انجمن ایرانی مطالعات سازمان ملل متحد

Special Consultative Status with the ECOSOC

دارای مقام مشورتی خاص نزد شورای اقتصادی و اجتماعی ملل متحد

ECOSOC

Iranian Association for United Nations Studies

سمپوزیوم برخط تالار گفتگوی
انجمن ایرانی مطالعات سازمان ملل متحد

«تاثیر علم و فناوری‌های نوین بر صلح و امنیت بین‌المللی»

با مشارکت جمعی از استادان و پژوهشگران

شهریورماه ۱۴۰۱

مجموعه مقالات سمپوزیوم

«تاثیر علم و فناوری های نوین بر صلح و امنیت بین المللی»

به کوشش:

دکتر علیرضا شمس لاهیجانی

دکتر کتایون حسین نژاد

شهریور۱۴۰۱

تالار گفتگوی انجمن ایرانی مطالعات سازمان ملل متحد

(unstudies.ir/iauns-forum)

فهرست مطالب به ترتیب انتشار برخط

تبعات حقوقی و سیاسی کلان داده ها در صلح و امنیت بین المللی

متینه السادات میرنظامی- دانش آموخته کارشناسی ارشد حقوق بین الملل دانشگاه مفید قم
زهره برادران مفید آستانه-دانش آموخته کارشناسی ارشد حقوق بین الملل دانشگاه مفید قم

با پیشرفت در حوزه ارتباطات، فناوری و تکنولوژی های نوین، دسترسی بشر به اینترنت، تلفن همراه و شبکه های اجتماعی بیشتر شده است. به دنبال آن با وقوع انقلاب داده، دریچه جدیدی به روی انسان گشوده شده است که مانند هر پدیده نوظهور فرصت ها و چالش های جدیدی را برای وی به دنبال دارد. در مقیاس وسیع تر، کلان داده به سیاستگذاران و متخصصان این فرصت را می دهد تا با استفاده از فناوری پردازش و جمع آوری کلان داده و اتخاذ تصمیم های منطقی تر، گامی بزرگ در راستای ایجاد و تثبیت صلح و امنیت جهانی، یکی از اهداف سازمان ملل متحد، بردارند. با وجود تمام فرصت‌ها و چالش‌ها، استفاده از کلان داده می تواند مسیر رسیدن به اهداف توسعه پایدار (به ویژه هدف شانزدهم) را هموار کند. کلان داده در حوزه های مختلفی چون بیان تنفر آمیز، مهاجرت، تروریسم، نظارت و ارزیابی، هشدار و پیش بینی اولیه، تغییرات آب و هوا، حوادث طبیعی و ... کاربرد دارد. با توجه به کاهش روند صلح از سال ۲۰۰۸ و افزایش گروه های تروریستی در جهان اهمیت کلان داده را در صلح و امنیت داخلی و بین المللی بیش از پیش آشکار می شود. از آنجا که پرداختن به تمامی کاربردهای کلان داده در این مقال نمی گنجد، با توجه به تاثیر مستقیم تروریسم بر صلح و امنیت بین المللی و روند افزایشی جریان‌های افراطی، در این نوشتار به ارتباط میان کلان داده و تروریسم پرداخته شده است.

کلان داده به مجموعه داده هایی اطلاق می شود که بیش از حد بزرگ یا پیچیده هستند و نمی توان با نرم افزارهای کاربردی پردازش داده سنتی به آنها پرداخت. چالش های تجزیه و تحلیل کلان داده ها شامل جمع آوری داده ها، ذخیره سازی داده ها، تجزیه و تحلیل داده ها، جستجو، اشتراک گذاری، انتقال، تجسم، پرس و جو، بروز رسانی، اطلاعات حریم خصوصی و منبع داده است.

در این نوشتار، تروریسم از منظر قطعنامه ۴۹/۶۰ مجمع عمومی سازمان ملل متحد (مصوب ۹ دسامبر ۱۹۹۴)، با عنوان «اقدامات برای از بین بردن تروریسم بین المللی» به این صورت تعریف می شود: «اعمال مجرمانه ای که به منظور ایجاد یک حالت وحشت در عموم مردم، گروهی از افراد یا افراد خاص با اهداف سیاسی انجام می شود، در هر شرایطی غیر قابل توجیه است، صرف نظر از ملاحظات سیاسی، فلسفی، ایدئولوژیک، نژادی، قومی، مذهبی یا هر ماهیت دیگری که ممکن است برای توجیه آنها مورد استناد قرار گیرد.» درواقع تعریف مشخص و جامعی در مورد پدیده تروریسم وجود ندارد؛ زیرا پدیده‌ای محصور به زمان و مکان است و می تواند توسط طرفداران یا مخالفان خود با توجه به منافعی که دارند تعاریف مختلفی داشته باشد. طرفداران، آن را پدیده‌ای بر حق و انقلابی می دانند و

تروریست ها را آزادی خواه و استقلال طلب تلقی می کنند و مخالفان، آن را حرکتی شورشی و ضد منافع دانسته و طرفداران آن را برانداز و شورشگر می دانند. از این رو می‌توان آن را پدیده‌ای با ریشه‌های سیاسی دانست که عامل محرک تحولات بسیار اجتماعی، اقتصادی، سیاسی و حقوقی است. عدم اجماع بر تعریف مشخصی از آن، ناشی از دیدگاه مختلف کشورها نسبت به این موضوع و منافع سیاسی شان است. از دیدگاه حقوقی نیز تلاش هایی برای جرم انگاری مصادیق اقدامات تروریستی صورت گرفته است که کنوانسیون سرکوب تصرف غیرقانونی هواپیما ۱۹۷۰ ، کنوانسیون سرکوب رفتارهای غیر قانونی ضد هواپیمای غیر نظامی ۱۹۷۱، کنوانسیون پیشگیری و مجازات علیه افراد تحت حمایت بین المللی از جمله دیپلمات ها ۱۹۷۳ را می توان از این جمله دانست. با تمام ویژگی ها و تعاریف مختلفی که دولت ها و اندیشمندان درباره تروریسم ارائه داده اند، به طور کلی می توان با توجه به کنوانسیون ۱۹۰۷ لاهه، کنوانسیون۱۹۴۹ و پروتکل های الحاقی آن، تروریسم را پدیده ای در زمان صلح دانست که دارای سه ویژگی اصلی زیر است:

۱. به کار گرفتن خشونت یا دست کم تهدید به اعمال آن؛

۲. اعمال خشونت با اهداف سیاسی؛ و

۳.هدف تهدیدات و آسیب های تروریستی قرار دادن غیر نظامیان

کلان داده و تروریسم

حادثه ۱۱ سپتامبر بار دیگر توجه جهانی به پدیده تروریسم را جلب کرد. گسترش تروریسم و ایجاد مانع برای توسعه صلح و امنیت باعث شده است تا اجماع جهانی و تلاشی چند ملیتی علیه تروریسم ایجاد شود که از نتایج آن می توان به تشکیل دفتر ضد تروریسم سازمان ملل اشاره کرد؛ همچنین اهمیت کنوانسیون مقابله با تامین مالی تروریسم که پیش از حادثه مذکور به تصویب رسیده بود بیش از پیش آشکار شد. انتشار محتوای افراطی در شبکه‌های اجتماعی منجر به گسترش خشونت های آفلاین و آنلاین شده که نتایج آن در حملات تروریستی نیوزلند ۲۰۱۹ قابل بررسی است. بیان تنفر آمیز(ص.۲۲) را نیز می توان یکی از عوامل محرک برای جذب نیرو و تشویق به انجام عملیات تروریستی دانست. با همه گیری اینترنت امکان دسترسی افراد به شبکه های اجتماعی برای بیان تنفر آمیز و استفاده از محتوای مرتبط افزایش یافته که خود می تواند تهدیدی علیه صلح و امنیت باشد. فناوری تشخیص صدا، تصویر و مکان های جغرافیایی از طریق سنجش احساسات و نحوه گفتار محتوای نفرت را شناسایی، تجزیه و تحلیل کرده و در نهایت الگوریتمی از تحرکات خشونت آمیز را ترسیم می نماید که در تامین امنیت بین المللی موثر خواهد بود. این الگوریتم ممکن است توسط شرکت ها ترسیم شود اما در نهایت دولت ها از آن به عنوان داده های سیاستگذاری، وضع قوانین و حفظ صلح و امنیت استفاده خواهند کرد.

با استفاده از کلان داده می توان نقشه فعالیت‌های ضد تروریستی را در سه مرحله پیشگیری، مقابله و جبران آسیب های وارده ترسیم کرد. پیشگیری از درگیری و خشونت در دو بخش ساختاری و عملیاتی انجام می شود. در پیشگیری ساختاری با ارزیابی شاخص های کلان زیرساخت سیاسی و اقتصادی، بحران های سیاسی و اقتصادی کشورها را پیش بینی می کنند. از نظر عملی، پیشگیری از طریق سیستم هشدار زودهنگام بر اساس ارزیابی های ریسک که خود بخشی از ابزار پیشگیری ساختاری است و مدیریت بحران، از وقوع خشونت و بروز تروریسم جلوگیری می کند. این امر از طریق رفتار شناسی در شبکه‌های اجتماعی و شناسایی مجرمان و تبهکاران در جهت تامین امنیت داخلی و خارجی امکان پذیر است. ناگفته نماند که استفاده از کلان داده بدین مقصود، تبعات حقوقی و سیاسی نیز به دنبال دارد که در ذیل به طور خلاصه به آن پرداخته شده است.

تبعات حقوقی و سیاسی استفاده از کلان داده

در عصری که کلان داده ها زندگی بشر را تحت تاثیر قرار داده، قدرت در اختیار افراد، گروه ها و دُوَلی است که بر نحوه استفاده از آن واقف باشند. قدرت ناشی از کلان داده ها دو روی یک سکه محسوب می شود؛ از یک سو به بقا و امنیت حکومت کمک می کند و از سوی دیگر می تواند به اخلال در صلح و امنیت بین المللی منجر شود تا آنجا که در قرن اخیر با ظهور تروریسم این تعارض بیش از پیش بروز یافته است.

در این مسیر ممکن است حقوق اساسی بشر تحت تاثیر قرار گیرد. بنابراین اولویت بندی حقوق مذکور و تنظیم مقررات برای استفاده ضد تروریستی از کلان داده ها ضروری است زیرا بر اساس میثاق بین المللی حقوق مدنی و سیاسی، دول عضو متعهد به احقاق حقوق نقض شده افراد هستند، حتی اگر حق مذکور توسط افرادی نقض شده باشد که به اجرای مشاغل رسمی خود مشغول بوده اند. بدین صورت تعادل بین حفاظت از امنیت بین المللی و حمایت از حقوق بشر برقرار خواهد شد. از طرفی کلان داده ها به دلیل عدم قطعیت و دشواری در تفسیر همیشه دقیق نیستند و احتمال خطا در آنها وجود دارد. ممکن است داده های ثبت و ضبط شده یک شخص تنها احتمال تروریست بودن وی را نشان دهد و موجب شود به طور مداوم تحت نظر باشد؛ در این صورت علاوه بر تبعیض میان او و سایرین و نقض حریم خصوصی وی، این برچسب گذاری آینده وی را نیز تحت تاثیر قرار خواهد داد و موجب نقض برخی از حقوق شخص از جمله منع تبعیض، آزادی بیان و حریم خصوصی می شود.

کنترل کنندگان در پروژه های امنیتی به دنبال سیگنال های خاصی در داده های شخص هستند. در صورتی که برخی از این نشانه ها در داده های شخص بروز کند تا زمان روشن شدن حقیقت، ممکن است از ورود فرد مورد نظر به مشاغل خاص جلوگیری شود و یا تمامی ارتباطات، اظهارنظر ها و رفت و آمدهای وی تحت کنترل باشد؛ گرچه ممکن است فرد از وقوع یا علل آن مطلع نباشد و آسیب آشکاری به حقوق وی وارد نشود اما با این حال به صورت پنهان نیز حقوق مذکور نقض شده است. همچنین زمانی که فرد در فضای اینترنت، در معرض دید ناظران نامرئی

قرار می گیرد دچار خودسانسوری می شود که منجر به نقض آزادی بیان است و شدت یا ضعف آن متاثر از شرایط سیاسی و اجتماعی محیطی است که در آن زندگی می کند.

یکی از موضوعات مهم دیگر در بحث کلان‌داده‌ها، مسئله تبعیض نژادی است. این تبعیض می تواند از طریق کدگذاری های سازماندهی شده و با سیاست های جانبدارانه و یا به صورت غیرعمدی باشد. در واقع رفتار انسان، داده های هوش مصنوعی را آموزش می دهد که در این میان تعصب و سوگیری مشکل بزرگی محسوب می شود. به بیان دیگر این انسان است که انتخاب می کند الگوریتم ها بر چه کسانی، با چه اهدافی و با چه روش هایی اعمال شود. به عنوان مثال برای نشان دادن پوست های سالم، چهره زنان سفید پوست و برای نشان دادن سرطان، چهره افرادی با پوست های تیره تر نمایش داده می شود. بنابراین داده ها ممکن است نژادپرستی سیستماتیک را رمزگذاری کنند. در نتایج نظرسنجی، الگوهای استخدام، سوابق جنایی یا سایر رفتارهای انسانی، نژاد، نمونه های نگران‌کننده‌تری از خطر سوگیری را ارائه می‌کند؛ نتیجه آن است که در هر حال این کدگذاری ها می‌تواند منجر به گردآوری داده هایی شود که نتایج واقعی را نشان نمی‌دهد. نتایج غیر واقعی نشان داده شده در یکی از برنامه های تشخیص چهره در سال ۲۰۱۵ را می توان مثالی بر این موضوع دانست که چهره دو آمریکایی آفریقایی تبار را به عنوان «گوریل» معرفی کرد چرا که به عقیده بسیاری، آموزش داده های هوش مصنوعی بیشتر به چهره های سفید متکی است. از این رو پارلمان اروپا با تصویب قطعنامه‌ای در سال ۲۰۱۷ بر ایجاد یک سیستم قوی و توجه به حفظ کرامت انسانی، برابری و عدالت با توجه به ماده ۲ معاهده اتحادیه اروپا و منشور حقوق اساسی تاکید کرد.

در جهان وابسته به تکنولوژی می توان گفت کلان داده ضمن کمک به ایجاد امنیت بین المللی به سلاحی خطرناک علیه امنیت نیز تبدیل شده است. از آنجایی که تروریست ها با نقض ماده ۲۰ میثاق بین المللی حقوق مدنی و سیاسی و استفاده از شبکه های اجتماعی به عضوگیری، تشکیل گروه، طراحی و اجرای عملیات می پردازند، دولت ها باید با استناد به ماده ۷ اعلامیه حق توسعه نهایت تلاش خود را برای تجزیه و تحلیل کلان داده در جهت مبارزه با تروریسم به کار گیرند. دولت ها می توانند با داده کاوی لیست تماس‌ها، سوابق خرید، رفت و آمد ها به مکان های حساس و حتی میزان رفت و آمد به یک مکان خاص را تحت نظر گیرند. همچنین ردیابی منابع تامین مالی تروریسم و ضبط و توقیف آن با استفاده از کلان داده قابل اجراست. استفاده از کلان داده این امکان را به دولت ها می دهد تا از حملات احتمالی آگاه شده و به موقع از آن جلوگیری کنند. چنین اقدامی در صورتی که برای مقابله با فعالیت های تروریستی نباشد، می تواند موجب تهدید امنیت ملی سایر کشورها تلقی شود. به عنوان مثال آژانس امنیت ملی آمریکا(NSA) با استفاده از سامانه prism می تواند به داده های بسیاری در شبکه های مجازی، ایمیل ها، چت های شخصی و نیز اطلاعات شرکت های گوگل و فیس بوک دسترسی داشته باشد و در صورت لزوم رمزگشایی از داده ها در اختیار آن قرار داده شود به طوری که تخلف از این الزام شرکت های مذکور را مجبور به پرداخت

جریمه خواهد کرد. چنین اقدامی در صورتی که برای مقابله با فعالیت های تروریستی نباشد موجب تهدید امنیت ملی سایر کشورها می شود.

همانطور که در اکتبر ۲۰۱۳ اطلاعاتی مبنی بر شنود تلفن آنگلا مرکل منتشر شد و نشان داد که آمریکا از این شبکه حتی برای فعالیت های جاسوسی علیه دوستان خود از جمله آلمان نیز استفاده می کند. برنامه پریسم در واقع یکی از راه های گردآوری اطلاعات برای اتحاد اطلاعاتی فایو آیز(Five Eyes) شامل آمریکا، بریتانیا، کانادا، استرالیا و نیوزلند است. کشورهای فوق برای همکاری در زمینه شنود الکترونیک توافقنامه چند جانبه یو کی یو اس (UKUS) را منعقد نمودند. آمریکا با حمایت دانمارک از کابل های اطلاعاتی این کشور برای جاسوسی از شهروندان سوئد، نروژ، فرانسه و آلمان استفاده کرده بود که اسنودن جزئیات آن را فاش کرد. پس از این افشاگری بسیاری از کشورها به ویژه سران اروپایی به این موضوع واکنش نشان دادند؛ از جمله برزیل که خواستار کاهش سطح روابط تجاری خود با آمریکا شد. آلمان نیز اصرار داشت که در خصوص جاسوسی NSA در آلمان تحقیق شود چرا که به گزارش اشپیگل، آلمان بیشترین قربانی را داشته و آمریکا از آلمان نیز استفاده کرده است. پارلمان اروپا نیز طی تحقیقاتی که نسبت به جاسوسی NSA به عمل آورد خواستار توقف برنامه های نظارت جمعی بود زیرا برنامه پریسم را سالب آزادی بیان، آزادی اندیشه، آزادی مطبوعات و ابزاری برای سوء استفاده از آن علیه مخالفان سیاسی می دانست. پارلمان، برنامه های نظارت جمعی غیرهدفمند، مخفی و گاهی غیرقانونی را برای مبارزه با تروریسم غیرقابل توجیه دانست.

از طرفی کشورهای هایی که برتری اطلاعاتی نسبت به سایر کشورها دارند با دستیابی و کنترل بیشتر بر داده ها، در راستای کنترل و جهت دهی افکار عمومی و انقلاب ها اقدام می کنند. این موضوع می تواند در مورد کشورهایی که دارای مواضع مخالف با قدرت های بزرگ مانند ایالات متحده آمریکا هستند، خطرناک و مشکل ساز باشد زیرا قدرت های اطلاعاتی می توانند در پروژه آپلود به گونه ای عمل کنند که رویکردها را به نفع خود تغییر داده و در پروژه دانلود از جهت گیری جوامع مختلف مطلع شده و در راستای اهداف خود برداشت کنند؛ به عبارت دیگر افکار عمومی را هدفمند سازند و در نتیجه آن به صورت نرم در حاکمیت سایر کشورها مداخله کنند.

نظر به اینکه مبارزه با تروریسم و حفظ صلح و امنیت بین المللی تعهد تمامی کشورهاست، می توان از ظرفیت دفتر مبارزه با تروریسم سازمان ملل و نیز همکاری های چندجانبه دولت ها در جهت مبارزه با تروریسم و استفاده صلح آمیز از کلان داده ها استفاده کرد. علاوه بر این، الحاق کشورها به معاهدات مربوط و اتخاذ قوانین ویژه ضد تروریسم در حیطه قوانین داخلی موثر خواهد بود.

با توسعه مداوم فناوری های نوین، استفاده و وابستگی ما به کلان داده ها امری اجتناب ناپذیر است. با این حال نباید از نظر دور داشت که حقوق افراد نباید قربانی امنیت عمومی و حفاظت از آن شود؛ از این رو باید به الزامات اولیه

مانند حریم خصوصی آنلاین افراد توجه شود. در تعارض بین حریم خصوصی و کلان داده باید به این موضوع توجه داشت که حفظ حریم خصوصی به معنای پنهان کردن اطلاعات نیست بنابراین با توجه به این که حریم خصوصی مفهومی سیال است می توان از طریق ارائه جزئیات نظام مند و ایجاد شفافیت به تعادل میان حریم خصوصی و کلان داده دست یافت. همچنین نباید فراموش کرد که در صورت تعارض بین قانون و اخلاق، اولویت با اخلاق است. زیرا قانون وضع شده زمانی مقبولیت عام دارد که از مسیر اخلاق گذشته باشد.

تضمین حقوق افراد از طریق مقررات و قانونگذاری در حوزه فناوری‌های دیجیتال و تصویب معاهدات در زمینه رعایت حریم خصوصی در جمع آوری، استفاده و اشتراک گذاری داده امکان پذیر است. وضع مقررات عمومی حفاظت از داده های عام (GDPR) اتحادیه اروپا اجرایی در سال ۲۰۱۸ و پذیرش حق فراموشی توسط اتحادیه اروپا را می توان از گام های مثبت در این راستا دانست. البته با توجه اینکه حق بر فراموشی هنوز در تمام کشورها پذیرفته نشده و از طرفی مقررات فوق تنها در منطقه اقتصادی و اتحادیه اروپا به تصویب رسیده است نمی توان اجرای آن را به خارج از مرزهای اتحادیه تسری داد؛ به عبارت دیگر حذف داده هایی که شخص در اینترنت وارد می کند تنها در همین منطقه امکان پذیر است در حالی که داده های وی در سایر مناطق جهان در دسترس دیگران خواهد بود؛ بنابراین انتظار می رود که در آینده از آن حمایت بین المللی به عمل آید و یا مقرراتی مشابه و به صورت گسترده، با توافق تمام کشورها به تصویب برسد. همچنین حذف داده ها در جهت اعمال حق بر فراموشی می تواند منجر به محدودیت حق آزادی بیان سایر افرادی شود که داده های شخص را بازنشر کرده و یا راجع به آن اظهار نظر می کنند؛ بنابراین پیش بینی می شود برای ایجاد تعادل در این خصوص اشخاص یا نهاد هایی که صلاحیت قضایی و دانش حقوق بشری دارند این وظیفه را به عهده گیرند.

هوش مصنوعی و ارزش‌های دموکراتیک

افشین عزیزی – دانش آموخته کارشناسی ارشد حقوق ارتباطات دانشگاه علامه طباطبائی
سارا صلح‌چی – دانشجوی کارشناسی ارشد حقوق مالکیت فکری دانشگاه علامه طباطبائی

مفهوم دموکراسی از دوران یونان باستان که از نگاه فلاسفه ای نظیر افلاطون، مفهومی هم راستای حکومت های جور و ستم داشت، تا آنچه امروز از دموکراسی می‌فهیم مسیری طولانی طی نموده است. امروزه دموکراسی مفهومی هم راستا با حقوق بشر یافته تا جایی که می‌توان مدعی شد حقوق بشر مولود دموکراسی نوین است و از زمان صدور اعلامیه حقوق بشر و شهروند فرانسه تا کنون، حقوق بشر و دموکراسی با تأثیر و تأثر متقابل، مردمی و کارآمدتر گشته و معنا و مفهومی مشخص و فراگیرتر یافته‌اند (اینجا، ص ۱۸۸) بگونه ای که درک یکی از این دو بدون درک دیگری دشوار می‌نماید. در همین راستا، برخی اندیشمندان بر این باور هستند که نیل به دموکراسی غایت دست نیافتنی و هدف اصلی اداره حیات جمعی انسان ها در سده های اخیر بوده (اینجا، ص ۴۱۲) و چه بسا بتوان مراد و خواست نهایی تهیه کنندگان اعلامیه ها و اسناد حقوق بشری از جمله منشور ملل متحد، اعلامیه جهانی حقوق بشر و میثاقین (اینجا و اینجا) را نیل به ارزش های دموکراتیک دانست.

