالت داده‌ها، نرم‌افزارها و مدل‌های یادگیری ماشین به یک ضرورت حیاتی تبدیل شده است. گارتنر این توانمندی را «خاستگاه دیجیتال» می‌نامد؛ یعنی توانایی این‌که بدانیم هر داده از کجا آمده، چه مسیری را طی کرده و امروز در کجا و چگونه به‌کار گرفته می‌شود.

در این زمینه پرسش‌های کلیدی برای سازمان‌ها از این قرار است: آیا می‌توانید مسیر ورود و گردش هر داده را در سامانه‌های خود ردیابی کنید؟ آیا به‌روشنی می‌دانید از آن داده چگونه استفاده شده و چه تصمیم‌هایی را تحت‌تأثیر قرار داده است؟ در چنین فضایی، شفافیت در زنجیره داده و سطح اعتماد به منابع و فرآیندها، خود به‌داری‌ها و مزیت‌های رقابتی سازمان تبدیل می‌شود.

۹. سکوهای امنیت هوش مصنوعی^۳

با گسترش به‌کارگیری مدل‌های اختصاصی در سازمان‌ها، گارتنر بر ضرورت شکل‌گیری نسل تازه‌ای از سکوها، چارچوب‌ها و نظام‌های پایش و حکمرانی امنیت هوش مصنوعی تأکید می‌کند؛ سامانه‌هایی که به‌طور ویژه برای مدیریت همه مؤلفه‌های مرتبط با هوش مصنوعی - از خود مدل‌ها و زنجیره‌های

1. Preemptive Cybersecurity
2. Digital Provenance
3. AI Security Platforms

پردازش گرفته تا رابط‌های برنامه‌نویسی و سایر صنایع هوش مصنوعی - طراحی می‌شوند. زمانی که هوش مصنوعی به جزء حیاتی مأموریت‌های اصلی سازمان بدل شود، موضوعاتی همچون ریسک مدل، انحراف عملکرد، حملات خصمانه و مخاطرات زنجیره تأمین هوش مصنوعی از سوی تأمین‌کنندگان ثالث، از سطح یک نگرانی صرفاً فنی فراتر رفته و به دغدغه‌هایی در تراز هیئت‌مدیره تبدیل می‌شوند.

1. Geopattribution

در نهایت، گارتنر مفهوم راهبردی «بازوطن‌سازی ژئوپلیتیک» را مطرح می‌کند؛ رویکردی که به معنای انتقال بارهای کاری و زیرساخت‌های حیاتی به فضاهای ابری منطقه‌ای یا حاکمیتی است. این تغییر جهت، پاسخی است به ریسک‌هایی که از تحولات ژئوپلیتیک، الزامات مقرراتی سخت‌گیرانه یا اختلال‌های زنجیره تأمین ناشی می‌شوند و می‌توانند دسترسی سازمان‌ها به خدمات ابری جهانی را تهدید کنند.

این گرایش، سازمان‌ها را وادار می‌کند تا تصمیمات معماری خود را جدی‌تر از گذشته بازنگری کنند. پرسش‌های کلیدی در این حوزه برای سازمان‌ها به قرار زیر است:

آیا قراردادهای فعلی شما با ارائه‌دهندگان جهانی خدمات ابری، سازمانتان را در معرض محدودیت‌ها و ریسک‌های مقرراتی قرار داده است؟ آیا ساختار فنی و عملیاتی سازمان برای تاب‌آوری منطقه‌ای طراحی شده است؟ و آیا وابستگی‌های خود به ارائه‌دهندگان ثالث را به صورت مستمر پایش و مدیریت می‌کنید؟

• سه اقدام راهبردی برای رهبران فناوری

گارتنر سه محور کلیدی را به عنوان دستورکار راهبردی برای تصمیم‌سازان و رهبران حوزه فناوری پیشنهاد می‌کند؛ محورهایی که نشان می‌دهند برای بهره‌گیری واقعی از موج جدید نوآوری، چه تغییراتی باید در سطح معماری، حاکمیت و نگاه راهبردی ایجاد شود.

