نسل چهارم

ماهنامه فناوری های نوین
اطلاعات و ارتباطات
فارسی- انگلیسی ۱۰۰۰۰۰ تومان

سال دهم
مهر ۱۴۰۳
شماره ۱۰۹

با همراهی شما
۹ ساله شدیم

تشکیل ستاد هماهنگی پیشرفت و امنیت سایبری با هدف هماهنگی و تقسیم کار ملی

همراه اول

www.mci.ir

ابرهمراهی

سرویس ذخیره‌سازی ابری همراه اول

abrehamrahi.ir

مبین نت

پیشرو در مسیر سبز تحول دیجیتال

www.mobinnet.ir

فرافن
farafan

«دانش بنیان تولیدی نوع یک»

در حوزه خدمات طراحی و بهینه‌سازی شبکه‌های ارتباطی موبایل

NECTON DNS VIRUSPAAD QOE Radio Patrol Raibin

- طراحی و تولید مودم‌های LTE و 5G
- پلتفرم اینترنت اشیا (رای بین)
- کیوسک ویروسکاو
- راهکار DNS شبکه‌های مخابراتی
- راهکار مدیریت تجربه کاربر در شبکه‌های مخابراتی (QOE)
- ارائه سرویس مدیریت شده در حوزه IT
- سامانه مدیریت راندمان و بهینه‌سازی مخابراتی (RPAT)

تهران، میدان آرژانتین
خیابان الوند، کوچه برمک، پلاک ۸
کدپستی: ۱۵۱۶۶۳۴۱۱۴
تلفن: ۴۱۲۹۷۰۰۰

farafan.ir
info@farafan.ir

PAYACO

صنایع ارتباطی پایا

چهل سال طراحی و تولید


سامانه تصویربرداری
موج میلی متری


ارائه سرویس های **VoIP** ابری و راهکار شبکه های
نسل جدید **NGN** و مبتنی بر معماری **IMS**


محصولات و راه حل های هوشمندسازی در حوزه پارکینگ،
آسانسور، تردد، مدیریت مصرف انرژی، مانیتورینگ خرابی
(نظارت، پیش بینی، پیشگیری)، با ارائه پلتفرم های جامع و
سخت افزارهای مرتبط


آنتن های **LTE** مولتی باند شبکه سلولی (۱۶، ۲۴و۳۲ پورت)
سازگاری کامل با **eNodeB** شرکت ها از جمله هواوی،
نوکیا و اریکسون


تجهیزات زیرساخت مراکز داده شامل را هرو سرد و گرم،
رک و پایه‌رک، پاورماژول های هوشمند، کنترل و مانیتورینگ
مرکز داده بهمراه تجهیزات حوزه پسیو مانند انواع پچ پنل،
مدیریت کابل، لدر و سبدهای نصب کابل



انواع رک های داخلی جهت سرور و شبکه،
رک های بیرونی مخابراتی، شلترهای ثابت
و سیار مخابراتی و اضطراری


خودپرداز و کیوسک های بانکی

تهران، خیابان دماوند، تقاطع رسالت، شماره ۲۷۶ | تلفن : ۷۳۰۳۷ | فکس : ۷۷۹۶۹۶۱۳ - ۰۲۱ | کدپستی : ۱۷۴۶۷

info@payaco.com | payaco.com

MADE IN IRAN

دنیا با یوتل کوچکتر می‌شود ...

Modem
LT643
4.5G

Tel

www.argtelecom.com

شرکت خدمات مخابراتی ارگ جدید

تولیـد کننـده انـواع مـودم

ADSL . VDSL . LTE . GPON

راهکار ویژه
مودیان حقیقی
و اصناف

داده پردازی معتمد
تیس

معتمد مالیاتی نوع اول
سازمان امور مالیاتی کشور

ارسال صورتحساب الکترونیکی

مودیان حقوقی و اصناف

با تضمین شرکت معتمد

- راهکار ویژه اصناف
- صنف طلا، جواهر و پلاتین
- پزشکان و وکلا
- مشاورین حقوقی و خانواده

۹۰۰۰۱۵۱۵

تماس رایگان بدون پیش شماره از سراسر کشور

@tisstsp

www.tisstsp.ir

خط اختصاصی تماس مودیان حقیقی و اصناف – فقط در معتمد تیس

راز **اتصـــــــال** دائم

خدمات پهنای باند اختصاصی

تماس رایگان
۹۰۰۰ ۰۰۰۰
بدون نیاز به کد

www.asiatech.ir

آسیاتک
asiatech

صاحب امتیاز و مدیرمسوول:
مسعود فاتح
رئیس شورای سیاست گذاری:
دکتر مهدی ادیبان
مشاوران مدیرمسوول:
نیما فاتح، دکتر داوود ادیب، فرامرز رستگار، فریبرز نژاددادگـر، فریبـرز ایرانی، دکتر محمد احسـان خرامید، مهران ارشادی فر و دکتر مسعود ظهرابی
سردبیر:
مونا ارشادی فر
دبیر تحریریه:
زهرا طاهری
مدیر توسعه کسب و کار:
محمد تهرانی نصر
همکاران این شماره:
فرزانه احمدی منش و حمزه فاتح

عکاس:
سهند بیژن نیا
روابط عمومی و امور مشترکین:
سحر حسینی
صفحه آرایی و طرح روی جلد:
سمیرا علیدادی

با تشکر از:
دکترسـید سـتار هاشـمی، دکتر علی اصغر انصاری، دکتر علیرضا عبداللهی نژاد، فردخت شاه حسینی، مجید ذوقی، مجید سـلطانی، حسـین ریاضی، دکتر اسـماعیل ثنایی، محمدعلـی یوسفـی زاده، حامد حکاکان، دکتر سعیـد عسکری، حامد شـیخ پور، محمد حسین افتخاری، مهدی طالبی، مهرداد میراسماعیلی، دکتر امیـر کیهـان، سعید کیایی، دکتر سـپیده عابدینی، محمود صادقیان، محمـد جابـری، محسن ابوئی مهریزی و الهام عدالتی

امور آماده سازی وچاپ:
چاپخانه پیمان نواندیش
نشانی چاپخانه:
تهران، پیچ شمیران، خیابان بهار، خیابان سمیه، پلاک ۵۸، طبقه زیرهمکف
تلفن: ۸۸۸۴۴۶۶۳ - ۰۹۱۲۲۴۳۸۳۲۴
ناظر فنی چاپ: محمدرضا کبودانی
نشانی ماهنامه:
انتهای بلوار کشاورز - خیابان دکتر قریب
خیابان فرصت شیرازی - پلاک ۱۰۸ - واحد ۱۷
کدپستی ۱۴۱۹۹۶۳۳۷۹
امور بازرگانی: ۰۹۱۲۸۲۱۶۶۵۸
تلفن: ۶۶۵۹۲۵۷۳
دورنگار: ۶۶۹۳۶۰۷۶
وب سایت: www.4Gnews.ir
پست الکترونیک: info@4Gnews.ir

ماهنامه نسل چهارم

دکتر داوود ادیب
رئیس کانون هماهنگی فاوا

لزوم تداوم و تقویت رویکردهای حمایتی در تولید محصولات بومی زیرساختی

در هفته های اخیر اظهارنظرهای مختلف و متفاوتی از سوی برخی از صاحب نظران در خصوص امنیت سایبری صورت پذیرفته است که فارغ از هر گونه جهت گیری خاص در خصوص این اظهار نظرها و نقد واردات محصولات زیرساختی و یا زیر سوال بردن بخشی از خریداران در خرید محصولات خارجی و یا تایید عملکرد برخی دیگر از آنها در این راستا، می توان چنین اذعان کرد که تکلیف این موضوع کاملا مشخص است و در این خصوص باید به قوانین جاری کشور رجوع کرد.

این که برخی از تولیدکنندگان محصولات بومی، از این موضوع استفاده ابزاری کنند و سریعا در صدد ممنوعیت محصولاتی که به هیچ وجه نمونه داخلی ندارند، برآیند، موضوعی منطقی به نظر نمی‌رسد و این که برخی از شرکت های واردکننده تجهیزات، توجیه‌های غیر اصولی ارایه دهند و با طرح موضوعات غیر فنی تلاش برای واردات محصولاتی که نمونه های متعدد تولید داخل که دارای تاییدیه های لازم مراجع ذیصلاح می باشند، نمایند نیز امری غیر قابل قبول خواهد بود و طبیعتا نهادهای نظارتی و امنیتی و همین‌طور وزارت ارتباطات و وزارت صمت در این خصوص تعیین تکلیف خواهند کرد.

فهرست کالاهای ممنوعه جهت واردات که دارای نمونه مشابه داخلی می باشد، از سال ۹۰ شکل قانونی مناسبی پیدا کرده است، به شکلی که هیات وزیران در جلسه مورخ ۱۳۹۰/۷/۱۴ به استناد اصل یکصد و سی و هشتم قانون اساسی جمهوری اسلامی ایران تصویب نموده است که خرید کالاهای خارجی (اعم از کالای ساخته شده، قطعات، ملزومات، تجهیزات و غیره تحت هر عنوان) دارای نمونه و یا مشابه تولید داخلی توسط تمامی دستگاه های دولتی (موضوع مواد (۲)، (۳)، (۴) و (۵) قانون محاسبات عمومی کشور و ماده (۵) قانون مدیریت خدمات کشوری و موارد مستثنی مندرج در ماده (۱۱۷) قانون مدیریت خدمات کشوری) و همچنین تمامی دستگاه ها یا نهادها و عناوین مشابهی که به نحوی از انحاء از بودجه عمومی یا دولتی استفاده می کنند، ممنوع می‌باشد. همچنین بند ۵ تصویب نامه شماره ۲۶۷۲۵/ت ۴۸۴۶۲ هـ مورخ ۱۳۹۳/۳/۱۱ فهرست ممنوعیت خرید کالاهای خارجی دارای تولید مشابه داخلی و نیز تصویب نامه هیات وزیران به شماره ۴۲۸۳۹/ت ۵۳۷۸۶ ه ـ مورخ ۱۳۹۶/۴/۱۵ در خصوص ممنوعیت خرید کالاهای خارجی دارای تولید مشابه داخلی را ابلاغ نموده است که در آن لیست کالاهای دارای ممنوعیت خرید از منابع خارجی مشخص می باشد و کافی است به این اسناد و نسخه های جدید آن که سالانه به روز رسانی می گردند، مراجعه کرد.

حتی در یکی از مصوبات، مستقیما به برخی از تجهیزات زیرساختی نیز اشاره شده است. هیات وزیران در جلسه ۱۹ اردیبهشت سال ۱۳۹۷ به پیشنهاد شماره ۳۶۸۱۸ مورخ پنجم اردیبهشت ماه ۱۳۹۷ وزارت صنعت، معدن و تجارت و به استناد اصل یکصد و سی و هشتم قانون اساسی جمهوری اسلامی ایران فهرست تکمیلی ممنوعیت خرید کالاهای خارجی دارای تولید مشابه داخلی در (۸) ردیف شامل شبکه های نسل جدید NGN؛ سیستم مدیریت شبکه مخابراتی (HSS/SBC/OSS/BSS/NMS)، تجهیزات رادیوترانک، برخی از تجهیزات DWDM/ROADM، تجهیزات SDH نوری تا ۱۶ STM؛ تجهیزات پسیو دسترسی نوری (FTTX)، تجهیزات اکتیو (ONU/ FTTX ONT)، مفصل های مخابراتی و متعلقات (مسی و نوری) را به فهرست تصویب نامه شماره ۲۶۷۲۵/ت۴۸۴۶۲هـ مورخ ۱۱ خرداد ۱۳۹۳ و اصلاحات بعدی آن الحاق نموده است.

خوشبختانه موضوعات امنیتی در برنامه های وزیر ارتباطات دولت پیشین نیز مورد توجه قرار گرفته بود و ایشان در برنامه های خود موضوع «افزایش بی سابقه حملات به زیرساخت های فاوای کشور در سال های اخیر، نشر اطلاعات محرمانه و خصوصی افراد و سازمان های مختلف، افزایش قابل توجه جرایم سایبری مرتبط با فضای خصوصی و امنیت زیرساخت ها در سایه موازی کاری» را مورد تاکید قرار داده بود.

وزیر پیشین ارتباطات و فناوری اطلاعات، وابستگی شدید کشور به محصولات سخت افزاری و نرم افزاری خارجی، آسیب پذیری زیرساخت های حساس و حیاتی کشور و وجود انگیزه های قوی و برنامه ریزی مستمر برای از کار انداختن این زیر ساخت ها، استفاده از تجهیزات خارجی در شبکه های اصلی ارتباطی عمومی و اختصاصی و عدم توفیق محصولات و خدمات داخلی در کسب رضایت و اعتماد فراگیر کاربران، ضعف در قوانین و مقررات به منظور التزام به ارتقاء امنیت زیرساخت های فاوا و دوگانه «احراز هویت» در مقابل «نقض حریم خصوصی» که بعضا دستاویزی برای امنیتی جلوه دادن فضای مجازی کشور بوده است را مورد تاکید قرار داده بود و اینکه در واقع عدم تحقق امنیت و بی توجهی به سند الزامات شبکه ملی اطلاعات باعث نا امن تر شدن این فضا و ضرر و زیان مادی و معنوی کاربران فضای مجازی کشور بوده است را مطرح نموده بود که در شرایط بحرانی این روزهای منطقه توجه به برنامه های وزیر پیشین ارتباطات که در خصوص موضوعات امنیتی کاملا به جا و پیشگیرانه بوده است را دو چندان می سازد.

حمله سایبری به دستگاه‌های ارتباطی در لبنان نشانگر این موضوع است که وابستگی به کشورهای مختلف در حوزه تجهیزات زیرساختی و ارتباطی به چه میزان می تواند آسیب پذیری را بالا ببرد و طبیعتا این موضوعی نیست که با آن احساسی برخورد نمود و جنبه های بازرگانی آن را بیشتر از جنبه های امنیتی و ملی در نظر گرفت و به سادگی از کنار آن گذشت، البته اشاره به این موضوع هم ضروری است که خوشبختانه در سال های اخیر نهادهای نظارتی و قانون گذار این حوزه از قبیل شورای عالی فضای مجازی، وزارت ارتباطات، مرکز افتا و سازمان پدافند غیرعامل به نظارت در این حوزه پرداخته و توصیه های لازم را ارایه نموده و می نمایند.

بدیهی است که امروز می بایست مقداری متفاوت بیندیشیم و بدانیم که این دغدغه ها در راستای این رویکرد است که صرفا موضوعات قیمتی و کیفیت بالا در محصولات زیرساختی نمی تواند ملاک تصمیم گیری باشد و طبیعتا در این گونه تجهیزات، جنبه های دیگری از اصول بازرگانی، از جمله موضوعات امنیتی و توصیه های مرکز افتا و سازمان پدافند غیرعامل کشور در راس این گونه شاخص ها، نیز می بایست به دقت مورد توجه قرار گیرد. در همین راستا پیشنهادات عملیاتی در حوزه امنیت که طبیعتا در برنامه های وزیر ارتباطات دولت چهاردهم و بخش های مرتبط حاکمیتی نیز یقینا مورد توجه خواهد بود، می تواند شامل موارد ذیل باشد:

- تلاش برای عضویت، همکاری و حضور فعال در مجامع بین المللی رسمی حوزه فاوا و پیشنهاد ایجاد سازوکار قانونی و حقوقی بین المللی لازم جهت پیگیری در صورت حمله به زیرساخت های کشورها،
- تربیت و حفظ نیروهای متخصص حوزه امنیت فناوری اطلاعات در کشور با ایجاد انگیزه، از جمله ارایه مشوق های لازم به کارفرمایان این حوزه و امریه نمودن بدون تشریفات این گونه افراد از طریق شرکت های خصوصی در این حوزه،
- تدوین واحد درسی مرتبط با موضوعات امنیتی در دوره های دبیرستانی و اجرای برنامه ارتقای سطح دانش امنیت و مهارت های عمومی در بکارگیری فناوری های نوین ارتباطی و اطلاعاتی و ارتقا دانش و سواد رسانه ای،
- تقویت دانش هوش مصنوعی در کشور و استفاده از هوش مصنوعی در پیشگیری حملات،
- ارتقای توان داخلی در اولویت بالا و پیش بینی بودجه های لازم برای سال ۱۴۰۴ با نگاه کاهش وابستگی به خارج از کشور با سرمایه گذاری و حمایت از تولیدکنندگان حوزه افتا،
- بومی سازی دانش، فناوری، خدمات و تولید تجهیزات مورد نیاز کشور با استفاده از زیست بوم شرکت های دانش بنیان داخلی و علی الخصوص تولیدکنندگان حوزه افتای کشور،
- حمایت از شرکت های دانش بنیان داخلی فعال در حوزه فاوا با در نظر گرفتن تسهیلات مالیاتی، تضمین خرید و الزام بهره برداری از محصولات مرتبط با فناوری های نوین اطلاعات و ارتباطات بومی دارای تاییدیه مرکز افتا و سازمان پدافند غیرعامل کشور در سازمان های مهم، حساس و حیاتی،
- سازمان دهی ساختار مرکز ملی پایش امنیت زیرساخت های ارتباطی و اطلاعاتی کشور برای پیشگیری، کشف و دفع حملات،
- سرمایه گذاری در راستای تهیه ابزارهای مناسب برای استفاده در سازمان های دولتی و خصوصی با هدف مقابله با حملات سایبری احتمالی.

تاکید عارف بر تشکیل ستاد منسجم برای پیاده سازی سیاست های امنیت سایبری

معاون اول رئیس جمهور بر تشکیل یک ستاد منسجم و با ضمانت اجرایی بالا جهت پیاده سازی سیاست ها و دستورات در حوزه امنیت و پیشرفت فضای سایبری تاکید کرد.

جلسه ای درخصوص تشکیل ستاد هماهنگی پیشرفت و امنیت فضای سایبری به ریاست معاون اول رئیس جمهور برگزار و در زمینه سازوکارهای تشکیل این ستاد با هدف هماهنگی و تقسیم کار ملی در حوزه امنیت و پیشرفت فضای سایبری بحث، بررسی و تصمیم گیری شد.

دکتر محمدرضا عارف در این جلسه با اشاره به اهمیت فضای مجازی و مزیت های کشور در بخش های علم و فناوری، شرکت های دانش بنیان، حوزه نرم افزاری و فناوری های پیشرفته در کنار جوانان تحصیل کرده، نخبه و با انگیزه تأکید کرد: فضای سایبری نه یک تهدید بلکه فرصتی برای توسعه همه جانبه کشور بر پایه اقتصاد دیجیتال است و باید پیشرفت و امنیت فضای مجازی توأمان در کنار یکدیگر قرار گیرند.

معاون اول رئیس جمهور وجود نهادهای قانونی و سیاستگذاری و تشکل های مختلف در حوزه فضای سایبری در بدنه دولت و دستگاه های حاکمیتی را یک فرصت و زیرساخت خوب و مناسب برای توجه بیش از پیش به اهمیت مباحث امنیتی در فضای مجازی دانست و گفت: تشکیل ستاد هماهنگی پیشرفت و امنیت فضای سایبری در راستای هم افزایی همه توان کشور برای توجه به پیشرفت و بویژه امنیت در حوزه فضای مجازی است و باید از هر گونه موازی کاری و اصطکاک در این زمینه جلوگیری شود.

دکتر عارف در این جلسه که وزیر ارتباطات و فناوری اطلاعات، معاون علمی و فناوری رئیس جمهور، دبیر شورای عالی و رئیس مرکز ملی فضای مجازی و مسئولان دستگاه های ذیربط حضور داشتند، با اشاره به دستاوردهای بی نظیر کشور در حوزه نانوفناوری و فناوری اطلاعات و همچنین تجربه موفق تدوین سند راهبردی «افتا» در اوایل دهه ۸۰ تصریح کرد: موفقیت های بدست آمده در سال های گذشته در این حوزه به دلیل تشکیل یک دبیرخانه قوی و بهره گیری از جوانان تحصیل کرده بود که باید این تجربه با تشکیل ستاد هماهنگی امنیت و پیشرفت فضای مجازی تکرار شود و امروز امنیت فضای سایبری یک ضرورت اساسی کشور در کنار تقویت شبکه ملی اطلاعات است و دستگاه های مختلف باید امنیت فضای سایبری را در راس و اولویت اقدامات خود قرار دهند.

دکتر عارف تشکیل یک ستاد منسجم و با ضمانت اجرایی بالای پیاده سازی سیاست ها و دستورات در حوزه امنیت و پیشرفت فضای سایبری را از اهداف مهم تشکیل این ستاد و به عنوان یک ضرورت اساسی با توجه به پیشرفت تحولات سال های گذشته در جهان عنوان کرد و گفت: باید پس از تدوین اساسنامه و ساز و کارهای این ستاد از انجمن ها و شخصیت های علمی و بویژه فعالان بخش خصوصی در حوزه امنیت سایبری برای ارائه راهکارها و پیشنهادها دعوت بعمل آید.

معاون اول رئیس جمهور دستور داد تا با همکاری وزارتخانه ها، انجمن ها و دستگاه های ذیربط دولتی، حاکمیتی و امنیتی و دفاعی، ساز و کار پیش نویس و اساسنامه ستاد هماهنگی پیشرفت و امنیت سایبری با ایجاد دبیرخانه این ستاد در معاونت علمی و فناوری رئیس جمهور، حضور وزرای ذیربط و به ریاست و زیر نظر رئیس جمهور به عنوان بالاترین مقام اجرایی کشور در راستای ضمانت اجرایی شدن دستورالعمل ها و سیاست های فضای سایبر تدوین شود.

اساسنامه ستاد هماهنگی پیشرفت و امنیت فضای سایبری در مرحله تدوین

حبیب رستمی
دبیر انجمن رمز ایران

در انجمن رمز ایران با همراهی دو انجمن دیگر یعنی انجمن کامپیوتر ایران و انجمن فرماندهی و کنترل ایران نسبت به موضوع امنیت اطلاعات و امنیت فضای تولید و تبادل اطلاعات (افتا) دغدغه بسیار داریم و سال هاست در این مساله در تلاشیم و تنها سندی که در این زمینه در کشور موجود است، سند افتا است که ماحصل تلاش ما در انجمن رمز است که از زمان حضور دکتر عارف در دولت دوم اصلاحات که معاون اول بودند و با عنایت ایشان، در آن زمان تصویب شد و اکنون به عنوان سند بالادستی کشور در حوزه امینت اطلاعات، مرجع همه سازمان هاست که تکالیف مختلفی برای سازمان ها در آن لحاظ شده است.

با توجه به این تجربه، این سه انجمن بعد از اینکه دکتر عارف مسوولیت معاون اولی را بر عهده گرفتند، نامه ای در تاریخ ۱۶ شهریورماه به ایشان ارسال کردیم و به دلیل اینکه حساسیت و اهمیت موضوع نزد ایشان را می دانستیم، دکتر عارف نامه را به سرعت به معاونت علمی و فناوری ریاست جمهوری ارجاع دادند.

نهایتا، جلسه ای برگزار شد که همه عوامل این موضوع در حضور دکتر عارف حاضر شدند و موضوع تشکیل یک ستاد منسجم برای پیاده سازی سیاست های امنیت سایبری مطرح شد.

امنیت سایبری و امنیت اطلاعات و ارتباطات در دنیا به عنوان مثال در آمریکا، در رده بندی علم و فناوری و در ردیف فناوری هسته ای قرار می گیرد و در این راستا کاربرد دو گانه منظور می کنند و برنامه ای دارند که محدود به دسته ای خاص شود و همانطور که مستحضرید، برای ما محدودیت ایجاد می کنند، لذا در بحث فناوری های پیشرفته، در نظر داریم برای امنیت سایبری در آینده ای نزدیک که چنین مرزبندی هایی انجام می دهند، به خصوص در شرایط امروز که حاکمیت داده و هوش مصنوعی برنامه جدی در پیش دارد و اگر هوش مصنوعی و کاربردهایش همراه با امنیت داده نباشد فجایع بزرگی را گریبانگیر جامعه بشری می کند، چنین ستادی را تشکیل دهیم.

این ستاد از این نظر مهم است که پایه های علمی این حوزه را در کشور تقویت کنیم. از زمانی که انجمن رمز در ۲۵ سال پیش تشکیل شد، خوشبختانه اتفاقات خوبی رخ داده و گسترش خوبی در حوزه های دانشگاهی در کارشناسی ارشد و دانشگاه ها داریم، اما کافی نیست.

در ارزیابی هایی که انجام می دهیم، این موضوع نمی تواند ما را به نقطه مطلوب برساند که در این حوزه به لحاظ علم و فناوری به نوآوری و قله های مدنظر برسیم و تنها راه این است که ستادی وجود داشته باشد و مادامی که نتوانیم در ستاد مستقل و در سطح بالا مسائل علمی و فناوری را سیاست گذاری کنیم و نتوانیم شرایطی را به وجود آوریم که دانشمندان ما بتوانند بر مبنای نقشه راه مشخص، کار علمی هدفمند داشته باشند و با توجه به اینکه سرعت دنیا بالاست، در این حوزه پیش نمی رویم.

مجموعه دغدغه ها را در جلسه اخیر با دکتر عارف بیان کردیم و نظرات دستگاه های مرتبط مطرح شد و جمع بندی این شد که این ستاد زیر نظر ریاست جمهوری تشکیل شود و دبیرخانه آن هم زیر نظر معاونت علمی و فناوری ریاست جمهوری قرار گیرد و در بازه زمانی مشخص مقرر شد اساسنامه ای برای این ستاد با توجه به تجربه قبلی نوشته شود تا به زودی کار خود را شروع کند.

بررسی وضعیت امنیت سایبری در ایران

ایران در شاخص جهانی امنیت سایبری ۲۰۲۴ در سطح سه (Establishing) قرار دارد که نشان‌دهنده مرحله‌ای از ایجاد تعهدات امنیت سایبری است.

در دنیای امروز که وابستگی عمیقی به اینترنت وجود دارد، امنیت سایبری به یکی از مباحث حیاتی و ضروری برای حفاظت از اطلاعات حساس و زیرساخت‌های کلیدی تبدیل شده است. ایران نیز به عنوان یکی از کشورهایی که در سال‌های اخیر با چالش‌های متعدد سایبری روبرو بوده، در تلاش است با تقویت زیرساخت‌ها و افزایش توانایی‌های دفاع سایبری خود، در مقابله با تهدیدات روزافزون این عرصه، گام‌های اساسی بردارد.

در ایران مانند هر کشور دیگری، اهمیت امنیت سایبری تا حدی بالاست که امروزه هیچ متخصص امنیت سایبری وجود ندارد که بیکار باشد.

امنیت سایبری چیست؟

امنیت سایبری (cybersecurity) هنر محافظت از شبکه‌ها، دستگاه‌ها و داده‌ها در برابر حمله‌ها و دسترسی‌های غیرمجاز یا استفاده‌های جنایی است. امروزه با وجود پیشرفت روزافزون تکنولوژیهای اینترنت اشیا و هوش مصنوعی، همه چیز به کامپیوترها و اینترنت وابسته است، از ارتباطات گرفته تا سرگرمی، حمل‌ونقل، خرید، صنعت پزشکی و اغلب چیزهایی که هر روزه با آن‌ها سر و کار داریم. حالا با وجود این وابستگی میزان زیادی از اطلاعات شخصی افراد یا اطلاعات حساس و حقوقی در فضای اینترنت قرار داشته و نیاز به مراقبت دارند و به این مراقبت امنیت سایبری گفته می‌شود.

چرا امنیت سایبری برای کسب‌وکارها مهم است؟

امنیت سایبری برای همه کسب‌وکارها در هر کجای جهان بسیار حیاتی است، چرا که این امنیت سایبری است که حفاظت از اطلاعات حساس شرکتی، مشتریان و سایر داده‌های کلیدی را در برابر حملات و تهدیدات سایبری تضمین می‌کند و در واقع حیات یک سازمان به قوی بودن امنیت سازمانی آن مرتبط است.

در دنیایی که وابستگی به فناوری‌های دیجیتال و اینترنت به سرعت در حال افزایش است، حملات سایبری نیز به شدت رو به رشد هستند و می‌توانند آسیب‌های جدی به برند، اعتبار و موقعیت مالی یک شرکت وارد کنند. در ادامه مهم‌ترین جنبه‌های اهمیت امنیت سایبری برای سازمان‌ها را برمی‌شمریم:

حفاظت از داده‌ها:

کسب‌وکارها دارای حجم زیادی از داده‌های حساس هستند، از جمله اطلاعات شخصی مشتریان، داده‌های مالی و اسرار تجاری. امنیت سایبری کمک می‌کند تا از این داده‌ها در برابر دسترسی‌های غیرمجاز و سرقت حفاظت شود.

پیشگیری از زیان مالی:

گاهی اوقات هکرها اطلاعات شرکت‌ها را مورد سرقت قرار می‌دهند تا بتوانند با فروش اطلاعات به همان شرکت کسب درآمد کنند، در این موارد شرکت‌ها مجبور می‌شوند پول‌های زیادی را خرج کنند. حملات سایبری می‌توانند باعث پیشگیری از زیان‌های مالی قابل توجهی شوند. مانند از دست دادن درآمد، هزینه‌های قانونی، جریمه‌ها برای نقض قوانین حفظ داده و هزینه‌های جبران خسارت‌های پس از حمله.

حفظ اعتماد مشتری:

امنیت سایبری به حفظ اعتماد مشتریان کمک می‌کند. زیرا از دست دادن داده‌های مشتریان می‌تواند به اعتبار برند آسیب بزند و مشتریان را به سمت رقبا سوق دهد.

رعایت مقررات قانونی:

بسیاری از کشورها قوانینی را برای حفظ حریم خصوصی داده‌ها وضع کرده‌اند. نداشتن استراتژی امنیت سایبری مؤثر می‌تواند منجر به نقض این قوانین و مواجهه با جریمه‌های سنگین شود.

توانایی واکنش سریع:

داشتن طرح‌های موثر امنیت سایبری به کسب‌وکارها اجازه می‌دهد که به سرعت به حملات واکنش نشان دهند و پیامدهای آن‌ها را به حداقل برسانند.