در این بستر، نقش آفرینی روزافزون فناوری در مناسبات مختلف بشری و شئون مختلف زندگی انسان، موجب حضور پررنگ هوش مصنوعی در تمام شئون زندگی فردی، سیاسی و اجتماعی شده است. هوش مصنوعی به عنوان شکلی از فناوری که با استفاده از مهارت‌های مرتبط با هوش انسانی، می‌تواند مانند انسان فکر کند، منطقی بیندیشد و منطقی عمل کند و با دارا بودن برخی توانایی های همانند انسان نظیر درک، یادگیری، استدلال و عملکرد هوشمندانه، در بهبود شرایط زندگی انسانی اثر گذاشته و تردیدی نیست که توانسته است از این رهگذر در مواردی به بهبود حکمرانی و برخی ارزش های دموکراتیک نیز یاری رساند. هوش مصنوعی در کنار فوایدی که در ادامه به برخی از آنها اشاره می شود، مضرات فراوانی نیز با خود به همراه داشته است، تا جایی که برخی آن را مخرب ترین فناوری عصر حاضر و فناوری ذاتا مخالف ارزش های دموکراتیک می‌دانند. در تحلیل این دو دیدگاه افراطی در ارزیابی تاثیر هوش مصنوعی، می توان گفت که هوش مصنوعی محصولی جدید و با زوایای ناشناخته فراوانی است که در کنار جنبه های مثبت خود می تواند مضرات و خطرات فراوانی نیز داشته باشد که بررسی آن ها می تواند به بهبود فرآیندهای موجود و تقویت محصولات آینده کمک کند و نمی توان به واسطه برخی مضرات به طور کل خواهان برچیده شدن آن شد.

در همین راستا مقررات مختلفی در سطح منطقه ای و بین المللی به منظور اخلاقی و ضابطه مند کردن استفاده از هوش مصنوعی وضع و تدوین شده است که از جمله می توان به منشور اخلاقی اروپا در مورد استفاده از هوش

مصنوعی در سیستم های قضایی تدوین شده توسط کمیسیون اروپا برای کارآمدی عدالت مصوب ۲۰۱۸ اشاره نمود که ضمن تأکید بر بهبود کارآیی نظام های قضایی توسط هوش مصنوعی، بر این مهم تأکید می کند که تحولات حوزه هوش مصنوعی باید به شکلی مسئولانه ضمن پاسداشت و تضمین حقوق بنیادین شهروندان، رعایت اصولی نظیر عدم تبعیض، امنیت، شفافیت، بی طرفی و انصاف را در سرلوحه اقدامات خود قرار دهد. علاوه بر این، پیش نویس نخستین توصیه نامه یونسکو در خصوص اخلاق هوش مصنوعی که با امضای ۱۹۳ کشور به تصویب رسیده، به عنوان اولین چارچوب قانونی جهانی در زمینه هوش مصنوعی، ضمن نشان دادن میزان اهمیت هوش مصنوعی و تهیه مقرراتی حول محور آن، بیانگر نگرانی دولت ها از مخاطرات احتمالی جنبه های اخلاقی هوش مصنوعی است. این پیش نویس چارچوبی منطقی برای ارزیابی اخلاقی ملاحظات در خصوص رعایت انصاف، دقت، شفافیت و همچنین برخی نگرانی های جدید نظیر عدالت جنسینی توسط هوش مصنوعی ارائه داده و می تواند شاخصی قدرتمند برای ارزیابی اخلاقی و حقوقی مسائل هوش مصنوعی باشد.(برای مطالعه بیشتر نک به اینجا و اینجا)

در این نوشتار نقش هوش مصنوعی را در ارتقاء یا تنزل جایگاه ارزش های دموکراتیک با معیارهای حقوق بشری در سه مؤلفه یعنی برابری، تضمین عدالت و مشارکت در حیات سیاسی که در سال های اخیر و با گسترش هوش مصنوعی بیش ازدیگر مؤلفه ها دارای حاشیه و موجب نگرانی بوده، مورد بررسی قرار می دهیم.

برابری، هوش مصنوعی و رسوب ذهنی تصورات تبعیض آمیز

اعتقاد به برابری انسان‌ها فارغ از رنگ، نژاد، دین و مذب، جنسیت و... در کنار یکی دانستن ارزش انسان ها بر پایه کرامت ذاتی نوع بشر از والاترین ارزش‌های بشری است، به نحوی که صدر مقدمه منشور ملل متحد با بیان «اعلام مجدد ایمان خود به حقوق اساسی بشر و به حیثیت و ارزش شخصیت انسانی و به تساوی حقوق بین مرد و زن و همچنین بین ملت ها اعم ازکوچک و بزرگ»، بر این مهم تأکید ویژه می نماید. اعلامیه جهانی حقوق بشر نیز ضمن مساوی شمردن روح انسان ها از نظر حیثیت و کرامت ذاتی ابناء بشر و با محکوم کردن تحقیر و تخفیف انسان ها در مقدمه اعلامیه، به موجب ماده ۱، برابری را در تمامی شئون ممکن برای انسان‌ها حتمی فرض می نماید.

امروزه هوش مصنوعی کاربردهای فراوانی در حوزه مدیریت و کمک به مدیران برای برنامه ریزی، تصمیم گیری و نظارت بر کارکنان در کنار زمینه هایی نظیر احراز هویت یافته است که می توان از جمله به تشخیص هویت فرد به وسیله صدا، تصویر، چهره، عنبیه چشم، شکل صورت و... اشاره کرد که در مواردی همچون بانکداری الکترونیک، ورود به سیستم های امنیتی و تلفن همراه و... کاربرد دارد. سپردن برخی از امور مرتبط با انسان به هوش مصنوعی، نویدبخش از بین رفتن نگاه های تبعیض آمیز یا ناشی از علقه های شخصی به دیگران بود، اما شیوه کار بعضی از انوع هوش مصنوعی نشان می‌دهد برخی نرم افزارهای آنالیز صورت و تشخیص چهره که عموما مراحل آزمایشی را بر روی صورت افراد سفیدپوست طی نموده‌اند، به دلایلی از جمله نحوه برنامه نویسی و الگوریتم های به کار رفته

در آنها فاقد امکان شناسایی و تشخیص چهره رنگین پوستان هستند. (اینجا و اینجا) از این‌رو این احتمال که سازندگان این ابزارهای هوش مصنوعی در تحقیقات و آزمایش‌های خود سیاه‌پوستان را درنظر نگرفته‌اند، می‌تواند توجیهی بر سوگیری و نگاه تبعیض آمیزی باشد که به‌صورت ناخواسته از سوی محققین و طراحان این حوزه به‌وجود آمده است.

این تبعیض علاوه بر رنگین پوستان شامل حال جامعه زنان نیز شده و بررسی برخی محصولات غول‌های فناوری نظیر IBM، مایکروسافت و آمازون نشان می دهد این دست ساخته های بشر در تشخیص چهره مردان سفیدپوست عملکرد بهتری از خود نشان داده اند. این تبعیض و تفاوت در تشخیص تا آنجاست که میزان اشتباه در تشخیص مردان سفیدپوست از ۱٪ فراتر نمی‌رود اما گاهی در زنانی با پوست تیره به ۳۵٪ نیز می رسد و حتی سیستم های هوش مصنوعی شرکت های پیشرو نتوانسته اند چهره اشخاص شناخته شده ای نظیر اپرا وینفری، میشل اوباما و سرنا ویلیامز را به درستی تشخیص دهند. (اینجا) اشکالات موجود در سیستم‌های تشخیص چهره رنگین پوستان از مواردی ساده و روزمره نظیر اخلال در استفاده این اشخاص در استفاده از الگوی تشخیص چهره برای باز کردن صفحه تلفن همراه گرفته تا ورود به محل کار در مشاغلی که ورود به فضای کاری آنان با اسکن تصاویر کارکنان انجام می‌پذیرد و اشتباه در تشخیص صحیح چهره رنگین پوستان در تصاویر وبکم ها و دوربین های دیجیتال را شامل می‌شود.

اما این نقصان به همین موارد ختم نمی‌شود و در مواردی اشتباهات و سوگیری های هوش مصنوعی به شکل هایی از تبعیض می انجامد که می تواند سلامت و یا امنیت فردی و آزادی شهروندان رنگین پوست را دچار مخاطره سازد که از جمله می توان به غربالگری بیماران با کمک هوش مصنوعی به منظور قرار گرفتن بیماران با خطر بالا در اولویت درمان در برخی مراکز درمانی اشاره کرد. بررسی نتایج غربالگری ها حاکی از آن بود که هوش مصنوعی شمار بیشتری از بیماران سفیدپوست را (که در شرایط مشابه با بیماران سیاه پوست قرار داشتند) در معرض خطر شناخته و در نتیجه در اولویت درمان قرار می داده است. همچنین، در حالی که در سال های اخیر استفاده از دوربین‌های تجزیه و تحلیل کننده چهره اشخاص در برخی اماکن عمومی و توسط نیروهای پلیس در ایالات متحده رو به افزایش است، بررسی ها نشان می دهد این دوربین ها که به کمک هوش مصنوعی به تجزیه و تحلیل چهر ها و پیش بینی خطرناک بودن شخص یا حضور شخصی با سابقه مجرمانه در محل های مختلف می پردازند، به طرز محسوسی رنگین پوستانی از جمله سیاه پوستان و چینی تباران را افرادی خطرناک تر از سفیدپوستان تشخیص داده و حتی در مواردی، به اشتباه فردی را مظنون به ارتکاب جرم شناخته و در معرض بازداشت اشتباه قرار داده است.

همچنین در مواردی ربات هوش مصنوعی که در مقام مدیر منابع انسانی فعالیت می کرد با پردازش این نکته از اسناد موجود که بیشتر همه مدیران برخی از بخش های شرکت مرد بوده اند، به صورت پیش فرض، متقاضیان جنسیت

دیگر را رد کرده است. درک این نکته زمانی ملموس تر می شود که بدانیم در ایالات متحده برای مشاغلی نظیر حمل بار نیز نمی توان به صورت مستقیم جنسیتی خاص را مخاطب آگهی شغلی قرار دهید و اساسا پرسش از جنسیت در زمان جذب نیروی کار می تواند با پیگرد قضایی، همراه باشد. سوءگیری هوش مصنوعی در این زمینه تا آنجا پیش رفت که علی رغم آن که گفته می شد هوش مصنوعی در زمینه مدیریت منابع انسانی کماکان بهتر از انسان عمل می کند، شرکت آمازون استفاده از این ابزار را متوقف نمود . همچنین، نهادهایی نظیر شورای شهر نیویورک و شورای شهر دیترویت استفاده از هوش مصنوعی را در فرایند استخدامی افراد محدود ساخته و منوط به برخی شفاف سازی ها و اثبات عدم وجود سوگیری جنسیتی و نژادی در این فرایند دانسته اند. بنابراین به نظر می رسد نگاه های تبعیض آمیز نهادینه شده در برخی انسان ها، به صورت آگاهانه یا غیرآگاهانه در قالب الگوریتم به دنیای بدون احساس هوش مصنوعی نیز وارد شده که جا دارد با آگاهی و تغییر فرآیند ساخت این ابزارها، چنین نواقصی مرتفع گردند.

دادرسی منصفانه و نقش دوگانه هوش مصنوعی

شیوه دادرسی همواره از دغدغه های مهم بشری بوده و تبلور آن در اسناد حقوق بشری و قوانین داخلی کشورها مبین اهمیت و ارزش دادرسی منصفانه است. بروز خطاهای اجتناب ناپذیر انسانی و تأثیرات عمیق فردی و اجتماعی اشتباه در نظام دادرسی در کنار بیم همیشگی نسبت به سوگیری دادرسان، منجر به طرح مباحث امکان سنجی استفاده از هوش مصنوعی در فرآیندهای قضایی شد. استفاده ای که می تواند جامعه بشری را هرچه بیشتر به اهداف مقرر در مواد مختلف اعلامیه جهانی حقوق بشر به ویژه مواد ۷ تا ۱۱ اعلامیه و بند ۳ ماده ۲ و مواد ۹ تا ۱۱، ۱۴ و ۱۵ میثاق بین المللی حقوق مدنی و سیاسی نزدیک سازد.

از جمله کمک‌های هوش مصنوعی به نظام قضایی می‌توان به کمک مدل‌های هوش مصنوعی به قضات نسبت به درک تعصب و جانبداری خود در رسیدگی به پرونده ها و مبارزه با آن اشاره کرد. می‌دانیم عوامل خارجی مانند شلوغی شعبه، زمان های مختلف از روز، خستگی، دمای هوا و همچنین نزدیک بودن به زمان انتخابات (در نظام های قضایی که قاضی با رأی شهروندان انتخاب می شود) از جمله عوامل خارجی با احتمال تأثیرگذاری بر رأی دادرس هستند. در این شیوه ها زمانی که هوش مصنوعی با وزن دادن به عوامل مختلف خارجی و نسبت سنجی میان آنها تشخیص دهد توجه دادرس نسبت به پرونده کم شده و با بی توجهی در شرف صدور رأی است به مقام قضایی هشدارهای لازم را می هد. همچنین در نظام قضایی ایالات متحده آمریکا نرم افزارهایی وجود دارند که با تحلیل داده های مجرمانه امکان تکرار عمل مجرمانه را محاسبه و در تعیین مواردی مانند صدور یا عدم صدور قرار بازداشت، تعیین میزان وثیقه و...، علی رغم انتقادات وارده ، به کمک مقام قضایی می شتابند.

با این تحولات، می توان به راحتی روزی را پیش بینی کرد که از هوش مصنوعی در برگزاری محاکم بین المللی نیز استفاده شود که چنین رویکردی با توجه به برخی انتقادات در مورد بی غرض نبودن قضات این مراجع (نک برای نمونه به اینجا و اینجا) یا در مواردی که با حضور قاضی اختصاصی یکی از طرفین برگزار می‌شود، می تواند در اعتباربخشی به آرای این قضات و پذیرش آن توسط طرفین و جامعه بین المللی نقشی موثر ایفا نماید. اما در کنار همه مواهبی نظیر افزایش اعتبار آرای صادره از منظر بی طرفی دادرس و عدالت قضایی در کنار کاهش هزینه‌ها و افزایش سرعت دادرسی، استفاده از هوش مصنوعی هنور به آن مرحله ای از دقت، صحت و سلامت نرسیده که بتوان با اطمینان کامل زمام امور را به دست این ابزارهای ساخته دست بشر سپرد. کما اینکه برخی بررسی های صورت گرفته در خصوص نرم افزارهای استفاده شده در نظام قضایی ایالات متحده نشان داد این نرم افزارها نسبت به متهمان سیاه پوست از خود حساسیت و سخت گیری بیشتری نشان می دهند، گویی که عدالت کیفری تا حدی به دست و ذهن مهندسان نرم افزار و برنامه نویسان رایانه ای سپرده شده است. از این رو در دادرسی های بین المللی نیز با توجه به تفوق علمی و دانش کشورهای اروپای غربی و آمریکای شمالی در دسترسی به فناوری های مرتبط با هوش مصنوعی و قرابت نژادی، دینی و مذهبی و رنگ پوست و باورهای مشترک این دو گروه، برخلاف رویه در پیش گرفته شده توسط برخی کشورها در استفاده از هوش مصنوعی در نظام قضایی خود ، اعتماد به هوش مصنوعی نمی‌تواند چندان اطمینان بخش باشد. از این رو اگر نتایج حاصل شده از تجربه نسبتا امیدوارکننده و موفقیت بیش از هفتاد درصدی هوش مصنوعی در پیش بینی آرای صادره از محاکم حقوق بشری اروپایی، مقدمه و زمینه ساز استفاده از هوش مصنوعی در این محاکم باشد، باید گفت هنوز شرایط مناسب برای سپردن امکان قضاوت در محاکم بین‌المللی به هوش مصنوعی فراهم نیست. در نتیجه، به نظر می رسد سپردن دادرسی یا تحقیقات مرتبط با پرونده به هوش مصنوعی در دادرسی های بین المللی در زمان فعلی، ممکن است بشریت را به دام تبعیض ناخواسته ای بیندازد و دادرسی ها را از مسیر انصاف و عدالت خارج ساخته و به سدی در مقابل تحقق اهداف مقرر در منشور ملل متحد و اعلامیه مبدل گردد.

با وجود آنکه فناوری فعلی هوش مصنوعی تا رسیدن به چنین مرحله ای فاصله دارد، اما تاکید بر این مهم ضروری است که قاعده مند نمودن هوش مصنوعی و کاهش خطرات ناشی از آن در حوزه عدالت قضایی، همان گونه که در منشور اخلاقی اروپا در مورد استفاده از هوش مصنوعی در سیستم های قضایی و قطعنامه ۱۶ فوریه ۲۰۱۷ پارلمان اروپا نیز تصریح شده است، در صورتی موفق خواهد بود که اقدامات هوش مصنوعی شفاف و قابل توضیح گردند. از این رو لازم است هوش مصنوعی بتواند برای تصمیمات خود استدلال نموده و فرد انسانی ناظر را در خصوص تصمیم اتخاذ شده قانع نماید، در غیر این صورت تا زمان رسیدن به چنین مرحله ای، استفاده از هوش مصنوعی در امور اداری اقدامات قضایی نظیر مدیریت پرونده ها، تقسیم دارایی زوجین در پرونده های طلاق و خسارت وارده به

اشخاص، رسیدگی به درخواست و سوال های شهروندان، تشخیص شواهد و اسناد مجعول و... می تواند تصمیمی معقول و کم خطر تر باشد.

هوش مصنوعی و تأثیر بر انتخابات آزاد در فراسوی مرزها

امروزه به دلیل شرایط مختلف حاکم بر جوامع و زندگی اجتماعی، امکان مشارکت مستقیم همه مردم در تعیین سرنوشت سیاسی و اجتماعی وجود ندارد و از این رو اصل نمایندگی به عنوان جانشین نه چندان مطلوب اما اجتناب ناپذیر برای دموکراسی مستقیم انتخاب شده، هرچند بسیاری نیز معتقدند نمایندگی می‌تواند ایفاگر نقشی به مراتب موثرتر از دموکراسی مستقیم ایفا کند (اینجا، ص ۱۱۰). از همین رو است که برخی بر این باورند اگر سه عنصر نصب حاکمان با رأی عمومی، نظارت بر اعمال حاکمان و امکان عزل آنان با رأی عمومی در جامعه‌ای فراهم گردد، آن زمان می توان مدعی تحقق ارزش های دموکراتیک در آن سرزمین شد (اینجا، ص ۴۱۳).

خودکامگان و آنان که با احترام به خواست و نظر عمومی بیگانه هستند و افکار و اندیشه های خود را در مقبول عامه شهروندان نمی بینند، از هیچ تلاشی برای تقلب و دستکاری در انتخابات و یا مهندسی آن فروگذار نیستند. بنابراین اگر تا همین اواخر تقلب و مهندسی در انتخابات با کمک نیروهای قهریه، گزینش کاندیداها و شمارش سلیقه ای آراء و امثال آن صورت می گرفت، امروزه برگزاری الکترونیک انتخابات در بسیاری از کشورها و گسترش بی سابقه و نفوذ فراوان تبلیغات پیدا و پنهان شبکه های اجتماعی بر ذهن مخاطب، منجر به تلاش دست اندرکاران به ویژه صاحبان قدرت و دولتمردان در اقصی نقاط دنیا برای تأثیرگذاری بر انتخابات از طریق هک سیستم های اخذ و شمارش رأی و یا مهندسی انتخابات توسط ابزارهای مختلف از جمله هوش مصنوعی شده است. به بیانی، از آنجایی که یکی از کارکردهای دموکراسی، نوعی مشروعیت گرفتن برای قدرت است، برخی به منظور مشروع جلوه دادن قدرت خویش از طریق کارکردهای فناوری از جمله هوش مصنوعی دست به اقداماتی می زنند که ارزش های دموکراتیک را در جهان با تهدید جدی مواجه می‌سازد.

از جمله روش ها برای تأثیرگذاری بر افکار عمومی در فضای مجازی می توان به استفاده از ربات های اجتماعی اشاره کرد که برای تقویت سبد رأی نامزدهای انتخابات و متقاعد کردن رأی دهندگان به رأی دادن یا ندادن به کاندیدایی خاص اقدام می نمایند. این گروه از ربات ها زمانی که وارد کارزارهای تبلیغاتی سیاسی باشند، «ربات های سیاسی» نامیده می شوند و می توانند با تولید لایک، حساب کاربری متعدد و دنبال کننده جعلی برای کاربران مدنظرشان، دست به تولید محتوای عمومی، کلمات کلیدی و هشتگ های مرتبط بزنند و یا محتواهای خود را در شبکه های اجتماعی و هشتگ های مرتبط با اهداف برنامه ریزی شده منتشر نمایند تا نوعی پروپاگاندا برای حمایت/تخریب کاندیدا یا جریانی خاص ایجاد شود و مخاطب نیز بدون اینکه بداند همه این جوسازی ها محصول فعالیت یک یا چند دستگاه رباتیک است، اسیر جوسازی ایجاد شده گردیده و به رأی دادن یا ندادن به شخص یا

اشخاصی خاص ترغیب می گردد. برای نمونه، بررسی ها نشان می دهد حدود یک پنجم کل توییت های مرتبط با انتخابات ریاست جمهوری ۲۰۱۶ ایالات متحده و یک سوم توییت ها در مورد برگزیت توسط ربات ها ارسال شده بودند. از بیم همین تهدیدها است که در سال های اخیر اسناد راهبردی متعددی از جمله توسط اتحادیه اروپا و همچنین در سطح دو جانبه، در راستای نظام مند ساختن تبلیغات سیاسی در دستور کار قرار گرفته اند، که از این میان می توان به همکاری مشترک فرانسه و کانادا برای گسترش مسئولیت پذیری بین‌المللی هوش مصنوعی و هرچه نزدیک تر ساختن شیوه کار این ابزارها با اصول حقوق بشری، دستورالعمل رفتاری اطلاعات نادرست کمیسیون اروپا سال ۲۰۱۸ و بازنگری آن در سال ۲۰۲۲ با تأکید بر شفافیت تبلیغات سیاسی و آگاه شدن مخاطب از چرایی مخاطب قرار گرفتن در این تبلیغات، برنامه عملیاتی اتحادیه اروپا علیه اطلاعات نادرست- ۲۰۲۰ و برنامه اقدام دموکراسی اروپا- ۲۰۲۰ ، اشاره کرد.

