



## موسسه آموزش عالی شهید اشرفی اصفهانی

دانشکده حقوق و الهیات

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته حقوق  
گرایش جزا و جرم شناسی

### عنوان پایان نامه

جرم جاسوسی رایانه ای در حقوق کیفری ایران و اسناد بین المللی

استاد راهنما:

راضیه قاسمی

استاد مشاور:

علی یوسف زاده

نگارش:

سیدعلی کاظمی

پاییز ۱۳۹۸

دسترس

تقدیم به:

پدر و مادر عزیزم که معجزه‌ی زندگی‌م هستند و به آمان که در راه کسب دانش را همایم بودند.

پاسکزاری:

پاس آفریدگار متعال را که رحمت بی کرانش را در هیچ زمانی از بندگانش دریغ نداشته است. اکنون که این  
پایان نامه به سرانجام رسیده است؛ بر خود لازم می دانم که از زحمات و راهنمایی های استاد بزرگوار سرکار  
خانم دکتر رضیه قاسمی که در تمامی صفحات با سه صدر و راهنمایی های ارزشمند خود مراد تدوین و تنظیم پایان نامه  
یاری کردند؛ تشکر و قدردانی نمایم.

## چکیده

جاسوسی از جمله جرایمی است که علاوه بر صورت سنتی به صورت رایانه ای نیز جرم انگاری شده است. پژوهش حاضر به بررسی اهمیت این جرم در سطح ملی و بین المللی می پردازد. در این پایان نامه در پی شناخت جرم جاسوسی رایانه ای در قوانین داخلی و اسناد بین المللی با روش توصیفی-تحلیلی هستیم تا خلاءها و نواقص هریک را بشناسیم و به یک نظریه جامع برسیم. برای رسیدن به این مهم ابتدا با مفهوم و ارکان این جرم در قوانین داخلی و سپس در اسناد بین المللی آشنا می شویم. جاسوسی رایانه ای در سطوح مختلف ارتکاب می یابد و همزمان با پیشرفت تکنولوژی روز به روز گسترش می یابد. قوانین داخلی ایران و اسناد بین المللی در زمینه مبارزه با این جرم پیشرفت های قابل توجهی داشته اند و با جرم انگاری، ایجاد ضمانت اجرا و اخذ تدابیر پیشگیرانه تا حدودی توانسته اند در زمینه مبارزه با این جرم موفقیت هایی را کسب کنند. از جمله مهم ترین اقدامات داخلی در زمینه مبارزه با جاسوسی رایانه ای می توان به تصویب قانون جرایم رایانه ای در این زمینه اشاره کرد. در عرصه بین المللی نیز تصویب کنوانسیون های مختلف و اقدامات سازمان ملل متحد از جمله گام های مثبت در این زمینه اند.

## واژه های کلیدی:

جاسوسی، جاسوسی رایانه ای، جرایم علیه امنیت، جرایم رایانه ای، اسناد بین المللی.

## فهرست مطالب

مقدمه.....	۱
۱. بیان مسأله .....	۱
۲. سابقه تحقیق.....	۲
۳. ضرورت و نوآوری تحقیق.....	۳
۴. سوال های تحقیق.....	۴
۵. فرضیه های تحقیق.....	۴
۶. اهداف و کاربردهای تحقیق.....	۴
۷. روش تحقیق.....	۴
۸. ساماندهی تحقیق.....	۵
فصل ۱: مفهوم شناسی، مبانی نظری و تحولات قانونی جرم جاسوسی رایانه ای.....	۶
بخش اول مفهوم شناسی و تاریخچه جاسوسی رایانه ای.....	۷
گفتار اول: جاسوسی رایانه ای.....	۷
۱. تعریف لغوی جاسوسی رایانه ای.....	۸
۲. تعریف اصطلاحی جاسوسی رایانه ای.....	۹
گفتار دوم تحولات تاریخی جاسوسی.....	۱۱
۱. جاسوسی در تاریخ اسلام.....	۱۲
۲. جاسوسی دوره باستان و قرون وسطی.....	۱۳
۳. جاسوسی در دوره جدید.....	۱۳
۴. جاسوسی در دوره معاصر.....	۱۴
بخش دوم: مبانی نظری جرم جاسوسی رایانه ای.....	۱۵
گفتار اول نظریه راست جدید.....	۱۵
گفتار دوم نظریه پست مدرن.....	۱۶
گفتار سوم: نظریه ساختار گرا.....	۱۷
۱. نظریات مبتنی بر فشار اجتماعی.....	۱۷

