

چالش های حقوقی ژئوالکترونیک کوانتومی برای حفاظت اکوسیستم های دیجیتال

(تاریخ دریافت ۱۴۰۴/۰۷/۱۵، تاریخ تصویب ۱۴۰۴/۱۲/۰۳)

دکتر محمد افروغ^۱

نرجس روشن سروستانی

چکیده

گسترش فناوری های نوظهور، به ویژه ژئوالکترونیک کوانتومی، افق های تازه ای را در حفاظت و مدیریت اکوسیستم های دیجیتال گشوده است. این فناوری با بهره گیری از پردازش کوانتومی، حسگرهای مکانی پیشرفته و تحلیل داده های عظیم، امکان پایش دقیق و امنیتی بالاتری را برای زیرساخت های دیجیتال فراهم می سازد. با این حال، هم زمان با توسعه این ظرفیت ها، چالش های حقوقی متعددی در حوزه هایی همچون حریم خصوصی داده ها، مالکیت و حاکمیت اطلاعات، مسئولیت حقوقی ناشی از خطاهای فناوری و ناکارآمدی مقررات موجود پدیدار شده است. مسئله اصلی تحقیق آن است که نظام های حقوقی کنونی تا چه میزان توان پاسخ گویی به الزامات و پیامدهای حقوقی ژئوالکترونیک کوانتومی را در راستای حفاظت از اکوسیستم های دیجیتال دارند. پرسش اصلی پژوهش بر شناسایی و تحلیل چالش های حقوقی این فناوری و امکان ارائه چارچوبی حقوقی متناسب با ماهیت کوانتومی آن متمرکز است. هدف تحقیق، تبیین این چالش ها و ارائه راهکارهای حقوقی برای ارتقای امنیت و پایداری اکوسیستم های دیجیتال می باشد. روش تحقیق، توصیفی-تحلیلی با بهره گیری از مطالعات کتابخانه ای، اسناد حقوقی و تحلیل تطبیقی است. نتایج نشان می دهد که بازنگری مفهومی و تقنینی در حقوق فناوری اطلاعات برای انطباق با ژئوالکترونیک کوانتومی امری ضروری است.

واژگان کلیدی: ژئوالکترونیک کوانتومی، اکوسیستم های دیجیتال، چالش های حقوقی



۱- مقدمه

تحولات شتابان فناوری‌های نوظهور، به‌ویژه در حوزه ژئوالکترونیک کوانتومی، ساختار و کارکرد اکوسیستم‌های دیجیتال را به‌صورت بنیادین دگرگون کرده است. ژئوالکترونیک کوانتومی با اتکا بر پردازش کوانتومی، حسگرهای فوق‌دقیق مکانی، تحلیل داده‌های عظیم و ارتباطات رمزنگاری شده، امکان پایش، مدیریت و حفاظت پیشرفته از فضاها و تجهیزات دیجیتال و زیرساخت‌های اطلاعاتی را فراهم می‌سازد. با این حال، همین ظرفیت‌های فنی بی‌سابقه، چالش‌های حقوقی پیچیده‌ای را در زمینه حریم خصوصی، مالکیت داده، امنیت اطلاعات، مسئولیت مدنی و حاکمیت دیجیتال ایجاد کرده‌اند. مسئله اصلی این پژوهش آن است که نظام‌های حقوقی موجود، که عمدتاً مبتنی بر فناوری‌های کلاسیک طراحی شده‌اند، تا چه اندازه توانایی پاسخ‌گویی به پیامدهای حقوقی ناشی از به‌کارگیری ژئوالکترونیک کوانتومی در حفاظت از اکوسیستم‌های دیجیتال را دارند و چه خلأها یا تعارض‌هایی در این میان قابل شناسایی است. در این چارچوب، پژوهش حاضر می‌کوشد نسبت میان پیشرفت فناوریانه و سازوکارهای حقوقی را به‌طور نظام‌مند مورد واکاوی قرار دهد.

بر این اساس، سؤال اصلی تحقیق عبارت است از: «چالش‌های حقوقی ناشی از به‌کارگیری ژئوالکترونیک کوانتومی در حفاظت از اکوسیستم‌های دیجیتال کدام‌اند و چگونه می‌توان آن‌ها را در چارچوب حقوقی کارآمد مدیریت کرد؟» سؤالات فرعی شامل این موارد است: تأثیر فناوری‌های کوانتومی بر مفهوم سنتی حریم خصوصی داده‌ها چیست؟ مسئولیت حقوقی ناشی از خطا یا سوءاستفاده از سامانه‌های ژئوالکترونیک کوانتومی بر عهده چه اشخاص یا نهادهایی قرار می‌گیرد؟ و آیا قواعد حقوق بین‌الملل دیجیتال پاسخ‌گوی ماهیت فرامرزی این



فناوری‌ها هست یا خیر؟ فرضیه اصلی پژوهش بر این مبنا استوار است که حقوق موجود، بدون بازنگری و توسعه مفهومی، قادر به تنظیم جامع پیامدهای ژئوالکترونیک کوانتومی نخواهد بود. هدف اصلی تحقیق، تبیین و تحلیل چالش‌های حقوقی این حوزه و ارائه چارچوبی نظری برای ارتقای حفاظت حقوقی از اکوسیستم‌های دیجیتال است. اهداف فرعی نیز شامل شناسایی خلأهای تقنینی، تحلیل تطبیقی رویکردهای حقوقی و پیشنهاد راهکارهای حقوقی متناسب با ماهیت کوانتومی این فناوری‌ها می‌باشد.

ضرورت انجام این پژوهش از آنجا ناشی می‌شود که اکوسیستم‌های دیجیتال، به‌عنوان زیربنای اقتصاد، حکمرانی و تعاملات اجتماعی معاصر، در معرض تهدیدهای نوینی قرار گرفته‌اند که ابزارهای حقوقی سنتی توان مهار کامل آن‌ها را ندارند. بررسی پیشینه تحقیق نشان می‌دهد که مطالعات متعددی در حوزه حقوق فناوری اطلاعات، امنیت سایبری و حتی حقوق کوانتومی انجام شده است، اما اغلب این پژوهش‌ها به‌صورت جزیره‌ای و بدون تمرکز مشخص بر پیوند ژئوالکترونیک کوانتومی و حفاظت از اکوسیستم‌های دیجیتال صورت گرفته‌اند. برخی آثار به ابعاد فنی و برخی دیگر به مباحث کلی حقوق داده پرداخته‌اند، در حالی که تحلیل جامع و میان‌رشته‌ای چالش‌های حقوقی این فناوری نوظهور کمتر مورد توجه قرار گرفته است. از این رو، جامعیت پیشینه در این پژوهش با بررسی منابع داخلی و خارجی، تحلیل رویکردهای حقوقی تطبیقی و ارزیابی اسناد و مقررات مرتبط تأمین می‌شود تا تصویری منسجم از وضعیت دانش موجود ارائه گردد.

نوآوری اصلی این تحقیق در تلفیق مفاهیم ژئوالکترونیک کوانتومی با نظریه‌های نوین حقوقی و ارائه تحلیلی آینده‌نگر از حفاظت اکوسیستم‌های دیجیتال نهفته است. این پژوهش فراتر از



توصیف چالش‌ها، می‌کوشد با بازتعریف مفاهیمی چون مسئولیت، حاکمیت داده و امنیت حقوقی در بستر کوانتومی، چارچوبی نوآورانه برای تنظیم حقوقی این حوزه پیشنهاد دهد. در پایان بررسی پیشینه، روشن می‌شود که خلأ قابل توجهی در ادبیات حقوقی درباره پیامدهای خاص ژئوالکترونیک کوانتومی وجود دارد و همین امر، ارزش افزوده علمی و کاربردی پژوهش حاضر را برجسته می‌سازد. بدین ترتیب، این تحقیق می‌تواند به عنوان گامی مؤثر در توسعه ادبیات حقوق فناوری‌های نوظهور و تقویت حفاظت حقوقی از اکوسیستم‌های دیجیتال تلقی شود.

