

حکمرانی داده در قوانین و توافقنامه‌های بین-المللی



اندیشکده حکمرانی شریف

گروه حکمرانی عصر دیجیتال
آذر ۱۴۰۰





نوع سند	گزارش پروژه
حوزه تخصصی	گروه حکمرانی عصر دیجیتال
برنامه	
عنوان	حکمرانی داده در قوانین و توافقنامه‌های بین‌المللی
نگارنده/نگارندگان	سیما رفسنجانی نژاد
ناظر کیفی	عمادالدین پاینده
تاریخ انتشار	آذر ۱۴۰۰
مخاطب	شورای راهبردی روابط خارجی

جملات کلیدی

کلمات کلیدی

حکمرانی داده حکمرانی اینترنت، حکمرانی سایبری

در عصر دیجیتال، مفاهیمی مانند قدرت، منازعه و امنیت دستخوش تحولات معنایی و کارکردی کرده است و عرصه جدیدی به نام «فضای سایبری» ایجاد شده است. ویژگی‌های فضای سایبر از جمله «بی‌حدومرز بودن»، «سرعت خیره‌کننده ارتباطات»، «تجهیزات قابل دسترسی»، «ارزان بودن»، «دسترسی فوری» و «نظارت ناکافی» در این فضا باعث شده است که جایگاه استراتژیک این فضا ارتقا یابد و به عنوان بعد پنجم به ابعاد سنتی تهدیدات (ابعاد چهارگانه زمین، دریا، هوا، فضا) افزوده گردد.

با توجه به روند سریع پیشرفت و توسعه فناوری‌ها، حقوق بین‌الملل نتوانسته خود را با این روند سریع وفق دهد و فاصله زیادی با پیشرفت فناوری دارد. حقوق بین‌الملل باید با وضع قوانین مربوطه همزمان با روند سریع پیشرفت فناوری‌ها توسعه یابد که این امر لاجرم در گرو همکاری بین کشورها است. در طول ۲۰ سال گذشته، هنجارهای نرم در حال تبدیل شدن به قواعد الزام‌آور بین‌المللی است و این فرآیند بدون حضور ایران و ایفای نقش مؤثر آن در حال اجرا است که این رویه و شکل‌گیری هنجارها و قواعد الزام‌آور که ممکن است بعضاً در تعارض با منافع ملی و حاکمیت ملی باشد، به شدت به حقوق و منافع ایران آسیب خواهد رساند و زمینه‌ها و بهانه‌های آتی برای اعمال فشار و تحریم از ناحیه فضای سایبری را فراهم خواهد نمود.

به طور کلی سه رویکرد در رابطه با حکمرانی اینترنت و حکمرانی داده وجود دارد:

- الگوی دولت-محور چین: در رویکرد چینی و روسی کنترل کامل فضای اینترنت و داده توسط دولت‌ها انجام می‌شود و بر بعد هژمونیک قدرت سایبری تأکید می‌شود.
- الگوی حریم خصوصی محور اتحادیه اروپا: احترام به حریم خصوصی شهروندان و حقوق بشر مهم‌ترین دغدغه این الگوی حکمرانی است. در این زمینه اروپا اقداماتی از جمله تصویب GDPR در زمینه حفظ حریم خصوصی انجام داده است.
- الگوی «آزاد» ایالات متحده آمریکا: الگوی حاکم در آمریکا مبتنی بر الگوی آزاد بوده است هرچند این الگو طی سال‌های اخیر دچار تغییراتی شده است. در این رویکرد، دولت مداخله نمی‌کند و اختیار در دست شرکت‌های بزرگ است. یعنی سیاست‌های دولت منتج از رشد شرکت‌های بزرگ است.

اجلاس جهانی جامعه اطلاعاتی (WSIS) و انجمن حکمرانی اینترنت (IGF)

موضوع حکمرانی اینترنت و حکمرانی داده از موضوعات مهم در دستور کار جهانی است که با فشار کشورهایی مانند چین و روسیه وارد ادبیات سازمان ملل متحد شده و متعاقباً منجر به نهادسازی در این حوزه شده است. شکل‌گیری اجلاس جهانی جامعه اطلاعاتی (WSIS) در سال ۲۰۰۳ اولین نتیجه تلاش این کشورها برای گسترده کردن دامنه شرکت‌کنندگان در زمامداری اینترنت بود.

