پیوند نظام کیفری و جاسوسی صنعتی در فضای سایبر: رویارویی یا هم‌کنشی؟

مرضیه جعفرخانی[۱]، حسن عالی‌پور[۲]

[۱] کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشکدگان فارابی، دانشگاه تهران
majafarkhani2@gmail.com
[۲] دکتری حقوق جزا و جرم شناسی، عضو هیئت علمی دانشگاه تهران
hassan.alipour@ut.ac.ir

چکیده

پدیده‌ی جاسوسی صنعتی در چهارراه حقوق کیفری، حقوق مالکیت فکری، اقتصاد و علوم مرتبط با سیاست دانسته می‌شود و چالش این نوشتار از همین‌جا آغاز می‌گردد که؛ نظام کیفری چگونه باید با پدیده‌ی جاسوسی صنعتی روبه‌رو شود؟ در رویکرد رویارویی، جاسوسی صنعتی به عنوان یک رفتار مجرمانه در سه حوزه سنتی، نظامی و سایبری مطرح می‌شود. با این حال عدم تصریح به جاسوسی صنعتی و اقتصادی در قوانین ایران، به استثنای مقررات مرتبط با جرایم نیروهای مسلح، جایگاه قانونی این پدیده را همانند خود جاسوسی مبهم کرده و چهره‌ای دوگانه به این جرم بخشیده است. از سوی دیگر، رویکرد هم‌کنشی انگاره‌ی دیگری را مطرح می‌کند که؛ چون در جاسوسی صنعتی، نقش دولت بیگانه یا عنصر وابسته به آن، تعیین‌کننده و وجه تمایز این پدیده با رفتارهای مشابه است، جاسوسی صنعتی، چیزی جز سیاست دولت‌ها در قبال یکدیگر نیست. از این منظر، جاسوسی صنعتی از جامه‌ی یک بزه به جامه‌ی یک پدیده‌ی تأثیرگذار در روابط کشورها در می‌آید. حاصل پژوهش در موضوع حاضر چنین نمایان میشود که رویکرد نظام حقوقی داخلی در رویارویی در سایه‌ی بزه جاسوسی و با رنگ‌مایه‌ی جرائم علیه امنیت بوده و در عرصه بین‌المللی رویکرد سیاسی کشورها در برابر یکدیگر، حاکم است.

کلمات کلیدی: اسرار صنعتی، جاسوسی صنعتی، فضای سایبر.

۱ مقدمه

با پایان جنگ سرد و اهمیت یافتن تجارت در عرصه داخلی و بین‌المللی، تلاش کشورها از رقابت در زمینه نظامی، به رقابت در زمینه اقتصادی تغییر یافت و تجارت به یکی از زمینه‌های کسب قدرت تبدیل شد. از سال ۱۸۷۵ رقابت بین جاسوسی صنعتی و نظامی آغاز گردید و پس از گونه نظامی و سیاسی آن، موج سوم از جاسوسی را در پیشینه روابط کشورها پدید آورد. به گواه تاریخ «در اواخر قرن ۱۹ مبارزه جدیدی در صحنه

مبارزات جاسوسی پیدا شد و آن ژاپن بود که با توجه به عقب ماندگی‌اش در صنعت، مصمم بود به هر ترتیب، این نقیصه را جبران نماید و خود را به کشورهای پیشرفته برساند. فعالیت ژاپن در این زمینه به اندازه‌ای بود که مجله آنترپریز ارگان صنایع و بازرگانی فرانسه در مورخ ۲۸ اکتبر ۱۹۶۷ نوشت: بیشتر متجاوزین و جاسوسان صنعتی، ژاپنی‌ها هستن» (عالی‌پور، ۱۳۸۹: ۱۷۲).

در جهان کنونی، در یک سو کشورهایی وجود دارند که توان مالی و نیروی انسانی متخصص و مبتکر به قدر کافی در اختیار داشته، مدام در حال تولید علم و صنعت می‌باشند و درعرصه رقابت تجاری نیز، گوی سبقت را از دیگران می-ربایند. در دنیای مدرن که صنعت و فناوری حرف اول را می‌زند، کشور تولید کننده اسرار صنعتی به جهت نوین و انحصاری بودن این اطلاعات به منافع مالی فراوانی می‌رسد. بر همین اساس، سعی در جهت کنترل آنها دارد برای مثال «دولت ایالات متحده از پروژه‌هاي فن‌آورانه شرکتهاي آمريکايي حمايت کرده يا به بهانه حفظ امنيت ملي در معاملات تجاري دخالت می‌کند» (صدیق، ۱۳۹۵: ۸۷).