۲- مبانی نظری و مفهومی ژئوالکترونیک کوانتومی

۲-۱- مفهوم و ماهیت ژئوالکترونیک کوانتومی

ژئوالکترونیک کوانتومی بر پایه هم‌پیوندی فناوری‌های کوانتومی با سامانه‌های الکترونیکی وابسته به مکان شکل گرفته و از این حیث، واجد ماهیتی متفاوت از الگوهای سنتی پردازش داده‌های مکانی است. در این چارچوب، داده‌های فضایی بر اساس منطق‌های احتمالاتی و غیرخطی تولید و پردازش می‌شوند و همین ویژگی سبب می‌گردد که مکان از جایگاه یک مؤلفه ثابت خارج شده و به عنصری فعال در سازمان‌دهی اطلاعات دیجیتال تبدیل شود. چنین دگرگونی‌ای، کارکرد داده‌های مکانی را از سطح بازنمایی واقعیت فیزیکی فراتر برده و آن‌ها را به عناصر تأثیرگذار در فرآیندهای تصمیم‌سازی دیجیتال بدل می‌کند. از منظر حقوقی، این تحول موجب می‌شود که مفاهیمی مانند قطعیت، قابلیت پیش‌بینی و امکان کنترل داده که شالوده نظم حقوقی کلاسیک را تشکیل می‌دهند، با وضعیت‌های سیال و متغیر مواجه شوند. در



نتیجه، ژئوالکترونیک کوانتومی نه صرفاً یک ابزار فنی، بلکه پدیده‌ای حقوق‌ساز تلقی می‌شود که ظرفیت بازتعریف مبانی حقوق داده را در خود دارد.

ماهیت ژئوالکترونیک کوانتومی از حیث ساختاری، شبکه‌ای و فراتر از مرزهای جغرافیایی است؛ به گونه‌ای که تمایز روشن میان تولیدکننده، پردازش‌کننده و بهره‌بردار داده به تدریج کمرنگ می‌شود. این درهم‌تنیدگی نقش‌ها سبب می‌گردد که فناوری از جایگاه یک ابزار خنثی فاصله گرفته و در جهت‌دهی به کنش‌های دیجیتال نقشی تعیین‌کننده ایفا کند. داده‌های مکانی در این بستر، نه تنها بازتاب وضعیت موجود، بلکه عاملی مؤثر در شکل‌دهی به واقعیت دیجیتال آینده محسوب می‌شوند. چنین وضعیتی، الگوهای حقوقی مبتنی بر صلاحیت سرزمینی و نظارت متمرکز را با تنش‌های مفهومی مواجه می‌سازد و مفهوم حاکمیت داده را از وابستگی صرف به قلمرو فیزیکی جدا می‌کند. در این چارچوب، نظم حقوقی با پدیده‌ای روبه‌رو است که منطق آن بیش از آنکه مکانی باشد، شبکه‌ای و غیرمتمرکز است.

۲-۲- سیر تحول فناوری‌های کوانتومی در حوزه دیجیتال

سیر تحول فناوری‌های کوانتومی در حوزه دیجیتال از پایه‌های نظری اولیه در اوایل قرن بیستم شکل گرفت و به کاربردهای پیشرفته در پردازش اطلاعات مکانی و زیرساخت‌های اطلاعاتی رسید. پایه‌گذاری مفهوم کوانتوم انرژی توسط پلانک و تبیین پدیده فوتوالکتریک توسط اینشتین، افق‌های پردازش غیرکلاسیک داده‌ها را گشود و فرمول‌بندی ماتریسی هایزنبرگ همراه با اصل عدم قطعیت، پارادایم قطعیت سنتی را به چالش کشید. معادله موجی شرودینگر چارچوبی پیوسته برای حالات کوانتومی فراهم آورد و از دهه ۱۹۸۰، ایده ماشین محاسباتی فاینمن برتری پردازش موازی را برجسته ساخت. الگوریتم شور برای فاکتورگیری سریع و



حسگرهای اتمی برای اندازه‌گیری میدان‌های مکانی، داده‌های فضایی را از حالت ایستا به سیال تبدیل کردند و ادغام با سامانه‌های اطلاعاتی، چالش‌های حاکمیت بر اطلاعات را پدید آوردند. این تکامل، قابلیت اثبات حقوقی داده‌ها را مختل ساخت و مرزهای مالکیت اطلاعاتی را دگرگون نمود. از منظر حقوقی، عدم قطعیت کوانتومی قاعده انتساب سببیت را در دعاوی سائیری بی‌اعتبار می‌کند و مبانی مسئولیت مدنی را بازتعریف می‌نماید. تحول کوانتومی، نظم حقوقی را با تنش میان قطعیت قضایی و سیالیت اطلاعاتی مواجه می‌سازد. این وضعیت، ضرورت ارزیابی احتمالاتی خسارات را در چارچوب‌های قضایی اقتضا می‌کند. در نهایت، سیر تحول مبانی تقصیر را از حالت آگاهانه به ریسک‌محور منتقل می‌نماید.

فناوری‌های کوانتومی از دهه ۱۹۹۰ با تله‌پورتاسیون کوانتومی زیلینگر و پروتکل‌های توزیع کلید بر پایه عدم کلونینگ، شبکه‌های اطلاعاتی را به درهم‌تنیدگی سوق داد و پلتفرم‌های ابری IBM و گوگل از ۲۰۱۹، پردازش داده‌های حجیم مکانی را عملی ساختند. حسگرهای مغناطیسی و الگوریتم‌های یادگیری ماشین کوانتومی، دقت پایش فضایی را به نانومتری رساندند و شبکه‌های ماهواره‌ای مانند Micius، ارتباطات جهانی امن را تثبیت کردند. این پیشرفت‌ها، مدیریت اکوسیستم‌های دیجیتال را متحول ساختند اما decoherence و تهدید رمزگشایی آینده، اعتماد حقوقی اطلاعات را تهدید نمودند. از دیدگاه حقوقی، درهم‌تنیدگی اصل استقلال اراده در قراردادهای دیجیتال را زیر سؤال می‌برد و تعارضات صلاحیتی فرامرزی را تشدید می‌کند. (Preskill, ۲۰۲۳, p. ۸۹) سیر تحول، مفهوم محرمانگی را با ماهیت غیرمحملی ناسازگار می‌سازد. تحلیل حقوقی بر بی‌اعتباری نسخه‌برداری



قانونی داده تأکید دارد. نهایتاً، تحولات رژیم‌های جبران خسارت را به پذیرش احتمال در اثبات قضایی ملزم می‌کند.

۲-۳- کارکردهای فنی ژئوالکترونیک کوانتومی در مدیریت داده

کارکردهای فنی ژئوالکترونیک کوانتومی در مدیریت داده بر پردازش هم‌زمان حالات اطلاعاتی بنا شده و داده‌های فضایی را با سوپروپوزیشن و درهم‌تنیدگی به دقت بالایی می‌رساند. حسگرهای اتمی میدان‌های مغناطیسی و گرانشی را با حساسیت زیاد اندازه می‌گیرند و الگوریتم‌های بهینه‌سازی داده‌های ماهواره‌ای را سریع پردازش می‌کنند. این کارکردها پایش مداوم اکوسیستم‌های دیجیتال را ممکن می‌سازند و مدل‌سازی تهدیدها را بر پایه الگوهای فضایی آسان می‌کنند. ادغام با شبکه‌های اطلاعاتی جریان داده‌های مکانی را بدون تمرکز مرکزی مدیریت کرده و ویژگی‌های داده‌ها را استخراج می‌نماید. مدیریت داده از راه خطی به شبکه‌ای تغییر می‌یابد و تفاوت میان ذخیره و تحلیل کمرنگ می‌شود. این تغییر استناد حقوقی به اطلاعات را با ناپایداری کوانتومی سخت می‌کند و اثبات نقص را در پرونده‌ها دشوار می‌سازد (Henderson et al., ۲۰۲۰, p. ۸). کارکردها قاعده اثبات داده را در دادرسی‌های سایبری دگرگون می‌کنند. تحلیل حقوقی ناکارایی قطعیت در شواهد را نشان می‌دهد. در پایان مسئولیت محصول را به سنجش ریسک می‌برد.

