مجله پژوهش و مطالعات علوم اسلامی
سال پنجم، شماره ۴۵، فروردین ۱۴۰۲
ISSN: ۲۶۶۶-۰۰۰۰
www.joisas.ir

اقدامات کشورهای اروپایی در رابطه با جرم جاسوسی صنعتی

ماندانا یکتا [۱]

[۱] کارشناس ارشد رشته حقوق جزاو جرم شناسی دانشگاه آزاد اسلامی واحد لاهیجان

چکیده

جاسوسی صنعتی عبارت است از به کار گیری روشهایی به صورت برنامه ریزی شده و هدفمند برای دسترسی به اطلاعات مهم و سری یک شرکت.در مورد مفهوم جاسوسی صنعتی ، این محققین بازار یابی هستند که غالبا مطالعاتی انجام داده اند و به یافته های ارشمندی دست پیدا کردند.در بازار یابی، مفهومی به نام هوشمندی تجاری وجود دارد که جالب این است که بعضی هوشمندی رقابتی را با جاسوسی اشتباه می گیرند. در صورتیکه در بازاریابی نوین ضمن تاکید بر هوشمندی رقابتی و هوشمندی بازاریابی، بر روی بازاریابی اخلاق مدار و پرهیز از هرگونه اعمال غیر اخلاقی در کسب اطلاعات تاکید می شود. برای این منظور افرادی به عنوان کارآگاه مسئولیت تفحص در کار های داخلی شرکت از یک طرف و جستجو و تفحص در کارهای رقبا را از طرف دیگر به عهده دارند . به این کارآگاهان اصطلاحا، کاروزان حرفه ای هوشمندی رقابتی می گویند که باید ترکیبی از خوب و بد، نقاط قوت و ضعف را منتقل کنند حتی در مواردی که مدیریت ترجیح می دهد در بی خبری باقی بماند. بعلاوه کاروزان حرفه ای هوشمندی رقابتی همراه با پیام خود باید توانایی ارائه ی پیشنهادات و توصیه هایی برای اجرا را داشته باشند. اگر اطلاعات جمع آوری شده استفاده نشوند و یا مورد غفلت قرار گیرند ارزشی نخواهند داشت. در نتیجه هوشمندی رقابتی یک نظم کلیدی برای حفظ شرکت و توسعه ی امتیاز رقابتی در محیط کسب و کار است.

واژه‌های کلیدی: جاسوسی صنعتی، جاسوسی رایانه ای و اقتصادی، قوانین و مقررات.

مقدمه

در هر علم و زمینه‌ای که رایانه می‌تواند تسهیل کنندهٔ بسیار خوبی باشد. نرم افزارهای رایانه‌ای امکان شبیه سازی هر کاری را می‌دهند. از شبیه سازی آزمایشگاهی گرفته تا شبیه سازی سفر به کرات دیگر، همه و همه با رایانه و علم کامپیوتر امکان پذیر است.از طرف دیگر شبکهٔ جهانی اطلاعات موسوم به اینترنت، امکان به اشتراک گذاشتن علم در سطح بسیار وسیع را می‌دهد. بدین ترتیب هر کسی بنا به نیاز و علاقهٔ خود می‌تواند از آن استفاده کند. این شبکه آن قدر توسعه یافته است که در دورترین نقاط هم قابل دسترس است. هم زمان با ورود به هزاره دوم، انسان همچنان شاهد جرم و جنایت های بی شماری است. امروز با فشار دادن یک کلید و وارد کردن چند عدد، می شود به حریم دیگران تجاوز و یا به مال او دست اندازی کرد. حوزه جرایم در زندگی امروز بشر آن قدر پیچیده شده است که قانون گذاران مجبورند تحولات جرم را به صورت مداوم زیر نظر داشته باشند.

در نیروی انتظامی جمهوری اسلامی ایران,اداره کل مبارزه با جرایم خاص و رایانه ای از سال ۱۳۸۱ آغاز به کار کرده است. از نظر سازمان ملل متحد جرم رایانه ای می تواند شامل فعالیت های مجرمانه ای باشد که ماهیتی سنتی دارند. اما از طریق ابزارهای مدرنی مثل رایانه و اینترنت صورت می پذیرند. از طرفی معتقدند سوءاستفاده از رایانه ، هر نوع رفتار غیرقانونی، غیراخلاقی و غیرمجاز مربوط به پردازش خودکار و انتقال داده ها جرم اینترنتی محسوب می شود.

رایانه محصول حیرت انگیز تفکر بشری طی سالیان اخیر است، که امروزه به نحوی شگفت انگیز وارد ساختار زندگی انسانها شده است. ورود این ماشین متفکر به عرصه حیات آدمی اساس زندگی وی را دگرگون ساخته و معضلات ناشی از زندگی در جوامع انسانی را که نیازمند حفظ و دسترسی به اطلاعات گسترده و نیز تسریع در تبادل این اطلاعات است، با سرعت و دقتی بسیار بالا مرتفع کرده است. تبیین شرایط و عناصر جاسوسی صنعتی و اقتصادی در فضای مجازی با رویکرد دستیابی غیر مجاز به اطلاعات اقتصادی و صنعتی و بر هم زدن امنیت کشور.