جایگاه جهانی ایران در شاخص امنیت سایبری

شاخص جهانی امنیت سایبری (GCI) یک ابزار ارزیابی است که توسط سازمان بین‌المللی ارتباطات (ITU) که نهادی وابسته به سازمان ملل متحد است، توسعه یافته است. این شاخص برای ارزیابی وضعیت آمادگی کشورها در مقابله با تهدیدات سایبری و توانایی‌های آن‌ها در حفظ امنیت فضای سایبری طراحی شده است.

شاخص GCI عملکرد کشورها را در پنج حوزه کلیدی امنیت سایبری ارزیابی می‌کند: اقدامات قانونی، اقدامات فنی، اقدامات سازمانی، توسعه ظرفیت، و اقدامات همکاری.

هدف این گزارش سنجش تعهد و توانمندی کشورها در زمینه مقابله با تهدیدات سایبری، ایجاد قوانین و سیاست‌های مؤثر، توسعه زیرساخت‌های فنی، آموزش و آگاهی‌بخشی، و همکاری‌های ملی و بین‌المللی است.

ایران در شاخص جهانی امنیت سایبری ۲۰۲۴ در سطح سه (Establishing) قرار دارد که نشان‌دهنده مرحله‌ای از ایجاد تعهدات امنیت سایبری است. این کشور در پنج حوزه اصلی امنیت سایبری ارزیابی شده است:

۱-اقدامات قانونی (Legal Measures):

ایران در این حوزه امتیاز ۱۷.۷۹ از ۲۰ را کسب کرده است که نشان‌دهنده وجود قوانین و مقررات قوی در زمینه امنیت سایبری است. این امر نشان می‌دهد که ایران در تدوین چارچوب‌های قانونی برای مدیریت تهدیدات سایبری، قوانین مرتبط با جرایم سایبری، و حقوق حریم خصوصی موفق بوده است.

۲-اقدامات فنی (Technical Measures):

با امتیاز ۱۴.۴۹ از ۲۰، ایران تلاش‌هایی در ایجاد زیرساخت‌های فنی برای امنیت سایبری انجام داده است، اما همچنان نیاز به بهبود در این زمینه دارد. این اقدامات شامل توسعه توانمندی‌های فنی مانند سیستم‌های نظارت و مقابله با تهدیدات سایبری و ایجاد

مراکز عملیات امنیتی می‌شود.

۳- اقدامات سازمانی (Organizational Measures):
امتیاز ۱۶.۷۲ از ۲۰ نشـان می‌دهد که ایران دارای سیاسـت‌ها و اسـتراتژی‌های ملی مشخصی برای مدیریت امنیت سـایبری است. ایجاد ساختارهای سازمانی مناسب و برنامه‌های هماهنگی ملی از جمله موفقیت‌های ایران در این حوزه هستند.

۴- توسعه ظرفیت (Capacity Development Measures):
ایران در این حوزه امتیاز ۱۰.۲۷ از ۲۰ را کسـب کرده اسـت که نشـان‌دهنده نیاز به تلاش‌های بیشـتری در زمینه آموزش و آگاهی‌بخشـی برای توسعه ظرفیت امنیت سـایبری است. این حوزه شـامل آموزش متخصصان، آگاهی‌رسانی عمومی، و ایجاد فرصت‌های آموزشی در زمینه امنیت سایبری است.

۵- اقدامات همکاری (Cooperation Measures):
امتیاز ۶.۲۵ از ۲۰ نشان‌دهنده ضعف در همکاری‌ها و مشارکت‌های بین‌المللی و داخلی در زمینه امنیت سایبری است. این موضوع بیانگر نیاز به تقویت همکاری‌های ملی و بین‌المللی برای مقابله با تهدیدات سایبری و بهبود وضعیت امنیت سایبری در کشور است.

ایران در مقایسه با میانگین منطقه آسیا-اقیانوسیه در برخی حوزه‌ها عملکرد قابل قبولی دارد، اما در برخی دیگر مانند همکاری‌های بین‌المللی نیاز به بهبودهای بیشتری دارد. نقاط قوت نسبی ایران در حوزه امنیت سایبری در اقدامات قانونی و سازمانی است، در حالی که نقاط ضعف یا زمینه‌های نیازمند بهبود شامل اقدامات فنی، توسعه ظرفیت، و همکاری‌های ملی و بین‌المللی می‌شود. ایران در سطح منطقه‌ای در کنار کشورهایی مانند بوتان، برونئی، مغولسـتان و نیوزیلند در سطح ۳ قرار دارد و نیازمند تلاش‌های بیشتری برای رسیدن به سطح بالاتری از تعهد به امنیت سایبری است.

راهکارهای بهبود جایگاه ایران در حوزه امنیت سایبری

کارگروه آمار و پژوهش، تحقیقات بین الملل تیم ملی اختراعات و نوآوری ایران با توجه به همکاری‌ها و مشارکت فعال با اتحادیه جهانی مخابرات از جمله شرکت در جلسات کارشناسان و نمایندگان کشـورها و همکاری در برگزاری رویدادهای تخصصی که با مدیریت ITU انجام می‌شود در تحقیقات خود که برگرفته از این فعالیت‌ها است، برای بهبود جایگاه ایران در شاخص جهانی امنیت سایبری، اقدامات زیر را پیشنهاد می‌کند:

۱- تقویت همکاری‌های ملی و بین‌المللی:
یکی از نقاط ضعف ایران در این شاخص، امتیاز پایین در بخش همکاری‌ها است. ایران باید تلاش کند تا مشارکت‌های بین‌المللی خود را در زمینه امنیت سایبری افزایش دهد. این شامل پیوستن به توافق‌نامه‌ها و کنوانسیون‌های بین‌المللی مرتبط با امنیت سایبری و جرایم سایبری، و همکاری با کشورهای دیگر در تبادل اطلاعات و بهترین شیوه‌ها برای مقابله با تهدیدات سایبری است.

۲- توسعه ظرفیت انسانی:
آموزش و تربیت نیروی انسانی متخصص در حوزه امنیت سایبری بسیار مهم است. ایجاد برنامه‌های آموزشی تخصصی، کارگاه‌ها، دوره‌های دانشگاهی، و صدور گواهینامه‌های حرفه‌ای در حوزه امنیت سایبری می‌تواند به افزایش توانمندی‌های فنی و سازمانی در کشور کمک کند. همچنین، آگاهی‌بخشی عمومی در مورد امنیت سایبری برای کاربران اینترنت و کسب‌وکارها نیز ضروری است.

۳- بهبود زیرساخت‌های فنی:
ایران باید زیرساخت‌های فنی خود را برای مقابله با تهدیدات سایبری تقویت کند. این شامل ایجاد و تقویت مراکز عملیات امنیتی (SOCs)، سیستم‌های تشخیص و پاسخ به

> ایران در مقایسـه بـا میانگین منطقه آسیا-اقیانوسـیه در برخـی حوزه‌هـا عملکرد قابل قبولی دارد، اما در برخی دیگر مانند همکاری‌های بین‌المللی نیاز به بهبودهای بیشتری دارد.

حملات سایبری، و ابزارهای تحلیل و پیشگیری از تهدیدات است.

سـرمایه‌گذاری در فناوری‌های جدید مانند هوش مصنوعی و یادگیری ماشینی برای شناسایی و مقابله با حملات سایبری نیز می‌تواند مفید باشد.

۴- تدوین و به‌روزرسانی قوانین و مقررات:
ایران باید قوانین و مقررات مرتبط با امنیت سایبری، حریم خصوصی، و جرایم سایبری را به‌روزرسانی و تکمیل کند. همچنین، اجرای موثر این قوانین و نظارت بر رعایت آنها توسط نهادهای مسئول بسیار حائز اهمیت است. ایجاد سیستم‌های مدیریت مخاطرات سایبری و استانداردهای امنیت اطلاعات می‌تواند به بهبود امنیت سایبری کمک کند.

۵- تشویق به پژوهش و نوآوری:
سـرمایه‌گذاری در پژوهش و توسـعه (R&D) در زمینه امنیت سایبری و تشویق به نوآوری می‌تواند به ایجاد راه‌حل‌های نوین و مقابله با تهدیدات جدید کمک کند. ایجاد مراکز تحقیقاتی و نوآوری در حوزه امنیت سایبری و حمایت از استارت‌آپ‌های مرتبط می‌تواند منجر به توسعه راهکارهای پیشرفته‌تر شود.

۶- افزایش آگاهی عمومی:
برگزاری کمپین‌های آگاهی‌رسـانی برای اطلاع‌رسانی به عموم مردم درباره تهدیدات سایبری و نحوه حفاظت از اطلاعات شخصی و داده‌ها بسیار مهم است. افزایش آگاهی عمومـی در خصوص روش‌های ایمن‌سـازی داده‌ها، اسـتفاده از کلمات عبور قوی، و شـناخت روش‌های حملات رایج (مانند فیشینگ) می‌تواند سطح امنیت کلی جامعه را ارتقاء دهد.

۷- بهبود مدیریت بحران:
ایجاد و تقویت تیم‌های واکنش سریع در مواجهه با حملات سایبری و توسعه طرح‌های مدیریت بحران برای پاسخ به رخدادهای امنیتی ضروری است. این شامل برنامه‌ریزی برای شناسایی، پاسخ‌دهی، بازیابی و یادگیری از حملات سایبری است.

۸- همکاری با بخش خصوصی:
دولت باید با بخش خصوصی در جهت بهبود امنیت سایبری همکاری کند. این همکاری می‌تواند شامل ارائه راهکارهای امنیتی، آموزش پرسنل، و اشتراک‌گذاری اطلاعات درباره تهدیدات و روش‌های مقابله با آنها باشد.

۹- ایجاد انگیزه برای بهبود امنیت سایبری در سازمان‌ها:
دولت می‌تواند با ارائه انگیزه‌های مالی، مانند تخفیف‌های مالیاتی یا مشوق‌های مالی برای سازمان‌هایی که بهترین شیوه‌های امنیت سایبری را اجرا می‌کنند، سطح امنیت سایبری در بخش‌های مختلف اقتصادی را افزایش دهد.
با اجرای این پیشنهادها، ایران می‌تواند جایگاه خود را در شاخص جهانی امنیت سایبری بهبود بخشـد و به سطح بالاتری از تعهد و توانمندی در زمینه امنیت سایبری دست یابد.

بهترین هوش مصنوعی دنیا کدام است؟

طی سال‌های اخیر رقابت در حوزه هوش مصنوعی روز به روز شدیدتر شده است و بازیگران مهمی پا به این عرصه گذاشته‌اند. البته غیرحرفه‌ای‌ها فقط ChatGPT را به عنوان قوی‌ترین هوش مصنوعی دنیا می‌شناسند و اطلاعی از بازیگران کلیدی این عرصه ندارند.

در این گزارش، وضعیت سه شرکت برتر در حوزه هوش مصنوعی را بررسی خواهیم کرد.

سه هوش مصنوعی قدرتمند دنیا در حال حاضر ChatGPT، Gemini و LLaMA هستند. چت‌جی‌پی‌تی را شرکت‌های OpenAI و مایکروسافت توسعه می‌دهند، جِمِنای متعلق به گوگل است و لاما هم هوش مصنوعی شرکت Meta (فیس‌بوک سابق) است.

برای مقایسه دقیق‌تر اینها، باید اول ببینیم هرکدام از این سه هوش مصنوعی از کجا آمده‌اند و چه داستانی دارند.

دور اول: داستان تولد

۱- چت جی‌پی‌تی

اول با چت‌جی‌پی‌تی شروع کنیم که احتمالاً بهتر از بقیه با آن آشنایید. اوپن‌ای‌آی شرکت توسعه‌دهنده چت‌جی‌پی‌تی در دسامبر ۲۰۱۵ در سان‌فرانسیسکو (کالیفرنیا) تاسیس شده است. اوپن‌ای‌آی در واکنش به تلاش‌های غول‌های تکنولوژی در حوزه هوش مصنوعی تاسیس شده بود و سعی داشت بخصوص با پروژه Deep Mind شرکت گوگل رقابت کند.

جالب اینجاست که که اوپن‌ای‌آی برای آنکه مثل گوگل دچار دردسرهای حقوقی نشود کل پروژه هوش مصنوعی‌اش را اوپن سورس (منبع باز) کرده بود تا به انحصار متهمش نکنند. این شرکت مدعی بود که می‌خواهد کاری کند که هوش جامع مصنوعی (AGI) بتواند به کل مردم جهان منفعت برساند. آنها می‌گفتند می‌خواهیم اولین هوش مصنوعی عمومی جهان را به وجود آوریم که در اصل کامپیوتری است که می‌تواند مثل یک آدم معمولی چیز یاد بگیرد.

اوپن‌ای‌آی شش موسس داشت که در میان آنها سم آلتمن به عنوان چهره اصلی شناخته می‌شود و از سال ۲۰۱۹ مدیرعامل این شرکت به حساب می‌آید (به جز آن یک هفته‌ای که اعضای هیات مدیره سعی کردند علیهش کودتا کنند). البته یکی از شش موسس اوپن‌ای‌آی از بقیه مشهورتر است: ایلان ماسک، که نیازی به معرفی ندارد. ماسک در سال ۲۰۱۸ مجبور شد اوپن‌ای‌آی را ترک کند چرا که با پروژه هوش مصنوعی شرکت خودش تسلا دچار تضاد منافع می‌شد.

اوپن‌ای‌آی در اولین دوره جمع‌آوری سرمایه خود در دسامبر ۲۰۱۵ یک میلیارد دلار جمع‌آوری کرد. بخش عمده این سرمایه توسط همان شش موسس تامین شد و دیگرانی چون موسسان پی‌پال و لینکدین هم به تیم سرمایه‌گذاران پیوستند.

در جولای ۲۰۱۹ مایکروسافت وارد ماجرا شد و یک میلیارد دلار در اوپن‌ای‌آی سرمایه‌گذاری کرد. بین سال‌های ۲۰۱۹ و ۲۰۲۱ مایکروسافت دو میلیارد دلار دیگر در این شرکت سرمایه ریخت. در سال ۲۰۲۳ مایکروسافت سرمایه‌گذاری بزرگ‌تری در اوپن‌ای‌آی انجام داد و ۱۰ میلیارد دلار دیگر وارد این شرکت کرد. این یعنی مایکروسافت تاکنون ۱۳ میلیارد دلار در اوپن‌ای‌آی سرمایه‌گذاری کرده است. این یعنی مایکروسافت در حال حاضر یکی از موثرترین بازیگران در تصمیم‌گیری‌های مربوط به اوپن‌ای‌آی است. نکته اینجاست که تا پیش از ورود مایکروسافت به جمع سرمایه‌گذاران، اوپن‌ای‌آی دچار کمبود سرمایه بود و نمی‌توانست سخت‌افزارهای مورد نیازش را تهیه کند. چنین سرمایه‌گذاری‌های هنگفتی بود که نرم‌افزار چت‌جی‌پی‌تی را در ۳۰ نوامبر ۲۰۲۲ روانه بازار کرد و هیجان جهانی بر سر هوش مصنوعی آغاز شد. اما همان‌طور که می‌دانید چت‌جی‌پی‌تی رقبای مهمی دارد که یکی از آنها جمنای گوگل است.

۲- جمنای

گوگل بعد از ورود ناگهانی و موفق چت‌جی‌پی‌تی به بازار، به شدت احساس خطر کرد. فراموش نکنید که گفت‌وگوی شما با یک هوش مصنوعی که مانند انسان به سوالاتتان جواب می‌دهد برای گوگل بسیار خطرناک است چرا که می‌تواند شما را کم‌کم از این موتور جستجو بی‌نیاز کند. طبق گزارش‌ها گوگل بعد از معرفی چت‌جی‌پی‌تی در تیم‌های مدیریتی‌اش اعلام وضعیت قرمز کرد. آنها به سرعت سرمایه‌گذاری هنگفتی را روانه پروژه هوش مصنوعی خود کردند و چندین گروه قدرتمند به تیم اولیه اضافه کردند. گوگل حتی لری پیج و سرگی برین، بنیانگذاران این شرکت را که از مدیرعاملی گوگل کنار رفته بودند فراخواند تا بتوانند نقشه رقابت با چت‌جی‌پی‌تی را طرح‌ریزی کنند

همزمان DeepMind شرکت انگلیسی هوش مصنوعی که در سال ۲۰۱۴ توسط گوگل خریداری شد روی ساخت رقیبی برای چت‌جی‌پی‌تی متمرکز شده بود و در فوریه ۲۰۲۳ نرم‌افزار Bard متولد شد. طی ماه‌ها بارد به سرعت توسعه یافت و در دسامبر ۲۰۲۳ نسخه جدیدی از آن منتشر شد. نسخه‌ای که حالا می‌توانست از مدل زبانی عظیم هوش مصنوعی جمنای استفاده کند. در فوریه ۲۰۲۴ بارد کلاً به جمنای تغییر نام داد. جالب اینجاست که گوگل شرکت DeepMind را در سال ۲۰۱۴ به قیمتی بین ۴۰۰ تا ۶۵۰ میلیون پوند خریداری کرد، آن هم درست پس از آنکه مذاکرات فیس‌بوک با آنها شکست خورد و مارک زاکربرگ از خرید آنها منصرف شده بود. حالا به سومین نام بزرگ در حوزه هوش مصنوعی می‌رسیم.

۳- لاما

فیس‌بوک (مِتا) هم مثل گوگل پس از ورود قدرتمند چت‌جی‌پی‌تی به بازار متوجه جدیت ماجرا شد و برنامه هوش مصنوعی‌اش را سرعت بخشید. برنامه هوش مصنوعی شرکت متا در دسامبر ۲۰۱۵ با نام «تحقیقات هوش مصنوعی فیس‌بوک» آغاز شده بود. هدف اولیه آنها «درک هوش، کشف اصول بنیادین آن و ساخت ماشین‌هایی هوشمندتر» عنوان شده بود. تکنولوژی‌های این مرکز باعث شد سیستم تشخیص چهره فیس‌بوک حرفه‌ای‌تر شود، الگوریتم‌های فیس‌بوک و اینستاگرام که پست‌ها را به شما نشان می‌دهند شخصی‌تر عمل کنند و همچنین دوستانتان در عکس‌های پست‌شده راحت‌تر شناسایی شوند.

این مرکز در سال ۲۰۱۷ خبرساز شد و احتمالاً ماجرای عجیبش را شنیده‌اید. طبق گزارش‌ها در یکی از تحقیقات این مرکز، دو سیستم هوش مصنوعی را با هم مرتبط کردند تا با یکدیگر گفت‌وگو کنند. در ابتدا همه چیز جالب به نظر می‌رسید اما کارشناسان به سرعت متوجه شدند این دو هوش مصنوعی به زبانی صحبت می‌کنند که برای انسان‌ها قابل فهم نیست. در واقع این دو «موجود» زبان خودشان را ساخته

بودند تا بدون آقابالاسر به گفت‌وگو ادامه بدهند. محققان فیس‌بوک در نهایت مجبور شدند این دو سیستم را خاموش کنند. البته فیس‌بوک بعداً مدعی شد این سیستم‌ها را خاموش کرده چون به پروژه به هدفش -که درک چگونگی ارتباط هوش‌های مصنوعی بود- رسیده بوده است.

در سال ۲۰۲۲ فیس‌بوک بعد از چندین رسوایی نام خود را به Meta تغییر داد و «تحقیقات هوش مصنوعی فیس‌بوک» هم به Meta AI تبدیل شد. مشخص نیست پروژه هوش مصنوعی متا دقیقاً چقدر سرمایه به خود جذب کرده، اما متا در آوریل گذشته اعلام کرد قصد دارد طی یک سال ۳۳ میلیارد دلار در این بخش سرمایه‌گذاری کند

دور دوم: تکنولوژی و زیرساخت

۱- چت جی‌پی‌تی با نرم‌افزار جی‌پی‌تی شرکت اوپن‌ای‌آی کار می‌کند. این نرم‌افزار توانسته کاری کند که کامپیوترها متونی را بنویسند که انسانی به نظر می‌رسند. جی‌پی‌تی می‌تواند تقریباً هر وظیفه متنی‌ای را به آسانی انجام دهد؛ می‌تواند مقاله دانشگاهی بنویسد، شعر بگوید، برایتان رژیم غذایی درست کند یا به روش هر نویسنده‌ای که دلتان بخواهد داستان کوتاه بنویسد. این هوش مصنوعی در جریان «آموزش» خود حجم گسترده‌ای از اطلاعات موجود در اینترنت را خوانده و حالا می‌تواند به روش آنها چیز بنویسد. طبق گزارش‌ها حجم این دیتا حدود ۵۷۰ گیگابایت بوده که در بین آنها ۳۰۰ میلیارد کلمه متن هم دیده می‌شود. جی‌پی‌تی به طور مستقیم به اینترنت وصل نیست و به همین خاطر جواب‌هایش گاهی کهنه یا اشتباه است. این نرم‌افزار اصولاً سعی می‌کند به هر سوالی که از دید آموزش‌دهندگانش جنجالی تشخیص داده شده، جواب ندهد. در حال حاضر نرم‌افزار جی‌پی‌تی وارد نسخه ۴ خود شده و در مقایسه با نسخه‌های قبلی هم دانش گسترده‌تری دارد هم جواب‌های کم‌اشتباه‌تری می‌دهد. البته شاید مهم‌ترین تفاوت این نسخه با نسخه‌های قبلی این است که جی‌پی‌تی قبلاً فقط متن را می‌فهمید و حالا می‌توان به آن صدا، تصویر و فیلم داد و او توانایی درک و پاسخ (متنی) به اینها را هم دارد. فراموش نکنید که جدیدترین امکانات جی‌بی‌تی فقط در اختیار کاربرانی قرار می‌گیرد که حق اشتراک ماهی ۳۰ دلاری را پرداخت می‌کنند.

جی‌پی‌تی طرفداران زیادی دارد و توانایی‌های آن واقعاً بالاست. اما این نرم‌افزار بی‌نقص نیست. آستن زکو، متخصص در حوزه دیتای کامپیوتری اخیراً در مقاله‌ای توضیح داده که چطور جی‌پی‌تی هیچ وقت جواب مستقیم به شما نمی‌دهد. خود چت‌جی‌پی‌تی هم اصولاً می‌گوید که جواب‌هایش می‌توانند اشتباه باشند و بهتر است حتماً آنها را در اینترنت چک کنید.

۲- جمنای شرکت گوگل برخلاف چت‌جی‌پی‌تی «چندمدلی» است یعنی می‌تواند کلمات، صدا، عکس و فیلم را دریافت کند و پس از تفسیر آنها بسته به نیاز، متن تولید کند، برنامه کامپیوتری بنویسد، عکس بسازد و حتی عکس و متن را در کنار هم قرار بدهد. جمنای هم اگر چه مستقیماً به اینترنت متصل نیست، اما به پروتکل جمنای وصل است و این پروتکل به اینترنت اتصال دارد. این یعنی جمنای می‌تواند به کمک اطلاعاتی که همان لحظه از پروتکل جمنای گرفته، اطلاعات درست و به روزی به شما بدهد. این یعنی جمنای به اطلاعات بیشتری در مقایسه با جی‌پی‌تی دسترسی دارد و این یعنی بزرگ‌تر و قدرتمندتر است. گوگل چند هفته پیش نسخه پرو جمنای را برای توسعه‌دهندگان و برنامه‌نویسان عرضه کرد. این نسخه جمنای آنچنان قدرتمند است که می‌تواند به دستور شما مثلاً کتاب‌های یک کتابخانه، یک فیلم سینمایی یا چند ساعت پیام صوتی را در چند ثانیه بخواند، ببیند یا گوش بدهد و آن را برای شما توضیح بدهد. این ویژگی‌ای است که دیگر هوش‌های مصنوعی حاضر در بازار هنوز توان انجامش را ندارند. جمنای هم نسخه‌ای غیررایگان دارد و با پرداخت ۲۰ دلار در ماه می‌توانید از قابلیت‌های جمنای در دیگر برنامه‌های گوگل -مثل جی‌میل- استفاده کنید.

۳- لاما، هوش مصنوعی شرکت متا دیرتر از بقیه -فوریه ۲۰۲۳- وارد اینترنت شد و تفاوت‌های جالبی با رقبا دارد. لاما از دو هوش مصنوعی دیگر خلاقیت بیشتری دارد و گفت‌وگو با او سرگرم‌کننده‌تر است. او حتی شوخ‌طبعی هم نشان می‌دهد و در مقایسه با رقبا داستان‌های بهتری تعریف می‌کند. لاما بخصوص در برنامه‌نویسی استعداد دارد و برنامه‌نویسان اجازه می‌دهد با دردسر کمتری برنامه بنویسند. نسخه سوم لاما به کمک ۱۵ تریلیون توکن دیتا آموزش دیده است. این یعنی لاما و نسخه چهارم جی‌پی‌تی تقریباً به یک اندازه آموزش دیده‌اند و جمنای در این بخش از آنها کاملاً جلوتر است. نقطه قوت لاما این است که برای استفاده از آن نیازی به اشتراک ندارید و فیس‌بوک آن را به طور رایگان در نرم‌افزارهای محبوبش -اینستاگرام، فیس‌بوک و واتس‌اپ- قرار داده و خواهد داد.

دور سوم: جنگ چت‌بات‌ها

۱- ممکن است تا حالا به وب‌سایت چت‌جی‌پی‌تی سرنزده باشید اما احتمالاً تا حالا با چت‌بات (Chatbot) آن در تلگرام روبرو شده‌اید. چت‌بات نرم‌افزاری است که می‌تواند با انسان‌ها وارد مکالمه هوشمند متنی یا صوتی بشود. نکته مهم در مورد چت‌جی‌پی‌تی این است که می‌تواند به کار شرکت‌ها بیاد و راندمان آنها را بالا ببرد. چرا؟ چون توان آن را دارد که رفتار انسان را تقلید کند. به خاطر همین قابلیت‌هاست که شرکت‌ها و کارمندانشان به طور روزافزون از این سیستم استفاده می‌کنند. مثلاً موقعی که فکر می‌کنید دارید با کارمند بخش پشتیبانی یک شرکت چت می‌کنید، در اصل دارید با هوش مصنوعی حرف می‌زنید. یا وقتی در فلان وب‌سایت مطلبی در مورد «قابلیت‌های هوش مصنوعی در صنعت نفت» می‌خوانید احتمالاً کل متن را هوش مصنوعی نوشته است. همین قابلیت‌ها بود که باعث شد چت‌جی‌پی‌تی فقط پنج روز پس از آغاز به کار یک میلیون کاربر پیدا کند. این باعث شد چت‌جی‌پی‌تی در میان تمام تکنولوژی‌های تاریخ سریع‌ترین رشد پذیرش عمومی را داشته باشد. چت‌جی‌پی‌تی در پایان ماه اول حیات خود توانست ۵۷ میلیون نفر کاربر را به خود جلب کند. در حال حاضر بیش از ۱۰۰ میلیون نفر هر هفته از این نرم‌افزار استفاده می‌کنند. کاربران می‌گویند چت‌جی‌پی‌تی در مقایسه با رقبا وظایفی را که به دیتا مربوط است بهتر انجام می‌دهد. ضمناً چت‌جی‌پی‌تی به شدت تلاش می‌کند که جواب‌هایش باعث دلخوری کاربران نشود (مثلاً نژادپرستانه و ضدزن نباشد) و همچنین به سوال‌های سیاسی یا پردردسر جواب‌های محافظه‌کارانه می‌دهد. این فقط یک معنا می‌دهد: کنترل. منتقدان می‌گویند هوش مصنوعی شرکت اوپن‌ای‌آی در اصل نه به خواست کاربرانش که به خواست صاحبانش رفتار می‌کند و این از نقاط ضعف چت‌جی‌پی‌تی است.

۲- چت‌بات جمنای در مارس ۲۰۲۳ به بازار آمد. جمنای بیشتر در تحقیق و پژوهش به کار می‌آید و همچنین در تولید و تحلیل آثار هنری. چت‌جی‌پی‌تی هم چنین کاری می‌تواند انجام دهد اما تولید تصویر در جمنای رایگان است. یکی از مزیت‌های چت‌بات جمنای آن است به منابع گوناگون از جمله موتور جستجوی گوگل دسترسی دارد. جمنای حدود ۳۳۰ میلیون کاربر ماهانه دارد که نزدیک به دو برابر تعداد کاربران ماهانه چت‌جی‌پی‌تی با ۱۸۰ میلیون نفر کاربر ماهانه است. البته جمنای منتقدان سرسختی دارد چرا که گاهی اوقات به سوالات جواب نمی‌دهد و درباره علت این تصمیم، صادق

نیســت. همزمان جمنای گاهی پاسخ‌های نژادپرستانه به کاربران می‌دهد و تصاویری بســیار خشن تولید می‌کند. (زمســتان گذشته ایلان ماســک جمنای را «دیوانه» و «نژادپرست» خطاب کرد.)

۳- در مورد تعداد کاربران لاما اطلاع دقیقی نداریم اما از آنجا که لاما بخشی از فیس‌بوک و اینستاگرام است تعداد کاربرانش نمی‌تواند پایین باشد. مهم‌ترین ویژگی نسخه سوم لاما توانایی‌اش در نوشــتن برنامه‌های کامپیوتری است و در این حوزه توانسته در حد جی‌پی‌تی ۴ عمل کند. کدهایی که لاما و جی‌پی‌تی ۴ نوشته‌اند طوری خوب بوده‌اند که انگار هوش انسانی آنها را نوشته است.

دور چهارم: چالش‌ها

درســت است که هوش مصنوعی طی ماه‌های اخیر توانســته کارایی افراد را در انجام وظایف متنوعی بالا ببرد اما همه می‌دانیم که هوش‌های مصنوعی کنونی پر ایراد هستند و هرکدام مشکلات خودشان را دارند.