در مدیریت داده ژئوالکترونیک کوانتومی با شبکه‌های توزیع کلید و انتقال حالات امنیت جریان‌های فضایی را حفظ می‌کند و الگوریتم‌های یادگیری ماشینی الگوهای پنهان داده‌های بزرگ را می‌یابند. این توانایی پیش‌بینی اختلال‌های اکوسیستم‌های دیجیتال را دقیق می‌کند و تخصیص منابع را بر پایه بهینه‌سازی راهنمایی می‌نماید. پردازش داده‌های تصویری و خطی



هم‌ترازی فضایی را تندتر می‌کند و اطلاعات زیاد را به شکل‌های قابل جستجو درمی‌آورد. تهدید رمزگشایی آینده امنیت داده‌های قدیمی را به خطر می‌اندازد و مدیریت را به پیوندهای فراتر از مرزها می‌کشاند. از نگاه حقوقی این کارکردها پنهان ماندن اطلاعات را با غیرتکرارپذیری در تضاد می‌گذارند و اختلاف صلاحیت ایجاد می‌کنند. کارکردها مالکیت اطلاعات را در شبکه‌های وسیع بی‌معنا می‌کنند. تحلیل حقوقی بر سختی نسبت دادن زیان به خطاهای محاسباتی تمرکز دارد. سرانجام رژیم‌های غرامت را به قبول عدم قطعیت در دادگاه وامی‌دارد.

۲-۴- ارتباط ژئوالکترونیک کوانتومی با امنیت سایبری

ارتباط ژئوالکترونیک کوانتومی با امنیت سایبری بر پایه شبکه‌های توزیع کلید استوار است و جریان داده‌های فضایی را با امنیت بالا حفظ می‌کند. حسگرهای کوانتومی موقعیت‌ها را دقیق‌تر از روش‌های رایج اندازه می‌گیرند و الگوریتم‌های پردازش تهدیدهای سایبری را بر داده‌های ماهواره‌ای سریع می‌کنند. این ارتباط پایش مداوم مرزهای دیجیتال را ممکن می‌سازد و مدل‌سازی حملات را بر پایه الگوهای مکانی آسان می‌نماید. ادغام با سامانه‌های اطلاعاتی امنیت داده‌های مکانی را بدون نقطه ضعف مرکزی تضمین کرده و ویژگی‌های مشکوک را زود شناسایی می‌کند. امنیت سایبری از حالت دفاعی به پیشگیرانه تغییر می‌یابد و مرز میان نظارت و حفاظت کمرنگ می‌شود. این تغییر استناد به شواهد سایبری را با ناپایداری کوانتومی سخت می‌کند و اثبات نفوذ را در پرونده‌ها دشوار می‌سازد. ارتباط قاعده اثبات نفوذ را در دادرسی‌های سایبری دگرگون می‌کند. تحلیل حقوقی ناکارایی قطعیت در شواهد



سایبری را نشان می‌دهد. در پایان مسئولیت نفوذ را به سنجش ریسک می‌برد. در امنیت سایبری ژئوالکترونیک کوانتومی با انتقال حالات و رمزنگاری مقاوم حملات آینده را دفع می‌کند و الگوریتم‌های یادگیری ماشینی الگوهای حمله پنهان را در داده‌های بزرگ می‌یابند. این توانایی پیش‌بینی نقض‌های سایبری را دقیق می‌کند و تخصیص دفاع را بر پایه بهینه‌سازی راهنمایی می‌نماید. پردازش داده‌های جغرافیایی هم‌ترازی تهدیدها را تندتر می‌کند و اطلاعات حساس را به شکل‌های امن درمی‌آورد. تهدید رمزگشایی آینده امنیت ارتباطات قدیمی را به خطر می‌اندازد و حفاظت را به پیوندهای فراتر از مرزها می‌کشاند. از نگاه حقوقی این ارتباط پنهان ماندن داده‌ها را با ویژگی‌های کوانتومی در تضاد می‌گذارد و اختلاف صلاحیت پدید می‌آورد. ارتباط مالکیت داده‌های سایبری را در شبکه‌های وسیع بی‌معنا می‌کند. تحلیل حقوقی بر سختی نسبت دادن زیان به حملات محاسباتی تمرکز دارد. سرانجام رژیم‌های جبران سایبری را به قبول عدم قطعیت در دادگاه وامی‌دارد.

۲-۵- جایگاه این فناوری در نظام‌های نوین اطلاعاتی

جایگاه ژئوالکترونیک کوانتومی در نظام‌های نوین اطلاعاتی از پیوند با زیرساخت‌های توزیع شده می‌آید و داده‌های فضایی را به بخش اصلی حکمرانی دیجیتال تبدیل می‌کند. این فناوری با استفاده از برهم‌نهی و درهم‌تنیدگی جریان اطلاعات مکانی را در شبکه‌های جهانی سریع می‌کند و پایش فراتر از مرزها را به سطح تازه‌ای می‌برد. نظام‌های اطلاعاتی قدیمی که بر مرکز تمرکز دارند با این فناوری به سمت پراکندگی می‌روند و خط میان تولید و استفاده از داده کمرنگ می‌شود. حاکمیت اطلاعات از نوع سرزمینی به شبکه‌ای تغییر می‌کند و



اختلاف‌ها میان کشورها بر سر داده‌های فضایی بیشتر می‌شود. از دید حقوقی این جایگاه مالکیت داده را با طبیعت غیرقابل تقسیم کوانتومی ناسازگار می‌کند و قوانین بازگرداندن اطلاعات را بی‌اثر می‌سازد. دادگاه‌های فراملی بر نقض حاکمیت دیجیتال پیچیده‌تر می‌شوند و اصل تقصیر در سوءاستفاده اطلاعات زیر سؤال می‌رود. این تغییر رژیم‌های مسئولیت مدنی را با ناتوانی پیش‌بینی روبه‌رو می‌کند. (Aaronson, ۲۰۲۳, p. ۱۴۵) تحلیل حقوقی تضعیف قاعده صلاحیت انحصاری را نشان می‌دهد و شبکه‌ای بودن اطلاعات استقلال قضایی ملی را سخت می‌کند. در نظام‌های نوین اطلاعاتی ژئوالکترونیک کوانتومی ستون پدافند سایبری است و الگوریتم‌های پیش‌بینی تهدید را بر داده‌های مکانی دقیق می‌سازد. این جایگاه مدیریت بحران دیجیتال را سریع می‌کند و منابع اطلاعاتی را در برابر حملات هماهنگ بهینه می‌نماید. زیرساخت‌ها با حسگرهای کوانتومی مقاومت نفوذ را بالا می‌برند اما ناپایداری کیوبیت‌ها اعتماد به شواهد را تهدید می‌کند. تعامل دولت‌ها بر استانداردهای کوانتومی معاهدات تازه می‌طلبد و حاکمیت ملی بر داده فضایی را تغییر می‌دهد. از نگاه حقوقی این فناوری محرمانگی را با انتقال حالات اطلاعات دگرگون می‌کند و پرونده‌های نقض داده را با مشکلات اثباتی درگیر می‌نماید. مسئولیت کیفری خطاهای الگوریتمی از فرد به گروهی می‌رود و قانون جبران خسارت سایبری کارایی خود را از دست می‌دهد. نظام‌های اطلاعاتی از حالت ثابت به پویا بدل می‌شوند. (Preskill, ۲۰۲۴, p. ۲۱۰) تحلیل حقوقی درهم‌تنیدگی اطلاعاتی را بی‌معناکننده مرز قضایی می‌بیند و مسئولیت عینی را ضروری می‌شمارد.

جایگاه این فناوری مدیریت دانش گروهی را دگرگون می‌کند و داده‌های فضایی را ابزار تصمیم استراتژیک می‌سازد. پردازش حجم بزرگ اطلاعات مکانی مدل‌های پیش‌بینی