تبیین رویکرد قوانین موضوعه ایران نسبت به جاسوسی صنعتی و اقتصادی در فضای مجازی بنظر می رسد جاسوسی صنعتی و اقتصادی سنتی با جاسوسی صنعتی و اقتصادی سایبری به دلیل این که در فضا های متفاوتی بوقوع می پیوندند جرایم متفاوتی می باشند. فرض بر این است که صرف دستیابی غیر مجاز به اطلاعات اقتصادی و صنعتی بدون برهم زدن امنیت کشور نمی تواند به عنوان جاسوسی تلقی شود.بنظر می رسد قوانین موضوعه ایران با جرم انگاری جاسوسی صنعتی و اقتصادی در فضای مجازی رویکرد متفاوت خود را با جرم جاسوسی سنتی مشخص کرده است.

۱-تعریف قانونی جاسوسی صنعت

جاسوسی صنعتی، جاسوسی اقتصادی یا جاسوسی ابرشرکتی نوعی از جاسوسی است که با مقاصد بازرگانی انجام می‌شود تا مقاصد صرفاً مرتبط با امنیت ملی - جاسوسی اقتصادی از سوی دولت‌ها انجام یا ترتیب داده می‌شود و حوزه اش بین‌المللی است، در حالی که جاسوسی ابرشرکتی یا صنعتی بیشتر ملی است و بین شرکت‌ها و ابرشرکت‌ها رخ می‌دهد .

" جاسوسی صنعتی " عبارت است از به کار گیری روشهایی به صورت برنامه ریزی شده و هدفمند برای دسترسی به

اطلاعات مهم و سری یک شرکت .مطالعات اخیر نشان داده است که افراد داخل یک شرکت ، مسئول بیش از ۷۰ ٪ از دزدیهای اطلاعاتی از شرکتها بوده اند با توجه به IT محور شدن بیشتر شرکت ها ،اعم از صادراتی و خدماتی و صنعتی،... تا ادارات دولتی ، نقش ارتباطات و اطلاعات در تمامی شرکت ها پر رنگ تر شده است.

با افزایش روز افزون ارتباطات به مراتب ، تبادل اطلاعات نیز بیشتر و بیشتر می شود و تبادل اطلاعات یعنی ارسال یک سری از اطلاعات از یک مبدا مشخص به مقصد مشخص، حال هر چه اهمیت و ارزش اطلاعات مبادله شده بیشتر باشد به تبع آن امنیت ارسال این اطلاعات موضوع حیاتی تری برای سازمان است .

در این میان اگر خدشه ای در این مبادلات صورت بگیرد و اطلاعات و اسرار مهم شرکت چه به شکل عمد و چه به شکل غیر عمد لو برود ، شرکت به نوعی دچار یک حمله ی جاسوسی شده است . چون ماهیت اطلاعاتی که مورد هجوم این نوع حمله ها قرار می گیرند نوعا بیزینسی- صنعتی است مهندسان اجتماعی ، این پدیده را جاسوسی صنعتی نام نهادند.

۲- تعریف فقهی جاسوسی صنعتی

به طور کلی جاسوسی از برخی دیدگاه ها بر دو نوع مشروع و نامشروع است. گاهی این عمل ستوده شده است و گاهی نیز از منظر دیگر مورد نکوهش قرار گرفته است. گروهی از حقوق دانان نیز عقیده دارند که جاسوسی تنها در زمان جنگ نامشروع است ومستوجب مجازات است اما جاسوسی در زمان صلح مجازات ندارد ، زیرا مرتکب آن قصد خدمت به کشور متبوعش را دارد.

مجازات کردن جاسوس در زمان جنگ مورد اختلاف نیست و کلیه قوانین آن را قبول کرده اند ولی نسبت به مجازات آن در زمان صلح از نظر عدالت و از نظر ضرورت تردید شده و می گویند هر فردی مکلف است اطلاعات کافی و مفیدی که از اوضاع کشورهای دیگر به دست می آورد در اختیار مملکت متبوع خود قرار بدهد و این اقدامات همیشه جنبه جاسوسی به منظور دفاع یا حمله نیست (گارو، ۲۹۲۲ش، ص۶۲۲).

