رویکردی تطبیقی به جاسوسی صنعتی سایبری از چیستی تا راهکارها

نفیسه کمره‌ای[1] نفیسه محمد نجار[2]

۱. دانشجوی کارشناسی‌ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی، تهران،

n_kamareie@yahoo.com

۲. دانشجوی کارشناسی‌ارشد حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، تهران

nmnajar@yahoo.com

چکیده

در طول تاریخ نمونه‌های بسیاری از جاسوسی صنعتی وجود داشته است و در واقع جاسوسی صنعتی پدیدهٔ جدیدی نیست. اما با گسترش فناوری اطلاعات و ارتباطات به خصوص با گسترش کاربرد رایانه و فضای سایبر زمینه تسهیل و گسترش آن هر چه بیشتر فراهم گردیده است. نوشتار حاضر تلاش دارد ضمن ارائه تعریفی جامع از جاسوسی صنعتی سایبری به بررسی تفاوت‌های جاسوسی صنعتی در فضای سنتی و سایبر بپردازد. در این نوشتار همچنین سعی شده است قوانین موجود در این زمینه در کشور ایران در مطالعه‌ای تطبیقی با قانون ایالات متحده آمریکا مورد بررسی قرار گیرد. هدف اصلی از نگارش این مقاله بررسی خلأهای قانونی موجود در این زمینه می‌باشد. بدین منظور راهکارهایی نیز برای مقابله با این پدیده ارائه گردیده است.

کلمات کلیدی:

فضای سایبر، امنیت سایبری، دفاع سایبری، جاسوسی، جاسوسی صنعتی، اسرار صنعتی و اقتصادی

۱- مقدمه

امروزه در عصر تکنولوژی و اطلاعات صرف هزینه‌های نظامی برای از بین بردن دشمن و فرستادن نیروهای متخصص به داخل خاک کشور متخاصم برای کسب اطلاعات و جاسوسی نظامی کاری پرخطر و دور از منطق به نظر می‌رسد. در جوامع اطلاعاتی معمولاً تمامی مبادلات اجتماعی، اقتصادی، سیاسی و فرهنگی ماهیتاً دیجیتال و وابسته به رایانه شده است. لذا در یک جنگ اطلاعاتی به جای هجوم نظامی، استفاده از شبکه‌های الکترونیکی برای تخریب و یا از کار انداختن اطلاعات دیجیتالی و غیر عملیاتی کردن زیر ساخت‌های اطلاعاتی طرف مقابل که می‌تواند بر ضد یک جامعه یا نیروی نظامی باشد، بهترین راه ممکن در جامعه‌های کنونی است.

اطلاعات و جاسوسی بخش خصوصی در حال تبدیل شدن به بخش مهمی از نظم نوین اطلاعات جهانی است. در حقیقت عرصه جاسوسی، در پی پیشرفت قابل توجه فناوری، تا حدود زیادی خصوصی شده است. امروزه جمع‌آوری اطلاعات از طریق فناوری پیشرفته و استفاده از ماهواره‌ها و وسایل الکترونیکی جای شیوه‌های قدیمی جاسوسی را که آژانس‌هایی مثل سیا دنبال می‌کردند، گرفته است.

پیشرفت نتیجه تلاش‌هاست، حمایت از پیشرفت‌ها با شرایط نهادی و هنجاری در جامعه امری قابل اهمیت است که حداقل در سال‌های اخیر در قالب قوانین و مقررات داخلی کشورها مورد توجه قرار گرفته است.

جاسوسی صنعتی یا اقتصادی، از دسته جرایم بسیار مهم علیه امنیت سایبری کشور و برعلیه اسرار تجاری، به عنوان جرمی که منافع کلان اقتصادی کشور را تهدید می‌کند، به روشنی در قانون کشور ما، تبیین و جرم‌انگاری نگشته است. این در حالی است که به علت پیشرفت صنعتی و اقتصادی چشم‌گیر در کشور، بایستی حمایت‌های کیفری لازم علیه این اقدامات صورت پذیرد.

۲- مفهوم و پیشینه جاسوسی صنعتی سایبری

۲-۱- مفهوم

تجسس در لغت به معنای جست و جوی دقیق و پیگیری خبر، جست و جو برای یافتن اخبار و اسرار دیگران برای گفتن به دیگران است. در اصطلاح فقه، اخبار و اوضاع و احوال گروهی را برای گروهی دیگر بردن و یا همان جاسوسی کردن به نفع دشمن است.[۲۴۶: ۱]

در گستره تعاریفی که برای جاسوسی صورت پذیرفته، این تعریف را می‌توان قدر متیقن تعریف دانست: «رفتار مجرمانه مبتنی براین که شخص اخبار، اطلاعات، اسناد، اسرار، نقشه‌ها و ... را در اختیار دشمن یا بیگانه یا دوست متخاصم و یا افرادی که صلاحیت اطلاع از آنان را نداشته قرار دهد.»[۲۴۷ : ۱]

لذا در حوزه‌ی بین‌المللی، در بعضی معاهدات و قطعنامه‌ها در تعریف جاسوسی از تئوری ذهنی (صرف جمع‌آوری اطلاعات به قصد تسلیم) پیروی شده است. از جمله ماده ۲۹ کنفدراسیون چهاردهم لاهه در مورد قوانین و عرف جنگ‌های زمینی (۱۹۰۷/۱/۱۸) آمده است: «جاسوسی در مورد اقدامات کسی صدق می‌کند که بصورت مخفی و تحت پوشش غیرواقعی اخبار و اطلاعات را در مناطق جنگی به قصد رساندن به دشمن جمع‌آوری کند.»

در پی پیشرفت قابل توجه تکنولوژی عرصه جاسوسی نیز خصوصی شده است. بدین معنا که به جای اهداف امنیتی صرف، جاسوسی در پی اهداف اقتصادی و تجاری برآمده است.

عرصه‌ی اسرار تجاری و نحوهٔ حمایت از این اسرار، یکی از اقدامات را که موجب مسئولیت برای فرد می‌داند جاسوسی صنعتی[1] است. در مفهوم اسرار تجاری، جاسوسی صنعتی عبارت است از هرگونه اقدام به منظور کشف اسرار تجاری یک شرکت از طریق روش‌های پنهانی یا غیر قانونی.

برطبق تعریف FBI[2]، جاسوسی اقتصادی[3] مفید این معناست که یک قدرت خارجی فعالیت‌های اطلاعاتی را علیه دولت آمریکا، شرکت‌ها یا مؤسسات یا اشخاص تبعه آمریکا به هدف دستیابی غیر قانونی به اطلاعات اقتصادی، سازماندهی، حمایت و هماهنگ می‌نماید.