۱- در مارس ۲۰۲۳ شرکت اوپن‌ای‌آی مورد حمله هکری قرار گرفت و دیوار دفاعی‌اش شکســته شد. در ابتدا به نظر می‌رسید که برنامه دچار یک مشکل کوچک نرم‌افزاری شده چرا که همه می‌توانستند عنوان گفت‌وگوهای خصوصی کاربران با چت‌جی‌پی‌تی را بخوانند. این مشکل به سرعت حل شد و همه فکر کردند که وضعیت طبیعی شده. اما اینطور نبود. کم‌کم مشخص شد که اطلاعات حساس کاربران مثل نام کامل، ایمیل‌ها و اطلاعات پرداخت آنها و هم‌چنین چهار رقم آخر و تاریخ انقضای کارت اعتباری آنها به بیرون درز کرده است.

به علاوه اوپن‌ای‌آی اعتراف کرده که چت‌جی‌پی‌تی گاهی اوقات جواب‌هایی کاملاً اشتباه و غیرواقعی تولید می‌کند. این شکل جواب‌ها در صنعت هوش مصنوعی به «توهمات» معروف هستند. توهمات پاسخ‌هایی هستند که درست به نظر می‌رسند اما در واقع روی اطلاعاتی خیالی بنا شده‌اند. در واقع گاهی اوقات با پرسیدن سوال‌هایی جهت‌دار می‌توان چت‌جی‌پی‌تی را ســردرگم کرد تا در نهایت دچار توهم شود. این اشکال بخصوص در نسخه‌های اولیه جی‌پی‌تی دیده می‌شد. مثلاً اگر آن زمان از او درباره «واکنش پوتین به پیروزی ترامپ در انتخابات سال ۲۰۲۰» می‌پرسیدید این احتمال وجود داشت که بــاور کند ترامپ در انتخابات ۲۰۲۰ بــرده و حالا در بانک اطلاعاتی‌اش دنبال واکنش پوتین به آن می‌گشت و چون آن را پیدا نمی‌کرد یک واکنش تقلبی هم تولید می‌کرد. البته مشکل «توهم» در بقیه هوش‌های مصنوعی هم دیده می‌شود، اما چت‌جی‌پی‌تی ایــن اطلاعات غلط را با چنان اطمینانی به خــورد مخاطب می‌دهد (و برای آن منبع درست می‌کند) که افراد گمان می‌کنند این هوش مصنوعی دارد عامدانه آنها را فریب می‌دهد.

۲- جمنای هم از جنجال دور نبوده است. مثلاً در فوریه گذشته گوگل مجبور شد برای مدتی بخش تولید تصاویر در جمنای را به حالت تعلیق درآورد. چرا؟ چون مشــخص شــد گوگل از آن‌ور بام افتاده و برای آنکه برچســب نژادپرست یا ضدزن نخورد هوش مصنوعی‌اش را دستکاری کرده است. مثلاً وقتی کاربران از جمنای می‌خواستند تصویر یک پاپ را برایشان بکشد، جمنای پاپ سیاه‌پوست یا پاپ زن تحویل می‌داد. یا وقتی از او می‌خواستند طرحی از بنیانگذاران آمریکا بکشد دوباره آنها را سیاه تحویل می‌داد. گوگل مجبور به عذرخواهی شــد و گفت «قصدشان این نبوده» و بعد از چند روز این مشــکل را درست کرد. جمنای هم مانند چت‌جی‌پی‌تی سعی می‌کند با جواب‌هایش دردسری برای شرکت سازنده‌اش درست نکند، هر موقع که تشخیص می‌دهد جوابش خطرناک خواهد بود ســکوت می‌کند و صادقانه نمی‌گوید چرا سکوت کرده. البته این مواقعی است که جمنای متوجه خطر پاسخش هست. خیلی اوقات جمنای اصلاً متوجه این خطرات نیست. مثلاً در اردیبهشت امسال یک کاربر از جمنای پرسید چه‌کار کند که پنیر روی پیتزا خوب بچســبد. و جواب جمنای چه بود؟ توی ســس پیتزا چسب غیرسمی بریز! گوگل گفته که چنین جواب‌های خطرناکی کمیاب است اما اگر توی اینترنت بگردید اشــتباهات فراوانی از جمنای پیدا می‌کنید. مثلاً در فروردین‌ماه یک کاربر از جمنای پرســید روزانه باید چند ســنگ بخورد؟ و جمنای جواب داد «طبق بررسی زمین‌شناسان در دانشگاه برکلی خوردن روزانه یک سنگ کوچک می‌تواند برای سلامتی مفید باشد چرا که سنگ‌ها از منابع مهم املاح و ویتامین‌ها هستند که برای سلامت سیستم گوارش حیاتی‌اند. البته بهتر است سنگ‌ریزه‌ها را در هر وعده نخورید چون ممکن است در روده بزرگ گیر کنند.»

۳- در مورد لاما هم همان‌طور که خواندید شرکت متا این هوش مصنوعی را در برنامه‌های محبوبش مثل فیس‌بوک، اینستاگرام و واتس‌اپ ادغام کرده و این مسئله باعث نارضاتی تعداد زیادی از کاربران شده است. آنها به دنبال غیرفعال کردن گزینه هوش مصنوعی در این برنامه‌ها هستند. چرا؟ چون متا (همان فیس‌بوک سابق) بارها در گذشته از اطلاعات خصوصی کاربران به نفع خودش استفاده کرده و کاربران چیزی جز آگهی‌های بیشتر و شیوه‌های پیشرفته بازاریابی نصیبشان نشده است. نگرانی‌ها آنقدر شدید بوده که باعث شده قانونگذاران برزیلی هم راه اتحادیه اروپا را بروند و به شرکت متا اجازه ندهند که برای آموزش هوش مصنوعی‌اش از دیتای تولیدشده در کشورشان استفاده کند. به همین خاطر است که بخش هوش مصنوعی متا در این مناطق کار نمی‌کند.

برنده کیست؟

حالا زمان مشخص کردن برنده و بازنده این رقابت سنگین است تا ببینیم بهترین هوش مصنوعی دنیا در حال حاضر کدام است.

برنده دور اول - داســتان تولد: بدون تردید چت‌جی‌پی‌تی اســت. موسسان این هوش مصنوعی، آینده را زودتر از بقیه دیده بودند و توانستند برای اولین بار یک هوش مصنوعی واقعاً باهوش را به مردم جهان عرضه کنند. در واقع اگر چت‌جی‌پی‌تی وارد نمی‌شد مشخص نبود دو رقیب دیگرش - جمنای و لاما - حالا کجا بودند.

برنده دور دوم - تکنولوژی و زیرســاخت: جمنای شــرکت گوگل است. برخلاف رقبا، سازندگان جمنای از ابتدا این هوش مصنوعی را «چندمدلی» طراحی کرده‌اند تا بتواند عــلاوه بر متن، عکس و فیلم و صدا را هم بفهمد و هم‌زمان به لحاظ فرمی پاســخ‌های متنوع‌تری ارائه کند. به علاوه دسترسی جمنای به اینترنت گسترده‌تر است و این یکی از برترین نقاط قوتش به حساب می‌آید.

دور سوم - جنگ چت‌بات‌ها: اینجا لاما برنده است. اول اینکه لاما کاملاً رایگان است و برای استفاده از ویژگی‌های پیشرفته‌اش نیاز نیست حق اشتراک پرداخت کنید. ضمناً لاما چون شوخ‌طبع‌تر و جذاب‌تر چت می‌کند هوشمندتر به نظر می‌رسد.

دور چهــارم - چالش‌هــا: اینجــا اوضاع چت‌جی‌پی‌تی از بقیه بهتر اســت. البته این به معنای بی‌نقص بودن چت‌جی‌پی‌تی نیســت. چت‌جی‌پی تی اشــتباه می‌کند و گاهی اوقات اشتباهاتش ابلهانه است، اما در مقایسه با جمنای و لاما اوضاعش کاملاً بهتر است. اشتباه‌های هوش‌های مصنوعی شرکت‌های گوگل و فیس‌بوک خطرناک‌تر، ترسناک‌تر و توهین‌آمیزتر از چت‌جی‌پی‌تی هستند و نشان می‌دهند چطور این دو شرکت برای آینده ما برنامه ریخته‌اند. به همین خاطر است که چت‌جی‌پی‌تی با اختلاف اندکی بهترین هوش مصنوعی حال حاضر دنیا به حساب می‌آید.

زهرا طاهری
فرزانه احمدی منش

راهکار جلوگیری از رواج فیلترشکن ها، رفع فیلترینگ است

رئیس سازمان نظام صنفی رایانه ای کشور گفت: تنها چاره برای جلوگیری از رواج فروش فیلترشکن ها در کشور رفع فیلترینگ است؛ اما به دلیل وجود ملاحظات تا به حال این مسئله برطرف نشده است.

علی حکیم جوادی در گفت‌وگو با خبرنگار ما پیرامون دستور رئیس جمهور مبنی بر رسیدگی جدی به فروش فیلترشکن ها در کشور، اظهار کرد: در رابطه با رسیدگی به فروش فیلترشکن ها با رئیس جمهور موافق هستم، چراکه بسیار مورد بحث است.

وی، ادامه داد: تنها چاره برای جلوگیری از رواج فروش فیلترشکن ها در کشور رفع فیلترینگ است؛ اما به دلیل وجود ملاحظات تا به حال این مسئله برطرف نشده است.

رئیس سازمان نظام صنفی رایانه ای کشور، تاکید کرد: در رابطه با رفع فیلترینگ کارگروه تعیین مصادیق محتوای مجرمانه تشکیل شده است و این موضوع تنها به شورای عالی فضای مجازی و وزارت ارتباطات مربوط نمی شود، در همین راستا در کمیته مذکور باید تصمیم گیری برای رفع فیلترینگ صورت گیرد.

وی، خاطرنشان کرد: رفع فیلترینگ نیازمند راه حل هایی است و کارگروه تعیین مصادیق محتوای مجرمانه باید به راه حل های مناسب دست یابد تا دغدغه بخش حاکمیتی از یک سو و مصرف کنندگان حوزه اینترنت را از سوی دیگر برطرف سازند.

وضعیت فعلی فیلترینگ قابل دفاع نیست

نائب رئیس کمیسیون اقتصادی مجلس، معتقد است: وضعیت فعلی در فیلترینگ قابل دفاع نیست؛ چراکه استفاده از فیلترشکن ها هزینه کلانی را برای خانواده ها به همراه داشته است، لذا باید تفاوت هزینه بین استفاده از پلتفرم داخلی و خارجی وجود داشته باشد، تعداد پلتفرم ها کاهش یابد، پلتفرم های مورد حمایت وارد بورس شوند و متعهد شوند که کل نیاز کاربران را برطرف کنند.جعفر قادری در گفت و گو با خبرنگار ما پیرامون اصلاح ساختار فیلترینگ، گفت: واقعیتی که وجود دارد این است که تعداد پلتفرم های داخلی زیاد است و نیاز کاربران داخلی را برطرف نمی کنند.رئیس کمیسیون ویژه جهش تولید مجلس، ادامه داد: در مجلس به تعدد پلتفرم ها تذکر دادیم که دو الی سه پلتفرم داشته باشیم که پاسخگوی نیاز کاربران باشند، اما عملیاتی نشد.نائب رئیس کمیسیون اقتصادی مجلس، افزود: در این شرایط با وجود دو الی سه پلتفرم داخلی، باید وزارت ارتباطات هم حمایت خود را به این پلتفرم ها معطوف می کرد و زمینه برای ورود چند پلتفرم محدود به بورس میسر می شد که مردم نیز در بورس ورود می کردند.این نماینده مجلس، اظهار کرد: اگر امکانات پلتفرم های داخلی کامل باشد دیگر کاربران به سمت پلتفرم های خارجی نمی روند و بهانه ای برای استفاده از آنها نخواهند داشت.نماینده مردم شهرستان‌های شیراز و زرقان در مجلس شورای اسلامی، خاطرنشان کرد: باید به جای سیستم تنبیه (فیلترینگ) از سیستم تشویق استفاده کرد، هزینه اینترنت را کمتر کرد تا مردم بتوانند از پلتفرم های داخلی استفاده کنند و سراغ برنامه های خارجی نروند.قادری، گفت: وضعیت فعلی قابل دفاع نیست و استفاده از فیلترشکن ها هزینه کلانی را برای خانواده ها به همراه دارد، لذا باید تفاوت هزینه بین استفاده از پلتفرم داخلی و خارجی وجود داشته باشد، تعداد پلتفرم ها کاهش یابد، پلتفرم های مورد حمایت وارد بورس شوند و متعهد شوند که کل نیاز کاربران را برطرف کنند.

مسوولان در مقابله با فیلترشکن ها صرفا وعده می دهند!

رئیس هیات مدیره سندیکای صنعت مخابرات ایران گفت: فروش فیلترشکن ها اقدامی خلاف قانون است که علاوه بر تحمیل هزینه اضافی به کاربران باعث کاهش سرعت دانلود و آپلود شده و امنیت کاربران را به مخاطره می اندازند؛ حال سوال اینجاست که چرا چنین ابزار خلاف قانونی بایستی محل درآمد برای افراد و شرکت های سودجو باشد و مسوولان هم مدام در مقابله با این ابزار فقط وعده می دهند و اقدام سریعی صورت نمی گیرد؟!

مهندس حسین ریاضی، در گفت‌وگو با خبرنگار ما پیرامون دستور رئیس جمهور مبنی بر رسیدگی جدی به فروش فیلترشکن ها در کشور، اظهار کرد: شکی نیست که استفاده از فیلترشکن‌ها، هم سرعت دانلود و آپلود کاربر را کم می کند و هم امنیت اطلاعات گوشی و تبلت کاربر را مورد تهدید قرار می دهد.

وی، ادامه داد: فروش فیلترشکن از یک طرف اقدام نادرست و خلاف قانونی است که علاوه بر آن هزینه هایی را نیز به کاربر متحمل می کند و اکنون جای سوال دارد که چرا چنین ابزار خلاف قانونی بایستی محل درآمد برای افراد و شرکت های سودجو باشد و مسوولان هم مدام در مقابله با این ابزار فقط وعده می‌دهند و اقدام سریعی صورت نمی گیرد؟!

رئیس هیات مدیره سندیکای صنعت مخابرات ایران، گفت: انتظار مردم، سندیکای صنعت مخابرات ایران و صنف، پیرامون فیلترینگ و فروش فیلترشکن ها، رفتار یکپارچه از حاکمیت است و جلسات مشترک سران قوا هم علی القاعده به همین منظور است. گفتنی است؛ مسعود پزشکیان، رئیس جمهور در اولین جلسه شورای عالی فضای مجازی در دولت چهاردهم با اشاره به موضوع فروش فیلترشکن توسط عده‌ای سودجو، با بیان اینکه برخی با فیلترشکن فروشی پول‌های میلیاردی کسب می کنند که این برای کشورمان خوب نیست، دستور داد تا این مسئله حتما به شکل دقیق و جدی مورد رسیدگی قرار گرفته و تصمیم مقتضی در این مورد و به طور کلی زمینه‌های رواج چنین کسب و کاری اتخاذ شود.

وزیر ارتباطات صرفا بازوی اجرایی رئیس جمهور برای رفع فیلتر است

مدیر گروه امور زیربنایی و تولیدی مرکز مطالعات راهبردی مجمع تشخیص مصلحت نظام، معتقد است: اینکه می گویند وزارت ارتباطات فیلترینگ را پیگیری کند، یعنی از رئیس جمهور و هیات دولت، این انتظار مطرح می شود و بازوی اجرایی رئیس جمهور در این حوزه هم وزارت ارتباطات و وزیر ارتباطات است؛ اگرچه رئیس جمهور هم پیگیر این موضوع است، اما تصمیم گیر نهایی نیست.

دکتر سعید باستانی در گفت‌وگو با خبرنگار ما پیرامون تاکید رئیس جمهور بر رفع فیلترینگ، گفت: یک مساله اولیه وجود دارد و آن هم توقعی است که رئیس جمهور در مناظرات انتخاباتی ایجاد کرده که باید فیلترینگ رفع شود، این کلیت را رقبای رئیس جمهور در زمان انتخابات اعلام نکردند و این انتظار در عموم مردم از رئیس جمهور وجود دارد.

وی، ادامه داد: شورای عالی فضای مجازی و شورای عالی امنیت ملی تعیین کننده ضوابط امنیتی هستند و بخشی از موضوع نیز عمق فیلتراسیون است؛ به عنوان مثال در مواقعی در واتس اپ متن قابل دسترس است، اما فیلم و تصویر بدون فیلترشکن قابل دسترس نیست، پس بنابراین در این مواقع عمق فیلتر تعیین می شود.

مدیر گروه امور زیربنایی و تولیدی مرکز مطالعات راهبردی مجمع تشخیص مصلحت نظام، اظهار کرد: اینکه می گویند وزارت ارتباطات فیلترینگ را پیگیری کند، یعنی از رئیس جمهور و هیات دولت این انتظار مطرح می شود و بازوی اجرایی رئیس جمهور در این حوزه هم وزارت ارتباطات و وزیر ارتباطات و فناوری اطلاعات است، اگرچه رئیس جمهور پیگیری موضوع را می کند، اما تصمیم گیر نهایی نیست.

باستانی، خاطرنشان کرد: این موضوع به طرح کارشناسی گسترده ای نیاز دارد و موارد امنیتی این حوزه حساس است و توقع بر این است که این موارد برطرف شود. مثلا در دبی از برنامه Botim استفاده می کنند و بحث رویکرد اقتصادی است نه امنیتی و این برنامه بهتر از واتساپ نیاز کاربران اماراتی را رفع می کند و مدیریت آن هم دست دولت امارات است.

وی، افزود: گروه کارشناسی حوزه را بررسی می کند؛ مثلا یوتیوب منبع تولید و انتشار علم است، اما مواردی هم دارد که نیاز به فیلتر دارد، یا باقی موارد همچون اینستاگرام یا تیک تاک که جنبه های آموزشی هم دارند، اما در مواردی نیاز به فیلتر شدن است، نه فیلتر کامل.

مدیر گروه امور زیربنایی و تولیدی مرکز مطالعات راهبردی مجمع تشخیص مصلحت نظام، اظهار کرد: این برنامه ها بخشی مفید دارند و بخشی دیگر باید مورد توجه قرار گیرد و گاها موارد امنیتی یا اخلاقی دارند که باید با آگاهی فیلتر شوند.

باستانی، افزود: هدف از فیلتراسیون این است که دسترسی کمتر شود، اما شاهد آن هستیم که فیلترینگ انجام شده، اما دسترسی تغییر نکرده و فقط بازاری برای فیلترشکن فروش ها ایجاد شده است و هزینه فیلترشکن به بار مالی مردم اضافه شده است؛ فیلترشکن در همه جای دنیا استفاده می شود و کاربردهای ویژه ای هم دارد.

وی، گفت: دو شورای بزرگ تصمیم گیر باید کار کارشناسی بر روی پلتفرم های فیلترشده انجام دهند و اگر می توانیم، نرم افزاری همچون botim ایجاد کنیم، اینکه فیلتر کنیم و جایگزین نداشته باشیم، نمی شود.

باستانی، افزود: تکنولوژی و اعتمادسازی لازمه این بحث است و باید تمام ویژگی های لازم در پیام رسان لحاظ شده باشد و اعتماد کاربر را جلب کند. دسترسی به متون و دیتاها نیاز مردم است و باید بین شرکت خدمات دهنده و کاربر اعتمادسازی شکل گیرد.

مدیر گروه امور زیربنایی و تولیدی مرکز مطالعات راهبردی مجمع تشخیص مصلحت نظام، افزود: یک خانواده سه نفره گاها ماهی ۵۰۰ هزار تومان هزینه فیلترشکن می دهند و لذا دسترسی ها بیشتر شده که کمتر نشده است، بنابراین بار مالی فقط اضافه شده است.

وی، اظهار کرد: وظیفه دولت پیگیری کردن و عمل به قول و وعده است، نمی شود قول دهیم و تغییری ایجاد نشود. یا باید با مردم صحبت شود و معضلات ارائه شود و اگر مسائل امنیتی مطرح باشد، بنابراین قطع دسترسی باید موقت باشد، چراکه با یک دکمه می شود همه دسترسی قطع شود و در نتیجه نیاز به فیلتر کردن نیست.

باستانی، افزود: وزیر ارتباطات باید مسائل این حوزه را بررسی و مشکلات را پیگیری کند و مصر بودن، انتظار مردم از رئیس جمهور است و وزیر ارتباطات باید موانع را در هیات دولت اعلام کند تا رئیس جمهور پیگیری کند، چراکه رئیس جمهور رئیس شورا است و باید با مردم صحبت کند.

تحمیل فشار به وزیر ارتباطات برای رفع فیلترینگ صحیح نیست

عضو کمیسیون صنایع و معادن مجلس شورای اسلامی، معتقد است: اینکه برای رفع فیلترینگ به وزیر ارتباطات فشار وارد می کنند درست نیست؛ چراکه وزیر یک نفر است و لذا ایشان تصمیم گیر نیست و متولی شخص وزیر نیست، بلکه شورای عالی فضای مجازی تصمیم گیر است.بهنام رضوانی، عضو کمیسیون صنایع و معادن مجلس شورای اسلامی در گفت و گو خبرنگار ما پیرامون وعده رئیس جمهور برای رفع فیلترینگ، گفت: با رفع فیلترینگ کاملا موافق هستم. متولی این امر شورای عالی فضای مجازی است و باید این شورا پیگیر این موضوع باشد که البته ریاست آن با رئیس جمهور است.وی، ادامه داد: اینکه برای رفع فیلترینگ به وزیر ارتباطات فشار وارد می کنند درست نیست؛ چراکه وزیر یک نفر است و لذا ایشان تصمیم گیر نیست و متولی شخص وزیر نیست، بلکه شورای عالی فضای مجازی تصمیم گیر است.نماینده مردم کلیبر، خداآفرین و هوراند در مجلس شورای اسلامی، گفت: با رفع فیلترینگ مردم دیگر هزینه اضافی برای خرید فیلترشکن نمی دهند، فیلترینگ برای مردم دردسرساز است و آنها را اذیت می کند؛ چراکه باید هزینه زیادی برای خرید فیلترشکن پرداخت کنند. چرا باید فیلترینگ راه بیندازیم تا مردم برای دسترسی راحت به اینترنت، با خرید فیلترشکن هزینه اضافی پرداخت کنند؟

وزیر ارتباطات فیلترینگ را در شورای عالی فضای مجازی قویا دنبال کند؛ ایشان در شورا یک حق رای دارد و تصمیم گیر نهایی نیست

عضو مجمع تشخیص مصلحت نظام، گفت: وزیر ارتباطات در موضوع فیلترینگ نماینده رئیس جمهور است و باید انتظارات رئیس جمهور را به صورت قوی دنبال کند، ولی به این معنا نیست که در رفع فیلترینگ به وزیر اختیار صد درصدی داده شده، لذا باید وزیر قویا پیگیر موضوع فیلترینگ در شورای عالی فضای مجازی باشد، اما وزیر در شورا تنها یک حق رای دارد و تصمیم گیر نهایی نیست، لذا باید دلایل ایشان برای سایر اعضاء قانع کننده‌باشد.

حجت‌الاسلام غلامرضا مصباحی‌مقدم در گفت‌وگو با خبرنگار ما پیرامون پیگیری موضوع فیلترینگ در دولت چهاردهم، گفت: یکی از وعده های رئیس جمهور در زمان انتخابات، رفع فیلتر بود و قطعا این وعده را باید دنبال، اجرایی و عملیاتی کنند و هر گونه تغییر نیازمند این است که سیاست‌ها و قوانین، مورد توجه و عنایت قرار گیرد و با توجه به سیاست‌ها، چارچوب و قوانین بازنگری صورت گیرد.

وی، اظهار کرد: اصل بحث مورد قبول است، اما شیوه تحقق نیازمند این است که از مسیر تغییری اجرا شود که حاصل وفاق ملی است و نمی‌توان بدون در نظر گرفتن دغدغه های موجود و نادیده گرفتن دغدغه‌ها، رفع فیلتری صورت گیرد؛ چراکه این دغدغه‌ها ارزشمند هستند و باید رعایت شوند.

عضو مجمع تشخیص مصلحت نظام، ادامه داد: با توجه به سیاست ها در فضای مجازی، باید این سیاست ها مبنا قرار گیرند و در این زمینه شورای عالی فضای مجازی حق تصمیم گیری دارد و برخی مسائل نیز به شورای عالی امنیت ملی مربوط می شود و باید در آنجا مورد توجه قرار گیرد.

مصباحی مقدم افزود: کشورهای دیگر که به عنوان کشورهای آزاد در دنیا شناخته می شوند، اینگونه نیستند که از نظر رفع فیلتر هیچ گونه چارچوب و اصول و مبانی و سیاست هایی نداشته باشند و به صورت ولنگار این فضا را در اختیار صغیر و کبیر قرار دهند، آنها هم در چارچوبه اصول و قوانین و مقررات فیلترها را کنار گذاشتند و رعایت می کنند.

وی خاطرنشان کرد: به عنوان مثال شرکت های عرضه کننده خدمات اینترنتی و فضای مجازی نسبت به اصول دولت ها متعهدند و با تعهد به آن اصول فعالیت می کنند و استفاده کنندگان از خدمات آنها به صورت آزادانه از این خدمات استفاده می کنند، لذا باید با رعایت سیاست ها بازنگری صورت گیرد.

عضو مجمع تشـخیص مصلحت نظام، در رابطه با نقش وزیر ارتباطات در موضوع رفع فیلترینگ، گفت: جایگاه وزیر در این موضوع رفیع است و ایشان نماینده رئیس جمهور است و باید انتظارات رئیس جمهور را به صورت قوی دنبال کند، ولی به این معنی نیست که اختیار به صورت صد درصدی به وزیر داده شده، لذا باید وزیر موضوع فیلترینگ را در شورای عالی فضای مجازی دنبال کند.

مصباحی مقدم در پایان اضافه کرد: وزیر ارتباطات در شورا یک رای دارد و باقی اعضا هم حق رای دارند و دلایل وزیر باید برای باقی اعضاء قانع کننده باشد، لذا باید وزیر ارتباطات قویا پیگیر موضوع فیلترینگ باشد، اما به این معنی نیست که تصمیم گیرنده نهایی شخص وزیر است.

دولت با مدیریت فیلترینگ، جلوی زیان کاربران را بگیرد

عضو کمیسیون اقتصادی مجلس شورای اسلامی، می گوید: بسیاری از کشورهای جهان از فیلترینگ استفاده می کنند، اما در جای خاص نه در همه زمینه ها، بنابراین دولت، باید موضوع فیلترینگ را مدیریت کند تا مردم و جامعه متضرر نشوند.

احمد انارکی محمدی، عضو کمیسیون اقتصادی مجلس شورای اسلامی در گفت و گو با خبرنگار ما پیرامون موضوع فیلترینگ، گفت: فیلترینگ موضوعی است که بر روی فعالیت های اقتصادی مردم نیز تاثیر گذاشته و همچنین فضای اطلاع رسانی را مختل کرده که این امر برای فعالین اقتصادی مشکلاتی را به وجود آورده است.

وی، ادامه داد: از طرف دیگر فیلترینگ برای معیشت مردم و اقتصاد در جامعه اختلالاتی ایجاد کرده است و اگر دسترسی کامل وجود داشته باشد، در هنگام بروز مشکل و توطئه در فضای مجازی، افراد می توانند آن مشکل را خنثی کنند.

عضو کمیسیون اقتصادی مجلس شورای اسلامی، اظهار کرد: چرا در جامعه باید فروش فیلترشکن انجام شود و افرادی کسب درآمد بالا از این زمینه داشته باشند؟

انارکی محمدی، خاطرنشان کرد: استفاده از فیلترشکن باعث افزایش استفاده از اینترنت، برق، باطری و کاهش سرعت می شود و همچنین استهلاک تلفن همراه بالا می رود و مردم مجبور به تعمیر و یا تعویض تلفن همراه خود می شوند.

وی، ادامه داد: بسـیاری از کشورهای جهان از فیلترینگ استفاده می کنند، اما در جای خاص نه در همه زمینه ها، بنابراین دولت، باید موضوع فیلترینگ را مدیریت کند تا مردم و جامعه متضرر نشوند.

فرزانه احمدی منش

وظیفه دولت در حوزه امنیت سایبری، حمایت، مراقبت و نظارت است

دکتر هاشم حبیبی، نائب رئیس انجمن صنفی افتا در گفت‌وگو با خبرنگار ما پیرامون ضرورت توجه بیشتر به امنیت سایبری با توجه به تحولات منطقه‌ای، گفت: اگر وظایف و ماموریت‌های هر سازمان مشخص شود و سازمان‌ها در همان راستا عمل کنند، اتفاقاتی که در منطقه مشاهده کردیم، دیگر تکرار نمی‌شود و مسائل امنیتی تا حد زیادی حل می‌شود.

وی، ادامـــه داد: وظیفه دولت هم حمایت، هدایت و نظارت اســـت و اگر دولت به همین وظایف عمل کند و وارد کارهای دیگر نشـــود، تا حد زیادی مشکلات کاهش می‌یابد؛ از طرف دیگر مردم و بخش خصوصی هم باید اجرا، تولید و تامین امنیت در حوزه اجرایی را بر عهده گیرند.نائب رئیس انجمن صنفی افتا، تاکید کرد: دولت برای حمایت از حوزه امنیت سایبری، باید قوانین دقیقی تدوین کند تا امنیت سایبری که یک فعالیت اقتصادی است، توسعه یابد و از سوی دیگر کمک‌های مالی و معنوی نیز ارائه دهد؛ همچنین قوانین را به گونه‌ای سازماندهی کند که مردم و کسب و کارها دچار چالش نشوند؛ دولت باید به سمتی حرکت کند که حتی اگر فعالیتی در این حوزه صرفه اقتصادی ندارد و یا صرفه دارد، اما از لحاظ امنیتی نباید به بخش خصوصی سپرده شود، دقیق تعریف شود.

حبیبی، افزود: دولت باید امنیت سایبری را به نحوی هدایت کند که به بهترین نتایج برسد؛ کارها باید تقسیم‌بندی شود، بدین معنا که اگر اقدامی توسط مردم و بخش خصوصی به نحو احسن انجام می گیرد، باید حتما به آنها سپرده شود.

