دانشکده حقوق وعلوم سیاسی

پایان نامه دوره کارشناسی ارشد در رشته حقوق جزا و جرم شناسی

موضوع:

تحلیل حقوقی جرم جاسوسی در فضای مجازی

استاد راهنما:

دکتر: سید ابراهیم قدسی

استاد مشاور:

دکتر: کیومرث کلانتری

نام دانشجو:

انسیه سلیمی

دی ماه ۱۳۹۲

چکیده

جاسوسی یکی از مهم ترین جرایم علیه امنیت ملی است که با توسعه علوم و افزایش ارتباطات، حوزه ارتکاب آن از دنیای واقعی فراتر رفته و به فضای مجازی نیز راه یافته است. جاسوسی در فضای مجازی، تحت عنوان جرایم علیه محرمانگی اطلاعات که متشکل از سیستم‌های رایانه‌ای و مخابراتی می‌باشد، مطرح می‌شود. این شکل نوین جاسوسی، در بخش های مختلفی ظهور می یابد که بطور اخص، در دو بخش جاسوسی صنعتی و امنیتی قابل بررسی است. در پژوهش حاضر ابتدا با تفکیک جاسوسی امنیتی و صنعتی در فضای مجازی، به تعریف و تبیین انواع آن پرداخته شده است. در جاسوسی امنیتی، افشا و دسترسی غیرمجاز به اسناد سری و محرمانه، صدمه جدی به منافع عمومی و امنیت کشور وارد می‌سازد. در جاسوسی صنعتی نیز دستیابی غیرمجاز به اسرار تجاری و اقتصادی یک کشور، منجر به در خطرافتادن دادوستد افراد با یکدیگر و یا از بین رفتن اموال و خدمات آنها می شود، که در صورت برهم‌زدن امنیت کشور، خود نوعی جاسوسی امنیتی تلقی می شود. در ادامه بحث، مصادیق هریک از انواع جاسوسی امنیتی و صنعتی با توجه عناصر سه گانه جرم (قانونی، مادی و معنوی)، در قانون مجازات اسلامی و جرایم نیروهای مسلح، و نیز با ملاحظه رویکرد جدید قانون گذار در قانون جرایم رایانه ای و قانون تجارت الکترونیک مورد بررسی قرار گرفته است. آنگاه به تفاوت انواع جاسوسی در فضای مجازی و سنتی از جنبه های مختلف پرداخته شده است. بدین ترتیب با توجه به تاکید قانون گذار بر حفظ حاکمیت ملی، جاسوسی در فضای مجازی نه تنها از بعد امنیتی بلکه از بعد صنعتی نیز، در زمره جرایم علیه امنیت کشور قلمداد می‌شود.

واژگان کلیدی

اطلاعات، فضای مجازی، امنیت، جرم، اسرار.

فهرست مطالب

مقدمه

امنیت یکی از عوامل اساسی ثبات سیاسی و اقتصادی کشورها محسوب می شود، از این رو آنچه که همواره دولت ها را به وضع قوانین با ضمانت اجرای سنگین وادار می سازد، جرایم علیه امنیت ملی است که بیش از هر بزه دیگری مورد توجه دولت ها و قانون‌گذاران می‌باشد. از طرفی دیگر نیز، گسترش فناوری اطلاعات حوزه جنایات را از حیطه مرزها خارج ساخته و به جنایت سازمان یافته فراملی تسری می‌بخشد، که علاوه بر تأثیر بر سیستم های اقتصادی بین المللی، ساختار سیاسی حکومت و نظم جهانی را نیز مختل می سازد. درواقع با پیشرفت روز افزون علم و گسترش سیستم های رایانه‌ای که در رأس آنها اینترنت قرار دارد، جرایم شکل جدیدی به خود گرفته‌اند. در این میان، جرایم علیه امنیت نیز با قالبی نوین ظهور پیداکرده‌اند که یکی از این اشکال، جرم جاسوسی در فضای مجازی است.

درواقع آنچه که دولت ها را با فضای مجازی پیوند می زند، اطلاعاتی است که جنبه امنیتی دارند. امنیت این اطلاعات از گذشته‌های دور مورد توجه دولت‌ها بوده است و همواره تلاش شایانی برای حفظ اطلاعات و جلوگیری از افشای آنها صورت گرفته است. با ورود به عصر اطلاعات، این داده ها بیش از پیش مورد توجه بزهکاران قرار گرفته است؛ چرا که فضای مجازی با گستردگی فراوان و دستیابی آسان، امکان دسترسی غیرمجاز به اطلاعات و افشای اطلاعات امنیتی را در قالب داده ها و سیستم‌های رایانه‌ای و مخابراتی فراهم کرده است. از این رو دولت ها درصدد برآمدند، قوانینی را به موجب کنوانسیون های بین‌المللی تصویب نمایند تا به حفاظت از اطلاعات امنیتی در فضای مجازی بپردازند؛ از جمله این قوانین در کشور ما، قانون تجارت الکترونیک و قانون جرایم رایانه ای است. تصویب این قوانین زمینه ای برای آغاز بررسی دقیق جرایم مربوط به رایانه در حوزه اختصاصی حقوق کیفری می‌باشد.

آنچه که در این پژوهش مورد بررسی قرار میگیرد، تحلیل حقوقی جرم جاسوسی در فضای مجازی است، تا با نگاهی عمیق تر جرایم علیه محرمانگی اطلاعات و عناصر این جرم در فضای مجازی بررسی و خلأهای قانونی آن نیز آشکار گردد. البته تعبیر «محرمانگی اطلاعات»، مفهوم عامی است که اطلاعات شخصی، حرفه ای و دولتی را دربر می‌گیرد. اما آنچه در جرایم علیه امنیت مورد توجه قرار می‌گیرد، صرفاً اطلاعات دولتی است که دستیابی و افشای آنها، آسیب جدی به امنیت کشور و منافع ملی

وارد می‌سازد. باتوجه به این‌که شیوه‌ها و اشکال ارتکاب جرم جاسوسی در فضای مجازی از پیچیدگی و تنوع بیشتری در مقایسه با فضای واقعی برخوردار است، در این پژوهش جاسوسی از منظری نو مورد بررسی قرار می‌گیرد.