اما در سوی دیگر جامعه جهانی، کشورهای جهان چندم هستند که توان تولید فن‌آوری ندارند و در اصطلاح مصرف کننده و مشتری فناوری کشورهای جهان اولند. از همین روست که در عرصه بین‌المللی شاهد این هستیم که کشورهایی که توانایی تولید صنعت را ندارند، دست به هرگونه عملی می‌زنند تا از چرخه رقابت عقب نمانند؛ که مهمترین و کارآمدترین آن، ربودن اطلاعات اقتصادی و صنعتی سایر کشورها، علی‌الخصوص از کشورهای پیشرو، می-باشد. براي مثال، «بر اساس مطالعه انجام شده، به طور متوسط دوازده سال کار مداوم و ۲۳۱ میليون دلار سرمايه لازم است تا داروي جديدي وارد بازار آمريکا شود. اين در حالي است که آزمايشگاه‌هاي تايلند، هند و برزيل، پس از عرضه آن دارو در آمريکا، در عرض چند ماه با سرقت فرمول آن، اقدام به تجاري سازي همان محصول مي‌کنند. اين مسئله سالانه چهار ميليارد دلار براي شرکت‌هاي آمريکايي هزينه دربرداشته است» (میرمحمدی و سالارکیا، ۱۳۹۱: ۱۲۸). البته تنها کشورهای ضعیف نیستند که به دنبال اسرار صنعتی رقبا می‌باشند بلکه کشورهای پیشرو نیز پیوسته در حال رصد سایر کشورها می‌باشند؛ معرفی آمریکا به عنوان بزرگ‌ترین جاسوسی صنعتی در سال ۲۰۱۳، گواه بر این مدعاست.

حالی در پژوهش حاضر تلاش شده تا با بهره‌گیری از روش تحلیلی توصیفی در قالب مطالعات نظری، در چند بخش به پیوند جاسوسی صنعتی و فضای سایبر، شاخص‌های جاسوسی صنعتی، رویارویی با جاسوسی صنعتی در عرصه داخلی و بین‌المللی به این سوال پاسخ داده شود که نظام کیفری چگونه باید با پدیده جاسوسی صنعتی روبه‌رو شود و به واقع رویکرد حال حاضر در برابر این پدیده چیست؟

۲ پیوند جاسوسی صنعتی و فضای سایبر

فضای سایبر به عنوان فناوری جدیدی که وارد زندگی بشر شد، تاثیرات فراوانی بر جنبه های مختلف زندگی وی گذاشت. یکی از بسترهای ورود و تاثیر آن، بخش اقتصاد و صنعت بود. به دلیل ویژگی‌های منحصر به فردی که دارد، سرعت و سهولت ایجاد و نگهداری اطلاعات در این فضا بالاست. از همین رو کمک بسیاری به بخش صنعت کرده و پیوند تنگاتنگی پیدا کرده است به گونه‌ای که بسیاری از اطلاعات صنعتی در این فضا صورت می‌گیرد. از همین رو شکل اطلاعات، نحوه نگهداری و حفاظت از آنها نسبت به گذشته تغییرات

فراوان کرده است.

همچنین با ورود فضای سایبر به زندگی بشر، فضای ارتکاب جرم نیز تغییر کرده و از محیط فیزیکی و ملموس به دنیای ناملموس تبدیل شده است همین تغییرات و ایجاد اطلاعات در بستر فضای سایبر، شیوه ارتکاب جرائم را متغیر ساخته است. به عقیده برخی، جرم جاسوسی در محیط سایبر، تحول انقلابی در ساختار سنتی این جرم ایجاد کرده و ماهیت، گستره عمل و حوزه آن را تغییر داده است (Sterken, 2013). اکنون ارتکاب جاسوسی صنعتی نیاز به ورود در فضای نگهداری اطلاعات ندارد با هزینه بسیار اندک و در فضایی هرچه مخفی‌تر، امکان دسترسی به اطلاعات صنعتی به سهولت امکان‌پذیر شده است. جاسوسی اقتصادی و صنعتی در پایان سده بیستم، با پدید آمدن فضای سایبر و همنشینی با مفهوم‌هایی مانند جنگ اطلاعات، جنگ نرم و رزم سایبری، برجسته‌ترین و شایع‌ترین گونه از جاسوسی به شمار می‌رود. فن‌آوری سایبر در تمام ابعاد زندگی بشر رسوخ کرده است و با گسترش اینترنت و ارتباطات سایبری، تاثیر این فضا ملموس‌تر و همه جانبه شده است. تاثیر این فن‌آوری در جرم جاسوسی تا اندازه‌ای است که به عقیده برخی در این جرم «انقلاب ایجاد کرده، که این انقلاب ناشی از تحولی است که در مورد اطلاعات و دسترسی به آنها رخ داده» (Benner, 2015). در حال حاضر جاسوسی سایبری اصطلاحی جدید در حوزه امنیت می‌باشد و تهدیدات سایبری، گونه جدیدی از رفتارها برضد امنیت را در بین کشورها ایجاد کرده است. حملات مخرب و مهم و در عین حال سریع و مبهم، امنیت ملی کشورها را به چالش کشیده است و یکی از بدترین تهدیدات علیه منافع ملی به شمار می‌رود؛ چراکه در حال حاضر حجم زیادی از اطلاعات در این فضا شکل گرفته است، اطلاعاتی مهم که چه بسا سندی فیزیکی از آنها وجود ندارد.