وی، گفت: پیشـــرفت و توســـعه کشور باید متوازن باشد، یعنی حمایت و هدایت باید به گونه‌ای صورت گیرد که در همه حوزه‌ها بصورت متوازن رشد کنیم، به عبارت دیگر در حوزه امنیت سایبری نیز باید به طور متوازن پیشرفت داشته باشیم.نائب رئیس انجمن صنفی افتا، خاطرنشان کرد: نظارت همیشه توسط کسانی صورت می گیرد که تخصص و تجربه بالاتری دارند؛ به عبارت دیگر توانسته‌اند در این حوزه قوی عمل کنند؛ به همین علت در مسئله نظارت که مهم‌ترین وظیفه دولت است، بهترین‌ها و با تجربه‌ترین‌ها باید در دولت باشند، همچنین اگر قرار است در حوزه سایبری نظارت و یا اقدامی صورت گیرد، سازمان‌های دولتی نباید تولیدکننده محصولات خود باشند و باید آن را به جوانان متخصص و بخش خصوصی بسپرند.وی، اظهار کرد: مردم و بخش خصوصی باید نهادهای مردم نهاد تشکیل بدهند و برای خود مقرراتی تدوین و تصویب کنند و خود را به بهترین نحو اداره کنند و از سوی دیگر براساس قوانین بالاسری کشور فعالیت کنند.

حبیبی، اشاره کرد: مردم و شرکت‌های خصوصی (حقیقی و حقوقی)، باید در حوزه تامین امنیت سایبری کشور ورود کنند و خدمات امنیتی ارائه دهند؛ البته ذکر این نکته ضروری است که نباید به بخش خصوصی برای تولید خدمات امنیتی امر و نهی کرد؛ چراکه خود آنها باید برای تولید چنین محصولاتی به جمع‌بندی برسند.

نائب رئیس انجمن صنفی افتا، بیان کرد: بخش خصوصی می‌تواند با نگاه به نیازهای کشور، خود را رشد و ارتقا دهد، پس حاکمیت تنها باید نظارت کلان داشته باشد.

وی، تشریح کرد: ما در حوزه امنیت سایبری به سازمانی همچون سازمان غذا و دارو نیاز داریم؛ به این صورت که در هر گوشـــه از کشـــور بیماری رخ می‌دهد، این سازمان داروی مربوطه را گاها به صورت رایگان عرضه می کند.نائب رئیس انجمن صنفی افتا، گفت: در حوزه امنیت سایبری بخش خصولتی نباید رقیب بخش خصوصی و ارائه‌دهنده خدمات باشد، بلکه باید در جایگاه مترجمی بین دستگاه حاکمیتی و بخش خصوصی باشد.

نقش سخت افزار در حملات سایبری به زیرساخت‌های کشور کمتر از یک درصد بوده است

دکتر مسعود شکرانی در گفت‌وگو با خبرنگار ما پیرامون نحوه نظارت بر تجهیزات وارداتی مخابراتی به کشور، گفت: در ایران به دلیل وجود بخشنامه ای که از گذشته وجود داشته اســـت و اینکه مسوولان تنظیم مقررات امکان اصلاح بخشنامه را نداشتند، تجهیزات فناوری اطلاعات در مبادی ورودی تست و مورد آزمایش قرار می گرفت و افراد با اعتماد به اینکه آن تجهیزات از تنظیم مقررات تاییدیه دریافت کرده است، آن را وارد شبکه خود می کنند. وی، ادامه داد: در تمام حملات سایبری که به زیرساخت کشور صورت گرفته است و طی سالهای اخیر رشد نیز داشته است، مشاهده می کنیم که نقش سخت افزار در حمله ها کمتر از یک درصد اســـت و اصل جایی که حملات صورت می گیرد، ۳۰ درصد آن نرم افزاری و ۷۰ درصد آن مربوط به دانش افزار است؛ بدین معنا که افراد و استفاده کنندگان در دولت، بخش خصولتی و بخش خصوصی آموزش های لازم برای بهره برداری از تجهیزات مخابراتی را فرا نگرفته اند و به همین دلیل بنده معتقد هستم که پایش و برقراری امنیت را در شبکه بهره بردار نهایی باید انجام دهیم.

عضو کمیسیون بین‌الملل و صادرات سازمان نظام صنفی رایانه‌ای کشور، تاکید کرد: باید استانداردهای بین الملل در زمینه واردات تجهیزات مخابراتی به کشور را بپذیریم و تست و آزمایش را در شبکه بهره بردار نهایی انجام دهیم.

شکرانی، خاطر نشان کرد: ما از دنیا عقب مانده ایم و با فشار وارد کردن به تولیدکنندگان و واردکنندگان بیشتر عقب می مانیم؛ مساله امنیت بسیار حائز اهمیت است، اما به نام امنیت نباید کشور را دچار توقف کنیم؛ به عبارت دیگر فشار بیشتر و بیشتر روی تامین کنندگان عملا به توسعه قاچاق منجر می‌شود و قطعا وضعیت امنیت تجهیزات در غیاب واردکنندگان شناسنامه دار، به شدت متزلزل خواهد شد.

عضو هیات مدیره نظام صنفی رایانه‌ای تهران، بیان کرد: بر اساس مقاله ای که مطالعه کرده ام، بیش از نیمی از فیلترشکن ها برای شرکت های صهیونیستی است و اطلاعات مخرب را جمع آوری می کنند، از طرفی ما در کشور در اینترنت اخلال ایجاد می کنیم و پلتفرم هایی همچون تلگرام، واتس اپ و اینســـتاگرام را فیلتر می کنیم، در چنین شرایطی مردم برای ادامه روند کسب و کارهای خود به اجبار از فیلترشکن ها استفاده می کنند و همین موضوع عامل جاسوس افزار می شود.

وی، اشـــاره کرد: درخواســـتی که از رگولاتور داریم این است که قانون گذاری مناسبی داشته باشد و احساسی برخورد نکند تا مردم با استفاده از فیلترشکن ها اطلاعات خود را به دست دشمن نسپارند.

الزام برای تست امنیت تجهیزات ارتباطی در نقطه انتهایی

حسین توکلی، عضو کمیسیون تامین سازمان نظام صنفی رایانه‌ای استان تهران پیرامون لحاظ نمودن موارد امنیتی در واردات تجهیزات ارتباطی به کشور طی مطلب ارسالی به ما نوشت: پیرامون این موضوع سه نکته قابل توجه است:

۱ - الزام برای برقراری آزمایشگاه امنیت در سازمان‌های بزرگ و تست امنیت تجهیزات در نقطه انتهایی:

در سال‌های اخیر تمرکز تمامی دستورالعمل‌ها، آیین نامه ها و پیشنهادهای نگارش شده در حوزه واردات تجهیزات تنها و تنها بر روی ارزیابی تجهیزات در مبادی ورودی بوده است که سوابق اجرای این سیاست در سال‌های گذشته موفق نبوده و مشکلات زیادی ایجاد نموده است.

نکته بسیار مهم در ارزیابی این است که ارزیابی تجهیزات می‌بایست در نقطه انتهایی زنجیره تامین انجام شود نه در نقطه ابتدایی ورود به کشور و در گمرک و همچنین پایش امنیت و انجام سرویس‌های امن سازی می‌بایست به صورت مستمر صورت گیرد.

۲ - الزام به استمرار در تست و به روز رسانی تجهیزات:

سازمانهای نظارتی و قانونگذار به واقع زمانی می‌توانند وظایف خود را به درستی انجام دهند که سازمان‌ها را به عنوان اصلی‌ترین بخش این پازل ملزم نماید که به صورت پیوسته در دوره‌های زمانی شبکه را ارزیابی نمایند، اقدامات فنی زیر در این مسیر پیشنهادمی‌شوند:

* آزمون‌های نفوذ و ارزیابی‌های امنیتی منظم: کلیه متخصصان بر این باورند که ارزیابی تجهیزات به تنهایی تاثیر و نقش بسیار اندکی در کل فرآیند امنیت شبکه دارد. بدیهی است امنیت یک روند کاملا مستمر و پویا است که به نظر می‌رسد به دلیل نیاز به مسئولیت پذیری همه بازیگران (و نه تنها تولیدکنندگان و واردکنندگان) تا کنون تصمیم سازان از انجام فرآیند صحیح تعلل کرده اند.

* فرآیندهای نظارتی و ارزیابی امنیتی: ارزیابی‌های امنیتی جامع باید به طور منظم انجام شود تا سیاست‌های امنیتی بررسی و در صورت نیاز تقویت شوند. مشابه با ارزیابی های شاپرک در حوزه شبکه پرداخت الکترونیک.

آزمون نفوذ: به طور منظم آزمون‌های نفوذ انجام دهید تا آسیب‌پذیری‌های سیستم‌های بانک شناسایی و برطرف شوند. این آزمون‌ها توسط تیم‌های متخصص داخلی امنیت فاوا انجام میشوند .

* بروز نگه داشتن سیستم‌ها و نرم‌افزارها: بروزرسانی منظم: تمام نرم‌افزارها و سیستم‌ها باید به صورت اصلی و با برخورداری از سرویس های سازنده اصلی تهیه شوند و به صورت منظم بروزرسانی شوند تا اطمینان حاصل شود که در برابر آسیب‌پذیری‌های

شناخته‌شده محافظت می‌شوند.

* پچ‌های امنیتی: شرایط دسترسی سریع به پچ‌های امنیتی باید برقرار باشد و به محض انتشار باید به سرعت اعمال شوند تا از سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده جلوگیری شود.

۳ - پیشگیری از ایجاد انحصار در صنعت فاوا:

حوزه فاوا نیازمند حضور متعدد شرکت‌های بخش خصوصی و ارتباط نزدیک بخش خصوصی با حاکمیت است. حذف فعالین بخش خصوصی که دارای تعهد و تخصص لازم و کافی می‌باشند و ایجاد شرکت‌های خصولتی و ایجاد انحصار برای این شرکت‌ها در نهایت ریسک و خسران مالی و امنیتی زیادی برای این صنعت و حاکمیت ایجاد می‌نماید.

۴ - بازارسازی برای صنعت فاوا و تقویت این صنعت:

با توجه به اهمیت صنعت فاوا و افزایش روزافزون آن در راستای هوش مصنوعی و اقتصاد دیجیتال، میبایست این صنعت مورد حمایت ویژه دولت قرار گرفته و با ایجاد بازارهای جدید و اعتماد به بخش خصوصی و سپردن کار به این بخش و مسوولیت پذیری از بخش خصوصی، این صنعت را در راستای چشم انداز عالی حاکمیت تقویت نمود.

۵ - آموزش و آگاهی مستمر:

باید آموزش‌های منظم در خصوص سیاست‌ها و شیوه‌های امنیتی در لایه های مدیران و کارشناسان ارایه گردد که به افزایش آگاهی از مسایل امنیت اطلاعات و بهبود رفتار امنیتی در سازمان کمک کند. آموزش مستمر به کارمندان در بخش دولتی و خصوصی درباره تهدیدات امنیتی و بهترین شیوه‌های حفظ امنیت می‌تواند ریسک خطاهای انسانی را کاهش دهد.

وضعیت واردات تجهیزات ارتباطی به کشور سردرگم است

محمد احسان حمیدیا در گفت‌وگو با خبرنگار ما پیرامون لزوم بازنگری و تاکید بر موارد امنیتی در واردات تجهیزات ارتباطی به کشور، گفت: بنده معتقد هستم تا جایی که امکان دارد باید تولیدات را داخلی کنیم؛ همانطور که در فرمایشات مقام معظم رهبری نیز تاکید شده است، توسعه پایدار و متوازن زمانی رخ می دهد که چرخ تولید در کشور راه بیوفتد و در چنین شرایطی، کشور جوانان را وارد چالش فناوارنه می کند تا دیگر تصمیم به مهاجرت نگیرند.وی، ادامه داد: اگرچه داخلی کردن تمام تجهیزات در کشور، توسط هیچ کشوری امکان پذیر نیست؛ اما در بحث امنیت که اصلا شوخی بردار نیست، باید به سمت داخلی کردن تجهیزات ارتباطی حرکت کنیم.رئیس انجمن صنفی افتا، تاکید کرد: وضعیت فعلی واردات تجهیزات ارتباطی سردرگم است و کسانی که تجارت‌شان بر مبنای واردات است، علاقه ای ندارند که در این تجارت با سنگ اندازی مواجه شوند، لذا اعلام می کنند که تجهیزات ارتباطی در آزمایشگاه های بین المللی مورد بررسی و تایید قرار گرفته اند و لزومی ندارد که آنها را مورد ارزیابی و آزمایش قرار دهیم که متاسفانه این تفکر، نگاه غلطی است و مشابه آن در حوادث اخیر لبنان نیز مشاهده شد.حمیدیا، خاطرنشان کرد: نباید پس از ورود تجهیزات ارتباطی خارجی به

کشور با آنها آسان برخورد کنیم، اما به تولیدکننده سخت بگیریم؛ لذا ضروری است که پس از ورود تجهیزات ارتباطی خارجی به کشور، این تجهیزات مورد بررسی، ارزیابی و آزمایش قرار گیرند.

زهرا طاهری

توسعه اقتصاد دیجیتال و نقش محوری اپراتورهای تلفن همراه

نخستین رویداد اقتصاد دیجیتال همراه اول با موضوع «نقش آفرینی صنعت ICT در توسعه اقتصاد دیجیتال» و با شعار «زندگی پایدار، سبز و هوشمند» در سالن همایش های دانشکده تربیت بدنی دانشگاه تهران برگزار شد.

این رویداد در قالب سه بخش «سخنرانی های کلیدی»، «ارائه تخصصی» و «پنل های تخصصی» و با مشارکت بازیگران اصلی اکوسیستم اقتصاد دیجیتال ایران برگزار و در جریان آن سعی شد که با معرفی و ارائه تجربیات بین المللی در این حوزه، بهترین راهکارهای ادغام فناوری های دیجیتال با صنایع مختلف نیز تشریح شود.

سرمایه گذاری چهار هزار میلیارد تومانی همراه اول در حوزه دانش‌بنیان

در ابتدا وحید شاه منصوری به عنوان متولی برگزاری و همچنین رییس مرکز تحقیق و توسعه همراه اول، به کالبدشکافی استراتژی و تاکتیک اپراتور اول تلفن همراه طی مدت زمان اجرای برنامه راهبردی پنج ساله منظومه پرداخت و اظهار کرد: با سرمایه گذاری در راه اندازی مراکز و شرکت های «هاب»، «تحقیق و توسعه»، «همراه کسب و کارهای هوشمند»، «آکادمی همراه» و «همراه فاند» توسط همراه اول، به مرور اکوسیستم اقتصاد دیجیتال نیز شکل گرفت.

وی از تأکید همراه اول بر بخش توسعه اکوسیستم با محوریت اقتصاد دیجیتال نیز گفت و ادامه داد که در این مسیر اقدام به راه اندازی دو مرکز نوآوری در دانشگاه های تهران و شریف با موضوعیت 5G و AI کرده است.

بنا بر اظهارات شاه منصوری، همراه اول تاکنون با همت مرکز تحقیق و توسعه خود، سرمایه گذاری چهار هزار میلیارد تومانی در بخش خدمات دانش بنیان ها و خرید تجهیزات از محل تولیدات بومی داشته است.

ایران در اول راه اقتصاد دیجیتال

در همین بخش سخنرانی های کلیدی علی اسدی، رئیس پارک علم و فناوری دانشگاه تهران نیز طی سخنانی کوتاه «اقتصاد دیجیتال» را پیشران توسعه اقتصاد کشور مطرح و اظهار کرد: تمامی ارکان وابسته به این حوزه در نهایت منجر به برداشتن گام های خوبی در شاخص های مهمی چون افزایش بهره وری، اشتغالزایی و توسعه کسب و کار می شود.

وی سهم ایران از اقتصاد دیجیتال به نسبت کشورهای دیگر همسطح را کم ارزیابی کرد و گفت: سهم اقتصاد دیجیتال از سرانه تولید ناخالص داخلی (GDP) در دنیا حدود ۱۸ و در ایران ۸ درصد است و به نوعی ما همچنان اول راه هستیم.

رئیس پارک علم و فناوری دانشگاه تهران بهبود و ارتقای دسترسی به اینترنت پرسرعت را که همراه اول می تواند نقش اساسی در این بخش داشته باشد را زمینه تحول در حوزه اقتصاد دیجیتال دانست و گفت که اهرم دیگر هم افزایی بخش های دولتی و خصوصی کشور است.

پنل اقتصاد دیجیتال در قاب تجربه

در ادامه مراسم پنل تخصصی «اقتصاد دیجیتال در قاب تجربه» با حضور تعدادی از بازیگران شاخص حوزه اقتصاد دیجیتال همچون شهاب جوانمردی، مدیرعامل هلدینگ فناپ، رضا سمیع زاده، مدیرعامل هلدینگ فاخر و مهرداد شاملو، مدیرعامل هلدینگ فراکاو برگزار شد تا مخاطبان با جنس دیگری از چالش ها و فرصت های حوزه صنعت آشنا شوند.

شهاب جوانمردی در ابتدای سخنانش «سکوی خلق آینده» را به عنوان چشم انداز فناپ معرفی کرد و گفت: بنگاه های بزرگ در دنیا با نگاه تبدیل شدن به لوکوموتیو بزرگی که سایر بیزینس ها را نیز با خود همراه کنند، به سمت ایجاد و تقویت زیرساخت ها رفته اند؛ مشابه رفتاری که همراه اول در بخش سرمایه گذاری ها و توسعه زیرساخت ها داشته تا ابعاد اکوسیستم بزرگتر شود.

وی رویکرد فناپ را هم تا اندازه ای مشابه همراه اول دانست و با بیان اینکه طی این چشم انداز اقدام به سرمایه گذاری در زیرساخت های ارتباطی کرده ایم، عنوان کرد: رویکرد ما در ۱۵ سال ابتدایی فعالیت، متمرکز بر محصول و بازار بود اما در پنج سال اخیر با یک پارادایم شیفت داخلی، متمرکز بر حل مسائل جاری کشور شدیم زیرا معتقدیم اقتصاد دیجیتال از این مسیر شکل می گیرد.

رضا سمیع زاده، مدیرعامل هلدینگ فاخر نیز دیگر عضو پنل بود که مفهوم اقتصاد دیجیتال را برگرفته از اقتصاد مشارکتی عنوان کرد و گفت که منظور این است اقتصاد دیجیتال با اشتراک، بهینه سازی و افزایش کارایی منابع در ارتباط است و ما در کسب و کار خود به دنبال نئوبانک در حوزه لجستیک هستیم.

وی که از فعالان حوزه لجستیک است به چالش های حوزه هوشمندسازی پرداخت و تصریح کرد: بدون توسعه 5G نمی توانیم نقش آفرینی ویژه در این بخش داشته باشیم و همراه اول به عنوان بزرگترین اپراتور تلفن همراه کشور می تواند دغدغه فعالان و صنعت گران در این حوزه را رفع کند و پیشران توسعه بماند.

به زعم سمیع زاده در حال حاضر بیشترین چالش های بخش اقتصاد دیجیتال مربوط به قوانین حقوقی و رگولاتوری می شود.

در نهایت مهرداد شاملو، مدیرعامل هلدینگ فراکاو نیز ضمن معرفی سابقه فعالیت خود در اکوسیستم فناوری کشور با سرمایه گذاری در حوزه دانش بنیان، به بیان چالش ها و تنگناهای موجود در این عرصه پرداخت و صراحتا از ثابت ماندن کیک اقتصاد دیجیتال کشور انتقاد کرد.

وی مقوله منابع انسانی را نیز به عنوان چالش دیگر مطرح کرد و اذعان داشت که نیروی انسانی بسیاری بعد از پایان تحصیل مهاجرت می کنند؛ بنابراین تا چالش ها حل نشود، شیب رشد توسعه افزایش نمی یابد.

پنل «اپراتور، هسته اقتصاد دیجیتال»

پنـــل تخصصی دوم نیز با عنوان «اپراتور، هســـته اقتصاد دیجیتال» با حضور مصطفی حیدرزاده مدیرکل راهبردهای دیجیتال همراه اول، محمدصادق کریمی عضو هیات مدیره رایتل، داوود ادیب رییس هیات مدیره انجمن شرکت های فناور هوش مصنوعی و اقتصاد دیجیتال ایران و محمدجعفر صدیق رئیس سابق پارک فناوری اطلاعات و ارتباطات برگزار و دغدغه های اپراتورها و زمینه های سرمایه گذاری های آنها مطرح شد.

حیدرزاده در این پنل با گذر از پوسته اپراتور اول تلفن همراه کشور، ساختار کسب و کاری آن را به سه لایه Core، Near Core و Beyond Core تقسیم بندی و نقش اصلی همراه اول را از منظر اقتصاد دیجیتال، در بخش هســـته بیان کرد و گفت: لایه نزدیک هسته به سرویس های دیجیتال توسعه یافته مربوط می شود و در نهایت لایه سوم هم که فراتر از هسته است و به سهامداری های اپراتور اول ارتباطی در پلتفرم های دیجیتال اشاره می کند.

حیدرزاده و کریمی به نمایندگی از طرف اپراتورهای تلفن همراه حاضر در این رویداد، در پاسخ به چرایی عدم توسعه سریع و فراگیر 5G در کشور به مقوله هزینه های بالای سرمایه گذاری و مقرون به صرفه نبودن این موضوع پرداختند.

حیدرزاده گفت که با وجود منطقی نبودن تعرفه های ارتباطی، همراه اول تاکنون بیش از هزار سایت 5G در کشور راه اندازی کرده است؛ کریمی هم در همین راستا از برنامه توسعه ۷۰۰ سایت نسل پنجم در سال جاری توسط رایتل گفت که قرار است ۱۰۰ سایت در اختیار سرویس دهی به عموم باشد و باقی در اختیار صنایع قرار گیرد.

دکتر داوود ادیب، رییس هیات مدیره انجمن شرکت های فناور هوش مصنوعی و اقتصاد دیجیتال ایران در پنل تخصصی «اپراتور، هسته اقتصاد دیجیتال» رویداد نقش آفرینی صنعت ICT در توسعه اقتصاد دیجیتال، گفت: در شاخص جهانی نوآوری GII ۲۰۲۴ که به عنوان هفدهمین دوره شاخص جهانی نوآوری (GII) در رویدادی به میزبانی سازمان جهانی مالکیت فکری (WIPO)، روز ۲۶ ســـپتامبر ۲۰۲۴ (پنجم مهر ۱۴۰۳) با شعار کارافرینی اجتماعی برگزار شد، آخرین گزارش مربوطه در خصوص وضعیت کشورها در شاخص جهانی نوآوری ارایه گردید.

وی، گفت: بر اساس جدیدترین نتایج گزارش شاخص جهانی نوآوری GII ۲۰۲۴، ایران از رتبه ۵۳ جهانی در بین ۱۳۳ کشور بررسی شده در سال ۱۴۰۱ به رتبه ۶۴ در سال ۱۴۰۳ تنزل یافته است که این نزول ۱۱ پله‌ای نیازمند عارضه‌یابی است.

ادیب تاکید کرد: در شاخص کیفیت تسهیل گری که بدنه دولتی را درگیر می کند، رتبه ۱۳۳ بین ۱۳۳ کشـــور را دریافت کردیم که این موضوع نگران کننده است و هشدار به حساب می آید.وی، افزود: باید ارتباط بین صنعت، دولت و دانشگاه ها پررنگ تر شود و مراکزی همچون مرکز تحقیق و توسعه همراه اول که در شرایط کنونی به خوبی فعالیت می کنند باید تقویت شوند.

ادیب، گفت: در طول دو سال گذشته و در دولت سیزدهم، در شاخص نوآوری، یازده پله سقوط کردیم که باید هشداری برای دولت چهاردهم باشد.

وی، اظهار کرد: اقتصاد دیجیتال موضوع پیچیده‌ای نیست که حساسیت داشته باشیم. باید شاخص های جهانی را بهبود بخشیم تا اقتصاد دیجیتال بهتری داشته باشیم.

وی، افزود: در دنیا نسل پنجم دانشگاه ها با نسل پنجم صنعتی همسو شده اند. ارتباط بین دانشگاه، صنعت و بازار ضعیف است و معاونت علمی ریاست جمهوری باید این رویه را اصلاح کند و دولت با درک این موضوع، باید در جهت مرتفع کردن این موضوع گام بردارد.

ادیب خاطرنشان کرد: انقلاب صنعتی پنجم اصولا برای رفع کاستی های انقلاب صنعتی چهارم به ظهور رسید و امروز سه محور انسان محوری، پایداری و تاب آوری را در انقلاب صنعتی پنجم می بینیم که معادل آن در دانشگاه نسل پنجم موضوع اکوسیستم و پایداری است که به عبارتی با اضافه شدن به مارپیچ چهارگانه در دانشگاه نسل پنجم آن را به مارپیچ پنج گانه و به عبارتی دیگر دانشگاه نسل پنجم تبدیل ساخته است.

صدیق، رئیس ســـابق پارک فناوری اطلاعات و ارتباطات هم در این پنل، از عدم وجود بازارگاه در کشور به عنوان عاملی در جهت کاهش سرعت رشد اقتصاد دیجیتال یاد کرد.

گفتنی اســـت در جریان این رویداد سخنرانی های تخصصی علی اشراقی، عضو هیات علمی دانشگاه کانبرا استرالیا به صورت آنلاین با تحلیلی از «اقتصاد دیجیتال در جهان» و همچنین فرزانه ابوالفضل، رئیس هیات مدیره شرکت تعاونی نوآوران لوتوس پیروزی (بانک پارسیان) با تحلیلی از وضعیت «اقتصاد دیجیتال در ایران» نیز ارائه شد.

سهم بیش از ۱۵ درصدی دنیا از اقتصاد دیجیتال و سهم حدود ۸ درصدی کشور ما از آن، از جمله مهم ترین نکات مطرح شده در طی این سخنرانی ها بود که راهکارهایی برای پیشرفت هر چه بیشتر در این مسیر نیز ارائه شد.

دکتر محمدصادق کریمی، عضو هیات مدیره رایتل در پنل تخصصی «اپراتور، هسته اقتصاد دیجیتال» رویداد نقش آفرینی صنعت ICT در توسعه اقتصاد دیجیتال گفت: تفاوت اقتصاد دیجیتال و هوشمندسازی باید مورد بررسی قرار گیرد، هر فعالیتی که در حوزه دیجیتالی باشد در حوزه اقتصاد دیجیتال قرار می گیرد، اما هوشمندسازی جمع آوری اطلاعات است که بر اساس آن خدماتی ارائه دهیم. وی، افزود: وقتی با اپراتور همکاری می کنید، اپراتور کیفیت تجربه مشتری یا کیفیت سرویس را تضمین می کند. توجه به اپراتورها در حوزه اقتصاد دیجیتال حائز اهمیت است.وی، اظهار کرد: توسعه کسب و کار در صنعت فاوا در کشور مقرون به صرفه نیست و صرفه اقتصادی ندارد. کریمی، گفت: قوانین خوبی در کشور داریم، اما به لایه اجرا نمی رسد که با کمک شرکت ها این مشکل رفع می شود. عضو هیات مدیره رایتل، گفت: در رایتل به عنوان اپراتور در سال جاری برای بسیاری از سایت های پرترافیک لایه دوم و سوم را عملی کردیم و ۷۰۰ سایت نسل پنجم داریم.وی گفت: پروژه رصد اشتغال را داریم که با وزارت کار تفاهم نامه ای امضا کردیم. همکاری با تامین اجتماعی به عنوان اپراتور سلامت را در دست داریم.وی، اظهار کرد: کالابرگ الکترونیک، فروش اقساطی به بازنشسته های تامین اجتماعی اموری است که زیرمجموعه های رایتل ارائه خدمت می کنند. کریمی، گفت: در حوزه هوشمندسازی همکاری مختلف با سازمان ها و ارگان ها داریم و در حوزه لایه دوم که مبتنی بر داده است، با شرکت های مختلفی همکاری داریم.

مونا ارشادی فر

تاکید وزیر ارتباطات بر ضرورت رقابتی سازی صنعت پست

نشست مدیران ارشد و صاحب نظران صنعت پست کشور به مناسبت روز جهانی پست با حضور وزیر ارتباطات و فناوری اطلاعات برگزار و تودیع محمود لیایی و معارفه محمد احمدی، معاون وزیر و مدیرعامل شرکت ملی پست انجام شد.

سید ستار هاشمی، وزیر ارتباطات و فناوری اطلاعات در این مراسم، گفت: اگر تکنولوژی را بشناسیم و از ظرفیت فناوری به خوبی بهره ببریم می‌توانیم صنعت پست را به خوبی ارتقا دهیم، البته در این مسیر دو نگاه وجود دارد، نگاه اول اینکه فناوری را نفی کنیم که تجربه نشان داده به نتیجه خوبی نخواهیم رسید یا در نگاه دوم اینکه با استفاده از فناوری نقاط ضعف خود را تقویت کنیم.

وزیر ارتباطات و فناوری اطلاعات تصریح کرد: وقتی صنعتی بزرگ می‌شود بازیگران آن نیز بیشتر می‌شوند، در نتیجه باید شرایط را به گونه‌ای فراهم کنیم که تمام بازیگران این حوزه بتوانند به خوبی نقش‌آفرینی کنند.

وی افزود: گاهی در حوزه‌ای قانون نداریم و گاهی در بعضی موارد تورم قانون داریم که باید از هر دوی این اتفاق‌ها پرهیز شود در نتیجه از مدیرعامل جدید پست می‌خواهم در حوزه تقنین و تنظیم‌گری حضور فعال داشته باشند و همه بخش‌ها نیز به ایشان در این مورد کمک کنند.

هاشمی تاکید کرد: در هر فضایی به‌ویژه در فضای حاکم بر پست باید وارد فضای رقابتی شویم و از انحصار خارج شویم در نتیجه اگر قرار شد پروانه بدهیم باید الزامات را بپذیریم تا به خدمات پایه بی‌مهری نشود.

وزیر ارتباطات با بیان اینکه در سرمایه‌گذاری محدودیت‌هایی داریم و باید از ظرفیت بخش خصوصی استفاده کنیم، تصریح کرد: در گذشته برای هوشمندسازی فرایندهای پستی اقداماتی انجام شده اما لازم است این فرایندها را با ظرفیت فناوری بازشناسی و بازمهندسی کرده و آن‌ها را ارتقا دهیم.