ظهور اینترنت و آمیختگی آن با ارتباطات و نیز برقراری پیوند روز افزون رایانه با دیگر پدیده‌های مجازی مانند ماهواره، امواج و حتی رادیو و تلویزیون، باعث گردید تا واژه فضای سایبر برای نامگذاری همه پدیده‌هایی که به نحوی به رایانه وابسته یا با آن مرتبط هستند؛ به کار گرفته شود. فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصت‌های زیادی را برای یک کشور بوجود آورد به همان میزان نیز می‌تواند تهدیدهای بزرگی را ایجاد کند. جرم سایبر[4] به رفتارهایی که ضد این فضا یا بستر بی مرز و بی‌کران یا توسط آن

[1] . economic espionage
[2] . Federal Bureau of Investigation
[3] . Industrial espionage
[4] . cyber crime

ارتکاب می‌یابد اطلاق می‌شود. در واقع از عمر رواج اصطلاحی جرم سایبری کمتر از دو دهه می‌گذرد [۱۳۰ : ۲]

چالش‌های امنیتی ایجاد شده در فضای سایبر به تناسب ماهیت طراحان آن از ویژگی خاصی برخوردار است. برای مثال بازیگران دولتی معمولاً با اهداف شبه جنگی به طراحی حملات سایبری می‌پردازند. در مقابل هکرها یا گروه‌های تبهکار اقتصادی معمولاً اهداف شبه جنگی نداشته و به دنبال منافع یا انگیزه‌های شخصی خویش می‌باشند.

بنابراین، باتوجه به مطالب فوق‌الذکر، در یک تعریف عام، جاسوسی سایبری عبارتست از جست و جوی غیر مجاز برای آزمودن وضعیت اهداف رایانه‌ای یا ارزیابی سیستم دفاعی رایانه یا رؤیت اطلاعات یا کپی‌برداری غیرقانونی از داده‌های فایل به انگیزه‌های سیاسی یا اقتصادی. بنابراین جاسوسی سایبری شامل وارسی غیرمجاز جهت کشف پیکره‌بندی رایانه مورد هدف یا ارزیابی حفاظت‌های سیستم آن یا مرور و کپی‌برداری غیر مجاز از فایل‌های داده می‌باشد.

جاسوسی صنعتی سایبری، نقطه تلاقی جاسوسی با اهداف اقتصادی در معنای سنتی و محیط سایبر است آنگاه که بستر، ابزار و موضوع جرم متفاوت می‌شود و باید آنها را در فضای سایبر جست و جو کرد. لذا در تعریف جرم جاسوسی صنعتی سایبری، انگیزه و اطلاعات اقتصادی، مخصص آن از تعریف جاسوسی سایبری به معنای اعم می‌باشد.[۱]

۲-۲- پیشینه

نظر به اینکه بررسی پیدایش و سیر تاریخی جرم جاسوسی صنعتی سایبری و چگونگی تحول و تکامل شیوه‌های ارتکاب این نوع جرم در شناسایی ماهیت، تعریف و طبقه‌بندی آن تأثیر به سزایی دارد، در این بخش مورد بررسی قرار خواهد گرفت.

ابتدا شیوه‌های جرم جاسوسی صنعتی بررسی می‌گردد. سپس با مرور تاریخ پیدایش رایانه و جرایم مرتبط با آن به بحث پیرامون جاسوسی صنعتی و جاسوسی رایانه‌ای پرداخته می‌شود.

قانون ثبت اختراعات در فرانسه، مصوب (۱۹۷۱) میلادی که برای اولین بار به تعیین حقوق مخترع و حفظ حقوق مرتبط با وی پرداخته است را می‌توان اولین قانونی دانست که بطور ضمنی جاسوسی صنعتی را در خارج از فرانسه تشویق کرده است. طبق یکی از مواد این قانون «اولین کسی که هر نوع صنعتی را از خارج به فرانسه وارد نماید دارای همان حقوقی خواهد بود که شخص مخترع دارا است.» این ماده بطور ضمنی مشوق جاسوسی صنعتی در خارج از فرانسه می‌باشد. نتیجه تصویب این قانون در واقع افزایش تعداد ثبت اختراعات در سال‌های مختلف پس از آن بود، که سبب شد کشور فرانسه محل هجوم جاسوسان به خصوص جاسوسان انگلیسی قرار بگیرد. از آن جمله می‌توان به سرقت سند اختراع متعلق به نیکل روبر توسط جاسوسان اشاره کرد. سند مذکور مربوط به اختراع کاغذ مخصوصی بطول ۱۲ تا ۱۵ متر که با وسایل الکترونیکی و بدون دخالت کارگر تهیه می‌شد. این امر به دولت انگلیس امکان چاپ اسکناس تقلبی را می‌داد. مسئله حائز اهمیت در مثال مذکور، همکاری جاسوسی صنعتی با جاسوسی سیاسی برای نخستین بار بود. در قرن هجدهم در انگلستان جاسوسی صنعتی به منظور مبارزه برای آزادی علیه بیدادگری انحصار یا طبق اصطلاح آن زمان «غارتگری صنعتی افزایش یافت.[۲] به عنوان اولین اقدام موفقیت‌آمیز در این زمینه می‌توان به لغو انحصار چینی‌سازی درسال (۱۷۹۶) در منچستر اشاره کرد که به جهت مبارزه با ثبت اختراعات و انحصارات، اتحادیه‌ای تأسیس گردید و در واقع اولین اتحادیه‌ای بود که مشوق جاسوسی صنعتی گردید. بدین صورت که گروهی از صاحبان صنایع و بانک‌ها، انجمن تشویق صنایع و بازرگانی را تشکیل داده بودند و به مخترعین جایزه می‌دادند تا از ثبت اختراع خود صرف‌نظر کرده و آن را مخفی نکنند و بالعکس اختراع‌شان را در اختیار عموم قراردهند.[۳]

در نیمه‌ی اول قرن نوزدهم جاسوسی صنعتی رسماً از طرف صاحبان صنایع و کشورها تشویق می‌شد این مسئله به عامل مهم جاسوسی صنعتی و سیاسی مبدل گشت که می‌توان گفت افزایش تعداد ثبت اختراعات در انگلستان همانند فرانسه باعث روئیدن شاخه جدیدی در صنایع شد یعنی صنایعی که در شرف تبدیل به غارتگران صنعتی

---

[۵] . عده‌ای میان واژهٔ اقتصادی و صنعتی قائل به تفکیک شده‌اند. جاسوسی اقتصادی را هماهنگ شده یا اجرایی توسط دولت می‌دانند و عرصه بین المللی برای آن قائلند در حالی که جاسوسی صنعتی یا شرکتی اغلب در سطح ملی یا بین دو کارخانه یا شرکت به منصه ظهورمی رسد. در این نوشتار، از هر یک از این واژه ها، معنای دیگر نیز مراد است .

[۲]. برای نمونه می توان به انحصار بخار ثبت شده به نام وات (واحد اندازه گیری نیروی برق) اشاره کرد که سبب متوقف ساختن استفاده از ساختمان ماشین بخار در صنایع و راه آهن گردید. بدین جهت که در آن زمان پارلمان انگلیس همانند چینی و رنگ، انحصار بخار را از سال ۱۷۷۵ تا ۱۸۰۰ تصویب نموده بود. باتوجه به این وضعیت کاملاً طبیعی به نظر می‌رسید که صاحبان صنایع انگلستان به این فکر بیفتند که لازم است اسناد و اسرار صنعتی را سرقت نمایند و پس از سرقت در برابر صاحبان انحصار از منابع خود دفاع کنند.

[۳]. از آن جمله می توان به پرداخت ۱۴ هزار پوند به توماس لمبو جهت جلوگیری از تجدید انحصار ساخت پارچه های ابریشمی و ۳۰ هزار پوند به جنر جهت جلوگیری از ثبت واکسن توسط انجمن مذکور اشاره کرد.