سؤالاتی که این پژوهش درصدد پاسخگویی به آنهاست عبارتند از این که :

۱ -در قوانین موضوعه ایران، جرم جاسوسی در فضای مجازی چه نوع اسرار و اطلاعاتی را دربرمی‌گیرد؟

۲ -آیا جرم جاسوسی در فضای مجازی، مانند شکل سنتی خود دارای عناصر سه‌گانه جرم می‌باشد یا خیر؟

۳ -واکنش قانون‌گذار نسبت به جرم جاسوسی در فضای مجازی چگونه است؟

در پاسخ به این سؤالات می‌توان عنوان کرد که :

۱ -جاسوسی در فضای مجازی، علاوه بر اسرار امنیتی که در شکل سنتی آن هم دیده می‌شود، اسرار تجاری را نیز در برمی‌گیرد.

۲ -جرم جاسوسی در فضای مجازی مانند شکل سنتی خود، دارای عناصر سه‌گانه جرم می‌باشد. اما در بحث عنصر قانونی، قانونگذار همه موارد رفتار مجرمانه جاسوسی سنتی را در فضای مجازی جرم‌انگاری نکرده است.

۳ -رویکرد قانون‌گذار نسبت به جرم جاسوسی در فضای مجازی، شکلی متفاوت از شکل سنتی آن دارد؛ به‌طوری‌که مجازات این جرم در فضای مجازی علاوه بر حبس، جزای نقدی و یا یکی از این دو مجازات خواهد بود، که میزان مجازات تعیین شده در زمینه جاسوسی در فضای مجازی بسیار سبک تر از انواع مصادیق جاسوسی به شکل سنتی است.

باتوجه به بررسی های نگارنده، تألیفی نسبت به ارتکاب جرم جاسوسی در فضای مجازی، تبیین انواع و مصادیق آن و بررسی جوانب حقوقی موضوع، به نحو خاص یافت نشد. البته از کتب، مقالات، منابع الکترونیکی و پایان نامه ها مرتبط با موضوعات کلی جرایم علیه امنیت و جرایم مرتبط با رایانه به شیوه کتابخانه ای بهره‌برداری شده است. کتاب هایی تحت عنوان جرایم علیه امنیت و آسایش عمومی

وجود دارند که به طورکلی به بررسی عناوین جرایم علیه امنیت و آسایش عمومی پرداخته اند. جرایمی وجود دارند که به طور مستقیم با مفاهیم امنیت ملی و آسایش عمومی در ارتباط می‌باشند مانند جاسوسی، شورش، تحریک مردم، شورش، جمع آوری اطلاعات محرمانه، سوءقصد به جان مقامات سیاسی و...که با حاکمیت ملی و پایه های یک نظام وحکومت برخوردارند. (میرمحمد صادقی، ۱۳۸۱ : ۴۵) برخی این گونه جرایم را به دو دسته تقسیم‌بندی می کند که به طور خاص جرایم جاسوسی، محاربه، تشکیل جمعیت و افشای اسرار و در معنای عام، محاربه، بغی، تروریسم، تحریک و... را دربرمی گیرد. (زراعت، ۱۳۷۷ : ۵۲) برخی از کتب نیز به جرایم رایانه ای به طور کلی پرداخته اند. به طور مثال کتاب بررسی فقهی و حقوقی جرایم رایانه‌ای نوشته حسینعلی بای، به تعریف جرایم رایانه‌ای می‌پردازد و سپس هریک از جرایم علیه رایانه را به صورت مجزا از دیدگاه فقهی و حقوقی بررسی می کند. اما نکته قابل ذکر در این است که این کتاب، علاوه برآن که پیش از تصویب قانون جرایم رایانه ای تألیف شده است به بررسی تفصیلی در همه جوانب حقوقی نپرداخته است و بیشتر مباحث فقهی را مطرح کرده است. اما به طورکلی، در زمینه بحث جرایم علیه امنیت، می توان به کتاب «جاسوسی و خیانت به کشور» دکتر ساریخانی، و در زمینه موضوعات مرتبط با جرایم رایانه ای نیز می توان به کتاب «حقوق کیفری فناوری اطلاعات» نوشته دکتر عالی پور اشاره کرد، که در این پژوهش از آن استفاده شده است.

این نگاشته در فصل اول، به بررسی کلی بحث جاسوسی در فضای مجازی، در ذیل دو گفتار تحت عناوین مفهوم شناسی و بررسی تاریخی می پردازد. فصل دوم به تفکیک و بازشناسی انواع جاسوسی، براساس قوانین تجارت الکترونیک و جرایم رایانه‌ای می‌پردازد و ویژگی مرتکبین این جرایم و انگیزه‌های آنان را مورد بررسی قرار می دهد. در فصل سوم مصادیق جاسوسی در فضای مجازی با رویکردی به عناصر سه گانه جرم مورد بررسی قرار می گیرد و در نهایت در فصل چهارم با مقایسه میان جاسوسی سنتی و نوین، با نتیجه‌گیری از بحث آن را به پایان می‌رساند.

فصل اول- کلیات

جاسوسی یکی از جرایم علیه امنیت است که بُعد فراملی آن، بر اهمیت این جرم در عرصه بین‌المللی افزوده است. جاسوسی در فضای مجازی، به عنوان یکی از جدیدترین و مهم ترین انواع جرایم علیه امنیت است که از طریق سامانه های رایانه‌ای و مخابراتی واقع می شود. از این رو این فصل درصدد است تا به بررسی مفاهیم اساسی مرتبط با این جرم که در فضای مجازی واقع می شود، بپردازد. این فصل در دو گفتار نگارش یافته است، که ابتدا به مفهوم شناسی مباحثی مرتبط با جاسوسی پرداخته می شود؛ سپس در گفتار دیگر، تاریخچه جرم جاسوسی در فضای مجازی در نظام حقوقی ایران و کشورهای دیگر مورد بررسی قرار می گیرد. در قسمت اول این گفتار، تحت عنوان پیشینه برون مرزی، به بررسی تاریخچه وقوع جرم جاسوسی از طریق سامانه های رایانه‌ای و مخابراتی، در کشورهای مختلف پرداخته می‌شود. سپس در قسمت دوم، تاریخچه این جرم در نظام حقوقی ایران، با توجه به قوانین کیفری موجود بررسی می گردد.