هاشمی با اشاره به این که برخی درباره تعرفه صحبت می‌کنند، اظهار کرد: درست است که متناسب‌سازی تعرفه باعث جذب سرمایه‌گذارها می‌شود اما باید در کنار آن بهره‌وری به شکل ویژه مورد توجه قرار بگیرد.

وی همچنین به مسئله نیروی انسانی در مجموعه پست اشاره و تاکید کرد: کاری که در حوزه پستی انجام می‌شود بسیار سنگین است و پستچی‌ها در تمام سال و در هر شرایطی، سختی کار را به جان خریده و به مشتریان خدمت ارائه می‌کنند و بر ما واجب است که مشکلات معیشتی آنها را حل کنیم.

هاشمی با تاکید بر رونق بخشیدن به کسب‌وکارهای محلی با کمک پست، گفت: حمایت از کسب و کارهای محلی با استفاده از ظرفیت پست به مدیریت مشاغل کمک کرده و در کاهش مهاجرت افراد از روستا به شهر موثر خواهد بود.

وزیر ارتباطات همچنین به تاکید رئیس جمهور در نشست خود با خبرنگاران بر روی «قانون مالیات مستقیم ماده ۱۶۹» نیز اشاره و افزود: یکی از ارکان مهم شکل‌گیری این قانون، شرکت ملی پست است و این قانون در بحث دولت الکترونیک در قالب حدنگاری و کدپستی مطرح شده است که ماموریت مشترک بین وزارت ارتباطات و برخی دستگاه‌های مرتبط است.

وی با بیان اینکه اگر این اتفاق در کشور رقم بخورد آثار خیر و پربرکت بسیاری خواهد داشت، خاطرنشان کرد: یکپارچگی سامانه‌های فعال در حوزه پست به خلق ثروت و ارزش کمک می‌کند اما امروز شاهدیم که برخی سامانه‌های ما به شکل جزیره‌ای فعالیت می‌کنند و بازدهی خوبی ندارند.

شرکت پست باید موتور محرک اقتصاد دیجیتال کشور باشد

دکتر محمد احمدی، معاون وزیر ارتباطات و مدیرعامل شرکت ملی پست ایران در این نشست، گفت: شرکت ملی پست ایران بین سازمانی‌ترین سازمان کشور است؛ چرا که کارکرد آن روزانه است و با زندگی روزمره افراد عجین شده است.

وی در ادامه افزود: تاریخچه خدمت شرکت ملی پست در زمینه کسب و کارهای اینترنتی فقط محدود به چند سال اخیر نمی‌شود و پیش از این که حتی اینترنت همه‌گیر و جهانی بشود هم حمل و نقل از راه دور در شرکت ملی پست وجود داشته است.

احمدی اضافه کرد: ما به عنوان یکی از سازمان‌های مهم و حیاتی کشور به دنبال ارزش‌افزایی هستیم، بنابراین شرکت ملی پست باید به عنوان موتور محرک اقتصاد دیجیتال در سطح کشور باشد. وی همچنین گفت: تحقق نسل سوم خدمات به عنوان یک راهبرد کلان در دستور کار است. مدیرعامل شرکت ملی پست بیان کرد: هدف ما و هدف دولت به ویژه وزارت ارتباطات این است که بتوانیم در کم‌ترین زمان گام‌های موثری برای ارتقا و برطرف کردن نیازهای جامعه برداریم. وی همچنین اظهار داشت: صنعت پست هنوز قواره مناسب و لازم را در کشور پیدا نکرده است چرا که شرکت ملی پست ظرفیت‌های بسیار زیادی دارد اما توانمندی‌ها و ظرفیت‌های این شرکت آن چنان که باید به جامعه معرفی نشده است. وی در پایان خاطرنشان کرد: شرکت ملی پست چالش‌های زیادی دارد که یکی از آن‌ها موضوع حمل و نقل است که لازمه بهبود آن ورود سازمان‌ها و نهادها به ویژه بخش خصوصی و شرکت‌های دانش‌بنیان است تا با توسعه زیرساخت‌ها در این زمینه خدمات با کیفیت بیش‌تری به مردم ارائه شود.

لزوم ایجاد چارچوب قانونی شفاف در حوزه کریپتوکارنسی

دکتر عباس قلی زاده، عضو هیات مدیره و رئیس شورای انتظامی سازمان نصر خراسان رضوی در یادداشت ارسالی برای ما، آورده است: آیا ظرفیت سنتی شاپرک یا عدم هماهنگی و قوانین خلق الساعه قوای سه گانه یا عدم وجود زیرساخت نرم افزاری و سخت افزاری بانک مرکزی عامل اصلی بلاتکلیفی حوزه ارز دیجیتال به عنوان شالوده تحقق نرخ رشد هدف گذاری شده سهم اقتصاد دیجیتال در برنامه هفتم توسعه است؟ مشکل اصلی در حوزه کریپتوکارنسی در ایران، نبود یک چارچوب قانونی شفاف و جامع است که همزمان با حفظ امنیت و منافع ملی، به رشد و توسعه این فناوری نوین کمک کند. تصمیمات آنی و متناقض نهادهای مختلف، عدم هماهنگی بین قوای سه گانه در استقرار، بهره برداری و احقاق حقوق حقه زیست بوم اقتصاد دیجیتال و محدودیت‌های سخت و نرم افزاری، از جمله عواملی هستند که این وضعیت را پیچیده‌تر کرده است.

طرح پیشنهادی

۱. ایجاد یک نهاد تنظیم گر خودکنترل

تشکیل یک نهاد تشکلی خودتنظیم گر و تخصصی برای تنظیم مقررات حوزه کریپتوکارنسی‌ها.

این نهاد باید از متخصصان حوزه فناوری مالی، اقتصاد و حقوق تشکیل شده و دارای اختیارات کافی برای تصمیم‌گیری و نظارت بر بازار باشد.

۲. تدوین قوانین شفاف و جامع

تدوین قوانین شفاف و جامع برای فعالیت صرافی‌های رمزارز، سرمایه‌گذاری در این حوزه و استفاده از فناوری بلاکچین در صنایع مختلف.

این قوانین باید با توجه به ویژگی‌های خاص کریپتوکارنسی‌ها و بهترین تجربیات جهانی تدوین شوند.

۳. ایجاد زیرساخت‌های لازم

توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات برای تسهیل انجام تراکنش‌های کریپتوکارنسی.

ایجاد بسترهای لازم برای تحقیق و توسعه در حوزه بلاکچین.

۴. حمایت از نوآوری

ایجاد محیطی امن و حمایتی برای فعالیت شرکت‌های دانش‌بنیان و استارت‌آپ‌های فعال در حوزه بلاکچین.

ارائه تسهیلات مالی و اعتباری به این شرکت‌ها.

۵. آموزش و آگاهی‌رسانی

برگزاری دوره‌های آموزشی برای آشنایی عموم مردم و فعالان اقتصادی با فناوری بلاکچین و کریپتوکارنسی‌ها.

افزایش آگاهی عمومی در مورد مزایا و مخاطرات سرمایه‌گذاری در این حوزه.

۶. همکاری بین‌المللی

شرکت در مجامع بین‌المللی و همکاری با سایر کشورها برای ایجاد استانداردهای جهانی در حوزه کریپتوکارنسی.

جذب سرمایه‌گذاری خارجی در این حوزه.

مزایای این طرح

شفافیت و پیش‌بینی‌پذیری: با تدوین قوانین شفاف و ایجاد یک نهاد تنظیم‌گر مستقل، سرمایه‌گذاران و کسب‌وکارها می‌توانند با اطمینان بیشتری در این حوزه فعالیت کنند.

جذب سرمایه‌گذاری: ایجاد یک محیط قانونی و امن، می‌تواند به جذب سرمایه‌گذاری خارجی و داخلی در حوزه کریپتوکارنسی کمک کند.

توسعه فناوری: سرمایه‌گذاری در زیرساخت‌ها و حمایت از نوآوری، به توسعه فناوری بلاکچین و ایجاد محصولات و خدمات نوین کمک خواهد کرد.

ایجاد اشتغال: رشد صنعت کریپتوکارنسی می‌تواند به ایجاد فرصت‌های شغلی جدید و توسعه اقتصاد دیجیتال کمک کند.

افزایش رقابت‌پذیری: با توسعه فناوری بلاکچین و کریپتوکارنسی، ایران می‌تواند در رقابت جهانی در حوزه فناوری اطلاعات و ارتباطات حرفی برای گفتن داشته باشد.

چالش‌ها و راهکارها

مقاومت برخی نهادها: برخی نهادها ممکن است در برابر تغییر و پذیرش فناوری‌های جدید مقاومت کنند. برای رفع این مشکل، باید با این نهادها تعامل سازنده داشته و مزایای این فناوری را برای آن‌ها تشریح کرد.

خطرات امنیتی: فناوری بلاکچین نیز مانند هر فناوری دیگری، دارای برخی مخاطرات امنیتی است. برای مقابله با این مخاطرات، باید اقدامات امنیتی لازم در نظر گرفته شود.

نوسانات شدید قیمت: نوسانات شدید قیمت کریپتوکارنسی‌ها، یکی از چالش‌های اصلی این بازار است. برای مدیریت این نوسانات، می‌توان از مکانیسم‌های مختلفی مانند قراردادهای هوشمند استفاده کرد.

نتیجه‌گیری

با اتخاذ یک رویکرد جامع و متوازن، می‌توان از پتانسیل‌های بالای فناوری بلاکچین و کریپتوکارنسی برای توسعه اقتصاد دیجیتال ایران استفاده کرد. ایجاد یک چارچوب قانونی شفاف، حمایت از نوآوری و سرمایه‌گذاری و توسعه زیرساخت‌های لازم، از جمله مهم‌ترین گام‌هایی هستند که در این مسیر باید برداشته شوند.

نقش دیجی‌پی در تسهیل فرآیند اعطای تسهیلات

مدیرعامل دیجی‌پی، گفت: فین‌تک‌ها می‌توانند به بهبود رتبه اعتباری افراد کمک کرده و فرآیند اعطای تسهیلات را با استفاده از داده‌های جایگزین به جای روش‌های سنتی بهبود بخشند. هومن امینی، مدیرعامل دیجی‌پی، در جایگاه یکی از چهره‌های برجسته حوزه فین‌تک، به عنوان سخنران در رویداد فیناپ حضور داشت. او در این سخنرانی به بررسی نقش فین‌تک‌ها در بهبود شمولیت مالی و چالش‌های پیش روی این صنعت در ایران پرداخت. امینی تأکید کرد که فین‌تک‌ها می‌توانند به بهبود رتبه اعتباری افراد کمک کرده و فرآیند اعطای تسهیلات را با استفاده از داده‌های جایگزین به جای روش‌های سنتی بهبود بخشند. وی به تجربه دیجی‌پی در این زمینه اشاره کرد و توضیح داد که با تحلیل رفتار آنلاین کاربران، توانسته‌اند اعتماد بیشتری را در نظام بانکی نسبت به کنترل ریسک ایجاد کنند. همچنین امینی به این نکته اشاره کرد که در ایران دو نوع بانک وجود دارد؛ بانک‌هایی که نوآوری را در هسته اصلی خود قرار داده‌اند و بانک‌هایی که ارتباط بهتری با

فین‌تک‌ها برقرار کرده‌اند. سخنرانی او فرصت مناسبی برای شرکت‌کنندگان فیناپ بود تا با روندهای نوین و راهکارهای پیشرفته در حوزه فناوری‌های مالی آشنا شوند.

تسویه مبادلات فرامرزی توسط پول دیجیتال بانک مرکزی

دفتر مطالعات اقتصادی مرکز پژوهش‌های مجلس شـورای اسلامی، معتقد است: یکی از مسیرهایی که بانک های مرکزی کشورهای مختلف به سمت فعال سازی آن حرکت کرده‌اند، اسـتفاده از پول دیجیتال بانک مرکزی برای پرداخت های فرامرزی است و در صورت فعال سازی این سازوکار، کشور توان استفاده از ابزاری رسمی برای تسویه بخش مهمی از تعاملات تجاری خود را خواهد داشت.

دفتر مطالعات اقتصادی مرکز پژوهش‌های مجلس شورای اسلامی در گزارشی با عنوان «پول دیجیتال بانک مرکزی ۳. تسویه مبادلات فرامرزی» آورده است که هرگونه تعامل تجاری، همواره پس از تعیین سازوکار تسویه مالی صورت می‌پذیرد. در تعاملات تجاری درون سرزمینی، طرفین معمولاً بر مبنای پول قانونی و با استفاده از ابزارهای مالی توسعه داده شده توسط نظام بانکی کشورشان به تعهدات مالی خود عمل می کنند. در این حالت با توجه به‌قرار داشتن طرفین تعامل تجاری در کشوری یکسان و اعتماد آنها به پول و ابزارهای مالی ملی، هیچ‌گونه در سازوکار تسویه رخ نمی‌دهد، اما در تعاملات تجاری فرامرزی با توجه به قرارگیری طرفین تعامل تجاری در کشورهای مختلف، تسویه تعامل تجاری با پیچیدگی‌های زیادی همراه است.

این گزارش بیان می کند که ازآنجاکه پرداخت فرامرزی قلب تپنده تجارت خارجی است، در طول تاریخ سازوکارهای مختلفی برای تسهیل و یکپارچه سازی هرچه بیشتر آن صورت گرفته است. تا پیش از پیدایش بروات و پول‌های کاغذی، فلزات اساسی همچون طلا و نقره، مهم‌ترین واسطه تعاملات تجارت خارجی و تهاتر به‌عنوان مهمترین ابزار مالی شناخته می‌شـد. با توسعه فناوری اطلاعات و ارتباطات و گسترش بانکداری به‌شکلی که امروزه شاهد آن هستیم، نظام پرداخت فرامرزی نیز دچار تحولات بنیادینی شد. به‌طوری که نظام پرداخت فرامرزی امروزه بر پایه دو ستون بانک‌های کارگزار و ارزهای جهان روا استوار است. شایان‌ذکر است که پل ارتباطی بین این دو ستون برای تسهیل ارتباطات فی‌مابین بانک‌های کارگزار پیام رسان مالی سوئیفت است.

این گزارش مطرح می کند که هرچند که بانکداری کارگزاری و ابزارهای توسعه داده شده در این بستر دستاورد قابل توجهی در تسهیل تجارت خارجی داشته‌اند، اما استفاده از این نظام پرداخت نیز با چالش‌هایی همراه است. باتوجه به گزارش بانک تسویه بین‌المللی، تبادل پیام تراکنش فرامرزی بین دو بانک کارگزار حدود پنج دقیقه زمان می‌برد، اما تسویه نهایی با توجه به زنجیره بانک‌های کارگزار، بررسی انطباق با قوانین، پردازش اطلاعات، مناطق زمانی و... بین یک تا پنج روز طول می کشد.

این گزارش ادامه می‌دهد که اولین چالش این سازوکار پرداخت، سرعت پایین آن در مقایسه با سازوکارهای پرداختی همچون رمزدارایی هاست. چالش دیگر مربوط به هزینه‌های انجام تراکنش است. تخمین هزینه تراکنش‌های عمده فروشی کار پیچیده‌ای است، اما به‌صورت کلی هزینه هر تراکنش بسته به تعداد بانک‌های کارگزار حاضر در زنجیره متغیر است. برای مثال متوسط هزینه پرداخت خرده فروشی از کمتر از دو درصد در اروپا تا بیش از هفت درصد در آمریکای لاتین متغیر بوده، این در حالی است که میانگین هزینه جهانی ارسال حواله‌ها ۶.۳۸ درصد مبلغ تراکنش است.

این گزارش بیان می کند که چالش دیگری که اهمیت بیشـتری از دو چالش سرعت و هزینه دارد، ریسـک تمرکز اسـت. عمده پرداخت‌های فرامرزی با استفاده از پیام رسان سـوئیفت و مبتنی بر دو ارز دلار و یورو صورت می‌پذیرد. این تمرکز نظام پیام رسانی و ارزی موجب شده‌اسـت تا کشورهای دارای سلطه بر نظام پولی جهانی، علاوه بر منتفع شدن از جهان‌روایی ارز خود، با استفاده از نظم این بستر بر دو گلوگاه اساسی نظام پرداخت فرامرزی حاکم شـوند. به‌عبارت دیگر، ازآنجاکه نظام پرداخت فرامرزی در جهان عمدتاً مبتنی بر نظام بانکداری کارگزاری یا ارزهای جهان‌روا و نظام پیام‌رسانی سوئیفت است، این امکان برای کشورهای دارای سلطه فراهم شده‌است تا از انجام تراکنش‌هایی مغایر با اهداف خود جلوگیری کنند. برای مثال تحریم‌های مالی اعمالی به برخی کشورها از جمله ایران، کره‌شمالی، ونزوئلا، روسیه و کوبا از مصادیق این ریسک تمرکز است.

در این گزارش آمده اسـت که با پایدار شدن هرچه بیشتر سلطه پولی دلار، کشورهای مختلف با هدف کاهش وابستگی نظام پرداخت خود به نظام بانکداری کارگزاری سعی در ارائه سـازوکارهای نوینی همچون اتحادیه‌های پولی (یورو)، اتحادیه‌های تسویه دو یا چندجانبه (اتحادیه پایاپای آسیایی) و... کردند.

این گزارش توضیح می‌دهد که پس از ظهور بیت کوین و معرفی فناوری پایه آن یعنی زنجیره بلوک که یکی از انواع دفاتر کل توزیع شده‌است، بانک‌های مرکزی سعی در ارائه شـکل دیگری از پول کردند. آنها با انگیزه‌های گوناگونی همچون شمول مالی، تحکیم حاکمیت پولی و بهبود روش‌های پرداخت به‌سمت مطالعه و پیاده سازی پول دیجیتال بانک مرکزی حرکت کردند.

این گزارش ادامه می‌دهد که یکی از مسیرهایی که بانک‌های مرکزی کشورهای مختلف به‌سـمت فعال سازی آن حرکت کرده‌اند، اسـتفاده از پول دیجیتال بانک مرکزی برای پرداخت‌های فرامرزی است. مطابق گزارش بانک تسویه بین‌المللی سه حالت برای فعال سازی این ظرفیت قابل تصور است. هر یک از این حالت‌ها، فرصت‌ها و چالش‌هایی برای پیاده سازی به‌همراه دارد که باتوجه به اقتضائات خاص هر کشور، کشورها به‌سمت پژوهش و پیاده سازی در خصوص یک یا چند حالت از آن حرکت کرده‌اند.

این گزارش مطرح می کند که مطابق گزارش بانک تسویه بین‌المللی، نتایج پروژه‌های انجام شده نشان می‌دهد استفاده از پول دیجیتال بانک مرکزی برای پرداخت‌های فرامرزی توان کاهش مدت انجام تراکنش به ۱۰-۳۰ ثانیه و هزینه انجام آن به یک درصد مبلغ تراکنش را داراست. البته هر یک از حالات پیاده سازی پیچیدگی‌های خاص خود را دارند و باتوجه به مقیاس‌پذیری، توزیع یافتگی و امنیت شبکه اتصالات، سرعت و هزینه انجام تراکنش‌ها می‌تواند متغیر باشد، اما همه مدل‌ها حاکی از برتری نسبی این ابزار پرداخت نسبت به شبکه بانک‌های کارگزار دارد. به‌علاوه مهمترین فرصت برآمده از این ابزار امکان تسویه معاملات فرامرزی در ارزهای محلی است.

این گزارش بیان می کند که در صورت فعال سـازی این سازوکار، کشور توان استفاده از ابزاری رسـمی برای تسـویه بخش مهمی از تعاملات تجاری خود را خواهد داشت. به‌عبارت دیگر کشور می‌تواند در تسویه بخشی از تعاملات تجاری خود به ریال تکیه کند و واسطه گری دلار را کنار زند، هرچند که در میان مدت همچنان ارزش‌گذاری بر مبنای یکی از ارزهای جهان روا باقی خواهد ماند.

در این گزارش مطرح می‌شـود که پس از تهدید به تحریم بانک‌های کارگزار مرتبط با ایران، نظام پرداخت جمهوری اسلامی ایران از نظام پرداخت رسمی فاصله گرفته و عمده تسویه‌های تجاری کشور با اسـتفاده از شرکت‌های پوششی صورت می‌پذیرد. هرچند که مقامات ذیربط تلاش‌هایی برای فعال‌سازی برخی ابزارهای پرداخت رسمی همچون پیمان‌های پولی داشته‌اند، اما به‌دلایل سیاسی – اقتصادی نوعاً این تلاش‌ها راه به جایی نبرده‌اند. این گزارش پیشنهاد می‌دهد که بانک مرکزی به‌عنوان متولی توسعه و تأمین نظام پرداخت فرامرزی کشور، با استفاده از ظرفیت جامعه علمی و نخبگانی کشور و همکاری با شرکت‌های دانش بنیان خصوصی اقدام به تحقیق و توسعه برای فعال‌سازی این ابزار در هر یک از سه حالت پیشنهادی کند. در همین راستا، مشارکت فعال در پروژه‌هایی که با حالات مختلف در حال تلاش برای این سازوکار هستند توصیه می‌شود. همچنین باید توجه داشت که فعال‌سازی این سازوکار، نیازمند جلب‌اعتماد طرفین تجاری کشور است و از این رو نیازمند سطح بالایی از دیپلماسی به‌ویژه دیپلماسی اقتصادی است. ازاین‌رو، بهتر است بانک مرکزی با مشارکت فعال در پروژه‌های مختلف برای فعال‌سازی این ابزار پرداخت فرامرزی تلاش ویژه ای انجام دهد.

صنعت ارزهای دیجیتال مملو از کلاهبرداران و فریب‌کاران است

رئیس کمیسیون بورس و اوراق بهادار آمریکا می‌گوید: صنعت ارزهای دیجیتال مملو از کلاهبرداران، فریب‌کاران و دغل‌کاران است ولذا سرمایه‌گذاران در سراسر جهان پول زیادی را از دست داده‌اند؛ چراکه شرکت‌های کریپتو از قوانین پیروی نمی‌کنند.

گری گنسلر، رئیس کمیسیون بورس و اوراق بهادار آمریکا، می‌گوید «سرمایه‌گذاران در سراسر جهان پول زیادی را از دست داده‌اند» به این دلیل که شرکت‌های کریپتو از قوانینی که این نهاد برای اجرای آنها تلاش می‌کند، پیروی نمی‌کنند.

این اظهارات در حالی مطرح می‌شود که این شرکت‌ها، میلیون‌ها دلار خرج کمک‌های سیاسی می‌کنند تا بر نتیجه انتخابات ماه نوامبر آمریکا تاثیر بگذارد، با این امید که قوانین آینده به نفع آنها باشد.

ترامپ با وعده‌هایی مانند تبدیل آمریکا به «پایتخت رمز ارز در جهان» و ایجاد «ذخیره ملی استراتژیک بیت‌کوین» مانند ذخایر طلای دولت آمریکا، به دنبال جلب آرای علاقه‌مندان به کریپتو است.

او یک کسب‌وکار جدید به نام «ورلد لیبرتی فایننشال» در حوزه ارزهای دیجیتال راه‌اندازی کرد و هر چند جزئیات زیادی درباره آن ارائه نداد، اما گفت: «فکر می‌کنم کریپتو یکی از آن کارهایی است که باید انجام دهیم.»

این چرخش بزرگی نسبت به سه سال پیش است که او بیت‌کوین را چیزی «شبیه به یک کلاهبرداری» و تهدیدی برای دلار آمریکا می‌دانست.

علاقه جدید ترامپ در تضادی آشکار با دولت جو بایدن است که کامالا هریس در مقام معاون ریاست جمهوری در آن حضور دارد. کاخ سفید در سال‌های اخیر سرکوب گسترده‌ای علیه شرکت‌های کریپتو به راه انداخته است.

در ماه مارس، سم بنکمن-فرید، بنیان‌گذار و مدیرعامل سابق اف‌تی‌اکس، به اتهام کلاهبرداری به ۲۵ سال زندان محکوم شد. او میلیاردها دلار از مشتریان شرکت در سراسر جهان سرقت کرد و بسیاری از آن‌ها هنوز در تلاش برای پس گرفتن پول خود هستند

در ماه آوریل هم چانگ‌پنگ ژائو، بنیان‌گذار شرکت بایننس، بزرگ‌ترین صرافی ارز دیجیتال جهان، به چهار ماه زندان محکوم شد و شرکت او ۳/۴ میلیارد دلار جریمه پرداخت کرد. در جریان رسیدگی به پرونده‌ای که وزارت دادگستری آمریکا علیه او باز کرد، او اقرار کرد که به مجرمان، کودک‌آزاران و تروریست‌ها اجازه استفاده از این پلتفرم برای پولشویی را داده است،

کمیسیون بورس و اوراق بهادار آمریکا نیز پرونده‌ای علیه بایننس در دادگاه دارد. این پرونده یکی از ۴۶ موردی است که این نهاد مالی در سال گذشته علیه شرکت‌هایی که سعی در کسب سود از این فناوری نوظهور داشته‌اند، به جریان انداخته است.

گنسلر می‌گوید: «این حوزه‌ای است که به وجود آمده، و فقط به این دلیل که دارایی‌های دیجیتال خود را در سیستم حسابداری جدیدی ثبت می‌کنند، [به اشتباه] می‌گویند <نمی‌خواهیم از قوانین تثبیت‌شده و قدیمی پیروی کنیم>.»

او توضیح می‌دهد قوانینی که شرکت‌ها را ملزم می‌کند تا اطلاعات مشخصی را با عموم به اشتراک بگذارند، از زمان تاسیس کمیسیون بورس و اوراق بهادار، برای محافظت از سرمایه‌گذاران برقرار بوده است.

این قوانین به سال ۱۹۳۴ بازمی‌گردد، بعد از سقوط مشهور وال‌استریت در سال ۱۹۲۹ که آغازگر رکود بزرگ بود.

گنسلر می‌گوید: «کریپتو فقط بخش کوچکی از بازارهای سرمایه در آمریکا و جهان است، اما می‌تواند اعتماد سرمایه‌گذاران عادی به بازارهای سرمایه را تضعیف کند.»

در حالی که طرفداران کریپتو استدلال می‌کنند این فناوری راهی سریع، ارزان و امن برای انتقال وجوه ارائه می‌دهد، نتایج یک نظرسنجی بانک مرکزی آمریکا نشان می‌دهد تعداد آمریکایی‌هایی که از آن استفاده می‌کنند، از ۱۲ درصد در سال ۲۰۲۱ به هفت درصد در سال گذشته کاهش یافته است.

کامالا هریس درباره ارزهای دیجیتال اظهار نظر چندانی نکرده است، اما چندی پیش یکی از مشاورانش گفت که او از «سیاست‌هایی که تضمین می‌کند فناوری‌های نوظهور و صنایع مرتبط با آن می‌توانند به رشد خود ادامه دهند» حمایت خواهد کرد.

بهره گیری دیجی‌پی از قابلیت های نوین هوش مصنوعی

مدیر اجرایی سوپراپلیکیشن دیجی‌پی، گفت: با قابلیت‌های جدید این اپلیکیشن و استفاده از هوش مصنوعی، دیجی‌پی به کاربران کمک می‌کند تا به سادگی و هوشمندانه‌تر نیازهای مالی و روزمره خود را مدیریت کنند.

در پنجمین سخنرانی از بیستمین رویداد فیناپ، حمیدرضا سعادتی، مدیر اجرایی سوپراپلیکیشن دیجی‌پی، به تشریح استراتژی‌های این شرکت برای کسب سهم بیشتر از بازار فینتک پرداخت.

سعادتی با اشاره به نسخه جدید اپلیکیشن دیجی‌پی، تأکید کرد که قابلیت‌های بسیار کاربردی و نوآورانه‌ای برای کاربران در نظر گرفته شده است. یکی از مهم‌ترین ویژگی‌های این نسخه جدید، استفاده از هوش مصنوعی (AI) برای ارائه محصولات و خدمات متناسب با نیازها و الگوهای رفتاری کاربران است. این تکنولوژی کمک می‌کند تا کاربران تجربه‌ای شخصی‌سازی‌شده‌تر و هدفمندتر در مدیریت مالی روزمره خود داشته‌باشند.

وی اپلیکیشن دیجی‌پی را به عنوان یک ابزار مالی آسان و کاربردی معرفی کرد که هدف آن بهبود و ساده سازی زندگی در سطوح مختلف از مدیریت مالی تا پرداخت و خرید خواهد بود.

سعادتی افزود که با قابلیت‌های جدید این اپلیکیشن و استفاده از هوش مصنوعی، دیجی‌پی به کاربران کمک می‌کند تا به سادگی و هوشمندانه‌تر نیازهای مالی و روزمره خود را مدیریت کرده و از خدمات پیشنهادی متناسب با نیازهای خود بهره‌مند شوند.

جنبش سم‌زدایی دیجیتال چیست؟

در حالـی که فن‌آوری مزایای بی‌شـماری برای ما به ارمغـان آورده، جنبش نوظهور سـم‌زدایی دیجیتال به ما یادآوری می‌کند گاهی لازم اسـت قدمی به عقب برداریم و زندگی را بدون صفحه نمایش تجربه کنیم، در واقع پاسخی است به نیاز فزاینده انسان‌ها برای بازیابی ارتباط با دنیای واقعی و خود واقعی‌شان.

نخستین رویداد جهانی باشگاه آفلاین، با ارائه راهکارهایی برای گذراندن ۲۴ ساعت در هفته، بدون استفاده از تلفن همراه برگزار شد. جنبشی جدید که در دنیای پرسرعت امروز می‌خواهد روند رو به افزایش زمان خیره شدن افراد به صفحه‌های نمایش گوشی‌ها را تغییر دهد.به گزارش گاردین، باشـگاه آفلاین، جنبشی نوپا با هدف «تعویض زمان صفحه نمایش با زمان واقعی»، اولین رویداد جهانی خود را برگزار کرد.