در سال های اخیر گزارش های متعددی از تأثیر ربات های اجتماعی و اخبار جعلی در انتخاب مختلف از جمله همه پرسی خروج از برگزیت در بریتانیا و انتخابات ریاست جمهوری ایالات متحده آمریکا در سال ۲۰۱۶، انتخابات ایالتی ۲۰۱۷ در آلمان، انتخابات ریاست جمهوری ۲۰۱۷ فرانسه، و انتخابات سوئد در سال ۲۰۱۸ مخابره شده است. یکی از معروف ترین این نمونه ها تاثیر الگوریتم های به کار رفته در فیسبوک در انتخابات ریاست جمهوری ۲۰۱۶ ایالات متحده آمریکا است. در این ماجرا که به جنجال سیاسی بزرگی در این کشور تبدیل شد، هوش مصنوعی فیسبوک با کمک داده های مرتبط با یک تست شخصیت شناسی، تبلیغات هر شخص واجد رأی دادن را متناسب با تیپ شخصیتی او به کار می برد، همچنین اخبار و پست‌های نمایش داده شده در صفحه هریک از کاربران به گونه ای طراحی شده بود که اخبار حمایتی از دونالد ترامپ و در مخالفت با هیلاری کلینتون را به صورتی هدفمند و بر اساس علایق کاربران نشان دهد و به صورت غیرمستقیم افراد فاقد تمایل به رأی دادن را برای رأی دهی به ترامپ ترغیب نماید.

تردیدی نیست که دست کاری هایی از قبیل موارد اشاره شده در پاراگراف پیشین، در صورت اثبات اهرمی علیه تحقق ارزش های دموکراتیک و تهدید کننده آن به شمار می روند و در صورتی که مشخص شود دولتی خارجی یک طرف این تبلیغات غیرمستقیم اما هدفمند است، می‌تواند از مصادق نقض اصول مهم و بنیادین حقوق بین الملل همچون عدم مداخله و حق تعیین سرنوشت باشد. ازجمله در انتخابات ایالات متحده، انگشت اتهام به سوی حکومت روسیه و شخص رئیس جمهور این کشور دراز بود و دخالت نهادهای امنیتی، نظامی و همچنین مجالس ایالات متحده و واکنش تند این نهادها را در پی داشت. اهمیت برگزاری انتخابات سالم و بدون حاشیه در تعیین شاخص‌های دموکراسی در حدی است که گزارش سالانه سنجش شاخص دموکراسی اکونومیست در سال ۲۰۱۷، به‌سبب تردیدهای ایجاد شده در خصوص صحت انتخابات ریاست جمهوری ۲۰۱۶ ایالات متحده، سطح دموکراسی

این کشور را از دموکراسی کامل به دموکراسی ناقص تنزل داد. اگرچه در این زمینه عموما به دلیل هزینه و تخصص فراوان ، نقش سرویس های اطلاعاتی دولت های خارجی در دستکاری انتخابات پررنگ است و در نتیجه وضع قوانین کیفری فاقد بازدارندگی لازم است، اما برخی ایالات ها نظیر کالیفرنیا با وضع برخی قوانین ایالتی نسبت به ارائه تعریف از ربات ها در فضای مجازی اقدام نموده و فعالیت ربات ها را به صورتی که برای کاربران نامشخص باشد، ممنوع ساخته اند و بر این اساس ربات ها باید با علامت و مشخصاتی خاص، قابل شناسایی باشند.

همچنین استفاده غیر اخلاقی و غیرقانونی از هوش مصنوعی و به ویژه در قالب «جعل عمیق» که برای اولین بار با ویدیویی از باراک اوباما به شهرت رسید، می تواند علاوه بر انتخابات، در برخی بزنگاه ها نظیر روزهای پرتنش جنگ روسیه و اوکراین، بر آتش مخاصمات بیفزاید و چه بسا اگر جعل عمیقی از رئیسان یا مقامات ارشد یکی از این کشورها یا سازمان های ثالثی نظیر اتحادیه اروپا و ایالات متحده در این روزها منتشر شود، پیش از آن که جعلی بودن آن به اثبات برسد، موجب بر زمین ریختن خون انسان های بسیاری گردد. تهدیدی که نیازمندی به تمهیدات لازم نظیر الزام به درج علامت «دیپ فیک» بر روی تصاویری تولیدی از این ابزار در کشور چین، اقدام به شناسایی و حذف ویدیوهای دیپ فیک توسط فیسبوک، توییتر، اینستاگرام و ردیت علی رغم دشواری های عملیِ این اقدام، جرم انگاری دیپ فیک و انعقاد موافقت نامه های بین المللی برای توسعه همکاری بین کشورها برای مقابله با استفاده های غیر مجاز و وضع تحریم های اقتصادی علیه دولت های استفاده کننده از این فناوری برای رفع ایرادات موجود را ضروری می نماید. (برای بررسی بیشتر این اقدامات برای نمونه نک. به اینجا)

سخن پایانی

در پایان باید توجه داشت، همان گونه که در توصیه نامه اخلاقی یونسکو نیز ذکر شده است، اگرچه استفاده غیراصولی و به دور از مقررات حقوق بین الملل می تواند به تعمیق شکاف و نابرابری ها چه در عرصه داخلی و چه بین المللی منجر شود، اما این ملاحظات و نگرانی ها نباید به سدی در راه توسعه علم و تکنولوژی مبدل گردد، بلکه باید با شناخت دقیق این قبیل نوآوری ها، دست به اقداماتی اساسی برای قانون مند و اخلاقی نمودن آن ها زد. توصیه نامه یونسکو همچنین تأکید می کند که به کارگیری اصول اخلاقی پذیرفته شده بشری از جمله موارد مندرج در منشور ملل متحد، اعلامیه جهانی حقوق بشر و سایر اسناد بین المللی حقوق بشری در زمینه هوش مصنوعی می تواند در کاهش نگرانی ها نسبت به جنبه های اخلاقی هوش مصنوعی راهگشا باشد.

همچنین برخی تمهیدات توسط ارائه دهندگان خدمات آنلاین و همچنین دولت ها نظیر ضابطه مند نمودن و وضع مقرراتی برای تبلیغات سیاسی ـ اجتماعی آنلاین، برخی محدودیت ها برای حساب های کاربری رباتیک و یا ممنوعیت استفاده از آن، برچسب دار و مشخص نمودن نظرات و پست های تبلیغاتی و با خاستگاه غیرانسانی، نظارت بر هرچه بیشتر منطقی شدن تصمیمات اتخاذ شده توسط هوش مصنوعی و افزایش شفافیت در خصوص شیوه کار

این ابزار و اطلاع رسانی شفاف به شهروندان در صورت وجود نقص در سیستم های هوش مصنوعی در کنار تصویب اسناد بین المللی برای همکاری در راستای کاهش سوء استفاده از این فناوری، می تواند منجر به کاهش خطرات و نگرانی های ناشی از هوش مصنوعی شده و این فناوری را در هرچه بیشتر همگام شدن با ارزش های دموکراتیک یاری رساند.

با این حال به نظر می رسد در مواردی، هرچه توانایی دولت ها بر کنترل و نظارت بر هوش مصنوعی افزایش یابد، امکان تعرض به ارزش های انسانی و دموکراتیک نیز فزونی می یابد (برای نمونه نک به سیاست چین در قبال هوش مصنوعی در اینجا). بنابراین باتوجه به اینکه به نظر می رسد اعتماد به شرکت ها و اتکا به خود تنظیم گری نیز نتوانسته است توقعات نظارتی در خصوص استفاده از هوش مصنوعی را جبران سازد، جا دارد تا حد ممکن وضع و نظارت بر مقررات از طریق نظام های تنظیم گری غیردولتی و یا مشارکتی صورت بپذیرد و توجه دولت‌ها به تضمین حقوق و حمایت های بنیادین بشری در راستای ارزش های دمکراتیک در طراحی و بکارگیری هوش مصنوعی معطوف گردد.

آیا ربات‌ها باید قاضی شوند؟ از «نویز» تا عدالت

دکتر سید محسن اسلامی- گروه فلسفه دانشگاه تربیت مدرس

ساعت چند است؟

برای آنکه سطح عدالت در یک سیستم قضایی را بسنجیم لازم نیست بدانیم عدالت دقیقاً چیست و در هر موردی چه اقتضایی دارد. فرض کنید می‌خواهید بدانید ساعت چند است. ساعت مچی خود را نگاه می‌کنید: حدود ۱۰:۱۵ را نشان می‌دهد. چند دقیقه بعد از جلوی مغازه‌ای می‌گذرید و چشم‌تان به ساعت روی دیوار می‌افتد: ساعت حدود ۱۱ را نشان می‌دهد. سریعاً متوجه می‌شوید یک جای کار می‌لنگد – نمی‌دانید الان ساعت چند است، اما می‌دانید در موقعیت خوبی برای دانستن زمان نیستید. به کدام ساعت باید اعتماد کرد؟ ساعت چند است؟

«نویز» چارچوبی را فراهم می‌کند تا این موقعیت را بهتر بفهمیم. در ادامه با این مفهوم بیشتر آشنا خواهیم شد. اما اجمالاً منظور این است: ما انتظار داریم سیستم‌ها به نحو منسجم و قابل‌اعتمادی کار کنند. مثلاً انتظار داریم وقتی به ساعت‌ها نگاه می‌کنیم زمان را درست نشان دهند. اگر ساعت‌ها با هم نخوانند معلوم می‌شود مشکلی در کار است و در معرض خطا هستیم. حالا مثال دیگری را در نظر بگیرید: به توصیه پزشک آزمایشی داده‌اید. نتیجه آزمایش را، محض احتیاط، به دو پزشک نشان می‌دهید. یکی از آن‌ها می‌گوید «همه چیز عادی و خوب است! سبک زندگی فعلی‌ات را حفظ کن.» دیگری می‌گوید «وضعیت قند خون نگران‌کننده است و باید تغییرات اساسی در سبک زندگی‌ات اعمال کنی. ضمناً چند نکته دیگر هم هست که بهتر است درباره آنها با متخصص مربوط صحبت کنی.» این موقعیت نگران‌کننده است. لازم نیست متخصص پزشکی یا تفکر انتقادی یا فلسفه علوم تجربی باشیم تا این موقعیت ما را به فکر وادارد. اگر پزشکان در موضوع واحدی که ما انتظار داریم قضاوت واحدی داشته باشند و در واقع قضاوت‌های مختلفی ارائه کنند با نویز مواجه هستیم و می‌گوییم سیستم پزشکی نویزی است. یا اگر کارشناسی امروز یک نظر بدهد و فردا درباره همان موضوع نظر دیگری بدهد، قضاوت‌های او نویزی هستند – ما انتظار داریم او درباره موضوع واحد قضاوت واحد داشته باشد. هر گاه که انتظار قضاوت واحد داریم اما در عمل قضاوت‌ها مختلف هستند با نویز سروکار داریم و نویز علی الاصول خبر خوبی نیست: اگر قضاوت‌های یک فرد یا سیستم نویزی باشد، با این سؤال مواجه می‌شویم که چگونه و چرا به او اعتماد کنیم. پدیده ساده است، اما لغزنده و مستعد غفلت. (فیلسوفان طی دو ده اخیر به این مسئله ذیل عنوان «اختلاف‌نظر» (disagreement) توجه ویژه داشته‌اند و امروزه این بحث از موضوعات مهم در معرفت‌شناسی است.)

حال چرا همین نکته را درباره عدالت قضایی در نظر نگیریم و ابعاد آن را نکاویم؟ شاید گفته شود این نکته به خودی خود تازگی ندارد. برای مثال، عموماً در سیستم‌های قضایی نوعی احتمال خطا لحاظ شده است و بنابراین

می‌توان به احکام اعتراض کرد. چرا؟ مثلاً شاید در مواردی حکم بنا بر قصد وغرضی بوده باشد. پس این انتظار بی‌راهی نیست که سیستم قضایی باید جایی برای احتمال خطا داشته باشد و تدبیری برای آن اندیشیده باشد. اما نکته فوق فقط درباره امکان خطا نیست. موضوع فراتر، عام‌تر، و پیچیده‌تر از این است. ما انسانیم و قضاوت انسانی در معرض انواع خطاهاست. اگر درک درستی از نوع خطا و ابعاد آن نداشته باشیم، احتمالاً راهکارها برای جلوگیری از آن هم کارآمد نخواهند بود.

نقص‌های قضاوت چیست؟

اجازه دهید موضوع را در سطح کلی‌تری در نظر بگیریم: در حوزه‌های مختلف (از جمله، و از جهاتی، به ویژه) با قضاوت سروکار داریم: حکم می‌کنیم چیزی چنین و چنان است. عموماً هدف از این کار رسیدن به پاسخی است که به نحوی جهان را توصیف می‌کند. گاهی می‌خواهیم ببینیم ارزش کالایی چیست و گاهی می‌خواهیم چیزهایی را رتبه‌بندی کنیم و گاهی می‌خواهیم رویدادی را پیش بینی کنیم و گاهی می‌خواهیم درباره مسائل روزمره یا کلان زندگی خود تصمیم بگیریم. در همه این موارد قضاوت می‌کنیم و در معرض خطا هستیم. حواسمان هست که اینجا «قضاوت» آنطور که در فضای عمومی مصطلح است معنا ندارد، بلکه فعالیتی پایه است که از آن گریزی نیست. ما در همه زندگی خود با قضاوت به این معنا سروکار داریم، پس خطاهای قضاوت تمام وجوه زندگی ما را متأثر می‌کنند – از زندگی روزمره تا تصمیم‌های مهم زندگی شخصی تا تصمیم‌های مالی و کاری و حرفه‌ای.

اما در اینجا موضوع ما قضاوت‌ها در عرصه قضایی است. برای مثال، اینکه اتهامی وارد است یا نه، حکم متناسب با جرم چیست، و مانند آن. بدین ترتیب، عملاً تمام مطالعات مربوط به قضاوت و خطاهای آن برای سلامت قضاوت در عرصه قضایی لازم است. یکی از خطاهای آشنا در این باره «سوگیری» است. امروزه دیگر می‌دانیم که ما دچار خطاهایی نظام‌مند هستیم – بسیاری از ما، خواسته یا ناخواسته، سوگیری‌هایی علیه گروه‌هایی داریم.

اما آیا خطاهای قضاوت فقط منحصر به سوگیری است؟ واضحاً پاسخ منفی است. برای مثال، اگر اطلاعات کافی نداشته باشیم و در عین حال قضاوت کنیم رویکرد ما به قضاوت مستعد خطاست، گرچه این خطا از جنس سوگیری نیست. به همین ترتیب، مثال‌های بالا درباره زمان یا تفسیر آزمایش‌های پزشکی هم مستقیماً راجع به سوگیری نیستند.

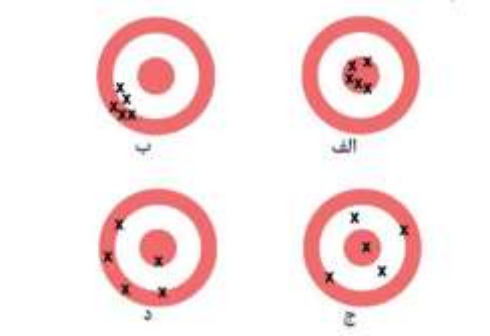
نویز فراتر از سوگیری است

دنیل کانمن، استاد ممتاز روانشناسی دانشگاه پرینستون و برنده نوبل اقتصاد، از تأثیرگذارترین افرادی است که بحث از خطاهای قضاوت و سوگیری‌های شناختی را از مطالعات دانشگاهی به عرصه عمومی کشانده است، چنانکه کتاب *تفکر کند و سریع* او هم از آثار بسیار پرارجاع در محافل دانشگاهی است و هم در کتابفروشی‌های کشورهای مختلف عرضه می‌شود و پرفروش است. در نتیجه، امروزه سوگیری‌ها بخشی از دانش عمومی هستند. مثلاً می‌دانیم افراد در ارزیابی‌های خود عوامل ظاهراً نامربوط را هم دخالت می‌دهند، چنانکه در رزومه‌های عکس‌دار نسبت به

افراد خوش‌چهره سوگیری مثبت دارند – این همان اثر هاله‌ای است؛ یا ما در فرایند فکر کردن از لنگرگاه‌هایی استفاده می‌کنیم و مثلاً اگر ابتدا از ما دو رقم آخر شماره شناسنامه‌مان را بپرسند و بعد بخواهند که قیمت کالایی را تخمین بزنیم، تخمین ما با اعداد آخر شماره شناسنامه نسبتی دارد – انگار که آن عدد نوعی لنگرگاه است و این همان سوگیری لنگر است. خلاصه، توجه به سوگیری به ما می‌آموزد که ذهن ما در معرض خطاهای نظام‌مندی است. مثلاً وقتی می‌خواهیم تخمین بزنیم که چقدر زمان برای انجام کاری لازم داریم، عموماً تخمین ما کمتر از زمان واقعی است، نه برعکس.

سال گذشته کانمن به همراه دو همکارش، کاس سانستین (حقوق‌دان هاروارد و مؤسس و مدیر برنامه اقتصاد رفتاری و سیاست‌گذاری عمومی در آن دانشگاه) و اولیویه سیبونی (استاد استراتژی در مدرسه کسب‌وکار HEC در پاریس) به نقصی دیگر در قضاوت انسانی توجه دادند: خطاهای قضاوت منحصر به سوگیری نیست؛ اگرچه سوگیری از موانع عمده است، «نویز» در عرض آن قرار دارد و خیلی اوقات تأثیر نویز حتی مخرب‌تر از سوگیری است. آن‌ها در کتاب *نویز: نقصی در قضاوت انسان* (۲۰۲۱) این پدیده را توضیح می‌دهند، ابعاد آن را می‌کاوند، و لوازم آن را در چندین حوزه، از جمله حقوق، مدیریت، کسب‌وکار، و پزشکی می‌کاوند. ترجمه این کتاب با خرید حق انتشار در ایران از سوی نشر نوین منتشر شده است.

موضوع کتاب از جهتی این است که چگونه بهداشت تصمیم را رعایت کنیم و خطا را به حداقل برسانیم، اعم از آنکه درباره استخدام نیروی کار باشد یا تشخیص حرفه‌ای و جز آن. در اینجا فقط موارد محدودی از عرصه حقوق را در نظر می‌گیریم. اما ابتدا باید با مفهوم محوری کتاب آشنا شویم: نویز.



هدف کتاب معرفی نویز به عنوان پدیده‌ای مستقل از سوگیری و تفکیک انواع آن است. نویز عبارت است از بی‌ثباتی ناخواسته و پراکنده. تصویر بالا را ببینید: تیرهای سیبل الف به هدف خورده‌اند. اما تیرهای سیبل ب دچار سوگیری هستند – خطای آن‌ها نظام‌مند است و می‌توان پیشبینی کرد که احتمالاً تیرهای بعدی هم دچار خطای مشابهی هستند. اما نویز متفاوت است. تفاوت اصلی نویز با سوگیری آن است که نظام‌مند نیست. آنچه در سیبل ج می‌بینیم نویز است: پراکندگی، خطاهای غیرنظام‌مند. و البته گاهی نویز و سوگیری همراه می‌شوند – چنانکه در سیبل د دیده می‌شود. نکته قابل‌توجه این است که حتی اگر ندانیم مرکز سیبل کجاست، می‌توانیم تشخیص بدهیم که در سیبل ج شاهد نویز هستیم. این خطایی است که می‌توانیم تشخیص بدهیم، حتی اگر ندانیم پاسخ درست کدام است. (مقایسه کنید: اگر از پشت به سیبل الف و ب نگاه کنیم، یعنی وضعیتی که معلوم نباشد قلب سیبل کجاست، نمی‌دانیم تعیین کنیم کدام به هدف زده و کدام دچار سوگیری است.)

بدین ترتیب، در موضوع قضاوت نویز را اینطور در نظر می‌گیریم: هر گاه افراد مختلف در برخورد با مسئله واحد پاسخ‌های مختلفی داشته باشند و این نامطلوب باشد، با نویز طرف هستیم. حتی وقتی فردی در پاسخ با مسئله واحد در زمان‌های مختلف پاسخ متفاوتی ارائه می‌کند با نویز طرف هستیم. گفتنی است که نویز خود انواعی دارد، شامل نویز ترازی، نویز الگویی، و نویز موقعیتی. با چند مثال منظور از این پدیده موضوع روشن‌تر خواهد شد.

نظام‌های قضایی هم نویزی هستند

نویز به نحو عجیبی در حوزه‌های مختلف حاضر است، اما همچنان دیده نمی‌شود و گویی نامرئی است، چنانکه سوگیری نیز زمانی نامرئی بود و حالا دیگر به چشم می‌آید. بگذارید نمونه‌هایی از عرصه حقوق را مرور کنیم و ببینیم اصلاً مسئله چیست. در واقع، حقوق از عرصه‌هایی است که از دهه‌ها پیش متوجه پدیده نویز بوده است، گرچه آن را نامگذاری و صورتبندی نکرده است.

نمونه کلاسیک این بحث فعالیت‌های ماروین فرانکل (۱۹۲۰ – ۲۰۰۲)، قاضی معروف امریکایی است. فرانکل با چند نمونه ملموس ادعایش را توضیح می‌داد. مثلاً دو فرد با جرم مشابه، یکی «۱۵ سال» حبس می‌گرفت و دیگری «۳۰ روز». یا در موردی دیگر، دو نفر با جرم مشابه اختلاس، یکی به «۱۱۷ روز» حبس متهم می‌شد و دیگری «۲۰ سال». به عبارت کلی، مشکل این است که قوانین بازه‌ای برای مجازات تعیین می‌کنند (فرضاً بین ۴ الی ۷ سال برای

فلان نوع جرم)، اما «این که چه عددی تعیین شود کمتر به خود پرونده و شخص متهم بستگی دارد و بیشتر به شخص قاضی – یعنی دیدگاه‌ها، تمایلات و سوگیری‌هایش – مربوط است.» (۲۰) (نقل‌قول‌ها از کتاب *نویز: نقصی در قضاوت انسان* است و اعداد داخل پرانتز ارجاع به صفحات کتاب.)

تصدیق وجود این پدیده دشوار نیست. اما گام بعدی مطالعه نظام‌مند و کاربست ابزارهای کمی برای تحلیل است. در ادامه فعالیت‌های فرانکل، جنبش‌های سیاسی و حقوقی قابل‌توجهی شکل گرفت و به چنین تحقیقاتی دامن زد. در واقع مرور بخشی از این نزاع‌ها فصل ۱ کتاب نویز را تشکیل می‌دهد و در حکم درآمدی به اهمیت بحث است. برای مثال، در مطالعه‌ای محققان احکام صادره طی سال‌های ۱۹۸۶ و ۱۹۸۷ را بررسی کردند و دریافتند که «تفاوت مورد انتظار در طول مدت مجازات بین قضاوت [...] معادل ۱۷٪ یا ۴٫۹ ماه بود.» سپس این مقدار را با احکام صادره طی ۱۹۸۸ تا ۱۹۹۳ مقایسه کردند تا ببینند آیا اقدامات صورت‌گرفته برای کاهش نویز مؤثر بوده است یا نه. از قضا، دریافتند که این مقدار ۳٫۹ ماه کاهش یافته است، یعنی ۱۱٪. (۲۵) و در گام بعد مهم این است که چه اقداماتی به چنین نتایجی منتهی شده است. مرور تجربه‌های موفق در جهت کاهش نویز، از جمله در عرصه قضایی است، کاری است که در بخش پنجم کتاب انجام شده است.