۱-۱- مفهوم شناسی

برای تبیین جرم جاسوسی در فضای مجازی، ابتدا باید مفهوم شناسی مطلوبی از تعابیری چون جرم جاسوسی، فضای مجازی، شبکه اینترنت و داده پیام ارائه گردد تا با واژه شناسی مطلوبی، بحث آغاز گردد.

۱-۱-۱-جرم جاسوسی

«جرم» کلمه‌ای با ریشه عربی، به معنای «گناه، تعدی، بزه، عصیان و خطا» می باشد. (دهخدا، ۱۳۷۳، ج۵: ۶۷۲۲) در اصطلاح حقوقی، «جرم عملی است که قانون آن را از طریق تعیین کیفر منع کرده باشد.» (جعفری لنگرودی، ۱۳۷۶ : ۱۹۱) در قانون مجازات اسلامی نیز قانون گذار جرم را «فعل یا ترک فعلی می‌داند که در قانون برای آن مجازات تعیین شده باشد.» (ماده۲ قانون مجازات اسلامی)

کلمه «جاسوسی» از «جسّ به معنای لمس نمودن چیزی با دست گرفته شده است. ماده جسَ به معنای جستجوی خبر است» (ابن منظور، ۷۱۱ق، ج۲ : ۲۸۳) که در واژگان فارسی در معنای خبر پرسی به کارگرفته شده است و به عمل جاسوس نیز اطلاق می شود. (دهخدا، ۱۳۷۳، ج۵ : ۶۴۵۸)

در قوانین کیفری ایران تعریفی از جرم جاسوسی به عمل نیامده است. این رویکرد علاوه بر قانون مجازات اسلامی مصوب ۱۳۷۵ در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نیز مشاهده می‌شود. در برخی از مواد قانونی، صرفاً به مصادیقی از جرم جاسوسی اشاره شده است و همین امر زمینه بروز ابهام در تعیین رویکرد قانونی نسبت به جرم جاسوسی را فراهم کرده است که به برخی از آنها اشاره می‌شود.

قانون‌گذار در ماده ۵۰۱ قانون مجازات اسلامی عنوان کرده است: «اگر فردی نقشه، اسرار یا تصمیمات راجع به سیاست کشور در اختیار افرادی که صلاحیت رسیدگی به آنها را ندارند قرار دهد یا از مفاد آن مطلع کند، عمل او از مصادیق جاسوسی قلمداد می‌شود.»

ماده ۳ قانون جرایم رایانه ای نیز که به جاسوسی از طریق سامانه های رایانه‌ای پرداخته است، بیشتر جاسوسی اسرار امنیتی و سری را مدنظر تعریف خود قرار داده است.[1] به موجب این ماده: «هرکس به طور غیرمجاز نسبت به داده های سری در حال انتقال یا ذخیره شده در سیستم های رایانه ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال یا هر دو مجازات.

ب) دردسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشا یا در دسترس قرار دادن داده های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.»

همچنین براساس ماده ۲۹ آیین نامه ضمیمه قرار داد سال ۱۹۰۷ که در لاهه منعقد گردیده است، «جاسوسی» به عمل شخصی گفته‌می‌شود که تحت عناوین غیرواقعی و به نفع یکی از متخاصمین، درصدد

[1] . موید این نظر، تبصره همین ماده است که داده های سری را اسراری می‌داند که افشای آنها موجب برهم زدن امنیت کشور می‌شود.

تحصیل اطلاعات یا اشیایی باشد. (گارو، ۱۳۴۳، ج ۳: ۷۱۹) به فردی که مرتکب عملیات جاسوسی می‌شود، جاسوس گفته می شود. از نظر حقوق بین الملل عمومی نیز «جاسوس» به کسی اطلاق می گردد، که به صورت محرمانه یا تحت عنوان های نادرست و به نفع دشمن، درصدد تحصیل اطلاعاتی از نقشه و قوای طرف و مقاصد او برآید. (جعفری لنگرودی، ۱۳۷۶ : ۱۸۹)

به موجب ماده ۲۴ قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲: « افراد زیر جاسوس محسوب و به مجازات‌های ذیل محکوم می‌شوند:

الف – هر نظامی که اسناد یا اطلاعات یا اشیای دارای ارزش اطلاعاتی را در اختیار دشمن و یا بیگانه قرار دهد و این امر برای عملیات نظامی یا نسبت به امنیت ت أسیسات، استحکامات، پایگاه ها، کارخانجات، انبارهای دائمی یا موقتی تسلیحاتی، توقفگاه های موقت، ساختمان های نظامی، کشتی ها، هواپیماها یا وسائل نقلیه زمینی نظامی یا امنیت ت أسیسات دفاعی کشور مضر باشد ، به مجازات محارب محکوم خواهد شد.

ب – هر نظامی که اسناد یا اطلاعات برای دشمن یا بیگانگان تحصیل کرده، به هردلیلی موفق به تسلیم آن نشود، به حبس از سه تا پانزده سال محکوم می گردد.

ج – هر نظامی که اسرار نظامی، سیاسی، امنیتی، اقتصادی و یا صنعتی مربوط به نیروهای مسلح را به دشمنان داخلی یا خارجی یا بیگانگان یا منابع آنان تسلیم و یا آنان را از مفاد آن آگاه سازد به مجازات محارب محکوم خواهد شد.

د – هر نظامی که برای به دست آوردن اسناد یا اطلاعات طبقه بندی شده، به نفع دشمن و یا بیگانه به محل نگهداری اسناد یا اطلاعات داخل شود، چنانچه به موجب قوانین دیگر مستوجب مجازات شدیدتری نباشد، به حبس از دو تا ده سال محکوم می گردد.»

