وب تاریک و چالش‌های فراروی حقوق کیفری

پریسا حاجی زاده[۱]

[۱] کارشناسی ارشد، حقوق جزا و جرم‌شناسی، دانشگاه شیراز
pari.hajizadeh@gmail.com

چکیده

هنگامی که فناوری های ارتباطی مدرن همچون اینترنت توسط مجرمان برای تسهیل فعالیت هایشان استفاده می گردد، مجرمان باهوش به دنبال ابزارهایی هستند که به آنها کمک نمایند فعالیت ها و ارتباطات خود را پنهان نمایند. وب تاریک و فناوری زیربنای آن، نحوه ی انجام جرم و جنایت را تغییر داده است و از آن جایی که برقراری ارتباط از طریق فناوری وب تاریک به طور پیش فرض شامل رمزگذاری و ناشناس بودن است، مجرمان امروزی بیش از پیش به وب تاریک برای فرار از اجرای قانون در هنگام برنامه ریزی و اجرا تکیه می کنند و چالش های بزرگی را برای مجریان قانون در سراسر جهان ایجاد نموده اند. برای دانستن این که چه مشکلاتی پیش روی مجریان قانون در وب تاریک قرار دارد؛ این مقاله نگاهی به تجربه کشور های پیشرو و بررسی چالش های پررنگ در حقوق کیفری را دارد وپیشنهاداتی در این خصوص ارایه می نماید.

کلمات کلیدی: وب تاریک، تحقیقات سایبری، نظارت سایبری، حقوق کیفری.

۱ مقدمه

وب تاریک یا dark web و فناوری زیربنای آن، اساساً نحوه‌ی انجام جرم و جنایت را تغییر می‌دهد. حجم قابل توجهی از جنایات در این فضا، فرامرزی و بین‌المللی است که هریک از بازیگران اصلی آن،شواهد و عواید حاصل از جرم می‌توانند در حوزه‌های قضایی مختلف باشند. در جامعه امروزی که از نظر فناوری زیرکانه است، شیوه انجام جرم و جنایت با سرعت فزاینده‌ای در حال تغییر است. جرایم در وب تاریک، جدیدترین و تکامل‌یافته‌ترین نوع جرایم سایبری است. وب تاریک «مکانی مخفی و ناشناس است که در آن کاربران سایه به خدمات پنهان، دسترسی دارند» [۱]. به‌ویژه، بازارهایی که در آنجا میزبانی می‌شوند یک چالش حقوقی مهم ایجاد می‌کنند. این بازارها مجرمان را قادر می‌سازند تا بدون زحمت، مجموعه وسیعی از کالاها و خدمات غیرقانونی را از خانه خود خریداری کنند یا بفروشند.

فناوری‌ای که زیربنای وب تاریک است، چالشی منحصربه‌فرد برای مجریان قانون در سراسر جهان و قوانین کیفری به طور گسترده‌تر فراهم می‌کند. استفاده از یک شبکه خصوصی مجازی (VPN) در ارتباط با

Tor (“The Onion Router”) برای اهداف رمزگذاری و امنیتی، این امکان را برای مجرمان فراهم می‌کند تا به طور ناشناس، جنایات فرامرزی را انجام دهند و به‌طور قابل توجهی به مخاطبان، فراتر از حد معمول، دسترسی پیدا کنند. آسایشی همچون خانه خودشان. مهم‌تر از همه، استفاده از ارزهای دیجیتال به‌عنوان وسیله‌ای برای پرداخت کالاها و خدمات خریداری شده در وب تاریک، این امر را تسهیل می‌کند. در نتیجه، وب تاریک، چالش‌های جدیدی به‌وجود آورده و همچنین چالش‌های سنتی قدیمی را بارزتر می‌کند.

قانون و فناوری هرکدام پیچیدگی خود را دارند و وقتی در تعامل با هم قرار بگیرند این پیچیدگی بیشتر نیز می‌شود. اگرچه، دفتر مبارزه با مواد مخدر و جرایم سازمان ملل متحد (UNODC) اعلام کرده است که: «مجریان قانون و سیستم عدالت کیفری در بسیاری از کشورها هنوز در موقعیتی نیستند که بتوانند به‌طور مؤثر با بازار آنلاین ناشناس معروف به وب تاریک مقابله کنند» [۲]. بنابراین در ابتدا وب تاریک به عنوان چالش نوظهور تکنولوژی برای حقوق کیفری با رویکرد توسعه دادن به تنظیم این فناوری نوظهور و سپس چالش‌های بارز موضوع را مورد تجزیه و تحلیل قرار می‌دهد که چالش ایجاد شده توسط وب تاریک را برجسته می‌نماید.