بودند. با ادامه این وضعیت در اواخر قرن نوزدهم، اهمیت جاسوسی صنعتی مورد تائید عموم قرار گرفت و رقابت میان جاسوسی صنعتی و نظامی آغاز شد. در این زمان، مبارز جدیدی در صحنه مبارزات جاسوسی صنعتی پیدا شد و آن کشور ژاپن بود که به لحاظ عقب‌ماندگی از صنعت مصمم شد به هر نحو و قیمتی که شده، عقب‌ماندگی خود را جبران نموده و به کشورهای صنعتی برسد. ژاپن تا حدودی با دادن وعده سفارش موفق به کسب اطلاعات از اسرار صنایع گردید ولی به جهت نگرانی صاحبان صنایع به خصوص صاحبان کارخانجات کشتی سازی انگلستان و اسکاتلند این رویه قابل استمرار نبود. در نتیجه از شیوه‌های جاسوسی بهره جست. رونق جاسوسی صنعتی در ژاپن را می‌توان مصادف با دوران تفوق و برتری صنعتی انگلستان دانست. هم گام با ژاپن، آمریکائی‌ها نیز اواسط قرن نوزدهم صنایع انگلستان را غارت کردند.[1]

ریشه‌ی آمیخته شدن جاسوسی صنعتی با جاسوسی نظامی را می‌توان در دوره‌ای دانست که دفاتر خصوصی اختراعات در آمریکا برای آلمان و در آلمان برای انگلیسی‌ها کار می‌کردند. زیرا در گذشته ناسیونالیسم مانند امروزه متداول نبوده و کارکردن برای دیگر کشورها حتی در زمینه تحقیقات نظامی تعجب برانگیز نبوده است. با پیشرفت تکنیک‌های نظامی، همبستگی جاسوسی صنعتی و نظامی روز به روز بیشتر شد که بیشترین میزان شدت آن را می‌توان در جنگ جهانی اول مشاهده نمود. هنگامی که طرفین جنگ در جست وجوی سلاح‌های سری برآمدند و به این نتیجه رسیدند که فقط صنایع قادر به تأمین آن نیازها هستند و جاسوسی صنعتی یکبار دیگر اهمیت خود را نشان داد. همزمان با جاسوسی نظامی، سیاسی و صنعتی توسط کشورهای متخاصم در جنگ جهانی اول، کمپانی‌های بزرگ اسلحه‌سازی نیز برای شکست دادن رقیب و حفظ منافع خود، جاسوسی صنعتی وسیعی ترتیب دادند.[2]

در سال‌های پس از جنگ جهانی اول تا شروع جنگ جهانی دوم، فعالیت‌های جاسوسی صنعتی وسعت قابل ملاحظه ای یافتند. به گونه‌ای که برخی از شرکت‌های صنعتی فرانسه وادار به اعمال اقدامات جدی‌تری برای حفاظت و امنیت صنایع فرانسه گردیدند. نکتهٔ حائز اهمیت اینست که دوران بین دو جنگ جهانی، آلمان هیتلری در صنعت جاسوسی صنعتی در اروپا تسلط کامل یافته بود. در صورتی که کشورهای دیگر گویا کمتر متوجه جاسوسی صنعتی بودند و می‌توان گفت همان جاسوسی صنعتی و اقتصادی موجب پیدایش رسوایی‌های عظیم مالی در اروپا گردید. از اوضاع و احوال قبل از جنگ دوم جهانی مشخص است که نسبت به کسب اطلاعات علمی و صنعتی بی‌اعتنایی کرده و علاقه‌ای بدان نشان نمی‌دادند[3]. در دوران بین دو جنگ جهانی برعکس آنچه که در اروپا رخ داد، جاسوسی صنعتی با جاسوسی نظامی و خرابکاری‌های سیاسی به هم آمیخته شده در آمریکا جاسوسی صنعتی به معنای واقعی در حال توسعه بود و محدود به رقابت میان شرکت‌ها شده بود و در واقع می‌توان گفت تقریباً به سطح وسعت کنونی رسیده بود. در آمریکا شرکت‌های بزرگ فعالانه مشغول جاسوسی از یکدیگر بودند ولی لازم است گفته شود که باز هم عامل اصلی جاسوسی، دولت و هدف آن صنایع و بانک‌ها بودند.[4]

درآن زمان قوانین آمریکا موازی با علم و تکنیک پیشرفته نبود و تنها پس از جنگ دوم جهانی بعضی از ایالات عقب‌ماندگی قوانین را برای حفاظت از اسرار صنایع پیشرفته جبران و قوانینی وضع نمودند. اما در ایالت کالیفرنیا عقب‌ماندگی قانون از علوم برای حفاظت صنایع محسوس نبود زیرا در سال (۱۸۶۲) قانونی درآن ایالت وضع شد بطوری که طبق آن قانون، اشخاص یا شرکت‌ها مجاز به دایر نمودن

---

[1]. انگلستان برای جلوگیری از ادامه این وضعیت قانونی را تصویب کرد که از صدور ماشین‌های بخار و سایر ماشین ها و نقشه‌های ماشین سازی و نساجی جلوگیری به عمل می آورد. نتیجه تصویب قانون ذکرشده، توسعه ی صدور ماشین آلات به صورت قاچاق و در نهایت افزایش مهاجرت صنعت کاران و کارگران متخصص از انگلستان بود که اغلب به امریکا مهاجرت می کردند. می توان این وضعیت را همانند قاچاق استراتژیک فرار مغزها در زمان حاضر دانست که دعوت به آمریکا در قرن نوزدهم نیز وجود داشته است.

[2].نمونه آن اسلحه فروشان عمده ماکسیم وزاخارف بودند که قبل از جنگ نیز دستگاه جاسوسی بسیار منظم و وسیعی داشتند و هر دو کمپانی بزرگ انگلیسی بودند

[3]. این مطلب از آنجا آشکار شد که وقتی اخباری مبنی بر اینکه ممکن است آلمان به دستگاههای رادار مجهز شده باشند به انگلستان رسید ؛ سرویس مخفی انگلستان نتوانست میان مأموران خود شخصی را پیدا کند که واجد شرایط و معلومات کافی و تخصص لازم در الکترونیک باشد و در نهایت مخترع رادار انگلیسی روبرت واتسون شخصاً مجبور شد جهت جمع آوری اطلاعات به کشور آلمان سفر کند. در همان زمان ، روسها که از جاسوسی صنعتی و نظامی کاملاً در امان بودند با خاطری آسوده راکت (همان سلاحی است که ما در اصطلاح نظامی، موشک می نامیم.) می ساختند تا بتوانند تانک های متجاوزین را متوقف کنند و پس از آن به تسخیر فضا بپردازند. می توان گفت اگر در آن زمان امکان جاسوسی صنعتی و نظامی در اتحاد جماهیر شوروی وجود داشت بطور قطع آلمان ها از آن استفاده می کردند و در آن صورت راکتهای شوروی تا آن اندازه نوظهور به نظر نمی رسید. اما در تمام دوران قبل از جنگ، در طول جنگ و پس از آن تشکیلات سرویس های ضد جاسوسی شوروی می توانستند راز راکت‌ها را کاملاً مخفی نگاه دارند.