در تحقیق مفصل دیگری (که اولین بررسی در سطح ملی در امریکا محسوب می‌شود) محققان ۱۶ پرونده فرضی ساختند و از ۲۰۸ قاضی فدرال راجع به آن‌ها نظر خواستند. مقایسه احکام این قضات نکات جالبی را نشان می‌دهد. برای مثال، می‌بینیم بعضی از قاضی‌ها در موارد خاصی سخت‌گیرند و در مواردی سهل‌گیر. یا بعضی قضات به طور کلی نسبت به میانگین سخت‌گیری بیشتر یا کمتری دارند. بنابراین تنوع بین قاضی‌ها اساسی است. برای مثال، در پرونده‌ای که میانگین مدت حبس حدود پانزده سال بوده است، بعضی قضات حکم به ده سال داده‌اند و بعضی حکم به ۲۰ سال. (۷۶) باید دقت کنیم که این خطاها یکدیگر را خنثی نمی‌کنند، بلکه انباشته می‌شوند و این یکی از مضامین محوری کتاب درباره نویز است. به بیان دیگر، اینطور نیست که در نهایت اختلاف قاضی‌ها با یکدیگر (یا اختلاف یک قاضی با خودش در پرونده‌های مختلف) باعث حصول عدالت شود، بلکه چه‌بسا در موردی کسی کمتر از آنچه باید و در مورد دیگر کسی بیشتر از آنچه شایسته است مجازات شود!

شاید تصور کنیم موضوع به سخت‌گیری/سهل‌گیری ختم می‌شود. اما تحقیقات کلان دیگری نشان می‌دهند که عواملی به نظر نامربوط مثل زمان روز، آب‌وهوای آفتابی و ابری، یا تاریخ تولد متهم می‌توانند رابطه‌ای معنادار با احکام صادره قاضی داشته باشند. همچنین دامنه نویز بسیار گسترده‌تر است و به حکم کیفری قاضی محدود نمی‌شود. از جمله، فصلی از کتاب به تحقیقات مربوط در حوزه پزشکی قانونی اختصاص دارد. حتی تشخیص‌های کارشناسان اثرانگشت هم ممکن است نویزی باشد – نه فقط کارشناسان مختلف، بلکه یک کارشناس درباره یک

اثرانگشت واحد و تطبیق آن با اثرانگشت برگرفته از صحنه جرم. به عبارتی، مسئله‌ای اساسی‌تر از آن است که در ابتدا به نظر می‌رسد.

مثال ساعت را به خاطر بیاورید. اگر اختلافی بین ساعت مچی و ساعت دیواری باشد خود را در وضعیت نامناسبی می‌یابیم - یک جای کار می‌لنگد. با بررسی نویز در حوزه‌های مختلف (که آن را «نویزرسی» یعنی بازرسی نویز (noise audit) می‌نامند) نسبت به آن حوزه واکنش مشابهی حاصل می‌کنیم. به نظر می‌رسد مشکلی اساسی در کار است و باید برای آن چاره‌ای جست.

آیا ربات‌ها باید قاضی شوند؟

طبیعتاً یک کتاب نمی‌تواند چاره مشکلات و پاسخ همه سؤالات را فراهم کند. اما می‌تواند به بخشی از مشکل اشاره کند. کانمن و همکارانش در این کتاب پدیده نویز را می‌شکافند و انواع آن را توضیح می‌دهند و مقایسه می‌کنند. چنانکه گذشت، آن‌ها ابزارهایی معرفی می‌کنند که می‌توانیم مقدار نویز را اندازه بگیریم. بدین ترتیب، می‌توانیم بررسی کنیم که آیا اقدامی خاص باعث کاهش نویز شده است یا خیر. همچنین، می‌توانیم ببینیم تأثیر نویز مخرب‌تر است یا تأثیر سوگیری. از قضا، در بسیاری از موارد نویز خطای بیشتری را به دنبال دارد. در عین حال، سوگیری را همه می‌شناسیم و عموماً به وجود پدیده نویز بی‌توجه هستیم.

در اینجا هدف توجه دادن به مسئله نویز در عرصه قضایی است. اما بد نیست به بعضی دورنماها برای حل مسئله نیز اشاره شود. از مضامین اصلی کتاب تأکید بر اهمیت ابزارهای کمّی برای بهبود کیفیت قضاوت‌های کیفی است. نویسندگان البته تأکید می‌کنند که تلاش برای حذف قضاوت‌کننده‌های انسانی و کمی‌سازی همه چیز لزوماً هدف مطلوبی نیست و چه‌بسا امکان عملی هم نداشته باشد. با این حال، جا دارد از این ابزارها تا حد امکان استفاده کنیم.

یکی از ابزار مربوطه کاربست هوش مصنوعی در حوزه‌های مختلف است، از جمله در حوزه قضایی.

در حال حاضر تجربه‌های موفقی از کاربست یادگیری ماشین با استفاده از کلان‌داده‌ها برای تربیت سیستم‌هایی تشخیصی (برای مثال، در مورد توده‌های سرطانی) وجود دارد. این تحقیقات رو به گسترش هستند. ایده راهنما این است که الگوریتم‌ها از حیث سوگیری و نویز نسبت به انسان عملکرد بهتری دارند، حتی الگوریتم‌های ضعیف در مقایسه با انسان‌های قوی. این تلاش‌ها به حوزه قضایی نیز کشیده شده است. از نمونه‌های کاربرد هوش مصنوعی در عرصه قضایی سامانه‌هایی برای بررسی رد و قبول درخواست‌های آزادی مشروط با قرار وثیقه است. به طرز قابل‌توجهی این سامانه‌ها سوگیری و نویز کمتری دارند و بنابراین کیفیت قضاوت را بهبود می‌بخشند.

آیا عرصه قضایی ما هم نویزی است؟

با این اوصاف، اهمیت بررسی نویز در سیاق سیستم حقوقی ایران واضح است. این‌ها نمونه‌هایی از سؤالات متعددی است که در این باره جای طرح و بررسی دارد: آیا نویزرسی در سیستم حقوقی ایران سابقه‌ای دارد؟ آیا این ادبیات،

در صورت وجود، گردآوری و نظام‌مند شده است؟ آیا ما می‌دانیم نویز موجود در احکام صادره در حوزه‌های مختلف (مثلاً مالی، کیفری، سیاسی و غیره) چقدر است؟ درباره کاربست هوش مصنوعی در عرصه قضایی نیز مسائل فراوانی پیش رو هستند. آیا در نظام حقوقی ما مجالی برای چنین امری هست؟ آیا زمینه‌های لازم برای دسترسی به داده‌های مربوط جهت استفاده در یادگیری ماشین موجود است؟ کدام یک از تجربه‌های موفق نویزکاهی (= کاهش نویز) در حوزه‌های مختلف را می‌توان در سیستم حقوقی ایران به کار گرفت و آن را بهبود بخشید؟

مسئله نویز دامنه گسترده‌ای دارد، اما همیشه به یک اندازه مهم نیست. در این باره کانمن و همکارانش از این مثال استفاده می‌کنند: نمره‌دهی امتحانات مدارس نویزی است – اگر معلمان مختلفی برگه واحدی را تصحیح کنند احتمالاً نمرات مختلفی به آن می‌دهند (و کم و کیف این موضوع را باید سنجید). اما شاید فکر کنیم نویز در نمرات مدارس ابتدایی آنقدری مهم نیست. شاید نویز در بعضی حوزه‌ها چندان مهم نباشد یا به هزینه نویزکاهی نیرزد. در این باره هر چه فکر کنیم و هر ملاکی برای درجه اهمیت نویز در نظر بگیریم، نویز در سیستم قضایی در صدر مهم‌ترین‌هاست، مسئله سیستم قضایی مسئله عدالت است.

از این جهت اهالی عرصه حقوق از مخاطبان مهم کتاب *نویز: نقصی در قضاوت انسان* (۲۰۲۱) هستند، چه اینکه یکی از نویسندگان نیز از محققان شاخص همین حوزه است. به طور خاص، بعضی فصل‌ها (مانند ۱، ۶، و ۲۰) ادبیات مربوط به نویز در عرصه حقوقی را مرور می‌کنند و داده‌ها را در اختیار می‌گذارند. از سوی دیگر، این تحقیقات می‌توانند از حیث شناسایی مسئله و روش‌شناسی برای محققان ایرانی الهام‌بخش باشند. نهایتاً، بخش پنجم کتاب (با عنوان «بهبود قضاوت» از فصل ۱۸ تا ۲۵) به استراتژی‌های نویزکاهی می‌پردازد. مرور تجربه‌ها در کاهش نویز می‌تواند به فعالان و سیاست‌گذاران کمک کند تا متناسب با مقتضیات تدبیراندیشی کنند.

بگذارید دوباره به مثال ساعت برگردیم. اگر دور ما پر از ساعت باشد و همه زمان واحدی را نشان بدهند، باز غیرممکن نیست که در تشخیص زمان اشتباه کنیم. اما اگر چند ساعت داشته باشیم و هر کدام زمان متفاوتی را نشان دهند، بعید است راهی به دانستن زمان درست داشته باشیم. این‌گونه تنوع و بی‌ثباتی نگران‌کننده است. عدالت هم مثل زمان است، اما مهم‌تر.

امنیت سایبری؛ ظرفیت های حقوق بین الملل

حبیبه فرج زاده – دانشجوی دکترای حقوق بین الملل عمومی دانشگاه علامه طباطبائی

دستورالعمل تالین در مورد حقوق بین الملل قابل اعمال در عملیات سایبری، به عنوان نخستین تلاش جامع برای تحلیل کاربرد حقوق بین الملل در جنگ سایبری که توسط یک تیم بین المللی از کارشناسان حقوقی و به درخواست مرکز عالی دفاع سایبری سازمان همکاری ناتو تدوین شده است، در فهرست واژگان خود، فضای سایبری را این گونه تعریف میکند: «محیطی که متشکل از اجزای فیزیکی و غیرفیزیکی است برای ذخیره، اصلاح و تبادل داده ها با استفاده از شبکه های رایانه ای». درواقع، فضای سایبر، محیط یا قلمرویی ساخته دست بشر است که ارتباطات جهانی شامل فعالیتهای سیاسی، اقتصادی و اجتماعی را در بر می گیرد. به تبع جهانی شدن ارتباطات، بحران‌های امنیتی جدید هم در حوزه های سیاسی، اقتصادی، اجتماعی و فرهنگی ایجاد شد.

آنتونیو گوترش، دبیرکل سازمان ملل، در اولین سخنرانی خود در افتتاحیه نشست سران مجمع عمومی سازمان ملل متحد در سال ۲۰۱۷، تشدید تهدیدات امنیت سایبری را به‌عنوان یک تهدید اصلی برای امنیت بین المللی برجسته کرد. برای درک وخامت این تهدیدها، کافی است نگاهی به نمونه های اخیر حمله های سایبری داشته باشیم که علاوه بر تهدید جنگ سایبری، این حمله ها منجر به توقف کار بیمارستانها، قطع شبکه های برق، توقف فعالیت شهرهای بزرگ و حتی یکپارچگی فرآیندهای دموکراتیک شده است(اینجا).

از نمونه های جدید و مهم تهدیدهای سایبری، می توان به حمله جاسوسی Solarwinds در سال ۲۰۲۰ اشاره کرد، که سازمانها و شرکتهای آمریکایی و ایمیل مقامات وزارت امنیت آمریکا مورد حملات گسترده قرار گرفتند. دامنه این حمله ها که ادعا می شد توسط هکرهای روسی صورت گرفته، آنچنان گسترده بود که مؤسسه ملی بهداشت، پنتاگون، وزارت انرژی و همچنین مشتریان کمیسیون بورس اوراق بهادار نیز در فهرست آسیب دیدگان این حمله قرار گرفتند (اینجا). تهدیداتی نیز که در سایه همه گیری کووید-۱۹ پیش آمد، به ویژه در نشستهای غیر رسمی شورای امنیت (Arria Formula) مورد بحث قرار گرفت و بر ثبات سایبری، پیشگیری از درگیری و ظرفیت سازی تأکید شد (اینجا).

از آنجا که تهدیدهای امنیت سایبری هر روزه، رواج، پیچیدگی و شدت بیشتری می یابند، دولتها و جامعه فنی و صنعتی بر تقویت امنیت سایبری تمرکز کرده اند. درواقع، امنیت و ثبات فضای سایبری، سنگ بنای بحث در مورد فضای سایبری، حاکمیت اینترنت و آزادی اینترنت قرار گرفته است.

نگرانی جامعه بین المللی در این زمینه، موجب شد از سال‌های ۱۹۹۸ مجمع عمومی ملل متحد آغاز به تصویب قطعنامه های سالانه نماید و تأکید کند که فناوری اطلاعات بالقوه می تواند برای مقاصدی مغایر حفظ ثبات و امنیت

بین المللی به کار گرفته شود (نخستین، آخرین). مجمع عمومی در قطعنامه ۵۸/۳۲ از دبیر کل درخواست کرد تا گروهی متشکل از کارشناسان دولتی را برای پیشبرد رفتار مسئولانه دولتها در فضای سایبری در چارچوب امنیت بین المللی تشکیل دهد. این کار گروه که متشکل از ۲۵ عضو بود، از زمان آغاز به کار در سال ۲۰۰۴ تاکنون ۶ کارگروه تشکیل داده است و آخرین کارگروه، کار خود را در ماه مه ۲۰۲۱ با تصویب یک گزارش به اتفاق آراء به پایان رسانید. در دوره های پیشین، مهم ترین دستاورد گروه کارشناسان دولتی، پذیرش کاربرد حقوق بین الملل در فضای سایبری (۲۰۱۳) و معرفی هنجارهای غیرالزام آور داوطلبانه رفتار مسئولانه دولت در سال ۲۰۱۵ بوده است. مذاکرات دور ۲۰۱۶-۲۰۱۷ این کارگروه به علت اختلاف نظر کارشناسان در مورد مسائل مربوط به کاربرد حقوق بین الملل به ویژه حقوق بشردوستانه، اقدامات متقابل و دفاع مشروع سایبری با شکست مواجه شد و نتیجه ای در پی نداشت (اینجا).

به دنبال افزایش تنش‌ها میان قدرت‌های سایبری و شکست گروه کارشناسان دولتی در دور پیشین، مجمع عمومی در سال ۲۰۱۸ قطعنامه ای با حمایت روسیه مبنی بر ایجاد کارگروه باز بررسی تحولات در زمینه ارتباطات و اطلاعات در چارچوب امنیت بین المللی (OEWG) به تصویب رساند. تأسیس این کارگروه به انشعاب تلاشهای سازمان ملل در این زمینه منجر شد و کارگروه باز به موازات گروه کارشناسان دولتی موظف شد موضوعات اساسی را که گروه کارشناسان در مورد آنها به اجماع رسیده اند،به بحث گذارد. نخستین گزارش این کارگروه به اتفاق آراء کشورهای شرکت کننده در مارس ۲۰۲۱ تصویب شد، که به دلیل مشارکت مستقیم دولتها در تصویب آن می تواند از جایگاه مهم تری نسبت به سایر گزارشها و اقدامات در این زمینه برخوردار باشد (اینجا).

این گزارش، فراوانی، پیچیدگی و تنوع رویدادهای خرابکارانه فناوری اطلاعات و ارتباطات و همینطور افزایش احتمال استفاده از ابزارهای سایبری در مخاصمات آینده توسط تروریستها و گروه های تبهکار و آثار بالقوه ویرانگر آنها را از جمله افزایش تعداد حملات سایبری خصمانه که خدمات عمومی ضروری مثل امکانات پزشکی، خدمات مالی، انرژی، آب، حمل و نقل و بهداشت را به مخاطره می اندازند، شناسایی کرده است. موضوع دومی که در این گزارش بدان پرداخته شده، هنجارها و اصول است و بر ارتباط و محدودیتهای هنجارهای غیرالزام آور داوطلبانه برای صلح، امنیت و ثبات بین المللی تأکیده شده است. همچنین بر وظایف دولتها برای جلوگیری از گسترش ابزارهای مخرب و بر لزوم گزارش دهی آسیب پذیری ها تأکید می کند. در این گزارش مشارکت فعال و مستمر دولتها در گفتگوهای سازمانی منظم تحت نظارت سازمان ملل نیز مورد تأکید قرار گرفته است (اینجا).

در مورد کاربرد حقوق بین الملل، گزارش کارگروه باز بیانیه پیشین گروه کارشناسان دولتی را مبنی بر قابلیت اعمال حقوق بین الملل در فضای سایبری تأیید می کند. همچنین مکانیسمهای حل و فصل اختلافات ارائه شده توسط منشور ملل متحد را به رسمیت شناخته و دولتها را تشویق به حل و فصل اختلافات از راه های مسالمت آمیز می

نماید. گزارش مذکور اینگونه نتیجه می گیرد که راهکار مؤثر برای دست یابی به نقاط مشترک در مورد کاربرد عینی حقوق بین الملل در محیط فناوری اطلاعات و ارتباطات، تبادل منظم دیدگاهها و شناسایی موضوعات خاص حقوق بین الملل است که نیاز به گفت و گوهای عمیق زیر نظر سازمان ملل و دبیر کل دارد. با این حال، در این گزارش به دلیل مخالفت برخی از دولت ها از تعیین شاخه های خاص حقوق بین الملل که قابلیت اعمال در این حوزه را دارند (از جمله حقوق بین الملل بشردوستانه) صحبتی به میان نیامده است، که قابل انتقاد به نظر می رسد.

این گزارش همچنین به اقدامات اعتمادساز (CBMs) می پردازد و توصیه می کند که دولتها داوطلبانه اقدامات اعتمادساز را در چارچوب فضای سایبری شناسایی کرده و در اجرای آنها با یکدیگر همکاری نمایند (برای بررسی بیشتر در مورد این اقدامات نک به اینجا). همچنین، اصول ظرفیت سازی هدفمند و پایدار را شرح می دهد با این توضیح که این اصول باید مشخص، نتیجه گرا، مبتنی بر شواهد، از نظر سیاسی بی طرف، شفاف، پاسخگو و با احترام کامل به اصل حاکمیت دولتها باشد (اینجا).

اندکی پس از دور نهایی کارگروه باز، گروه کارشناسان دولتی نیز نسخه نهایی گزارش خود را منتشر کرد که با توجه به شکست دور قبلی، نشان از پیشرفت دیپلماتیک در مورد رفتار مسئولانه در سازمان ملل و دست یابی به اتفاق نظر در مورد موضوعات کلیدی دارد. این سند در هفت بخش تنظیم شده که از لحاظ عناوین تقریباً با گزارش کارگروه باز همپوشانی دارد. اما برخلاف گزارش کارگروه باز، اساسی ترین گام رو به جلو در گزارش گروه کارشناسان دولتی، اذعان به قابلیت اعمال حقوق بین الملل بشردوستانه و اصولی نظیر انسانیت، ضرورت، تناسب، تفکیک و غیره در عملیات سایبری در حین درگیری مسلحانه است. اما از آنجا که هنوز اختلاف نظر بر سر تفسیر اصول حقوق بشردوستانه وجود دارد بر ضرورت گفتگوی بیشتر در مورد کیفیت این اصول در حوزه سایبری تأکید شده است.

نکته حائز اهمیت دیگر در مورد مسئولیت دولت‌ها در قبال فعالیت های سایبری است. در هنجار ۱۳(ج) این گزارش مقرر شده است که دولتها نباید آگاهانه اجازه دهند که با استفاده از فناوری اطلاعات و ارتباطات از قلمروشان برای اعمال مغایر حقوق بین الملل استفاده شود(اینجا). این هنجار که به مفهوم مراقبت مقتضی(Due Diligence) معروف است، اخیراً در حوزه سایبری به عنوان راهکاری امیدوار کننده برای پاسخگویی دولتها در قبال عملیات سایبری که از قلمرو آنها سرچشمه می گیرند یا از قلمروی آنها عبور می کند، بسیار مورد توجه قرار گرفته است(برای مطالعه بیشتر نک به اینجا). در گزارش ۲۰۱۵ گروه کارشناسان، به این اصل به عنوان یک هنجار داوطلبانه و غیرالزام آور رفتار مسئولانه اشاره شده بود، اما گزارش ۲۰۲۱ با توصیف حدود و ثغور آن، این اصل را به عنوان یک انتظار عمومی و عقلانی تعریف می کند که یک دولت در چارچوب ظرفیت خود اقدامات معقول را برای پایان دادن به اقدامات سایبری مخرب در قلمروی خود با ابزار مناسب و مؤثر و مطابق با حقوق بین الملل و

حقوق داخلی اتخاذ خواهد کرد. از آنجا که انتظار نمی رود دولتها قادر به نظارت بر تمام فعالیتهای فناوری اطلاعات و ارتباطات در قلمروی خود باشند، بر ویژگی معقول بودن این وظیفه و ارائه کمک به دولتهایی که فاقد ظرفیت های لازم هستند تأکید شده است؛ که این امید را ایجاد می کند که دولتها در نهایت این وظیفه را به عنوان یک قاعده حقوق بین الملل به رسمیت بشناسند (اینجا).

علی رغم اینکه قابلیت اعمال حقوق بین الملل و به طور خاص منشور ملل متحد و اصول و قواعد دیگر حقوق بین الملل در مورد فضای سایبری امری پذیرفته شده است، این سؤال به قوت خود باقی است که قواعد و اصول مرتبط چگونه در این زمینه اعمال می شوند؟ به امید یافتن پاسخ این سؤال، انجمن آکسفورد برای اخلاق، حقوق و مخاصمه مسلحانه، کارشناسان مختلف را در ابتکار «تلاش آکسفورد در مورد حمایت های حقوق بین الملل در فضای سایبری» گرد هم آورد که برونداد این تلاشها، چند بیانیه است که به موضوعات خاص مطرح در حوزه امنیت سایبری پرداخته اند. به عبارت دیگر، هسته اصلی این ابتکار یک تلاش مشترک بین کارشناسان حقوقی بین المللی از سراسر جهان است که با هدف شناسایی و شفاف سازی قواعد حقوق بین الملل قابل اجرا در عملیات سایبری در زمینه های مختلف انجام می شود. تا به امروز، این فرآیند پنج بیانیه مختلف را ارائه کرده است:۱- بیانیه حمایت های حقوق بین الملل در برابر عملیات سایبری که بخش مراقبت های درمانی را هدف قرار می دهند؛ ۲- حفاظت از تحقیقات واکسن؛ ۳-حمایتهای حقوق بین الملل در برابر مداخلات انتخاباتی خارجی از طریق ابزارهای دیجیتال؛۴- مقررات عملیات و فعالیت های اطلاعاتی؛ و ۵- مقررات عملیات های باج افزار.