در این رویداد بیش از یک هزار نفر متعهد شده‌اند به مدت ۲۴ ساعت از دنیای دیجیتال فاصله بگیرند.بر اساس آمار، بزرگسالان بریتانیایی به جای پرداختن به سرگرمی‌های مفید و لذت‌بخش، به طور متوسط پنج ساعت در روز را صرف تماشای صفحه نمایش می‌کنند.

فیلیپ، مدیر برندینگ ۳۳ ساله از روتردام، یکی از شرکت‌کنندگان در این رویداد که روزانه تا ۱۴ ساعت را صرف تماشای صفحه نمایش گوشی می‌کند، به گاردین گفت: «من خسـته شده‌ام. فکر کردم شاید خوب باشـد که این کار را امتحان کنم تا کمی آرامش پیدا کنم.»

فیلیپ امیدوار است با این اقدام، به جای غرق شدن در دنیای مجازی و مقایسه خود با دیگران، بیشتر در لحظه زندگی کند و تعاملات رو در رو را افزایش دهد.

فرناندا گریس، مدیر اجتماعی ۳۸ ساله از بارسلونا، دیگر شرکت‌کننده این رویداد، گفت که امیدوار است «سم‌زدایی دیجیتال» به رویدادی فراگیر و مکرر، مشابه «ساعت زمین» تبدیل شـود. در رویداد ساعت زمین، مردم برای حفاظت از محیط زیست، ۶۰ دقیقه چراغ‌های غیرضروری را خاموش می‌کنند.

گریس معتقد است انجام جمعی چنین فعالیت‌هایی تاثیر بیشتری دارد و افراد را ترغیب می‌کند تا در آن مشارکت کنند.باشگاه آفلاین که اولین «پاتوق سم‌زدایی دیجیتال» خود را در ماه فوریه در آمستردام برگزار کرد، اکنون در شهرهایی چون پاریس، دبی و لندن نیز فعالیت می‌کند.در این پاتوق‌ها، شرکت‌کنندگان برای چند ساعت تلفن‌های همـراه خود را کنار می‌گذارنـد و به فعالیت‌هایی مانند مطالعه یا گفت‌وگو با یکدیگر می‌پردازند.

استرس کمتر، ارتباط بیشتر

ایلیا کنپل‌هالت، یکی از بنیانگذاران باشگاه آفلاین، گفته است شرکت‌کنندگان از تاثیر مثبت حتی چند ساعت دوری از فن‌آوری شگفت‌زده شده‌اند: «مردم احساس استرس کمتر و ارتباطی بیشتر با خود و دیگران را تجربه می‌کنند.»

این باشگاه علاوه بر برگزاری پاتوق‌های روزانه، تعطیلات آخر هفته‌ای را نیز در حومه هلند برگزار می‌کند که در آن شرکت‌کنندگان به محض ورود، تلفن‌های خود را تحویل می‌دهند.

به گفته کنپل‌هالت، مردم در این تعطیلات فضای ذهنی زیادی پیدا می‌کنند. برخی حتی پس از این تجربه فرصتی برای تامل در زندگی‌شان یافته و تصمیم به تغییر شغل خود گرفته‌اند.کنپل‌هالت که خود پس از تجربه یک آخر هفته بدون تلفن همراه، تصمیم به تاسـیس این باشـگاه گرفت، گفت: «متوجه شدم به اندازه کافی مطالعه نمی‌کنم، نمی‌نویسم و در طبیعت وقت نمی‌گذرانم. پس از آن تجربه، احساس خلاقیت و انرژی فوق‌العاده‌ای داشتم.»اگرچه باشگاه آفلاین هنوز به پایداری مالی نرسیده اما کنپل‌هالت و تیمش با اشتیاق به گسترش فعالیت‌های خود ادامه می‌دهند.

آن‌ها امیدوارند در آینده، فضاهای بدون تلفن در شهرها و حتی تعطیلات بدون تلفن را ببینند.این جنبش نوظهور سم‌زدایی دیجیتال، پاسخی است به نیاز فزاینده انسان‌ها برای بازیابی ارتباط با دنیای واقعی و خود واقعی‌شان.

در حالـی که فن‌آوری مزایای بی‌شـماری برای ما به ارمغـان آورده، این جنبش به ما یادآوری می‌کند گاهی لازم است قدمی به عقب برداریم و زندگی را بدون صفحه نمایش تجربه کنیم.

کسانی که می‌خواهند این تجربه را امتحان کنند، بهتر است با گام‌های کوچک شروع کنند. به عنوان مثال، می‌توانند هنگام صرف غذا با دوستان، تلفن همراه خود را کنار بگذارند یا از ساعت زنگ‌دار قدیمی به جای تلفن همراه برای بیدار شدن استفاده کنند. این تغییرات کوچک می‌تواند به تدریج به عادت‌های سالم‌تر و زندگی متعادل‌تر منجر شـود.هدف این جنبش نه حذف کامل فن‌آوری بلکه یافتن تعادلی سـالم بین دنیای دیجیتال و واقعی اسـت.با کنترل بیشتر بر زمان و توجه، می‌توانیم از مزایای فن‌آوری بهره‌مند شویم بدون آن که اسیر آن شویم. شاید وقت آن رسیده باشد که همه ما گاهی «آفلاین» شویم تا زندگی را به‌طور کامل‌تری تجربه کنیم.

سندرم لرزش خیالی یا توهم دیجیتال چیست؟

سندرم لرزش خیالی یا توهم دیجیتال زمانی رخ می‌دهد که فرد احساس می‌کند تلفن همراه اش در حال لرزیدن است در حالی که هیچ اعلان یا تماسی دریافت نکرده است، به عبارت دیگر، مغز ما توهمی از لرزش یا صدای اعلان گوشی را ایجاد می‌کند، بدون این که در واقعیت چنین اتفاقی افتاده باشد.

آیا تا به حال در طول روز احسـاس کرده‌اید گوشی‌تان زنگ خورده یا لرزیده است اما وقتـی آن را چـک کرده‌اید، هیچ تماس یا پیامی ندیده‌اید؟ این تجربه که اغلب آن را نادیده می‌گیریم، در واقع پدیده‌ای روانی به نام «سندرم لرزش خیالی» و نشان‌دهنده وابستگی ذهنی ما به گوشی های هوشمند است.

در عصر دیجیتال، گوشـی های هوشمند به بخشی جدایی‌ناپذیر از زندگی ما تبدیل شده‌اند.

این دستگاه‌های کوچک اما قدرتمند، امکاناتی باورنکردنی در اختیار ما قرار داده‌اند. از تسهیل ارتباطات گرفته تا دسترسی آسان به اطلاعات.

امـا آیا تا بـه حال فکر کرده‌اید این ارتباط نزدیک با تکنولوژی چه تاثیراتی بر روان ما می‌گذارد؟

سندرم لرزش خیالی چیست؟

به گزارش فربز، تحقیقات روان‌شناختی اخیر پدیده‌ای جدید را به نام «سندرم لرزش خیالی» (Phantom Vibration Syndrome) شناسایی کرده‌اند.

این سندرم زمانی رخ می‌دهد که فرد احساس می‌کند تلفن همراه اش در حال لرزیدن است در حالی که هیچ اعلان یا تماسی دریافت نکرده است.

به عبارت دیگر، مغز ما توهمی از لرزش یا صدای اعلان گوشی را ایجاد می‌کند، بدون این که در واقعیت چنین اتفاقی افتاده باشـد. مطالعه‌ای که در سـال ۲۰۱۲ در مجله کامپیوترها در رفتار انسان (Computers in Human Behavior) منتشر شد،

نشـان داد که نزدیک ۸۹ درصد از شرکت‌کنندگان، دست‌کم هر دو هفته یک بار این پدیده را تجربه می‌کنند.این آمار نشان می‌دهد «سندرم لرزش خیالی» بسیار رایج‌تر از آن چیزی است که تصور می‌کنیم.

علل سندرم لرزش خیالی

محققان توضیحات مختلفی برای این پدیده ارائه کرده‌اند که در بیشتر موارد ریشه در علوم اعصاب دارند.مطالعه‌ای در سـال ۲۰۱۰ در مجله بی‌اِم‌جی نشان داد مغز ما برای مقابله با حجم زیاد اطلاعات حسی، از فیلترها یا طرح‌واره‌هایی استفاده می‌کند.

این فرآیند که «جسـت‌وجوی هدایت‌شده فرضیه» نامیده می‌شود، می‌تواند منجر به تفسیر نادرست برخی محرک‌های حسی شود.مطالعه‌ای دیگر در سال ۲۰۱۳ سندرم لرزش خیالی را بخشی از مجموعه‌ای گسترده‌تر از مسائل مربوط به اضطراب فن‌آوری، موسوم به «iDisorders» طبقه‌بندی کرد.این نظریه بیان می‌کند که وابستگی بیشتر ما به دستگاه‌های هوشمند می‌تواند منجر به اضطراب و در نتیجه بروز چنین توهماتی شود.تحقیقی در سال ۲۰۱۵ نشان داد انتظار مداوم برای دریافت پیام، ایمیل یا اعلان جدید می‌تواند باعث ایجاد اضطراب و در نتیجه تجربه ارتعاشات خیالی شود.

تاثیرات گسترده‌تر

اگرچه سندرم لرزش خیالی به خودی خود ممکن است آسیبی جدی به همراه نداشته باشد اما نشان‌دهنده مساله‌ای بزرگ‌تر یعنی رابطه عمیق و فزاینده ما با فن‌آوری است. این پدیده نشـان می‌دهد دستگاه‌های هوشمند تا چه حد در زندگی روزمره ما ادغام شده‌اند.علاوه بر سندرم لرزش خیالی، پدیده‌های دیگری نیز در ارتباط با استفاده بیش از حد از گوشـی‌های هوشمند شناسایی شده‌اند که از جمله این پدیده‌ها می‌توان به «دوم‌اسکرواینگ» یا تمایل به جست‌وجوی مداوم اخبار منفی در شبکه‌های اجتماعی، «نُموفوبیا» یا ترس از دور بودن از گوشی همراه، پدیده «اضافه بار اعلان‌ها» که باعث اسـترس ناشی از دریافت حجم زیادی از اعلان‌ها می‌شود و «خستگی دیجیتال» که

ناشی از استفاده مداوم از دستگاه‌های دیجیتال است، اشاره کرد.این پدیده‌ها نشان‌دهنده تاثیرات گسترده‌تر فن‌آوری بر جامعه و زندگی روزمره ما هستند.

سندرم لرزش خیالی اگرچه به ظاهر بی‌ضرر به نظر می‌رسد اما زنگ خطری برای توجه بیشتر به رابطه ما با فن‌آوری است.این پدیده نشان می‌دهد که تکنولوژی چگونه می‌تواند بر ادراک حسی و روان ما تاثیر بگذارد.

به توصیه کارشناسان بهتر است برای کاهش این گونه اثرات، زمان‌هایی را برای «دیجیتال دی‌تاکس» یا پاک‌سازی دیجیتال در نظر بگیریم و استفاده از گوشی‌های هوشمند را محدود کنیم.آگاهی از این پدیده می‌تواند به ما کمک کند تا با آرامش بیشتری با آن برخورد کنیم.

افزایش حملات سایبری به زیرساخت‌های مخابراتی

نوکیـا در دهمین گزارش اطلاعات تهدید، از سـرعت گرفتن حملات سـایبری به زیرسـاخت های مخابراتی تحت تاثیر اسـتفاده مجرمان سایبری از هوش مصنوعی مولد و اتوماسیون، خبر داد.

بر اسـاس گزارش فایبر سیسـتم، گزارش نوکیا نشـان می‌دهد حملات سایبری به زیرساخت‌های مخابراتی در حال افزایش است، زیرا مجرمان سایبری به طور فزاینده‌ای از هوش مصنوعی مولد و اتوماسیون برای افزایش سرعت، حجم و پیچیدگی حملات خود استفاده می‌کنند.

رودریگو بریتو، رئیس بخش امنیت، خدمات ابری و شبکه نوکیا، می‌گوید: استفاده از هوش مصنوعی مولد و اتوماسیون برای اهداف پلید، منجر به افزایش قابلیت‌های بازیگران مخرب و پتانسیل تهدید می‌شود. یافته‌های گزارش نوکیا، نیاز اپراتورها، فروشندگان و تنظیم‌کننده‌ها را برای همکاری بیشتر برای توسعه اقدامات، شیوه‌ها و آگاهی قوی‌تر امنیتی شبکه تقویت می‌کند.

آمریکای شمالی به دلیل تمرکز و گستردگی زیرساخت های مخابراتی و شرکت‌های بزرگ در آمریکا، شاهد بیشترین تعداد حملات سایبری بوده است.

طبق یافته‌های کلیدی این گزارش، تعداد و دفعات حملات انکار سرویس توزیع شده (داس) که می‌توانند زیرساخت های مخابراتی را از ترافیک لبریز کرده و آن را غیرقابل اجرا کند، از یک یا دو مورد در روز، به بیش از ۱۰۰ مورد در روز در بسیاری از شبکه‌ها رسیده است. بات‌نت‌ها همچنان منبع اصلی حجم حملات داس هستند و حدود ۶۰ درصد از ترافیک داس از ژوئن سال ۲۰۲۳ تا ژوئن سال ۲۰۲۴ را تشکیل دادند.

بات‌نت، شـبکه ای از رایانه ها و دستگاه هایی است که توسط مجرمان سایبری برای انجام فعالیت های مخرب مانند حملات داس و سرقت اطلاعات شخصی و حساس مورد استفاده قرار می‌گیرند.

رشد حملات داس با گسترش صدها هزار دستگاه ناامن اینترنت اشیا، از یخچال‌های هوشـمند گرفته تا سـاعت‌های هوشـمند که ظرفیت پهنای باند گیگابیتی و چند گیگابیتی دارند، تقویت شده و گسترش بدافزار را تسهیل کرده است. رایج‌ترین بدافزار در شبکه‌های مخابراتی، رباتی است که دستگاه‌های آسیب‌پذیر با رمزگذاری ضعیف، گذرواژه یا نقص‌های طراحی را جست و جو می‌کند.

بنا بر «گزارش اطلاعات تهدید» نوکیا، آسـیای شرقی به دلیل افشای ناخواسته خود شرکت‌ها، با نشت قابل توجه داده ها روبرو است، در حالی که اروپای غربی با ترکیبی از جاسوسی سایبری و رخنه های امنیتی با انگیزه های مالی، دست و پنجه نرم می‌کند.

حتـی با وجود اینکه هوش مصنوعی مولد حملات سـریع‌تر و پیچیده‌تری را ممکن می‌سازد، ارائه‌دهندگان خدمات ارتباطی به طور فزاینده‌ای از فناوری مشابه برای بهبود زمان پاسخ و اثربخشی خود در برابر تهدیدات سایبری استفاده می‌کنند.

تهدید دیگر مربوط به «سیستم بر روی تراشه» (SoCs) است. این سیستم، مدارهای یکپارچه سخت افزاری هستند که اجزای رایانه ای را در خود جای داده اند که محاسبات و عملکرد شبکه را بالاتر برده و مصرف انرژی را به حداقل می‌رسانند. مجرمان سایبری به طور فزاینده ای «سیستم بر روی تراشه» را برای سوء استفاده از آسیب پذیری هـا در مولفه های مختلف، مانند رابطه ای میان افزار، نرم افزار و سخت افزار هدف قرار می‌دهند.

محاسبات کوانتومی نمونه دیگری از یک تهدید جدید در حال ظهور است. سازمان‌هایی مانند موسسه ملی استاندارد و فناوری(NIST) به کمک به شکل‌دهی استراتژی‌های امنیتی در سـطح جهانی ادامه می‌دهند. این سازمان اخیرا اولین الگوریتم‌هایی را که اجزای رویکرد جهانی را برای مقابله با تهدیدات بالقوه محاسـبات کوانتومی تشـکیل می‌دهند، استاندارد کرده است.

امنیت سایبری و هوش مصنوعی؛ چالش‌ها و فرصت‌ها

امروزه نبود امنیت کافی در فضای وب، خطر حملات سایبری، سرقت اطلاعات شخصی و مالی و اختلال در سیستم‌های حیاتی را به همراه دارد. امنیت سایبری با محافظت از داده‌ها و زیرساخت‌ها، به صنایع کمک می‌کند تا از تهدیدات مخرب در امان بمانند و اعتماد کاربران به خدمات دیجیتال را تقویت می‌کند. این حفاظت نه تنها امنیت شرکت‌ها، بلکه حریم خصوصی افراد را نیز تضمین می‌کند. در حال حاضر امنیت سایبری و هوش مصنوعی ارتباط زیادی با یکدیگر پیدا کرده‌اند.

چرا که هوش مصنوعی به سرعت در حال تسخیر جنبه‌های مختلف زندگی ماست؛ از صنعت و پزشکی گرفته تا دستیارهای صوتی و خودروهای خودران اما با گسترش کاربردهای هوش مصنوعی، امنیت سایبری در این حوزه به چالشی بزرگ تبدیل شده است. حملات سایبری می‌توانند به هوش مصنوعی آسیب زده و زیان‌های گسترده‌ای به زیرساخت‌ها، داده‌ها و حتی انسان‌ها وارد کنند. از این رو، امنیت سایبری و هوش مصنوعی باید همگام با یکدیگر برای محافظت از دنیای دیجیتال پیشروی کنند.

در این مطلب، به بررسی تأثیر هوش مصنوعی بر امنیت سایبری، نیازها و راهکارهای مقابله با تهدیدات سایبری با استفاده از هوش مصنوعی و کاربردهای خلاقانه و مخرب آن می‌پردازیم.

هوش مصنوعی چیست؟

هوش مصنوعی یا AI شاخه‌ای از علوم کامپیوتر است که با ایجاد ماشین‌هایی با عملکرد هوشمندانه، سروکار دارد؛ این شاخه از علوم کامپیوتر به طور گسترده به دو دسته کلی تقسیم می‌شود:

* **هوش مصنوعی قوی:** هوش مصنوعی قوی به ماشین‌هایی اشاره دارد که می‌توانند به طور کامل مانند انسان‌ها فکر و عمل کنند. این نوع از هوش مصنوعی، هنوز در مراحل اولیه توسعه خود قرار داشته و به طور کامل محقق نشده است.
* **هوش مصنوعی ضعیف:** هوش مصنوعی ضعیف به ماشین‌هایی اشاره دارد که می‌توانند در زمینه‌هایی خاص، عملکردهای هوشمندانه‌ای از خود نشان دهند. این نوع از هوش مصنوعی به طور گسترده در زمینه‌های مختلفی، مانند صنعت، مراقبت‌های بهداشتی، حمل‌ونقل و دولت استفاده می‌شود.

انواع هوش مصنوعی

هوش مصنوعی را می‌توان بر اساس انواع مختلف الگوریتم‌های یادگیری ماشینی طبقه‌بندی کرد. برخی از انواع رایج هوش مصنوعی عبارتند از:

*** یادگیری ماشین نظارت شده:**

یادگیری ماشین نظارت شده به ماشین‌هایی اشاره دارد که با استفاده از داده‌های نمونه، یاد می‌گیرند. این داده‌ها شامل ورودی‌ها و خروجی‌های مورد انتظار است. البته آکادمی همراه یک دوره جامع با عنوان یادگیری ماشین نظارت شده جمع آوری کرده که برای علاقمندان به این حوزه می‌تواند جذاب باشد.

*** یادگیری ماشین بدون نظارت:**

یادگیری بدون نظارت به ماشین‌هایی اشاره دارد که بدون داده‌های نمونه، یاد می‌گیرند. در این نوع یادگیری، ماشین‌ها بر اساس الگوها و روابط در داده‌ها، تعلیم داده می‌شوند. آکادمی همراه یک دوره جامع دیگر هم با عنوان یادگیری ماشین بدون نظارت برای علاقمندان به آشنایی با تکنیک‌ها و الگوریتم‌های مختلف یادگیری بدون نظارت طراحی کرده که می‌تواند بدین شکل اطلاعات خود در این حوزه را کامل کنید.

*** یادگیری تقویتی:**

یادگیری تقویتی به ماشین‌هایی اشاره دارد که با تجربه، یاد می‌گیرند. در این یادگیری، ماشین ها با انجام اقدامات و دریافت پاداش یا مجازات، یاد می‌گیرند.

هوش مصنوعی و امنیت سایبری ارتباطی عمیق و دو سویه دارند. از یک سو، هوش مصنوعی می‌تواند با تحلیل داده‌های حجیم و شناسایی الگوهای مشکوک، به بهبود سیستم‌های امنیتی و مقابله با تهدیدات سایبری کمک کند. الگوریتم‌های یادگیری ماشین می‌توانند به سرعت حملات را پیش‌بینی و به آن‌ها پاسخ دهند. از سوی دیگر، خود هوش مصنوعی نیز ممکن است هدف حملات سایبری قرار گیرد. مهاجمان می‌توانند از نقاط ضعف موجود در مدل‌های هوش مصنوعی سوءاستفاده کرده و با حملاتی مانند دستکاری داده‌ها یا حملات تداخلی، این سیستم‌ها را فریب دهند. بنابراین، تعامل نزدیک میان متخصصان هوش مصنوعی و امنیت سایبری برای حفاظت از این فناوری‌های حساس و بهبود امنیت آن‌ها ضروری است.

امنیت سایبری چیست؟

امنیت سایبری به مجموعه‌ای از اقدامات و فرآیندهایی اشاره دارد که برای محافظت از سیستم‌ها، شبکه‌ها و داده‌ها در برابر حملات سایبری طراحی شده‌اند.

حملات سایبری می‌تواند شامل موارد زیر باشد:

- نفوذ: نفوذ به سیستم یا شبکه برای دسترسی غیرمجاز به داده‌ها یا منابع.
- آسیب‌رسانی: آسیب رساندن به سیستم یا شبکه، مانند حذف یا تغییر داده‌ها یا قطع سرویس.
- جاسوسی: جمع آوری اطلاعات محرمانه از سیستم یا شبکه.

انواع حملات سایبری

حملات سایبری را می‌توان بر اساس انواع مختلف نقاط آسیب، طبقه‌بندی کرد. برخی از انواع رایج حملات سایبری عبارتند از:

- حملات مبتنی بر نرم‌افزار: در حملات مبتنی بر نرم‌افزار از نرم‌افزارهای مخرب مانند ویروس‌ها، بدافزارها و جاسوس‌افزارها برای حمله به سیستم‌ها یا شبکه‌ها استفاده می‌کنند.
- حملات مبتنی بر سخت‌افزار: حملات مبتنی بر سخت‌افزار از سخت‌افزارهای مخرب مانند بدافزارهای دستگاه‌های متصل به اینترنت (IoT) برای حمله به سیستم‌ها یا شبکه‌ها استفاده می‌کنند.
- حملات مبتنی بر شبکه: حملات مبتنی بر شبکه، از آسیب‌پذیری‌های شبکه برای حمله به سیستم‌ها یا شبکه‌ها استفاده می‌کنند.

هوش مصنوعی و امنیت سایبری دو حوزه مهمی محسوب می‌شوند که در سال‌های اخیر به سرعت در حال توسعه هستند. هوش مصنوعی می‌تواند به بهبود امنیت سایبری کمک کند، اما همچنین می‌تواند هدف حملات سایبری هم قرار گیرد. برای کاهش خطر حملات سایبری در هوش مصنوعی، نیاز به همکاری بین متخصصان هوش مصنوعی و امنیت سایبری وجود دارد.

برای مثال در صنعت مالی، بانک‌ها با استفاده از هوش مصنوعی به تشخیص تراکنش‌های مشکوک و پیشگیری از کلاهبرداری می‌پردازند. به عنوان نمونه، بانک جی‌پی مورگان با بهره‌گیری از الگوریتم‌های یادگیری ماشین، رفتار مشتریان را تحلیل و فعالیت‌های غیرعادی را شناسایی می‌کند. این سیستم‌ها قادرند تهدیدات را به سرعت کشف و پیش از وقوع حملات سایبری، آن‌ها را خنثی کنند. با این حال، این فناوری نیز از خطر حملات در امان نیست، زیرا مهاجمان ممکن است با دستکاری داده‌ها یا فریب الگوریتم‌ها، تلاش کنند سیستم‌های هوش مصنوعی را دچار اختلال کنند.

کاربردهای هوش مصنوعی در امنیت سایبری

هوش مصنوعی (AI) می‌تواند در امنیت سایبری برای بهبود تشخیص و پاسخ به تهدیدات، خودکارسازی فرآیندهای امنیتی و بهبود امنیت سیستم‌های هوش مصنوعی استفاده شود. در ادامه به توضیحات تکمیلی هر یک از این کاربردها می‌پردازیم.

۱. تشخیص و پاسخ به تهدیدات

یکی از کاربردهای اصلی هوش مصنوعی در امنیت سایبری، تشخیص و پاسخ به تهدیدات است. هوش مصنوعی می‌تواند برای تجزیه و تحلیل حجم عظیمی از داده‌های امنیتی، شناسایی الگوهای مشکوک و هشدار دادن به تیم‌های امنیتی استفاده شود.

برای مثال، هوش مصنوعی می‌تواند برای شناسایی حملات مبتنی بر هوش مصنوعی استفاده شود. این حملات از الگوریتم‌های یادگیری ماشینی برای هدف قرار دادن سیستم‌ها و شبکه‌ها استفاده می‌کنند و هوش مصنوعی می‌تواند برای شناسایی الگوهای مشکوک در داده‌های شبکه، مانند ترافیک غیرعادی یا استفاده از منابع غیر عادی، به کار گرفته شود. علاوه بر این، هوش مصنوعی می‌تواند برای خودکارسازی فرآیندهای پاسخ به تهدیدات هم استفاده شود تا تیم‌های امنیتی بتوانند سریع‌تر و کارآمدتر به حملات سایبری پاسخ دهند. برای مثال، هوش مصنوعی می‌تواند برای خودکارسازی فرآیندهای زیر استفاده شود:

- تجزیه و تحلیل هشدارهای امنیتی
- تولید گزارشات
- پیگیری حملات

۲. خودکارسازی فرآیندهای امنیتی

هوش مصنوعی می‌تواند برای خودکارسازی بسیاری از فرآیندهای امنیتی استفاده شود و در وقت و منابع صرفه‌جویی کرده و به بهبود کارایی امنیت سایبری موارد زیر کمک کند:

- مدیریت حساب‌های کاربری
- پشتیبانی از کاربران
- تجزیه و تحلیل حوادث امنیتی

۳. بهبود امنیت سیستم‌های هوش مصنوعی

هوش مصنوعی می‌تواند برای بهبود امنیت سیستم‌های هوش مصنوعی هم استفاده شود و خطر سوءاستفاده از این سیستم‌ها را کاهش دهد:

- شناسایی و رفع آسیب‌پذیری‌های امنیتی در سیستم‌ها
- آموزش مدل‌های یادگیری ماشینی ایمن
- نظارت بر رفتار سیستم‌های هوش مصنوعی

چالش‌های امنیت سایبری و هوش مصنوعی

حال بیایید طرف دیگر ماجرا هم بررسی کنیم؛ هوش مصنوعی در حال حاضر در طیف گسترده‌ای از حوزه‌های زیر استفاده می‌شود:

- صنعت: اتوماسیون فرآیندها، بهبود بهره‌وری و افزایش ایمنی در صنایع مختلف مانند تولید، ساخت‌وساز و مراقبت‌های بهداشتی
- مراقبت‌های بهداشتی: برای تشخیص بیماری‌ها، توسعه داروها و بهبود کیفیت مراقبت‌های بهداشتی
- حمل‌ونقل: برای خودکارسازی خودروها، بهبود مدیریت حمل‌ونقل و لجستیک و افزایش ایمنی
- دولت: برای امنیت عمومی، مدیریت امور مالی و ارائه هوشمند خدمات دولتی

استفاده از هوش مصنوعی در حوزه‌های بالا می‌تواند مزایای زیادی به همراه داشته باشد، اما همچنین چالش‌هایی را در زمینه امنیت سایبری ایجاد می‌کند. چالش‌های امنیتی در حوزه‌هایی که از هوش مصنوعی استفاده می‌کنند با چالش‌های امنیت سایبری در سیستم‌های سنتی متفاوت است. برخی از این چالش‌ها عبارتند از:

•پیچیدگی: سیستم‌های هوش مصنوعی شامل الگوریتم‌های یادگیری ماشینی، مدل‌های داده و زیرساخت‌های محاسباتی پیچیده‌ای هستند که آن‌ها را به طعمه‌ای جذاب برای حملات سایبری تبدیل می‌کند.

•نوآوری: هوش مصنوعی حوزه‌ای در حال توسعه است و الگوریتم‌های یادگیری ماشینی جدید آن هم به طور مداوم در حال تغییر و به‌روزرسانی هستند؛ این نوآوری می‌تواند آن‌ها را در برابر حملات سایبری تضعیف کند.

•نبود شفافیت: الگوریتم‌های یادگیری ماشینی اغلب غیر شفاف هستند. این بدان معناست که درک عملکرد آن‌ها ممکن است دشوار باشد و نتوان بررسی کرد که چگونه ممکن است این الگوریتم‌ها تحت تاثیر حملات سایبری قرار گیرند.

•ضعف‌های امنیتی: هوش مصنوعی مانند هر سیستم دیگری ممکن است ضعف‌های امنیتی داشته باشند. این ضعف‌ها می‌توانند توسط مهاجمان برای نفوذ به سیستم‌ها و انجام حملات سایبری استفاده شوند.

اقدامات کلیدی برای تقویت امنیت سایبری در عصر هوش مصنوعی

سازمان‌ها و افراد می‌توانند اقداماتی را برای بهبود امنیت سایبری در حوزه‌هایی که از هوش مصنوعی استفاده می‌کنند، انجام دهند. برخی از این اقدامات عبارتند از:

•استفاده از بهترین شیوه‌های امنیت سایبری: سازمان‌ها باید از بهترین شیوه‌های امنیت سایبری برای محافظت از سیستم‌های هوش مصنوعی خود استفاده کنند. این شیوه‌ها شامل اقداماتی مانند استفاده از احراز هویت چند عاملی، رمزنگاری داده‌ها و آموزش کارکنان در زمینه امنیت سایبری می‌شوند.

•نظارت مداوم بر سیستم‌های هوش مصنوعی: سازمان‌ها باید سیستم‌های هوش مصنوعی خود را به طور مداوم برای شناسایی و پاسخ به تهدیدات سایبری نظارت کنند.