۲. نظریات واکنش اجتماعی. .... ۱۸
- بخش سوم تحولات قانون گذاری در زمینه جرم جاسوسی..... ۱۹
- گفتار اول : قانون مجازات عمومی..... ۲۰
- گفتار دوم قانون مجازات اسلامی..... ۲۱
- گفتار سوم: قانون مجازات جرایم نیروهای مسلح..... ۲۳
- گفتار چهارم قانون جرایم رایانه ای..... ۲۴
- فصل ۲: ارزیابی جرم جاسوسی رایانه ای در نظام حقوقی ایران و اسناد بین المللی..... ۲۵**
- بخش اول: بررسی جرم جاسوسی رایانه ای در نظام حقوقی ایران..... ۲۷
- مبحث اول : نظام جرم انگاری جرم جاسوسی رایانه ای..... ۲۷
- گفتار اول مبانی جرم انگاری جرم جاسوسی رایانه ای..... ۲۸
۱. اصل رفاه..... ۲۹
۲. اصل ضرر..... ۳۰
۳. اصل مصلحت اندیشی قانونی..... ۳۱
۴. اصل کمال گرایی قانونی..... ۳۲
- گفتار دوم عناصر سه گانه جرم جاسوسی رایانه ای..... ۳۳
۱. بررسی مواد قانون جرایم رایانه ای..... ۳۳
- الف. ماده ۳ قانون جرایم رایانه ای..... ۳۳
- یک) بررسی رکن مادی دسترسی غیرمجاز..... ۳۴
- دو) بررسی رکن معنوی دسترسی غیرمجاز..... ۳۵
- سه) بررسی رکن مادی ارائه غیر مجاز به افراد فاقد صلاحیت..... ۳۶
- چهار) بررسی رکن معنوی ارائه غیرمجاز به افراد فاقد صلاحیت..... ۳۶
- پنج) رکن مادی ارائه یا افشای غیرمجاز به بیگانگان..... ۳۶
- شش) رکن معنوی جرم ارائه یا افشای غیرمجاز به بیگانگان..... ۳۸
- هفت) بررسی تبصره ۱ ماده ۳..... ۳۸
- ب) بررسی ماده ۴ قانون جرایم رایانه ای..... ۳۹
- یک) رکن مادی..... ۳۹
- دو) رکن معنوی..... ۴۰
- ج). بررسی ماده ۵ قانون جرایم رایانه ای..... ۴۰

۴۰	یک) رکن مادی.....
۴۱	دو) رکن معنوی.....
۴۲	د). بررسی بند «ج» ماده ۲۵.....
۴۳	یک) رکن مادی.....
۴۳	دو) رکن معنوی.....
۴۴	۲. بررسی مواد قانون تجارت الکترونیک.....
۴۴	الف). بررسی ماده ۶۴ قانون تجارت الکترونیک.....
۴۴	یک) بررسی رکن مادی.....
۴۶	دو) بررسی رکن معنوی.....
۴۷	ب) بررسی ماده ۷۵ قانون تجارت الکترونیک.....
۴۸	یک) بررسی رکن مادی.....
۴۹	دو) بررسی رکن معنوی.....
۵۰	۳. ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح.....
۵۱	الف) رکن مادی.....
۵۲	ب) رکن معنوی.....
۵۲	مبحث دوم: ارزیابی ضمانت اجرای جرم جاسوسی رایانه ای.....
۵۲	گفتار اول: مجازات جاسوسی رایانه ای در قانون جرایم رایانه ای.....
۵۲	۱. مجازات دسترسی غیرمجاز.....
۵۲	۲. مجازات ارائه غیر مجاز.....
۵۳	۳. مجازات ارائه یا افشای غیر مجاز به بیگانگان.....
۵۳	۴ - مجازات نقض تدابیر امنیتی.....
۵۴	۴. مجازات سهل انگاری در حفاظت از داده ها.....
۵۴	۵. انتشار یا در دسترس قرار دادن محتویات آموزش جاسوسی.....
۵۴	گفتار دوم: ارزیابی تناسب و بازدارندگی مجازات جرم جاسوسی رایانه ای.....
۵۸	بخش دوم: جرم جاسوسی رایانه ای در اسناد بین المللی.....
۵۹	گفتار اول: کنوانسیون بوداپست و پروتکل الحاقی آن.....
۶۵	گفتار دوم کنوانسیون جرایم سایبری شورای اروپا (OECD).....
۶۸	گفتار سوم: سند کمیته پیشگیری و بسط عدالت کیفری (۲۰۰۵) شورای اروپا و ملل متحد.....