سازمان ملل در سال ۲۰۰۵ در تونس اقدام به برگزاری دوره دوم اجلاس جهانی جامعه اطلاعاتی نمود. در این اجلاس، به‌منظور تسهیل گفت‌وگوی بین‌المللی حول مسائل حکمرانی اینترنت، تصمیم به ایجاد مجمع و انجمنی چندملیتی گرفته شد. درخواست تشکیل این انجمن به دبیر کل سازمان ملل ارسال شد و پس از موافقت، **انجمن حکمرانی اینترنت** (Internet Governance Forum (IGF) تأسیس شد.

انجمن حکمرانی اینترنت به‌منظور گرد هم‌آیی افراد مختلف و گروه‌های ذینفع تأثیرگذار در آینده اینترنت تشکیل شده است. این انجمن جایگاه حقوقی برای تصمیمات الزام‌آور ندارد، بلکه در طراحی آن تلاش شده است که فارغ از محدودیت‌های موجود ساختارهای رسمی بین‌المللی، محلی برای تبادل نظر آزاد و برابر افراد درباره مسائل اصلی و مهم اینترنت در جهان باشد. هرچند که این انجمن صلاحیت تصمیم‌گیری ندارد و بیشتر در حوزه تصمیم‌سازی برای سازمان‌ها و نهادهای تصمیم‌گیر ایفای نقش می‌کند، اما نمی‌توان این موضوع را به‌عنوان ضعف IGF محسوب نمود، چرا که این انجمن پایه و مبنای تصمیمات دیگر سازمان‌ها را بنا می‌نهد و این چنین قدرت خود را در اثرگذاری به نمایش می‌گذارد.

در نشست چهاردهم انجمن حکمرانی اینترنت در سال ۲۰۱۹ به منظور افزایش همکاری‌های دیجیتالی، موضوع تشکیل **انجمن حکمرانی اینترنت پلاس (IGF+)** مطرح شد. این مکانیسم در چارچوب ملل متحد تشکیل و اعضای آن شامل همه ذینفعان خواهد بود. مجمع اینترنت پلاس به دنبال برطرف کردن نقاط ضعف IGF است. از جمله تغییراتی که سازوکار جدید به دنبال ایجاد آن است اتخاذ تصمیم‌های الزام‌آور توسط مجمع است.

در سال ۲۰۲۰، انجمن حکمرانی اینترنت با حضور نمایندگان دولت‌ها، جوامع فنی و آکادمیک، کسب‌وکارها، جامعه مدنی و سازمان‌های میان‌دولتی به منظور بحث پیرامون پیشبرد طیفی از مباحثات سیاستی مرتبط با اینترنت برگزار شد. از جمله مباحث اصلی که در اجلاس ۲۰۲۰ مطرح شد، موضوع «داده» بود. «دموکراتیزه کردن تولید داده و کاربرد داده»، به طوری که خود کاربران، قوانین خودشان را وضع کنند و خودشان در مورد اینکه داده‌هایشان چگونه استفاده می‌شوند، تصمیم بگیرند. در گردآوری داده، نباید حریم خصوصی شخصی و حریم خصوصی جمعی جامعه به خطر بیفتد. از جمله مباحث دیگر مجمع این بود که مزایای فناوری‌های داده‌محور باید در دسترس همه قرار داشته باشد نه فقط دولت‌ها و بخش خصوصی. برای این منظور مردم باید به وسایل دیجیتال و اتصال و نیز مهارت سواد دیجیتال دسترسی داشته باشند تا از فناوری‌های داده‌محور استفاده کامل کنند. شانزدهمین نشست IGF تحت عنوان «اینترنت یکپارچه» از ۶ تا ۱۰ دسامبر ۲۰۲۱ در لهستان برگزار خواهد شد.