در تمامی این بیانیه ها بر اعمال حقوق بین الملل در این موضوعات تأکید شده است و بیان شده که حقوق بین الملل، دولت ها را از عملیات سایبری موضوع هر بیانیه منع می کند. به عنوان مثال در بیانیه مربوط به بخش مراقبت های درمانی، به صراحت بیان شده است که حقوق بشر دولتها را ملزم می کند که حق حیات و حق سلامت همه افراد در قلمروی تحت صلاحیت خود را از طریق اتخاذ تدابیری برای جلوگیری از مداخله اشخاص ثالث در این حقوق با ابزار سایبری تضمین کنند. همچنین، تعهد دولتها را در صورت آگاهی و اطلاع از یک عملیات سایبری در قلمرو یا زیرساخت های تحت صلاحیت یا کنترل آنها، و انجام تمام اقدامات ممکن برای جلوگیری از این اقدامات شناسایی می کند (برای بررسی بیشتر این بیانیه نک به اینجا).

در بیانیه مربوط به باج افزارها نیز، کشورها باید از انجام، هدایت، صدور مجوز یا کمک به عملیات باج افزارها که اصول حاکمیت یا عدم مداخله در امور داخلی یا خارجی یک دولت را نقض می کند یا به منزله تهدید یا توسل به زور در معنای منشور است خودداری کنند. به ویژه دولتها باید از عملیات باج افزارها با هدفی که منجر به نقض حقوق بشر افراد در حوزه صلاحیت آنهاست جلوگیری کنند و نباید به دولتها یا بازیگران غیردولتی اجازه انجام چنین عملیات هایی را در قلمرو و یا با استفاده از زیرساختهای خود بدهند.

با وجود تلاشها و اقدامات برشمرده شده توسط کشورهای عضو سازمان ملل و حقوقدانان بین المللی در نهایت، دست یابی به راه حل اصلی در تنظیم مقررات سایبری دشوار به نظر می رسد. از سویی، دولتهای غربی و ذی نفعان عرصه سایبری، بر این نظرند که حقوق بین الملل موجود برای تنظیم رفتار دولتها در فضای سایبر کافی است و تنها باید به چگونگی عملیاتی کردن این قواعد پرداخت. اما در مقابل، برخی کشورها مانند ایران، روسیه و کوبا معتقدند در حقوق موجود شکافها و ناکارآمدیهایی وجود دارد که نیازمند تنظیم قواعد جدید در این زمینه از طریق تدوین یک معاهده جدید و یا تحول حقوق بین الملل عرفی است. (اینجا) حتی در رویکرد معتقدان به ضرورت قواعد جدید نیز همسویی وجود ندارد. برخی دولتها بر معاهده ای متمرکز هستند که از دولت‌ها در برابر مردم محافظت می‌کند و برخی دیگر به دنبال معاهده ای هستند که از مردم در برابر دولت‌ها محافظت کند (اینجا).

از آنجا که مانند هر حوزه دیگر، حقوق بین الملل در زمینه فضای سایبری همواره در حال تحول است و روز به روز بر پیچیدگی آن افزوده می شود، انتظار می رود تا زمان رسیدن به راه حلی جامع و مورد توافق، تلاشهای مشترک دولتها، سازمانهای بین المللی، جامعه مدنی و دانشگاهیان در این زمینه ادامه یابد. در این راستا، به ویژه دولت‌ها باید برای تقویت اجرای هنجارها و اصول موجود، با تلاش‌های داوطلبانه و رفتار مسئولانه خود برای دستیابی به امنیت سایبری تلاش کنند.

دارایی‌های مجازی؛ یک بحران بین‌المللی

امیر فامیل زوار جلالی - کاندیدای دکتری حقوق بین‌الملل دانشگاه تهران

بلاکچین، دارایی‌های مجازی، ارزهای مجازی، رمزارزها، Stable coins، متاورس همگی واژگانی جدید هستند که تکنولوژی نوآورانه برای انتقال دارایی‌ها در سراسر جهان را توصیف می‌کنند. تحول و نوآوری در این فناوری به گونه‌ای باشتاب به سمت جلو در حرکت است که حتی در زمان نگارش این سطور نیز شاهد تحول و اختراع در گونه‌های جدیدی از آنها می‌باشیم. این حجم بالا از تولید، تحول و اختراع و اکتشاف در دارایی‌هایی که غیر محسوس و غیر ملموس هستند، چنان جهان را فرا گرفته است که مطابق گزارش‌ها، ارزش کل بازارهای آن در زمان نگارش این متن، حدود نهصد میلیارد دلار می‌باشد. حجم مبادلات بازار این نوع دارایی‌ها به همراه ویژگی‌های منحصر به فرد آنها باعث شده است تا کشورها و مراجع مالی بین المللی از جمله بانک جهانی و کارگروه اقدام مالی (FATF) زنگ خطر تهدید این دارایی برای صلح و امنیت را به صدا در آورند. در این یادداشت تلاش شده است تا به طور مختصر ریسک‌های بالقوه دارایی‌های مجازی و نقش حقوق بین‌الملل در حل بحران‌های ناشی از آن توصیف گردد.

ریسک‌های بالقوه دارایی‌های مجازی

«دارایی مجازی» به هر نمایش دیجیتالی از ارزش گفته می‌شود که قابلیت معامله به صورت دیجیتالی را دارد و می‌تواند به صورت الف- وسیله پرداخت، ب- یک واحد حساب و یا ج-ذخیره ارزش عمل نماید اما وضعیت پول رایج با همان ارز فیات (پولی که فی نفسه ارزش مالی ندارد بلکه ارزش آن وابسته به دولت است یعنی دولت به آن ارزش داده تا در معاملات مورد استفاده قرار گیرد، مثال ریال ایران که نوعی ارز فیات است، برای اطلاعات بیشتر نک به اینجا) را ندارد. این نوع دارایی توسط هیچ مرجع قانونی صادر و تضمین نمی‌شود و کلیه وظایف فوق الذکر بر اساس توافق میان جامعه کاربران این نوع دارایی مجازی صورت می‌گیرد.

از میان دارایی‌های مجازی آن دسته که با ارائه امکانات و قابلیت‌های متنوع، بیش از پیش توجه سرمایه گذاران، قانون گذاران و مجریان قانون را به خود جلب کرده است، رمزارزها هستند. رمزارزها، نوعی دارایی مجازی قابل تبدیلِ غیرمتمرکزِ ریاضی محور هستند که بوسیله رمزنگاری محافظت می‌شوند. این نوع دارایی‌ها هر کدام از فناوری متفاوتی بهره می‌برند و تفاوت‌های آنها نیز به دلیل تفاوت در بستر بلاکچین آنها است.

دارایی‌های مجازی و تکنولوژی‌های مرتبط با آن به دلیل هزینه کم، سرعت بالا و رفع موانع و واسطه‌ها، وعده‌های بزرگی برای متحد کردن جهان می‌دهد. اما ویژگی‌هایی همچون عدم نظارت، غیر متمرکز بودن، گمنامی و تلقی آن به عنوان یک روش جایگزین پرداختِ سریع، آسان و ارزان می‌تواند آنها را برای بسیاری از مجرمانِ جرایم مالی

جذاب نماید (اینجا، ص ۲) . به عبارت دیگر در کنار همه مزایا، این سیستم در برابر جرایم مالی همچون پولشویی، تامین مالی تروریسم، فرار مالیاتی و فساد آسیب پذیر است، زیرا امکان ناشناس ماندن هویت کاربر بیش از سیستم‌های پرداخت الکترونیک سنتی بوده و همچنین به دلیل آنکه تحت نظارت هیچ مرجعی نیست، پولشویان می توانند ریشه غیر قانونی پول بدست آمده را مخفی کرده و کنترل و نظارت بر جریان وجوه را سخت‌تر نمایند. برای مثال، آدرس بیت کوین، بدون داشتن نام و سایر مشخصات و بدون داشتن سرور مرکزی به عنوان یک شماره حساب عمل می‌کند، و تراکنش‌ها بدون نیاز به شناسایی یا تایید هویت کاربران یا ایجاد سوابق تراکنش‌ها صورت می‌گیرد.

رمز ارزها، برای انتقال وجوه یا انجام پرداخت‌ها، عموماً متکی به زیرساخت‌های پیچیده‌ای هستند که ممکن است شامل چندین نهاد در چندین کشور باشد و این چندپارگی ارائه خدمات، به این معناست که مسوولیت مطابقت و نظارت مبارزه با پولشویی و تامین مالی تروریسم (CFT/AML) نامشخص و مبهم بوده و از طرفی سوابق معاملات و تراکنش‌ها ممکن است در حوزه‌های قضایی مختلفی نگهداری شود که دسترسی مجریان و نهادهای تنظیم‌کننده به این اطلاعات را دشوارتر می‌کند. این مساله به دلیل ماهیت در حال تحول تکنولوژی دارایی‌های مجازی، در حال تشدید است.

مجرمان مالی با استفاده از ابزارهایی در حوزه دارایی‌های مجازی می‌توانند، درصد موفقیت در فعالیت‌های خود را افزایش دهند. از جمله مهمترین این ابزارها «ناشناس‌سازها» هستند. ناشناس‌سازها ابزارهایی هستند که برای پنهان کردن منبع و لایه‌گذاری تراکنش‌های ارزهای مجازی و تسهیل گمنامی آنها طراحی شده‌اند. «مخلوط‌کن‌ها» و «پشتک زن‌ها» از جمله ناشناس‌سازهایی هستند که ارزهای مجازیِ کاربران متعدد را جمع آوری و بازتوزیع کرده و از این طریق مسیر تراکنش‌ها را پنهان می‌کنند(اینجا، ص ۷ .) یک مخلوط‌کن، تراکنش‌ها را از طریق مجموعه‌ای پیچیده و نیمه تصادفی از تراکنش‌های ساختگی ارسال می‌کند که باعث می‌شود پیوند آدرس یک ارز مجازی خاص با یک تراکنش خاص دشوار گردد (اینجا، ص ۶)

حقوق بین‌الملل و مقابله با ریسک‌های نوظهور

در ارتباط با حوزه فناوری‌های مالی، دو قضیه مهم باعث گردید تا نگرانی جامعه جهانی نسبت به آسیب پذیر بودن حوزه فناوری‌های نوین بیش از پیش بر انگیخته شود و پس از آن اقدامات جدی تری در رابطه با این حوزه‌ها صورت گرفت. اولین مورد مربوط به بزرگترین پولشویی آنلاین تحت عنوان رزرو آزادی در سال ۲۰۱۳ بود. (اینجا، ص. ۳۲) رزرو آزادی یک سیستم انتقال پول مجازی متمرکز در کاستاریکا بود که در سال ۲۰۰۶ به جهت کاهش نظارت مراجع اعمال قانون نسبت به تراکنش‌های مالی ایجاد گردید. این سازمان با بیش از ۶ میلیون کاربر در سراسر جهان، بیش از ۵۵ میلیون دلار تراکنش مالی را که قریب به اتفاق آن غیرقانونی بود، پوشش می داد. در

نهایت نهاد قضایی ایالات متحده آمریکا، این سازمان را به اتهام انتقال بیش از ۶ میلیارد دلار از عواید غیرقانونی محکوم نمود و ۷ نفر از مدیران و کارمندان آن نیز دستگیر شدند.

مورد بعدی، یک وبسایت تحت عنوان راه ابریشم بود که به عنوان یک بازار سیاه جهانی واسطه مبادله کالا و خدمات غیرقانونی میان چندین هزار فروشنده و خریدار عمل می‌کرد. راه ابریشم با پذیرش انحصاری بیت کوین به عنوان ارز، و با اعمال شبکه تور مخفی و سایر ناشناس سازها، هویت خریداران و فروشندگان را پنهان می نمود. در نهایت در سپتامبر ۲۰۱۳ وزارت دادگستری امریکا، این وبسایت و بیش از ۱۷۳ هزار بیت کوین آن را مصادره کرد (اینجا، ص ۱۱).

دو پرونده فوق‌الذکر که از جمله قدیمی ترین، مهمترین و بزرگترین پولشویی مرتبط با فناوری‌های نوین از جمله دارایی مجازی می باشد، آسیب پذیر بودن در برابر خطرات این حوزه را که برای مدت طولانی بدون نظارت و وضع مقررات در حال توسعه بود، بارز و نمایان کرد. در واقع قانون گذاران بعد از مواجهه با موارد گوناگونی از جمله رزرو آزادی و راه ابریشم متوجه خلاء بزرگ قانونی در این حوزه شدند (اینجا، ص ۱)

کشورهای جهان در راستای مواجهه، تعامل و مقابله با دارایی‌های مجازی واکنش‌های متفاوتی را در پیش گرفتند. در حالی که برخی کشورها تصمیم به ممنوعیت تجارت از طریق دارایی مجازی گرفتند (مانند چین) برخی از کشورها نیز اقدام به صدور مجوز برای برخی صرافی‌های مجازی نمودند (از جمله نیویورک آمریکا). اتخاذ رویکردهای گوناگون، خود یک چالش در زمینه مقابله و قانونگذاری به صورت متحدالشکل را ایجاد می‌کند. مقابله با تهدیدات نوآوری‌ها از جمله دارایی‌های مجازی نیازمند این است که سیاست گذاری و قانونگذاری در سطح جهانی نیز در راستای هماهنگی میان قانونگذاری های کشورها مختلف انجام شده باشد. زیرا در دهکده جهانی حاضر، اقدامات جزیره‌ای دیگر کارساز نخواهد بود و نیاز به هماهنگی‌های جهانی و اقدامات متحد الشکل، مبرم است.

در این میان حقوق بین‌الملل نقش ویژه‌ای در راستای رفع نگرانی‌ها و حفظ صلح و امنیت بین‌المللی در برابر تهدیدات نوظهور ایفا خواهد کرد. مجمع عمومی سازمان ملل، از دیرباز با فراهم نمودن بستر وضع معاهدات بین‌المللی گام‌های مثبتی در راستای مبارزه با جرایم مالی بین المللی به طور کلی برداشته است. در این میان می‌توان به کنوانسیون سرکوب تامین مالی تروریسم ۱۹۹۹، کنوانسیون مبارزه با جرایم سازمان یافته فراملی (پالرمو) ۲۰۰۰ و کنوانسیون مبارزه با فساد (مریدا) ۲۰۰۳ اشاره کرد. این کنوانسیون‌ها که اکثریت دولت‌ها نیز به عضویت آنها درآمده اند حاوی استانداردها و الزاماتی برای کشورها در حوزه مبارزه با جرایم مالی از جمله پولشویی، تامین مالی تروریسم و فساد می‌باشد. شورای امنیت سازمان ملل متحد نیز که مسئول اصلی و اولیه حفظ صلح و امنیت بین‌المللی است با صدور قطعنامه‌های متعددی که غالب آنها ذیل فصل هفتم صادر گردیده، نقش ویژه و مخصوصاً عملی در

حوزه مبارزه با جرایم مالی داشته است. اگرچه کنوانسیون‌ها و قطعنامه‌های یاد شده محور اصلی خود را مبارزه با جرایم مالی از جمله تروریسم قرار داده اند اما اشاره مستقیمی به خطرات ناشی از دارایی های مجازی ندارند. از این میان تنها قطعنامه ۲۴۶۲ شورای امنیت است که دارایی‌های مجازی و خطرات جرایم مالی مرتبط با آن را گوشزد می‌نماید. در این قطعنامه که ذیل فصل هفتم صادر گردیده، دولت‌ها موظف شده اند اقدامات لازم را به منظور تضمین توانایی حقوقی و قانونی در جهت تعقیب قضایی و جرم انگاری تامین مالی سازمان‌های تروریستی به انجام برسانند. همچنین قطعنامه از دولت‌ها می‌خواهد تا در راستای استانداردهای FATF، واحدهای خودکار و مستقل ملی جهت مقابله با تامین مالی تروریسم ایجاد نمایند. در نتیجه مشاهده می‌گردد که با وجودآنکه دارایی های مجازی و خطرات بالقوه ناشی از آن به طور مستقیم مورد توجه این اسناد قرار نگرفته و راهکارهای مقابله با آن به طور کلی و ورای بستر تروریسم ارائه نشده است، لذا با تفسیر آن اسناد و انطباق آن با مسائل نوظهور و از طرفی اعمال استانداردهای FATF (که در ادامه به آن اشاره می گردد) به واسطه الزام ناشی از قطعنامه‌های شورای امنیت سازمان ملل می تواند یکی از راهکارهای موقت برای مقابله با چنین ریسک‌هایی باشد.

گروه اگمونت، کمیته بازل، گروه ناظران بیمه، گروه بانک‌های ولفسبرگ، صندوق بین‌المللی پول نیز از دیگر نهاد هایی بودند که با تهیه گزارش‌ها و استانداردسازی‌ها نقش مهمی در کنترل جرایم مالی داشتند. اما از این میان، پویاترین و به روزترین نهاد در راستای مبارزه با جرایم مالی که نگاه ویژه به گام‌های سریع تکنولوژی نیز داشته است، FATF می‌باشد. FATF یا همان گروه ویژه اقدام مالی، به طور کلی با ارائه توصیه‌های ۴۰ گانه برای نظام-های مالی کشورها، انتشار راهنمای اجرای این توصیه‌ها، و با ارزیابی دوره‌ای کشور در جهت انطباق قوانین و مقررات آنها با استانداردهای این نهاد و تشکیل جلسات عمومی در طول هر سال نقش قابل توجهی در توسعه قواعد مرتبط با مبارزه با جرایم مالی داشته است. اما در حوزه دارایی‌های مجازی، FATF نخستین بار در سال ۲۰۰۶ با انتشار گزارشی در خصوص شیوه های نوین پرداخت پا به عرصه فناوری‌های نوین گذاشت. پس از این گزارش، در سال ۲۰۱۴ با ارائه گزارشی به صورت مستقیم به ارزهای مجازی و ریسک‌های بالقوه آن پرداخت و یک سال بعد راهنمای عملی برای کشورها در خصوص چگونگی مقابله با جرایم مرتبط با دارایی مجازی را منتشر نمود که این راهنما در سال ۲۰۲۱ بروز رسانی شد. FATF همچنین با انتشار گزارشی تحت عنوان «ریسک‌های در حال ظهور تامین مالی تروریسم»، نگرانی کشورها و جامعه بین المللی نسبت به استفاده تروریست‌ها از ارزهای مجازی را مورد تاکید قرار داد. با توجه به توسعه محصولات و خدمات در این حوزه، FATF در سال ۲۰۱۸ دو تعریف جدید در لغت نامه خود ایجاد کرد که عبارتند از: VA یعنی دارایی‌های مجازی و VASP یعنی ارایه دهندگان خدمات مرتبط با دارایی مجازی. هدف از این تغییرات اعمال استانداردهای FATF در حوزه دارایی‌های مجازی برای کاهش خطرات پولشویی و تامین مالی تروریسم و محافظت از تمامیت سیستم مالی جهانی بود. در ادامه در سال

FATF ۲۰۱۹ جدیدترین گزارش خود در دارایی مجازی و ارائه دهندگان خدمات مرتبط با این نوع دارایی را منتشر ساخت که ضمن معرفی ابعاد دارایی‌های مجازی و انواع محصولات مرتبط با آنها، حاوی اطلاعاتی در خصوص چگونگی اعمال استانداردهای FATF در مورد دارایی‌های مجازی می‌باشد. هرچند توصیه‌های این کارگروه اساساً جنبه رهنمود داشته و ممکن است حتی در شرایطی در زمره حقوق نرم قرار گیرند، اما با توجه به پذیرش جامعه جهانی و مقبولیت گسترده آنها نزد کشورها و سازمان‌های بین‌المللی، از اعتبار و جایگاه بالایی برخوردار است به طوری که علیه کشورهای غیر همکار یا منفعل اقدامات تنبیهی صورت می گیرد که برای نمونه می‌توان به قرار گرفتن دو کشور ایران و کره شمالی در لیست کشورهای غیر همکار این سازمان و اقدامات متقابل کشورها علیه این دولت ها اشاره نمود. علاوه بر FATF، حقوق بین‌الملل از طریق سایر ابزارهای نهادی خود از جمله سازمان‌های یادشده، با حمایت از ایجاد یک سیستم یکپارچه نظام مالی بین‌المللی و تشویق کشورها به اتخاذ رویه‌های یکسان در سطح جهانی و معاضدت‌های قضایی می تواند نقش مهمی در کنترل بحران‌های ناشی از نوآوری های سیستم های مالی از جمله دارایی‌های مجازی داشته باشد. البته با عنایت به اینکه سازمان‌های یادشده هریک کارکرد و حوزه اختیارت خاص خود را دارند و عملاً نمی‌توانند به صورت سنتی قانونگذاری نمایند، همکاری و اقدامات اینگونه سازمان‌ها اگرچه موثر است اما تنها می‌تواند نقشی موقتی برای مقابله با چنین ریسک‌هایی را داشته باشد. در گام بعدی، همکاری مجمع عمومی سازمان ملل برای نگارش پیش نویس یک معاهده جامع برای قانونمند کردن حوزه دارایی‌های مجازی و مقابله با ریسک‌های ناشی از آن می تواند بهترین گزینه باشد.

برآیند:

بی تردید، تکنولوژی همواره سریع‌تر از قانون گذاران حرکت می‌نماید. در نتیجه وقتی قانون به دنبال قاعده‌مند سازی یک تکنولوژی قدیمی است، ابتدا باید ابعاد مختلف و ویژگی‌های خاص و متمایز آن تکنولوژی نیز درک و شناسایی شود تا بتوان طیف گسترده‌ای از موضوعات ناشی از آن تکنولوژی مدنظر قرار گیرد. ظهور دارایی‌های مجازی در انواع مختلف و نمایش خلأ قانونی برای کنترل آنها از جمله مهمترین چالش حوزه دارایی مجازی می‌باشد که در برخی موارد با توجه به امکانات گسترده‌ای که در اختیار مجرمان مالی از جمله پولشویان و تروریست‌ها قرار می‌دهد، می‌تواند این دسته از مجرمان را در رسیدن به اهداف خود و به خطر انداختن صلح و امنیت بین‌المللی تقویت نماید. ویژگی‌های ارزهای مجازی همچون بیت‌کوین، یک گزینه‌ی جذاب برای شبکه‌های تروریستی هستند تا با ادغام آن در ساختار مالی خود، امکان رهگیری خود را بیش از پیش دشوار سازند. در اینجا حقوق بین‌الملل می‌تواند حافظ صلح و امنیت بین‌المللی بوده و از بحران‌های محتمل جلوگیری نماید. همانطور که گفته شد، برای مقابله با چنین ریسک‌هایی، می بایست از جزیره‌ای عمل کردن خودداری نمود و با اتخاذ رویه‌های

یکسان در سطح جهانی و معاضدت‌های قضایی به مقابله با بحران‌های ناشی از نوآوری های سیستم های مالی از جمله دارایی‌های مجازی اقدام نمود. همکاری و اقدامات سازمان‌هایی نظیر FATF می‌تواند نقش مهمی در مقابله با چنین ریسک‌هایی داشته باشد اما گام اصلی در این زمینه، تصویب یک معاهده جامع برای قانونمند کردن حوزه دارایی‌های مجازی و مقابله با ریسک‌های ناشی از آن باید باشد.