در نظر برخی حقوق دانان، «جاسوسی» عبارت است از جمع آوری و تملیک اطلاعات و تعلیمات اسناد قابل استفاده یک کشور خارجی بر ضد امنیت کشور خارجی دیگر. (گارو، ۱۳۴۳، ج۳: ۱۲) البته می‌توان گفت «جاسوسی» در اصطلاح حقوقی عبارتست از گردآوری اطلاعات و اسناد مخفی و طبقه بندی شده راجع به عملیات آفندی و پدافندی یا کسب اطلاع از اوضاع و احوال سیاسی یا اقتصادی و

اسرار علمی و صنعتی و امور نظامی مملکت، به قصد دادن آن به افراد فاقد صلاحیت و بیگانگان (در مقابل هر نوع پاداش یا بی اجرت) که در راستای اهداف دشمن است و نقاط قوت و ضعف ما را بدست آورد، تا بتواند راه‌های نیرومند شدن ما را مسدود کرده، از نقاط ضعف ما برای ضربه زدن استفاده نماید. (مرتضوی، ۱۳۸۵ : ۶۴)

شورای اروپا [۲] در فهرست اختیاری توصیه نامه شماره R (۸۹)۹، جرم جاسوسی رایانه ای را پیش‌بینی کرده است. به موجب این توصیه نامه جاسوسی رایانه ای عبارتست از: «بازرسی و تفتیش با ابزارهای لازم برای افشا، انتقال یا استفاده از اسرار تجاری بدون داشتن حق یا بدون هیچ توجیه قانونی دیگر، خواه به قصد ایجاد ضرر اقتصادی به شخص محق اسرار و خواه به قصد دستیابی به یک منفعت اقتصادی غیر قانونی برای خود یا دیگری باشد.» (توصیه نامه شماره R (۹) ۸۹ ۱۹۹۰ استراسبورگ)

لازم به ذکر است که چنین تعریفی، جامع و مانع نیست. چراکه به موجب این تعریف تنها جاسوسی اسرار تجاری و صنعتی جرم انگاری شده است و به انواع دیگر اسرار که جنبه امنیتی دارند توجهی نشده است. در قصد و انگیزه مرتکب نیز صرفاً به ایراد ضرر اقتصادی یا کسب منفعت اقتصادی پرداخته شده است، در حالی که ممکن است فرد جاسوس، هدف دیگری را نیز از عمل خود دنبال نماید.

باتوجه به مباحث ارائه شده، تعریفی که می توان برای جاسوسی رایانه‌ای پیشنهاد کرد عبارتست از: تجسس، دستیابی و افشای غیرمجاز و عمدی داده پیام ها و اطلاعات ارزشمند، اعم از تجاری، سیاسی، نظامی، فرهنگی و امنیتی، که به قصد ضربه زدن به اشخاص حقیقی یا حقوقی اعم از حقوق خصوصی و عمومی، به هر طریقی در فضای مجازی صورت بگیرد.

جاسوسی در معنای وسیع کلمه دو دسته اقدامات را در بر می گیرد: یک دسته اقدامات مقدماتی که عبارت است از تفحص و تحصیل اطلاعات مخفی و دسته دیگر عملیات اجرایی که عبارت است از ایجاد ارتباط و رساندن اطلاعات مزبور به کسانی که باید از آن بهره‌برداری کنند. زمانی که تحصیل اطلاعات محرمانه که به طور متقلبانه صورت می گیرد، در فضای مجازی واقع شود و اسرار مورد جاسوسی، داده‌های رایانه‌ای محرمانه باشد یا تحصیل اطلاعات از طریق رایانه و دیگر وسایل الکترونیکی در فضای مجازی صورت بگیرد، جاسوسی رایانه‌ای محقق می‌شود.

[2] .European council

در جاسوسی امنیتی، سیاسی، نظامی و صنعتی، نوع اطلاعات مورد حمایت قرار می گیرد و بر آماج جرم که در اثر جاسوسی تهدید می شود تأکید دارد؛ اما در جاسوسی رایانه ای علاوه بر تکیه بر همان اهداف، شیوه‌های جدید ارتکاب جرم، مانند رایانه مدنظر قرار می گیرد. البته عده‌ای معتقدند درصورتیکه عمل جاسوسی به وسیله رایانه صورت بگیرد، عنوان جاسوسی رایانه‌ای بر آن صدق نمی‌کند و درواقع این عمل نیز جزئی از جاسوسی کلاسیک یا سنتی محسوب می شود و صدق عنوان جرم جاسوسی رایانه‌ای را محدود به ارتکاب آن در فضای مجازی می دانند. (ر.ک نظر میرمحمدصادقی در فناوری اطلاعات و ارتباطات و چالش در مفهوم جرم های سنتی، ۱۳۸۶: ۲۴) اما به نظر نگارنده این امر مورد پذیرش نیست. چراکه محتوای اصلی هر دو نوع جاسوسی سنتی و رایانه ای با یکدیگر مشابه است و تنها ابزار ارتکاب جرم یا مکان ارتکاب آن است که سبب تفاوت این دو نوع جاسوسی، حتی در عناصر تشکیل دهنده آنها می‌شود.

۱-۱-۲- فضای مجازی[3]

«فضای مجازی» تعبیری است که در دنیای ارتباطات بسیار به چشم می خورد. از حیث اصطلاحی «فضای مجازی به مجموعه محیط هایی همچون اینترنت گفته می شود که اشخاص در آنها از طریق رایانه‌هایی متصل به هم، با یکدیگر ارتباط برقرار می‌کنند.» (قلی زاده نوری، ۱۳۸۱ : ۱۹۵)

فضای مجازی به مجموعه از ارتباطات افراد جوامع مختلف اطلاق می شود که از طریق سامانه‌های رایانه‌ای و مخابراتی با یکدیگر درتماس هستند. در فضای مجازی برخلاف فضای واقعی، نیاز به جابجایی فیزیکی وجود ندارد و کاربران می‌توانند بدون توجه به این که این اطلاعات و خدمات در کدام نقطه دنیا واقع شده‌اند، در هر زمان و در هر مکانی به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند. این خصیصه همراه با ویژگی‌های دیگر فضای مجازی، مانند پنهانی بودن، غیرقابل‌کنترل بودن، گزینشی بودن اطلاعات و جهان شمول بودن آن، عوامل اساسی وقوع ارتکاب جرایم رایانه ای در فضای مجازی هستند.