[4]. درآن هنگام ، آزمایشگاهها بیشتر از کارخانجات مورد توجه جاسوسان قرار می گرفتند و بیشتر اختراعات از آزمایشگاهها سرقت می شد و بیشتر سرقتها نیز مربوط به پلاستیک سازی بود چون در کارپلاستیک سازی، رقیب می توانست پلاستیک جدید را زودتر از خود مخترع تولید و به بازار عرضه کند.

خطوط تلگراف بدون تحصیل مجوز نبودند. بعداً همان قانون مورد استفاده حمایت از صنایع و جلوگیری از جاسوسی صنعتی قرارگرفت. بعدها با گسترش وسایل و فناوری اطلاعات و ارتباطات از جمله رایانه، فضای سایبر و اینترنت زمینه تسهیل جاسوسی صنعتی بیش از پیش فراهم گردید. وقتی در خصوص فناوری بحث می‌شود؛ نمی‌توان رایانه را نادیده گرفت. رایانه هم خود بزرگترین فناوری عصر حاضر است و هم سایر فناوری‌های نوین یا به وسیله آن و یا در بستر آن شکل می‌گیرند. رایانه‌های نسل نخست از دهه (۱۹۴۰) میلادی برابر با دهه (۱۳۲۰) شمسی وارد بازار شد. شمار این نوع رایانه‌ها اندک، حجم آن بسیار، قیمت آن گران و شمار افرادی که چگونگی کار با آن را می‌دانستند؛ اندک بود [۳۰ : ۳]. اما با گسترش سریع فناوری، رایانه‌های نسل دوم و سوم و چهارم به بازار آمدند که هر یک از خصایص ویژه‌ای برخوردار بودند. پس از ساخته شدن رایانه‌های نسل جدیدی که قابلیت ارتباط با دیگر رایانه‌ها را داشتند، شبکه‌های رایانه‌ای به وجود آمدند. استفاده از اینترنت و ارتباط میان شبکه‌ای موجب انقلابی بزرگ در فناوری اطلاعات و ارتباطات گردید البته فناوری‌های نوین در کنار مزایای خود می‌توانند بستر ساز سوءاستفاده‌هایی نیز باشند. به خصوص اگر این فناوری رایانه باشد؛ دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین امروزه با جرایم و مجرمان رایانه‌ای طرف است. از آن جمله می‌توان به جاسوسان رایانه‌ای اشاره کرد که گاه بوسیله رایانه و گاه با هدف قراردادن رایانه مقاصد خود را عملی می‌سازند. برای مثال می‌توان به کرم‌های نرم‌افزاری رایانه‌ای استاکس نت، دیوکیو[1] که با هدف وارد کردن خسارت به ساختارهای صنعتی ایران طراحی شده بودند، اشاره کرد. این مسئله بیان‌گر اهمیت تأمین امنیت شبکه‌های رایانه‌ای در کشور و در محافل فناوری اطلاعات می‌باشد که در ادامه به آن اشاره خواهد شد.

۳- تفکیک جاسوسی صنعتی سایبری از جاسوسی صنعتی کلاسیک

جاسوسی صنعتی سایبری از جرایم ناشی از فناوری است و لذا در رسته جرایم مدرن قرار دارد. مؤلفه‌های فارق جرایم مدرن با جرایم سنتی یا کلاسیک به شرح آتی می‌باشد:

فعالیت مجرمانه در فضای سایبر قابلیت پنهان ماندن موقعیت جغرافیایی و در نتیجه هویت مجرم را به او می‌دهد. این فضا، امکانات نامحدودی بر اقدامات بزهکارانه افراد ارائه می‌کند تا ارضای امیال شخصی خود را به روح تعاون و اشتراک منافع در فضای سایبر مقدم دارند.

سرعت و پیچیدگی ماهیت جرایم سایبر و فرامکانی بودن آنها، چهره جرایم سایبری را از جرایم کلاسیک متمایز می‌کند. بنابراین پندار یک بزهکاری خارج از کنترل، واقعیتی آشکار می‌یابد بدین سان این اندیشه که جرم دیگر حد و مرزی ندارد تقویت می‌شود. و این بدان معناست که قوانین کیفری ملی دولت‌ها دیگر نمی‌تواند اینگونه بزهکاری را کنترل کند. جاسوسی شبکه‌ای که ذیل عنوان جرایم سازمان یافته فراملی[2] می‌گنجد به منزله پدیده‌ای پیچیده در پی فرا ملی شدن بزهکاری، حاصل مدرن‌گری و پدیده جهانی شدن است. جهانی شدن جرم را می‌توان به منزله در هم تنیدگی و یا وابستگی فزاینده جرم در سرتاسر جهان در نظر گرفت. جاسوسی شبکه‌ای در جنگ اطلاعاتی نقش مهمی را ایفاء می‌کند.

عوامل دیگر تفکیک دو حوزه، لزوم دانش، فناوری و تخصص در ارتکاب جرم سایبری، ناشناخته بودن بسیاری از جنبه‌های این پدیده نوظهور، وهمچنین نرخ وقوع جرم است. شرکت‌ها و آژانس‌های دولتی و غیردولتی هر روزه به صورت ناشناخته مورد حمله و تجاوز قرار می‌گیرند. فرصت‌های اقتصادی خود را از دست می‌دهند و اسرارهای آنها در اختیار رقبایشان قرار می‌گیرد. این امر بزرگترین انتقال دارایی در قالب مالکیت معنوی کشورها در تاریخ بشر لقب گرفته که مقیاس این انتقال، بسیار بسیار ترسناک است. ۲۳۷/۰۰۰/۰۰۰ حمله امنیتی، عدد گزارش شده توسط IBM در نیمه نخست سال (۲۰۰۵) می‌باشد. سرویس‌های مالی با ۳۴/۰۰۰/۰۰۰ حمله رتبه سوم را به خود اختصاص داده‌اند. پرواضح است نرخ واقعی جرم، رقمی فراتر از این اعداد است.

جاسوسی صنعتی سایبری می‌تواند به هدف تروریسم سایبر و سابوتاژ واقع شود. در واقع جاسوسی سایبری، از شیوه‌های سایبر تروریسم است به عنوان مثال، ورود بدافزار استاکس نت به چند پلنت حساس و راهبردی در ایران می‌توانست موجب خسارات فیزیکی جدی به تاسیسات بزرگ صنعتی شود. این ویروس از طریق بازنویسی

[1] . DUQU

[2] .Crime organized transnational

برنامه‌های هدایت کننده تاسیسات بزرگ صنعتی، باعث وارد آمدن خسارات بسیار جدی به آنها می‌شود.

برخی جاسوسی صنعتی سایبری را از دسته جرایم سنتی که تنها با ابزارهای نوین صورت می‌پذیرد می‌دانند. ابزارهای جاسوسی صنعتی سنتی را می‌توان به دو گروه شخصی و فنی تقسیم نمود. قسم اول، شامل ارتشاء کارکنان برای افشاء اطلاعات محرمانه، استقرار یک جاسوس به معنای کارکنان یک شرکت، سرقت اسناد محتوی اطلاعات محرمانه، تحت نظرگیری پنهانی[1]، شناسایی[2] و استفاده از اخاذی[3] و مزدوری، به کارگیری مسائل عشقی و روش‌های عاطفی با ابزاری چون مردان[4] و زنان[5] خوش سیما. قسم دوم عبارتند از: استراق سمع تلفنی، میکروفن مخفی، تحصیل اطلاعات ذخیره، اتصال یک کابل مخفی و ...

