رویکردهای حقوقی به تهدیدات سایبری در حیطه مالکیت فکری

افشین جعفری[۱]

علیرضا حجت‌زاده[۲]

محمدتقی رضایی[۳]

چکیده

زمینه و هدف: حقوق مالکیت فکری (معنوی)، یکی از گونه‌های حقوق مالکیت است که به حمایت و استفاده از آفرینش‌های فکری بشر مربوط می‌شود. با توجه به گسترش ارتباطات، فرصت‌ها و تهدیدات ناشی از فضای سایبری همچون حملات و جرائم سایبری، بررسی رویکردهای حقوقی نسبت به تهدیدات سایبری در حیطه مالکیت فکری حائز اهمیت است که در این پژوهش به این موضوع پرداخته می‌شود.

روش: روش پژوهش حاضر، توصیفی ـ تحلیلی از نوع کاربردی و با استفاده از قواعد حقوقی مالکیت فکری در حوزه فضای سایبر و منابع کتابخانه‌ای صورت پذیرفته است.

ملاحظات اخلاقی: در به سامان‌رسیدن این تحقیق ضمن رعایت اصالت متون، صداقت و امانتداری رعایت شده است.

یافته‌ها: کنوانسیون‌ها و معاهدات بین‌المللی، هرچند رویکردهایی عام و حتی نقشه راهی برای مقابله با تهدیدات سایبری شناخته می‌شوند، اما نمی‌توانند به طور خاص مشکلات جوامع دیگر را در حیطه حمایت از مالکیت فکری پوشش دهند. به همین دلیل ارتقای فرهنگ استفاده از فضای سایبر، تعیین مجازات متناسب با نقض مالکیت

۱. دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵. (نویسنده مسؤول)

Email: jafariafshin@yahoo.com

۲. استادیار دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵.

۳. استادیار دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵.

نوع مقاله: پژوهشی **تاریخ دریافت مقاله:** ۱۳۹۳/۱۰/۱۵ **تاریخ پذیرش مقاله:** ۱۳۹۴/۴/۱۵

فکری، جرم تلقی‌نمودن تهدیدات سایبری و همچنین ایجاد قوانین مدون برای به رسمیت‌شناختن مالکیت فکری به عنوان عناصر حقوقی برای حمایت از مالکیت فکری ضروری هستند.

نتیجه‌گیری: مالکیت فکری برخلاف مالکیت مادی، بیشتر جنبه پنهان و غیر رسمی دارد. به همین دلیل، قوانین موجود در زمینه حمایت از مالکیت فکری غالباً ناقص و یا از تحولات سایبری باز می‌ماند. به نظر می‌رسد در قوانین بین‌المللی نیازمند رویکردی منسجم و پذیرفته‌شده از سوی کشورهای جهان هستیم. همچنین در قوانین داخلی نیازمند نهاد مالکیت فکری تحت لوای قوانین موجود هستیم. به علاوه مالکیت فکری و قوانین مرتبط با آن از جمله قوانین کپی‌رایت، نشر مطالب در فضای مجازی و بهره‌مندی از اینترنت نیازمند اتخاذ رویکردهای سخت‌گیرانه‌تری است که هم بتواند قوانین بین‌المللی را مد نظر قرار دهد و هم این‌که حقوق مالکان معنوی را همانند مالکیت صنعتی مراعات نماید.

واژگان کلیدی

حقوق بین‌الملل، تهدیدات سایبری، مالکیت، مالکیت فکری

مقدمه

با گسترش روزافزون علم و تکنولوژی و به دنبال آن، پیدایش اختراعات و اکتشافات، جنبه مادی علوم و فنون، چهره جدیدی از خود نشان داد و مالیت پیداکردن ایده و فکر به عنوان یک پدیده جدید، در محافل حقوقی و بین‌المللی رخ نمود. از این رو و برای تعیین محدوده حقوقی، برای ایده و فکر که منجر به خلق طرح‌های صنعتی، تجاری، فرهنگی، هنری و... می‌شوند، عنوان مالکیت معنوی یا فکری انتخاب شد تا صاحبان ایده و فکر از حقوقی مشابه حقوق مالکین برخوردار شوند، اما با ورود به عصر ارتباطات و اطلاعات این حقوق نیز همچون دیگر حقوق بشری، در معرض تعرض و سوءاستفاده از طریق تهدیدات و جرائم سایبری قرار گرفته است. بنابراین نوع جدیدی از تهدیدات پدیدار شده که نیازمند به کارگیری قوانین جدیدی نیز می‌باشد. به طور کلی، از نظر استراتژیک همه ملت‌های دنیا در برابر تهدید ناخواسته‌ای قرار دارند، تهدیدی که دارایی‌های آن‌ها را بر اساس اهمیت دنبال می‌کند. کشورهای دنیا بر اساس استراتژی امنیتی و دفاعی خود اقدام به تشکیل تیم‌ها و ستادهایی در جهت تحقیق، پژوهش و اقدام در فضای سایبر نموده تا بتوانند ضمن این‌که تهدیدات در این فضا را شناسایی نمایند، در مواقع لزوم با آن‌ها مقابله نمایند. از این رو بسیاری از کشورها نه‌تنها اقدام به شناسایی، کاوش و جاسوسی در فضای سایبر می‌نمایند، بلکه در حال ایجاد توانایی‌های لازم در جنگ و تهدیدات سایبری هستند و در نتیجه فضای سایبر در تعیین اهداف سیاست کشورها، نقش غیر قابل انکاری به خود گرفته است.

توسعه تهدیدات و جرائم سایبری و نفوذ به شبکه‌های رایانه‌ای، نشان می‌دهد که سرمایه‌های مالی، معنوی و زیرساخت‌های حیاتی یک کشور، اهدافی هستند

که همیشه در معرض تهدیدات جدی قرار دارند. رویداد تأسف بار این است که کمبود قواعد و مقررات بین‌المللی باعث گردیده که کنترل بسیار کمی بر این تعارضات باشد، به همین منظور کشورها با ایجاد فناوری‌های لازم در فضای سایبر تلاش دارند ضمن اتخاذ سیاست‌های راهبردی جدید در این حوزه، اقدامات پیشگیرانه را در مقابل سوءاستفاده‌های سایبری تدوین نموده و به‌کار گیرند. علیرغم ضرر و زیان و حتی مرگ‌آوری احتمالی و بالقوه برخی از انواع تهدیدات سایبری، این شکل از حمله در حال حاضر در محیطی قانونی به شکل‌هایی دیگر در حال رخ‌دادن است. یکی از این موارد نقض حقوق مالکیت فکری در فضای سایبر، نقش مالکیت فکری است که پژوهش حاضر درصدد است تا به این مسأله بپردازد. بنابراین سؤال پژوهش حاضر به طور مشخص این است: فرصت‌ها و موانع موجود در ارتباط با رویکردهای حقوقی در زمینه تهدیدات سایبری از جمله مالکیت فکری شامل چه مواردی است؟ فرضیه این است: تهدیدات سایبری در حیطه مالکیت فکری برخلاف مالکیت صنعتی دارای جنبه‌های پنهان و پیچیده‌ای است که فقدان نهاد بین‌المللی مشخص در این زمینه باعث بروز برخی موانع و چالش‌های برای شناسایی و مقابله با تهدیدات سایبری شده است.

الف ـ مفاهیم و تعاریف

ابتدا لازم است برخی مفاهیم اساسی مورد بحث قرار گیرد.