[3]. cyber space

جرایم ارتکابی در فضای مجازی نسل سوم از جرایم کامپیوتری هستند ،[۴] که یکی از این جرایم، جرم جاسوسی اسرار تجاری و امنیتی است که توسط جاسوسانی چون هکرها، کراکرزها و فریک ها در فضای مجازی صورت می گیرد. برخی از پژوهشگران در زمینه جرایم رایانه ای، فضای مجازی را محدود به فضای اینترنت نموده‌اند، (باستانی، ۱۳۸۳ : ۶۵) اما به نظر نگارنده محدوده فضای مجازی علاوه بر فضای اینترنت، سامانه‌های مخابراتی را نیز شامل می شود. به همین خاطر در بحث جرم جاسوسی رایانه ای علاوه بر ارتکاب جرم در فضای اینترنت، می‌توان به شنود مکالمات تلفنی افراد نیز اشاره نمود.

۱-۱-۳- شبکه اینترنت[۵]

«شبکه» به گروهی از رایانه های مرتبط با یکدیگر گفته می شود که به وسیله تسهیلات ارتباطی به یکدیگر متصل می شوند. این ارتباطات ممکن است با اتصالات دائمی (مانند کابل ها) یا اتصالات موقتی (مانند خطوط تلفن) یا دیگر پیوندهای ارتباطاتی باشد. (قلی زاده نوری، ۱۳۸۱ : ۵۱۵)

در بند ۲۴ گزارش توجیهی کنوانسیون جرایم سایبر، «شبکه» عبارتست از «عامل برقراری اتصال دو یا چند سیستم رایانه ای، که این اتصال می تواند به صورت زمینی (با کابل یا سیم) یا بدون سیم (از طریق امواج رادویی، مادون قرمز یا ماهواره) صورت بگیرد.» (جلالی فراهانی، ۱۳۸۹ : ۱۹)

تعبیر «سیستم رایانه‌ای» موجود در تعریف شبکه، خود متشکل از دو واژه «سیستم» و «رایانه» است. «سیستم» سخت افزاری متشکل از تراشه ها و مدارات مرتبط با آن است که وسایل ورودی وخروجی، وسایل جانبی و یک سیستم عامل متشکل از مجموعه ای از برنامه ها و فایل های داده‌ای، نمونه‌هایی از آن محسوب می‌شوند. «رایانه» نیز وسیله ای است که قابلیت پردازش اطلاعات را جهت تولید نتیجه مورد نظر دارا می باشد، که عموماً کارهای خود را، در سه مرحله پذیرش ورودی، پردازش ورودی مطابق با برنامه‌های از پیش تعریف شده و تولید خروجی، صورت می دهد. (قلی زاده نوری، ۱۳۸۱ : ۷۱۷ و ۱۶۶)

---

[۴]. در طبقه بندی جرایم رایانه ای می توان سه نسل را برای آنها در نظرگرفت. نسل اول اقدامات غیرمجازی است که عموماً منجر به اختلال در کارکرد سیستم های رایانه ای می‌شود. نسل دوم جرایم رایانه ای را بیشتر هجوم به داده ها تشکیل می دهد. در نهایت نسل سوم جرایم رایانه ای، ارتکاب آنها در فضای مجازی است. (برای اطلاعات بیشتر ر.ک دزیانی، مقدمه بر ماهیت و تقسیم بندی تئوریک جرایم رایانه ای/۵-۴)

[5]. **Intenet** Network

در بند «و » ماده ۲ قانون تجارت الکترونیک نیز تعریفی از «سیستم های رایانه ای» ارائه شده است. به موجب این ماده سیستم های رایانه ای عبارتند از: «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری - نرم‌افزاری که از طریق اجرای برنامه‌های پردازش خودکار «داده‌پیام» عمل می کنند.» درمقابل سیستم‌های رایانه‌ای «سیستم‌های مخابراتی» نیز وجود دارند، که به هرنوع دستگاه که برای انتقال الکترونیکی اطلاعات، میان یک منبع فرستنده و یک منبع گیرنده اطلاق می شود که از طریق یک یا چند مسیر ارتباطی، به وسیله قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد صورت می گیرد، مانند تلفن همراه‌های امروزی و تلفن‌های ثابت حافظه دار و غیره.

«اینترنت» نیز یک سرویس میان شبکه ای بین المللی است که میلیون ها شبکه رایانه ای را با کاربردهای متفاوت به یکدیگر مرتبط کرد ه است. از دیدگاه فنی، فناوری اینترنت شامل یکسری استانداردهای شبکه ای است که چگونگی ارتباط رایانه ها را تشریح می کند و شامل یکسری قواعدی است که ارتباط میان شبکه‌ها و مسیرهای ترافیک را معین می‌سازد. (داگلاس، ۱۳۷۵ : ۲)

بند ۲۴ گزارش توجیهی کنوانسیون جرایم سایبر، «اینترنت» را یک شبکه جهانی می‌داند که از شبکه‌های متصل بسیاری تشکیل شده است که همه آنها از پروتکل‌های یکسانی استفاده می کنند. (جلالی فراهانی، ۱۳۸۹ : ۱۹) بنابراین «شبکه اینترنت» عبارتست از مجموعه ای از رایانه ها و پایانه های مرتبط با یکدیگر، که قادر به مبادله اطلاعات می باشند. این شبکه برحسب فاصله فیزیکی به شبکه های محلی و شبکه‌های راه دور تقسیم می شوند. شبکه های محلی معمولاً ارتباط بین چند رایانه واقع در یک اتاق یا ساختمان یا تعدادی از ساختمان های واقع در یک بلوک را برقرار می کنند. اما از شبکه‌های راه دور برای ارتباط بین رایانه های واقع در محل های مختلف یک شهر یا رایانه های مستقر در شهرهای مختلف یک کشور استفاده می شود. (آندرواس، ۱۳۷۶ : ۲ – ۴) باتوجه به این که هر یک از شبکه ها اجزای مستقلی هستند که نیازهای یک گروه خاص را برآورده می کنند، برای ارتباط بین شبکه‌های مختلف واقع در یک شهر یا یک کشور یا دو یا چند شهر یا کشور یا قاره مختلف از فن اوری ارتباط بین شبکه‌ای[6] استفاده می‌شود. (داگلاس، ۱۳۷۵ : ۱)

[6] .Internetworking

در مقابل اینترنت نیز «اینترانت» قرار دارد ، یعنی شبکه ای که برای پردازش اطلاعات در یک شرکت یا سازمان طراحی شده است. سرویس هایی چون توزیع سند، توزیع نرم افزار، دسترسی به پایگاه‌های داده و آموزش، از کاربردهای این شبکه است. این شبکه به این دلیل «اینترانت» نام دارد که در آن برنامه های کاربردی مربوط به اینترنت ، مانند صفحات وب، سرورگردان وب، پست الکترونیکی، گروه‌های خبری و لیست‌های پستی، فقط برای کاربران درون شرکت یا سازمان قابل دسترسی است. (بای و پورقهرمانی، ۱۳۸۸ : ۱۹) درواقع اینترانت یک اینترنت خصوصی در داخل یک شبکه است.