از بعد سیاسی، جنگ سایبری گزاره‌ای است که پیرو تحولات فوق‌الذکر، پا به عرصه سیاست گذاشت چراکه امروزه، رفتارهایی متفاوت از رفتارهای جنگی سنتی به وجود آمده است که البته در مورد تشخیص آنها معیار صریحی وجود ندارد لیکن این دلیل بر نادیده گرفتن سرشت خطر آفرین آنها نیست. به همین دلیل است که در کشوری مانند آمریکا می‌بینیم که در سیاست خود، جاسوسی سایبری را نمونه رفتار جنگی می‌داند و پس از کشمکشی طولانی با کشوری مانند چین، به پیمان بر سر خاتمه جنگ سایبری توافق می‌کند.

۳ شاخص‌های جاسوسی صنعتی

جاسوسی صنعتی به عنوان پیوندگاه چندین حوزه، در سنجش با دیگر پدیده‌های مجرمانه، ویژگی‌های متمایزی دارد که در ادامه به آنها پرداخته می‌شود:

۱.۳ جاسوسی صنعتی در چهره بزه امنیتی

علی‌رغم اینکه هنوز هم برخی از حکومت‌ها امنیت را در گرو حفظ امنیت نظامی می‌دانند و ارتکاب بزه جاسوسی علیه اطلاعات نظامی را تهدید علیه امنیت خود برمی‌شمرند، اما با پایان جنگ سرد و تغییر در منابع قدرت، جاسوسی صنعتی نیز رفتاری ضد امنیت تلقی می‌شود. به عبارت دیگر «برای کشورهایی که اسرار تجاری معنایی برابر با منافع ملی و پیرو آن امنیت ملی دارد، جاسوسی صنعتی در شمار بزه‌های ضد امنیت

ملی است و حتی در ایران با تصریح بیشتر به عنوان گونه‌ای از جرائم نظامی آمده است» (عالی‌پور، ۱۳۹۶: ۲۲۶). بر این اساس، جاسوسی صنعتی از جرائم علیه امنیت است و مشمول سخت‌گیری‌ها و حساسیت‌های قانونگذار در مورد این دسته از جرائم می‌باشد.

این نگاه از این نظرتقویت می‌شود که جاسوسی صنعتی، همان رفتار جاسوسی نسبت به اطلاعات و اسرار صنعتی می-باشد و به نوعی صورت تخصصی جرم جاسوسی است و جاسوسی، تهدیدی علیه امنیت کشور می‌باشد، بنابراین جاسوسی صنعتی نیز به تبع عنوان عام خود، بزهی امنیتی محسوب می‌گردد. همچنین به دلیل اینکه جاسوسی صنعتی همواره پشتوانه خارجی دارد، کشورها این رفتارها را علیه خود، منافی حاکمیتشان می‌دانند و سعی می‌کنند که از کنار آن به آسانی گذر نکنند و برای برخورد شدیدتر با مرتکبین، آنها را در زمره مجرمین امنیتی قرار دهند، چراکه همواره شدیدترین واکنش‌ها در مقابل بزه‌های امنیتی صورت می‌گیرد.

۲.۳ جاسوسی صنعتی در چهره بزه اقتصادی

چالش هویت حقوقی بزه اقتصادی، سبب می‌شود تا مصداق‌هایی که در ذیل آن جای می‌گیرند، گمان‌آور باشند. بیشتر نویسندگان و اندیشمندان نسبت به ارائه تعریف جرم اقتصادی به دشواری آن اذعان نموده‌اند و «اغلب دلیل این دشواری را، گستردگی موضوعات و مصادیق این جرم می‌دانند» (آقایی‌جنت‌مکان، ۱۳۹۶: ۲۸) و برخی دیگر «علت را در مبهم بودن تعریف اقتصاد می‌دانند» (نورزاد، ۱۳۸۹: ۱۷۴).