۳- تعریف جاسوسی از دیدگاه حقوق بین الملل

جاسوسی در حقوق بین الملل بطور صریح منع نشده است و مقرره خاصی در این خصوص وضع نگردیده است. از دید حقوق بین الملل بویژه حقوق جنگ، جاسوسی عملی مشروع محسوب می شود که هر یک از طرفین مخاصمه برای کسب اطلاعات بیشتر از وضعیت نظامی دشمن می-تواند از این روش استفاده کند و جاسوسان خود را به سمت اردوگاه دشمن روانه کند.بنابراین با اینکه همواره یکی از استراتژیهای مهم در زمان جنگ استفاده مناسب از اطلاعات مربوط به نقاط قوت و ضعف دشمن است که این اطلاعات از طریق جاسوسی قابل دسترسی بوده لیکن طبق بند ۱ ماده ۴۶ پروتکل شماره ۱ الحاقی به عهدنامه های چهارگانه ژنو جاسوس در صورت دستگیری توسط دشمن حق برخورداری از رفتار مربوط به اسیران جنگی را ندارد. در مورد منع جاسوسی در دریا نیز باید گفت کنوانسیون۱۹۸۲حقوق دریاها نیز در ماده۳۰۱ خود اشعار میدارد:

کشورهای عضو این کنوانسیون در اعمال و اجرای حقوق و وظایف خود از هر گونه تهدید یا استفاده از زور بر علیه تمامیت ارضی یا استقلال سیاسی هر کشور یا به هر شکل دیگر که مغایر با اصول حقوق بین الملل مندرج در منشور ملل متحد باشد خودداری خواهند نمود. مسلما با توجه به اینکه اقدام به جاسوسی امری غیردوستانه و به عنوان یک اقدام خصمانه تلقی می شود مغایر صریح اصول و مقرره های منشور ملل متحد بویژه مقدمه و مواد ۱و۲ میباشد. این موضوع بویژه در بند ۴ ماده ۲ امری غیر قابل خدشه میباشد:

کلیه اعضاء 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.

۴- صلاحیت کیفری در جرم جاسوسی رایانه ای

صلاحیت کیفری را می‌توان به توانایی و شایستگی قانونی و نیز تکلیف مرجع قضایی، به رسیدگی به یک دعوای کیفری تعبیر کرد. بنابراین نخستین مسأله‌ای که مراجع تحقیق باید به آن بپردازند، بررسی صلاحیت خود جهت شروع به تحقیقات است و در صورتی که خود را صالح به رسیدگی ندانند موظف به اصدار قرار عدم صلاحیتند. ماده ۳۲ قانون تشکیل دادگاه های عمومی و انقلاب، تشخیص صلاحیت را عهده همان دادگاه رسیدگی کننده نهاده است.

این ماده مقرر می‌دارد: «تشخیص صلاحیت یا عدم صلاحیت هر دادگاه نسبت به دعوای مطروحه با همان دادگاهی است که قانوناً مکلف به رسیدگی به پرونده بوده است».

ماده ۳۳ قانون مذکور می‌افزاید: «در صورتی که دادگاه رسیدگی کننده، خود را صالح به رسیدگی نداند با صدور قرار عدم صلاحیت، پرونده را به دادگاه صالح ارسال می‌نماید ...».

در یک رویکرد کلی در خصوص جرایم سایبری می‌بایستی فضای ذهنی قانونگذار را از محیط واقعی و فیزیکی خارج نموده ودر محیط کاملاً مجازی و غیر واقعی قرارداد. از سوی دیگر ماهیت غیر واقعی جرایم سایبری باعث گردیده تا مرزهای جغرافیایی و مفهوم سرزمین های مجزا، رنگ باخته و اصطلاحاً عبارت «صلاحیت غیر مبتنی برمرز» یا «صلاحیت فرامرزی» جایگزین صلاحیت های مبتنی بر حیطه بندی های جغرافیایی سیاسی و طبیعی گردد. چرا که ماهیت جرائم سایبری اصولاً ماهیتی فرامرزی بوده و می‌بایست بدون در نظر گرفتن مکان وموقعیت فیزیکی مرتکب، محل ارتکاب و ... مورد بررسی قرار گیرند .

جرم سایبری به لحاظ ماهیت مجازی وغیر واقعی خود, حقیقتاً نمود عینی و ملموسی، شبیه آنچه در جرایم سنتی مثل ضرب وجرح و یاسرقت و ... مشاهده می‌کنیم از خود به نمایش نمی‌گذارد . بلکه جرم سایبری در واقع در بستر مبادلات الکترونیکی و برروی داده‌ها و اطلاعات وبعضاً (بندرت) بر روی سیستم‌های فیزیکی و سخت افزاری ارتکاب می‌یابد. در جائیکه جرم سایبری برروی داده‌ها ارتکاب یافته ,تعیین محل ارتکاب جرم کاری بس دشوار ودر برخی موارد حتی غیر ممکن بنظر می‌رسد . محل وقوع

جرم سایبری بطور دقیق یعنی محل و مکانی که این داده‌ها دستخوش حملات مجرمانه قرار گرفته ودیگرگون شده‌اند .