۲ وب تاریک، چالشی برای حقوق کیفری

اتاق های گفتگو و خدمات ارتباطی ناشناس در وب تاریک، آن را به یک محل ایده‌آل برای برنامه‌ریزی و هماهنگی فعالیت‌های خطرناک جنایی و تروریستی تبدیل می‌کند. به‌عنوان مثال، وب تاریک، میزبان هکرها و هکرها برای استخدام است. در آوریل ۲۰۲۱، یک مرد ایتالیایی به اتهام استخدام یک قاتل در وب تاریک برای حمله به دوست دختر سابقش با پرتاب اسید روی او و مجبور کردن او به استفاده از ویلچر، دستگیر شد. یوروپل با انتشار بیانیه‌ای اعلام کرد که این شهروند ایتالیایی ۱۰۰۰۰ یورو برای استخدام قاتل از یک «وب‌سایت ترور اینترنتی» که در شبکه Tor میزبانی شده بود، پرداخت کرده است.

جرم در وب تاریک یک تهدید جدی برای مجریان قانون است؛ چرا که نخست، فناوری پیچیده مورد استفاده وب تاریک، دامنه وسیع آن، عدم احترام به مرزهای ملی و دشواری بار مسئولیت بر شواهد به‌دست آمده را درپی دارد. دوم، نهادهای بین‌المللی و منطقه‌ای که مسئولیت رسیدگی به جرایم وب تاریک را دارند، صلاحیت‌های محدودی دارند و نمی‌توانند تحقیقات را رهبری نمایند. سوم، تلاش حوزه‌های قضایی مختلف برای مقابله با جنایات فراملی و همکاری با یکدیگر در جهت تسهیل همکاری، مدت‌ها ناکارآمد بوده است. چهارم، در اختیار گرفتن نظارت برای دولت محلی به‌ویژه در صورت قدرتمند بودن از لحاظ ملی در جایی که موضوع فراملی نباشد، اجتناب‌ناپذیر است. پنجم، تکنیک‌های تحقیق و رویکرد نظارتی اتخاذ شده همیشه متناسب نیستند و در برخی موارد تکنیک‌های مورد استفاده با غیرقانونی بودن، محدود می‌شوند. ششم،اگرچه استفاده از بخش خصوصی برای تحقیقات در وب تاریک تا حدودی اجتناب‌ناپذیر است، ولی خطراتی را نیز در پی دارد.

۱.۲ ضرورت نظارت بر وب تاریک

چشم‌انداز اجرای قانون در نتیجه افزایش روزافزون فعالیت‌های مجرمانه از طریق اینترنت تغییر کرده است. در حالی که پیشرفت‌های گسترده در فناوری ممکن است ردیابی مجرمان را متمایز سازد و امروزه وب تاریک به عنوان پدیده‌ی نوظهور تکنولوژی و روی آوردن مجرمان به این فضا، نیاز ورود نظارتی به این فضا را بیش از پیش واضح نموده است و آن استفاده مجرمان از فضای وب تاریک برای حفظ ناشناس بودن و فرار از تعقیب و اجرای قانون است. برای درک بهتر از چالش مجریان قانون، سه نکته را می‌توان برشمرد.اینترنت به دو بخش دسته‌بندی می شود.اول، دنیای قابل رویت یا وب سطحی یا به‌عبارتی surface web یاvisible web و دیگری، دنیای عمیق یا deep web. دنیای قابل رؤیت، هرچیزی است که می‌تواند توسط یک موتور جستجوی معمولی مانند گوگل یا یاهو نمایه شود [۳]. بنابراین، هرچیزی که از طریق موتورهای جستجو، قابل دسترسی باشد، در حوزه‌ی دنیای قابل رؤیت است. فراتر از این دنیا، وب عمیق است. این بخش، شامل بخش باقی‌مانده از وب است که وب سطحی آن را پوشش نمی‌دهد [۳]. این بدان معناست که؛ هرچیزی که از طریق موتور جستجو غیر قابل دسترسی باشد، به‌عنوان بخشی از وب عمیق است؛ این یعنی، هم سرورهای خصوصی که دارای مجوز هستند، اینترانت‌هایی که توسط سازمان‌های مختلف استفاده می‌شوند، یا حتی صفحات معمولی رسانه‌های اجتماعی که کاربران می‌خواهند از عموم مردم پنهان نگه دارند، باشد. بخش آخر وب، وب تاریک است.