بطور کلی، «جرم اقتصادی هر رفتاری است که تهدیدی علیه امنیت اقتصادی کشور باشد» (نورزاد، ۱۳۸۹: ۱۷۴)؛ لیکن نهادن مصادیق پدیده‌های زیانبار اقتصادی در دسته بزه‌های اقتصادی، بستگی به نوع نظام حقوقی دارد که به شدت از منابع عمده اقتصادی هر جامعه، متاثر است؛برای مثال جرایم رایانه‌ای یا سایبری در برخی کشورها به عنوان جرم اقتصادی معرفی شده اند چراکه؛ در مواردی حملات رایانه از طریق انتشار برنامه‌های مخرب و موجد اختلال چون ویروس‌های رایانه‌ای ضربه جبران‌ناپذیر و خسارت هنگفتی را به اقتصاد آنها وارد می‌کند. حال آنکه در کشورهایی که اساسا استفاده چندانی از شبکه های رایانه‌ای نمی‌شود و یا اینکه این استفاده به صورت کاملاً محدود می‌باشد، اطلاق جرایم اقتصادی به این طیف از جرائم چندان مورد قبول نمی‌باشد.

در یک جمع‌بندی می‌توان گفت، در نظام حقوقی ایران که اقتصاد هم بخشی از امنیت ملی است، سخن از بزه اقتصادی بدون آنکه این پدیده را در جرگه بزه امنیتی دانست، شدنی نیست. بنابراین هرچند از دید قانون، نشانه‌هایی از قرار داشتن جاسوسی صنعتی در دسته بزه اقتصادی نیست؛ به ویژه آنکه تبصره ماده ۳۶ قانون مجازات اسلامی ۱۳۹۲ که بر پایه بند ب ماده ۱۰۹ این قانون، در مقام شمارش بزه‌های اقتصادی است، به جاسوسی اقتصادی و صنعتی اشاره نمی‌شود؛ اما بخش بزرگی از بزه اقتصادی در ایران همچنان دارای چهره امنیتی است؛ لیکن در این میان پروایی نیست که در یک نظام حقوقی بدون مرز روشن در شناخت طبقه‌بندی بزه‌ها، جاسوسی صنعتی را در جرگه بزه اقتصادی یا بزه امنیتی یا هر دو دانست.

۴ رویارویی با جاسوسی صنعتی

در برابر ارتکاب رفتار جاسوسی صنعتی، چگونگی رویارویی با این پدیده نیز به عنوان جزئی از این پدیده بایستی مورد بررسی قرار گیرد که در زیر بیان می‌گردد:

۱.۴ رویارویی کیفری

با وجود عدم تصریح قانونی در مورد جرم انگاری جاسوسی صنعتی، نمی‌توان این جرم را رفتاری بدون سرزنش تلقی کرد، بلکه باتوجه به عموم عنوان جاسوسی می‌توان این رفتار در زیر عنوان جاسوسی جای داد. البته پیش‌بینی قانونی رفتار جاسوسی رایانه‌ای این مشکل وجود ندارد اما تشخیص موضوع این جرم وابسته به تصویب آیین نامه‌ای گردیده است که در تبصره ۲ ماده ۷۳۱ قانون مجازات اسلامی به آن اشاره شده است که تاکنون این تبصره به تصویب نرسیده است و همین کوتاهی از سوی مرجع مذکور در قانون موجب شده تا اجرای این مواد به حالت تعلیق درآید و در حال حاضر امکان اجرای این مواد وجود ندارد.

به‌طور کلی، ضمانت اجرای جاسوسی صنعتی در ایران بر حسب جایگاه مرتکب و نوع اطلاعات و چگونگی ارتکاب، متفاوت است؛ بطورکلی، بر اساس نقش فضای سایبر و رایانه در ارتکاب بزه، به سراغ قوانین مربوط به جاسوسی سنتی و رایانه‌ای می‌رویم و با توجه به جایگاه مرتکب به قواعد مربوط به جرم‌انگاری نظامیان و موارد تشدید مجازات در ارتکاب جرائم رایانه‌ای توجه می‌نماییم. با این حال ضمانت اجرای اصلی، زندان است. هرچند جاسوسی اقتصادی با انگیزه مالی انجام می‌شود ولی جزای نقدی در اینجا تناسبی با این انگیزه ندارد؛ زیرا جاسوس به ویژه اگر برای دولت بیگانه می‌کوشد، سودش را نه از بزه بلکه از دولت بیگانه می‌گیرد، از این رو جزای نقدی کیفر شایسته‌ای برای این پدیده نیست. جاسوسی اقتصادی برای بیگانه به ویژه برای نظامیان با عنوان دیگری یعنی محاربه مطرح می‌شود و نیز گاه جاسوسی بر پایه گستردگی انجام رفتار و پیآمدهای آن با عنوان حدی افساد فی‌الارض تفهیم می‌شود.