۱ـ مالکیت فکری (معنوی)

مالکیت فکری به نوع خاصی از مالکیت اشاره می‌کند که حاصل فکر و اندیشه انسان و خلاقیت وی است و در زمره امور غیر قابل لمس قرار می‌گیرد. مالکیت معنوی و مالکیت فکری غالباً به جای یکدیگر نیز به کار می‌روند، زیرا هر دو به

موضوع غیر قابل لمس‌بودن مالکیت اشاره می‌کنند. به هر صورت واژه معنوی در برابر مادی قرار می‌گیرد و امور انتزاعی را دربر می‌گیرد. برخی بر این عقیده هستند که مالکیت فکری از مالکیت معنوی رساتر است، زیرا آنچه با فکر و اندیشه انسان سروکار دارد، می‌تواند مالکیت فکری باشد (امامی، ۱۳۸۹ ش.)، اما به هر صورت مالکیت معنوی نیز به معنای مالکیتی است که بر آثار هنری و فکری اطلاق می‌شود و به عنوان یک حق منافعی برای صاحب آن پدید می‌آورد (نقیبی، ۱۳۸۶ ش.). قوانین داخلی ایران به صراحت مالکیت معنوی را تعریف نکرده‌اند، اما همچنان قانون مصوب ۱۳۴۸ به عنوان قانون حاکم بر مالکیت فکری شناخته می‌شود. با توجه به همین قانون و سایر قوانین می‌توان مالکیت معنوی را این‌گونه تعریف نمود: «حقوق معنوی، مزایایی است قانونی، غیر مادی و مربوط به شخصیت پدیدآورنده یک اثر فکری که به موجب آن، وی برای همیشه از یک دسته حقوق خاص برخوردار است» (آیتی، ۱۳۷۵ ش.).

۲ـ فضای سایبر

مفهوم فضای سایبر، معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود. بدون وجود فناوری، سخن‌گفتن از فضای سایبری بی‌معناست. فضای سایبر تقریباً به موضوعات علمی ـ تخیلی شبیه است. در واقع فضای سایبری نوعی ناکجاآباد است که هویت‌های متعددی در آن دیده می‌شود (هانِی، ۲۰۰۶ م.). فضای سایبر همسان و هم‌عنان با اینترنت نیست، اما وجود اینترنت از ملزومات آن است. جرم سایبری نیز، جرمی است که طریق فضای مجازی و با بهره‌گیری از ابزارهای اتصال به این فضا ارتکاب می‌یابند.

۳ـ مالکیت و مالکیت فکری

در علم حقوق مالکیت را به دو قسم مالکیت عمومی و خصوصی تقسیم کرده‌اند، مالکیت خصوصی که مالکیت شخصی نیز نامیده می‌شود، زیربنای آن کار است و هر مالی که از کار خاص بشری به وجود می‌آید و شکل گیرد، جزء ثروت‌های خصوصی است. مالکیت عمومی نیز عبارت است از مالکیت اموالی که خارج از اراده و اختیار مردم است و در تصرف و اختیار دولت می‌باشد. در قانون مدنی تعریفی از مالکیت نشده است و فقط دو قسم آن را (مالکیت عین و مالکیت منفعت) آورده است. در قانون اساسی جمهوری اسلامی، هرچند به طور صریح به انواع مالکیت اشاره نکرده است، اما در برخی اصول با آوردن انواع مال، خصوصی (اصول ۴۶ و ۴۷) و عمومی (اصول ۴۵ و ۴۹) و دولتی (اصول ۴۳ و ۴۹) مالکیت را به سه نوع مالکیت شخصی، دولتی و عمومی دانسته است (بزرگی، ۱۳۹۴ ش.). مالکیت معنوی دارای گونه‌های متعددی است که در حقوق داخلی ایران با عنوان مالکیت فکری نیز خوانده می‌شود. در هر صورت و در یک نگاه کلی می‌توان مالکیت فکری و یا معنوی را به همان حقوق ناشی از خلاقیت فکری و آفرینش‌های علمی، هنری، ادبی و... اطلاق نمود. با توجه به این تعریف، حقوق مالکیت فکری می‌تواند شامل دو گونه زیر باشد:

۱ـ حقوق مالکیت صنعتی.

۲ـ حقوق کپی‌رایت.

در یک تقسیم‌بندی جزئی‌تر نیز می‌توان حقوق مالکیت صنعتی را در دو بخش عمده نیز تقسیم نمود:

۱ـ حقوقی که به علائم از جمله علائم تجاری و علائم جغرافیایی اشاره می‌کند که در صورت حفظ شکل هر یک از علائم ذکر شده تا مدت‌های نامحدودی می‌توانند مورد حمایت قرار گیرند.

۲ـ حقوقی که به اختراع و طراحی صنعتی مربوط می‌شوند و می‌تواند اختراعات، طرح‌های صنعتی و تجاری را نیز دربر گیرد و معمولاً حمایت از این نوع حقوق محدود است.

علاوه بر این، کپی‌رایت نیز دارای قوانین خاصی است که به حق نسخه‌برداری یا حق مؤلف مربوط می‌شود. از نظر اصطلاحی نیز به حقوق پدیدآورندگان آثار هنری و علمی گفته می‌شود که دربرگیرنده آثار مکتوب تا آثار سمعی بصری و آثار تجسمی و صنایع دستی و نقشه قالی و گلیم و نرم‌افزارهای رایانه‌ای است. حقوق مربوط به کپی‌رایت نیز در دو دسته زیر قابل تقسیم هستند:

۱ـ کپی‌رایت و حقوقی که برای پدید آورندگان آثار آن وجود دارد.

۲ـ حقوق جانبی کسانی که با این آثار سروکار دارند و می‌تواند شامل حقوق اجراکنندگان، تولیدکنندگان آثار صوتی و سازمان‌های پخش رادیو و تلویزیونی باشد (بزرگی، ۱۳۹۴ ش.).

ب ـ ساختار و کارکرد فضای سایبر

وقتی صحبت از فضای سایبر به میان می‌آید مردم اغلب به رایانه یا رایانه‌هایی فکر می‌کنند که به اینترنت متصل است، در حالی که این فقط بخش بسیار کوچکی از فضای سایبری را تشکیل می‌دهد. فضای سایبر فقط مجموعه‌ای از سخت‌افزار و نرم‌افزار نیست، بلکه مجموعه‌ای از تعاریف نمادین است که شبکه‌ای

از اطلاعات، برنامه‌ها، سیستم‌های کنترل پرواز، سیستم‌های کنترل تأسیسات و... را در قالب صفر و یک رد و بدل می‌کنند (جی‌پست، ۱۳۸۵ ش.).

اغلب امکانات و تجهیزات پیشرفته رایانه‌ای، چه در بخش‌های نظامی و چه در بخش‌های غیر نظامی، به صورتی بنیادی آسیب‌پذیر هستند که این امر ناشی از وابستگی این سامانه‌ها به دستورالعمل‌های مجازی می‌باشد که در حافظه اصلی آن‌ها قرار گرفته و هدایت سیستم‌های سخت‌افزاری ملموس را که بخشی از اجزای کنترلی هستند، به عهده می‌گیرند. به عبارت دیگر، آسیب به یک سامانه رایانه‌ای، چیزی غیر از قراردادن مجموعه‌ای از دستورالعمل‌های خاص با اهداف ویژه در حافظه اصلی سامانه، و هدایت واحد مرکزی پردازش[1] به اجرای این دستورالعمل‌ها نیست که این امر می‌تواند منجر به تولید سیگنال‌ها و اطلاعات نادرست و در نهایت مسبب حملات سایبری گردد. بنابراین فضای سایبر با سایر فضاهای اطلاعاتی مورد استفاده در جوامع بشری که تاکنون وجود داشته، تفاوت دارد که این تفاوت به ویژگی این فضای جدید مرتبط می‌باشد، لذا در ادامه به ویژگی‌های این فضا و قلمروی فضای سایبر می‌پردازیم.