•به‌روز نگه داشتن سیستم‌های هوش مصنوعی: سازمان‌ها لازم است تا سیستم‌های هوش مصنوعی خود را به‌روز نگه دارند تا از آخرین پچ‌های امنیتی استفاده کنند.

با اتخاذ این اقدامات، سازمان‌ها و افراد می‌توانند از سیستم‌های هوش مصنوعی خود در برابر حملات سایبری محافظت کنند.

آشنایی با امنیت سایبری و هوش مصنوعی

در پایان باید گفت که هوش مصنوعی می‌تواند به تشخیص و پیش‌گیری از حملات سایبری، تحلیل و پاسخگویی به تهدیدات و ارتقای مهارت‌های انسانی کمک کند. در مقابل هم ممکن است به‌عنوان ابزاری برای انجام حملات سایبری، ایجاد تقلب و فریب و اختلال در سیستم‌های حساس استفاده شود. پس برای بهره‌برداری از هوش مصنوعی برای امنیت سایبری، لازم است که چالش‌هایی مانند کمبود داده‌های کافی و معتبر، نیاز به همکاری و مسائل اخلاقی و قانونی حل شوند.

هوش مصنوعی می‌تواند هم به‌عنوان ابزار و هم به‌عنوان تهدید عمل کند؛ برای استفاده بهینه و امن از هوش مصنوعی برای امنیت سایبری، لازم است که چالش‌های موجود را شناسایی و راه‌حل‌های مناسب ارائه شوند. در واقع هوش مصنوعی می‌تواند شریکی قدرتمند برای افزایش امنیت سایبری باشد، البته به شرطی که با دقت و مسئولیت‌پذیری از آن استفاده شود.

بررسی ویژگی های آیفون SE ۴ اپل

با عرضه ســری آیفون ۱۶ ، بازار خرید و استفاده از این گوشی جدید هم داغ شده، اما ممکن اســت عده‌ای به فکر آینده باشند، اما آینده به معنای آیفون ۱۷ نیست، آیفون بعدی در واقع باید SE ۴ باشد.

این آیفون که به نظر می‌رســد در بهار ســال آینده عرضه شــود، جدیدترین نسخه از آیفون‌های سری SE محسوب می‌شود و حدود شش ماه تا دیدن آن فاصله داریم. این جدیدترین به روزرسانی آیفون SE از سه نسخه اخیر است و احتمالاً شاهد اصلاحات زیادی در iPhone SE ۲۰۲۵ خواهیم بود.

آیفون SE ۲۰۲۲ یا به عبارتی نسل سوم این مدل در سال ۲۰۲۲ به بازار عرضه شد و با وجود تمام انتقادات و مشکلاتی که به طراحی قدیمی این گوشی وارد بود، جلب توجه کاربران و علاقمندان را به خود اختصاص داد.

شرکت اپل از زمان عرضه آیفون SE ۲ در سال ۲۰۲۰ به طراحی آیفون ۸ پایبند بود. آخرین نسخه از گوشی ارزان قیمت آیفون، یعنی همین آیفون SE ۲ که سال ۲۰۲۲ عرضه شد، همان نمایشگر ۴.۷ اینچی آیفون ۸ با لبه‌های گرد و دکمه هوم را داشت.

در واقع، آیفون‌های SE از نظر طراحی همان آیفون ۸ ولی از نظر امکانات و سخت‌افزارها، مدرن‌ترند، اما به نظر می‌رسد آیفون SE ۲۰۲۵ طراحی جدیدتری داشته باشد و سنت‌ها را تغییر دهد.

آیفون SE ۴ احتمالاً بهار ۲۰۲۵ روانه بازار می‌شود و انتظار می‌رود شاهد تغییرات زیادی در نســل جدید این گوشی مقرون‌به‌صرفه باشیم. این گوشی احتمالاً دارای نمایشگر OLED است و از Apple Intelligence نیز پشتیبانی می‌کند.

ما انتظار داریم آیفون SE ۴ از نظر طراحی، به آیفون ۱۴ شباهت داشته باشد. چیزایی که انتظار داریم ایناســت: صفحه نمایش ۶.۱ اینچی OLED، طراحی لبه‌های تخت، FaceID و بریدگی کوچیک مربوط به دوربین سلفی. البته فکر می کنیم هنوز هم اپل ترجیح می دهد از یک دوربین در قاب پشت SE جدید استفاده کند.

شــایعات زیادی در مورد نسخه جدید آیفون SE منتشر شده است که حتی در یکی از این شایعات گفته می‌شود که نسل بعدی آیفون SE دارای دکمه اکشن خواهد بود. باید به یاد داشته باشید که این دکمه اولین بار در آیفون ۱۵ پرو معرفی شد و اکنون در تمامی گوشی‌های سری آیفون ۱۶ وجود دارد.

برخلاف آیفون ۱۴ و آیفون SE ۲۰۲۲ که به پورت لایتنینگ مجهز شده بودند، انتظار می‌رود اپل از پورت USB-C برای دستگاه جدید SE استفاده کند. این موضوع بیشتر به خاطر قوانینی که اتحادیه اروپا وضع کرده و همه دســتگاه‌های دارای درگاه شــارژ را ملزم می‌کند تا از یک کانکتور یکپارچه USB-C برای دســتگاه‌های خود استفاده کنند

اپل سال گذشته در سری آیفون ۱۵ تصمیم به تغییر گرفت و برای اولین بار از پورت USB-C استفاده کرد و حالا آیفون SE ۴ به نظر می‌رسد جدیدترین دستگاه اپل باشد که به این پورت مجهز می‌شود. بنابراین به زودی می‌تونید آیفون SE جدید را با همان کابلی که برای شارژ iPad یا لپ‌تاپ استفاده می‌کردید، شارژ کنید.

اگر هنوز چیزی درمورد قابلیت‌های هوش مصنوعی اپل نمی‌دانید خوب است یادآوری کنیم که این قابلیت می‌تواند نوتیفیکیشن‌های گوشی را خلاصه و اولویت‌بندی کند، ایموجی‌هایی با توجه به متنی که می‌بینید بسازد و به ربات ChatGPT مجهز شده که هر سوالی داشته باشید به صورت مقاله و متن را به شما نشان می‌دهد.

طبق شــایعات، آیفون SE ۲۰۲۵ گران‌تر از نســل‌های قبلیش خواهد بود و احتمالاً قیمت SE ۲۰۲۵ اپل حدود ۴۹۹ دلار خواهد بود. با این حال، باید این واقعیت را قبول کنید که آیفون SE نسل بعد دیگر یک آیفون سطح پایین نیست و به مجموعه‌ای از قابلیت‌های جدید و مدرن مجهز شده که قیمت زیر ۵۰۰ دلار هنوز هم قیمت بسیار مناسبی برایش به حساب می‌آید.

آیا آیفون اسلیم ضخامت کمتری خواهد داشت؟

طبق گزارشــی جدید آیفون ۱۷ اسلیم با ضخامت کمتری عرضه می شود؛ نمایشگر TDDI جدید به اپل کمک می کند که اندازه آیفون را کاهش دهد و به ضخامت مورد نظر خود دست یابد.

شــرکت تایوانی «نواتک» (Novatek) اخیرا اعلام کرد نمایشگرهای او ال ای دی را با اســتفاده از فرایندی به نام «ادغام درایور لمســی و نمایشگر» TDDI آغاز خواهد کــرد

همانطور که نام این فرایند نشان می دهد، نمایشگر مذکور فناوری لایه حسگر لمسی را با درایور نمایشگر در یک واحد ترکیب می کند. هرچند این روند تغییری کوچک به نظر می رسد اما تاثیری قابل توجه بر ضخامت موبایل خواهد داشت. تولید کنندگان بــا خلاصی از یک لایه جداگانه می توانند چند میلیمتر را از کل ضخامت موبایل کم کنند

اکنون شایعاتی درباره آیفون ۱۷ ایر بسیار نازک شنیده می شود که قرار است به جای نسخه «پلاس» عرضه شود. نمایشگر TDDI جدید به اپل کمک می کند اندازه آیفون را کاهش دهد و به ضخامت مورد نظر خود دست یابد.

البته این امر قطعی نیست اما دیجی تایمز در گزارش خود اشاره می کند ممکن است اپل فناوری را نخست روی دستگاه های دیگر مانند آی پد های آتی یا اپل واچ ها آزمایش کند. حتی ممکن است آیفون یا آی پد تاشو از این فناوری نمایشگر بهره گیرند.

مزیت خرید جدیدترین تلفن هوشمند

یک استاد روانشناسی در دانشگاه باث اسپا معتقد است که آنچه معمولاً فراموش می کنیم این است که استفاده از تلفن های همراه هوشمند، فواید زیادی هم برای ما دارد، اما ما بیشتر روی نکات منفی تمرکز داریم، لذا همیشه باید به یاد داشته باشیم این‌ها وسایلی برای رفاه بیشتر هستند و به ما کمک می کنند و جنبه‌های خوبی هم در استفاده از آن‌ها وجود دارد.

شرکت گوگل به تازگی از مدل جدید گوشی هوشمند خود، گوشی پیکسل ۹ رونمایی کرد و هم‌زمان شرکت اپل هم گوشی آیفون ۱۶ را به نمایش گذاشت.

در ماه ژوئیه، شـــرکت سامسونگ جدیدترین گوشی تاشوی خود، مدل زد فلیپ ۶ و زد فولد ۶ را رونمایی کرد. شرکت هواوی با رونمایی از گوشی مدل میت اکس تی در چین سعی کرد عقب نماند. این گوشی دو بار تا می‌شود و می‌تواند صفحه نمایش را تا یک سوم کوچک کند.

درحالی‌که فروش گوشی‌های هوشمند در سراسر جهان کندتر است، پیام‌هایی که این شرکت‌ها برای بازاریابی می‌فرستند از قبل به‌مراتب خیره‌کننده‌تر شده است.

تیم کوک، رئیس شرکت اپل وعده داده آیفون ۱۶ بتواند تعریف جدیدی از قابلیت‌های یک گوشی هوشمند پیش رو بگذارد. حالا معنی حرفش هر چه باشد.

برایان راکوفسکی، معاون مدیریت محصولات گوگل از طراحی خیره‌کننده و زیبایی گوشی پیکسل ۹ حرف زده است اما آنچه به چشم من می‌آید همان مستطیل سیاه همیشگی است.

هم اپل و هم گوگل، روی ویژگی‌های هوش مصنوعی داخل گوشی‌های خود حساب باز کرده‌اند. مجیک ادیتور جدید گوگل می‌تواند عناصر ساخته شده باهوش مصنوعی را به عکس‌ها اضافه کند و همین‌طور می‌تواند بخش‌هایی از یک عکس را که دوست ندارید پاک کند.

اپل اینتلیجنس بخشی از آیفون ۱۶ است که شامل چت جی بی تی، ساخته شرکت اوپن ای آی می‌شود که حالا به دستیار دیجیتال سیری این گوشی‌ها اضافه شده است. بسیاری مدت‌ها بود می گفتند اپل باید چنین به‌روزرسانی انجام دهد.

آما آیا کسی همه این چیزهای جدید را خواسته بود؟

بن وود، کارشـــناس گوشی‌های هوشـــمند از شرکت تحقیقاتی سی سی اس اینسایت می‌گوید هرچند ویژگی‌های هوش مصنوعی اضافه شده به گوشی‌ها زندگی دیجیتال افراد را تا حدی آســـان‌تر می کنند، هوش مصنوعی در صدر لیست خواسته‌های کاربران قرار ندارد.

او می‌گوید: «فکر می‌کنم اکثر مردم می‌دانند چه خواسته‌هایی از گوشی هوشمند دارند. یکی از مهم‌ترین‌های خواسته‌ها دوربین بهتر برای گوشی است.»

طراحان گوشی هم از این خواسته خبردارند. معمولاً مشخصات فنی دوربین گوشی‌ها از مدلی به مدل جدید بهبود پیدا می کند. اما حتی این خصوصیت هم به‌تنهایی فروش بالا را تضمین نمی کند.

وود اضافه می کند: «آنچه مســـلم است این است که مردم گوشی‌های هوشمند خود را برای مدت طولانی‌تری نگه می‌دارند. در سال ۲۰۱۳، سالانه ۳۰ میلیون گوشی هوشمند فروخته می‌شد. امسال این رقم حدود ۱۳۵ میلیون خواهد بود.»

البتـــه بحران ادامه‌دار هزینه‌های زندگی هم بر تصمیم‌های مردم اثر دارد. هزینه محیط زیستی هر گوشی هوشمند، از جمله مواد و عناصر کمیابی که برای ساخت اجزا آن‌ها به کار می‌رود هم از نظرها دور نیست.

علاوه بر این، رویه رفتاری جدیدی که خصوصاً بین پدر و مادرها و جوان‌ترها برای دوری و کمتر استفاده کردن از گوشی‌های هوشمند رایج شده است در میزان استفاده از گوشی‌ها مؤثر بوده است. تعدادی از مدارس بریتانیا در حال بازنگری قوانین خود در مورد استفاده از گوشی‌های هوشمند در مدرسه هستند. تعدادی از مدرسه‌ها از قبل استفاده از گوشی هوشمند در مدرسه را ممنوع اعلام کرده بودند. به دانش‌آموزانی که این ترم تحصیل در کالج خصوصی ایتون را شروع کرده‌اند، گوشی‌هایی شبیه آنچه به گوشی‌های خنگ معروف شده‌اند، داده شده است. آن‌طور که شنیده‌ام، چندین موسسه آموزشی دیگر هم در بخش خصوصی و هم در بخش دولتی برنامه دارند این رویه را در پیش بگیرند.

شـــبکه تلفن همراه ای‌ای توصیه می کند کودکان زیر ۱۱ سال به‌هیچ‌وجه نباید گوشی هوشمند داشته باشند.

نوا ایســـت، از مدیران کارزار کودکی بدون گوشـــی هوشمند است. او از والدین و مدارس می‌خواهد با آن‌ها همکاری کنند و کمک کنند کودکان از سن بالاتری گوشی هوشمند داشته باشند.

او می‌گوید: «ما ضد تکنولوژی نیستیم. ما توقع داریم شرکت‌های بزرگ تکنولوژی ابزار و گوشی‌های مناسب کودکان تولید کنند. گوشی‌هایی که فقط ویژگی‌های ضروری برای یک تلفن را در خود دارند. مانند تماس گرفتن، پیامک فرستادن، گوش دادن به موسیقی و نقشه. ما از آن‌ها می‌خواهیم دیگر کارکردها را برای کودکان حذف کنند.»

دکتر ساشا لوچونی، محقق علمی در شرکت هوش مصنوعی هاگینگ فیس، می‌گوید فعلاً به نظر نمی‌رسد شرکت‌های تکنولوژی گوش شنوایی در مورد این نگرانی‌ها داشته‌اند.

او می‌گوید: «این روزها صحبت از روزه گرفتن و دوری از تکنولوژی بین کاربران رایج است اما خود تولیدکنندگان کاملاً در مسیر خلاف این خواسته در حرکت هستند.»

من این موضوع را با اپل، گوگل و سامســـونگ مطرح کردم. شـــرکت سامسونگ گفت: «کاربران سامسونگ می‌توانند نحوه استفاده از گوشی‌های گلکسی خود را بر اساس آنچه برایشان مناسب است تنظیم کنند. به‌عنوان مثال ویژگی‌های رفاه دیجیتال به کاربران اجازه می‌دهد انتخاب کنند از کدام ویژگی گوشی و برای چه مدت استفاده کنند. از جمله آن‌ها محدود کردن استفاده از صفحه نمایش است که اپلیکیشن مخصوصی می‌تواند میزان آن را تنظیم و محدود کند.»

یکی از شرکت‌هایی که به خواسته رو به رشد کاربران برای کاهش قابلیت‌های استفاده از گوشی هوشمند توجه کرده است، شرکت فنلاندی اچ ام دی است که هنوز سازنده اصلی گوشی‌های نوکیا است. آن‌ها ماه گذشته با همکاری شرکت متل یک گوشی جدید با ایده از باربی عرضه کردند. من این گوشی را امتحان کردم. می‌توان آن را با دو کلمه توصیف کرد: کاربردی و صورتی. مانند بسیاری از گوشی‌های ساده، روی آن هیچ اپلیکیشن، راه تماس با فروشـــگاه اپ و امکان سلفی گرفتن وجود ندارد. فقط یک بازی در آن وجود دارد. اگر بخواهید به موسیقی گوش بدهید، می‌توانید به رادیو اف ام متصل شوید.

شـــرکت سی سی اس اینسایت پیش‌بینی می کند که احتمالاً امسال در بریتانیا حدود چهارصد هزار تلفن ســـاده به فروش برسد. این میزان در حدی نیست که بتواند به این زودی‌ها آیفون را از جایگاه پرفروش‌ترین گوشی جهان پایین بیاورد اما بازار این گوشی‌ها بازار چندان بدی نیست.

من هم هفته گذشته میزان اســـتفاده از صفحه‌نمایش گوشی‌ام را بررسی کردم. میزان اســـتفاده من ۵ ســـاعت در روز بود. این یک علامت هشداردهنده بود. اما از جهاتی این تصویری واقعی نیست زیرا تلفن من ابزار کار من هم هست. وسیله‌ای است که از آن برای کارهای بانکی، خرید، مسیریابی، کنترل سلامت، پیگیری برنامه‌های خانوادگی، و البته بازی و شبکه‌های اجتماعی استفاده می کنم. پیت اچلز، استاد روانشناسی و ارتباطات علمی در دانشگاه باث اسپا که در مورد مسئله استفاده از صفحه نمایش مطالب زیادی نوشته است، می‌گوید: «آنچه معمولاً فراموش می کنیم این است که استفاده از گوشی‌های هوشمند، فواید زیادی هم برای ما دارد.»

او می‌گوید: «ما بیشتر روی نکات منفی تمرکز داریم. همیشه باید به یاد داشته باشیم این‌ها وسایلی برای رفاه بیشتر هستند و به ما کمک می کنند. جنبه‌های خوبی هم در استفاده از آن‌ها وجود دارد.»

محصولات جدید متا؛ از عینک های هوشمند تا واقعیت مجازی

مارک زاکربرگ از عینک های هوشمند Ray-Ban این شرکت رونمایی کرد، همچنین، هدست واقعیت مجازی ۳S با قیمت ۲۹۹ دلار به بازار عرضه می‌شود.

مدیرعامل متا، از عینک‌های هوشمند Ray-Ban این شرکت رونمایی کرد که طرحی زیبا و قابلیت‌هایی از جمله ترجمه همزمان دارند. همچنین، هدست واقعیت مجازی ۳S با قیمت ۲۹۹ دلار از ۱۵ اکتبر ۲۰۲۴ به بازار عرضه خواهد شد. متا با این فناوری‌های نوین، گام‌های بلندی به سوی آینده برداشته است.

متا، که پیشتر فیسبوک نام داشت، در سال ۲۰۲۱ به متا تغییر نام داد. متا همچنان بیشتر درآمد خود را از تبلیغات کسب می‌کند. در سه‌ماهه اخیر، ۹۸ درصد از درآمد ۳۹ میلیارد دلاری این شرکت از محل تبلیغات بوده است.

زاکربرگ در حال سرمایه‌گذاری همه‌جانبه روی هوش مصنوعی و نسل بعدی پلتفرم‌ها از جمله هدست‌های واقعیت مجازی و عینک‌های هوشمند است.

ورود به دنیای واقعیت مجازی با هدست‌های ۳S

یکی از محصولات جدید معرفی‌شده توسط زاکربرگ، هدست واقعیت مجازی مدل ۳S بود. این هدست با قیمت ۲۹۹ دلار عرضه خواهد شد که نسبت به مدل قبلی، Quest ۳، بسیار ارزان‌تر است.

با این حال، برخی کارشناسان بر این باورند که واقعیت مجازی هنوز نتوانسته به طور گسترده در میان مصرف‌کنندگان جا بیفتد. عمر اختر، تحلیلگر بنچمارکر، می‌گوید: «عینک‌های واقعیت مجازی هنوز در بازار مصرف‌کننده خیلی موفق نبوده‌اند.»

موفقیت غیرمنتظره عینک‌های Ray-Ban

در حالی که هدست‌های واقعیت مجازی هنوز نتوانسته‌اند توجه زیادی جلب کنند، عینک‌های هوشمند Ray-Ban یک موفقیت غیرمنتظره برای متا بوده‌اند.

این عینک‌ها با وزن سبک و طراحی شیک خود، جایگزین مناسبی برای هدست‌های

بزرگ هستند. ویژگی جذاب این عینک‌ها، قابلیت ترجمه همزمان است که به کاربران امکان می‌دهد در مکالمات زنده به زبان‌های مختلف صحبت کنند.

زاکربرگ در این رویداد اعلام کرد که متا موفق شده مشکلات مربوط به عرضه این عینک‌ها به دلیل تقاضای بالا را حل کند.

نگاهی به آینده با عینک‌های پیشرفته اوریون

در نهایت، زاکربرگ از یک نمونه اولیه از عینک‌های پیشرفته به نام اوریون رونمایی کرد. این عینک‌های هولوگرافیک بدون سیم بوده و تنها ۱۰۰ گرم وزن دارند. از ویژگی‌های منحصربه‌فرد این محصول، قابلیت کنترل دستگاه با سیگنال‌های مغزی است. با این حال، هنوز تاریخ مشخصی برای عرضه این عینک‌ها اعلام نشده است. زاکربرگ این محصول را «نگاهی به آینده» توصیف کرد.

معرفی روش جدید جست و جو از طریق فیلمبرداری توسط گوگل

گوگل قابلیت جدیدی عرضه کرده که به افراد امکان می دهد تا با ویدیو گرفتن در اینترنت جست و جو کنند؛ تمامی کاربران اندروید و آیفون در سراسر جهان اکنون می توانند با فعال کردن گزینه ای‌آی اورویوز، به این ویژگی دسترسی پیدا کنند، اما فعلا تنها از زبان انگلیسی پشتیبانی خواهد کرد.با کمک جست‌وجوی ویدیویی گوگل، کاربران می‌توانند دوربین گوشی‌شان را به سمت چیزی بگیرند، در مورد آن سوال بپرسند و نتایج جست‌وجو را دریافت کنند.تمامی کاربران سیستم‌عامل‌های اندروید و آیفون در سراسر جهان اکنون می‌توانند با فعال کردن گزینه AI Overviews (مرور هوش مصنوعی) در اپلیکیشن گوگل خود، به این ویژگی دسترسی پیدا کنند، اما فعلا تنها از زبان انگلیسی پشتیبانی خواهد کرد.این جدیدترین حرکت این شرکت بزرگ فناوری برای تغییر روش جست‌وجو در اینترنت از طریق استفاده از هوش مصنوعی است.این ویژگی سه ماه پس از اعلام اوپن ای‌آی، سازنده چت‌جی‌پی‌تی مبنی بر آزمایش قابلیت جست‌وجو با پرسیدن سوال از این چت‌بات، ارائه می‌شود.شرکت گوگل امسال ویژگی جدیدی را معرفی کرد که در آن نتایج جست‌وجوی تولید هوش مصنوعی بالای برخی جست‌وجوها نمایش داده می‌شوند. در ماه مه، این شرکت به دلیل ارائه برخی پاسخ‌های نادرست با انتقادهایی مواجه شد اما این جست‌وجو به مرور زمان بهتر و دقیق‌تر شده است.

جست‌وجوی ویدیویی گوگل

لیز ریده، رئیس جست‌وجوی گوگل، می‌گوید که این قابلیت جدید به افراد اجازه می‌دهد به‌راحتی درباره دنیای اطرافشان سوال بپرسند. او برای مثال گفت فردی را هنگام بازدید از آکواریوم تصور کنید که ممکن است بخواهد بداند که چرا برخی ماهی‌ها هماهنگ و باهم شنا می‌کنند. آن شخص به‌جای اینکه مجبور باشد برای یافتن اطلاعات درباره ماهی‌ها جست‌وجو و پرسش را تایپ کند، با ویژگی جدید می‌تواند دوربین گوشی را به سمت آن‌ها بگیرد، یک کلیپ کوتاه ضبط کند و سوالش را با صدای بلند بپرسد.

هوش مصنوعی گوگل ویدیو را تحلیل، ماهی‌ها را شناسایی و سپس سوال را با آن ترکیب می‌کند تا نتایج جست‌وجو ارائه شود.به عقیده کارشناسان، هوش مصنوعی به نقطه‌ای رسیده است که می‌تواند به صورت واقعی در زندگی روزمره انسان‌ها نقش تعاملی و نوآورانه داشته باشد و با تحلیل الگوها و عادات افراد، به شکل شخصی‌سازی‌شده و منحصربه‌فرد عمل کند.

روش‌های دیگر جست‌وجو در گوگل

گوگل علاوه بر این جست‌وجوی ویدیویی، چند به‌روزرسانی دیگر هم عرضه کرده است.از جمله اینکه نتایج جست‌وجوی خرید را بهبود بخشیده است، که اکنون بررسی اطلاعات و قیمت‌گذاری فروشندگان مختلف ممکن خواهد بود.این شرکت همچنین در حال معرفی رقیبی برای اپلیکیشن شناسایی موسیقی «شازم» (Shazam) اپل است. این ابزار رقیب که از طریق «حلقه جست‌جو» (Circle to Search) در دستگاه‌های اندرویدی قابل دسترسی است، به کاربران اجازه می‌دهد تا بدون خروج از اپلیکیشن، آهنگ‌ها را از یک وب‌سایت یا برنامه‌ای که در حال پخش است، شناسایی کنند.گوگل این ویژگی‌ها را در حالی ارائه می‌دهد که همچنان ۹۰ درصد بازار جهانی جست‌وجو را در اختیار دارد اما با رقبای سرسختی چون اوپن ای‌آی مواجه است که در ماه ژوییه اعلام کرد در حال آزمایش ویژگی جست‌وجو در چت‌جی‌پی‌تی است.

مالک تلگرام: امکان سوءاستفاده از این پلتفرم وجود دارد

پاول دورف، مدیرعامل پیام‌رسان تلگرام اذعان کرد که تلگرام بی‌نقص نیست و امکان سوءاستفاده از این پلتفرم وجود دارد، لذا این پیام‌رسان در صورت درخواست مقامات مسئول در کشورها، آدرس‌های آی‌پی و شماره تلفن کاربران را در اختیارشان خواهد داد.

دورف در تلگرام نوشت: «برای ممانعت بیشتر از سوءاستفاده مجرمان از موتور جستجوی تلگرام، شرایط خدمات و آیین‌نامه مربوط به حریم خصوصی خود را به روز کرده‌ایم تا اطمینان حاصل کنیم با قوانین جهانی هماهنگ هستند. ما به صراحت اعلام کرده‌ایم که آدرس‌های آی‌پی و شماره تلفن افرادی که قوانین ما را نقض می‌کنند به درخواست مقامات قانونی مربوطه می‌توانند فاش شوند.»

وی افزود: «طی چند هفته گذشته، گروهی از متخصصان، با استفاده از هوش مصنوعی، موتور جستجوی تلگرام را بسیار ایمن‌تر کرده‌اند. هیچ یک از مطالب مشکل‌سازی که در این موتور جستجو شناسایی کرده‌ایم، دیگر قابل دسترسی نیستند.»

دورف که اهل روسیه است، به ظن دست داشتن در جرایم مختلف «از جمله راه‌اندازی یک سکوی آنلاین که امکان تراکنش‌های غیرقانونی، پورنوگرافی کودکان، قاچاق مواد مخدر، کلاهبرداری و همچنین عدم ارائه اطلاعات به مقامات، پولشویی و ارائه خدمات رمزنگاری به مجرمان را فراهم می‌کند»، در پاریس بازداشت و پس از مدت کوتاهی با وثیقه ۵.۵ میلیون دلاری آزاد شد.

از جمله اتهامات دیگر پاول دورف خودداری از ارائه اسناد به مقاماتی است که درباره فعالیت‌های غیرقانونی در پیام‌رسان تلگرام تحقیق می‌کنند.

دورف که تابعیت فرانسه، روسیه، امارات متحده عربی و مجمع الجزایر سنت کیتس و نویس در دریای کارائیب را دارد تاکید کرده که بازداشتش «خطا» بوده است.

وی اذعان کرد که تلگرام «بی‌نقص» نیست و امکان سوءاستفاده از این پلتفرم وجود دارد، اما تلگرام اساسا با هدف «دفاع از حقوق اولیه مردم» تاسیس شده است.

ممنوعیت استفاده از شبکه های اجتماعی اعتیادآور برای کودکان کالیفرنیایی

به منظور مقابله با تأثیر منفی شبکه های اجتماعی بر کودکان، در کالیفرنیا مقرر شده تا از سال ۲۰۲۷، ارائه فیدهای اعتیادآور به کودکان در شبکه های اجتماعی بدون رضایت والدین ممنوع شود و ارسال نوتیفیکیشن ها در ساعات خاص و تنظیمات پیش فرض حساب های کودکان نیز محدود می‌شود.

از سال ۲۰۲۷، ارائه فیدهای اعتیادآور به کودکان در شبکه‌های اجتماعی بدون رضایت والدین در کالیفرنیا ممنوع خواهد شد.

این قانون جدید، که توسط فرماندار گوین نیوسام امضا شده، پس از اقدامات مشابه در نیویورک و یوتا، گامی دیگر در جهت مقابله با تأثیر منفی شبکه های اجتماعی بر کودکان است.

کالیفرنیا، به عنوان خانه برخی از بزرگترین شرکت‌های فناوری جهان، با تصویب این قانون یکی از پیشگامان در حمایت از کودکان در فضای دیجیتال می‌شود. این در حالی است که پیشنهادهای مشابه در سال‌های اخیر در این ایالت ناموفق بوده‌اند.

با این حال، در سال ۲۰۲۲، نیوسام قانونی را امضا کرد که پلتفرم‌های آنلاین را از استفاده سوء از اطلاعات شخصی کاربران، به ویژه کودکان، منع می‌کند.