۲.۴ اقدامات پیشگیرانه

بر اساس عبارت معروف که پیشگیری بهتر از درمان است، وفق حکم عقل سلیم قبل از هر تهدیدی، بایستی امنیت را در مقابل آنها افزایش داد، برهمین اساس در مورد اطلاعات نیز باید اقدامات پیشگیرانه صورت گیرد. البته لزوم حفظ امنیت در لفظ «محرمانگی» نهفته است اما منظور از اقدامات پیش‌گیرانه در اینجا مقصود افزایش و نگهداری امنیت در سطحی مطلوب و متناسب با نوع اطلاعات است و چاره‌اندیشی در این مورد، یک قدم قبل از عرصه اصلی ارتکاب جرم است. به عبارت دیگر با اعمال اینگونه تدابیر می‌توان از آسیب‌پذیری اطلاعات کاست و با سخت‌تر کردن ارتکاب جرم نسبت به آنها، به نوعی پیش‌گیری وضعی در مورد آن اعمال کرد. همچنین افزایش نظارت بر این اسرار می‌تواند به نوعی اقدام پیشگیرانه محسوب گردد. در برخی موارد نیز افراد موقعیت‌های خطر را پیش‌بینی می‌کنند و سعی می‌کنند از این موقعیت‌ها بپرهیزند، مانند اینکه دو نفری که در مورد فرمول نوشابه کوکاکولا اطلاع دارند، هم زمان با هم در یک مسافرت هوایی حق شرکت ندارند. مقصود از ارائه این بحث بررسی این نکته است که شناسایی این ضرورت و چاره‌اندیشی قانونگذار

نسبت به این مرحله از تهدید تا چه حد بوده است و این دست از تهدیدات تا چه حد دارای ضمانت اجرا قانونی است. بطور کلی اطلاعات ممکن است داده‌ها[1]ی رایانه‌ای باشد یا اطلاعات فیزیکی و اسناد کاغذی، از همین رو حفظ امنیت در مورد آنها متفاوت صدق می‌کند.

در مورد پیش‌گیری قانونی از ارتکاب رفتارهایی که می‌تواند به ارتکاب جاسوسی صنعتی در فضای سایبر ختم شود، قانونگذار چاره‌اندیشی کرده و در ماده ۷۵۳ ق.م.ا به جرم‌انگاری رفتارهایی پرداخته است که «گاهی زمینه و مقدمه ارتکاب جرائم رایانه‌ای می‌شوند و گاهی تشکیل‌دهنده رفتار اصلی جرائم ناب رایانه‌ای می‌باشند که با توجه به موارد مذکور در ماده می‌توان آنها را در سه عنوان جای داد:

- تولید یا انتشار یا توزیع یا در دسترس گذاری یا معامله نرم افزارهای مجرمانه: در این جرائم، نرم افزارها موضوع جرم هستند؛ البته نه به این معنی که خود دارای ارزش می‌باشند، بلکه به این دلیل که استفاده از آنها پیش‌سازی برای ارتکاب جرم رایانه‌ای قرار می‌گیرند، به جرم‌انگاری رفتار نسبت به آنها پرداخته است.

- فروش یا پخش یا در دسترس گذاری داده های رخنه‌گر : سه عمل مذکور، رفتارهای این جرم هستند که بر روی گذر واژه و داده های رخنه گر صورت می‌گیرند. البته «این سه رفتار راهی برای انجام دسترسی غیر مجاز هستند و دارای موضوع مستقیم نمی‌باشند و تنها به جهت منتهی شدن به دسترسی غیر مجاز، جرم دانسته شده‌اند

- انتشار یا در دسترس قرار دادن محتویات آموزنده جرائم ناب رایانه‌ای: در اینجا نیز، همانند بند قبلی، در این جرم، محرمانگی داده ها و صحت و تمامیت آنها مورد نظر بودن است که، پیش‌بینی این دو رفتار برای بازدارندگی از تهدید آنها بوده است.

اما آنچه ذکر گردید مربوط به حمایت از داده‌های رایانه‌ای است» (عالی‌پور، ۱۳۹۵: ۴۵۲) و در جایی که این اطلاعات در قالب اسرار رایانه‌ای نباشند، فاقد حمایت قانونی هستند و این در حالی است که علی‌رغم گسترش فناوری رایانه هنوز هم بسیاری از اطلاعات در قالب اسناد فیزیکی و کاغذی تهیه و نگهداری می‌شوند که همواره امکان تهدید در مورد آنها وجود دارد که حمایت پیشگیرانه قانونی در مورد آنها صورت نگرفته است.