وب تاریک، بخش کوچکی از وب عمیق است که عمداً پنهان شده است و از طریق مرورگرهای وب استاندارد، غیرقابل دسترسی است [۳]. کاربران اینترنت بدون استفاده از مرورگرهایی که برای ارایه ناشناس بودن مطلق به کاربر، اختصاص داده شده اند؛ قادر به دسترسی به این بخش از وب نیستند. مرورگرهایی خاص، این ناشناس بودن را برای کاربران فراهم می‌نمایند و وب تاریک را محلی برای فعالیت‌های مجرمانه و چالشی برای مجریان قانون بدل می‌نمایند.

مرورگر Tor یکی از این مرورگرهاست که کاربران تشویق می‌شوند تا با استفاده از آن، هویت خود را پنهان نموده و اتصال امن و رمزگذاری شده ایجاد نمایند. روش پیچیده رمزگذاری در این مرورگر،کاربر را از طریق رایانه‌های سایر کاربران به‌منظور پنهان کردن اطلاعات، هدایت می‌نماید [۶]. اساساً این فرایند را می‌توان مانند یک پیاز در نظر گرفت، با عبور هرلایه، هویت یک فرد را بیشتر پنهان می‌کند. علاوه بر این، مرورگر Tor چالش دیگری را نیز به وجود می‌آورد و آن، تغییر مکان سایت‌هایی است که در آنجا میزبانی می‌شوند و تغییر هر هفته‌ی آن، چالشی برای مجریان قانون در جمع‌آوری شواهد ایجاد می‌نماید؛ بر خلاف وب سطحی که مکان یا IP آن ثابت است.

مطالعه محققان کالج کینگ لندن در سال ۲۰۱۶ برای نشان دادن دامنه این چالش با استفاده از بررسی وب‌سایت های قابل دسترسی از طریق Tor (The Onion Router) نشان داد که ۱۵۴۷ سایت از ۲۷۲۳ سایت فعال در این فضا به عنوان محتوای غیرقانونی طبقه‌بندی می‌شوند [۷]. رایج‌ترین محتویات این وب‌سایت‌ها شامل؛ مواد مخدر،امور مالی غیرقانونی و پورنوگرافی شامل خشونت علیه کودکان و حیوانات است. به‌عبارتی بیش از ۵۰ درصد مواردی که در Tor میزبانی می‌شوند، غیر قانونی و نامشروع است، اگرچه در مطالعات

دیگری این رقم حتی بالاتر نیز می‌رود [۸]. از آن جایی که بازارهای موجود در وب تاریک در فراسوی مرزها فعالیت می کنند و فروش آن محدود به حوزه‌ی قضایی نیست؛ به همین دلیل این بازارها، عامل کلیدی برای جنایات فرامرزی و بین‌المللی هستند. هریک از بازیگران اصلی، شواهد و عواید حاصل از جرم می‌توانند در حوزه‌های قضایی مختلف قرار داشته باشند یا حداقل این طور به نظر می‌رسند.

موارد فوق با استفاده از ارزهای دیجیتال مانند بیت‌کوین به‌عنوان روش پرداخت تشدید می‌شود. آنها جابه‌جایی وجوه را به روشی سریع، ساده و با نام مستعار تسهیل می‌کنند و از سیستم مالی رسمی به‌شدت اجتناب می‌کنند [۹]. چالش‌هایی که وب تاریک ایجاد می‌کند به جرمی که در این فضاست محدود نمی شود و به مجرمان اجازه می دهد جنایات وب سطحی را نیز برنامه‌ریزی یا تسهیل نمایند.

۳ چالش‌های مهم حقوق کیفری

اگرچه داشتن دانش و درک مناسب از وب تاریک و ارزهای دیجیتال توسط مجریان قانون برای بررسی جرایم این فضا آن ها را قدرتمند می‌سازد، درحال حاضر حتی کشورهای پیشرو در عرصه فناوری نیز با کمبود تجربه در سازمان‌های مجری قانون در انجام تحقیقات مؤثر و پیگرد قانونی جرایم مربوط به ارزهای دیجیتال روبرو هستند. بنابراین آموزش مداوم افسران در رابطه با خطرات نوظهور، لازم و ضروری است و نکته‌ی مهم تعامل بخش خصوصی برای رفع شکاف دانش اجرای قانون است. اگرچه چالش‌های حقوق کیفری در قبال جرایم وب تاریک، تقریباً همان چالش های سنتی پیشین است، اما موارد تازه ای نیز به این چالش‌ها افزوده شده که به مهم‌ترین آنها اشاره می نماییم.