«گروه کارشناسان دولتی» و «گروه کاری باز ملل متحد» در خصوص توسعه در زمینه‌ی اطلاعات و ارتباطات در حوزه امنیت بین‌المللی:

دو سازوکار دیگری که در چارچوب ملل متحد در رابطه با موضوعات مرتبط با اینترنت شکل گرفته است گروه کارشناسان دولتی^۱ (GGE) با تعداد محدود (۲۵ دولت انتخاب‌شده توسط دبیر کل ملل متحد) و گروه باز^۲ (OEWG) با امکان مشارکت تمامی دولت‌ها عضو ملل متحد در سال ۲۰۱۸ می‌باشند. هر دو گروه در زمینه‌ی امنیت اطلاعات در فضای سایبر، توسط روسیه ایجاد شده است. هدف از تشکیل گروه‌های مذکور، افزایش نقش دولت‌ها برای تضمین امنیت و ثبات بین‌المللی است که می‌تواند توسط فضای سایبر دچار مشکل گردد.

سازوکار انتخاب و تشکیل گروه کارشناسان در مجمع عمومی بدین صورت است که اگر اعضای مجمع عمومی، در یک موضوع تشخیص دادند که بررسی موضوع، نیازمند تشکیل گروه کارشناسان دولتی است، با صدور قطعنامه‌ای از دبیرکل سازمان ملل می‌خواهند که گروه را تشکیل دهد. کم و کیف تشکیل گروه نیز در قطعنامه مشخص می‌شود. معمولاً ذکر می‌شود که بر اساس توزیع عادلانه جغرافیایی تعیین شود. اما در عمل، این عدالت چندان رعایت نمی‌شود و کشورهای ذی‌نفوذ در سازمان ملل، مخصوصاً پنج عضو دائم شورای امنیت، در تمام گروه‌های کارشناسی، فعال هستند. البته گفته می‌شود که قدرت و پیشرفت سایبری کشور منتخب در موضوع سایبر نیز در نظر گرفته می‌شود. اما در عمل باز موارد نقض زیادی وجود دارد. مثلاً کشور ما هیچ‌گاه عضو هیچ یک از گروه کارشناسان دولتی نبوده است، اما کشورهایی مثل اردن، مصر، غنا، کلمبیا، کنیا و مالی، عضویت در گروه کارشناسان دولتی را تجربه کرده‌اند، بعید به نظر می‌رسد که در عرصه فناوری سایبری، این کشورها قوی‌تر از کشور ما باشند. این موضوع البته با میزان فعالیت دیپلماتیک کشورها نیز ارتباط مستقیم دارد.

قطعنامه‌های مرتبط با موضوع امنیت سایبری

هر چند صنعت اینترنت از بدو امر در دست آمریکا بوده و این کشور سال‌های متمادی در پی هنجارسازی در این فضا بوده است، بعد دیپلماتیک فضای سایبری را کشورهایی چون روسیه و چین در محیط بین‌الملل پیش برده‌اند. به عنوان مثال اولین قطعنامه در ارتباط با امنیت سایبری را روسیه در سال ۱۹۹۸، به کمیته اول مجمع عمومی سازمان ملل ارائه کرد. آمریکا نیز در مقام مقابله قطعنامه‌هایی به کمیته‌های دوم و سوم ارائه نمود. پیش‌نویس اولین کنوانسیون در مورد امنیت سایبری را روس‌ها در اجلاس ایکاترین بورگ در سال ۲۰۱۱ رونمایی کردند که غرب با آن مقابله کرد. اولین کردارنامه در مورد امنیت سایبری از طرف شانگهای صادر شد که غربی‌ها از آن استقبال نکردند. روس‌ها در سال ۲۰۱۷

¹ Group of Governmental Experts

² Open-ended working group

از اولین پیش نویس بین المللی در زمینه جرایم سایبری رونمایی کردند که بررسی این پیش نویس همچنان در دستور کار دولت ها می باشد.