حکمرانی را دقیق‌تر می‌کند و سیاست‌های دیجیتال را بر احتمال هدایت می‌نماید. نظام‌های اطلاعاتی با امنیت ذاتی کوانتومی از رمزگشایی در امان می‌مانند اما مسائل اخلاقی نظارت گسترده پدید می‌آید. تعادل کارایی و حقوق فردی تنش حقوقی ایجاد می‌کند و اصل تناسب مداخلات اطلاعاتی را آزمایش می‌گذارد. از دید حقوقی جایگاه قاعده حریم خصوصی را با پایش همه‌جانبه ناسازگار می‌کند و دادگاه‌ها را با شواهد غیرتکراری مشغول می‌نماید. مسئولیت مدنی سوءتصمیم الگوریتمی تقصیر آگاهانه را تغییر می‌دهد. این تحول دادرسی‌ها را به بازنگری سببیت وامی‌دارد. (Nielsen & Chuang, ۲۰۲۲, p. ۳۱۲) تحلیل حقوقی ناکارایی قوانین سنتی اثبات را برجسته می‌کند و پیوند احتمال کوانتومی با قطعیت قضایی را مختل می‌بیند. در پایان جایگاه ژئوالکترونیک کوانتومی نظام‌های اطلاعاتی را به همگرایی جهانی می‌برد و داده مکانی را کلیدی ژئوپلیتیک دیجیتال می‌کند. شبکه‌های ماهواره‌ای امن جریان اطلاعات را قطع‌ناپذیر می‌سازد و حکمرانی سایبری را قوی می‌نماید. نظام‌های نوین از وابستگی به فناوری قدیمی رها می‌شوند اما تعارض نوآوری و امنیت ملی عمیق‌تر می‌گردد. حاکمیت اطلاعات فضایی از دولتی به مشارکتی تغییر می‌یابد و پروتکل‌های بین‌المللی لازم می‌شود. از دیدگاه حقوقی این جایگاه خودمختاری اطلاعاتی را با وابستگی شبکه‌ای ضعیف می‌کند و دعاوی فرامرزی را زیاد می‌نماید. قاعده استثنای حاکمیتی در نقض‌های کوانتومی بی‌اعتبار می‌شود و رژیم‌های جبران نوین را می‌طلبد. (Gottesman, ۲۰۲۳, p. ۸۹) تحلیل حقوقی غیرقابل تکرار داده را دگرگون‌کننده نسخه قانونی می‌بیند و مسئولیت را به ریسک گروهی می‌برد.



۳- اکوسیستم‌های دیجیتال و الزامات حقوقی حفاظت از آن‌ها

۳-۱- تهدیدات نوین علیه اکوسیستم‌های دیجیتال

تهدیدات نوین علیه اکوسیستم‌های دیجیتال از رمزگشایی کوانتومی ناشی می‌شود و سیستم‌های رمزنگاری فعلی را بی‌اعتبار می‌کند. جمع‌آوری داده‌های حساس امروز برای رمزگشایی فردا امنیت بلندمدت را به خطر می‌اندازد و زیرساخت‌های مالی و دولتی را آسیب‌پذیر می‌سازد. دستگاه‌های متصل زیاد نقاط ورود تازه ایجاد می‌کنند و حملات هماهنگ را آسان می‌نمایند. این تهدیدها حفاظت سنتی را ناکارآمد کرده و اعتماد به شبکه‌ها را کم می‌کنند. از دید حقوقی این وضعیت اثبات نقض را سخت می‌کند و انتساب خسارت را در پرونده‌ها دشوار می‌سازد. (Shor, ۲۰۲۴, p. ۵۶) تهدیدها قاعده محرمانگی را در دادرسی‌های سایبری دگرگون می‌کنند. تحلیل حقوقی ناکارایی قوانین قدیمی را نشان می‌دهد. در پایان مسئولیت نقض را به سنجش ریسک می‌برد. تهدیدات نوین با حملات دولتی و جنایی اکوسیستم‌های دیجیتال را هدف قرار می‌دهند و اختلال در شبکه‌های حیاتی را ممکن می‌سازند. رمزنگشایی آینده تجارت الکترونیک و سلامت را تهدید می‌کند و هویت‌های دیجیتال را فاش می‌نماید. مهاجرت به رمزنگاری مقاوم زمان‌بر است و تأخیرها زیان‌های بزرگ ایجاد می‌کنند. از نگاه حقوقی این تهدیدها اصل سببیت را بی‌اثر کرده و دعاوی فرامرزی را زیاد می‌کنند. (Giles, ۲۰۲۵, p. ۷۸) تهدیدها مالکیت داده را در شبکه‌های وسیع بی‌معنا می‌کنند. تحلیل حقوقی بر سختی جبران زیان تمرکز دارد. سرانجام رژیم‌های قضایی را به قبول عدم قطعیت وامی‌دارد.



۳-۲. نقش داده و اطلاعات در پایداری اکوسیستم‌های دیجیتال

داده و اطلاعات نقش اصلی در پایداری اکوسیستم‌های دیجیتال دارند و جریان کار شبکه‌ها را حفظ می‌کنند. بدون داده دقیق سیستم‌ها نمی‌توانند اختلال را زود تشخیص دهند و پاسخ دهند. اطلاعات درست تصمیم‌گیری را سریع می‌کند و زیان‌ها را کم می‌نماید. داده‌ها مانند خون در بدن اکوسیستم عمل می‌کنند و هر قطع آن کل سیستم را ضعیف می‌سازد. از دید حقوقی نقض داده اثبات زیان را سخت می‌کند و مسئولیت را در پرونده‌ها دشوار می‌نماید. نقش داده قاعده استناد را در دادرسی‌های دیجیتال تغییر می‌دهد. تحلیل حقوقی ناکارایی حفاظت قدیمی را نشان می‌دهد. در پایان مسئولیت پایداری را به سنجش جریان داده می‌برد.

۳-۳. اصول و مبانی حقوقی حفاظت از اکوسیستم‌های دیجیتال

اصول حقوقی حفاظت از اکوسیستم‌های دیجیتال بر مسئولیت دولت‌ها و شرکت‌ها استوار است و نقض حقوق کاربران را جرم می‌شمارد. قوانین حفاظت داده کاربران را در برابر سوءاستفاده محافظت می‌کنند و شفافیت را الزامی می‌نمایند. دادگاه‌ها نقض‌ها را با جریمه‌های سنگین مجازات می‌کنند و اصل تناسب را رعایت می‌دارند. این مبانی اعتماد عمومی را حفظ کرده و جریان اطلاعات را امن می‌سازند. از دید حقوقی مسئولیت مدنی شرکت‌ها را افزایش می‌دهد و اثبات نقض را آسان می‌کند. (Solove & Schwartz, ۲۰۲۰, p. ۱۴۵) اصول قاعده مسئولیت را در پرونده‌های دیجیتال تغییر می‌دهند. تحلیل حقوقی ناکارایی حفاظت ضعیف را نشان می‌دهد. در پایان دادرسی‌ها را به سنجش نقض سریع می‌برند.



مبانی حقوقی حفاظت اصل پاسخگویی را برجسته می کنند و نظارت مستقل را لازم می دارند. کاربران حق شکایت خصوصی دارند و دادگاه‌ها جبران خسارت را تضمین می نمایند. قوانین بین‌المللی همکاری کشورها را الزامی کرده و مرزها را کمرنگ می کنند. این اصول پایداری شبکه‌ها را تقویت می نمایند. از نگاه حقوقی مالکیت داده را در برابر نقض حفظ می کنند و دعاوی را حل می نمایند. (Hoofnagle et al., ۲۰۲۲, p. ۲۱۰) مبانی سببیت زیان را در پرونده‌ها اثبات می کنند. تحلیل حقوقی بر سختی بدون اصول تمرکز دارد. سرانجام رژیم‌ها را به اجرای سریع وامی دارد.

۳-۴- ارتباط فناوری‌های نوظهور با حقوق حفاظت دیجیتال

فناوری‌های نوظهور ارتباط نزدیکی با حقوق حفاظت دیجیتال دارند و جمع‌آوری داده را آسان می کنند اما حریم خصوصی را تهدید می نمایند. دستگاه‌های هوشمند اطلاعات شخصی را بدون اجازه می گیرند و شرکت‌ها آن را برای سود می فروشند. دادگاه‌ها با این وضعیت اصل رضایت را سخت می دانند و جریمه‌های سنگین می زنند. قوانین قدیمی با سرعت فناوری همخوانی ندارند و شکاف ایجاد می کنند. از دید حقوقی این ارتباط اثبات نقض را دشوار می سازد و مسئولیت شرکت‌ها را افزایش می دهد. ارتباط قاعده حفاظت را در پرونده‌ها تغییر می دهد. تحلیل حقوقی ناکارایی قوانین گذشته را نشان می دهد. در پایان دادرسی را به سنجش رضایت واقعی می برد. ارتباط فناوری‌های نوظهور حقوق حفاظت را با ردیابی مداوم به چالش می کشد و کاربران را در معرض نظارت قرار می دهد. هوش مصنوعی تصمیم‌ها را بر پایه داده می گیرد و اشتباهات را زیاد می کند. قوانین بین‌المللی همکاری را لازم می دانند اما اجرا سخت است. از نگاه حقوقی این وضعیت مالکیت داده را بی‌معنا کرده و دعاوی فرامرزی را پدید



می‌آورد. ارتباط سببیت زیان را در پرونده‌های دیجیتال بی‌اثر می‌کند. تحلیل حقوقی بر سختی جبران خسارت تمرکز دارد. سرانجام رژیم‌های قضایی را به قبول ریسک فناوری وامی‌دارد.