۱.۳ چالش بین‌المللی

در سطح بین‌المللی، تحقیقات برعهده اینترپل و در اروپا، یوروپل و مرکز جرایم سایبری اروپایی و در سطح ملی نیز سازمان‌های مجری قضایی کشورهاست. محدودیت صلاحیت این ارگان‌ها (اینترپل و یوروپل) برای مقابله با جرایم وب تاریک،چالش مهمی است. هردو ارگان، صلاحیت خود را از عضویت خود می‌گیرند چراکه نهادی قانونگذار نیستند و به‌تنهایی قدرت اجرایی کمی دارند و در درجه اول یک عملکرد هماهنگ‌کننده دارند.

جنایات بین‌المللی نیازمند پاسخ بین‌المللی هستند. نهادهای بین‌المللی و منطقه‌ای، صلاحیت رهبری تحقیقات در وب تاریک را ندارند و نقش آنها صرفاً کمک به آژانس‌های مجری قانون ملی در همکاری با یکدیگر برای مقابله با جرایم سازمان‌یافته بین‌المللی از طریق انتشار بهترین شیوه‌ها و هماهنگ کردن واکنش آنهاست. بنابراین، اولویت در این مبارزه با قانون ملی هر کشوری است؛ چرا که هیچ مکانسیم بین‌المللی رسمی برای اطمینان از این که حوزه های قضایی اقدامات متقابلی را برای مقابله با جرایم وب تاریک دارند و در حال اجرای آن هستند، وجود ندارد. بنابراین هر حوزه قضایی اختیار دارد که در این امر مشارکت نماید یا خیر و احتمال این که دولت های قدرتمند در این عرصه ابتکار عمل را به دست بگیرند، وجود دارد.

۲.۳ چالش صلاحیت

همان‌طور که برشمردیم، یکی از مسائل اساسی در برخورد با جرایم وب تاریک، این است که یک عنصر فرامرزی وجود دارد. در واقع، هریک از عوامل دخیل در ارتکاب جرم و عواید حاصل از آن، همگی می‌توانند در حوزه های قضایی مختلف باشند. در حالی که روش‌ها تغییر کرده‌اند؛ جهانی شدن و جرایم فرامرزی موضوع جدیدی نیست. دفتر مبارزه با مواد مخدر و جرایم سازمان‌یافته سازمان ملل (UNODC) در این خصوص بیان می‌دارد: «جهانی شدن از مراحل رشد حکمرانی جهانی، پیشی گرفته است و این کمبود فقط نوعی خلاء نظارتی ایجاد کرده است که در آن جرایم سازمان‌یافته فراملی می‌تواند رشد کند» [۸].

اگرچه مجریان قانون به دلیل اختلافات قانونی و فرهنگی برای همکاری با یکدیگر تلاش می‌کنند؛ اما کمک حقوقی متقابل حدود ۷۰ درصد از ابزارهای همکاری بین‌المللی در تحقیقات جرایم سایبری را تشکیل می‌دهد و این روند معمولاً کند است. عوامل چندی در این کندی مؤثر هستند، همچون؛ پیگیری‌های متعدد در نتیجه فقدان اطلاعات یا گزارش ناکافی، کمبود منابع در حوزه قضایی دریافت‌کننده و درخواست میان کشورهایی که قوانین متفاوتی دارند و نیازهای داخلی را برای کمک در اولویت قرار می‌دهند. این در حالی است که زمان در تحقیقات جرایم سایبری برای جمع‌آوری شواهد از ضرورت‌ها محسوب می‌شود.