اینکه مرتکب دارای چه تابعیتی است در بسیاری موارد کشور متبوع وی را صالح به رسیدگی به اتهامات وی می‌نماید. چنانکه در ماده ۷ قانون مجازات اسلامی نیز رسیدگی به کلیه جرائم ارتکابی توسط ایرانیان در هر کجای جهان را در صلاحیت دادگاه های کیفری داخلی دانسته . اما در جرائم سایبری ,حتی تابعیت مرتکب نیز ناشناخته است . چرا که در فضای مجازی کاربران با شناسه‌های قرار دادی که تماماً مجازی وغیر قابل مشاهده و لمس هستند، شناسایی می شوند و حتی در صورت شناسایی کاربر مرتکب جرم , در واقع ما هویت مجازی و قرار دادی وی راشناسایی کرده‌ایم نه هویت واقعی او را همچنان که در ادارات تشخیص هویت پلیس کشورها صورت می‌پذیرد .

در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی , می‌توان باتأسیس یک هیأت و یاشعبه مرکزی، در خصوص رسیدگی به جرائم سایبری در کشور، که باتوجه به قابلیت‌های تخصصی وامکانات مالی وتجهیزاتی علی القاعده در تهران برپا خواهد شد, به تمامی مراجع قضایی سراسر کشور تکلیف نمود، تا در صورت دریافت هرگونه گزارش از مقامات ذیصلاح و یا وصول شکوائیه و یا مشاهده هرگونه جرمی از جرائم محیط سایبری ,بلافاصله شعبه مرکز ی را در جریان امر قرار داده و منتظر تعیین تکلیف از سوی شعبه مرکزی بمانند.

مبنایی‌ترین و قدیمی‌ترین قاعده‌ای‌که برای اعمال قوانین جزایی مورد استناد محاکم کیفری قرار می‌گیرد، صلاحیت سرزمینی است که ماده۳ ق.م.ا چنین مقرر می‌دارد: «قوانین جزایی درباره کلیه‌کسانی‌که در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی‌ایران مرتکب جرم شوند، اعمال می‌گردد مگر آنکه به موجب قانون ترتیب دیگری مقرر شده باشد» این قاعده با بیان روزآمد و متناسب با جرایم رایانه‌ای در بند «الف» ماده ۲۸ ق.ج.ر نیز تکرار شده است: «علاوه بر مواد پیش‌بینی شده در دیگر قوانین دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

داده‌های مجرمانه یا داده‌هایی‌که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی ج.ا.ا ذخیره شده باشد».

دلیل پذیرش مجازات سرزمینی‌که در کنار تمام سوابق تاریخی آن این است که اصولاً جرم ماهیتی محلی دارد و بهترین شیوه مجازات آن اجرای محلی آن است؛ البته سهولت جمع‌آوری دلایل، قراین و امارات محاکمه‌پسند در کنار تأمین اهداف ارعاب انگیزی و عبرت‌آموزی مجازات را نباید فراموش کرد(جلالی فراهانی، ۸۵: ۹۵). از آن جا که موضوع جرم جاسوسی رایانه‌ای اصولاً داده‌های سری است، از این مطابق بند «الف» ماده۲۸ ق.ج.ر هر زمان‌که داده‌های سری موجود در رایانه‌های ایران یا سیستم‌های مخابراتی و... مورد تهاجم مجرمانه قرار گیرنددادگاه‌های ایران صلاحیت رسیدگی خواهند یافت.

بند ب ماده مزبور اشعار می‌دارد: «جرم از طریق تارنماهای(وب سایت‌های) دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد».

قبل از ورود ماهوی به بند بالا این توضیح ضروری است که وب‌سایت یا معادل فارسی آن تارنما، خلاصه اصطلاح «شبکه جهانی وب» می‌باشد، از این اصطلاح برای تعریف و توضیف اسنادی استفاده می‌شودکه در اینترنت قابل دسترسی بوده و از قالب گرافیکی خاصی(برای نمایش) بهره می‌جوید. این اسناد را می‌توان به کمک نرم‌افزارهایی‌که کاوشگر اینترنتی نامیده می‌شوند نمایش داد.(سالمی‌فیه، ۶۸: ۹۰).

۵- داده رایانه ای

هرنمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای پردازش در یک سیستم رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا بگذارد. مقصود آن است که فرد بزهکار با نقض تدابیر امنیتی و به صورت غیر مجاز به داده‌های حفاظت شده دست یابد. به عنوان مثال، فردی با هک کردن سایت سازمان سنجش، اطلاعات مربوط به داوطلبان کنکور را برباید. همچنین، ممکن است یک بزهکار سایبری اقدام به هک کردن سایت و سیستم یک اپراتور تلفن همراه کرده و سپس اطلاعات و سوابق کاربری یکی از مشترکان را برداشت کند.

۵-۱ شنود غیرمجاز

مقصود از شنود غیرمجاز، آن است که بزهکار محتوای در حال انتقال ارتباطات شخصی را در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی و... شنود نماید. به این ترتیب، دسترسی به رمز ورود پست الکترونیکی افراد و خواندن پیام‌های موجود در آن‌ها، یا دسترسی به ارتباطاتی که افراد از طریق شبکه‌های ارتباطی با یکدیگر دارند؛ می‌تواند مصداقی از شنود غیرمجاز باشد.