رمزارزها و مخاصمات مسلحانه

خدایار سعیدوزیری – دانشجوی دکتری حقوق بین‌الملل دانشگاه علامه طباطبائی

رمزارزها امروز بخش مهمی از سیستم مالی جهانی محسوب می‌شود و این بدان معناست که فارغ از مثبت یا منفی بودن آن، باید رمزارزها را به عنوان بخشی از اقتصاد بین‌المللی پذیرفت. یکی از شرایطی که رمزارزها اهمیتی بیش ازهمیشه پیدا می‌کنند، شرایط مخاصمه مسلحانه بین‌المللی است که امنیت اقتصادی معمول را به مخاطره انداخته و دسترسی افراد و دولت‌ها به منابع مالی و مسیرهای انتقال پول را محدود می‌نماید.

در شرایط اخیر که نیروهای روسیه به اوکراین حمله کردند و جنگی ترکیبی یعنی هم جنگ در معنای سنتی آن و جنگی سایبری میان دو طرف درگرفته است، اهمیت این جنبه از رمزارزها بیش از تئوری مطرح شده است و از آن به عنوان یکی ابزارهای کاربردی در شرایط بحران یاد می‌شود.

بسیاری از اوکراینی‌ها به ارزهای دیجیتال به عنوان جایگزینی برای سیستم مالی نیمه تعطیل اوکراین در شرایط جنگ روی آورده‌اند که دسترسی مردم به حساب‌های بانکی خود و حساب‌های ارزی را محدود کرده‌اند .به طورکلی در سناریویی که دولت‌ها دچار آشفتگی قرار می‌گیرند، تکیه بر بانک‌های سنتی دشوار است و کنترل‌گری دولت جنبه حداکثری پیدا می‌کند و در چنین شرایطی یک سیستم مالی نسبتا ناشناس که هیچ دولتی بر آن کنترل ندارد، طبیعتا برای اغلب فعالان مالی و کسانی که خواستار دسترسی همیشگی و سریع و بدون محدودیت به دارایی‌های خود هستند، جذاب است.

الکس گلادشتاین، کارشناس ارشد مسائل استراتژیک در بنیاد حقوق بشر، بیان داشته است: «این واقعیت که نمی‌توان رمزارزها را بلوکه کرد یا تحت کنترل قرار داد و در عین حال بدون شناسایی از آنها استفاده کرد، ویژگی بسیار بسیار مهمی است.» و به همین سبب می‌توان رمزارزها و در راس آنها بیت‌کوین را به سبب آسانی نقل و انتقال و کارمزد کم و در دسترس بودن، یک ابزار بشردوستانه‌ی مهم تلقی کرد، چنانکه صلیب سرخ نیز در فکر استفاده از این فناوری در مناطق بحران‌زده افتاده است و جمعیت های صلیب سرخ نروژ، دانمارک و کنیا تلاش‌هایی را در این زمینه آغاز کرده‌اند.

در جنگ حاضر میلیون‌ها دلار ارز دیجیتال برای حمایت از ارتش اوکراین و گروه‌های سایبری این کشور سرازیر شده است. الکس بورنیاکوف، معاون وزیر تحول دیجیتال اوکراین، در ۹ مارس گفت که تقریبا ۱۰۰ میلیون دلار رمزارز برای حمایت از اوکراینی‌ها طی چند هفته از جنگ ارسال شده است. دولت اوکراین نیز حداقل ۱۵ میلیون دلار از رمزارزهای دریافتی خود را تا ۱۱ مارس خرج کرده و چندین شرکت فعال در حوزه‌ی رمزارزها از جمله Kuna، FTX و همچنین شرکتی به نام Everstake را برای جمع‌آوری کمک‌ها به کار گرفته است.

دولت اوکراین علاوه بر اقدامات فوق‌الذکر یک وبسایت راه‌اندازی کرده است تا تلاش‌های خود را برای جمع‌آوری سرمایه مبتنی بر رمزارزها متمرکز کند. در این وبسایت توضیح داده شده است که اوکراین برای حمایت از خود در نبرد با روسیه، بیت کوین و دوج کوین و رمزارزهایی دیگر را می‌پذیرد و البته راه کمک از طریق ارز فیات نیز باز است. البته هنوز نمی‌توان درباره میزان مفید بودن این ابزار مالی در چنین شرایطی به طور دقیق اظهار نظر کرد، چرا که استفاده از آن نیازمند اشنایی به فناوری است و به علاوه تولید محتوا برای دریافت کمک مالی جهت تجهیز نظامی، خلاف قوانین برخی پلتفرم‌های تولید محتوا مانند Patreon است و کاربران را از تولید چنین محتواهایی منع می‌کنند. این درحالی است که به گفته‌ی مایکل چوبانیان، مدیر صرافی اوکراینی Kuna در ابتدا دو صندوق ایجاد شد که یکی با هدف بشردوستانه بود و دیگری حمایت از ارتش اوکراین، اما با تشدید جنگ در سراسر اوکراین، این بودجه به طورکامل بر حمایت از ارتش متمرکز شد و بیشتر این کمک‌ها به شکل بیت‌کوین، اتریوم و استیبل کوین تتر بوده است.

اما نکته‌ی کلیدی درباره‌ی رمزارزها در چنین مناقشه‌ای آن است که همه‌ی آن ویژگی‌هایی گروه یا مردم تحت محاصره را به سمت رمزارزها جلب می‌کند و از رمزارزها ابزاری بشردوستانه می‌سازد، در مورد طرف مهاجم نیز صدق می‌کند. در واقع در بسیاری از اوقات رمزارزها موضوع استفاده‌ی بازیگران منفی نیز قرار می‌گیرد و در این مورد نیز روسیه می‌تواند با استفاده از آن برای دور زدن تحریم‌ها علیه خود استفاده کند و بسیاری از الیگارش‌های روس نیز دارایی‌های خود را برای جلوگیری از توقیف در بانک‌های غربی به رمزارز بدل کردند و از سوی دیگر خطر حملات هکری به دارایی‌ها را بالا می‌برد. از سوی دیگر برخی این ادعا را که بیت‌کوین همچون طلای دیجیتال است، با این استدلال که قیمت آن در بحران‌ها نوسانات شدیدی دارد، زیر سوال می‌برند. فرض کنید برای خروج دارایی از یک شرایط جنگی دارایی خود را که برابر ۱۰ هزار دلار است به بیت کوین تبدیل کرده و از اوکراین خارج می‌شوید و چند روز بعد وقتی قصد تبدیل آن به ارز فیات را دارید، دچار کاهش ارزش شده و ۷۰۰۰ دلار دریافت کنید! قطعا موضوع جذابی نیست، اما وقتی تنها گزینه است چطور؟

اما استفاده از رمزارز در میانه‌ی یک بحران مانند جنگ لزوما آسان نیست. برای چنین ابزاری، حداقل نیاز به یک دستگاه و اتصال به اینترنت دارید. به علاوه در زمان‌هایی که تعداد زیادی از جمعیت یک کشور قصد تبدیل دارایی‌هایشان به رمزارز را دارند، ممکن است صرافی‌های دیجیتال نیز با چالش‌هایی مواجه شود، از جمله در قضیه اوکراین، در ماه فوریه ۲۰۲۲ گزارش شد که صرافی‌ها با کمبود تتر مواجه شدند. این بدان معناست که در حال حاضر، رمزارزها برای کسانی که از قبل در این حوزه فعال بوده‌اند، مفید است اما برای کسانی که امروز تصمیم به ورود گرفته‌اند، دشوار خواهد بود. از سوی دیگر این فرضیه که بیت‌کوین را طلای دیجیتال می‌نامد نیز در این جنگ تا حدی زیرسوال رفت چرا که پس از حمله‌ی روسیه به اوکراین، درحالی که قیمت طلا رو به افزایش

گذاشت، بیت کوین همراه با بازارهای بورس افت شدیدی را تجربه کرد و با بازگشت شاخص S&P بود که بیت‌کوین نیز افزایشی را تجربه کرد. هرچند بسیاری این کاهش قیمت رمزارزها و مشخصا بیت‌کوین در شرایط بحران را نتیجه‌ی عدم آشنایی کافی مردم با ظرفیت رمزارزها به ویژه بیت کوین می‌دانند.

از سوی دیگر چنانکه اشاره شد، موضوع استفاده از رمزارزها از سوی روسیه نیز مطرح است و به علاوه روسیه در حال توسعه‌ی روبل دیجیتال است که می‌تواند به تجارت این کشور فارغ از سیستم سوئیفت کمک کند و به همین سبب نیز شاهد آن هستیم که مداخله‌ی صرافی‌های دیجیتال که محل تبدیل اصلی رمزارزها و ارز فیات (منظور از ارز فیات ارزهای جاری در کشورها مانند دلار، یورو، روبل و غیره هستند) به یکدیگر است، به سمت جلوگیری از ارایه خدمت به شهروندان روس رفته‌اند، امری که وجود آن می‌تواند غیرمتمرکز بودن رمزارزها را که مهمترین ویژگی آن است، تهدید نماید و صرافی‌ها را به رگولاتوری در این حوزه بدل کند و از سوی دیگر فعالان این حوزه را به سمت زیرزمینی شدن تجارت رمزارزها و خرید و فروش آن در فضای دارک وب هدایت کند. هرچند شاید این بحث مطرح شود که در حال حاضر نیز مبادلات زیرزمینی وجود دارد، اما باید گفت امروز این مبادلات زیرزمینی صرفا توسط گروه‌های غیرقانونی و در سطحی کم و قابل رصد انجام می‌گیرد، اما محدودیت‌ها می‌تواند سیلی از افراد را به سمت فعالیت‌های زیرزمینی هدایت کند که امکان کنترل و نظارت را به طورکلی سلب نماید. از سوی دیگر رقابت سیاسی بین دولت‌ها و همچنین نهادهای مالی بین‌المللی در روابط بین‌المللی با هدف حفظ سلطه و انحصار سیاستگذاری‌های پولی و مالی، سبب برقراری مقررات محدودکننده در حوزه رمزارزها نیز می‌گردد، چنانکه کریستین لاگارد، رئیس بانک مرکزی اروپا، رمزارزها را تهدید دانسته و صرافی‌هایی مانند کوین‌بیس از این موضوع ناراحتند؛ اما نکته آن است که استفاده از رمزارزها برای مقابله با تهدیدات مالی مانند تحریم، مستلزم آن است که اولا دسترسی کافی به رمزارزها وجود داشته باشد و ثانیا کالاهای مورد نیاز که کشوری قصد پرداخت هزینه‌ی آن با رمزارز را دارد، قابل انتقال به آن باشند.

من حیث المجموع باید گفت رمزارزها را باید ابزار مالی‌ای مهم دانست که در شرایط بحران می‌تواند به وسیله‌ای برای نقل و انتقال ارزش و حمل آسان دارایی در مهاجرت و برای پناهجویان استفاده شود و در عین حال برای جمع‌آوری کمک نیز به کار رود، چنانکه در استفاده‌هایی نامشروع، گروه‌های تروریستی نیز سالهاست از این طریق به جذب منابع مالی می‌پردازند، اما هنوز نمی‌توان آن را ابزاری قابل اتکا برای دولت‌ها تلقی کرد، چرا که نوسانات شدیدی که این بازار در نتیجه‌ی تاثیرپذیری از تحولات گوناگون دارد، می‌تواند سبب ورود ضربات سنگین اقتصادی به دولت‌هایی شود که بخش زیادی از سرمایه‌های خود را به شکل رمزارز نگهداری می‌کنند.

عملیات سایبری و حمله مسلحانه در معنای ماده ۵۱ منشور سازمان ملل متحد

دکتر کتایون حسین نژاد - پژوهشگر حقوق بین الملل

برای سالیان سال، مجاز یا متضادی بود برای حقیقی و حقیقت، یا استعاره و کنایه ای بود به حقیقتی دیگر. امروز اما، ما آدمیان می خواهیم فراجهانی بسازیم از فضای مجازی که ملاط اصلی آن صفر است و یک (اگر چه کامپیتورهای کوانتومی، فراتر از صفر و یک خواهند بود) برای آسان تر کردن و گسترش دادن روابط و مبادلات انسانی. اما همانطور که در افسانه های ایرانی می خوانیم که «برای ضدیت با هر یک از آفریدگان روشن نیک... حریفی از اهریمنان هست» (مهرداد بهار، ص ۹۳)، در این فضای ساختگی، فضای سایبری معادلی شد برای رویه تاریک و تهدیدآمیز مجازی (برای بررسی امنیتی بودن مفهوم فضای سایبری نک به اینجا). این تهدیدها که شاید بتوان گفت برای اولین بار در سال ۱۸۳۴ با هک سیستم تلگراف فرانسه و ربودن اطلاعات مالی بانکی آغاز شد (اینجا)، به چنان قدرت انهدام و ویرانگری رسیده است که امروزه دولت ها از امکان تلقی برخی عملیات سایبری به عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور ملل متحد و توسل به دفاع مشروع فردی یا حتی جمعی در مواجه با آن، سخن می گویند. (برای بررسی مواضع برخی دولت ها نک به اینجا)

در مواجهه با این تهدیدها، رویکرد اصلی حقوق بین الملل آن است که هر قاعده در دنیای واقعی قابل سرایت و اعمال است بر فضای مجازی؛ (برای نمونه نک به بند ۶۹ آخرین گزارش گروه کارشناسان دولتی در مورد رفتار مسولانه در فضای مجازی، بند ۷ آخرین گزارش گروه کاری نامحدود و قطعنامه شورای حقوق بشر در مورد اینترنت) ـ گویی که فضای مجازی همان آرایه ادبی است به کنایه از دنیای واقعی ما. از این منظر، حمله مسلحانه قلمداد کردن عملیات سایبری ممکن بوده و در نتیجه علاوه بر موضع بسیاری از دولت ها، بسیاری از صاحبنظران حقوقی از جمله کارشناسان مورد مشورت در دستورالعمل تالین ۲ نیز بر این نظر هستند که «دولت قربانی عملیات سایبری که به *سطح* حمله مسلحانه رسیده باشد، می تواند به حق دفاع مشروع ذاتی خود متوسل شود». (تاکید اضافه شده است، قاعده ۷۱). این کارشناسان، عملیات سایبری را هنگامی حمله مسلحانه قلمداد می کنند که «گستره و تاثیر» آن مشابه آستانه ای باشد که برای تلقی توسل به زور به حمله مسلحانه در دنیای واقعی اعمال می شود و در نتیجه بر این نظر هستند که چنانچه عملیات سایبری منجر به «صدمات جدی یا مرگ تعدادی یا ایراد خسارت یا نابودی اموال» شود، یعنی آثار فیزیکی همانند یک حمله مسلحانه به بار آورد، می تواند به عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور تلقی گردد. (بند ۸، قاعده ۷۱)

این کارشناسان دو مبنای عمده برای چنین نتیجه گیری عنوان می کنند: نخست، نظر دیوان بین المللی دادگستری در مورد قابل اعمال بودن ممنوعیت توسل به زور و همچنین ماده ۵۱ منشور بر هر نوع «سلاح» (بند ۳۹ نظریه مشورتی

دیوان در مورد سلاح های هسته ای)؛ و دوم وجود اجماع بر آنکه حمله های غیرکینتیک (یا غیرجنبشی) به مانند شیمیایی یا بیولوژیک در صورت ایراد آثاری مشابه با حمله های کینتیک می تواند در گستره مفهوم حمله مسلحانه مندرج در منشور قرار گیرد. (بند ۴ قاعده ۷۱).

با وجود مشابهت عملکرد عملیات سایبری با یک حمله شیمیایی از لحاظ غیرکینتیک بودن، در این واقعیت تردیدی نیست که در مورد اول ما با یک برنامه کامپیوتری مواجه هستیم که جز در فضای رایانه ای وجود ندارد و جز به کمک رایانه اثر نخواهد کرد و در مورد دوم با یک عنصر شیمیایی موجود در عالم واقع. به دیگر سخن، تاثیر یک عملیات سایبری به خودی خود و مستقیم نیست بلکه به دلیل تاثیری است که بر عملکرد کامپیوتر و شبکه ها و افزارهای متصل به آن گذاشته و در نتیجه عملکرد نادرست سیستم های کامپیوتری، ممکن است خسارتی به اموال یا لطمه ای به افراد وارد شود. دقیقا به دلیل همین تفکیک است که اخیرا، اشمیت و بیلر در مقاله ای در مورد ابزار یا روش جنگی بودن عملیات سایبری، می نویسند از آنجا که در هیچ سلاح دیگری این مرحله میانی وجود ندارد که از خود هدف خواسته شود که زیان مورد نظر را پدید آورد، عملیات سایبری که متشکل است از مجموعه کدهایی که دستور اقدامات زیان آور را به یک سیستم رایانه ای می دهد، نمی تواند در مفهوم «سلاح» یا «ابزار» جنگی قرار گیرد بلکه توصیف درست از آن، در ذیل «روش جنگی» است. با توجه به اینکه اشمیت خود بانی و موتور اصلی دستورالعمل های تالین است، بعید نیست در دستورالعمل تالین ۳ که شروع آن کلید خورده است، تغییراتی در تقسیم بندی عملیات سایبری به سلاح و روش جنگی صورت گیرد (قاعده ۱۰۳ دستورالعمل تالین ۲ در حال حاضر ابزارهای سایبری را سلاح سایبری و سیستم های متصل به آن و روش های سایبری را تاکتیک، تکنیک و آیین های سایبری هدایت مخاصمات می خواند). با آنکه مقاله اشاره شده در بالا در مقام بیان تبیین یک قاعده از هدایت مخاصمات در حقوق بشردوستانه است (و خود تاکید می کند که چنین تفکیکی تاثیری در اجرای قواعد حقوق بشردوستانه ندارد)، چنین روشنگری نمی تواند بدون تاثیر در حوزه های دیگر حقوق و به خصوص حقوق توسل به زور باشد. برای نمونه، اگر عملیات سایبری در هر شکل و ابعاد به مانند توسل به حیله، صرفا یک روش جنگی است، به طور طبیعی نمی تواند در مفهوم «سلاح» قرار گیرد و در نتیجه، از نظر موضوعی از دامنه شمول نظریه مشورتی دیوان در مورد سلاح های هسته ای در مورد قابل اعمال بودن ماده ۲ و ۵۱ منشور بر هر «سلاحی» خارج می شود.

در زمان تدوین دستورالعمل تالین ۲، این بحث مطرح شد که آیا استفاده از «سلاح» برای تحقق حمله مسلحانه ضروری است یا خیر. پیش از ادامه این بحث، اشاره به این مطلب ضروری است که در دستورالعمل تالین ۲، کارشناسان بر تفاوت میان «تجاوز» و «حمله مسلحانه» اذعان داشته و هر «تجاوزی» را لزوما مساوی با «حمله مسلحانه» نمی دانند (بند ۲ قاعده ۷۱)، که خود تاییدی است بر تفکیک میان «تجاوز مسلحانه» یا همان حمله مسلحانه با سایر

اشکال «تجاوز». با این حال، در بحث ضرورت استفاده از سلاح، نظر اکثر کارشناسان بر این بود که لازم نیست حمله مسلحانه با استفاده از سلاح باشد ـ امری که با تعریف تجاوز مسلحانه می تواند در مغایرت باشد – اما این نظر را نیز رد نکردند که واژه «مسلحانه» بودن صرفا بر استفاده از سلاح اطلاق می شود و در نتیجه جز عملیات سایبری که با استفاده از سلاح سایبری در مفهوم قاعده ۱۰۳ انجام گیرد، سایر عملیات های سایبری صرفنظر از گستره و آثار نمی تواند به عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور در نظر گرفته شود.» (بند ۵ قاعده ۷۱). با این توصیف، اگر طبقه بندی اشمیت در مورد روش جنگی بودن عملیات سایبری پذیرفته شود، این دو دیدگاه قطعا غیرقابل جمع خواهند شد یعنی یا بایستی قائل به تعمیم حمله مسلحانه به عملیات سایبری به صرف آثار بود و یا با توجه به اینکه عملیات سایبری صرفا مجموعه از دستورهای کامپیوتری است و در نتیجه هیچ اقدام مسلحانه ای در عالم واقع صورت نگرفته است، در صورت وجود سایر شرایط آن را صرفا مشمول مداخله، توسل به زور و یا حتی تجاوز دانست و نه حمله مسلحانه.

چنانچه قایل به نظر اول شویم، یعنی تنها آثار را به عنوان معیار حمله مسلحانه بودن عملیات سایبری در نظر بگیریم، آیا این امر منجر نمی شود که بتوان سایر روش هایی را نیز که منجر به مرگ و آسیب گسترده می شوند، برای نمونه تحریم های اقتصادی یکجانبه، در مفهوم حمله مسلحانه ماده ۵۱ قرار داد؟ مقایسه عملیات سایبری با تحریم ها از این جهت جالب توجه می نماید که آثار تحریم، به خصوص خسارات و لطمات معمولاً فوری نبوده بلکه در طولانی مدت رخ دهد. این تاثیر مشابه همان اتفاقی بود که در مورد ویروس استاکس نت روی داد؛ با وجود اینکه کدهای دستوری مختلف مدت های مدیدی بود که در سیستم های رایانه ای وارد شده بودند، (گفته می شود حدود چهار سال) اما امکان تلقی آن به عنوان «حمله مسلحانه» تنها زمانی در نظر گرفته شد که خسارات گسترده تر وارد شده بود. (ذکر این مطالب ضروری است که تاکنون نه استاکس نت و نه هیچ عملیات سایبری دیگر به عنوان حمله مسلحانه مورد شناسایی دولت ها قرار نگرفته و حتی در مورد استاکس نت، کارشناسان تالین در مورد حمله مسلحانه قلمداد کردن آن تردید داشتند، با وجود آنکه همه موافق بودند که این عملیات توسل به زور بوده است. (بند ۱۰، قاعده ۷۲)) حال، چرا بایستی تفاوتی بین کدهای دستوری زیان بار و وضع قوانین تحریمی زیان بار قائل شد زمانی که ـ همانطور که همه تجربه کرده ایم ـ هر دو موجب مرگ و آسیب می شوند؟ در این خصوص، توجه به این مساله مهم است که با وجود اینکه از موارد تجاوز مندرج در اساسنامه دیوان بین المللی کیفری، توسل به روش «محاصره بنادر و سواحل توسط نیروهای مسلح دولت دیگر» (بند ج ماده ۸ مکرر اساسنامه دیوان بین المللی کیفری) است که در معنای سنتی، جنگی است اقتصادی برای ممانعت از ورود کالا و افراد به قلمروی کشور دشمن (تفسیر جنایت تجاوز، ص. ۴۴۳) اما آنچه این روش را تبدیل به تجاوز می کند، حضور نیروهای مسلح دولت

محاصره کننده است که می توانند عملا مانع ورود و خروج کالا و خدمات شوند (همان، ص. ۴۴۴) و نه صرف تحریم.