سیاست امنیت سایبری ناتو

کشورهای عضو ناتو برای اولین بار در سال ۲۰۰۲ و در نشست پراگ بر لزوم تقویت خود در مقابل حملات سایبری تاکید و در سال ۲۰۰۸ نیز اعضای این سازمان "سیاست دفاع در برابر حملات سایبری" را امضا کردند. در سال ۲۰۱۴، متحدین ناتو دفاع سایبری را به عنوان بخشی از "دفاع مشترک" پذیرفتند و تصمیم گرفتند که ماده ۵ این سازمان را در صورت حمله سایبری، اجرا کنند. طبق ماده ۵ این توافق، اعضای ناتو حمله نظامی علیه دیگر متحدان خود در اروپا یا آمریکای شمالی را حمله به تمامی کشورهای عضو تلقی و با آن مقابله می کنند.

اعضای ناتو در اجلاس سران ورشو ۲۰۱۶ فضای سایبری را نیز در کنار حریم هوایی، زمینی و دریایی به حریم عملیاتی خود اضافه کردند و متعهد شدند توانایی های دفاع سایبری خود را بهبود بخشند. ناتو سال ۲۰۱۸ «مرکز عملیات سایبری» را تاسیس کرد. در سال ۲۰۲۱ وزرای ناتو با ایجاد اولین «استراتژی هوش مصنوعی» در این اتحاد موافقت کردند. این استراتژی استانداردهایی را برای استفاده مسئولانه از هوش مصنوعی مطابق با قوانین بین المللی تعیین می کند. همچنین ایجاد «صندوق نوآوری ناتو» با ذخیره مالی یک میلیارد یورو از جمله اقدامات ناتو در سال ۲۰۲۱ بوده است. صندوق نوآوری، بخشی از پروژه جدید نوآوری دفاعی اتحادیه برای آتلانتیک شمالی خواهد بود که شامل ایجاد شبکه ای از مراکز آزمایش فناوری و استنادات تقویت کننده به منظور استفاده بهتر از نوآوری های غیرنظامی برای امنیت ناتو است و پیوند فناوری بین اروپا و آمریکای شمالی را تقویت می کند.

طرح «کنوانسیون دیجیتال ژنو» و «توافقنامه فنی امنیت سایبری»

طرح پیشنهاد «کنوانسیون دیجیتال ژنو» (Digital Geneva Convention) در سال ۲۰۱۷ توسط رئیس شرکت مایکروسافت داده شد و پس از آن «توافقنامه فنی امنیت سایبری» و ائتلاف ۳۴ شرکت از مجموعه شرکت های فناوری، با شعار مقابله با حملات سایبری دولت ها و حفاظت از کاربران و شرکت ها اعلام شد. به جز ترندمیکرو (ژاپن)، نوکیا (سوئد)، آواست (جمهوری چک)، تلفونیکا (اسپانیا) و SAP (آلمان)، بقیه شرکت ها، همگی آمریکایی هستند. یکی از زمینه های اصلی طرح کنوانسیون دیجیتال و توافق فنی شرکت های آمریکایی، گسترش حملات سایبری در سال های اخیر است. این حرکت با هدایت دولت آمریکا و با محوریت شرکت های بزرگ زیرساخت و فناوری سایبری شکل گرفته است و هنجارسازی در حوزه امنیت سایبری با استفاده از دیپلماسی غیررسمی و ظرفیت های غیردولتی به یکی از اولویت های اصلی آمریکا که به دنبال رهبری جهانی در حوزه اینترنت است، تبدیل شده است.

از نظر حقوق بین‌الملل، آن چه مورد توافق این شرکت‌ها قرار گرفته، تنها یک اعلامیه است و اعلامیه‌ها در قالب حقوق نرم قرار می‌گیرند، یعنی دولت‌ها الزامی برای اجرای آن‌ها ندارند. اصول توافق فنی که توسط این ۳۴ شرکت امضا شده است هر چند الزام‌آور نیست اما می‌تواند در آینده مبنای شکل‌گیری اسناد الزام‌آور برای دولت‌ها باشد.