۳.۴ اقدامات بعد از ارتکاب

به این معنی که سیستم کیفری، پس از تکمیل جرم توسط مجرم کار را تمام شده نداند و به نوعی در صدد به حداقل رساندن آسیب جرم و جلوگیری از پیش‌روی جرم و تکرار جرم برآید؛ مثلاً بتوان اطلاعات لو رفته را به نوعی بازیابی امنیتی کرد و اطلاعات هرچند سوخته را از دسترس فرد مجرم خارج کند و مجرم را تا زمان فراموش شدن اطلاعات در بازداشت نگهدارد، در فضای سایبر نیز می‌توان با تغییر رمزهای عبور و سامانه‌ها و حامل‌های ذخیره اطلاعات این عمل را انجام داد و یا تمامی سامانه‌های الکترونیکی وی ضبط شود و پیگیری

[1] Data

سریع صورت گیرد تا اطلاعات در دسترس وی به سرعت امحاء گردد و اطلاعات ارسال شده احتمالی حذف گردد. همچنین سایر اطلاعات حساس شناسایی گردد تا ضریب امنیت آنها افزایش یابد. چرا که ممکن است مجرم تا زمانی که از ناآگاهی بزه‌دیده مطمئن است به پیشروی خود ادامه می‌دهد.

با توجه به اینکه بخش اعظمی از آسیب‌پذیری ناشی از عدم آگاهی است می‌توان اقداماتی را در جهت آگاه‌سازی افراد انجام داد، مانند اینکه بخشی از اقدامات پیشگیرانه را در قالب الزامات اداری گنجاند؛ همچون لزوم آگاهی و داشتن دانش مورد نیاز در زمینه راه‌های حفظ و تامین امنیت فضای سایبر و بایگانی اسناد محرمانه، آگاهی از تهدیدات سایبری و... به افرادی که به هر نحو به اطلاعات دسترسی دارند.

۵ همکاری یا رویارویی بین‌المللی

در زمینه رویارویی با جاسوسی صنعتی، وجود همکاری بین‌المللی نقشی اساسی دارد؛ چراکه در ارتکاب این جرم، عامل بیگانه، عنصر اصلی رفتار است. در نتیجه کوچکترین پیگیری در مورد این جرم نیاز دارد که پا را از مرزهای یک کشور فراتر گذاشت، عرصه‌ای که قلمرو کشوری دیگر است. در نگاه اول چنین به نظر می‌رسد که جامعه بین‌الملل از چنان پیشرفتی برخوردار است که کشوری بیگانه عرصه جولان مجرمین سایر کشورها نشود و نهادهای بین‌المللی تیزبینانه خلاءهای احتمالی موجود را پر خواهند کرد؛ لیکن اندکی تأمل ما را به نتیجه‌ای عکس می‌رساند.

۱.۵ شورای امنیت سازمان ملل متحد

این شورا، نهادی بین‌المللی است، که بر اساس بند یکم ماده ۳۶ منشور سازمان ملل متحد، «کشور قربانی یا زیاندیده می‌تواند یک جرم را به شورای امنیت ارجاع نماید» و در صورتی که شورای امنیت وضعیت را تهدیدی علیه صلح، نقض صلح یا اقدام تجاوزکارانه تلقی کند، می‌تواند اختیارات خود را بر مبنای فصل هفتم منشور اعمال کند. «هرچند در نظر طراحان منشور ملل متحد تهدید علیه صلح با استفاده از قوای مسلح متعارف محدود بود، اما دامنه آن به تدریج توسعه یافت؛ به نحوی که شورای امنیت می‌تواند با ارزیابی شرایط خاص هر قضیه، هرگونه اقدامی را تهدیدی علیه صلح تلقی کند؛ مانند یک حمله سایبری» (تقی‌زاد، ۱۳۹۵: ص۸۲) لیکن در پذیرش رفتار جاسوسی به عنوان بزهی علیه کشور دیگر از سوی سازمان، تردید وجود دارد؛ چراکه جاسوسی رفتاری اجتناب‌ناپذیر و طبیعی در عرصه بین‌المللی می‌باشد ضمن اینکه ادله اثبات این جرم، همواره مخفی و تا حد زیادی غیر قابل دسترس است. از همین رو، بسیار بعید به نظر می‌رسد که شورای امنیت در زمینه جاسوسی صنعتی ورود کرده و این عمل را تهدید علیه صلح بداند، رویه‌ای که تاکنون در پیش گرفته است.