رویه دیوان بین المللی دادگستری در تبیین تفاوت میان توسل به زور و حمله مسلحانه به صرف اشاره به گستره و آثار نبایستی توجه را از این مطلب دور کند که در هر سه پرونده فعالیت های نظامی و شبه نظامی در نیکاراگوئه، سکوهای نفتی و فعالیت های مسلحانه در کنگو، تردید یا حتی بحثی در مسلحانه بودن اقدامات انجام شده در مفهوم عادی و کلاسیک و واقعی آن نبود؛ بلکه محل تردید، تعیین آستانه یا مصادیق حمله مسلحانه در توجیه اقدامات نظامی متقابل در قالب دفاع مشروع بود. از این دیدگاه، صرف در نظر گرفتن معیار گستره و آثار بدون بستر آن، که همان عملیات نظامی مشروحه در هر پرونده ای بود، به مثابه حکایت ناودان خواندن فیل در شعر مولاناست.

با وجود آنکه عملیات سایبری می تواند آثار بسیار مخربی داشته باشد، اما، همگام با صاحبنظرانی که ماده ۵۱ منشور سازمان ملل متحد را استثنایی نه بر منع توسل به زور بلکه بر اقدامات جمعی سازمان ملل متحد ذیل فصل هفتم منشور و تحت لوای شورای امنیت و محدود به موارد تجاوز مسلحانه ای می دانند که اقتضای اقدام فوری پیش از اتخاذ تدابیر ضروری توسط شورای امنیت در تامین صلح و امنیت را دارد (نک برای نمونه به اینجا)، به دلیل ماهیت مجازی، چنین عملیاتی نمی تواند در مفهوم حمله مسلحانه قرار گیرد. این ایده، منصرف از این استدلال است که حتی اگر عملیات سایبری را حمله مسلحانه بدانیم، متناسب ترین دفاع در برابر آن به احتمال قوی مقابله مجازی با آن و نه استفاده از بمب و موشک است.

نقش هوش مصنوعی در مخاصمات مسلحانه و پیامدهای حقوقی آن

پیمان حکیم زاده خوئی – استادیار و عضو هیات علمی گروه حقوق بین الملل، دانشکده حقوق،الهیات و علوم سیاسی، دانشگاه آزاد اسلامی واحد تبریز، ایران

ریحانه دروگری – دانشجوی دوره دکتری حقوق بین الملل عمومی، گروه حقوق، دانشگاه پیام نور، تهران، ایران، مدرس دانشگاه

در طول قرن‌ها، حقوق مخاصمات مسلحانه در پوشش‌های مختلف خود، همواره تمرکز خود را بر قاعده مند ساختن درگیری های مسلحانه برای محافظت از قربانیان جنگ معطوف کرده است. از آغازین سالهای قرن نوزدهم و در پاسخ به توسعه فناوری نظامی و آداب و رسوم اجتماعی رایج آن زمان، قواعد مخاصمات مسلحانه شروع به رسمی شدن و بازتاب چارچوبی نموده که امروزه با آن آشنا هستیم (اینجا، ص ۲۷۱) . یکی از ویژگی‌های قابل توجه این چارچوب، انعطاف پذیری تکاملی آن است. این انعطاف‌پذیری اجازه داده است تا این حقوق به گونه‌ای تکامل یابد که با پیشرفت‌های صورت گرفته در فن‌آوری و تاکتیک‌های به کار رفته در درگیری‌های مسلحانه سازگاری یافته و مجموعه اقداماتی را برای ممنوعیت استفاده از سلاح‌ها و تاکتیک‌های خاص در بر گیرد. نکته قابل توجه در این خصوص این مساله است که حقوق مخاصمات مسلحانه انعطاف‌پذیری خود را از طریق اصول تعیین‌کننده زیربنایی خود نشان داده است. اهم این اصول که عبارتند از: ضرورت نظامی، رعایت معیارهای انسانی، تمایز و تناسب، کیفیتی دیرپا دارند و معیاری را ارائه می‌دهند که براساس آن می‌توان تحولات فناوری و تاکتیک‌ها را از نظر قانونی بودن آنها ارزیابی کرد.(اینجا، ص۲۷۲)

هوش مصنوعی

هوش به شیوه های مختلفی تعریف شده است. به طور کلی، می توان هوش را یک توانایی ذهنی بسیار کلی دانست که از جمله توانایی استدلال، برنامه ریزی، حل مسائل، تفکر انتزاعی، درک ایده های پیچیده، یادگیری سریع و یادگیری از طریق تجربه را شامل می شود. چنین توانایی از صرف یادگیری یک کتاب یا یک مهارت تحصیلی محدود یا هوشمندی در آزمون فراتر رفته و توانایی گسترده‌تر و عمیق‌تر را برای درک محیط پیرامون منعکس می‌کند؛ همانند درک کردن و معنا کردن چیزها یا پیدا کردن آنچه باید انجام داد. (اینجا، ص۱۳)

هوش مصنوعی به قدرت استدلال و برنامه ریزی در رایانه یا سایر ماشین ها گفته می شود. هوش مصنوعی در مبنا یکی از رشته های علوم رایانه است که به مطالعه و توسعه دستگاه های هوشمند از طریق ارائه الگوریتم مناسب می پردازد تا ماشین ها را قادر به ادراک، استدلال و یادگیری سازد. (اینجا، ص۲) این رشته با تحقیق و توسعه نظریه‌ها، روش‌ها، فناوری‌ها و سیستم‌های کاربردی برای شبیه‌سازی و گسترش هوش انسانی بر آن است که ماشین‌ها را قادر به انجام کارهای پیچیده‌ای کند که معمولاً برای انجام آنها به هوش انسانی نیاز است. البته ناگفته نماند که چنین

ماشین هایی ممکن است هوش انسانی را تقلید، تقویت یا جایگزین کنند (اینجا، ص۱۴۷). هوش مصنوعی را می توان با قابلیت های خاصی دسته بندی کرد، به عنوان مثال هوش مصنوعی ضعیف یا باریک، به هوش مصنوعی اطلاق می شود که می تواند رفتارهای هوشمند خاص انسان ها مانند تشخیص، یادگیری، استدلال و قضاوت را شبیه سازی کند به عبارتی دیگر، هدف هوش مصنوعی ضعیف حل وظایف خاصی مانند تشخیص گفتار، تشخیص تصویر و ترجمه برخی از مطالب خاص است. (اینجا) هوش مصنوعی قوی، به هوش مصنوعی اطلاق می شود که هوشیاری مستقل و توانایی نوآوری مشابه مغز انسان دارد. (اینجا) هوش مصنوعی قوی می تواند فکر کند، برنامه ریزی کند و مشکلات را حل کند و همچنین درگیر تفکر انتزاعی شده، ایده های پیچیده را درک کرده، سریع یاد بگیرد و از تجربیات بیاموزد که در نتیجه آن را به هوش انسانی نزدیکتر می کند. نوع دیگری از هوش مصنوعی ابر هوش مصنوعی است که به هوش مصنوعی آینده اشاره دارد که از نظر توانایی محاسباتی و تفکر از مغز انسان بسیار پیشی خواهد گرفت و بسیار باهوش تر از بهترین مغزهای انسان در هر زمینه ای از جمله خلاقیت علمی، خرد عمومی و ... مهارت های اجتماعی خواهد بود. (اینجا)

کاربرد هوش مصنوعی در مخاصمات مسلحانه

بدون تردید با پیشرفتهای تکنولوژیک در زمینه های مختلف از جمله صنایع نظامی، ماهیت جنگ، بعداز پایان جنگ جهانی دوم به طور قابل توجهی تغییر کرده است. امروزه، به دلیل استفاده از فناوری های جدید، خطوط مقدم نبرد به طور کامل و واضح مشخص نیست. حمله می تواند از طریق پهپادهایی که با چشم قابل رویت نیستند یا با موشک های بالستیک که از فاصله ۱۶ هزار مایلی پرتاب می شوند، انجام شود. (اینجا) با این سرعت تحولات، چه بسا در جنگهای بزرگ بعدی، هوش مصنوعی حاکم اصلی میدان نبرد خواهد بود و ربات‌هایی که سریع‌تر، قوی‌تر و دقیق‌تر هستند، طرف پیروز را تعیین خواهند کرد. هوش مصنوعی با کاربرد روزافزون خود در زمینه نظامی، در حال تبدیل شدن به یک عامل توانمندساز مهم برای اصلاحات نظامی است که الگوهای جدیدی از جنگ را به وجود می آورد و مکانیسم ذاتی پیروزی در جنگ را تغییر می دهد. (اینجا، ص ۱۴) با این حال، چنین جنگ‌هایی می‌توانند بی‌تردید و بی‌سابقه ویرانگر باشند و شاید این امر منجر به یک فروپاشی فناوری جهانی و نابودی کامل جهان گردد.

به طور کلی، کاربردهای نظامی هوش مصنوعی دو بعد عمده و کلی را پوشش می دهد: نخست، استفاده از هوش مصنوعی در جهت بهبود عملکرد سیستم های تسلیحات سنتی و موجود و دوم، استفاده از هوش مصنوعی برای تصمیم‌گیری. با این وصف هوش مصنوعی به عنوان یک فناوری پیشرفته با کاربرد دوگانه، کاربرد عمیق و گسترده ای در سیستم ها و تجهیزات تسلیحاتی داشته و مطمئناً در پروژهای نظامی آینده نقش مهمی ایفا خواهند نمود (اینجا).

به طور قطع و یقین در مقایسه با فناوری سنتی، سیستم‌های تسلیحاتی مجهز به هوش مصنوعی از مزایای مختلفی مانند داشتن قابلیت مبارزه همه جانبه و قابلیت بقای قویتر در میدان جنگ و همچنین هزینه کمتر برخوردار خواهند بود. (اینجا) یکی از بزرگترین مزیت‌های سیستم‌ها و تجهیزات تسلیحاتی مجهز به هوش مصنوعی، سرعت پاسخگویی است که ممکن است از مغز انسان بسیار فراتر رود. (اینجا) به عنوان مثال در یک نبرد هوایی شبیه‌سازی شده در سال ۲۰۱۶، یک هواپیمای جنگنده F-15 با نرم‌افزار هوشمند آلفا که توسط دانشگاه سینسیناتی توسعه داده شده بود، یک هواپیمای جنگنده F-22 با خلبان انسانی را شکست داد زیرا این نرم‌افزار هوشمند می‌توانست ۲۵۰ برابر سریع‌تر از مغز انسان واکنش نشان دهد.(اینجا) جای شک و تردید نیست که با توسعه فناوری‌های هوش مصنوعی، سیستم‌های تسلیحاتی هوشمندی که می‌توانند به طور مستقل اهداف خود را شناسایی، قفل و ضربه بزنند در حال افزایش هستند و می‌توانند دستورهای ساده تصمیم‌گیری را به جای انسان انجام دهند.

فناوری‌های هوش مصنوعی می‌توانند برای آگاهی از موقعیت و پردازش اطلاعات هوشمند در میدان جنگ و در سکوهای نظامی بدون سرنشین مانند وسایل نقلیه هوایی خاص و وسایل نقلیه کنترل از راه دور استفاده شوند؛ برای نمونه سیستم‌های فرماندهی و کنترل هوشمند توسعه‌یافته توسط ارتش‌ها می‌توانند به تصمیم‌گیری کمک کرده و ظرفیت ارزیابی هوشمند را بهبود بخشند. (اینجا) کاربرد نظامی هوش مصنوعی همچنین تأثیر زیادی بر سازماندهی نظامی خواهد داشت و این امر پتانسیل تغییر اساسی در آینده مخاصمات را (اینجا، ص۱۱) به عنوان مثال، با استفاده ترکیبی از مهمات با ضربه دقیق، تجهیزات بدون سرنشین و سیستم های اطلاعات شبکه، و تئوری های جنگی هوشمند جدید (اینجا) دارد.

بالطبع این مزیت ها باعث شده که نیروهای نظامی هرچه بیشتر به استفاده از این فناوری متمایل شوند حتی اگر در میان خود آنها مخالفان متعددی در این خصوص وجود داشته باشد. برای مثال، مخالفان خاطر نشان می کنند که اغلب سلاح های خودآیین نمی تواند بین رزمندگان و غیر رزمندگان تمایز قائل شود. نوئل شارکی، یکی از مبارزان پیشرو علیه سلاح های خودآیین (اینجا)، بیان کرده است که آیا یک ربات می تواند بین کودکی که یک بستنی در دست دارد و بزرگسال جوانی که تفنگ در دست دارد، تمایز قائل شود (اینجا). البته استفاده از سیستم‌های دارای هوش مصنوعی در حوزه‌های مورد مناقشه و مسئول قلمداد کردن آنها برای تصمیم‌گیری‌های حیاتی، به احتمال زیاد زمینه را برای نتایج فاجعه بار فراهم خواهد کرد ولی از آنجایی که سلاح‌های مجهز به هوش مصنوعی توسط انسان طراحی، تولید، برنامه‌ریزی و به کار گرفته می‌شوند، عواقب و مسئولیت‌های قانونی ناشی از اعمال غیرقانونی و قانونی آن‌ها متوجه انسان است .(اینجا) اصول راهنمای تایید شده توسط گروه کارشناسان در زمینه فناوری های نوظهور در حوزه سیستم سلاح های خودآیین مرگبار نیز اعلام می کند که مسئولیت انسان برای تصمیم گیری در مورد استفاده از سیستم های تسلیحاتی باید حفظ شود زیرا مسئولیت پذیری نمی تواند به ماشین ها منتقل شود. این

مساله، باید در کل چرخه حیات سیستم تسلیحاتی در نظر گرفته شود. بدین معنا که علیرغم این که هوش مصنوعی از کاربرد گسترده ای در زمینه نظامی برخوردار است ولی در هر حال سربازان و فرماندهان انسانی بایستی تصمیم گیرندگان نهایی برای حرکت به داخل و خارج از زنجیره عملیات و انجام اقدامات مداخله جویانه باقی بمانند. امری که خود به بزرگترین چالش برای توسعه فناوری مشترک انسان و ماشین تبدیل شده است. (برای مطالعه بیشتر نک برای نمونه به اینجا)

چالش های کاربرد هوش مصنوعی

به مانند سایر فناوری های نوظهور، هوش مصنوعی یک شمشیر دو لبه است و با کاربرد نظامی گسترده‌تر هوش مصنوعی، مسائل جدیدی ظهور کرده که باعث گسترش نگرانی‌هادر سراسر جهان شده است. به عنوان مثال، با توجه به اینکه در حوزه مسایل نظامی، پتانسیل هوش مصنوعی در همه زمینه ها (به عنوان مثال زمین، دریا، هوا، فضا و اطلاعات) و همه سطوح جنگ (یعنی سیاسی، استراتژیک، عملیاتی و تاکتیکی) وجود دارد، یکی از چالش های استفاده از هوش مصنوعی در سطوح سیاسی و استراتژیک، آن است که این هوش ممکن است برای بی ثبات کردن حریف با تولید و انتشار مقادیر زیادی اطلاعات جعلی استفاده شود. (اینجا) از آنجا که بسیاری از تجهیزات مجهز به هوش مصنوعی، علاوه بر کارایی بالا به شفافیت بالا، ایمنی بالا و اعتماد یا درک کاربر نیاز دارند، به طور کلی می توان مهم ترین چالشهای موجود در کاربرد هوش مصنوعی را در عرصه نظامی موارد زیر دانست: شفافیت، آسیب پذیری و یادگیری. الزاماتی که در سیستم‌های حیاتی ایمنی سیستم‌های نظارتی، عوامل مستقل، پزشکی و سایر کاربردهای مشابه نیز، معمول هستند.

شفافیت در کاربرد هوش مصنوعی

با پیشرفت های اخیر در توسعه هوش مصنوعی، علاقه تحقیقاتی به شفافیت برای حمایت از کاربران نهایی در چنین برنامه هایی نیز افزایش یافته است.(اینجا) شفافیت، چالشی است که به دنبال حصول اطمینان از سازگاری عملکرد هوش مصنوعی با الزامات نظامی است؛ اگرچه افزایش سرعت و دقت را می توان به عنوان مزایای بالقوه هوش مصنوعی در عرصه نظامی نام برد، اما همچنان نگرانی های در خصوص قابلیت هایی چون سرعت تصمیم گیری وجود دارد که ممکن است سبب این امر شود که سیستم ها نتوانند با پیچیدگی های اجتناب ناپذیر جنگ، سازگار شوند. در نتیجه، امکان دارد چنین سیستم هایی نتوانند به طور دقیق بین رزمندگان و غیر رزمندگان یا تهدیدها تمایز قائل شوند و در نهایت ممکن است دقت کمتری نسبت به اپراتورهای انسانی داشته باشند (اینجا) و اگر سیستم‌ها قبل از آزمایش کافی فعال شوند یا اگر دشمنان موفق به جعل یا هک کردن آنها شوند، این مشکلات می‌توانند تشدید شوند.(اینجا)

آسیب پذیری در کاربرد هوش مصنوعی

این معیار نشان می‌دهند که چگونه می‌توان به طور بالقوه از جعل، استخراج داده‌ها و آلوده کردن داده‌های آموزشی برای سوءاستفاده از آسیب‌پذیری ها و ایجاد تأثیرات منفی امنیتی نامطلوب استفاده کرد. آسیب‌پذیری‌ها و خطرات هوش مصنوعی می تواند انواع مختلفی داشته باشد از جمله آسیب پذیری های انسانی. برای نمونه بدون آموزش و بازآموزی نیروی کار جهت مطابقت با سرعت تغییرات فناوری و انواع مختلف تهدیدات، دشمنان هنگام تلاش برای سوء استفاده از آسیب‌پذیری‌های هوش مصنوعی با موانع کمتری مواجه خواهند شد. بنابراین آموزش، خطاهای ناخواسته را کاهش می دهد. (اینجا) برای مثال با توجه به اینکه قابلیت‌های هوش مصنوعی دارای کاربردهای غیرنظامی و نظامی می باشد، سیستم‌هایی که به نیروهای نظامی در برنامه‌ریزی ماموریت و تخصیص منابع کمک می‌کنند، ممکن است توسط مهاجمان برای شناسایی اهداف آسیب‌پذیر مورد سوءاستفاده قرار گیرد.

یادگیری ماشینی

توسعه برنامه های کاربردی مبتنی بر یادگیری ماشینی در زمینه نظامی چالش برانگیز است؛ زیرا روش های جمع آوری داده‌ها در سازمان های نظامی، امکانات آموزشی، پلتفرم ها، شبکه های حسگر و سلاح ها در ابتدا برای اهداف یادگیری ماشینی طراحی نشده بودند. در نتیجه، در این حوزه، یافتن مجموعه داده‌های واقعی، با کیفیت و به اندازه کافی بزرگ که بتوان از آنها برای یادگیری و کسب بینش استفاده کرد، اغلب دشوار است.

اصول اخلاقی حاکم بر کاربرد هوش مصنوعی

هوش مصنوعی به سرعت در حال تبدیل شدن به بخشی از جنبه های زندگی در قرن بیست و یکم، از جمله جنگ است و با پیشرفته‌تر شدن و فراگیرتر شدن آن، یک سؤال اصلی به طور فزاینده‌ای حیاتی جلوه می کند و آن این است که آیا هوش مصنوعی می‌تواند اخلاقی باشد؟ بدیهی است که سیستم های مجهز به هوش مصنوعی نمی توانند ارزش های انسانی را درک کنند؛ امری که خود موجد یکی از بزرگترین چالش های هوش مصنوعی از لحاظ اخلاقی است. از این رویکرد، در نظر گرفتن چگونگی ساخت ماشینی برای خودآموزی ارزش های انسانی و اجتناب از خطر و همچنین کدهای اخلاقی هوش مصنوعی باید موضوع اصلی گفتگو مابین دولت ها و سازمان‌های مختلف بین المللی باشد. در زمینه نظامی، این چالش اخلاقی بسیار عمیق تر شده و به ویژه مسائلی از قبیل نقض کرامت انسانی در مواجهه با سیستم های تسلیحاتی خودآیین را مطرح می کند. با توجه به اینکه عاملیت انسانی در هدایت مخاصمات صراحتاً در اسناد حقوق بشردوستانه درج نشده است (برای نمونه نک به اینجا)، تحقیق در مورد اخلاق و امنیت هوش مصنوعی امری ضروری است.

در این راستا، باید تلاش‌های مربوطه در حوزه فناوری و جامعه را یکپارچه نمود تا اطمینان حاصل شود که توسعه هوش مصنوعی همچنان برای انسان و طبیعت مفید است. بدیهی است فناوری و پیشرفت آن، الزامات جدیدی را

برای کدهای اخلاقی ایجاد خواهد کرد؛ با این حال، با توجه به تفاوت های موجود از لحاظ فرهنگی و مکانی هماهنگی استانداردهای اخلاقی بین کشورها و سازمان‌های مختلف بین المللی بسیار مهم است.(اینجا) در آوریل ۲۰۱۹، کمیسیون اروپا یک کد اخلاقی برای هوش مصنوعی منتشر و از راه‌اندازی مرحله آزمایشی این کد خبر داد و از شرکت‌ها و مؤسسات تحقیقاتی برای آزمایش آن دعوت کرد. در ۲۵ مه ۲۰۱۹، آکادمی هوش مصنوعی پکن اصول هوش مصنوعی پکن را منتشر کرد. به موجب این اسناد، در مرحله تحقیق و توسعه، هوش مصنوعی بایستی تابع منافع کلی نوع بشر بوده و طراحی آن اخلاقی باشد. به منظور جلوگیری از سوء استفاده، در بکارگیری هوش مصنوعی بایستی اطمینان حاصل شود که افراد ذینفع از تأثیر بر حقوق و منافع خود آگاهی و رضایت کامل داشته و از نظر حکمرانی، بایستی در مورد جایگزینی کار انسانی با هوش مصنوعی با احتیاط عمل نمود. (اینجا) توصیه نامه یونسکو در خصوص هوش مصنوعی نیز «با در نظر داشتن این واقعیت که فناوری‌های مبتنی بر هوش مصنوعی می‌توانند خدمات مفید و قابل توجهی به زندگی بشر ارائه نمایند، به این حقیقت اذعان دارد که کاربرد بی‌قیدوشرط این تکنولوژی می‌تواند بنیان‌های مبانی اخلاقی و کرامت انسانی را به لرزه بیفکند.» (برای بررسی بیشتر نک به، اینجا)

اصول حقوقی ناظر بر کاربرد هوش مصنوعی در مخاصمات مسلحانه

کاربردهای نظامی فناوری‌های جدید و نوظهور اجتناب‌ناپذیر نیستند بلکه گزینه هایی هستند در برابر دولت‌ها که در صورت انتخاب باید در مطابقت با قواعد و مقررات موجود و با در نظر گرفتن پیامدهای بشردوستانه بالقوه آن برای نظامیان و غیرنظامیان با توجه به ملاحظات گسترده‌تر انسانیت و وجدان عمومی باشند. در حقوق بین‌الملل بشردوستانه، مفاهیم انسانیت و وجدان عمومی از اصل مارتنز استخراج می‌شود، اصلی که برای اولین بار در کنوانسیون‌های لاهه در سال‌های ۱۸۹۹ و ۱۹۰۷ ظاهر شد و بعداً در پروتکل‌های الحاقی ۱۹۷۷ به کنوانسیون‌های ژنو گنجانده شد و امروزه قاعده عرفی محسوب می‌شود. (اینجا) این اصل مقرر می‌دارد که در مواردی که مشمول معاهدات موجود نیست، غیرنظامیان و رزمندگان تحت حمایت و اقتدار اصول حقوق بین الملل برآمده از اصول بشریت و دستورات وجدان عمومی باقی می مانند. در این راستا امروزه اصل مارتنز در تمام حوزه های حقوق بین الملل بشردوستانه قابلیت اعمال دارد.