تفاوت محیط سایبر در مقایسه با سایر محیط‌ها در چند ویژگی مهم نهفته است. این ویژگی‌ها که بعضاً از ویژگی‌های منحصر به فردِ فضای سایبر نیز محسوب می‌شوند. از جمله جهانی و فرامرزی بودن: جهانی‌بودن به عنوان مهم‌ترین ویژگی فضای سایبر شناخته می‌شود که آن را از سایر فضاهای موجود و رسانه‌های سنتی متمایز می‌سازد. جهانی و فرامرزی‌بودن بدین‌معناست که هر فردی در هر مکانی به راحتی می‌تواند با دیگران ارتباط برقرار کند و یا این‌که به اطلاعات تازه‌ای دسترسی پیدا کند، ضمن این‌که در شرایط کنونی و با گسترش اطلاعات و ارتباطات، مرزهای جغرافیایی چندان اهمیتی ندارند و یا این‌که

نمی‌توانند مانعی برای برقراری ارتباطات باشند. به همین دلیل در فضای سایبر، دسترسی پیداکردن به اطلاعات علمی اعم از مقاله، کتاب، اخبار و یا امور تخصصی دیگر بسیار آسان و سهل‌الوصول است (سلطانا و سبحان، ۲۰۱۲ م.). جذابیت و تنوع: رسانه‌ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب‌کردن خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است، به ویژه آنگاه که هیچ نظارت و فیلتری توان محدودکردنش را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوع و جذابیت فضای سایبر تأثیر به سزایی دارد، مشتری محوری محض است (سلطانا و سبحان، ۲۰۱۲ م.). آزادی اطلاعات و ارتباطات: معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این رو شما هر نوع اطلاعاتی را که بخواهید ـ اعم از فرهنگی، سیاسی و اقتصادی ـ بدون محدویت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست (سلطانا و سبحان، ۲۰۱۲ م.).

ج ـ جرائم سایبری

گسترش ابزارهای ارتباطی و به دنبال آن شکستن مرزهای جغرافیایی و امکان برقراری ارتباط با کم‌ترین هزینه با سایر نقاط جهان، از یکسو فرصتی بی‌نظیر به شمار آمده و از سوی دیگر، تهدیدهایی را برای امنیت اقتصادی، فرهنگی، سیاسی بشر موجب شده است. یکی از مهم‌ترین این تهدیدها، پدیده‌ای به نام جرائم سایبری است. جرائم سایبری دارای ویژگی‌هایی هستند که آن‌ها را از سایر جرائم متمایز می‌کند. سالانه، بزهکاران سایبری، خسارات فراوانی به امنیت ملی، اقتصادی، فرهنگی و... کشورها وارد می‌آورند. از آن گذشته، باید توجه داشت که

بزهکاری سایبری گاه با حمایت دولت‌ها صورت گرفته و هدف از ارتکاب این جرائم، واردکردن صدمه به کشورهای دیگر بوده است. جرائمی که در مقایسه با جرائم سنتی، هر روز قربانیان بیشتری از بشریت گرفته و نیز روش‌های سنتی مبارزه با جرائم در خصوص آن‌ها راهگشا نیست.

از نظر حقوقی، جرم سایبری این‌گونه تعریف می‌شود: «هر اقدامی که از طریق فضای مجازی و با بهره‌گیری از ابزارهای اتصال به فضای مجازی صورت گرفته و حقوق شناسایی‌شده برای افراد را نقض می‌کند.» به این ترتیب، تنها جرائمی در دامنه شمول این تعریف قرار می‌گیرند که از طریق فضای مجازی و با بهره‌گیری از ابزارهای اتصال به این فضا ارتکاب می‌یابند. به عنوان مثال، کلاهبرداری یک جرم سنتی است که از دیرباز در نظام حقوقی کشورها وجود داشته است. در جریان این جرم، بزهکار از طریق مانورهای متقلبانه همچون معرفی‌کردن خود به عنوان یک فرد صاحب نفوذ، رییس یک شرکت تجاری بزرگ و...، اقدام به بردن مال دیگری می‌کند. در مقابل، اخیرا با پدیده‌ای به نام کلاهبرداری رایانه‌ای یا همان کلاهبرداری سایبری مواجه هستیم. در جریان این جرم، بزهکار با ایجاد اختلال در سامانه‌های رایانه‌ای اشخاص و کشف رمز عبور و نام کاربری آن‌ها، فریب شهروندان نسبت به اموری مانند شرکت در قرعه کشی و... اقدام به بردن وجه یا مالی از آن‌ها می‌نماید. در خصوص جرم سرقت سایبری نیز وضعیت به همین نحو است. در جریان ارتکاب سرقت به صورت سنتی، فرد سارق اقدام به ربایش مال از منزل، مغازه یا ... می‌نماید، اما در خلال سرقت رایانه‌ای، بزهکار به صورت غیر مجاز اقدام به ربایش اطلاعات محرمانه اشخاص، سازمان‌ها، شرکت‌ها و... می‌نماید و به این طریق به صاحبان داده‌ها خسارت وارد می‌کند. با توجه به دو مثال مطرح‌شده، می‌توان به تفاوت جرائم سنتی و جرائم سایبری پی برد.

یکی از چالش‌های موجود در اکثر مقالات و کتاب‌های موجود، نبود تعریفی جامع در خصوص «حمله سایبری» می‌باشد. فعلاً به عنوان یک تعریف پایه، حمله سایبری را به شکل زیر تعریف می‌نماییم: «حمله سایبری، نوعی عملیات مبتنی بر اطلاعات به صورت تهاجمی یا تدافعی می‌باشد که به منظور ایجاد اختلال و یا تخریب اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای، به کار گرفته می‌شود.» از آنجا که حمله سایبری نوعی تلاش برای تغییر اطلاعات موجود در رایانه‌ها و یا شبکه‌های رایانه‌ای می‌باشد، لذا می‌توان حمله سایبری را، نوعی عملیات اطلاعاتی تهاجمی با طبقه‌بندی جدید در مقوله جنگ معرفی و به صورت زیر تعریف نمود: «حمله سایبری، نوعی عملیات اطلاعاتی تهاجمی یا تدافعی می‌باشد که به منظور ایجاد اختلال، تنزل و یا تخریب اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای، به کار گرفته می‌شود» (مَتیو، ۲۰۱۲ م.). چالش اولیه در ارزیابی و تعریف حملات سایبری، ماهیت و قلمروی این‌گونه عملیات می‌باشد. به عنوان مثال، شورای پژوهش ملی ایالات متحده آمریکا، حمله سایبری را به مثابه اقدامی آگاهانه برای جایگزینی، اختلال، فریب، تغییر، یا تخریب سیستم‌های رایانه‌ای و اطلاعات آن‌ها تعریف کرده است. از سوی دیگر سازمان همکاری‌های شانگهای از زاویه‌ای دیگر حمله سایبری را به مثابه «شستشوی مغزی گسترده جهت ناامن و بی‌ثبات‌کردن جامعه داخلی و وادارکردن دولت به اتخاذ تصمیم به نفع طرف مخالف» تعریف کرده است (مَتیو، ۲۰۱۲ م.).