۲.۵ دیوان کیفری بین‌المللی

گرچه در مورد جرائم ارتکابی در سطح بین‌المللی نهادی تحت عنوان «دیوان کیفری بین‌المللی» وجود دارد. طبق ماده ۵ اساسنامه «دیوان نسبت به چهار جرم نسل‌کشی، جرائم علیه بشریت، جرائم جنگی و تجاوز دارای

صلاحیت است». همچنین «صلاحیت دیوان تکمیلی و در کنار صلاحیت محاکم داخلی می‌باشد و هنگامی که تحقیقات و تعقیبی در سطح ملی انجام می‌شود، صلاحیت نخواهد داشت» (میانی و فردین، ۱۳۹۵: ۵۰).

باتوجه به تعریف ارائه شده از تجاوز بند یک ماده هشت مکرر اساسنامه دیوان کیفری بین‌المللی؛ جاسوسی صنعتی را نمی‌توان نمونه‌ای از رفتار تجاوز دانست، چراکه؛ این عمل نه علیه حاکمیت و تمامیت ارضی یک کشور است و نه علیه استقلال سیاسی. به عبارت دیگر، این عبارات کلی مذکور در ماده را نمی‌توان بیش از حد گسترش داد و به حدی وسیع معنا کرد، که هر رفتار خلافی را علیه یک کشور، تجاوز به حساب آورد و تحت صلاحیت دیوان قرار داد. بر همین اساس «بهتر است که جنایت تجاوز فقط به موارد تجاوز توأم با جنگ یا هرگونه حمله و تهاجم به سرزمین یک دولت و یا اشغال و یا الحاق سرزمینی ناشی از حمله و تجاوز محدود گردد. چراکه گسترش بیش از حد این مفهوم به صلاح هیچیک از دولت‌ها نیست» (شایگانفرد، ۱۳۸۷: ۲۶۱).

بطور کلی در زمینه جاسوسی صنعتی، علی رغم مبتلابه بودن این جرم، همکاری بین‌المللی صریح و جامعی صورت نگرفته است و پشتیبانی دولت‌ها از جاسوسی صنعتی، همچنان پایه چنین همکاری‌ها را سست می‌کند. اینطور به نظر می‌رسد که کشورها تمایلی ندارند تا در این زمینه خود را ملزم به رعایت قواعد بین‌المللی کنند، چراکه؛ برخی از کشورها این عمل را در قانون داخلی خود جرم‌انگاری نکرده که یا ناشی از نقص قوانین و غفلت قانونگذاران بوده یا واقعاً عمل از دید آنها سرزنش پذیر نیست(مانند کشور فرانسه). «از دید برخی، این یک روند طبیعی است که موجبات رشد اقتصادی و صنعتی کشورهای کم توان را فراهم می‌کند و از ایجاد قطب ضعیف و قوی در اقتصاد جهانی جلوگیری می‌نماید» (عالی‌پور، ۱۳۹۶: ص۲۲۵).

به‌راستی در این یک دهه، هیچ پرونده جاسوسی صنعتی باز نشده است چرا که «عنصر سود دولت بیگانه بازدارنده‌ای دیگر در رویه قضایی دانسته می‌شود» (Edelma, 2011: 449) که گاه پیگرد پرونده‌ها را به بن بست می‌کشاند. با آنکه گفته می‌شود از دید «حقوق بین‌الملل راهکارهای چندی هست که برجسته‌ترین آنها مسؤولیت دولت در برابر زیان-های برخاسته از جاسوسی اقتصادی است» (Lotrionte, 2015: 512) ولی این راهکارها هیچ‌یک چهره کیفری ندارد و در هر حال پیگرد و دادرسی نسبت به جاسوسی اقتصادی به ویژه سایبری که بدون حضور مرتکب در سرزمین کشور دیگر است، بزرگ‌ترین چالش فراروی دولت‌ها است.

۶ نتیجه‌گیری

جاسوسی صنعتی در فضای سایبر نسبت به اطلاعات حساس یا اسناد اقتصادی طبقه‌بندی شده متعلق به کشور دیگر است که چهره سیاسی و امنیتی آن کم رنگ شده ولی چهره اقتصادی آن پررنگ گردیده است. از این رو تحت سایه اقتصاد که چهره‌ای جهانی داشته و نیز رقابت های تجاری و صنعتی که معمولاً در حوزه خود، رفتارهای سرزنش‌پذیر نمی شود، قرار گرفته است. نتیجتاً جاسوسی صنعتی در فضای سایبر، پدیده‌ای نیست که بتوان با استفاده از نظام کیفری در سرکوب یا کنترل آن کوشید. از آنجا که دولت‌ها خود در تحقق این پدیده نقش دارند و در این زمینه حتی رقابت می کنند، در نتیجه تعامل و همکنشی سیاستی بس موثرتر از سیاست کیفری در قبال این پدیده است.