۵-۲ داده‌های سری

در تبصره۱ ماده۳ داده‌های سری تعریف شده است: «داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند».

در اصلاحات این لایحه در مجلس، ماده۴ دچار تغییرات عدیده‌ای شد از جمله آنکه عبارت داده‌های رایانه‌ای به‌کلی‌سری از مواد جدید۳،۴ و۵ قانون ج.ر حذف شد! متأسفانه معلوم نیست با توجه به اهمیت بیشتر داده‌های به کلی سری نسبت به داده‌های سری چرا حذف صورت گرفته است. البته با تمسک به قیاس اولویت می‌توان گفت وقتی افشای داده‌های سری جرم باشد، به طریق اولی افشای داده‌های به‌کلی‌سری که به مراتب از اهمیت و تأثیرگذاری بیشتری نسبت به داده‌های سری برخوردار است نیز جرم محسوب می‌شود. البته حذف قید داده‌های به‌کلی‌سری از این ماده با وجود اصلاحات به جایی که در آن

اعمال شده، محل انتقاد است. چراکه ماهیت این داده‌ها به گونه‌ای است که افشای آن می‌تواند به اساس حکومت و مبانی نظام و حتی تمامیت ارضی کشور ضرر جبران‌ناپذیری وارد کند و ضروری بود با توجه به تأثیرات افشای آن، در کنار داده‌های سری ذکر می‌شد. تفاوت داده‌های به‌کلی‌سری با سری در این است که افشای داده‌های گروه اول موجب ضرر و زیان جبران‌ناپذیر به امنیت ملی کشور می‌شود ولی افشای داده‌های دوم صرفاً به امنیت کشور و نظام لطمه زده وآن را به مخاطره می‌اندازد.

۵-۲-۱ بررسی عنصر مادی (بند«الف» ماده ۳)

در بند الف ماده۳ اعمال مجرمانه عبارتند از: ۱- دسترسی به داده‌های سری۲-تحصیل داده‌های سری۳- شنود محتوای سری در حال انتقال.

برای روشن شدن مفاد این بند توجه به این مطلب لازم است که «جاسوسی در معنی وسیع کلمه دو دسته اقدامات را شامل می‌شود: دسته اول، اقدامات مقدماتی که عبارت است از تفحص و تحصیل اطلاعات مخفی، دسته دوم، عملیات اجرایی که عبارت است از ایجاد ارتباط و رساندن اطلاعات مزبور به کسانی که باید از آن بهره‌برداری‌کنند.دسته اول ممکن است متضمن قصد جاسوسی یا خیانت نباشد، مثلاً متهم صرفاً از لحاظ کنجکاوی یا میل به دانستن یا اینکه برحسب غفلت و بی‌احتیاطی اقدام‌کرده یا اینکه اقدام به تحصیل اطلاعات محرمانه نموده تا بتواند مردم مملکت خود را آگاه سازد نه خارجیان را، اما دسته دوم همیشه کاشف از وجود اراده خاص بر آگاه کردن عوامل غیرمجاز وغیر صلاحیت دار است.» (گلدوزیان، ۸۲: ۴۷۶).

سیاق تنظیم بند «الف» و وجود قرائنی از جمله عدم مقید کردن اعمال غیر مجاز مذکور به رساندن این اطلاعات به افراد غیر صلاحیت دار، ما را به این نتیجه رهنمون می‌سازد که اقدامات ذکر شده در بند الف در زمره اقدامات مقدماتی پیش گفته قرار می‌گیرد. یعنی قراین و اماراتی دال بر جاسوسی وجود نداشته باشد نمی‌توان صرف انجام این اعمال را جاسوسی قلمداد کرد. آنچه دسترسی، تحصیل و یا شنود محتوای سری را صبغه جرم می‌بخشد، ارتکاب آنها به صورت غیرمجاز است لذا بهتر بود قید غیرمجاز به جای ابتدای ماده در ابتدای این بند به کار می‌رفت.

دسترسی از نظر لغوی عبارت است، قدرت، توانایی، قدرت دست یافتن به چیزی(عمید،ص ۷۱: ۶۰) لذا باتوجه به این معنی فردی که دسترسی غیرمجاز به داده‌های سری پیدا کند، خود رأساً این کار را می‌کند بدون آنکه از کسی یاری بگیرد، برای مثال با توسل به روش‌هایی مثل هک کردن، داده‌های مزبور را جمع آوری می‌کند و تفاوت آن با تحصیل داده‌های سری در این است که مجرمی‌که داده‌های سری را تحصیل می‌کند خود، ابتدا به ساکن امکان دسترسی مستقیم به این داده‌ها را ندارد. بلکه برای مثال با ایجاد ارتباط با کسی که این داده‌ها را در اختیار دارد، این داده‌ها را برای خود فراهم می‌آورد. توجه به معنی لغوی واژه تحصیل استدلال فوق را تقویت می‌کند، در فرهنگ فارسی یکی از معانی تحصیل عبارت است، به دست آوردن، کسب کردن (معین، ۷۶، ۱۰۳۸)، بنابراین طبیعی است که هرگاه مراد ما تحصیل

دانش باشد آن را از طریق معلم و استاد کسب می‌کنیم و هرگاه تحصیل داده‌های سری منظور باشد، آن را از طریق فرضاً یک مسؤول در اداره‌ای دولتی یا مرکزی نظامی‌کسب می‌کنیم.