همچنین در تعریفی دیگر نیز چنین بیان شده است: «هر اقدامی که به منظور تضعیف کارکرد شبکه‌های رایانه‌ای یک کشور با هدفی سیاسی و یا برضد امنیت ملی کشور مورد هدف واقع شود»، یک حمله سایبری می‌باشد (مَتیو، ۲۰۱۲ م.). لازم به ذکر است به دلیل عدم اجماع جهانی در خصوص مفهوم حمله سایبری،

برخی از دولت‌ها از این خلأ استفاده کرده و هرگونه تعریفی که به صلاح نظام امنیتی خودشان باشد را مبنای تصمیم‌گیری قرار می‌دهند. از این رو به تعاریفی که برخی از دولت‌ها و یا نهادهای وابسته به آن‌ها ارائه نموده‌اند، اشاره می‌گردد. با توجه به رویکرد متفاوت برخی از دولت‌ها به مصادیق حمله سایبری، تعریف پیشنهادی برای مفهوم حمله سایبری به شرح ذیل می‌باشد: «هر عملیاتی که موجب مختل‌شدن عملکرد یک شبکه رایانه‌ای و یا تجهیزات الکترونیکی، مخابراتی و... با اهداف سیاسی و یا برهم‌زدن امنیت ملی و صدمه‌زدن به زیرساخت‌های حیاتی یک کشور انجام پذیرد، حمله سایبری می‌باشد.»

د ـ رویکردهای حقوقی به تهدیدات سایبری

حملات سایبری و جرائم سایبری از مهم‌ترین تهدیدات سایبری می‌باشند که لازم است در این قسمت به آن‌ها بپردازیم به همین دلیل، از یک طرف موضوع اثبات مالیت داده‌های رایانه‌ای در جهت اثبات تخریب داده‌ها و ورود خسارت به کشورها مورد مطالعه در سطح حقوق بین‌الملل و به خصوص حقوق بین‌الملل بشردوستانه می‌باشد و از سوی دیگر مالکیت فکری و یا مصادیق مربوط به آن همانند سایر موارد که در فضای اینترنت و سایبری قرار دارند، نیازمند حفاظت و حراست هستند، زیرا عدم توجه به قوانین مربوطه در این زمینه و یا نادیده‌گرفتن مسأله مالکیت در حیطه مالکیت فکری، حقوق اشخاص حقیقی و حقوقی را با تهدید رو به رو می‌سازد. به همین دلیل بررسی رویکردهای حقوقی و تلاش برای مقابله با این‌گونه تهدیدات سایبری امری ضروری است که به برخی از مهم‌ترین موارد پرداخته می‌شود:

۱ـ تخریب و مالیت داده‌های رایانه‌ای در حملات سایبری

با توجه به رشد روزافزون استفاده از فناوری اطلاعات، بحث از مال‌بودن داده‌های رایانه‌ای و انطباق آن بر مبانی مال‌بودن اشیا بسیار اهمیت دارد. مفهوم مال از جهات مختلفی مورد مداقه حقوقدانان قرار گرفته است، مانند مثلی و قیمی‌بودن، کلی یا معین‌بودن و... .

اما به منظور ارزیابی قابلیت کاربرد قواعد حقوق بین‌الملل بشردوستانه در مواجهه با حملات سایبری، اثبات مالیت داده‌های رایانه‌ای مهم است.

۱-۱- مبانی حقوقی مالیت داده‌های رایانه‌ای: برای تشخیص مالیت داده‌های رایانه‌ای لازم است که ویژگی‌های این داده‌ها را بررسی نماییم.

ـ داشتن ارزش اقتصادی: این ویژگی از بدیهیات داده‌های رایانه‌ای می‌باشد.

ـ برآوردن نیازها: اکثر داده‌های رایانه‌ای به قصد رفع نیازهای مادی و معنوی تولید گردیده‌اند.

ـ قابلیت اختصاص‌داشتن: همین که می‌گوییم «نرم‌افزار فروش محصولات ایران خودرو»، به این معناست که این نرم‌افزار اختصاص به شخص خاص و معینی دارد.

ـ منقول‌بودن: از آنجایی که داده‌های رایانه‌ای بدون ایجاد خسارت از مبدأ به محل دیگری قابل انتقال می‌باشند، بنابراین در حکم مال منقول محسوب می‌گردند.

ـ عینیت‌داشتن: برخی بر این عقیده هستند که داده‌های رایانه‌ای در گروه حقوق قرار می‌گیرند نه اموال، اما با استناد به «قانون مجازات پیشه‌وران و کسانی که کالای خود را مخفی می‌کنند یا گران می‌فروشند» مصوب ۱۳۲۲، می‌توان گفت که داده‌های رایانه‌ای نیز همانند نیروی برق، مال محسوب می‌گردد.

ـ مبنای عرف و عقلا: داده‌های رایانه‌ای در نظر عرف و عقلا مالیت داشته و دارای ارزش اقتصادی هستند و معامله بر آن‌ها صحیح است (بهمن‌پور و همکار، ۱۳۹۳ ش.).

۲-۱- تخریب داده‌های رایانه‌ای در حملات سایبری: جرم تخریب داده‌های رایانه‌ای یکی از انواع مهم جرائم رایانه‌ای است که به علت تفاوت قابل توجه آن با تخریب سنتی توانسته است به عنوان معضلی نوین توجه صاحب‌نظران عرصه حقوق را به خود جلب نماید. تخریب مصدر باب تفعیل و به معنای ویران کردن و خراب‌کردن است و در اصطلاح حقوقی به معنای تباه‌نمودن ابنیه و خراب کردن اموال است. در قانون جرائم رایانه‌ای ایران نیز همین تعریف تکرار گردیده است.

البته در تبیین و تعریف جرم تخریب داده‌های رایانه‌ای، تفاوت‌هایی وجود دارد که در قوانین اکثر کشورهای خارجی به آن اشاره گردیده است .

شورای اروپا در توصیه‌نامه این جرم را بدین شرح تعریف نموده است: «محوکردن، خسارت‌زدن، کم‌ارزش‌کردن یا متوقف‌کردن داده‌های رایانه‌ای به طور غیر قانونی» (دزیانی، ۱۳۷۶ ش.).

کنوانسیون ۲۰۰۱ بوداپست نیز در ماده ۴ خود، جرم تخریب داده‌ها را به همین شکل تعریف کرده است.

حال از آنجایی که در قوانین اکثر کشورها از طرفی جرم تخریب را از انواع جرائم ملموس و فیزیکی دانسته‌اند و از سوی دیگر تخریب داده‌های رایانه‌ای، ماهیتی ناملموس دارد، لذا اجرای مقررات مربوط به تخریب داده‌ها در بسیاری از این کشورها دچار مشکل گردیده است.

برای حل این چالش اکثر کشورهایی همچون اتریش، کانادا، آلمان، ایتالیا، انگلستان و نروژ خسارت عمدی به داده‌های رایانه‌ای را، خسارت به اموال و از نوع تخریب سنتی دانسته‌اند (زیبر،۱۳۸۳ :۱۴۴).

به نظر می‌رسد که امروزه اکثر کشورها به سمت روش تدریجی اصلاح قوانین روی آورده و چنین خسارت‌هایی را نیز مشمول تخریب فیزیکی دانسته‌اند.