تصریح بر اعمال این اصل در حیطه کاربرد نظامی هوش مصنوعی از آن جهت اهمیت دارد که انواع و اقسام «روش‌های» بکارگیری هوش مصنوعی در جریان مخاصمه و پیامدهای بالقوه آن هنوز به طور کامل شناخته شده نیست.

وقتی صحبت از تسلیحات به میان می آید، ترکیبی از سلاح ها و فناوری هوش مصنوعی به طور فزاینده ای توجه جامعه جهانی را به خود جلب کرده، به ویژه در مورد سلاح های خودآیین. کمیته بین‌المللی صلیب سرخ سلاح های

خودآیین را به عنوان سلاح‌هایی تعریف می کند که می‌توانند به طور مستقل اهداف را انتخاب کرده و به آنها حمله کنند. (اینجا، ص ۱) در زمینه این تسلیحات مسائل متعدد حقوقی و اخلاقی مطرح شده است و جای بحث دارد که آیا چنین سیستم‌های تسلیحاتی با عملکردهای یادگیری، استدلال، تصمیم‌گیری و توانایی عمل مستقل از مداخله انسانی، می توانند در میدان‌های نبرد آتی مورد استفاده قرار گیرند یا خیر. (برای اطلاعات بیشتر و موضع کمیته بین المللی صلیب سرخ در مورد این سلاح ها نک به اینجا)

تردیدی نیست که استفاده از این سلاح ها در هر شرایطی باید طبق اصول و قواعد حقوق بین الملل بشردوستانه باشد. پروتکل اول الحاقی به کنوانسیون‌های ژنو ۱۹۴۹ مقرر می‌دارد که دولت‌ها باید به تعهدات خود برای تعیین اینکه آیا استفاده از سلاح، وسیله یا روش جنگی جدید توسط حقوق بین الملل بشردوستانه یا سایر موارد مرتبط و قواعد حقوق بین الملل در برخی یا همه شرایط در زمان تحقیق، توسعه، تملک یا در اختیار گرفتن آن سلاح ممنوع است یا نه، عمل نمایند. (ماده ۳۶). به طور خاص، قانونی بودن استفاده از سلاح های جدید باید با استفاده از معیارهای مختلف ارزیابی شود از جمله اینکه :آیا سلاح های جدید توسط کنوانسیونهای بین المللی خاص، مانند کنوانسیون سلاح های شیمیایی، کنوانسیون سلاح های بیولوژیکی یا کنوانسیون برخی از سلاح های متعارف ممنوع هستند یا خیر؟ آیا چنین سلاح‌هایی طبق ماده ۳۵ پروتکل اول باعث صدمات مضاعف یا رنج غیرضروری یا آسیب گسترده، طولانی مدت و شدید به محیط زیست طبیعی می‌شوند یا خیر؟ آیا چنین سلاح‌هایی احتمالاً اثرات حملات کورکورانه را به دنبال دارند یا خیر؟ (بند ۵ ماده ۵۱ پروتکل اول) آیا چنین سلاح هایی با اصول انسانیت و ندای وجدان عمومی طبق بند ۲ ماده ۱ پروتکل اول مطابقت دارد یا خیر؟

در این زمینه لازم به تصریح است که ماهیت یک سلاح متفاوت است از نوع استفاده یا نحوه عملکرد آن در یک وضعیت خاص. چرا که همانگونه که انسان ها دچار خطا و اشتباه می شوند ماشین ها نیز ممکن است دچار خطا و اشتباه شوند هر چند که هوشمند باشند. به دیگر سخن، حتی اگر سلاح هوشمندی در مطابقت با مقتضیات ماده ۳۶ باشد، بازهم ممکن است در عمل در مغایرت با اصول و قواعد حقوق بشردوستانه مورد استفاده قرار گیرد. تصادفی که در آن یک ماشین بدون سرنشین با یک عابر پیاده برخورد می کند، دلیل اصلی ناتوانی هوش مصنوعی در شرایط خاص را روشن می کند. در واقع هنگام تصمیم گیری، هوش مصنوعی بر الگوریتم های داخلی و حجم عظیمی از داده ها تکیه کرده و با پردازش آن به نتیجه گیری خاصی می رسد. برای فراهم کردن زمینه لازم برای تصمیم‌گیری مناسب هوش مصنوعی، باید ورودی‌ها و خروجی‌های کاملاً تعریف‌شده را تنظیم کرد، اهداف و معیارها را به وضوح تعریف نمود، دستورالعمل‌های کوتاه و دقیق ارائه داد و زنجیره‌های طولانی استدلال را با تکیه بر عقل سلیم حذف کرد، یعنی محیطی تا حد امکان بدون ابهام و قابل پیش بینی ایجاد کرد. (اینجا) مضافا کنترل

موثر انسانی بر عملکرد سیستم های تسلیحاتی مجهز به هوش مصنوعی بایستی اعمال شود تا در صورت لزوم، امکان توقف یا تغییر عملکرد سلاح ممکن باشد.

بنابراین انسان ها نباید از خطای سیستمهای هوش مصنوعی به عنوان بهانه ای برای طفره رفتن از مسئولیت های خود استفاده کنند، چرا که این امر با روح و ارزش حقوق سازگار نیست. در هر شرایطی، هدف گیری اشتباهی که توسط سیستم های تسلیحاتی هوش مصنوعی انجام می شود، صرفا مشکل خود سلاح نیست. بنابراین، هنگام استفاده از سیستم‌های تسلیحاتی هوش مصنوعی، برنامه‌نویسان و کاربران نهایی موظفند کلیه اقدامات احتیاطی لازم را اتخاذ نماید تا از عملکرد مطابق با قواعد اساسی حقوق بشردوستانه اطمینان حاصل نمایند. (در خصوص معیار اشتباه در حقوق بین الملل بشردوستانه نک برای نمونه به اینجا)

هدف گیری سیستمهای تسلیحاتی هوش مصنوعی نه تنها ارتباط تنگاتنگی با طراحی و برنامه ریزی آنها دارد، بلکه به محیط و بستری که در آن بکار گرفته می شوند نیز وابسته است. هرچه این تسلیحات استقلال بیشتری داشته باشند، استانداردهای طراحی و برنامه نویسی باید بالاتر باشد تا الزامات حقوق بین الملل بشردوستانه برآورده شود. برای این منظور، جامعه بین‌المللی مصراً دولت ها را تشویق می کند که کنوانسیون جدیدی را در خصوص سلاح‌های هوش مصنوعی تصویب نمایند. در چارچوب چنین کنوانسیون جدیدی، می توان استانداردهای طراحی سلاح‌های هوش مصنوعی، میزان و شکل کنترل انسانی، هدف های مجاز و گستره استفاده از این سلاح را تدوین نمود. تردیدی نیست که به کارگیری تسلیحات به شیوه ای مغایر با قواعد بین المللی مربوطه، از جمله حقوق بین الملل بشردوستانه ، باید مسئولیت بدنبال داشته باشد. علاوه بر این، دولت ها باید مشاوران حقوقی را نیز برای یاری به طراحان و برنامه نویسان در نظر داشته باشند. در کنار این مسائل دولتها باید در زمینه توسعه قوانین و رویه‌های ملی خود نیز تلاش نمایند و در این مورد، دولتهایی که در فناوری هوش مصنوعی پیشرفته هستند باید نقشی مهمی ایفا نمایند.

نتیجه گیری

هوش مصنوعی به عنوان یک فناوری توانمندسازی همه منظوره، کاربردهای بالقوه زیادی برای دفاع ملی دارد. استفاده نظامی از هوش مصنوعی احتمالاً به اندازه استفاده نظامی از رایانه یا برق گسترده خواهد بود. هوش مصنوعی احتمالاً بر استراتژی، عملیات، لجستیک، پرسنل، آموزش و هر جنبه دیگر ارتش تأثیر می گذارد. برخی از کاربردهای نظامی خاص هوش مصنوعی می تواند مضر باشد، مانند سلاح های خودآیین مرگبار یا استفاده از هوش مصنوعی در عملیات هسته ای. علاوه بر این، تأثیر هوشمندسازی یا شناخت عملیات نظامی می‌تواند جنگ را به شیوه‌های متعددی تغییر دهد. انقلاب‌های صنعتی اول و دوم به‌طور چشمگیری جنگ را تغییر دادند و دامنه و مقیاس تخریب‌هایی را که می‌توانستند سلاح‌های عصر صنعتی وارد کنند، افزایش دادند، گرچه سیاست گذاران در آن زمان برای این تغییرات آماده نبودند و نتیجه آن دو جنگ جهانی با جان باختن ده ها میلیون نفر بود. این افزایش

مقیاس تخریب ناشی از یک یا دو استفاده ویژه از فناوری صنعتی در جنگ نبود، بلکه بیشتر به دلیل تأثیر عمیق صنعتی شدن بود. انقلاب‌های صنعتی بسیج توده‌ای کل جوامع را برای «جنگ کامل» ممکن کرد، زیرا دولتها بهره‌وری و کارایی افزایش‌یافته‌ای که توسط فناوری صنعتی ممکن شده بود را به اهداف خشونت‌آمیز تبدیل کردند. تأثیر هوش مصنوعی بر جنگ، به احتمال زیاد شبیه به انقلاب صنعتی است، با تغییرات بی‌شماری که به‌دلیل کاربرد گسترده فناوری‌های همه‌منظوره، به جای یک فناوری مجزا مانند سلاح‌های هسته‌ای ایجاد شد. صنعتی‌سازی دامنه فیزیکی و مقیاس جنگ را افزایش داد و به ارتش اجازه داد تا ارتش‌های بزرگ‌تر و مخرب‌تری را که می‌توانستند دورتر و سریع‌تر حرکت کنند و قدرت شلیک بیشتر و در طیف وسیع‌تری از حوزه‌ها ارائه کنند، وارد میدان شوند. هوش مصنوعی در حال ایجاد یک انقلاب شناختی است و چالش این است که چگونه این انقلاب شناختی ممکن است جنگ را متحول کند. پیش بینی این امر که آیا هوش مصنوعی به طور کامل جایگزین منابع انسانی خواهد شد و به اصطلاح جنگ‌های روباتیک پدید می‌آیند، در حال حاضر بسیار دشوار است. با این حال، باید توجه داشت که شکاف بزرگی بین دولتها از نظر قابلیت‌های فناوری هوش مصنوعی وجود دارد و تهیه و استفاده نظامی از چنین قابلیت هایی برای اکثر کشورها هنوز یک هدف دست نیافتنی است.

جایگاه علم و فناوری در نظم بین‌المللی

دکتر علیرضا شمس لاهیجانی - پژوهش‌گر روابط بین‌الملل

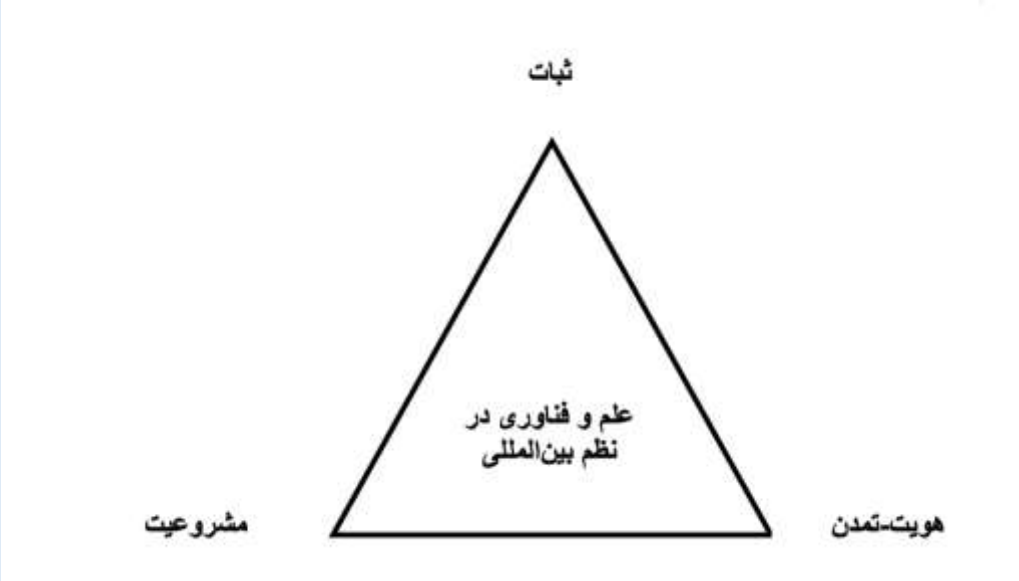
یکی از ویژگی‌های نظم بین‌المللی معاصر، و شکل‌گیری و پایداری آن، نقش علم و فناوری و تحولات مرتبط، در هدایت روابط بین ملل و دولت‌ها، و مطالعه علمی حقوق و روابط بین‌الملل است. مجموعه مطالب منتشره در سمپوزیوم «تاثیر علم و فناوری‌های نوین بر صلح و امنیت بین المللی»، با بررسی جلوه‌های مختلف موضوع در عرصه جهانی به چالش‌های امنیتی فعلی در نظم بین‌المللی پرداختند. این مجموعه نوشتارها، به خوبی به تهدیدات و فرصت‌های بالفعل و بالقوه منتج از علم و فناوری‌های نوین اشاره کرده‌اند.

در سال‌های اخیر، با توجه بیش‌تر به مطالعات علم و فناوری (Science and Technology Studies یا STS) در رشته روابط بین‌الملل، اثر فضای بین‌الملل، نیروهای اجتماعی و ایده‌های سیاسی، این رشته نیز بیش از پیش به نقش علم و فناوری در موضوعات راهبردی، امنیتی، اقتصادی و محیط زیستی پرداخته است. در این میان، به نقش علم و فناوری در نظم بین‌المللی به صورت مفهومی، نظری و موردی کم‌تر توجه شده است. نوشتار حاضر سعی دارد تا ضمن تبیین کارکرد علم و فناوری از سوی دولت‌ها، به سئوالاتی اساسی در مورد آینده نظم بین‌الملل و پایداری امنیت بین‌المللی پاسخ دهد: نظم بین‌المللی را چگونه تعریف می‌کنیم؟ جایگاه و نقش علم و فناوری در این نظم چیست؟

ریشه پاسخ به این سئوالات در گرو مرور شکل‌گیری نظم بین‌المللی است. توجه به جهان معاصر، نباید ما را از درهم‌تنیدگی تاریخی این نظم با علم و فناوری باز دارد. در قرون شانزدهم و هفدهم میلادی، مبنای نظم بین‌المللی ملهم از گفتمان سیاسی اروپا و سلطنت بود. این نظم، اهداف آن و هم‌چنین هدف اعضای جامعه جهانی، کم‌کم از اواخر قرن هجدهم و بویژه در قرن نوزدهم دست‌خوش تغییر شد. به یمن علم و فناوری، ایده «بهبود» (improvement) و «پیشرفت» (progress) به مفاهیم اصلی سیاست بین‌الملل بدل گشتند. استعمار نیز با توسل به شعار «بهبود»، بسیاری از فتوحات استعماری و توافقات تجاری بین‌المللی را پیش برد. مفاهیمی هم‌چون «رشد» و «توسعه»، حکمرانی اقتصادی را به بخش جداناپذیر نظم بین‌المللی بدل کرد. موفقیت فیزیک هسته‌ای و مهندسی در جنگ جهانی دوم، توامان با گسترش دانش اقتصادی و محبوبیت یافتن الگوهای پیشرفت و تخصص‌گرایی، به نهادینه شدن نقش و اهمیت علم و فناوری در دولت‌ها، سازمان‌های بین‌المللی و نظم بین‌المللی انجامید. نفوذ علم و فناوری به حدی اثرگذار بود که به نوشته جان راگی، نظریه‌پرداز برجسته روابط بین‌الملل و معاون برنامه‌ریزی راهبردی کوفی عنان در ملل متحد، سازمان‌های بین‌المللی «محصولی» از برقراری تعادل میان فناوری، نیاز سیاسی، و بهره‌مندی از منابع عمومی از طریق مساعی جمعی جهت حل مشکلات مشترک به حساب می‌آیند. گسترش و

پیشرفت‌های فناوری، بر هدف‌گذاری دولت‌ها، وضعیت نظم بین‌المللی و تسریع یا کاهش روندهای جهانی موثر بوده‌اند. یکی از آخرین جلوه‌های این تاثیر، واکسیناسیون در واکنش به همه‌گیری کووید-۱۹ است.

این مرور کوتاه تاریخی، به تبیین سه کارکرد علم و فناوری در نظم بین‌المللی کمک می‌کند. از یک سو، علم و فناوری‌های نوین با نقش‌آفرینی در شکل‌گیری نظم بین‌المللی، به سرچشمه ثبات و یا تغییر نظم بین‌المللی (stability or change) تبدیل شدند. در عین حال، به عنوان منبعی برای مشروعیت نظم بین‌المللی نیز به حساب می‌آیند. استفاده از علم و فناوری و چگونگی توسل به آن، در کنار تبعات حاصله، جلوه‌ای هویتی-تمدنی نیز به علم و فناوری در نظم بین‌المللی بخشیده است.



روابط و رفتارهای پایدار میان دولت‌ها و دیگر بازیگران جهانی، یکی از تعاریف پایه‌ای نظم بین‌المللی در ادبیات روابط بین‌الملل است. از این رو، ثبات و پایداری یکی از ویژگی‌های شاخص نظم بین‌المللی به حساب می‌آید که از علم و فناوری بهره جسته و در عین حال زیان دیده است. این ثبات می‌تواند خود را در تغییرات در زمینه‌های توزیع قدرت، نهادی، پذیرش قواعد و عرف نظم بین‌المللی و رفاه جمعیت نشان دهد (ص ۴۰). تسلیحات هسته‌ای، یکی از برجسته‌ترین جلوه‌های اثرگذاری علم و فناوری بر ثبات نظم بین‌المللی است. ظهور و بروز قدرت‌های دیجیتالی در کنار پیشرفت‌های فناوری‌های ارتباطات، برخی را به گمانه‌زنی برای برهم‌خوردن نظم بین‌المللی از سوی قدرت‌های دیجیتال واداشته است. این احتمال، محدودیت علم و فناوری را نیز به رخ می‌کشد: «گرچه افول فضای دیجیتال باعث رنج و آلام زیاد خواهد شد، ولی شاکله جهان را از هم نخواهد پاشید ... چرا که در نهایت در چارچوب سیاسی و نهادی دولت‌های ملی بقا پیدا می‌کنند.».

وجه مشروعیت‌بخش علم و فناوری در نظم بین‌المللی، یکی از تبعات اثر آن در شکل‌گیری این نظم است. فناوری، از دستیابی به آن تا (چگونگی) استفاده و ترویج، به مولفه‌ای برای کسب مشروعیت در نظم بین‌المللی یا

مشروعیت‌زایی برای برخی اقدامات بدل شده است. یکی از جلوه‌های رابطه مشروعیت و علم و فناوری، بهره‌برداری از پیشرفت‌های فناوری در تغییر شیوه و ابزار جنگ است. اقداماتی که پیش‌تر شاید نامشروع تلقی می‌شدند، به یمن بهره‌مندی از تبعات پیشرفت فناوری، اکنون سهل، عادی و مشروع به نظر می‌آیند. یکی دیگر از نمونه‌های این رابطه، استفاده از علم و تخصص (expertise) در مشروعیت بخشیدن به برخی سیاست‌ها مانند مقابله با تغییرات اقلیم است.

سومین جلوه علم و فناوری در نظم بین‌الملل، رابطه‌ای نزدیک به دو جلوه پیشین دارد. دست یافتن به آخرین فناوری‌ها و یا انحصار در علم، در کنار این‌که نمادهایی از قدرت تلقی می‌شوند، تشکیل‌دهنده هویت و دارای مولفه‌های تمدنی است. این ابعاد تمدنی، علم و فناوری را نمادی از قدرت، جایگاه، و مدرن بودن قلمداد می‌کند که مبین سلسه مراتب نظم بین‌المللی و آشکارساز تفاوت‌ها می‌نماید. مفهوم Standard of Civilisation (معیار تمدن) که در مطالعات روز روابط بین‌الملل ساخته‌ای نژادی و استعماری شمرده می‌شود، ریشه در نگاهی حقوقی به «متمدن» دانستن جوامع مختلف در قرن نوزدهم بر مبنای معیارهای غربی و استعماری برای به رسمیت شناخته شدن از سوی دولت‌های اروپایی دارد. نقش علم و فناوری در جوامع در کنار میزان پیشرفت آن، امروزه نمایان‌گر میزان توسعه اجتماعی و مادی، و نماد تمدنی-هویتی به حساب می‌آید. مصادیق هویتی-تمدنی علم و فناوری در سیاست جهانی امروز، تاریخچه پرتاب ماهواره از سوی کشورهای مختلف، انحصار در علوم خاص و اخیرا توسعه واکسن‌های کووید-۱۹ است.

لحاظ کردن این سه کارکرد علم و فناوری در نظم بین‌المللی، می‌تواند به مطالعه دقیق‌تر گذشته، حال و آینده آن کمک نماید. نقش علم و فناوری نه تنها به صورت موردی یا در رشته‌های خاص، بلکه باید به صورت همه‌جانبه‌نگر به طوری که هویت، مشروعیت و ثبات نظم حاضر را تغییر یا تثبیت نماید، بررسی شود. در حالی که تغییر نظم بین‌المللی ناشی از افزایش قدرت چین یا تحولات اخیر مرتبط با اوکراین به کلیدواژه عرصه عمومی و تخصصی تبدیل شده، تدقیق در توسعه نقش علم و فناوری در شکل‌گیری نظم بین‌المللی و اثرگذاری آن بر آینده نظم با عنایت به مولفه‌های ذکر شده، می‌تواند چارچوب مفهومی و نظری جدیدی از تغییرات نظم بین‌المللی و اثر آن بر صلح و امنیت بین‌المللی ارائه دهد.