شنود نیز به معنای دزدیده گوش دادن به مکالمات دیگران است(گلدوزیان، ۸۲: ۲۷۲) که در اینجا در خصوص محتوای سری در حال انتقال به کار رفته است. البته شنود غیرمجاز در حالی که محتوا، داده‌های سری نباشد به صورت مجزا در ماده۲ این قانون جرم انگاری شده است. مطابق این ماده، «هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی‌در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. جرم بند الف م. ۳ ق. ج. ر جرمی‌مقید است از این جهت برای تحقق آن، عملیات اجرایی مجرم جهت دسترسی، تحصیل شنود داده‌های سری می‌باید منجر به حصول به این داده‌ها گردد در غیر این صورت ممکن است عمل مرتکب مشمول ماده۴ قانون فوق الذکر گردد.

۵-۲-۲ بررسی عنصر روانی بند « الف » ماده ۳

عنصر روانی جرم بند الف علاوه بر عمد در دسترسی، تحصیل و یا شنود محتوای سری عبارت است از آگاهی و علم به غیر مجاز و بدون مجوز بودن دسترسی یا تحصیل ویا شنود داده‌های سری ونیز علم به سری بودن داده‌هایی که شخص به آنها دسترسی و... پیدا کرده است. از این رو اگر داده‌ها را عادی تصور کند، مرتکب این جرم نخواهد شد.

۵-۳-۱ بررسی عنصر مادی بند ب ماده۳

باتوجه به صراحت و تأکید این بند بر «در دسترس قراردادن داده‌های مذکور »منطقاً به نظر می‌رسد که این داده‌ها اعم از فیلم، عکس، متن و.... باید به طور مستقیم در اختیار فرد فاقد صلاحیت قرار گیرد. افشای مفاد این داده‌ها که شکل غیر مستقیم در دسترس قراردادن است. شامل ماده نمی‌شود و جرم نمی‌باشد.زیرا اگر قانونگذار نظر «در دسترس قراردادن مفاد داده‌ها» را جرم می‌دانست. مانند ماده۵۰۱ ق.م.ا از واژه ای «مفاد» در این ماده استفاده می‌کرد و آنگاه مقرر می‌نمود: «در دسترس قراردادن داده‌های مذکور یا مفاد آن....» این امر یکی از نقایص بندب ماده۳ ق.ج.ر. است زیرا با توجه به سری بودن داده‌ها واهمیت بالای آن عقلاً تفاوتی میان تسلیم خود و مفاد داده‌ها نیست و اطلاع افراد فاقد صلاحیت از خود داده یا مفاد آن به امنیت کشور لطمه می‌زند.

البته می‌توان در دسترسی قراردادن مفاد این داده‌ها را طبق ماده۵۰۱ ق.م.ا جرم دانست به این ترتیب اگر این داده‌ها در برگیرنده نقشه‌ها، اسرار یا اسناد وتصمیمات راجع به سیاست داخلی یا خارجی کشور باشد، آن گاه در دسترس قرار دادن مفاد آنها به افراد فاقد صلاحیت، جرم محسوب می‌شود.به هر

روی، بهتر بود قانونگذار برای جلوگیری از بروز این دست ابهام‌ها، کلمه مفاد را نیز به همان ترتیبی که گفته شد به این بند اضافه می‌کرد.

نکته قابل بحث در این بند همانند ماده۵۰۱ ق.م.ا این است که آیا اشاره ماده به اینکه داده‌ها در دسترس افرادی‌که فاقد صلاحیت هستند قرار گیرند، به معنی آن است که خود فرد اطلاعات دهنده صلاحیت دسترسی به این اسناد را دارد یا اینکه لزوماً اینگونه نیست. در صورت قبول تفسیر اول، این بند فقط شامل مأموران دولتی می‌شود که به مقتضای شغل خود از داده‌های سری آگاه هستند.