۱. **تحکیم زیربنا:** پیش از آن‌که بر کاربردهای نمایشی یا راه‌حل‌های پرحلوه تمرکز کنید، باید از استواری معماری داده، ظرفیت محاسباتی و چارچوب‌های حکمرانی فناوری در سازمان اطمینان یابید. زیربنای پایدار، پیش‌شرط بهره‌گیری مؤثر از نسل تازه نوآوری‌هاست؛ بدون آن، حتی بهترین مدل‌ها نیز به نتیجه مطلوب نخواهند رسید.

۲. **سرمایه‌گذاری در هماهنگی و لایه پیوند پلتفرمی:** سامانه‌ها و معماری‌هایی طراحی کنید که عامل‌ها، مدل‌های تخصصی هر حوزه، چارچوب‌های اعتماد و سازوکارهای خاستگاه دیجیتال را به صورت ترکیب‌پذیر و هم‌افزا به یکدیگر متصل کنند. هدف این است که پشته هوش مصنوعی سازمان یکپارچه، سازگار و آماده تعامل با سایر زیرسامانه‌های محیطی باشد؛ چه

در سطح عملیات داخلی و چه در سطح اکوسیستم‌های بیرونی.

۳. **نگاه فرصت‌محور به ریسک و تنظیم‌گری:** روندهایی مانند بازوین‌سازی ژئوپلیتیک، محاسبات محرمانه و خاستگاه دیجیتال را صرفاً به‌عنوان الزامات انطباق نبینید؛ بلکه به‌مثابه ابزارهایی برای تمایز، امنیت پایدار و خلق ارزش راهبردی در نظر بگیرید. درک این‌که ریسک و تنظیم‌گری می‌توانند به مزیت رقابتی تبدیل شوند، بخشی از بلوغ سیاست‌گذاری فناوریانه در آینده است.

این سه محور، چارچوبی فراهم می‌کنند تا سازمان‌ها بتوانند نه‌فقط با موج تحولات فناوریانه هماهنگ شوند، بلکه آن را به موتور پیش‌ران رشد و نوآوری خود تبدیل کنند.

جمع‌بندی

دستورکار فناوری سال ۲۰۲۶ گارتنر نشان می‌دهد که مرزهای آینده فناوری سازمانی دیگر صرفاً رخدادهایی در افق‌های دور نیستند؛ بلکه همین امروز، در تصمیم‌ها، ساختارها و الگوهای سرمایه‌گذاری سازمان‌ها در حال شکل‌گیری‌اند. پلتفرم‌های بومی هوش مصنوعی، سامانه‌های چندعاملی، هوشمندی فیزیکی و پویای ژئوفناورانه، دیگر سناریوهایی محتمل و نظری نیستند؛ بلکه به متغیرهایی بالفعل در معادلات حکمرانی دیجیتال تبدیل شده‌اند.

در این چشم‌انداز، سازمان‌هایی که از درون متحول شوند و معماری فناوری خود را با مدل کسب‌وکار و سیاست‌گذاری داده‌محور هم‌راستا کنند، همچنین سازوکار انطباق مستمر با تغییر را درونی سازند، نه‌تنها در مسیر تحول جهانی عقب نخواهند ماند، بلکه به رهبران موج جدید تحول فناوریانه بدل خواهند شد.