بنابراین نتیجه‌ای که از این بحث می‌توان گرفت، این است که:

ـ داده‌های رایانه‌ای در حکم مال منقول می‌باشند.

ـ تخریب داده‌های رایانه‌ای در حکم (معادل) تخریب فیزیکی و سنتی می‌باشند یا به عبارتی در خصوص داده‌های رایانه‌ای می‌توان از اصطلاح تخریب فنی به جای تخریب فیزیکی استفاده نمود.

ـ رکن مادی جرم تخریب فنی با رکن مادی جرم تخریب فیزیکی قابل تشبیه می‌باشند، چراکه هر دو جرم مقید به نتیجه می‌باشند.

از آنجایی که در اصول و قواعد حقوق بین‌الملل بشردوستانه صحبتی از تخریب داده‌های رایانه‌ای به میان نیامده است، برای بیان مفهوم تخریب داده‌های رایانه‌ای در زمان حمله سایبری از منظر قواعد حقوق بین‌الملل بشردوستانه، می‌توانیم از استدلال زیر بهره ببریم.

همان‌گونه که اصطلاح مسلحانه‌بودن یک حمله، خصوصاً در مواردی که ابزارهای اعمال زور فاقد سلاح‌های جنبشی باشند، از طریق بررسی پیامدهای ناشی از آن و بدون توجه به ابزارهای اعمال زور صورت می‌گیرد، لذا مفهوم اصطلاح تخریب نیز گاهی مواقع با ملاحظه پیامدهای تخریب داده‌های رایانه‌ای قابل درک می‌گردد، نه صرف تخریب فیزیکی داده‌ها، مثلاً مختل‌نمودن سامانه بانکداری و یا بازار بورس اصلی که منجر به سقوط شدید و یا فروپاشی اقتصاد و

در نتیجه موجب افزایش بیکاری، گرسنگی، اضطراب و در نهایت موجب رنج و عذاب روحی می‌گردد، به نظر می‌رسد کم‌تر از تخریب فیزیکی سیستم اقتصادی یک کشور با جنگ افزارهای مرسوم نباشد.

۲ـ سازمان جهانی مالکیت فکری

کنوانسیون پاریس برای حمایت از حقوق مالکیت فکری در سال ۱۸۸۳ ماه مارس در پاریس به امضا رسید و اولین موافقت‌نامه بین‌المللی در حیطه مالکیت فکری و حقوق مؤلفین، در ۹ سپتامبر ۱۸۸۶ در «برن» منعقد و تصویب شد. به طور مشخص، این موافقت‌نامه بین‌المللی به «میثاق برن برای حمایت از آثار ادبی و هنری» مشهور است. این میثاق توسط سازمان جهانی مالکیت فکری[۲] در ژنو به اجرا گذاشته می‌شود. در این توافق‌نامه علاوه بر حقوق مادی و اقتصادی، حقوق معنوی مؤلف نیز در نظر گرفته شده است (بهمن‌پور و همکار، ۱۳۹۳ ش.). این رویکرد، هرچند در گذشته بر وجوه آشکار و سنتی مالکیت افراد تأکید می‌کرد، اما امروزه و با توجه به گسترش اینترنت و فضای ارتباطاتی فراگیر، تهدیدات مرتبط با آن نیز به حوزه فضای سایبری نیز کشیده شد.

علاوه بر موافقت‌نامه برن، رویکردهای بین‌المللی از جمله اصل ۲۷ اعلامیه جهانی حقوق بشر که در سال ۱۹۴۸ تصویب شد، به وضع قوانین در حوزه مالکیت فکری نیز پرداخته است. در این اصل و در راستای حمایت از حقوق مالکیت فکری نیز آمده است: «هر کس این حق را دارد که آزادانه در فرهنگ جامعه مشارکت جدید از هنرها بهره گیرد و در پیشرفت علمی و مزایای آن سهیم شود. هر کس این حق را دارد که از منافع مادی و معنوی اثر هنری، ادبی یا علمی که خود خلق کرده است، بهره‌مند شود» (شفیعی و شکیب، ۱۳۸۱ ش.). این رویکرد عام و فراگیر می‌تواند قانونی برای فضای سایبری نیز در نظر گرفته شود، زیرا

نقض حقوق مالکیت افراد اعم از ادبی یا هنری و علمی در فضای سایبر نیز نیازمند حمایت از سوی قوانین بین‌المللی می‌باشد.

سازمان جهانی مالکیت فکری، دو هدف اصلی را دنبال می‌کند: هدف اول ارتقای حمایت از مالکیت فکری در سراسر جهان از طریق همکاری بین دولت‌ها و در صورت لزوم با همکاری سایر سازمان‌های بین‌المللی است و هدف دوم وایپو، ایجاد همکاری اداری بین اتحادیه‌های تأسیس شده به وسیله معاهدات تحت نظر وایپو است. به جز موافقت‌نامه تریپس، وایپو کلیه کنوانسیون‌هایی را که به آن‌ها اشاره شد، دربر می‌گیرد. به عبارتی دیگر، وایپو برای تحقق اهدافش، علاوه بر انجام وظایف اداری اتحادیه‌های مذکور این اقدامات را نیز انجام می‌دهد: اقدامات تجویزی یا هنجارآفرینی از طریق وضع استانداردهایی برای حمایت از مالکیت فکری، اجرای برنامه‌های اعطای کمک‌های فنی و حقوقی به کشورها در زمینه مالکیت فکری، اقدامات مربوط به طبقه‌بندی و یکسان‌سازی بین‌المللی در زمینه مستندسازی حق اختراع، علائم تجاری و طرح‌های صنعتی، اقدامات ثبتی نظیر ارائه خدمات مربوط به تقاضانامه‌های ثبت اختراع، علائم تجاری و طرح‌های صنعتی می‌باشد (لایقی، ۱۳۸۱ ش.).

جهان معاصر در حوزه‌های مختلفی باعث تحول در شیوه‌های ارتباطی و انتقال اطلاعات شده است. تصویب دو عهدنامه جدید به نام عهدنامه حق مؤلف WCT و عهدنامه اجراها و صوت ـ نگاشت‌ها[۳] که در سال ۱۹۶۰ انجام شد، به همین موضوعات اشاره دارند، ضمن این‌که میثاق WCT حق تکثیر مؤلف را با رجوع به ماده ۹ میثاق برن در نظر گرفته است و میثاق WPPT حقوق انحصاری تکثیر برای اجراکنندگان و تولیدکنندگان صوت ـ نگاشت‌ها مورد تأکید قرار داده است. با این وجود مهم‌ترین خدماتی که از این دو عهدنامه در حیطه مالکیت فکری

پدید آمده، این است که حقوق مؤلف خوانندگان و تولیدکنندگان صوت ـ نگاشت‌ها را در نظر گرفته و اجازه انتقال آن‌ها را نیز به رسمیت شناخته است (بزرگی، ۱۳۹۴ ش.). این معاهدات بین‌المللی به طور مشخص و بر حسب مصوبات خود نسبت به دستور کار دیجیتال ورود می‌کنند و از حقوق مالکین حمایت به عمل می‌آورند. این موارد بدین صورت است: ۱ـ به رسمیت‌شناختن حق تکثیر درباره ذخیره در سیستم‌های دیجیتالی؛ ۲ـ توجه به محدودیت‌ها و موارد استثنایی در فضای دیجیتالی؛ ۳ـ اقدامات تکنولوژیکی حمایتی؛ ۴ـ مدیریت حقوقی اطلاعات تکنولوژیکی و دیجیتالی.