۷۳	مبحث دوم ارزیابی جرم جاسوسی رایانه ای در اسناد بین المللی
۷۸	نتیجه گیری و پیشنهادها
۷۸	نتیجه گیری
۸۰	پیشنهادها
۸۱	منابع و مآخذ
۸۶	چکیده انگلیسی

## مقدمه:

### ۱. بیان مسأله:

پیشرفت تکنولوژی و علم و دستیابی بشر به فناوری اطلاعات و استفاده از رایانه و به تبع آن پیدایش فضای مجازی دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده است. از جمله پیامدهای منفی آن پیدایش جرایم نوظهور رایانه ای است. ویژگی جهانی و بدون مرز بودن این فضا که مهمترین مشخصه اش نورافکنی در هر تاریک خانه بی خبر و اسرارآمیز با توسل به فناوری تبادل اطلاعات است، امنیت ملی را با چالشی جدید و جدی مواجه کرده است. اگرچه این فشارها کارهای نوینی مانند اطلاع رسانی، رمزنگاری و خبرگیری را برای تأمین امنیت ملی پیش رو نهاده است، اما در مقابل تهدیداتی را وارد این حوزه کرده که ماهیتاً با نظایر فیزیکی متفاوت است. علم حقوق نیز به عنوان شاخه ای از علوم اجتماعی که تنظیم روابط انسان ها را در چارچوب حیات جمعی به عهده دارد، عمیقاً تحت تاثیر انقلاب فناوری اطلاعات قرار گرفته است. جرایم جدیدی که این فناوری در ارتباط با شاخه های مختلف رشته حقوق به وجود آورده است، منجر به شکل گیری رشته ای جدید از حقوق به نام «حقوق جرایم رایانه ای» گردیده است.

لذا کشورهای پیشرفته در راستای مقابله با این پدیده ابتدا اقدام به تعریف جرم رایانه ای نموده و سپس با تصویب قوانین و کنوانسیون های مختلف از جمله کنوانسیون بوداپست اقدام به جرم انگاری موضوعاتی چون جرائم علیه محرمانگی، تمامیت و دسترس پذیری داده ها، جعل، کلاهبرداری، هرزه نگاری کودکان و نقض حق نشر نمودند. اما در این بین آنچه حساس تر به نظر می رسد مسئله مربوط به جاسوسی و دسترس پذیری به اطلاعات محرمانه اشخاص و دولت ها در زمینه های مختلف از جمله اقتصادی، صنعتی و از همه مهم تر نظامی می باشد. جاسوسی رایانه ای جرمی است، که در آن رایانه به منزله ی موضوع جرم، جزء رکن مادی این جرم است که ارتکاب آن قبل از پیدایش رایانه امکان پذیر نبوده است. (زبیر، ۱۳۸۴، ۲۰)

آنچه مسلم است با توجه به وابستگی و پیچیدگی روابط بین دول و ملت ها، جنگ های نظامی و مسلحانه جای خود را به جنگ های سایبری و الکترونیک داده اند. در کشور ما نیز اگرچه دیرتر از کشورهای پیشرفته، قوانینی از جمله قانون تجارت الکترونیک و قانون جرایم رایانه ای در این زمینه تصویب شده است.

آنچه در این پژوهش مورد بررسی قرار می گیرد بررسی جرم جاسوسی رایانه ای در حقوق ایران

و قوانین بین المللی است تا با نگاهی عمیق تر عناصر این جرم در فضای مجازی آشکار گردد . همچنین به لزوم همکاری بین المللی هرچه بیشتر کشورها به دلیل فرامرزی بودن این جرم جهت مقابله و پیشگیری هرچه بهتر از آن، بیان مسائل و مشکلات و نقاط قوت و ضعف قوانین مصوبه و ارائه پیشنهادات و راه حل هایی برای حل این مشکلات پرداخته می شود.

## ۲. سابقه تحقیق:

در رابطه با موضوع تحقیق آثاری نگاشته شده است که به طور غیر مستقیم به برخی از جنبه های موضوع اشاره دارد . در ادامه این آثار بررسی می شوند:

۱. جاویدینیا(۱۳۸۷) در کتاب «جرایم تجارت الکترونیکی» به بررسی جرایم تجارت الکترونیکی که از طریق فضای مجازی ارتکاب می یابد (مثل سرقت، کلاهبرداری، جعل اسناد) پرداخته و با تکیه بر بعد جرم شناسی پیشگیرانه، در راستای این است که با ارائه راهکارهای نظارتی از ارتکاب این جرایم پیشگیری نماید و با وجود اینکه بسیاری از اطلاعات تجارت الکترونیک جنبه محرمانه دارند و چه بسا اطلاعات کثیری که برای اشخاص حقیقی و حقوقی محرمانه است و به طور غیرمجاز دسترسی یا شنود می شوند ولی نویسنده توجهی به جنبه محرمانگی این داده ها و سامانه ها نداشته و فقط به توصیف بعد ضررهای اقتصادی و نحوه پیشگیری از جرایم الکترونیکی مذکور بسنده کرده است .