۱-۱-۴- داده پیام[۷]

اصطلاح «داده»، یک واژه نسبی است؛ به این معنی که اگر موجب درک و فهم کامل در یک مرحله شود، به عنوان اطلاعات[۸] از آن نام برده می‌شود و چنانچه موجب درک و فهم کامل نگردد، تحت عنوان همان داده به شمار می آید. داده‌ها در رایانه به صورت نمادهای قراردادی (رمزهای صفر و یک) ارائه می‌شوند. برای شکل دهی اطلاعات، داده های خام باید پردازش شوند تا به اطلاعات پرورش یافته تبدیل گردند. (عالی پور، ۱۳۹۰ : ۳۶ و ۳۸) در واقع اطلاعات مفهومی گسترده تر از داده پیام است و به نتیجه‌ای که حاصل پردازش بر روی داده های خام باشد، اطلاعات گفته می شود؛ بنابراین می توان گفت که اطلاعات شکل تغییر یافته داده‌هاست.

«داده رایانه‌ای» در متن کنوانسیون بوداپست به معنای هرگونه نماد حقایق اطلاعات یا مفاهیم، به شکلی مناسب برای پردازش در یک سیستم رایانه ای است که شامل برنامه ای می‌شود که برای کارکرد یک سیستم رایانه ای مناسب است. (جلالی فراهانی، ۱۳۸۹ : ۲۰) طبق بند «الف» ماده ۲ قانون تجارت الکترونیک نیز «داده» عبارتست از «هر نمادی از واقعه، اطلاعات یا مفهوم که با وسائل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.»

مفهوم «داده پیام» خود به دو بخش «داده رایانه ای» و «داده محتوا» تقسیم می شود. «داده رایانه‌ای» همانطور که عنوان شد، عبارتست از هر نمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای

---

[7] .Data

[8] .Information

پردازش در یک سیستم رایانه‌ای یا مخابراتی، که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا بگذارند. اما «داده محتوا» به معنا هر نمادی از موضوع‌ها، مفهوم‌ها یا دستور العمل‌ها نظیر متن، صوت یا تصویر است، که به منظور برقراری ارتباط میان سیستم‌های رایانه‌ای ایجاد می شود. (مانلی و هولدن، ۱۳۸۵ : ۴۲)

«حامل‌های داده» نیز عبارتند از مجموعه‌ای گوناگون از وسایل ذخیره‌سازی اطلاعات، که قابلیت حمل دارند و می‌توان به سادگی آنها را، از یک رایانه به رایانه دیگر منتقل ساخت. مانند دیسک نرم،[9] دیسک سخت، [10] لوح فشرده، [11] نوار مغناطیسی، [12] دیسک ویدئویی دیجیتال [13] و حافظه فلش [14] که این حامل‌ها، هریک ظرفیت‌های متعددی برای ذخیره‌سازی اطلاعات دارند. (مانلی و هولدن، ۱۳۸۵ : ۴۲)

۱-۲- پیشینه تاریخی جرم جاسوسی در فضای مجازی

برای بررسی پیشینه جرم جاسوسی در فضای مجازی، ابتدا باید تاریخچه جرم جاسوسی و جرایم رایانه‌ای که به طور خاص جاسوسی رایانه ای در محور آن جای می گیرد، مورد بحث قرار داد. لازم به ذکر است با توجه به جنبه بین المللی و فراملی جرم جاسوسی، پیشینه این جرم در دو گفتار، تحت عنوان پیشینه تاریخی در عرصه خارجی و داخلی مورد بررسی قرار خواهد گرفت.

۱-۲-۱- پیشینه تاریخی در عرصه برون مرزی

باتوجه به جنبه امنیتی اطلاعات مربوط به حکومت ها، سابقه جرم جاسوسی باید به زمان تشکیل اولین دولت‌ها بازگردد؛ یعنی زمانی که هریک از حکومت‌ها با تعیین مرزهای مشخص برای قلمرو خود،

---

[9] . Floppy Disk

[10] .Hard Disk

[11] .Compact Disk(CD)

[12] .Magnetic Tape

[13] .Digital Video Disc (DVD)

[14] .Flash Memory

به استقلال دست پیداکردند. با مطالعه منابع تاریخی ، اینگونه دریافت می شود که قدیمی‌ترین دولتی که روی کار آمد دولت سومر بوده است که در حدود شش هزار سال قبل ، در نواحی جنوبی بین النهرین مستقر گردیده است. اولین قانون مدون یعنی قانون اورنمو[15] و بعد از آن قانون حمورابی که توسط باستان شناسان کشف شده است متعلق به این دوره تاریخی است. با مراجعه به این قوانین مشاهده می‌شود در زمینه جرایم علیه امنیت عمومی به جرم جاسوسی اشاره نشده است.