هنگامی که مالکیت فکری افراد در حوزه‌های مختلف اعم از فضای مجازی و سایبری و همچنین حوزه‌های فناوری اطلاعات مورد تهدید واقع می‌شود، بهره‌گیری از اقدامات تکنولوژیک برای مقابله با این تهدیدات امری بایسته است، چنانچه بر مبنای همین قواعد بین‌المللی، اقدامات حمایتی تکنولوژیک برای جلوگیری از مسأله سرقت اطلاعات در نظر گرفته شده است. قواعد بین‌المللی موجود، رویه‌ای اجباری برای دولت‌ها ایجاد نموده است که از حقوق صاحبان آثار در فضای سایبر حمایت به عمل آورند و حتی اقدامات جبرانی برای اعاده خسارات افراد در نظر بگیرند (جعفری، ۱۳۸۸ ش.).

قوانین بین‌المللی موجود از جهت دیگر باعث ایجاد امنیت در فضای سایبری می‌شوند و زمینه را برای تعامل مناسب‌تر فراهم می‌آورند. به عنوان مثال، معاهده حق مؤلف که به حقوق مالکیت فکری مصوب ۱۹۶۶ مربوط می‌شود، حقوق مرتبط با حق مؤلف اینترنتی را نیز شامل می‌شوند که هدف اصلی آن، حمایت از حقوق پدیدآورندگان و کاربران و ایجاد تعادل میان نیازها و حقوق مرتبط با آنان نیز می‌باشد. رویکرد این مصوبه به این موضوع اشاره می‌کند که اگر آثار صاحبان

و حقوق آنان به خوبی محافظت نشود، نمی‌توانند آثار خود را در فضای سایبر در دسترس دیگران قرار دهند (نوروزی، ۱۳۸۱ ش.).

سازمان حمایت از مالکیت فکری بعد از این‌که دو کنوانسیون برن و پاریس در سال ۱۹۸۳ در هم ادغام شدند، در سال ۱۹۷۴ توانست به عنوان یکی از مهم‌ترین سازمان‌های تخصصی در حیطه مالکیت فکری مطرح شود (لطیفی، ۱۳۹۱ ش.).

حقوق مالکیت فکری در قوانین داخلی ایران نیز مورد توجه است، از جمله قانون تجارت الکترونیکی در سال ۱۳۸۳، قانون حمایت از نرم‌افزارهای رایانه‌ای در سال ۱۳۷۹ و در جهت به روزکردن قوانین، قانون ثبت اختراعات، علائم تجاری و طرح‌های صنعتی در سال ۱۳۸۶ تصویب و اصلاح شد. همچنین قانون حمایت از مالکیت فکری در فضای سایبر به کمک یکی از وزارتخانه‌ها در حال تدوین است (میرحسینی، ۱۳۹۱ ش.). بدین‌ترتیب در حقوق داخلی ایران نیز در حیطه تهدیدات سایبری و مالکیت فکری، قوانین متعددی دیده می‌شود که جنبه‌های مختلف مالکیت معنوی و فکری را تحت پوشش خود قرار داده است.

۳ـ کنوانسیون بین‌المللی جرائم سایبری

مقابله با جرائم سایبری بخش دیگری از راهکارهای حقوقی برای مقابله با تهدیدات سایبری است و به همین منظور، کنوانسیون بوداپست اولین پیمان بین‌المللی ایجادشده برای مقابله با جرائم اینترنتی است که حدود ۴۰ کشور مختلف در کنفرانس بین‌المللی بوداپست با موضوعیت جرائم اینترنتی، در ۲۳ نوامبر ۲۰۰۱ در مجارستان آن را امضا کردند که از آن پس این پیمان به نام پیمان بوداپست معروف شد. در ماده ۴ این کنوانسیون، جرم تخریب داده‌ها تعریف شده است (کنوانسیون جرم سایبری اتحادیه اروپا، ۲۰۰۱ م.). این پیمان شامل تعاریف دقیق برای همه نوع از جرائم اینترنتی بوده و کیفر مربوط به هر

کدام نیز مشخص شده است. همه کشورهایی که این پیمان را امضا کرده‌اند، قانون و مقررات یکسانی برای کنترل جرائم اینترنتی داشته و برای همکاری‌های بین‌المللی یک خط تلفن استاندارد برای این بخش فراهم کرده‌اند.

جرم تخریب داده‌های رایانه‌ای یکی از انواع مهم جرائم رایانه‌ای است که به علت تفاوت قابل توجه آن با تخریب سنتی توانسته است به عنوان معضلی نوین توجه صاحب‌نظران عرصه حقوق را به خود جلب نماید. «تخریب مصدر باب تفعیل و به معنای ویران‌کردن و خراب‌کردن است و در اصطلاح حقوقی به معنای تباه نمودن ابنیه و خراب‌کردن اموال است» (جعفری لنگرودی، ۱۳۸۸ ش.). در قانون جرائم رایانه‌ای ایران نیز همین تعریف تکرار گردیده است، البته در تبیین و تعریف جرم تخریب داده‌های رایانه‌ای، تفاوت‌هایی وجود دارد که در قوانین اکثر کشورهای خارجی به آن اشاره گردیده است.

۴ـ رسیدگی به نقض علائم تجاری

علائم تجاری، نام دامنه و همچنین سوءاستفاده از آن‌ها بخش‌های مهم دیگری از تهدیداتی است که به راحتی منافع و مالکیت بخش‌هایی از جامعه را تحت تأثیر خود قرار می‌دهد. با این حال، حل و فصل اختلافات نقض علائم تجاری از طریق نام دامنه دارای برخی ویژگی‌های اختصاصی می‌باشد که این ویژگی‌ها موجب می‌گردد، حل و فصل اختلافات این حوزه با برخی اصول حاکم بر حقوق مالکیت فکری تعارض پیدا کند، زیرا حمایت از علائم تجاری به عنوان یکی از صور اصلی حقوق مالکیت صنعتی در محدوده سرزمینی هر نظام قانونگذاری اتفاق می‌افتد این امر در برابر خصیصه جهانی‌بودن اینترنت، ایجاد مشکل کرده و نمی‌توان راه حل واحدی را جهت حل معضلات به وجود آمده برگزید (اصلانی، ۱۳۸۹ ش.). بدین‌ترتیب حمایت از حقوق مالکیت فکری، نیازمند وجود قوانین فرامرزی و

حاصل همکاری‌های بین‌المللی است، زیرا ماهیت لامکان و بدون مرزبودن فضای تبادل اطلاعات و امکان دسترسی به اطلاعات در هر لحظه و از هر مکان، نقطه مقابل این خصیصه، محسوب می‌شود. به عبارت دیگر اینترنت به عنوان بستری که در قالب مرزهای سرزمینی نمی‌گنجد و ممکن است در برابر حمایت‌های ملی از علائم تجاری تعارضاتی را ایجاد کند (اصلانی، ۱۳۸۹ ش.).

شیوه‌های حل و فصل اختلافات نقض علائم تجاری از طریق نام دامنه از راه‌های دیگری نظیر قوانین مدنی نیز قابل حصول است. اولین حالت مربوط به شرایطی است که نام دامنه نقض می‌شود که در این صورت پس از احراز سوءنیت نقض‌کننده نام دامنه، صاحب نام دامنه می‌تواند با استناد به این اقدام نزد مراجع قضایی شکایت کند که در این شرایط برای نقض‌کننده می‌توان قائل به ضمانت اجرای کیفری و مدنی شد (اصلانی، ۱۳۸۹ ش.).