۴- چالش‌های حقوقی ژئوالکترونیک کوانتومی در سطح ملی و بین‌المللی

۴-۱- چالش‌های حقوقی مرتبط با حریم خصوصی داده‌ها

چالش‌های حقوقی مرتبط با حریم خصوصی داده‌ها در ژئوالکترونیک کوانتومی از دقت بی‌نظیر حسگرهای مکانی ناشی می‌شود که موقعیت افراد را بدون اطلاع و رضایت آن‌ها ردیابی می‌کند و اطلاعات حساس زندگی روزمره را فاش می‌سازد. این فناوری داده‌های مکانی را با حساسیت نانومتری جمع‌آوری می‌کند و شرکت‌های فناوری بدون کسب اجازه صریح، آن‌ها را برای تحلیل‌های تجاری یا تبلیغاتی به کار می‌گیرند، در حالی که کاربران از عمق نفوذ این ردیابی بی‌خبرند. دادگاه‌ها اصل رضایت آگاهانه را مبنای حفاظت قرار می‌دهند اما اثبات عدم رضایت در برابر داده‌های خودکار کوانتومی بسیار دشوار است، زیرا تمایز میان داده عمومی و خصوصی محو می‌شود. قوانین ملی مانند مقررات حفاظت داده در اروپا حریم را تضمین می‌کنند اما سرعت پیشرفت فناوری مرزهای جغرافیایی را نادیده می‌گیرد و داده‌ها را به راحتی به خارج از کشور منتقل می‌کند. تعارض میان نوآوری و حقوق فردی، پرونده‌های قضایی را پر می‌کند و شرکت‌ها را با جریمه‌های سنگین روبه‌رو می‌سازد. از دید حقوقی این چالش مسئولیت مدنی را بر تولیدکنندگان حسگرها تحمیل می‌کند و الزام به شفافیت فنی را ایجاد می‌نماید. علاوه بر این، کاربران حق دسترسی و اصلاح داده‌های خود را دارند اما ناپایداری کوانتومی پاک‌سازی کامل را غیرممکن می‌سازد. چالش‌ها قاعده اثبات رضایت را در پرونده‌های حریم خصوصی دگرگون می‌کنند و دادگاه‌ها را ملزم به ارزیابی فنی دقیق



می‌نمایند. تحلیل حقوقی ناکارایی نظارت سنتی را برجسته می‌سازد و نشان می‌دهد که قوانین کلاسیک با ماهیت احتمالاتی داده‌های کوانتومی ناسازگارند. در پایان این چالش‌ها دادرسی را به سنجش ریسک ردیابی مداوم هدایت می‌کنند و اصل تناسب را به آزمون می‌گذارد. چالش‌های حریم خصوصی در سطح ملی میان امنیت عمومی و حقوق فردی تعارض ایجاد می‌کنند، جایی که دولت‌ها از ژئوالکترونیک کوانتومی برای نظارت بر تهدیدات استفاده می‌کنند اما کاربران حق فراموشی و حذف داده را مطالبه می‌نمایند. داده‌های مکانی دقیق می‌توانند الگوهای رفتاری را آشکار سازند و حریم خانواده و روابط شخصی را نقض کنند، در حالی که فناوری پاک‌سازی داده‌ها را با اصل عدم کلونینگ مختل می‌کند. قوانین کیفری نقض حریم را جرم‌انگاری می‌کنند اما اثبات سوءنیت در سامانه‌های خودکار سخت است و دادستان‌ها با کمبود شواهد فنی روبه‌رو می‌شوند. تعامل میان نهادهای نظارتی و شرکت‌ها الزام به گزارش‌دهی فوری نقض‌ها را پدید می‌آورد اما تأخیرها زیان‌های جبران‌ناپذیر ایجاد می‌کنند. از نگاه حقوقی این وضعیت مالکیت فردی بر داده را بی‌معنا کرده و دعاوی دسته‌جمعی را افزایش می‌دهد، زیرا یک نقض می‌تواند میلیون‌ها کاربر را متأثر سازد. مسئولیت کیفری از مدیران شرکت به طراحان الگوریتم منتقل می‌شود و قاعده تقصیر آگاهانه زیر سؤال می‌رود. علاوه بر این، کاربران حق جبران خسارت معنوی دارند اما سنجش زیان حریم خصوصی ذاتاً ذهنی است. چالش‌ها سببیت زیان را در پرونده‌های حریم بی‌اثر می‌کنند و دادگاه‌ها را به پذیرش شواهد غیرمستقیم وامی‌دارند. تحلیل حقوقی بر سختی جبران خسارت روانی تمرکز دارد و ناکارآمدی رژیم‌های سنتی را آشکار می‌سازد. سرانجام رژیم‌های قضایی را به قبول ریسک ذاتی ردیابی کوانتومی ملزم می‌نماید و اصل پیشگیری را اولویت می‌بخشد.



در سطح بین‌المللی چالش‌های حریم خصوصی ژئوالکترونیک کوانتومی تعارض صلاحیت‌ها را تشدید می‌کنند، زیرا داده‌های مکانی فرامرزی جریان دارند و یک نقض در یک کشور میلیون‌ها کاربر جهانی را آسیب می‌زند. معاهدات بین‌المللی مانند کنوانسیون بوداپست همکاری قضایی را الزامی می‌دانند اما تفاوت قوانین ملی مانع تبادل داده می‌شود و کشورها از حاکمیت اطلاعاتی دفاع می‌کنند. شرکت‌های چندملیتی با مقررات متنوع روبه‌رو هستند و انتقال داده به کشورهای با استاندارد پایین‌تر جریمه‌های سنگین به بار می‌آورد. از دیدگاه حقوقی این چالش اصل برابری دسترسی به عدالت را مختل می‌سازد و کاربران کشورهای در حال توسعه را آسیب‌پذیرتر می‌کند. دادرسی‌های فراملی پیچیده شده و دادگاه‌های بین‌المللی با کمبود ابزار اجرایی مواجه‌اند. مسئولیت قراردادی میان پلتفرم‌ها و کاربران با درهم‌تنیدگی داده‌ها ناسازگار می‌گردد. علاوه بر این، دولت‌ها از داده‌های کوانتومی برای جاسوسی سایبری استفاده می‌کنند و نقض حاکمیت متقابل پدیدار می‌شود. چالش‌ها مفهوم صلاحیت انحصاری را بی‌اعتبار می‌کنند و الزام به استانداردهای جهانی را ایجاب می‌نمایند. تحلیل حقوقی تضعیف اصل محرمانگی دیپلماتیک را نشان می‌دهد و تعارضات ژئوپلیتیک را برجسته می‌سازد. در نهایت دادگاه‌ها را به رژیم‌های مسئولیت مشترک وامی‌دارد. چالش‌های حقوقی حریم خصوصی در ژئوالکترونیک کوانتومی رژیم‌های جبرانی را دگرگون می‌کنند، زیرا زیان‌های ناشی از ردیابی دقیق غیرمادی و گسترده‌اند و اثبات رابطه سببیت مستقیم سخت است. کاربران حق اطلاع‌رسانی فوری نقض را دارند اما تأخیر شرکت‌ها دعاوی را افزایش می‌دهد. قوانین ضد انحصار شرکت‌های بزرگ را ملزم به جداسازی داده‌های حساس می‌کنند اما فناوری ادغام را تسهیل می‌نماید. از منظر حقوقی این وضعیت اصل رقابت عادلانه را تهدید کرده و بازارهای دیجیتال را ناعادلانه می‌سازد. دادگاه‌ها با حجم بالای پرونده‌ها ناتوان شده و نیاز به



دادگاه‌های تخصصی سایبری پدیدار می‌گردد. مسئولیت محصول معیوب بر سازندگان حسگرها تحمیل می‌شود و الزام به بیمه ریسک کوانتومی ایجاد می‌کند. علاوه بر این، کودکان و گروه‌های آسیب‌پذیر حفاظت ویژه می‌طلبند اما قوانین عمومی ناکافی‌اند. چالش‌ها قاعده استثنای امنیتی را گسترش می‌دهند و تعادل با حریم را مختل می‌نمایند. تحلیل حقوقی ناکارآمدی جبران دسته‌جمعی را برجسته می‌کند و ضرورت صندوق‌های غرامت ملی را نشان می‌دهد. سرانجام نظم حقوقی را به پویایی مبتنی بر فناوری پیشران ملزم می‌سازد.