۲. بای و پورقهرمانی(۱۳۸۸) نیز در کتاب «بررسی فقهی و حقوقی جرایم رایانه ای» معتقدند: «خاستگاه تعاریف و چارچوب جرایم علیه محرمانگی داده و سامانه های رایانه ای عبارتند از: مبانی و مایه های فقهی موجود، مصلحت اندیشی کارشناسانه مجتهدین که جامعه بشری در سایه این مصلحت اندیشی ها توانسته با بیشتر جرایم مقابله کند. فناوری رایانه ای و آنچه به آن پیوند می خورد نیز چاره ای جز سازگاری با مبانی فقهی ندارد؛ به ویژه وقتی خاستگاه اصلی و محور نخست مقررات، فقه اسلامی باشد.» در این کتاب که توسط پژوهشکده فقه و حقوق جمع آوری شده است، تکیه گاه اصلی خود را برای بررسی جرایم رایانه ای بر منابع و موازین فقهی و اجتهاد شیعی قرار داده و به طور تفصیلی به بررسی حقوقی این جرایم پرداخته است، و از آنجا که این کتاب قبل از تصویب قانون جرایم رایانه ای نوشته شده است بیشتر تاکید آن برای مستند کردن مطالب و بیاناتش بر قانون تجارت الکترونیک است، در حالی که هم اکنون با بودن

قانون جرایم رایانه ای باید به بررسی حقوقی جرایم علیه محرمانگی از دید این قانون پرداخت .

۳. خانزاده (۱۳۸۹) در مقاله ی «بررسی و تحلیل قانون جرایم رایانه ای» ضمن بررسی و تجزیه و تحلیل سیاست جنایی کشور در زمینه جرایم علیه محرمانگی داده ها و سامانه های رایانه ای مقرر می دارد که: «سامانه رایانه ای علیرغم تمامی امکانات و اطلاع رسانی در عرصه بین المللی که برای ما به ارمغان آورده است ولی متأسفانه بعضی از افراد سودجو و فرصت طلب با فرا گرفتن دانش و مهارت لازم، راه های دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه نسبت به سیستم های رایانه ای دولتی، خصوصی و... را به دست آورده اند، و به راحتی از طریق این سامانه بدون هیچ گونه قهر و غلبه فیزیکی وارد حریم خصوصی دیگران شده و از محتوای اطلاعات شخصی دیگران مطلع می شوند. این موجب بروز مشکلات و خسارات فراوانی گردیده و یک معضل حاد و بسیار مهم تلقی می گردد؛ لذا دولت ها درصدد پیدا نمودن راه حل های مختلفی در جهت جلوگیری از وقوع آن می باشند.» اگرچه نویسنده به اهمیت جرایم علیه محرمانگی داده ها و سامانه های رایانه ای که در مواد یک تا پنج قانون جرایم رایانه ای جرم انگاری شده مختصر توضیحی می دهد ولی به هیچ وجه به تشریح ماهیت آن جرایم و بررسی ارکان حقوقی تشکیل دهنده آنها نمی پردازد و بیشتر قانون مذکور را از لحاظ ایرادات شکلی قانون گذاری بررسی می کند. مختصرنویسی در زمینه جرایم علیه محرمانگی داده ها و سامانه های رایانه ای دلیل بر آن است که بررسی حقوقی این جرایم که بخش مهمی از قانون جرایم رایانه ای هستند را صرفاً با ذکر ایرادات و انتقاداتی به قانونگذار و در قالب یک یا دو مقاله نمی توان تشریح نمود؛ بلکه بررسی حقوقی این جرایم تحلیل و تشریح مفصلی را می طلبد .

۴. طارمی (۱۳۸۷) در مقاله «گذری بر جرایم رایانه ای» به تعریف کلی جرایم رایانه ای پرداخته و آن را به دو دسته ی سنتی و جدید تقسیم کرده است . این مقاله نیز حرف تازه ای در مورد جاسوسی رایانه ای و ابعاد آن ندارد .

۵. عمیدی (۱۳۸۷) در پایان نامه ی کارشناسی ارشد خود تحت عنوان «مطالعه ی تطبیقی جرایم رایانه ای از دیدگاه فقه و حقوق کیفری ایران» بیشتر به بررسی ابعاد فقهی جرایم رایانه ای به طور کلی پرداخته است .