محدودهٔ بالقوه جرایم سایبری، به همان گستردگی سیستم‌های ارتباطی بین‌المللی است، لذا شیوه‌های پیشرفته جاسوسی، روز به روز جای شیوه‌های قدیمی جاسوسی را می‌گیرند. این شیوه‌های نوین از قبیل: مهندسی اجتماعی، بدافزارها، رهگیری داده، افزارهای جاسوسی و کاوش دیتا می‌باشد.

برخی از این شیوه‌ها را به فراخور، مختصر شرحی در پیش است:

۴- بدافزارها[6]

ویروس‌های کامپیوتری[7]: به نرم‌افزارها و تکه‌های اطلاعاتی گفته می‌شود که نوشتن آنها به هدف تخریب یا جاسوسی در سطح شبکه صورت می‌گیرد. پخش ویروس به دو صورت جهنده و راکد است. جهنده به معنای توزیع خود به خود ویروس از ابزار انتقال است و راکد، ویروسی است که می‌بایست نسخه‌ای از آن در سیستم جدید کپی شود و گرنه خود جابجا نمی‌شود. انواع مختلف برنامه مخرب عبارتند از: Virus Email و Macro virus و اسب تروا، ویروس‌های بوت سکتور و پارتشین HAOX (گول زنک‌ها)

کرم‌ها[8]: برنامه‌هایی که با کپی کردن خود، تولید مثل می‌کنند. تفاوت اساسی میان کرم و ویروس این است که کرم‌ها برای تولید مثل نیاز به برنامه میزبان ندارند. کرم‌ها بدون استفاده از یک برنامه حامل به تمامی سطوح سیستم خزیده و نفوذ می‌کنند.

۴-۱- ابزارهای جاسوسی[9]

یکی از ابزارهای جاسوسی keyloggerها هستند. متخصصان انفورماتیک معتقدند، این نوع، بهترین ابزار جاسوسی محسوب می‌شود. keylogger ابزاری است که دنباله کلیدهایی که کاربر بر روی صفحه کلید کامپیوتر می‌فشارد را ثبت می‌کند. این ابزار که به صورت سخت‌افزاری و نرم‌افزاری تولید شده و در دسترس است در موارد متنوع و با کاربردهای مختلف به کار می‌رود. علی‌رغم اهمیت زیادی که این ابزار در سرقت اطلاعات دارد؛ توجه زیادی به آن و تهدیدات ناشی از آن نمی‌شود. شاید دلیل این امر شهرت بیشتر ویروس‌ها، اسب‌های تروا و کرم‌ها و هم‌چنین شناخت بیشتر نسبت به آنهاست.

قابلیت جالبی که تعدادی از keyloggerها دارند گرفتن عکس از صفحه کامپیوتر در فواصل زمانی قابل تنظیم است به این ترتیب مشخص می‌شود که چه برنامه‌هایی بر روی کامپیوتر نصب و در حال اجرا می‌باشد چه فایل‌هایی بر روی desktop دستگاه قرار دارد و چه فعالیت‌هایی بر روی دستگاه انجام می‌شود.

۴-۲- مهندسی اجتماعی[10]

در تدارک یا برنامه‌ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت‌های اجتماعی خاص، سعی می‌کند به اطلاعات حساس یک سازمان دستیابی و به آن آسیب رساند. یک مهاجم با طرح سوالات متعدد و برقراری یک ارتباط منطقی میان آنان، می‌تواند به بخش‌هایی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه یک سازمان دست یابد. وی توانمندی خود را با کسب اطلاعات تکمیلی و تلفیقی با اطلاعات اخذ شده از منبع اول، افزایش می‌دهد. فیشینگ در مفهوم انفورماتیکی که هم تلفظ واژه fishing به معنای ماهی‌گیری است، فعالیتی غیرقانونی است که با استفاده از یک

---

[1] .surveillance
[2] .reconnaissance
[3] .prostitute
[4] .raven
[5] .swallow
[6] . malware

نرم افزارهایی هستند که برای نفوذ یا آسیب به یک نظام رایانه ای بدون رضایت مالکان آنها طراحی شده اند. این اصطلاح ترکیبی از دو واژه Malicious به معنای بدخواهانه و softwareبه معنای نرم افزار است.

[7] . viruses
[8] . worms
[9] . spy ware
[10] . social engineering

تکنیک مهندسی اجتماعی به اطلاعات کاربر دسترسی پیدا می‌کند. با این روش، تمام اطلاعات از طریق سایت جعلی به یک در پشتی (back door) وارد می‌شود و برای مصارف جنایت کاری انفورماتیکی در اختیار هکر قرار می‌گیرد.

۵- ارکان جرم جاسوسی صنعتی سایبری

به طور کلی، قواعد حمایتی کیفری باید، اسرار تجاری را در موقعیت‌های مختلف ملحوظ داشته و دارنده را در هر شرایطی در برابر افشای غیر مجاز، سوء استفاده از اطلاعات محرمانه و سایر جرایم علیه اسرار تجاری، مورد حمایت قرار دهد. در این فرایند گاه اسرار تجاری مال تلقی می‌شود که ممکن است مثلاً در اثر افشای غیر مجاز تلف شود و یا سوء استفاده از آن معادل تجاوز به اموال محسوب گردد. در رویکرد دیگر که غلبه نیز با آن است؛ اسرار تجاری و اقتصادی، اطلاعات ارزشمند و محرمانه‌ای هستند که هر رفتاری علیه آنها، از دسته جرایم علیه امنیت تلقی می‌شود. به عبارت دیگر جرایم علیه اسرار، به لحاظ اختلالی که در نظام اقتصادی کشور ایجاد می‌کند؛ به دسته جرایم علیه امنیت تعلق می‌گیرد و بعد مادی آن اهمیت چندان ندارد.

جاسوسی اقتصادی عنوان شناخته شده‌ای در میان جرایم علیه امنیت داخلی به شمار می‌رود و رکن اصلی آن افشای اسرار کلان اقتصادی کشور برای خارجیان است.

بنابر این اگر ارزش مورد حمایت قانونگذار، حفظ محرمانگی داده و حفظ امنیت[1] سایبری باشد. جرم علیه اسرار صنعتی اقتصادی از جمله جرایم علیه امنیت محسوب می‌گردد و اگر ارزش مورد حمایت قانونگذار حمایت از مالکیت و دارایی افراد باشد؛ در دسته جرایم علیه اموال قرار می‌گیرد.

۵-۱- رکن قانونی

در تاریخ ۹ دی ماه (۱۳۸۲) در عرصه تجارت با رویکرد استفاده از فناوری‌های نوین قانون تجارت الکترونیک به تصویب مجلس رسید که محدوده اعمال آن منحصر به امور تجاری است.