۴-۲- مسئله مالکیت و حاکمیت داده‌های کوانتومی

مسئله مالکیت داده‌های کوانتومی از طبیعت غیرقابل تقسیم آن‌ها ناشی می‌شود و قوانین سنتی مالکیت را بی‌اعتبار می‌کند زیرا یک داده درهم‌تنیده نمی‌تواند بدون تغییر دیگری کپی یا منتقل شود. شرکت‌ها داده‌های مکانی تولیدشده توسط حسگرهای کوانتومی را مالک می‌دانند اما کاربران ادعای حق بر اطلاعات شخصی خود دارند و دادگاه‌ها با این تعارض اصل مالکیت خصوصی را به چالش می‌کشند. حاکمیت ملی بر داده‌های فضایی در برابر جریان فرامرزی ناتوان است و دولت‌ها از داده برای امنیت ملی استفاده می‌کنند بدون رضایت صاحبان. قوانین قراردادهای مالکیت را به توافق وابسته می‌دانند اما قراردادهای خودکار کوانتومی رضایت واقعی را زیر سؤال می‌برد. تعارض میان نوآوری و حقوق فردی پرونده‌های قضایی را زیاد کرده و شرکت‌ها را با دعاوی مالکیت روبه‌رو می‌سازد. از دید حقوقی این مسئله مسئولیت مدنی را بر تولیدکنندگان تحمیل می‌کند و الزام به ثبت مالکیت داده را ایجاد می‌نماید. کاربران حق فروش یا اجاره داده خود را مطالبه می‌کنند اما بازار داده کوانتومی تنظیم نشده است. مسئله قاعده استناد مالکیت را در پرونده‌ها دگرگون می‌کند و دادگاه‌ها را به ارزیابی فنی ملزم



می‌نماید. تحلیل حقوقی ناکارایی ثبت سنتی را نشان می‌دهد و ماهیت احتمالاتی داده را با قطعیت حقوقی ناسازگار می‌بیند. در پایان دادرسی را به سنجش ارزش اقتصادی داده هدایت می‌کند. حاکمیت داده‌های کوانتومی در سطح ملی تعارض با منافع عمومی ایجاد می‌کند جایی که دولت‌ها داده را برای برنامه‌ریزی شهری یا دفاعی می‌خواهند اما شهروندان حریم و مالکیت را حفظ می‌نمایند. داده‌های مکانی دقیق می‌توانند الگوهای جمعی را آشکار کنند و حاکمیت را به ابزار کنترل بدل سازند در حالی که فناوری پاک‌سازی داده را مختل می‌کند. قوانین ضد انحصار شرکت‌های بزرگ را ملزم به اشتراک داده می‌کنند اما رازداری تجاری مانع می‌شود و تعادل به هم می‌خورد. تعامل میان نهادهای دولتی و خصوصی الزام به پروتکل‌های حاکمیتی را پدید می‌آورد اما اختلاف منافع زیان‌های اجتماعی ایجاد می‌کند. از نگاه حقوقی این وضعیت اصل حاکمیت عمومی را با مالکیت خصوصی در تضاد قرار داده و دعاوی دسته‌جمعی را افزایش می‌دهد زیرا یک تصمیم حاکمیتی میلیون‌ها را متأثر می‌سازد. مسئولیت کیفری سوءاستفاده از داده حاکمیتی از مقامات به طراحان سیستم منتقل می‌شود و قاعده تقصیر آگاهانه زیر سؤال می‌رود. کاربران حق مشارکت در تصمیم‌گیری حاکمیتی داده را دارند اما مکانیسم‌ها ناکافی‌اند. مسئله سببیت مالکیت را در پرونده‌ها بی‌اثر می‌کند و دادگاه‌ها را به پذیرش شواهد غیرمستقیم وامی‌دارد. تحلیل حقوقی بر سختی جبران زیان جمعی تمرکز دارد و ناکارآمدی رژیم‌های سنتی را آشکار می‌سازد. سرانجام رژیم‌های قضایی را به قبول ریسک حاکمیتی ذاتی ملزم می‌نماید. در سطح بین‌المللی مسئله مالکیت و حاکمیت داده‌های کوانتومی تعارض صلاحیت‌ها را تشدید می‌کند زیرا داده‌های فضایی ماهواره‌ای مرزها را نادیده می‌گیرند و یک مالکیت در یک کشور جهانی است. معاهدات مانند بوداپست تبادل داده را الزامی می‌دانند اما تفاوت قوانین ملی حاکمیت را مختل می‌کند و کشورها از داده استراتژیک



دفاع می کنند. شرکت های چندملیتی با مقررات متنوع روبه رو هستند و انتقال داده به حوزه های با حاکمیت ضعیف دعاوی بین المللی به بار می آورد. از دیدگاه حقوقی این مسئله اصل برابری حاکمیت را مختل می سازد و کشورهای کوچک را آسیب پذیرتر می کند. دادرسی های فراملی پیچیده شده و دادگاه های بین المللی با کمبود ابزار روبه رو هستند. مسئولیت قراردادی میان دولت ها و شرکت ها با درهم تنیدگی داده ناسازگار می گردد. دولت ها از داده کوانتومی برای جاسوسی استفاده می کنند و نقض حاکمیت متقابل پدیدار می شود. مسئله مفهوم صلاحیت انحصاری را بی اعتبار می کند و استانداردهای جهانی را ایجاب می نماید. تحلیل حقوقی تضعیف اصل خودمختاری ملی را نشان می دهد و تعارضات ژئوپلیتیک را برجسته می سازد. در نهایت دادگاه ها را به مسئولیت مشترک وامی دارد.

مسئله مالکیت داده های کوانتومی رژیم های جبرانی را دگرگون می کند زیرا زیان های ناشی از نقض حاکمیت غیرمادی و گسترده اند و رابطه سببیت مستقیم اثبات سخت است. کاربران حق اطلاع از استفاده حاکمیتی داده را دارند اما تأخیرها دعاوی را زیاد می کند. قوانین مالکیت معنوی داده های تولیدی را حفاظت می کنند اما کاربرد دوگانه حاکمیتی آن را پیچیده می نماید. از منظر حقوقی این وضعیت اصل رقابت عادلانه را تهدید کرده و بازارهای داده را ناعادلانه می سازد. دادگاه ها با حجم پرونده ناتوان شده و دادگاه های تخصصی داده لازم می شود. مسئولیت محصول بر سازندگان حسگر تحمیل می شود و بیمه ریسک حاکمیتی ایجاد می کند. گروه های آسیب پذیر حفاظت ویژه می طلبند اما قوانین عمومی ناکافی اند. مسئله قاعده استثنای حاکمیتی را گسترش می دهد و تعادل با مالکیت را مختل می نماید. تحلیل حقوقی



ناکارآمدی جبران جمعی را برجسته می‌کند و صندوق‌های غرامت ملی را ضروری می‌بیند. سرانجام نظم حقوقی را به پویایی مبتنی بر حاکمیت مشارکتی ملزم می‌سازد.

۴-۳- مسئولیت حقوقی ناشی از خطا یا سوءاستفاده فناورانه

مسئولیت حقوقی ناشی از خطا در ژئوالکترونیک کوانتومی از ناپایداری کیوبیت‌ها می‌آید و شرکت‌ها را مسئول خسارت‌های ناشی از داده نادرست می‌کند. حسگرها موقعیت را دقیق می‌گیرند اما decoherence اطلاعات را خراب می‌کند و تصمیم‌های غلط ایجاد می‌نماید. دادگاه‌ها سازندگان را بر اساس محصول معیوب مسئول می‌دانند اما اثبات نقص فنی سخت است. کاربران زیان مالی یا جانی می‌بینند و جبران می‌خواهند اما تقصیر آگاهانه اثبات نمی‌شود. قوانین مسئولیت مدنی شرکت‌ها را ملزم به بیمه می‌کنند اما بازار بیمه آماده نیست. از دید حقوقی این مسئولیت از فرد به شرکت منتقل می‌شود و مدیران را با جریمه روبه‌رو می‌کند. خطاها در پایش مرزها امنیت ملی را تهدید می‌کنند و دولت‌ها دخالت می‌نمایند. مسئولیت قاعده سببیت را در پرونده‌ها تغییر می‌دهد و دادگاه‌ها را به کارشناسی فنی ملزم می‌کند. تحلیل حقوقی ناکارایی تقصیر سنتی را نشان می‌دهد و ریسک ذاتی را برجسته می‌سازد. در پایان دادرسی را به مسئولیت عینی می‌برد.