اما با گذر زمان و شکل گیری دولت‌های مستقل با قوانین مشخص، برخی از دولت‌ها جاسوسی شماری از اطلاعات را جرم‌انگاری کرده و برای آن مجازات سخت و خشنی تعیین کردند. به طور مثال چینی‌های قدیم برای حفظ انحصار خود در تولید ابریشم، دادن اطلاعات در این زمینه را با اعدام مجازات می کردند. (میرمحمدصادقی، ۱۳۸۱ : ۷۶) در اروپا نیز پس از قرن پنجم و تا قرن چهاردهم میلادی، هنگام طبقه‌بندی جرایم، جاسوسی در رده اولین و مهم ترین جرایم قرار داشت و از زمره گناهان کبیره محسوب می‌شد که شامل جرایم افسران و شاغلین به خدمت عمومی بود. (گارو، ۱۳۴۳، ج ۱ : ۹۸)

بعد از قرن چهاردهم ، با جرایمی از قبیل جاسوسی با شدت عمل بیش تری برخورد می شد و این جرایم تحت عنوان جرایم علیه سلطنت، که شامل سوء قصد علیه شاه یا نزدیکان وی و اعمال ضد حکومت بود، قرار می گرفت. در این دوره مجازات ها بسیار شدید بود و اصول قوانین جزایی از جمله اصل شخصی بودن مجازات ها رعایت نمی شد، لذا بستگان و خانواده محکوم نیز به تحمل مجازات محکوم می‌شدند.

از طرفی در اوایل قرن نوزدهم ، به موجب قانون جزای فرانسه که به اشاره و تحت سیطره و نفوذ ناپلئون تهیه و تنظیم گردیده بود، جرایم سیاسی (خیانت علیه امنیت داخلی و خارجی کشور) از جرایم عادی مجزا شده بود و این تجزیه به دلیل تشدید مجازات جرایمی ، از قبیل جاسوسی و خیانت به کشور نسبت به گذشته بود؛ به‌طوری‌که توطئه را که صرفاً یک عمل مقدماتی بود و از انواع خیانت ها شناخته می‌شد، مورد مجازات قرار می‌دادند. (اسلامی، ۱۳۷۳ : ۵۳– ۵۴) جنگ‌های جهانی اول و دوم که تغییراتی را در اکثر کشورها به وجود آورد، موجب تغییر خطوط مرزی گردید. در این هنگام که آمار جرایم جاسوسی و خیانت به کشور روند رو به افزایش را نشان می داد، تمامیت ارضی و امنیت کشورها در

15. ur-nammu) :(برای اطلاعات بیشتر به سایت زیر رجوع نمایید: http://wikipedia.org/wik/urnammu)

معرض تهدید قرار گرفت. در نتیجه دولت ها در فکر توسعه اقدامات کیفری شدیدتری بر علیه چنین اقدامات برآمدند. (ساریخانی، ۱۳۷۸ : ۳۳)

از طرفی دیگر، با وقوع انقلاب صنعتی عرصه جدیدی در زمینه جاسوسی پیدا شد و رفته رفته به آن میزان از اهمیت دست یافت که در کنار جاسوسی سیاسی، امنیتی و نظامی، ماهیت خود را به نمایش گذاشت. اهمیت انقلاب صنعتی و دستاوردهای آن به اندازه ای بود که به تدریج به عرصه رقابت تبدیل گردید و رقابت صنعتی با توسل به ابزارهای نامشروع، آغازگر عرصه جدیدی در زمینه جاسوسی صنعتی گشت. از سال ۱۸۷۵ اهمیت جاسوسی صنعتی مورد توجه عموم قرار گرفت و رقابت بین جاسوسی صنعتی و نظامی شروع شد. در اواخر قرن ۱۹ کشورهای مختلف درصدد برآمدند تا با بهره گیری از جاسوسی عقب ماندگی خود را جبران نمایند. به همین خاطر جاسوسی صنعتی نیز پشتوانه دولتی پیداکرد. (برژیه، ۱۳۵۵ : ۵۴)

با آغاز دوران جنگ سرد میان کشورهای توسعه‌یافته و گسترش علوم و پیشرفت فناوری اطلاعات، ارتکاب جاسوسی با شیوه های نوین رواج پیداکرد. یکی از این شیوه ها، ارتکاب جاسوسی در فضای مجازی و از طریق سامانه های رایانه ای و مخابراتی بوده است. همانطور که گفته شد، فضای مجازی عبارتست از محیطی غیر ملموس از واقعیت های جهان فیزیکی که از طریق شبکه های بین‌المللی اینترنت، امکان دستیابی کاربران را به این فضا برآورده می‌سازد. بنابراین آنچه که بیش از هر چیز در بررسی پیشینه جرم جاسوسی اهمیت دارد، آغاز ارتکاب جرایم رایانه ای است، که جرم جاسوسی رایانه‌ای نیز بخشی از آن محسوب می‌گردد.

رایانه از دیرباز به شکل اولیه مطرح بوده است. در سال ۱۶۴۲ میلادی پاسکال فرانسوی ماشین حسابی را اختراع کرد که می‌توانست عملیات جمع و تفریق را انجام دهد. (پرهامی، ۱۳۷۱ : ۱۸۵) سی سال بعد این ماشین توسط یک ریاضیدان آلمانی به نام لایپ نیتز تکمیل شد . این ماشین خودکار قادر به انجام عملیات جمع، تفریق، ضرب، تقسیم و گرفتن ریشه‌ها بود . (انزالی، ۱۳۷۴ : ۲) در سال ۱۸۰۱ یک فرانسوی به نام ژوزف ژاکارد، کارت‌های سوراخ دار که ماشین های نساجی را در بافتن پارچه‌های نقش دار هدایت می‌کرد، اختراع کرد. ۱۱ سال بعد، یعنی در سال ۱۸۱۲ یک فرد انگلیسی به نام چالز بابیج که اکثراً از او به نام پدر رایانه‌های نوین یاد می‌شود، نوعی ماشین حساب را به نام «دستگاه تفاضلی» اختراع