در صورت پذیرش تفسیر دوم، حتی اگر دسترسی کسی به داده‌های سری غیرمجاز باشد، بازهم در دسترس قرار دادن اطلاعات به افراد فاقد صلاحیت دیگر از سوی او موجب تحقق جرم مزبور می‌گردد. در پاسخ می‌توان گفت باتوجه به اطلاق ماده و به کار رفتن واژه هرکس در ابتدای آن تفسیر دوم ارجحیت دارد.(میرمحمدصادقی، ۸۱ص: ۸۵)

۵-۳-۲ بررسی عنصر روانی بند ب ماده ۳

عنصر روانی این جرم نیز عبارت است از: در دسترس قرار دادن داده‌های سری به صورت عمدی، از این رو اگر فرد در حالت مستی بی‌هوشی، خواب، اجبار، اکراه و نظایر اینها، مرتکب عمل شده باشد، عمل وی مشمول این بند نمی‌شود، همچنین مرتکب باید نسبت به سری بودن داده‌ها ونیز فاقد صلاحیت بودن طرف دیگر علم داشته باشد، اما سوءنیت خاص یعنی اینکه با انجام این کار قصد ضربه زدن به نظام یا برهم زدن امنیت کشور و نظایر آن را داشته باشد، ضروری نیست. (همان: ۸۶)

۵-۴-۱ بررسی عنصر مادی بند ج ماده ۳

تعریف خاص از قوانین جزایی به عمل نیامده، اما مطابق ماده ۱۹- ۲-۱ آیین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی شده نیروهای مسلح مصوب۱۳۷۵ ستاد کل نیروهای مسلح، افشا عبارت است از: «عرضه کردن مفاد اسناد یا اطلاعات طبقه‌بندی شده به طور شفاهی،کتبی و یا هر طریقی که حفاظت و امنیت از آن سلب شود».

به نظر می‌رسد تفاوت «افشا» با «در دسترس قرار دادن» این است که زمانی عمل فرد «افشا» تلقی می‌شود که فرد رأساً داده‌های سری را در اختیار افراد مذکور بگذارد، لیکن ماهیت «در دسترس قرار دادن» انفعالی است، به این ترتیب زمانی عمل مرتکب «در دسترس قراردادن» تلقی می‌شود که وی به نحوی از انحاء موجبات دسترسی افراد مذکور را به داده‌های سری فراهم کند، بدون آنکه داده‌ها به طور مستقیم از طرف خود وی به آنها ارائه شود مانند آنکه مرتکب، گذر واژه(۱۱) رایانه خود را عمداً در اختیار عوامل بیگانه قرار داده وآنها با ورود پنهانی به اطاق محل قرار گرفتن رایانه و واردکردن گذر واژه مزبور، وارد رایانه شده و داده‌های سری را برداشت کنند.

در خصوص واژه «بیگانه»که معمولاً به خارجیان اطلاق می‌شود، پر واضح است که استعمال آن به عنوان صفت دولت، سازمان، شرکت و یا حتی گروه، ابهامی‌ایجاد نمی‌کند و شامل هر دولت سازمان، شرکت و یا گروه غیر ایرانی می‌شود. اما ممکن است در رابطه با عاملان آن‌ها این تردید ایجاد شود که آنها نیز باید لزوماً یک فرد خارجی و غیرایرانی باشد؟ برای پاسخ باید به این نکته توجه کردکه دولت‌ها برای جاسوسی از یکدیگر معمولاً به صورت کاملاً پنهانی عمل می‌کنند و برای عادی‌سازی اقدامات خود، بسیار متحمل است برای کسب اطلاعات مورد نیاز خود دست به استخدام عوامل ایرانی بزنند و به اصطلاح یک ایرانی عامل آنها باشد.

بنابراین باتوجه به فرایند پیچیده جاسوسی و پنهان‌کاری‌های مختص آن، به نظر می‌رسد تفسیر صحیح تر آن باشد که چون یک ایرانی نیز می‌تواند عامل بیگانه باشد، پس افشا یا در دسترس قرار دادن داده‌های سری برای او نیز مشمول این ماده است و لزومی ندارد عاملی بیگانه هم یک فرد ایرانی باشد.ابهام دیگر این بند، واژه گروه بیگانه است. در ادبیات حقوقی، برای واژه‌های دولت، سازمان و شرکت تعاریف تقریباً مشخص وجود دارد، اما منظور از گروه چیست؟ آیا مراد گروه‌های غیر دولتی خارجی(۱۲) هستند که به منظور خاصی تشکیل می‌شوند؟ یا برای مثال حتی یک گروه جهانگرد خارجی‌که برای تفریح به ایران آمده‌اند را نیز شامل می‌شود؟

باتوجه به حساسیت قانونگذار نسبت به حفظ داده‌های سری و اینکه افشای آنها را موجب لطمه به امنیت ملی دانسته است، چنین استنباط می‌شود که به هر صورت هرجا که عنوان گروه بر اجتماع یک یا چند نفر غیر ایرانی صدق کند می‌توان آن را به عنوان گروه بیگانه قلمداد کرد و اگر داده‌های سری در دسترس آنان قرار گیرد یا برای‌شان فاش شود. عمل فرد مشمول این بند خواهد بود و لزوماً نیاز نیست که این گروه یک گروه سازمان یافته و دارای تشکیلات باشد. در هر حال قانون جرایم رایانه‌ای در این قسمت مجمل بوده و بهتر بودکه این‌گونه اصلاحات را به دقت تعریف می‌کرد.