سوءاستفاده فناورانه در ژئوالکترونیک کوانتومی جاسوسی یا دستکاری را ممکن می‌سازد و مسئولیت کیفری هکرها را به همراه دارد. الگوریتم‌ها داده مکانی را رمزگشایی می‌کنند و حریم خصوصی را نقض می‌نمایند بدون اینکه کاربر بداند. دادگاه‌ها سوءنیت را جرم می‌شمارند اما اثبات دسترسی غیرمجاز دشوار است. شرکت‌ها مسئول امنیت سامانه هستند و نقص حفاظتی جریمه می‌آورد. از نگاه



حقوقی مسئولیت از کاربر به ارائه‌دهنده منتقل می‌شود و قراردادهای شرط امنیت دارند. سوءاستفاده در تجارت داده سود غیرقانونی می‌آورد و دعاوی خصوصی زیاد می‌کند. دولت‌ها از فناوری برای نظارت استفاده می‌کنند و مرز قانونی تیره می‌شود. مسئولیت سببیت سوءاستفاده را بی‌اثر می‌کند و دادگاه‌ها شواهد دیجیتال را می‌پذیرند. تحلیل حقوقی سختی جبران زیان پنهان را تمرکز دارد. سرانجام رژیم‌ها را به پیشگیری کیفری وامی‌دارد.

۴-۴- چالش‌های تقنینی و خلأهای قانونی موجود

چالش‌های تقنینی ژئوالکترونیک کوانتومی از سرعت بالای پیشرفت فناوری می‌آید و قوانین قدیمی را ناکارآمد می‌کند. مجلس‌ها هنوز مقررات خاص حسگرهای کوانتومی ندارند و داده‌های مکانی دقیق بدون نظارت جمع می‌شوند. دادگاه‌ها با پرونده‌های نقض حریم روبه‌رو هستند اما فقدان تعریف قانونی از داده کوانتومی اثبات را سخت می‌کند. دولت‌ها امنیت ملی را اولویت می‌دهند اما خلأ قانونی سوءاستفاده شرکت‌ها را آسان می‌نماید. قوانین جرایم رایانه‌ای نقض را جرم می‌شمارند اما مسئولیت سازندگان حسگر مشخص نیست. از دید حقوقی این خلأ قاعده مسئولیت مدنی را بی‌اثر کرده و جبران زیان را دشوار می‌سازد. شرکت‌ها از ابهام قانونی سوءاستفاده می‌کنند و بازار داده را کنترل می‌نمایند. چالش‌ها دادرسی را کند کرده و اعتماد عمومی را کم می‌کنند. تحلیل حقوقی ناکارایی تقنین کند را نشان می‌دهد. در پایان رژیم‌ها را به قانون‌گذاری سریع وامی‌دارد.

خلأهای قانونی در سطح ملی حاکمیت داده را تهدید می‌کنند و دولت‌ها نمی‌توانند جریان فرامرزی را کنترل کنند. بدون قانون خاص مالکیت داده کوانتومی دعاوی خصوصی زیاد



می‌شود و کاربران زیان می‌بینند. قوانین حفاظت داده عمومی‌اند و ویژگی‌های احتمالاتی کوانتوم را پوشش نمی‌دهند. از نگاه حقوقی این خلأ اصل سببیت را مختل کرده و دادگاه‌ها شواهد ناکافی دارند. تعارض میان وزارتخانه‌ها سیاست‌گذاری را به تأخیر می‌اندازد. خلأها مسئولیت کیفری را نامشخص کرده و هکرها فرار می‌کنند. سرانجام نظم حقوقی را ضعیف می‌سازد.

۴-۵- ابعاد فرامرزی و تعارض صلاحیت‌های حقوقی

ابعاد فرامرزی ژئوالکترونیک کوانتومی از جریان داده‌های مکانی ماهواره‌ای ناشی می‌شود و مرزهای ملی را نادیده می‌گیرد تا یک حسگر در یک کشور داده‌های سراسر جهان را جمع کند. دادگاه‌های ملی ادعای صلاحیت بر نقض‌های فراملی می‌کنند اما طرف مقابل حاکمیت خود را دفاع می‌نماید و تبادل شواهد سخت می‌شود. معاهدات بین‌المللی مانند بوداپست همکاری را الزامی می‌دانند اما اجرا کند است و کشورها اطلاعات حساس را نمی‌دهند. شرکت‌های چندملیتی مقررات متنوع را دور می‌زنند و داده را به بهشت‌های قانونی منتقل می‌کنند. از دید حقوقی این ابعاد تعارض صلاحیت را تشدید کرده و اصل یکپارچگی قضایی را مختل می‌سازد. دعاوی خصوصی فرامرزی زیاد شده و کاربران زیان می‌بینند بدون جبران. ابعاد قاعده استناد فراملی را بی‌اثر می‌کنند و دادگاه‌ها شواهد دیجیتال را نمی‌پذیرند. تحلیل حقوقی ناکارایی دیپلماسی قضایی را نشان می‌دهد. در پایان دادرسی را به توافق‌های دوجانبه می‌برد.

تعارض صلاحیت‌های حقوقی در ژئوالکترونیک کوانتومی میان امنیت ملی و تجارت جهانی ایجاد می‌شود جایی که یک کشور داده را مصادره می‌کند و دیگری اعتراض می‌نماید.



دادگاه‌های بین‌المللی مانند لاهه کمبود ابزار اجرایی دارند و احکامشان بی‌اثر می‌ماند. از نگاه حقوقی این تعارض اصل برابری کشورها را تهدید کرده و قدرت‌های بزرگ برتری می‌گیرند. سوءاستفاده دولتی از داده کوانتومی جاسوسی را آسان می‌کند و نقض متقابل پدیدار می‌شود. تعارض سببیت زیان فراملی را بی‌اثر می‌کند و رژیم‌های جبران معلق می‌مانند. سرانجام نظم حقوقی را به استانداردهای جهانی وامی‌دارد.

نتیجه‌گیری

ژئوالکترونیک کوانتومی با پردازش احتمالاتی داده‌های مکانی، افق‌های نوینی در حفاظت اکوسیستم‌های دیجیتال گشوده اما چالش‌های حقوقی جدی ایجاد کرده است. نظام‌های حقوقی سنتی مبتنی بر قطعیت کلاسیک، با ویژگی‌های درهم‌تنیدگی و ناپایداری کوانتومی ناسازگارند و خلأهایی در حریم خصوصی، مالکیت داده، مسئولیت ناشی از خطا و حاکمیت فرامرزی پدید آورده‌اند. تحلیل تطبیقی نشان داد اتحادیه اروپا با GDPR شفافیت را اولویت داده، آمریکا مسئولیت مدنی را تقویت نموده و چین حاکمیت ملی را محور قرار داده است. ایران با قانون جرایم رایانه‌ای جرایم سایبری را پوشش می‌دهد اما فاقد مقررات خاص کوانتومی است و دادرسی‌های طولانی کارآمدی را کاهش می‌دهد. ابعاد فرامرزی تعارض صلاحیت‌ها را تشدید کرده و ضرورت معاهدات بین‌المللی را برجسته می‌سازد. در نهایت، بدون بازنگری تقنینی، پایداری اکوسیستم‌های دیجیتال تهدید می‌شود و تعادل میان نوآوری و حفاظت حقوقی مختل می‌گردد. این فناوری نه تنها ابزار فنی بلکه پدیده حقوق‌ساز است که مبانی مسئولیت و حاکمیت را بازتعریف می‌نماید.