نمود. (پرهامی، ۱۳۷۱ : ۱۸۵) بابیج به فکر ساختن وسیله‌ای بود که به رایانه‌های امروزی شباهت زیادی داشت، اما در این کار موفق نشد. بعد از مرگ بابیج، روند توسعه رایانه تا سال ۱۹۳۷ از حرکت باز ایستاد و کارت‌های منگنه شده بر دنیای پردازش داده‌ها حاکم شد. سرانجام نخستین نمونه رایانه الکترونیکی بین سال‌های ۱۹۳۷ و ۱۹۳۸ توسط دکتر جان وینسنت آتاناسوف پرفسور فیزیک و ریاضی مطرح شد و نهایتاً منجر به ساخت رایانه ABC[۱۶] شد؛ این رایانه اولین نمونه از نسل اول رایانه‌های امروزی به شمار می‌آید، که در آن از لامپ های خلاء برای ذخیره‌سازی و عملیات محاسباتی و منطقی استفاده می‌شد . (خرم آبادی، ۱۳۸۴: ۳۰) رایانه‌های نسل اول از دهه ۱۹۴۰ میلادی وارد بازار شدند. این نوع رایانه به لحاظ تعداد کم، حجم زیاد، قیمت گران و تعداد افراد منحصر به فردی که نحوه کار با آن را می دانستند، دارای امنیّت ذاتی بو د. رایانه‌های نسل دوم که از دهه ۱۹۵۰ میلادی وارد بازار شدند ، از رایانه های نسل اول کوچک تر، ارزان تر و سریع تر بودند. به دلیل کثرت افراد و مشاغلی که از یک رایانه استفاده می‌کردند، داده‌ها و برنامه های ذخیره شده آنها در دسترس دیگران قرار می گرفت و آسیب پذیر بودند . نسل سوم رایانه‌ها که به جای ترانزیستور از آی سی (IC)[۱۷] در ساخت آن استفاده شده بود، از اوایل دهه ۱۹۶۰میلادی وارد بازار شد. این رایانه ها دارای حجم و قیمت کمتر و قدرت پردازش و ذخیره بیشتری نسبت به رایانه های نسل های قبل بودند، ولی باز هم در رده رایانه های بزرگ محسوب م ی‌شدند. رایانه‌های نسل چهارم که رایانه های شخصی (PC)[۱۸] می‌باشند، از اوایل دهه ۱۹۷۰ وارد بازار شدند. از خصوصیات ویژه رایانه‌های نسل چهارم، به کارگیری مدارهای مجتمع الکترونیکی در تراکم زیاد بود که باعث کاهش فوق العاده حجم و افزایش قدرت و پردازش آنها می گردید. رایانه‌های نسل پنجم از نظر حجم تفاوتی با رایانه‌های نسل چهارم ندارند. از ویژگی‌های این نسل هوشمند بودن آنهاست، این رایانه‌ها مجهز به هوش مصنوعی اند. در نهایت رایانه‌های نسل ششم، رایانه هایی خواهند بود که مدارهای داخلی‌شان کپی برداری از مغز انسان است، به‌نحوی‌که بتوان از رایانه، انجام دادن کارهایی نظیر مغز انسان را خواست. در رایانه های نسل آینده از فناوری نانو استفاده خواهد شد و نانو رایانه‌ها و نانو روبات ها در بسیاری از علوم، انقلابی جدید ایجاد خواهند کرد. (خرم آبادی، ۱۳۸۴ : ۳۳-۳۰)

16. Atanasoff-Berry Computer
17. Integrated circuits
18. Personal Computer

با گسترش انواع رایانه‌ها، زمینه آغاز به‌کار شبکه اینترنت که یک سرویس میان شبکه‌ای بین‌المللی است، فراهم گشت. پیش نمونه اینترنت با عنوان «آرپانت» [19]را وزارت دفاع آمریکا در سال ۱۹۶۹ برای ایجاد تسهیلات مخابراتی، به هنگام وقوع یک حمله اتمی ایجاد کرد. آرپانت ابتدا صرفاً به وزارت دفاع آمریکا تعلق داشت، اما سپس گسترش پیداکرد و بانک ها و دانشگاه ها وکارگزاری‌های دولتی را نیز در برگرفت. در سال ۱۹۷۳ کشورهای دیگر هم به آن متصل شدند و امکان دسترسی افراد عادی نیز به آن امکان پذیر شد، می‌توان گفت که درواقع اینترنت از بطن فعالیت‌های نظامی زاده شد. (خرم آبادی، ۱۳۸۴ : ۳۳-۳۴)

با وجود گسترش رایانه ها و دسترسی کاربران به شبکه اینترنت، تعیین زمان ارتکاب واقعی اولین جرم رایانه ای کار دشواری اس ت. برخی از پژوهشگران معتقدند واژه جرم رایانه‌ای برای اولین بار در ۱۹۶۰ میلادی ظاهر شده است. اما ممکن است پیش از آن یعنی در زمان ظهور رایانه‌های نسل اول و دوم، جرمی به وسیله این رایانه‌ها یا علیه آنها واقع شده باشد ، اما با دلایلی چون عدم اطلاع بزه دیدگان، عدم آشنایی مأمورین کشف جرم با رایانه و غیره مورد توجه قرار نگرفته‌اند. تا دهه ۱۹۷۰ میلادی شمار سوءاستفاده‌های رایانه‌ای در کشورهای توسعه یافته به اندازه ای اندک بوده است که این کشورها ترجیح می‌دادند، در چارچوب قوانین سنتی با این جرایم برخورد کنند. لیکن پیشرفت فناوری اطلاعات و تنوع و کثرت سوءاستفاده‌هایی که از این فناوری به عمل آمد، حقوق کیفری سنتی کشورها را به چالش کشید. با گسترش علم و توسعه فناوری ارتباطات، داده‌پیام‌ها و اطلاعات رایانه‌ای موضوع جرایم ارتکابی در فضای مجازی قرارگرفتند. در این دوره نیاز به رویکرد نوینی برای برخورد با اَشکال مختلف جرایم رایانه ای ازجمله جاسوسی رایانه‌ای احساس شد. این رویکرد طی مراحلی موجب اصلاح نظام‌های قضایی در زمینه این نوع جرایم شد.

مرحله اول حمایت از اطلاعات خصوصی بود که در دهه های ۱۹۷۰ و ۱۹۸۰ به علت مشکلات ناشی از حفاظت اطلاعات خصوصی آغاز شد، که در این مرحله کشورهای مختلف قوانینی را در راستای حمایت از داده ها در حمایت از حقوق خصوصی و فردی شهروندان به تصویب رساندند . در مرحله بعد ایجاد و اصلاح قوانین ناظر به جرایم رایانه ای از جمله جرایم اقتصادی رایانه ای مدنظر قرار گرفت. در

19 . ARPANET