نام بسیاری از شرکت‌های بزرگ غربی مانند اپل، گوگل و آمازون در فهرست امضاکنندگان این موافقت‌نامه دیده نمی‌شود. شرکت‌های روسی و چینی نیز مطلقاً حضور ندارند، لذا در حال حاضر اجماع کاملی در این زمینه وجود ندارد. اما باید آگاه بود که این شرکت‌ها در آینده تلاش خواهند کرد تعداد امضا کنندگان موافقت‌نامه را افزایش دهند و از این طریق بر مشروعیت خود بیفزایند. اگر این توسعه با موفقیت صورت پذیرد این اصول، شکل قاعده عرفی به خود خواهد گرفت، یعنی در این مرحله دولت‌ها مجبور به اجرای مفاد این موافقت‌نامه خواهند شد بدون این که آن را امضا کرده باشند و این پدیده خطرناکی است که باید با اتخاذ تصمیمات مقتضی جلوی شکل‌گیری این قاعده عرفی را گرفت.

توافق کشورهای عضو کواد در زمینه امنیت سایبری

در سال ۲۰۲۱ کشورهای عضو گفتگوی راهبردی کواد (QUAD) (ایالات متحده، ژاپن، استرالیا و هند) در خصوص همکاری در زمینه امنیت سایبری به توافق رسیده‌اند تا گروه امنیت سایبری را راه‌اندازی کنند. براساس توافق، این گروه متخصص در سطح رهبران برای ارتقاء تعامل بین دولت‌ها و صنعت برای دستیابی به پیشرفت‌های پایدار در زمینه‌های مختلف از جمله تصویب و اجرای استانداردهای مشترک سایبری، تهیه نرم‌افزارهای امن، پرورش نیروی انسانی و استعدادها و ترویج یک زیرساخت دیجیتالی مطمئن و قابل اعتماد جلسات منظمی برگزار خواهد کرد.

نقشه راه استراتژی سه ساله امنیت سایبری ژاپن در سال ۲۰۲۱ تصویب شده است که در این سند بر اهمیت تقویت همکاری ژاپن با آمریکا، استرالیا و هند در قالب توافق کشورهای عضو کواد تاکید شده است. طبق سند مذکور، فهرستی شامل کشورهای چین، روسیه و کره شمالی به عنوان کشورهای تهدید سایبری احتمالی با ظرفیت‌های رو به رشد است.

دیپلماسی سایبری آمریکا در سال ۲۰۲۱

در سند رهنمود استراتژیک موقت امنیت ملی آمریکا ۲۰۲۱ تاکید شده است که آمریکا درصدد است شبکه‌ای از متحدان را به وجود آورد و از طریق همکاری با شرکا و دموکراسی‌های همفکر خود، قدرت جمعی را برای حمایت از قوانین موجود و شکل‌گیری هنجارهای جدید جهانی در فضای مجازی، ایجاد توافقنامه‌های جدید و نیز پیشبرد منافع مشترک و جلوگیری از تهدیدات مشترک، از تهدیدات سایبری گرفته تا اقتدارگرایی دیجیتالی، متحد نماید. از جمله استراتژی‌های وزارت خارجه آمریکا تاکید بر همگرایی با متحدان اروپایی و آسیایی با هدف تقویت ارزش‌های دموکراسی لیبرال در فضای مجازی و

مقابله با آن چیزی است که اقتدارگرایی کشورهای متخاصم در اینترنت لقب داده می‌شود. بدیهی است که هدف اصلی از چنین اتحادسازی‌هایی مقابله با نفوذ فزاینده کشورهایمانند چین، روسیه و ایران در فضای مجازی است که با تاثیرگذاری و تسلط آمریکا و غرب در فضای مجازی مخالف هستند.

آمریکا مدتی است که به دنبال ایجاد ابتکار عمل‌های دیپلماتیک فناوری محور نیز هست که از جمله آنها می‌توان به **"همکاری جهانی در حوزه هوش مصنوعی" یا GPAI** اشاره کرد. این ابتکار عمل توسط ۳۵ کشور عضو سازمان همکاری و توسعه اقتصادی (OECD) ابداع شد که خود را به اصول دموکراسی و اقتصاد آزاد متعهد می‌دانند. همچنین کشورهای عضو گروه G7 و نیز هند، کره جنوبی، سنگاپور، اسلوونی و تمامی کشورهای عضو اتحادیه اروپا در آن عضویت دارند.