هر چند قانون‌گذار در ماده (۱)این قانون قلمرو شمول آن را گسترش داده و در تعریف قانون تجارت الکترونیک آن را مجموعه اصول و قواعدی می‌داند که برای مبادله آسان و ایمن اطلاعات در واسطه‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود اما قانون ذکر شده در ماده ۶۴ در مقام احصای جرایم مربوط به این حوزه برآمده است و منظور اصلی از جرم‌انگاری مصادیق مذکور در این قانون را که شامل تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و موسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی است؛ حمایت از رقابت‌های مشروع و عادلانه، در بستر مبادلات الکترونیکی ذکر نموده است. از این رو، محدوده اعمال مقررات کیفری منحصر به مبادلات الکترونیکی است. با این توصیف، «بستر تجارت الکترونیکی» یا «بستر مبادلات الکترونیکی» بستری است که در آن هر گونه روابط مالی الکترونیکی صورت می‌پذیرد. [۴:۱۲۷] لذا ماده ۶۴ و ماده مکمل آن یعنی ماده ۷۵ قانون تجارت الکترونیک جاسوسی اقتصادی سایبری در معنای خاص را، در بر نمی‌گیرد و در مقابل جاسوسی صنعتی مابین طرفین را نیز هنگامی در بر می‌گیرد که مبتنی بر یک رابطه مالی قبلی باشد.

تا پیش از تصویب قانون جرایم رایانه‌ای در سال (۱۳۸۸)، علی‌رغم سکوت مقررات کیفری ایران به طور تلویحی در قانون مجازات جرایم نیروهای مسلح مصوب ۸۲/۱۰/۹ می‌توان از جاسوسی رایانه‌ای سراغ گرفت. ماده ۱۳۱ قانون فوق در جایی که اشاره می‌کند: ... هم‌چنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن را ندارند یا افشاء غیر مجاز اطلاعات ... به جاسوسی رایانه‌ای اشاره دارد. جاسوسی رایانه‌ای نظامیان هم از نوع جاسوسی نظامی و سیاسی است و با توجه به تعبیر «افشاء غیر مجاز اطلاعات» هم از نوع جاسوسی صنعتی و اقتصادی [۱۹۰ :۲]. پیش‌تر از آن بند ج ماده (۲۴) قانون فوق‌الذکر، جاسوسی صنعتی در محیط فیزیکی را نیز جرم‌انگاری کرده است.

مبحث سوم قانون جرایم رایانه‌ای به جاسوسی رایانه‌ای می‌پردازد که هرچند به خاموشی قانون‌گذار در این باره پایان داده ولی با توجه به این که موضوع بزه در اینجا تنها داده‌های سری است؛ جاسوسی صنعتی و تجاری را در بر نمی‌گیرد مگر این که مرتبط با امور نظامی و سیاسی باشد.

به لحاظ تطبیقی، در ایالات متحده آمریکا نیز، کنگره صد و چهاردهم در ۴ اکتبر (۱۹۹۶) قانونی را تحت عنوان قانون جاسوسی اقتصادی برای امضاء و تأیید رییس‌جمهور وقت (کلینتون) ارائه نمود و در ۱۱ اکتبر توسط وی امضا شد. این قانون در قالب H.R۳۷۲۳

۱. طبق تعریف کلاسیک، امنیت شبکه به معنای برآورده کردن سه مشخصه محرمانگی، صحت و در دسترس بودن می باشد.

درآمد و در قانون عمومی شماره ۲۹۴-۱۰۴ را به خود اختصاص داد. سایر قوانین مرتبط با جاسوسی صنعتی در ایالات متحده آمریکا عبارتند از:

ـ قانون جاسوسی[1] (۱۹۱۷): تدوین شده در زمینه درگیری‌های نظامی

ـ قانون امنیت ملی[2] (۱۹۴۷): مبنای تاسیس سازمان جاسوسی سیا (CIA)

ـ قانون ملی نقل و انتقال اموال مسروقه[3]

ـ قوانین تقلب پستی[4]

ـ قانون تقلب مخابراتی[5]

ـ قانون کپی رایت[6](۱۹۸۰)،

ـ قانون اسرار تجاری[7]

ـ قانون تقلب و سوء استفاده از کامپیوتر (۱۹۸۴)[8]

ـ قانون تقلب و سوء استفاده از کامپیوتر (۱۹۸۶)[9]

ـ قانون بهبود امنیت و ضد اطلاعات (۱۹۹۴)[10]: که در مقابله با جمع‌آوری، انتقال یا تحویل اطلاعات دفاعی برای کمک به دولت خارجی تدوین شده است.

ـ قانون حفاظت از داده‌های کدبندی شده ژنتیکی[11] مصوب ۲۰۰۸ که از سال ۲۰۱۲ اجرایی خواهد شد و هنوز به مرحله اجرا نرسیده است.

لازم به ذکر است که بیشترین استنادات در دعاوی کیفری به قانون جاسوسی اقتصادی است اما سایر قوانین مرتبط فدرال به محاق فراموشی سپرده نشده اند.

۵-۲- رکن مادی

۵-۲-۱- رفتار:

جاسوسی صنعتی سایبری از حیث تفکیک مراحل عملکرد جاسوس مانند جاسوسی صنعتی کلاسیک می‌باشد. در مرحله اول جاسوسی صنعتی سایبری، مرتکب به قصد به دست آوردن اطلاعات تجاری اقتصادی به سیستم رایانه‌ای قربانی رخنه می‌کند. این مرحله، همان دسترسی غیر مجاز است. مرحله دوم، ارزیابی و تحلیل داده می‌باشد که مهمترین قسمت فرآیند جرم جاسوسی محسوب می‌شود. مرحله سوم، در دسترس قرار دادن داده‌های تجاری و صنعتی برای اشخاص فاقد صلاحیت و یا با اقدام خطرناک‌تری افشاء یا در دسترس قرار دادن داده‌های مزبور، برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنهاست.

ماده ۱۳۱ قانون جرایم نیروهای مسلح (۱۳۸۲) تنها مرحله آخر این فرآیند در جاسوسی صنعتی را جرم‌انگاری نموده است. اما قانون جرایم رایانه‌ای (۱۳۸۸) جاسوسی مرتبط با داده‌های سری را، در هر یک از مراحل دسترسی غیر مجاز، در اختیار قرار دادن برای افراد فاقد صلاحیت و بیگانگان به تفکیک مورد حمایت کیفری قرار داده است.

در ایالات متحده آمریکا قانون جاسوسی اقتصادی مصوب (۱۹۹۶)، در ماده ۱۸۳۲ این قانون، سرقت اسرار تجاری را که در معنای اعم شامل مواردی چون سرقت، تصاحب از طریق خدعه و تقلب، نسخه‌برداری غیر مجاز به هر طریقی، ارسال، مبادله، دریافت، خرید، نگهداری، تحریف و نابودسازی اطلاعات محرمانه صنعتی اقتصادی، می‌شود را جرم دانسته است و هم‌چنین اقدام به شروع چنین جرایمی یا تبانی در ارتکاب آنها توسط افراد طبق این قانون قابل مجازات می‌باشد.

استفاده غیرمجاز اطلاعات و به تعبیری افشاء اطلاعات به طور غیرمجاز، هنگامی که دارا شدن اطلاعات به صورت مجاز صورت گرفته، در قانون جاسوسی اقتصادی آمریکا مطرح نشده است.