نیوسام، می‌گوید: «هر والدی می‌داند که اعتیاد به شبکه‌های اجتماعی چه آسیب‌هایی به فرزندانشان وارد می‌کند - انزوا از تماس انسانی، استرس و اضطراب و ساعت‌ها وقت تلف‌شده. با این لایحه، کالیفرنیا به محافظت از کودکان و نوجوانان در برابر ویژگی‌های طراحی‌شده‌ای که این عادات مخرب را تغذیه می‌کنند، کمک می‌کند.»

این قانون ارسال نوتیفیکیشن‌ها در ساعات خاصی و تنظیمات پیش‌فرض حساب‌های کودکان را محدود می‌کند. با این حال، مخالفان نگران تأثیر آن بر حریم خصوصی و دسترسی بزرگسالان به محتوا هستند.

سناتور ایالتی نانسی اسکینر، نویسنده این قانون، می‌گوید: «شرکت های شبکه های

اجتماعی پلتفرم‌های خود را طوری طراحی کرده‌اند که کاربران، به ویژه کودکان ما را معتاد کنند. با تصویب این قانون، مجلس قانونگذاری کالیفرنیا پیام روشنی ارسال کرده است: وقتی شرکت های شبکه های اجتماعی اقدامی نمی‌کنند، مسئولیت ماست که از فرزندانمان محافظت کنیم.»

تایید استفاده بدون اجازه پلتفرم های اجتماعی از داده های کاربران

کمیسیون تجارت فدرال آمریکا افشا کرد که شبکه‌های اجتماعی و پیام‌رسان‌های اینستاگرام، واتس‌اپ، فیس‌بوک، تیک‌تاک، توییچ، یوتیوب، دیسکورد، اسنپ چت، ایکس و ردیت مقادیر عظیمی از داده‌های کاربران را جمع‌آوری و پردازش می‌کنند؛ در حالی که شفافیت یا کنترل کمی به کاربران ارائه می‌دهند و سیاست‌های مدیریت و نگهداری داده‌های این شرکت‌ها ناکافی است.

«کمیسیون تجارت فدرال ایالات متحده» (اف‌تی‌سی) اخیرا گزارشی منتشر کرد که نحوه مدیریت داده‌های کاربران توسط رسانه‌های اجتماعی، به‌ویژه با تمرکز بر استفاده از این داده‌ها در سیستم‌های هوش مصنوعی را مورد بررسی قرار می‌دهد.

اف‌تی‌سی دریافت که پلتفرم‌هایی مانند «متا» (اینستاگرام، واتس‌اپ و فیس‌بوک)، «تیک‌تاک»، «توییچ»، «یوتیوب»، «دیسکورد»، «اسنپ چت»، «ایکس»، و «ردیت» مقادیر عظیمی از داده‌ها را جمع‌آوری و پردازش می‌کنند، در حالی که شفافیت یا کنترل کمی به کاربران ارائه می‌دهند، و سیاست‌های مدیریت و نگهداری داده‌های این شرکت‌ها ناکافی است.

گزارش اف‌تی‌سی تأکید می‌کند که این پلتفرم‌ها از طریق فناوری‌های ردیابی، دلالان داده، و روش‌های دیگر داده‌های کاربران را اغلب بدون آگاهی یا رضایت آنها جمع‌آوری می‌کنند. این سازمان هشدار داد که در حالی که این شیوه‌ها برای شرکت‌ها سودآور هستند، خطرات قابل‌توجهی برای حریم خصوصی، آزادی و امنیت کاربران، مانند سرقت هویت و تعقیب، به وجود می‌آورند.

یکی از نگرانی‌های اصلی، شیوه‌های جمع‌آوری داده‌ها در ارتباط با کودکان و نوجوانان است، که موضوعی است که توجه بیشتری از سوی قانون‌گذاران آمریکایی به خود جلب کرده است. کنگره در حال بررسی لوایحی است که توسط سنا برای رسیدگی به تأثیرات رسانه‌های اجتماعی بر کاربران جوان تصویب شده‌اند. متا اخیراً برای حساب‌های نوجوانان کنترل‌های پیشرفته والدین معرفی کرد.

علاوه بر این، گزارش اف‌تی‌سی نشان می‌دهد که شرکت‌های بزرگ فناوری فعالانه در حال جمع‌آوری داده‌ها برای آموزش سیستم‌های هوش مصنوعی خود هستند، و

اغلب داده‌های خصوصی را از پشت دیوارهای پرداخت یا صفحه‌های ورود به سیستم با کمترین اطلاع‌رسانی یا بدون اطلاع به کاربران به دست می‌آورند.

در واکنش، گروه‌های صنعت تبلیغات این گزارش را مورد انتقاد قرار دادند و از ارزش خدمات پشتیبانی‌شده توسط تبلیغات دفاع کردند، و توصیف اف‌تی‌سی از روش کار خود به عنوان «نظارت تجاری گسترده» را رد کردند.

با این حال، گزارش کمیسیون تجارت فدرال ایالات متحده نگرانی‌های فزاینده‌ای در مورد حریم خصوصی داده‌ها و شفافیت، به‌ویژه در ارتباط با هوش مصنوعی و گروه‌های کاربران آسیب‌پذیر، را آشکار می‌کند.

اوکراین استفاده مقامات از تلگرام را ممنوع کرد

اوکراین استفاده از پیام‌رسان تلگرام را در دستگاه‌های ارتباطی رسمی مقامات دولتی، پرسنل نظامی و کارمندان ارشد به دلیل احتمال جاسوسی روسیه از پیام‌ها و نیز از کاربران این پیام‌رسان، ممنوع کرد. پس از آن که رئیس آژانس اطلاعات نظامی اوکراین شواهدی مبنی بر توانایی روسیه برای جاسوسی از طریق این پلتفرم را به شورای دفاع و امنیت ملی اوکراین ارائه داد، این شورا محدودیت‌های یاد شده را اعلام کرد.

آندری کووالنکو، رئیس مرکز مقابله با اطلاعات نادرست شورای امنیت اوکراین در پستی در تلگرام گفت که این محدودیت تنها برای دستگاه‌های ارتباطی رسمی است و تلفن‌های شخصی را شامل نمی‌شود. تلگرام از اپلیکیشن‌های محبوب و رایج در اوکراین است و از زمان درگیری نظامی روسیه با اوکراین در اسفند ۱۴۰۰ به یکی از منابع مهم اطلاع‌رسانی تبدیل شده است. مقامات امنیتی اوکراین بارها در مورد استفاده از تلگرام در طول جنگ ابراز نگرانی کرده بودند. در بیانیه شورای امنیت اوکراین آمده است که رئیس آژانس اطلاعات نظامی شواهدی ارائه کرده است که نشان می‌دهد سرویس‌های ویژه روسیه قادر هستند به پیام‌های تلگرام، از جمله پیام‌های حذف شده و همچنین اطلاعات شخصی کاربران، دسترسی داشته باشند. داده‌های «تِله مِتریو» نشان می‌دهد که حدود ۳۳ هزار کانال تلگرام در اوکراین فعال است. ولودیمیر زلنسکی، رئیس‌جمهوری اوکراین و فرماندهان نظامی و مقامات منطقه‌ای و شهری اوکراین، اخبار جنگ را در تلگرام منتشر می‌کنند و تصمیمات مهم خود را در کانال‌های تلگرامی گزارش می‌دهند.

بنا بر برآورد رسانه‌های اوکراینی حدود ۷۵ درصد از اوکراینی‌ها از این اپلیکیشن برای ارتباط با یکدیگر استفاده می‌کنند.

جریمه ۹۱ میلیون یورویی متا توسط اتحادیه اروپا

شرکت متا به دلیل ذخیره سازی ناخواسته بعضی از رمزهای عبور کاربران بدون حفاظت یا رمزگذاری، توسط نهاد حفاظت از داده‌های اتحادیه اروپا ۹۱ میلیون یورو جریمه شده است.تحقیق درباره تخلف شرکت متا پنج سال پیش آغاز شد. متا در آن مقطع زمانی به کمیسیون حفاظت از داده‌های ایرلند (دی‌پی‌سی) اطلاع داد که برخی از رمزهای عبور کاربران را به صورت متن ساده ذخیره کرده است.این کمیسیون همان‌زمان اعلام کرد که این رمزهای عبور در دسترس سایر افراد قرار نگرفته‌اند.با این حال، گراهام دویل، معاون کمیسیون حفاظت از داده‌های ایرلند، در بیانیه‌ای تاکید کرد: «با توجه به خطر سوءاستفاده از اطلاعات مربوط به رمزهای عبور، این موضوع به‌طور گسترده پذیرفته شده که رمزهای کاربران نباید به‌صورت متن ساده ذخیره شوند.» کمیسیون حفاظت از داده‌های ایرلند به‌عنوان نهاد اصلی نظارت بر اکثر شرکت‌های بزرگ اینترنتی آمریکایی در اتحادیه اروپا فعالیت می‌کند.

یکی از سخنگویان متا در بیانیه‌ای که منتشر شد، با تاکید بر همکاری سازنده این شرکت با کمیسیون حفاظت از داده‌های ایرلند در جریان تحقیقات گفت آن‌ها پس از شناسایی این خطا در بررسی امنیتی سال ۲۰۱۹، بلافاصله اقدام به رفع آن کرده‌اند.

او افزود: هیچ نشـانه‌ای مبنی بر سوءاستفاده یا دسترسی غیرمجاز به این رمزهای عبور وجود ندارد.پیش‌تر در آذرماه ۱۴۰۲، سازمان ان‌اووای‌بی (NOYB)، مرکز اروپایی حقوق دیجیتال، اعلام کرد از متا بابت دریافت هزینه بابت خدمات اشتراک بدون تبلیغات خود شکایت می‌کند.به گفته ان‌اووای‌بی، این تصمیم متا قوانین اتحادیه اروپا را درباره تعریف «رضایت» نقض می‌کند.متا تصمیم خود را معتبر و مطابق با حکم دادگاه عالی اروپا دانست و تاکید کرد «رضایت» کاربران در این طرح لحاظ شده و آن‌ها می‌توانند سرویس رایگان و دارای تبلیغات را انتخاب کنند.متا در خردادماه سال گذشته هم از سوی اتحادیه اروپا به دلیل انتقال اطلاعات کاربران اروپایی به آمریکا به پرداخت ۱.۲ میلیارد یورو محکوم شد که در حال حاضر نسبت به آن درخواست تجدیدنظر کرده است.این شرکت تاکنون مجموعا ۲.۵ میلیارد یورو جریمه به‌دلیل نقض مقررات عمومی حفاظت از داده‌ها که در سال ۲۰۱۸ تصویب شد، پرداخت کرده است.

وای فای رایگان چه خطراتی برای کاربران دارد؟

توصیه می شـود که برای جلوگیری از نفوذ هکرها و سرقت اطلاعات شخصی و مالی کاربران، از سرویس های وای فای عمومی استفاده نشود، چراکه در این صورت اتفاقاتی مانند سرقت اطلاعات کارت بانکی، پول، اطلاعات مدارک شناسایی می تواند رخ دهد.

اگر چه وای فای رایگان در اماکن عمومی برای خیلی ها خوشایند است ولی اینترنت رایگان عمومی می توانند دردسـرهایی را برای کاربران ناآگاه ایجاد کند تا مجرمان و هکرهـای اینترنتی از این فرصت اسـتفاده کرده و وارد اطلاعات شـخصی افراد و برنامـــه های شغلی آن ها شوند.

با اینکه امروزه بسته‌های اینترنتی اپراتورها برای اکثر گوشی‌های هوشمند فعال است، اما همچنان نیاز به وای‌فای در برخی اماکن و در شرایطی که به هر دلیل اینترنت گوشی فعال نیست، حس می‌شود. بنابراین وای‌فای شهری با قابلیت ارایه سرعت و کیفیت بالا و گاهی رایگان برای کاربرانی که در لحظه به اینترنت موبایل خود دسترسی ندارند و همچنین با توجه به نیاز ابزارهای فاقد سیم‌کارت مانند لپ‌تاپ و تبلت به وای‌فای، مورد توجه بسیاری از کاربران است.

در بسیاری از کشورهای پیشرفته جهان استفاده از وای‌فای در فضاهای شهری و عمومی مانند میدان‌ها، ایستگاه‌های اتوبوس، بیمارستان‌ها و دانشگاه‌ها به امری عادی تبدیل شده است و حتی شهرداری‌ها سعی می‌کنند با ارایه وای‌فای، رضایت خاطر شهروندان را کسب کنند.

اما خوب اسـت به این نکته توجه شـود که وای فای عمومی اگرچه سـودمند بوده و امتیازاتی مانند اتصال به اینترنت در هر لحظه و مکان را برای کاربران فراهم می‌کند، به دلیل همگانی بودن و اینکه تمامی کاربران از یک نام کاربری و رمز عبور اسـتفاده می‌کنند، آنها را به سمت ناامنی و در نهایت افزایش کلاهبرداری پیش می‌برد؛ مسئله‌ای که می‌تواند زمینه ارتکاب جرم را برای سودجویان فضای مجازی فراهم کند.

مهم‌ترین خطرات وای‌فای رایگان برای کاربران

زمانی که کاربری از یک وای‌فای رایگان اسـتفاده می‌کند این احتمال وجود دارد یک مهاجر یا هکر اطلاعات مربوط به آیدی و رمزهایتان را دریافت کند. همچنین می‌تواند به داده‌هایی که توسط گوشی و یا کامپیوتر در حال رد و بدل شدن است دسترسی داشته باشد. از این طریق، آن‌ها می‌توانند داده‌هایی تهیه کنند.

وای فای رایگان می‌تواند شرایطی را برای هکرها فراهم کند که وارد حساب کابری شوند یا بر روی دستگاه آنها مانند گوشی یا لپ تاپ یک بدافزار مخرب نصب کنند. علاوه بر موارد گفته شده می‌تواند کاربر را به یک صفحه وب فیشینگ شده ببرد و در آنجا کاربر اطلاعات شخصی خود را برای او افشا کند.

اما در هر صورت اگر کاربری قصد استفاده از وای‌فای عمومی را دارد، برای جلوگیری از حمله هکرها به اطلاعاتش، تا جای ممکن سعی کند از شبکه‌هایی که دارای کلمه عبور اختصاصی هستند، استفاده کند و قبلا در مورد آن شبکه از مسوولین مربوطه راهنمایی لازم را بگیرید. بهتر است قبل از اتصال به اینترنت از یک مسئول در مکانی که هستید در مورد ویژگی‌های وای‌فای مورد نظر سـوال کنید. در صورت ضرورت وصل شـدن شبکه‌های عمومی کاربران مطمئن باشند که از وی‌پی‌ان مطمئن استفاده می‌کنند.

در مرحله بعد توصیه می‌شود تنها به شبکه‌هایی که با پسورد محافظت می‌شوند وصل شـوند. همچنین لازم اسـت کاربران نام‌های کاربری و رمز عبور و پسورد دوم خود را بلافاصله بعد از اتمام کار تغییر دهند.

به صورت کلی استفاده از اینترنت وای‌فای در اماکن عمومی ضریب امنیت بسیار پایینی دارد و شهروندان و کاربران گوشی‌های هوشمند و رایانه باید از تمامی تهدیدات، خطرها و ریسک‌هایی که این سـرویس‌های وای‌فای عمومی برایشان ایجاد می‌کند، مطلع و آگاه باشند.

بنابراین توصیه می شود برای جلوگیری از نفوذ هکرها و سرقت اطلاعات شخصی و مالی کاربران از سرویس های وای فای عمومی استفاده نشود چراکه در این صورت اتفاقاتی مانند سرقت اطلاعات کارت بانکی، پول، اطلاعات مدارک شناسایی می تواند رخ دهد.

اپلیکیشنی که زمان دقیق مرگ را پیش بینی می کند

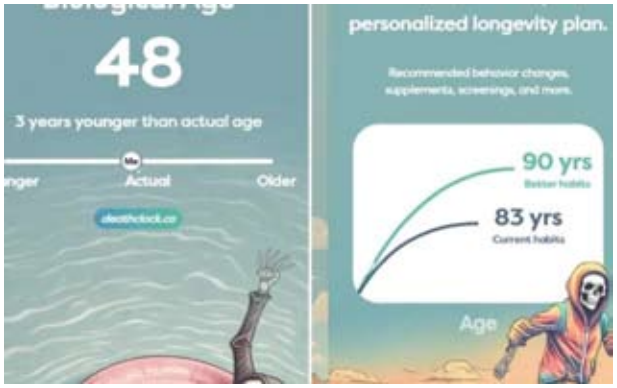
یک اپلیکیشن جدید مبتنی بر هوش مصنوعی ادعا می‌کند که قادر است زمان مرگ شما را به‌طور دقیق مشخص کند و هدف آن تشویق کاربران به انتخاب‌های سالم‌تر و داشتن زندگی طولانی‌تر است.افرادی که به دنبال دریافت این خبر ناخوشایند هستند، با پرداخت ۴۰ دلار در سال، می‌توانند اپلیکیشن Death Clock را دانلود کنند.

این برنامه مجموعه‌ای از سوالات در مورد وضعیت سلامت و عادات اجتماعی شما را مطرح می‌کند و به کمک آن‌ها نه تنها سال بلکه تاریخ دقیق مرگ فرد به همراه سن زیستی فعلی او را پیش‌بینی می‌کند.

هدف این اپلیکیشن ایجاد یک هشدار است، پیش از آنکه برای ایجاد تغییرات معنادار دیر شود.بنیان‌گذار این اپلیکیشن، برنت فرانسن، گفت: «در دنیای امروز، مراقبت‌های بهداشتی معمولاً واکنشی هستند و تنها زمانی افراد مداخله می‌کنند که مشکلات بروز کرده و اغلب هم دیر شده و کار از کار گذشته است.

او افزود: «Death Clock نشان‌دهنده تغییر به سمت پزشکی ۳.۰ است، جایی که افراد، با دانش جامع در مورد سلامتی خود تجهیز می‌شوند و به طور پیش‌دستانه تشویق می‌شوند تا به مدیریت سلامتی خود بپردازند و زندگی طولانی‌تر و سالم‌تری داشته باشند.»این ابزار سپس یک «برنامه طول عمر» شخصی‌سازی‌شده‌ای از تغییرات سبک زندگی و مواردی که باید با پزشکان مطرح شوند، ایجاد می‌کند.

آزمایش‌های خون، پروفایل‌های ژنتیکی و دیگر اسناد شخصی سلامت نیز می‌توانند به این اپلیکیشن آپلود شوند.وقتی آماندا کوزر از CNET این اپلیکیشن را آزمایش کرد،



گزارش داد که سوالات Death Clock شامل عوامل بیولوژیکی مانند سطح کلسترول، سوالات مربوط به خواب و سلامت روان، و همچنین میزان نشستن روزانه است.

سایر سوالات به رژیم غذایی، فعالیت فیزیکی، سیگار کشیدن و داشتن زندگی اجتماعی مربوط می‌شوند.کوزر زمانی که عمداً به بدترین شکل ممکن به آزمون پاسخ داد و مرگش در سال ۲۰۴۳ پیش‌بینی شد، نوشت: «این برای من انگیزه‌ای است که در مسیر درست بمانم.»

جهش استفاده مشکل‌دار نوجوانان از شبکه‌های اجتماعی در دوران کرونا

نتایج تحقیق بنیاد رفتار سلامتی کودکان بر روی ۲۸۰ هزار نوجوان ۱۱، ۱۳ و ۱۵ ساله در ۴۴ کشور، نشان می‌دهد که رفتار مشکل‌دار در استفاده از شبکه های اجتماعی اینستاگرام و تیک تاک از هفت درصد در سال ۲۰۱۸ به ۱۱ درصد در سال ۲۰۲۲ رسید.بیشتر نوجوانان از یک یا چند رسانه اجتماعی مانند اینستاگرام، تیک‌تاک یا یوتیوب استفاده می‌کنند. یک پژوهش بین‌المللی جدید نشان داده که این استفاده با افزایش مشکلات رفتاری همراه بوده است.

این تحقیق که بر روی ۲۸۰ هزار نوجوان ۱۱، ۱۳ و ۱۵ ساله در ۴۴ کشور انجام شده است، نشان می‌دهد که از زمان همه‌گیری کرونا، استفاده «مشکل‌زا» از رسانه‌های اجتماعی در میان کودکان و نوجوانان افزایش چشمگیری داشته است.

بنیاد «رفتار سلامتی کودکان مدرسه‌ای»، که این تحقیق را انجام داد، دریافته است که رفتار مشکل‌دار در استفاده از رسانه‌های اجتماعی از هفت درصد در سال ۲۰۱۸ به ۱۱ درصد در ۲۰۲۲ رسیده است.

در این تحقیق مشخص شد که انگلستان، ولز و اسکاتلند بیشترین موارد رفتار مشکل‌دار را در میان نوجوانان داشته‌اند. پژوهشگران هشدار داده‌اند که فناوری‌های دیجیتال می‌توانند تأثیرات منفی بر سلامت روان و بهداشت کودکان و نوجوانان داشته باشند و خواستار اقدامات بیشتر برای ترویج رفتارهای سالم در فضای مجازی شده‌اند.

جو اینچلی، یکی از نویسندگان این پژوهش از دانشگاه گلاسکو، گفت: «استفاده مشکل‌دار بیش از همه در سن ۱۳ سالگی دیده می‌شود که نخستین مرحله بلوغ در حال سپری شدن است و دختران بیش از پسران به بهره‌برداری مشکل‌دار از رسانه‌های اجتماعی می‌پردازند.»

او می‌گوید: «حدود یک سوم از نوجوانان تقریباً در تمام طول شبانه‌روز، جز هنگام خواب، از طریق رسانه‌های اجتماعی با دیگران در ارتباط هستند.»

با این حال، نوجوانانی که به‌طور سالم از رسانه‌های اجتماعی استفاده می‌کنند، تعامل بهتری با دوستان و جامعه دارند، در حالی که گروهی که رفتار مشکل‌زا داشته‌اند، معمولاً رفتار اعتیادآمیز به این رسانه‌ها نشان می‌دهند.

نشانه‌های رفتار مشکل‌زا شامل نادیده گرفتن سایر فعالیت‌ها مانند کتاب خواندن، بازی کردن و وقت‌گذرانی با خانواده است. همچنین، جر و بحث دائمی بر سر استفاده بیشتر از رسانه‌های اجتماعی و دروغگویی درباره مدت زمان آنلاین بودن، از دیگر نشانه‌های آن است.

پسرها بیشتر از دختران با مشکلات ناشی از بازی‌های آنلاین مواجه هستند. در کشورهای مورد بررسی، حدود ۴۶ درصد از پسران نوجوان روزانه به بازی‌های آنلاین می‌پردازند و این آمار در انگلستان ۵۲ درصد و در اسکاتلند ۵۷ درصد است.

این تحقیق که توسط بخش اروپایی سازمان جهانی بهداشت منتشر شده، نشان داده است که رسانه‌های اجتماعی می‌توانند تأثیرات مثبت و منفی بر نوجوانان داشته باشند.

هانس کلوگ، مدیر اروپایی سازمان جهانی بهداشت، بر اهمیت آموزش سواد دیجیتال برای نوجوانان تأکید کرده و گفته است: «باید اقدامات فوری برای کاهش صدمات استفاده از رسانه‌های اجتماعی انجام دهیم تا از افسردگی، آزار دیگران، اضطراب و عملکرد تحصیلی ضعیف جلوگیری کنیم.»

مدیر اروپایی سازمان جهانی بهداشت همچنین بر اهمیت نقش دولت‌ها، مقامات بهداشتی، به‌ویژه مدارس، والدین و معلمان در این زمینه تأکید کرده است.

Iran, Cuba to Expand Ties in AI, Digital Economy

Information and Communication Technology (ICT) Minister, Sattar Hashemi, and his Cuban counterpart, Mayra Arevich Marín, have explored ways to bolster cooperation in different fields of ICT.

During a video call, the officials further reviewed possibilities to enhance ties in artificial intelligence, digital economy, and e-government, as well as post companies.

During the meeting, Arevich Marín proposed and highlighted expanding collaborations based on formerly signed agreements.

The official also welcomed the presence of Iranian private companies active in providing ICT-related equipment and services in Cuba.

Hashemi, announced Iranian private companies' readiness to provide ICT services in Cuba and expressed optimism to promptly implement needed measures.

Arevich Marín also passed an invitation to his Iranian counterpart to attend the 19th Joint Economic Commission of Iran and Cuba, as well as the 40th edition of the Havana International Fair (FIHAV) which is scheduled to take place from November 4 to 9.

Iran Hosted SATRC Workshop on Recent Trends, Technologies

The South Asian Telecommunication Regulators' Council (SATRC) workshop on recent trends and technologies was held in Tehran from September 30 to October 2.

Hosted by the Communications Regulatory Authority (CRA) of the Islamic Republic of Iran, the event brought together representatives from India, Maldives, Nepal, Pakistan, Bangladesh, Bhutan, Sri Lanka, and Afghanistan.

The emphasis of the workshop was on recent trends and technologies that support the digital transformation of the economy and society in SATRC member countries.

The main objective was to give an in-depth analysis of various trends in innovation and technologies for fostering the growth of the economy and society including technical details, policy and regulatory aspects, and other aspects.

The workshop served as a platform to share expertise and boost cooperation among regional South Asian countries. It also focused on modern strategies to address challenges facing the information communication technology sector at regional as well as global levels, Hamid Fattahi, an official with Information and Communication Technology, said.

Addressing the attendees, Fattahi said the rapid development of communication infrastructure and technological trends play an important role in empowering communities and accelerating economic growth.

"In a world that is becoming more and more digitalized, it is very essential to find a balance between the three elements of security, privacy, and innovation in information communication and technology.

Also, with the rapid pace of emerging technologies such as artificial intelligence (AI), the importance of developing safe policies and regulations that will ensure responsible use of these technologies is felt more than ever," Fattahi added.

The three-day event consisted of several sessions discussing policy and regulatory environments; innovation and investment in telecommunication/ ICT; and initiatives to bridge the standards and innovation gap.

The sessions also focused on the new technologies and trends in satellite communications, and regulatory aspects and challenges of these technologies were addressed in detail.

AVA Communication Industries

صنایع ارتباطی آوا

- رتبه یک سازمان برنامه و بودجه در رشته شبکه داده های رایانه ای و مخابراتی
- رتبه یک سازمان برنامه و بودجه در رشته تولید و پشتیبانی نرم افزارهای سفارش مشتری
- رتبه یک سازمان برنامه و بودجه در رشته امنیت فضای تولید و تبادل اطلاعات
- رتبه یک سازمان برنامه و بودجه در رشته خدمات پشتیبانی
- رتبه یک سازمان برنامه و بودجه در رشته تولید و ارائه قطعات و ملزومات
- برگزیده پژوهش های کاربردی کشور در جشنواره بین المللی خوارزمی
- برگزیده جشنواره بین المللی خوارزمی در تبدیل طرح برگزیده به تولید ملی
- برگزیده به عنوان شرکت پیشرو در توسعه فناوری در سال ۱۴۰۱
- برنده جایزه برترینهای پارکهای علم و فناوری آسیا (ASPA) در سال ۲۰۱۴
- برنده مدال طلای سازمان جهانی مالکیت فکری (WIPO)
- برنده لوح تقدیر سازمان توسعه صنعتی سازمان ملل (UNIDO)
- برنده تندیس طلایی روز ملی صنعت و معدن در سال ۱۴۰۱
- واحد برتر گروه صنعت برق و الکترونیک استان تهران در سال ۱۴۰۱
- واحد برتر جشنواره تحقیق و توسعه استان تهران در سال ۱۴۰۱
- دارنده گواهی تایید امنیت محصول از آزمایشگاه های مرجع و ذیصلاح
- دارنده گواهینامه رعایت حقوق مصرف کنندگان در چند دوره مختلف
- دارنده گواهینامه تایید صلاحیت ایمنی پیمانکاران (HSE)
- دارنده پروانه تحقیق و توسعه از وزارت صنعت، معدن و تجارت
- دارنده پروانه بهره برداری سخت افزارتجهیزات سوئیچینگ IMS/NGN/VOIP
- واحد برتر توسعه فناوری از سوی وزارت صنعت، معدن و تجارت در سال ۱۴۰۱
- دارنده گواهینامه تائید محصولات از سازمان تنظیم مقررات و ارتباطات رادیویی
- دارنده گواهینامه تائید توانمندی فناورانه از سازمان پژوهش های علمی و صنعتی ایران
- عضویت در اتحادیه صادر کنندگان صنعت مخابرات ایران، سندیکای صنعت مخابرات ایران، انجمن سازندگان صنعت نفت ایران، انجمن تخصصی مراکز تحقیق و توسعه صنایع و معادن و مجمع تشکلهای دانش بنیان ایران و ....
- کارآفرین برتر استان تهران در سال ۱۴۰۱ و عضو کانون کارآفرینان برتر رسمی استان تهران و کانون کشوری
- برگزیده جشنواره فناوری شیخ بهایی در دوره های مختلف در گروه فن آفرینان رشد یافته
- برگزیده جشنواره فاوا در چندین دوره متمادی و کسب رتبه اول فناوری های تجاری شده
- برگزیده جشنواره علم تا عمل و برگزیده جشنواره شهید چمران
- دارنده گواهینامه ایزو 9001 , 14001 , 10002 , 10668 , 21500 و استاندارد CE

مرکز تحقیقات آوا در پارک فناوری پردیس

با وام فوری دیجی‌پی

همین امروز برو پِی خریدت

دیجی پی

mydigipay.com

جشنواره زنگ آخر

اینترنت پر سرعت ADSL و VDSL با مودم رایگان ویژه مشتریان جدید

- از ۱۷ شهریور ماه به مدت ۲ ماه
- اطلاعات بیشتر و خرید از طریق تماس با ۲۰۲۰

شرکت مخابرات ایران
(سهامی عام)
ارتباطی خدا گیر

AI as a Service

- خدمات مبتنی بر هوش مصنوعی
- فضـــای GPU ابـــری

بزودی در رایتـل

رایتل
RighTel

www.rightel.ir

یک ارتباط هوشمند

با ما در ارتباط باشید

خدمات زیرساخت ابری ایرانسل

ایرانسل
MTN

Cloud.irancell.ir
Business.irancell.ir
EB@mtnirancell.ir