۵-۴-۲ بررسی عنصر روانی بند«ج » ماده۳

عنصر روانی مرتکب این بند علاوه بر عمد در افشا یا در دسترس قرار دادن داده‌های سری، علم و آگاهی نسبت به بیگانه بودن طرف مقابل است؛ این بیگانه می‌تواند یک دولت، سازمان و... باشد. همچنین در این بند وجود سوءنیت خاص یعنی اینکه با انجام این‌کار قصد برهم زدن امنیت کشور یا ضربه زدن به نظام را داشته باشد ضروری نیست و به صرف افشا یا در دسترس قرار دادن داده‌های سری جرم محقق می‌شود.(همان: ۸۶).

نتیجه گیری

متخصصان معتقدند جرم جاسوسی رایانه‌ای، با شدت و پیچیدگی بیشتری در سطح وسیع جهانی ادامه پیدا خواهد کرد(بونی وکواسیچ، ۸۳: ۳۲۵). رفته رفته جاسوسی اینتر نتی به عنوان ابزاری برای حصول برتری در رقابت بی‌پایان کشورها در زمینه‌های صنعتی، اقتصادی، نظامی‌و... تبدیل خواهد شد وکشورهای بیشتری وارد صحنه کارزار رایانه‌ای می‌شوند. این جنگی است که در آن نیازی به استفاده از پیاده نظام، هواپیما جنگنده و موشک نیست. کلید موفقیت در این جنگ اطلاعات است، عوامل جاسوسی رایانه‌ای و اینترنتی نقش پیاده نظام این جنگ پسامدرن را بازی می‌کنند.

جاسوسی اسرار تجاری به شکل سنتی، در ماده ی ۵۰۱ قانون مجازات اسلامی و بند «ج » ماده ی ۲۴ قانون مجازات جرایم نیروهای مسلح جرم انگاری شده است و اَشکال نوین این جرم که از طریق سامانه های رایانه ای و مخابراتی صورت می گیرد یا به شکل داده پیام در فضای مجازی قابل بررسی است، افزون بر قانون تجارت الکترونیک، در قانون مبارزه با جرایم رایان های نیز مورد توجه قرار گرفته است.

بنابراین شایسته است در سطح جهان، فضای مجازی از نبود چنین قوانین بین‌المللی رنج می‌برد و حتی گاهاً دیده شده که برخی از دولت‌ها از این نرم‌افزارهای جاسوسی غیرقانونی بر ضد سایر کشورها به صورت علنی استفاده می‌کنند.

منابع و مأخذ

۱. عمید، حسن، فرهنگ عمید، شامل واژه نامه های فارسی و لغات عربی و اروپایی مصطلح در زبان فارسی و اصطلاحات ادبی، انتشارات جاویدان، ۱۳۴۹.

۲. فضلی، مهدی، مسئولیت کیفری در فضای سایبر، انتشارات خرسندی، ۱۳۸۹.

۳. گلدوزیان، ایرج، حقوق جزای عمومی ایران، انتشارات دانشگاه تهران، ۱۳۸۴.

۴. لنگرودی، محمد جعفر، ترمینولوژی حقوق، کتابخانه گنج دانش، ۱۳۸۴.

۵. معین، محمد، فرهنگ معین، دوره ۶ جلدی، نشر امیرکبیر، ۱۳۷۶.

۶. میر محمد صادقی، حسین، جرائم علیه امنیت و آسایش عمومی، نشر میزان، ۱۳۸۶

۷. میرمحمد صادقی، حسین، تحلیل مبانی حقوق جزا، نشر جهاد دانشگاهی شهید بهشتی، ۱۳۷۴.

۸. نوروزی فیروز، رحمت الله، حقوق جزای عمومی «مجازات»، نشر میزان، ۱۳۹۰.

۹. نوروزی فیروز، رحمت الله، حقوق جزای عمومی «صلاحیت»، نشر میزان، ۱۳۸۷.

۱۰. آشوری، داریوش، دان شنامه سیاسی، تهران: مروارید، چاپ نخست، ۱۳۶۶ .

۱۱. انوری، حسن، فرهنگ بزرگ سخن، ج ۴ ، چاپ اول، انتشارات سخن، سال ۱۳۸۱

۱۲. ظهیریان محمد مهدی، اصول کلی حقوق جزای انگلستان، چاپ اول ، گنج دانش، سال ۱۳۹۰

۱۳. شامبیاتی، هوشنگ، حقوق کیفری اختصاصی، بیچا، تهران، انتشارات ژوبین، ۲۹۶۷ش،ج ۹

۱۴. طباطبایی،سید محمدحسین،تفسیر المیزان، چ ۲ قم،دفتر انتشارات اسلامی، ۲۹۷۶ش،ج ۳

۱۵. مجیدی، محمود، حقوق کیفری اختصاصی، جرایم علیه امنیت، بیچا، تهران، میزان،۲۹۳۷