آمریکا از **اتحاد دیگری موسوم به D10** نیز پشتیبانی می‌کند که توسط انگلیس در سال ۲۰۲۰ شکل گرفته و هدف از راه‌اندازی آن مقابله با فناوری‌های چینی است. انگلیس مدعی است عضویت ده دموکراسی بزرگ جهان (کشورهای G7 در کنار استرالیا، کره جنوبی و هند) در این اتحاد، دسترسی به تجهیزات مخابراتی نسل پنجم و دیگر فناوری‌های نوظهور را بدون اتکا به چین ممکن می‌کند. نگرانی اصلی غرب این است که موفقیت فزاینده شرکت‌های فناوری چینی مانند هواوی در تسخیر بازار مخابراتی نسل پنجم باعث خواهد شد تا کنترل زیرساخت‌های فناورانه، اقتصادی و تجاری و بازرگانی ده‌ها کشور جهان به دست چین بیفتد و آمریکا و اروپا در رقابت با اژدهای زرد شکستی غیرقابل جبران را متحمل شوند.

مقررات‌گذاری هوش مصنوعی در اتحادیه اروپا

در بیست و یکم آوریل ۲۰۲۱ اتحادیه اروپا پیشنهادیه برای مقررات‌گذاری در هوش مصنوعی را منتشر کرد. این اقدام اتحادیه اروپا را می‌توان نخستین اقدام در سطح جهانی به منظور تنظیم مقررات هوش مصنوعی دانست. این مجموعه به ارائه تعدادی از قوانین و مقررات برای استقرار و استفاده از سیستم‌های هوش مصنوعی در اتحادیه اروپا شامل مجموعه‌ای از ممنوعیت‌ها برای کاربردهای خاصی از هوش مصنوعی، الزامات و وظایف اجباری در اپراتوری سیستم‌های پر ریسک و همین‌طور رویکرد این اتحادیه در پایش و نظارت بر بازار هوش مصنوعی می‌پردازد. هر پروپوزال قانونی برای بحث و بررسی بیشتر به پارلمان اروپا و شورای اروپا می‌رود.

کنفرانس جهانی اینترنت در چین

یکی از ابعاد مهم رویکرد چین به اینترنت توجه به توسعه و بعد اقتصادی آن است. شی جی پینگ رئیس‌جمهور چین در سخنرانی نشست کنفرانس جهانی اینترنت^۳ در سال ۲۰۱۵ مفهوم «ایجاد جامعه‌ای با سرنوشت مشترک در فضای سایبری» را مطرح نمود. این مفهوم دارای پنج عنصر شامل؛ سرعت دادن به ایجاد شبکه زیرساخت جهانی و ارتقای اتصالات متقابل، ایجاد بستر آنلاین برای به اشتراک گذاشتن تبادلات فرهنگی و ارتقای تبادلات چندجانبه، ارتقای نوآوری و توسعه اقتصاد اینترنت و کامیابی مشترک، حفاظت از امنیت شبکه و ارتقای توسعه منظم و ایجاد سیستم حکمرانی عادلانه و منصفانه سایبر است. بررسی پنج عنصر مذکور به‌خوبی نمایانگر این است که استفاده از اینترنت برای توسعه اقتصادی و فرهنگی در چین نسبت به سایر ابعاد آن ازجمله بعد امنیتی اولویت دارد. در نشست ۲۰۲۱ کنفرانس جهانی اینترنت حدود ۲۰۰۰ شرکت‌کننده از جمله نمایندگان دولت‌های داخلی و خارجی، سازمان‌های بین‌المللی، آژانس‌های صنعتی، شرکت‌های فناوری جهانی، اتاق‌های فکر دانشگاه و موسسات تحقیقاتی شرکت کردند.

^۳ World Internet Conference