بنابراین قانون مذکور از دارا شدن مجاز اطلاعات، مهارت‌ها و دانش از سوی اشخاص، در مواردی که کاربردی راهبردی دارند و ارائه به بیگانگان یا افراد فاقد صلاحیت را چشم‌پوشی کرده است و با این ترتیب این قانون از اطلاعات عمومی و مهارت‌هایی که عرفاً کارکنان یک شرکت یا موسسه می‌آموزند؛ حمایت ننموده است.

۵-۲-۲- موضوع جرم

جرم جاسوسی صنعتی سایبری، اطلاعات و اسرار صنعتی اقتصادی را هدف قرار می‌دهد. در این راستا، در قوانین ایران تنها ماده ۶۵ قانون تجارت الکترونیک مصوب سال (۱۳۸۲)، تعریفی از اسرار تجاری الکترونیکی ارائه داده است.

حمایت عام قانون جاسوسی اقتصادی از اطلاعات صرف نظر از ماهیت مادی و غیر مادی و نوع وسیله نگهداری آنان در ماده ۳-

[1] . espionage act of 1917
[2]. The National security act of 1947
[3] . The interstate transportation of stolen property Act
[4] . The mail Fraud statute
[5] . The Fraud by wire statute
[6] . The copyright Act of 1980
[7] . The Trade secrets Act
[8] . The computer Fraud and abuse act of 1984
[9] . The computer Fraud and abuse act of 1986
[10] . The counter intelligence and security Enhancements act of 1994
[11] . upholding the codificated genetic data's act 2008

۱۸۳۹ شامل این موارد نیز می‌شود. همه اشکال و انواع اطلاعات مالی، تجاری، علمی، فنی، اقتصادی و مهندسی که شامل الگوها، نقشه‌ها، فراگردها، ابزار، برنامه‌ها، فرمول‌ها، طرح‌ها، مدل‌ها، شیوه‌ها، فنون، فرآیندها و رمزها می‌شود، چه ملموس باشد یا غیرملموس و اعم از آن که چگونه ذخیره و گردآوری می‌شود خواه از طریق مادی یا الکترونیک یا گرافیک یا عکس، نوشته یا با سپردن به حافظه مشروط بر آن که:

۱. دارنده آن تدابیر متعارفی در حفظ محرمانگی چنین اطلاعاتی اتخاذ کرده باشد.

۲. اطلاعات ارزش اقتصادی بالقوه یا بالفعل مستقلی داشته باشد، از آن جهت که برای عموم ناشناخته است و به سادگی و از طرق قانونی، توسط آنها، قابل احراز نمی‌باشد.

۵-۳- رکن روانی

رفتارهای جرم جاسوسی صنعتی سایبری باید با عمد انجام گیرد. برجسته‌ترین عنصر رکن روانی در این جرم آگاهی مرتکب به اجزای رکن مادی است. مطابق قانون جاسوسی اقتصادی ایالات متحده آمریکا برای اعلام مجرمیت علاوه بر وجود عنصر مادی از قبیل ربایش تحصیل و تصاحب اسرار باید سه مسئله احراز شود: قصد متهم به ربایش اسرار تجاری و نه اطلاعات فاقد ارزش مالی اثبات شود. (علم موضوعی) دوم قصد ضرر رساندن به مالک از سوی متهم نیز لازم است ولی تحقق ضرر در عالم خارج ضروری نمی‌باشد. با احراز این دو نیازی به اثبات انگیزه سوء یا عداوت متهم وجود نخواهد داشت. سوم وجود علم در رفتارهای مرتکب است. به عبارت دیگر متهم باید به اینکه اطلاعات جزء دارایی اقراد بوده است آگاهی داشته باشد. [۵:۱۴] عامل جدایی عنوان مجرمانه‌ی اقتصادی با سرقت اسرار تجاری در وجود عنصر خارجی یا عامل بیگانه می‌باشد. از این رو سوء نیت خاص در مجرم که عبارت است از کسب منفعت برای عامل بیگانه یا قصد ضرر رساندن به ایالات متحده آمریکا به طبع تصریح قانون مذکور ضروری می‌باشد.

۶- راهکارهای رویارویی با جاسوسی صنعتی و نتیجه‌گیری

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات از طریق سازوکارهای الکترونیکی و تجاری انجام می‌پذیرد. این فضا که از آن با نام فضای تولید و تبادل اطلاعات یاد می‌شود (فتا) در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی قرار دارد. به طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانعی بزرگ پیش روی گسترش کاربرد فناوری اطلاعات و ارتباطات و ورود به جامعه اطلاعاتی خواهد بود. منظور از امنیت فضای تولید و تبادل اطلاعات (افتا) برقراری شرایط و حالتی است که دارایی‌های این فضا از خطرات مختلف محفوظ بماند و برای نیل به این منظور باید ابتدا نقاط ضعف و قوت خود را در حوزه فضای مجازی شناسایی کرده و درصدد رفع نقایص و معایب آن و تقویت توانایی‌ها برآییم. این امر مستلزم انجام طرح‌های پژوهشی و مشارکت همه جانبه بخش‌های حاکمیتی، اجرایی، بخش‌های غیر دولتی و همچنین آحاد شهروندان جامعه است. از جمله:

- ارتقای سطح آگاهی، دانش و مهارت‌های مربتط با (فتا)، امن‌سازی زیرساخت‌های حیاتی در قبال حملات الکترونیکی و شیوه‌های جاسوسی

ـ شناخت تهدیدات ناشی از به کارگیری تکنولوژی اطلاعات و ارتباطات علیه امنیت عمومی و برنامه‌ریزی، سیاستگذاری و هماهنگی میان دستگاه‌های ذی‌صلاح حاکمیتی برای مقابله با این تهدیدات.

ـ طراحی سیستم‌های داخلی در سازمان‌های حساس (اینترانت)

ـ مشخص کردن محدوده دسترسی افراد به اطلاعات بر مبنای میزان مسئولیت آنها

ـ حفظ سرمایه‌های مادی و معنوی اسرار تجاری و مالکیت خصوصی در فتا

ـ گسترش ثبت بیمه داده‌های تجاری، به معنای تعمیم دادن حفاظت مربوط به اموال و اشخاص به داده‌ها.

ـ تقویت دوره‌های دانشگاهی در زمینه افتا

ـ حمایت از تخمین و توسعه در صنایع مرتبط افتا

ـ آموزش، قضات، وکلا، ضابطین و افراد حقوقی در حوزه افتا

ـ اتکا به توانایی‌های دولتی و اهتمام به استفاده از بخش غیردولتی

اهتمام به همکاری‌های داخلی، منطقه‌ای و بین‌المللی با توجه به عدم محدودیت افتا به مرزهای جغرافیایی و تأثیرپذیری آن از حوزه‌های داخلی، منطقه‌ای و جهانی.

ترویج و توصیه توسط دولت ایران به شرکت‌های تجاری جهت پیوستن به مقاوله نامه‌های بین‌المللی.

ـ تشکیل کمیته تخصصی نظارت و کنترل بر تخلفات سرویس دهندگان رایانه‌ای و اینترنتی

ـ راه‌اندازی مجتمع ویژه قضایی جرایم رایانه‌ای همراه با امکانات و تجهیزات مربوط و قضات متخصص با توجه به اهمیت و افزایش جرایم رایانه‌ای.