هـ ـ خلأهای حقوقی در حیطه مالکیت فکری

یکی از خلأهای اساسی حقوقی در رابطه با حملات سایبری آن است که نهاد بین‌المللی مشخصی در این زمینه وجود ندارد (اُستردال، ۱۹۹۸ م.). ضمن این‌که سازمان ملل متحد به عنوان نهادی که حامی صلح شناخته می‌شود و بر همین مبنا می‌بایست به تهدیدات بپردازد، فعالیت‌های خود را چندان معطوف به حملات سایبری نمی‌نماید (زِمانک، ۲۰۱۰ م.). از این رو پشتوانه حقوقی مدونی نمی‌توان برای جلوگیری از حملات سایبری و یا عاملان وقوع آنان پیدا نمود. دلیل اصلی این مسأله آن است که در نظر طراحان منشور ملل متحد، تهدید علیه صلح محدود به قوای مسلح متعارف است. بنابراین هرچند بعدها تلاش شد تا با تفسیر اصطلاح «تهدید» و فراگیردانستن «صلح» برخی تهدیدات دیگر، از جمله

تهدیدات سایبری را در زمره تهدیدات و موانع صلح جهانی گنجاند، اما به دلیل عدم صراحت و فقدان نهاد بین‌المللی در این زمینه، همچنان با خلأهای قانونی در این زمینه رو به رو هستیم. همین فقدان نهاد بین‌المللی باعث نادیده‌گرفتن تهدیدات سایبری در حیطه مالکیت فکری به نحو جزئی نیز می‌شود.

به علاوه این‌که یکی دیگر از خلأهای قانونی و حقوقی در زمینه مقابله با تهدیدات سایبری آن است که مرزهای روشنی میان تهدیدات سایبری وجود ندارد. به عنوان مثال وقوع تلفات قابل ملاحظه انسانی که در کنار آن ممکن است باعث تخریب گسترده اموال عمومی، به عنوان مصداق حملات مسلحانه در نظر گرفته می‌شود (جی‌پست، ۱۳۸۵ ش.)، اما در سوی دیگر، مشخص نیست که اگر سرقت اطلاعات نظامی در یک کشور که می‌تواند تبعات خطرناکی نیز در پی داشته باشد، در زمره کدام تهدیدات در نظر گرفته می‌شود؟ زیرا تخریب و وقوع حملات مسلحانه به عنوان مشخصه تهدیدات در نظر گرفته شده که نمی‌تواند چندان گویا و جامع باشد. همچنانکه نمی‌توان درباره سرقت و یا دستکاری در اطلاعات مربوط به دانش هسته‌ای کشورها به عنوان مصادیق حملات سایبری قضاوت نمود. یکی دیگر از پیچیدگی‌های حقوقی مربوط به تهدیدات سایبری آن است که مفهوم «دفاع مشروع» در این حملات نیز مبهم و پیچیده است و معلوم نیست که برخی اقدامات، از جمله هک‌کردن اطلاعات، دستکاری و سرقت آنان برای کشورهای درگیر در آنچه معنا و مفهومی دارد. به علاوه این‌که معنا و مفهوم تهدیدات سایبری نیز از منظر کشورهای مختلف متفاوت است. به عنوان مثال، تهدیدات سایبری علیه برنامه هسته‌ای ایران معنا و مفهوم متفاوتی نیز به تهدیدات سایبری علیه برنامه هسته‌ای پاکستان دارد.

نتیجه‌گیری

بر مبنای سؤال پژوهش حاضر می‌توان چنین پاسخ داد که وجود برخی قوانین حقوقی و نهادهای بین‌المللی از جمله کنوانسیون بین‌المللی جرائم سایبری و سازمان مالکیت فکری در حیطه حملات سایبری و مالکیت فکری مؤثر هستند و می‌توانند به عنوان فرصت در نظر گرفته شوند، اما خصلت پنهان و پیچیدگی جرائم و تهدیدات سایبری و همچنین فقدان نهاد بین‌المللی قانونی در این زمینه، برخی جنبه‌های تهدیدات سایبری را نادیده گرفته است و از این جهت برای مقابله با این تهدیدات خلأهای قانونی مشاهده می‌شود. به علاوه، خصیصه فراملی بودن تهدیدات سایبری سبب شده است دغدغه اصلی دولت‌ها و کشورها از سطح ملی و حاکمیتی فراتر رفته و عرصه بین‌المللی که با چالش‌های عدیده‌ای در این زمینه مواجه گردیده است، بیش از پیش مرکز توجه آنان قرار گیرد. بنابراین منطق حاکم بر پیشگیری بین‌المللی از تهدیدات سایبری نیز متفاوت از فضای داخلی کشورها می‌باشد.

این در حالی است که فضای بی‌مرز سایبر، جهانی مجازی و موازی با جهان فیزیکی ایجاد نموده است که در واقع کنترل حقوقی آن از حیطه اعمال یک کشور ساخته نیست و مبارزه با جرائم مربوط به این حوزه نیز خارج از حوزه اجرایی قوانین داخلی کشورها خواهد بود. به عبارت دیگر عرصه حقوق فضای سایبری و جرائم ارتکابی در آن از جمله حوزه‌هایی است که به دلیل جهانی‌شدن و آثار آن، نیازمند تصویب قوانین و مقررات متحدالشکل در فضای ملی و بین‌المللی می‌باشد.

در حیطه داخلی نیز لزوم مشخص‌نمودن جرائم و تخلفات مرتبط با مالکیت فکری و تهدیدات سایبری هستیم. جرائم رایانه‌ای نیازمند سخت‌گیری بیشتری

هستند تا بتوانند اولاً قوانین بین‌المللی را مد نظر قرار دهند، زیرا تهدیدات سایبری به گونه‌ای هستند که از سوی بازیگران خارجی نیز ممکن است به مالکیت فکری آسیب برسانند. به علاوه، مشخص‌نمودن جرائم و تخلفات مرتبط با نقض مالکیت فکری و تهدیدات سایبری در قوانین داخلی می‌بایست مورد توجه قانونگذار باشد.

به هر ترتیب، برای حاکمیت بر این فضا و قانونمندنمودن و همچنین مقابله با جرائم روزافزون و پیچیده ارتکابی در آن، همکاری و همراهی جامعه بین‌المللی از اصول اولیه و غیر قابل انکار در این زمینه است، به گونه‌ای که تحت قوانین مدون و موضوعه بین‌المللی هیچ مجرمی با سوءاستفاده از خصیصه فرامرزی‌بودن جرائم ارتکابی نتواند بدون مجازات بماند. در حیطه بین‌المللی نیز، منطقی‌ترین گزینه برای ایجاد گفتمانی واحد و هماهنگ با هدف پیشگیری بین‌المللی از جرائم سایبری تبیین راهکارهایی توسط نهادهای ذی‌مدخل بین‌المللی و در رأس آن‌ها سازمان ملل متحد و رکن قضایی آن، یعنی دیوان بین‌المللی دادگستری است که متناسب با شرایط موجود، قوانین موضوعه را تبیین نموده و مجازات‌های متناسب با این‌گونه جرائم را در تصمیمات و آرای مأخوذه ملحوظ نمایند.

در این راستا از جمله مفاد منشور ملل متحد که می‌تواند به عنوان مبنایی برای مبارزه با جرائم سایبری استفاده نمود بند ۴ از ماده ۲ منشور ملل متحد می‌باشد که تأکید دارد کلیه اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد، خودداری خواهند نمود.