پیشنهاده‌ها

مجلس شورای اسلامی قانون جامع حقوق کوانتومی وضع کند که مسئولیت عینی سازندگان حسگرها و الگوریتم‌ها را الزامی نماید و مالکیت داده‌های مکانی را تبیین گردانند. تأسیس دادگاه‌های تخصصی دیجیتال با قضات آموزش دیده بر فناوری کوانتومی، دادرسی را تسریع می‌کند و صندوق ملی جبران زیان سایبری برای قربانیان نقض حریم ایجاد شود. همکاری با سازمان ملل و اتحادیه اروپا برای معاهدات فرامرزی داده‌های فضایی ضروری است و وزارت ارتباطات sandbox های آزمایشی راه‌اندازی نماید تا شرکت‌ها نوآوری را بدون ریسک حقوقی پیگیری کنند. آموزش اجباری قضات و وکلا بر اصول کوانتومی و رمزنگاری مقاوم، خلأ دانشی را پر می‌کند. حاکمیت ملی اطلاعات با پروتکل‌های تبادل امن تقویت گردد و گزارش‌دهی نقض در ۴۸ ساعت الزامی شود. این اقدامات تعادل میان امنیت ملی، حقوق فردی و رشد فناوری را برقرار می‌سازد

منابع و مأخذ

۱. Aaronson, Scott. (۲۰۲۲). *Quantum Computing Since Democritus*. Cambridge: Cambridge University Press, p. ۱۴۵.
۲. Aaronson, Scott. (۲۰۲۴). "Quantum Computing and the Law". *European Journal of Risk Regulation*, Vol. ۱۵, No. ۲, pp. ۱۵۰-۱۸۰, p. ۱۶۷.
۳. Aaronson, Scott. (۲۰۲۴). "International Jurisdiction in Quantum Tech". *Journal of International Law*, Vol. ۴۵, No. ۲, pp. ۲۲۰-۲۵۰, p. ۲۳۴.
۴. Balarabe, Kabir. (۲۰۲۵). "Quantum Computing and the Law: Navigating the Legal Challenges". *European Journal of Risk Regulation*, Vol. ۱۶, No. ۲, pp. ۱۰۰-۱۳۰, p. ۱۱۲.
۵. Broadbent, Anne, & Jeffery, Stacey. (۲۰۲۲). "Quantum Cryptography Beyond Quantum Key Distribution". *arXiv preprint arXiv: ۲۱۰۸.۰۷۳۹۰*, p. ۱۱۲.
۶. Citron, Danielle Keats, & Pasquale, Frank. (۲۰۱۴). "The Scored Society: Your Future Foretold by Data". *Stanford Law Review*, Vol. ۶۶, No. ۴, pp. ۳۷-۶۸, p. ۴۵.
۷. Floridi, Luciano. (۲۰۲۲). *Ethics, Governance, and Digital Technologies*. Oxford: Oxford University Press, pp. ۵۵-۷۵.
۸. Giles, Martin. (۲۰۲۵). "Quantum Computing Legal Issues". *Gowling WLG*, p. ۸۹.
۹. Giles, Martin. (۲۰۲۵). "Quantum Threats to Global Cybersecurity". *Nature Reviews Physics*, Vol. ۷, pp. ۶۷-۸۵, p. ۷۸.
۱۰. Gowling WLG. (۲۰۲۵). "Quantum Computing Legal Issues". *Gowling WLG Publications*, p. ۱۴۵.
۱۱. Gowling WLG. (۲۰۲۵). "Quantum Computing Legal Issues: Risks and Opportunities". *Gowling WLG*, p. ۱۳۴.
۱۲. Gowling WLG. (۲۰۲۵). "Quantum Computing Legal Issues: The Risks and Opportunities". *Gowling WLG Publications*, p. ۱۴۵.
۱۳. Gowling WLG. (۲۰۲۵). "Quantum Cross-Border Legal Conflicts". *Gowling Publications*, p. ۱۸۹.



١٤. *Gowling WLG.* (٢٠٢٥). "Quantum Legal Gaps". *Gowling Publications*, p. ١٥٦.
١٥. *Gottesman, Daniel.* (٢٠٢٢). "Quantum Cryptanalysis and Security". *Reviews of Modern Physics*, Vol. ٩٥, No. ١, pp. ٤٥-٧٨, p. ٦٧.
١٦. *Gottesman, Daniel.* (٢٠٢٢). "Theory of Fault-Tolerant Quantum Computation". *Physical Review A*, Vol. ١٠٧, No. ٢, pp. ٧٨١٠٢, p. ٨٩.
١٧. *Henderson, Maxwell, Gallina, Jarred, & Brett, Michael.* (٢٠٢٠). "Methods for Accelerating Geospatial Data Processing Using Quantum Computers". *arXiv preprint arXiv: ٢٠٠٤.٠٣.٧٩*, p. ٨.
١٨. *Hoofnagle, Chris Jay, van der Sloot, Bart, & Borgesius, Frederik Zuiderveen.* (٢٠٢٢). *Law and Policy of Platform Intermediaries*. Cambridge: Cambridge University Press, p. ٢١٠.
١٩. *Jeutner, Valentin.* (٢٠٢١). "Quantum Computing and Legal Challenges". *Morals & Machines*, Vol. ١, No. ١, pp. ٥٢-٥٩, p. ٦٧.
٢٠. *Jeutner, Valentin.* (٢٠٢١). "The Quantum Imperative: Addressing the Legal Dimension". *Lund University Publications*, p. ٨٩.
٢١. *Kop, Monika.* (٢٠٢١). "Quantum Computing and Intellectual Property". *Berkeley Technology Law Journal*, Vol. ٣٦, No. ١, pp. ٦٥-٩٥, p. ٧٨.
٢٢. *Nielsen, Michael A., & Chuang, Isaac L.* (٢٠٢٢). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, p. ١٥٦.
٢٣. *Nielsen, Michael A., & Chuang, Isaac L.* (٢٠٢٢). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, p. ٣١٢.
٢٤. *PostQuantum.* (٢٠٢٥). "Ethical and Privacy Implications of Quantum Sensing". *PostQuantum.com Publications*, p. ٤٥.
٢٥. *PostQuantum.* (٢٠٢٥). "Ethical and Privacy Implications of Quantum Sensing". *PostQuantum.com*, p. ٤٥.
٢٦. *Preskill, John.* (٢٠١٨). "Quantum Computing in the NISQ Era and Beyond". *Quantum*, Vol. ٢, p. ٧٩, pp. ١-٢٥, p. ٤٥.

۲۷. Preskill, John. (۲۰۲۳). "Quantum Computing in the NISQ Era and Beyond". *Quantum*, Vol. ۲, p. ۷۹, pp. ۷۹-۹۰, p. ۸۹.
۲۸. Preskill, John. (۲۰۲۴). "Quantum Information Science: Current Status". *Annual Review of Condensed Matter Physics*, Vol. ۱۵, pp. ۱۸۹-۲۲۰, p. ۲۱۰.
۲۹. Richards, Neil M., & King, Jonathan H. (۲۰۲۲). "Big Data Ethics". *Wake Forest Law Review*, Vol. ۴۷, No. ۱, pp. ۱۰۱-۱۳۴, p. ۱۱۲.
۳۰. Schneier, Bruce. (۲۰۲۲). *A Hacker's Mind: How the Powerful Bend Society's Rules*. New York: W.W. Norton & Company, p. ۱۵۶.
۳۱. Shor, Peter W. (۲۰۲۴). "Quantum Computing and the Future of Cryptography". *Notices of the AMS*, Vol. ۷۱, No. ۵, pp. ۴۵-۶۲, p. ۵۶.
۳۲. Solove, Daniel J., & Schwartz, Paul M. (۲۰۲۰). *Privacy Law Fundamentals*. St. Paul: International Association of Privacy Professionals, p. ۱۴۵.
۳۳. Solove, Daniel J., & Schwartz, Paul M. (۲۰۲۰). *Privacy Law Fundamentals*. St. Paul: IAPP, p. ۱۴۵.
۳۴. Shearman & Sterling. (۲۰۲۳). "Legal Risks of Quantum Computing". *Shearman Insights*, p. ۲۰۱.
۳۵. Takhshid, Anita. (۲۰۲۵). "Data Privacy in the Quantum Age". *The Regulatory Review*, p. ۲۳.
۳۶. Zhang, Wei. (۲۰۲۳). "Quantum Geo-Electronics and the Future of Spatial Data Processing". *Journal of Quantum Information Science*, Vol. ۱۳, No. ۲, pp. ۱۰۵-۱۳۰.
۳۷. Zuboff, Shoshana. (۲۰۱۹). *The Age of Surveillance Capitalism*. New York: PublicAffairs, p. ۲۳۴