۳.۳ چالش دستگیری مجرمان وب تاریک

کشورهای پیشرو همچون ایالات متحده از دو طریق عمل می‌نمایند. اول در همه‌ی دستگیری‌های بزرگ مجرمان، رهبری یا کمک کرده‌اند. یکی از روش‌هایی که سازمان‌های مجری قانون در سراسر جهان معمولاً از ان استفاده می‌کنند، تحقیقات مخفیانه در وب است. برای مثال، FBI با دستگیری Ross Ulbricht، خالق جاده ابریشم، در سال ۲۰۱۳ موفق شد پیچیده ترین و گسترده ترین بازار جنایی در آن زمان را کشف نماید [۹]. همچنین در تحقیقات مختلف، مانند «عملیات Onymous» مشارکت داشته‌اند[۱]. در حالی که عملیات مخفی از لحاظ تاریخی، موفقیت‌آمیز بوده است، اما به‌دلیل حضور پلیس مخفی زیادی در اینترنت که باعث مشکوک شدن مجرمان می‌شود، تأثیر این روش نیز کمرنگ می‌شود. اگرچه این تحقیقات، ابزار مفیدی در اجرای قانون در وب تاریک است؛ اما چالش دیگری پیش روی مجریان قانون است و آن عمر کوتاه وب‌سایت‌های این فضاست که به‌دلیل فرار از شناسایی به ۲۰۰ تا ۳۰۰ روز می‌رسد و روند تحقیق را با مشکل مواجه می‌سازد. دوم، ازرویکردی آرام برای تجاوزات سرزمینی حمایت می‌نمایند و موضوع مربوط به زمانی است که تحقیقات وب تاریک شامل دسترسی به دارایی دیجیتالی است. اما در خصوص دسترسی فراسرزمینی برای تحقیقات، کشورها با امضای معاهدات حقوقی، سعی در اجازه تحقیقات بدون اعطای مجوز دارند و این امر در تحقیقات سایبری از ملزومات است.

[۱] عملیات Onymous یک عملیات اجرایی بین‌المللی بود که توسط مرکز جرایم سایبری یوروپل EC3، FBI، و تحقیقات امنیت داخلی اداره مهاجرت و گمرک ایالات متحده رهبری می‌شد. وب‌سایت‌های تاریک مانند جاده ابریشم 2.0، ابر ۹ و هیدرا را هدف قرار داده است.

۴ نتیجه

روشن است که فناوری پیشرفته جهانی، طیف وسیعی از امکانات جدید را برای فعالیت‌های مجرمانه ارائه می‌دهد. وب تاریک و بازارهای آن قهرمانان فعلی هستند که مجریان قانون با آن روبرو هستند. وب تاریک عاملی برای جنایات فرامرزی و بین‌المللی است که در آن بازیگران و عواید حاصل از جرم می‌توانند همچون سایر جرایم در فضای سایبر در حوزه های قضایی مختلف باشند و چالش‌های فراروی حقوق کیفری تقریباً همان چالش‌های سنتی در جرایم فضای وب هستند اما موضوعات جدیدی چون روش پرداخت با ارز دیجیتال و فناوری پیچیده‌ی آن، نیاز مجریان قانون را به روزآمد کردن اطلاعات و دانش تخصصی را بیشتر نموده است و این شکاف با تعامل گروه‌های تخصصی و مجریان قانون تا حدودی برطرف می شود. از طرفی تعامل بیشتر کشورها برای تحقیقات فرامرزی در این خصوص بیشتراز پیش لازم است.

مراجع

[1] Amanda Haasz, Underneath it All: Policing International Child Pornography on the Dark Web, 43 Syracuse J. Int'l. L. & Com. 353 (2016) at 356.

[2] Cara McGoogan, Dark web browser Tor is overwhelmingly used for crime, says study, The Telegraph (2016) http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/.

[3] Daniel Moore & Thomas Rid, Cryptopolitik and the Darknet, Taylor and Francis Online Vol. 58 (2016). http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085.

[4] Danny Bradbury, 'Unveiling the Dark Web' (2014) 4 Network Security 14, 14.

[5] For a more technical and in-depth discussion of how this process works, see: Kristin Finklea, 'Dark Web' Congressional Research Service (10 March 2017), https://fas.org/sgp/crs/misc/R44101.pdf, accessed 26 April 2019.

[6] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) I.& C.T.L. 221, 225.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] United Nations Office on Drugs and Crime, The Globalisation of Crime (Report) (2010) E.10.IV.6, 29, https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf, accessed 26 April 2019.

[8] UNODC, 'World Drug Report 2016' (May 2016) UNODC Doc E.16.XI.7.

[9] Tim Hume, How the FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road, CNN (2013). http://www.cnn.com/2013/10/04/world/americas/

silk-road-ross-ulbricht/index.html, J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.