از دیگر تهدیدات موجود در فضای سایبر، حملات سایبری می‌باشد که برخی کشورها عقیده بر این دارند که به دلیل مالیت‌داشتن داده‌های رایانه‌ای، هرگونه

حمله سایبری به تأسیسات که باعث تخریب داده‌ها و ورود خسارات فیزیکی و یا جانی به زیرساخت‌های حیاتی کشور شود، برابر با حمله مسلحانه بوده و بنابراین طبق ماده ۵۱ منشور قابلیت دفاع مشروع مسلحانه را حق ذاتی خود می‌دانند.

پی‌نوشت‌ها

1. CPU: Centeral Procesing Unit
2. W.I.P.O: World Intellectual Property Organization.
3. WPPT: WIPO Performances and Phonograms Treaty

فهرست منابع

الف ـ فارسی:

اصلانی، حمیدرضا. (۱۳۸۹ ش.). *حقوق مالکیت صنعتی در فضای سایبر*. تهران: انتشارات میزان، چاپ اول.

امامی، سیدحسن. (۱۳۸۹ ش.). *حقوق مدنی*. تهران: کتابفروشی اسلامیه، ص ۱۹۳.

آیتی، حمید. (۱۳۷۵ ش.). *حقوق آفرینش‌های فکری با تأکید بر حقوق آفرینش‌های ادبی و هنری*. تهران: نشر حقوقدان، صص: ۱۳۳-۱۳۴.

بزرگی، وحید. (۱۳۸۲ ش.). *حقوق مالکیت فکری در سازمان جهانی تجارت*. تهران: نشر میزان، ص ۳۳.

بهمن‌پوری، عبدالله. شادمان‌فر، محمدرضا. پورغلامی فراشبندی، مجتبی. (۱۳۹۳ ش.). بررسی فقهی ـ حقوقی مال‌بودن داده‌های رایانه‌ای. *فصلنامه فقه و مبانی حقوق اسلامی*. سال چهل و هفتم، شماره دوم، صص ۲۴۴-۲۳۱.

جعفری لنگرودی، محمدجعفر. (۱۳۸۸ ش.). مبسوط در ترمینولوژی حقوق. تهران: انتشارات گنج دانش، جلد سوم، چاپ چهارم، ص ۳۵.

جعفری، افشین. (۱۳۸۸ ش.). *نقش شبکه اینترنت در توسعه آموزش حقوق بشر*. پایان‌نامه کارشناسی ارشد، تهران: دانشگاه پیام نور.

جی پست، دیوید. (۱۳۸۵ ش.). هرج ومرج، دولت و اینترنت، جستاری در باب قانونگذاری در فضای شبکه‌ای. مترجم پرویز علوی. *فصلنامه علمی پژوهشی دانشگاه آزاد اسلامی واحد آشتیان*. پیش‌شماره اول، صص ۴۴-۳۲.

دزیانی، محمدحسن. (۱۳۷۶ ش.). *جزوه جرائم رایانه‌ای*. گزارش دستاوردهای شورای اروپا در ارتباط با توصیه‌نامه ۹(۸۹). تهران: شورای عالی انفورماتیک، جلد اول، ص ۱۳۶.

زیبر، اولریش. (۱۳۸۳ ش.). *جرائم رایانه‌ای*. مترجم محمدعلی نوری. تهران: انتشارات گنج دانش، صص ۱۴۴-۱۴۵۵.

شفیعی شکیب، مرتضی. (۱۳۸۱ ش.). *حمایت از حق مؤلف قوانین و مقررات ملی و بین‌المللی*. تهران: انتشارات خانه کتاب ایران، چاپ اول، صص ۱۴-۱۳.

لطیفی، مهدی. (۱۳۸۱ ش.). حقوق مالکیت معنوی. *مجله معرفت*. شماره پنجاه و سوم، صص ۳۰-۱۹.

لایقی، علی‌رضا. (۱۳۸۱ ش.). *کپی‌رایت در کشورهای پیشرفته صنعتی*. تهران: انتشارات خانه کتاب، ص ۱۱.

میرحسینی، حسن. (۱۳۹۱ ش.). *مقدمه‌ای بر حقوق مالکیت فکری*. تهران: نشر میزان، چاپ دوم، ص ۱۹.

نقیبی، سیدابوالقاسم. (۱۳۸۶ ش.). جبران خسارت به حق معنوی، مبانی فقهی و حقوقی. *فصلنامه کتاب‌های اسلامی*. شماره نهم، صص ۳۶-۱۰.

نوروزی، علی‌رضا. (۱۳۸۱ ش.). حقوق مالکیت فکری، حق مؤلف و مالکیت صنعتی. تهران: انتشارات چاپار، ص ۱۳۳.

ب ـ لاتین:

Haney, WS. (2006). *Cyberculture, Cyborgs and Science Fiction: Consciousness and the Posthuman*. Netherlands: Publisher Rodopi, 35-36.

Sultana, I. Sobhan, M. (2012). *Creation of Cross Border Cyber Laws to Combat Cyber Warfare at Regional and Global Levels*. Dhaka: Daffodil International University, 3-19.

Matthew, EH. (2012). *Computer network attack and the Laws of Armed Conflict*. P.9-28.

Osterdahl, I. (1998). *Threat to Peace, Uppsala: Publisher Lustus Forlag*. 85-99.

Zemanek, K. (2010). *Armed Attack, Max Planck Encyclopedia of Public International Law*. Oxford: Publisher Oxford University Press, 21-40.

یادداشت شناسه مؤلفان

افشین جعفری: دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵. (نویسنده مسؤول)

پست الکترونیک: jafariafshin@yahoo.com

علیرضا حجت‌زاده: استادیار دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵.

محمدتقی رضایی: استادیار دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی، تهران، ایران، صندوق پستی ۳۶۹۷- ۱۹۳۹۵.

Legal Approaches to Cyber Threats in the Field of Intellectual Property

Afshin Jafari
Alireza Hojjatzadeh
Mohammad Taghi Rezaei

Abstract

Background and Aim: The Law of the Intellectual Property is one of the types of property rights that are related to the protection and use of human intellectual creations. Given the proliferation of communications, opportunities and threats posed by cyberspace, it is important to examine the legal approaches to cyber threats in the field of intellectual property, which is addressed in this study.

Method: The present research method is descriptive-analytical of applied type and has been done by using the legal rules of intellectual property in the field of cyberspace and library resources.

Ethical considerations: In organizing this research, while observing the originality of the texts, honesty and trustworthiness have been observed.

Results: International conventions and treaties, although known as general approaches and even roadmaps for dealing with cyber threats, do not specifically address the problems of other societies in protecting intellectual property. For this reason, promoting a culture of using cyberspace, determining punishment commensurate with infringement of intellectual property, criminalizing cyber threats, and establishing codified laws to recognize intellectual property as legal elements are essential to protecting intellectual property.

Conclusion: Intellectual property, unlike material property, has more hidden and informal aspects. For this reason, existing intellectual property protection laws are often incomplete or lacking in cyberspace. It seems that we need a coherent and accepted approach in international law by the countries of the world. In domestic law, we also need an intellectual property institution under existing laws. In addition, intellectual property and related laws, including copyright

laws, the publication of content in cyberspace, and the use of the Internet, require more stringent approaches that take into account both international law and law. Treat intellectual property as industrial property.

Keywords

International Law, Cyber Threats, Ownership, Intellectual Property