دستاورد این نوشتار در ترجمان جاسوسی صنعتی به عنوان رویکرد سیاسی و حقوقی در نظام کیفری کشورها است. به همان اندازه که ذکر جاسوسی صنعتی در قانون مجازات جرایم نیروهای مسلح می تواند نقش نهادهای نظامی در تولید صنعت دفاعی را نشان دهد، از سوی دیگر نبودِ این پدیده در قوانین کیفری دیگر، نشان می‌دهد چندان پدیده ای جدی برای صنعت نهادهای غیر نظامی نیست. به همین منوال برای کشورهای چون ایالات متحده، جاسوسی صنعتی یک بزه بسیار مهم تلقی می شود، چراکه؛ چنین کشورهای بستر شکل گیری اطلاعات عدیده صنعتی است؛ ولی همین نگرش را ممکن است کشوری دیگر چون چین که گرایش به روگرفت برداری دارد؛ نداشته باشد. بنابراین جاسوسی صنعتی خود می تواند به شاخصی تبدیل شود که نشان دهد حقوق کیفری تا چه اندازه از جایگاه و ماهیت اصلی خود دور شده است و به چه میزان به عنوان دستاویزی برای دولت در راستای سخت‌گیری یا سهل‌گیری بدل شده است.

مراجع

[۱] آقایی‌جنت‌مکان، حسین. «اجرای آرای کیفری بزهکاران اقتصادی». دانشنامه علوم جنایی اقتصادی. گردآورنده: امیرحسن نیازپور. تهران: میزان، ۱۳۹۶.

[۲] تقی‌زاد، مهرداد. سازمانهای بین‌المللی و قاعده‌مندسازی فضای سایبر. تهران: خرسندی، ۱۳۹۵.

[۳] شایگانفرد، مجید. «دیوان بین‌المللی کیفری و صلاحیت رسیدگی به جنایت تجاوز». فصلنامه حقوق دانشکده حقوق و علوم سیاسی، دوره ۳۸، ش ۴، زمستان ۱۳۷۸.

[۴] صدیق، میر ابراهیم. «انقلاب سایبری و تحول در پدیده جاسوس». فصلنامه مطالعات راهبردی، ش ۷۱، بهار ۱۳۹۵.

[۵] عالی‌پور، حسن. «جاسوسی اقتصادی». دانشنامه علوم جنایی اقتصادی. گردآورنده: امیرحسن نیاز پور. تهران: میزان، ۱۳۹۶.

[۶] عالی‌پور، حسن. حقوق کیفری فناوری اطلاعات. تهران: خرسندی، ۱۳۹۵.

[۷] قانون تجارت الکترونیکی، مصوب ۱۳۸۲.

[۸] قانون جرائم و مجازات‌های نیروهای مسلح، مصوب ۱۳۸۲.

[۹] قانون مجازات اسلامی، بخش تعزیرات، مصوب ۱۳۷۵.

[۱۰] قانون مجازات اسلامی، مصوب ۱۳۹۲.

[۱۱] میانی، علیرضا و فردین، مینا. «صلاحیت دیوان کیفری بین‌الملل». فصلنامه مطالعات علوم اجتماعی، دوره ۲، ش ۱، بهار ۱۳۹۵.

[۱۲] میرمحمدی، مهدی و سالارکیا، غلامرضا. «سازمانهای اطلاعاتی و توسعه اقتصادی». فصلنامه مطالعات راهبردی، سال پانزدهم، ش ۳، پاییز ۱۳۹۱.

[۱۳] نورزاد، مجتبی. جرائم اقتصادی در حقوق کیفری ایران. تهران: جنگل، ۱۳۸۹.

[۱۴] نیازپور، امیرحسن. دانشنامه علوم جنایی اقتصادی. تهران: میزان، ۱۳۹۶.

[15] K. Benner. “Cyber Spying Road Rules,” benner-on-tech-cyber-spying-road-rules, Bloomberg, 2020, available at: https://www.bloomberg.com.

[16] W. Edelman. ”The Benefit of spying: Defining the boundaries of economic espionage under the Economic Espionage Act 1996,” Stanford Law Revie , vol.63, 2011.

[17] C. Lotrionteatherine. ”Countering state sponsored cyber economic espionage under international law,” N.C.J.I-NT‘LL. & COM. REG, vol. XL, 2015.

[18] Rome Statute of International Criminal Court Done at Rome on, 17 July 1998.

[19] R. Sterken. “the digital revolution in international relation: Chinese accuse of widespread cyber-espionage,” 2018.