تحلیل گارتنر بر این نکته تأکید دارد که محور تحول فناوری جهانی از «نوآوری صرف فنی» به سوی «سیاست‌گذاری هوشمند مبتنی بر داده و هوش مصنوعی» تغییر یافته است. در چنین الگویی، فناوری از جایگاه یک ابزار تولید ارزش به سطح «زیرساخت قدرت و حکمرانی» ارتقا یافته و به عاملی برای شکل‌دهی نظم اقتصادی و امنیتی نوین تبدیل شده است. در این چارچوب، مدیران ارشد فناوری در سطح ملی و سازمانی باید به‌طور هم‌زمان سه نقش بنیادین را ایفا کنند:

۱. معمار تحول دیجیتال

- برای طراحی زیرساخت‌های داده‌محور، آینده‌نگر و منطبق با نیازهای توسعه پایدار کشور؛

۲. ترکیب‌گر هوش‌ها و سامانه‌های هوشمند

- به‌منظور هم‌افزایی میان ظرفیت‌های فناوریانه در صنایع، خدمات و حکمرانی؛

۳. پیش‌ران حکمرانی و اعتماد دیجیتال

- در جهت صیانت از سرمایه‌های داده‌ای، تقویت امنیت سایبری و ارتقای اقتدار فناوریانه ملی.

ترکیب و ایفای هم‌زمان این سه نقش، شرط گذار از وضعیت وابستگی فناورانه به شکل‌گیری اکوسیستم هوشمند و مقیاس‌پذیر ملی است؛ اکوسیستمی که ضمن حراست از امنیت و حاکمیت داده، بستر ظهور رقابت‌پذیری پایدار، تاب‌آوری زیرساختی و تصمیم‌سازی مبتنی بر هوش مصنوعی را فراهم می‌آورد. در این نگاه، تحول فناورانه صرفاً فرایند فنی یا صنعتی نیست، بلکه یک گذار تمدنی است که سیاست‌ها، استعداد انسانی و حاکمیت داده را در راستای اقتدار دیجیتال کشور بازآرایی می‌کند.

درس‌آموخته‌ها

۱. آینده‌ی فناوری در تصمیم‌های امروز نهادینه می‌شود.

نحوه‌ی سرمایه‌گذاری، تنظیم‌گری و سیاست‌گذاری فعلی در حوزه‌های داده و هوش مصنوعی، نه‌تنها جهت‌گیری فناورانه کشور را تعیین می‌کند بلکه مرزهای رقابت‌پذیری و امنیت دیجیتال آینده را مشخص می‌سازد. دوران «انتظار برای بلوغ فناوری» جای خود را به «پیش‌فعالیت راهبردی» داده است.

۲. تاب‌آوری فناورانه از درون سازمان آغاز می‌شود.

تغییرات محیطی (از ژئوپلیتیک تا تحول پلتفرمی) زمانی قابل مدیریت‌اند که سازمان‌ها دارای فرهنگ داده‌محور، ساختار یادگیرنده و معماری فناوری قابل انطباق باشند. تجهیز بیرونی بدون تغییر الگوی تصمیم‌سازی درونی، منجر به وابستگی فناورانه می‌شود نه اقتدار دیجیتال.

۳. اقتدار دیجیتال از هم‌افزایی سه محور به‌دست می‌آید: زیرساخت داده‌محور، حکمرانی هوشمند و اعتماد فناورانه.

هماهنگی میان این سه محور، پایه‌ی شکل‌گیری اکوسیستم هوشمند ملی است؛ جایی که داده‌های بومی با اتکا به سیاست‌های شفاف و قابل اعتماد به منبع تصمیم و نوآوری بدل می‌شوند.

۴. تحول فناورانه یک فرایند حکمرانی است نه پروژه فناورانه.

استقرار فناوری‌های تحول‌آفرین نیازمند همراهی ساختار نهادی، چارچوب‌های حقوقی داده، و ظرفیت انسانی تصمیم‌ساز است. به‌روزرسانی مداوم سیاست‌های فناوری باید در چرخه‌ی رسمی تصمیم‌سازی ملی نهادینه شود تا کشور از مرحله‌ی «پذیرش فناوری» به «هدایت فناوری» گذر کند.



پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

نشانی: تهران، انتهای خیابان کارگر شمالی،

پژوهشگاه ارتباطات و فناوری اطلاعات

ایمیل: info@itrc.ac.ir