.حفاظت از داده‌های صنعتی و تجاری سایبری با پیوستن به مقاوله نامه داخلی سازمان تجارت جهانی (WTO)[1]، صندوق بین‌المللی پول (IMF)[2] و ...

فناوری اطلاعات و ارتباطات زمینه تسهیل جاسوسی صنعتی و تعرض به حریم اسرار تجاری را بیش از پیش فراهم کرده است. این مسئله حائز اهمیت است که اطلاعات تجاری را می‌توان از طرق مختلف قانونی به صورت‌های سیستماتیک جمع‌آوری، تحلیل و مدیریت کرد که منابع مختلفی از جمله مقالات منتشر شده در روزنامه‌ها، وب‌سایت‌ها، پایگاه‌های داده‌های تخصصی، اطلاعات اعلان شده توسط اتحادیه و شرکت‌ها و ... را دربرگیرد. شاید بتوان گفت در تئوری مرز اطلاعات تجاری قانونی و جاسوسی صنعتی واضح و آشکار است اما در دنیای عمل گاه این دو حوزه با یکدیگر خلط می‌شوند. با عنایت به اهمیت این مسئله و ضرورت حفاظت از اسرار تجاری و حقیقت انکارناپذیر افزایش جاسوسی صنعتی در دنیای امروز به ویژه پس از گسترش کاربرد رایانه و فضای سایبر، هم‌چنین با توجه به اصل قانونی بودن جرم و مجازات و ضرورت پایبندی به آن نیاز جدی به قانونی احساس می‌شود که به طور کامل مسایل پیرامون جاسوسی صنعتیِ سایبری را پوشش دهد. همان‌گونه که ملاحظه شد قوانین موجود آن گونه که باید و شاید به این مسئله نپرداخته‌اند و هر یک در پرداختن به جاسوسی صنعتی چه در فضای سنتی و چه در فضای سایبر دارای نواقصی هستند. از جمله قانون مجازات جرایم نیروهای مسلح هر چند به جاسوسی صنعتی سایبری اشاره کرده است؛ اما تنها مرحله سوم جاسوسی یعنی افشای اطلاعات را در بر می‌گیرد و در مورد غیرنظامیان قابل اعمال نیست. قانون تجارت الکترونیک تنها در بستر مبادلات الکترونیک قابل اعمال است. قانون جرایم رایانه‌ای نیز با توجه به تصریح داده‌های سری تنها به جاسوسی سیاسی سایبری پرداخته و در رابطه با جاسوسی صنعتی ساکت است. هم چنین قوانین حاضر تنها حفاظت از اسرار، داده‌ها و اطلاعاتی را برعهده گرفته است که اقدامات حفاظتی لازم توسط دارنده آنها اعمال شده باشد. توجه به این نکته ضروری است که گاه ممکن است اطلاعات و اسراری برای اشخاص اعم از حقیقی یا حقوقی اهمیت فوق‌العاده‌ای داشته باشد اما تکنیک، علم و امکانات لازم برای حفاظت از آنها را در اختیار نداشته باشند. با توجه به شرایط و اوضاع و احوال موجود، نیاز جدی به قانونی احساس می‌شود که از تمامی انواع صنایع و اقسام اسرار تجاری در برابر جاسوسان حمایت به عمل آورد.

منابع فارسی

[۱] کوشا، دکترجعفر، بایسته‌های حقوق جزای اختصاصی، تهران، مجمع علمی و فرهنگی مجد، ۱۳۹۰.

[۲] عالی‌پور، دکترحسن، حقوق کیفری فناوری اطلاعات، تهران، انتشارات خرسندی، ۱۳۹۰.

[۳] خرم‌آبادی، عبدالصمد، تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، چاپ بهمن، ۱۳۸۴.

[۴] جاویدنیا، جواد، بررسی جرم‌های مندرج در قانون تجارت الکترونیک، مجله حقوقی دادگستری، شماره ۵۹، تابستان ۱۳۸۶.

[۵] السان، مصطفی، جرایم علیه اسرار تجاری، فصلنامه حقوق، مجله دانشکده حقوق و علوم سیاسی، شماره ۴، زمستان ۱۳۸۷.

[۶] پاکزاد، بتول، تروریسم سایبری، رساله دکتریِ حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۸۸.

[۷] پاکزاد، بتول، جرایم کامپیوتری، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۷۵.

[۸] رهبری، ابراهیم، حقوق اسرار تجاری، تهران، سازمان مطالعات و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، پاییز ۱۳۸۸.

[۹] زیبر، اولریش، جرایم رایانه‌ای، ترجمه نوری، محمد علی نخجوانی، رضا، بختی وند، مصطفی، رحیمی مقدم، احمد، تهران، انتشارات گنج دانش، ۱۳۸۴.

[۱۰] جعفری، امین، اسرار حرفه‌ای و حقوق کیفری اقتصادی و تجاری، فقه و حقوق، سال چهارم، شماره چهاردهم، پاییز ۱۳۸۸.

[۱۱] سلطانی فر، محمد، جاسوسی شبکه‌ای در عصر فناوری اطلاعات، ماهنامه فناوری اطلاعات، شماره شانزدهم، آذر ۱۳۸۵.

[1] . World trade organization

[2] . International Monetary fund

[۱۲] پور رحیم، مریم، اسرار تجاری الکترونیکی در حقوق تجارت الکترونیک، پایان‌نامه کارشناسی‌ارشد حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۸۹.
[۱۳] جمالی، فرزاد، حمایت کیفری از مالکیت صنعتی، پایان‌نامه کارشناسی‌ارشد در حقوق مالکیت فلکری، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۸۸.
[۱۴] برژیه، ژاک، جاسوسی صنعتی، ترجمه فرزانه رضا، تهران، انتشارات جاویدان، ۱۳۵۵.

منابع انگلیسی

[1] Fraumann, E., Economic espionage: security missions Redefined. Public Administration Review, 1997. 57 (4): P. 303-350.
[2] Doyle, C., Cybercrime: A sketch of 18 U.S.C. 1030 and Related Federal criminal laws. The library of U.S. congress, 2008.
[3] Wilson, C., Botntes cybercrime, and cyberterrorism: vulnerabilities an policy issues for congress, 2008.
[4] Edgar, H., and Schmidt, B.C., The spionage statutes and publication of Defen information. Columbia Law Review, 1973. 23(5): P. 929-1087.
[5] Eishcer, J.H., An analysis of the economic espionage act of 1996. Heinonline, 2001.
[6] Dempesy, G., Industrial espionage: criminal or civil Remedies. Australien Institue of criminology, 1999.
[7] Brenner , S.W., and crescenzi, C., Sponsered crime: the futility of the economic espionage Act. Houston Journal interratinal law, 2006. 28(2).
[8] www.cybercriminallaw.net
[9] www.justice.gov
[10] www.gpo.gov
[11] www.cybercrime.gov
[12] www.defense.gov
[13] www.rahavardnoor.com
[14] www.vekalat.com
[15] www.oncle.com
[16] www.cybercriminaljournal.com
[17] www.f PC.state.gov

This page is intentionally left blank