### ۳ ضرورت و نوآوری تحقیق:

همانطور که دیدیم هر کدام از منابع به بررسی کلی جرایم رایانه ای پرداخته اند . در واقع منبعی

که به طور اختصاصی و جزئی به جرم جاسوسی رایانه ای در حقوق ایران و اسناد بین المللی پردازد و کاستی های حقوق داخلی را در این زمینه بیابد و راهکاری برای آن ارائه دهد وجود ندارد و با توجه به اهمیت این امر لزوم تحقیق در این زمینه ضروری است.

#### ۴. سوال های تحقیق:

۱. آیا ارکان تشکیل دهنده جرم جاسوسی رایانه ای، متفاوت با عنوان سنتی مشابه در سایر قوانین کیفری هستند؟
۲. آیا مقابله با جرم جاسوسی نیازمند اتخاذ تدابیر کیفری پیشگیرانه خاصی است؟
۳. قوانین ایران در مقایسه با قوانین بین المللی در زمینه ی مقابله با جاسوسی رایانه ای چه مزایا و معایبی دارد؟

#### ۵. فرضیه های تحقیق:

۱. جرم جاسوسی رایانه ای جرم جدیدی است و ارکان تشکیل دهنده ی آن با نوع سنتی این جرم تفاوت دارد.
۲. رویارویی با جاسوسی رایانه ای نیازمند اتخاذ تدابیری افتراقی است.
۳. قوانین ایران در زمینه ی مقابله با جاسوسی رایانه ای کاستی هایی دارد و جامع و کامل نیست.

#### ۶. اهداف و کاربردهای تحقیق:

۱. تبیین ارکان تشکیل دهنده و جاسوسی رایانه ای و تفاوت های آن با جرم سنتی مشابه.
۲. مطالعه ی راه کارهای قانونی مقابله با جرم جاسوسی رایانه ای.
۳. بررسی قوانین کیفری داخلی و بین المللی در زمینه ی مقابله با جاسوسی رایانه ای و نقاط ضعف و قوت آنها.

از آنجا که در مورد جرم جاسوسی رایانه ای به طور خاص و به صورت تطبیقی تحقیق کامل و جامعی صورت نگرفته است ، لذا پژوهش حاضر می تواند به عنوان منبعی مستند و مستدل، برای مراجعه حقوقدانان باشد. همچنین تعمقی بر این موضوع می تواند تصمیم سازان عرصه عدالت کیفری را چه در عرصه تقنین و چه در عرصه اجرا و چه در عرصه قضا، جهت اتخاذ

تدابیر مناسب، خصوصاً پاسداری هر چه بهتر از اطلاعات امنیتی در عرصه ملی و بین المللی برای برخورد بهتر با جاسوسی رایانه ای یاری رساند.

#### **۷. روش تحقیق:**

روش تحقیق در این پایان نامه به صورت تحلیلی-توصیفی خواهد بود. روش گردآوری اطلاعات کتابخانه ای خواهد بود بدین صورت که با مراجعه به منابع علمی شامل کتاب، مجله و نشریات ادواری موجود در کتابخانه ها و همچنین سایت های اینترنتی اطلاعات مورد نیاز جمع آوری خواهد شد.

برای تجزیه و تحلیل داده ها از انواع نرم افزارهای کامپیوتری استفاده می شود.

#### **۸. ساماندهی تحقیق:**

این پایان نامه شامل دو فصل می باشد. در فصل اول به بیان مفاهیم و کلیات تحقیق می پردازیم در فصل دوم به بررسی جرم جاسوسی رایانه ای در حقوق ایران و اسناد بین المللی خواهیم پرداخت و جزئیات و عناصر این جرم را مطالعه می کنیم و در نهایت نتایج و پیشنهادات تحقیق را مطرح می کنیم.

# فصل ۱ :

## مفهوم شناسی، مبانی نظری و تحولات قانونی جرم جاسوسی رایانه ای

در این فصل ابتدا مفاهیم اصلی تحقیق را مطالعه می کنیم و سپس مبانی نظری مرتبط با موضوع پژوهش را مطرح می کنیم و در نهایت تحولات قانون گذاری جرم جاسوسی رایانه ای را بیان می کنیم.

### **بخش اول: مفهوم شناسی و تاریخچه ی جاسوسی رایانه ای**

برای فهم بهتر موضوع پژوهش لازم است؛ عنوان آن و دیگر اصطلاحات به کار رفته در آن را به طور جزء جزء مورد بازخوانی قرار داده و مفاهیم پنهان در آن را که تا پایان پژوهش مورد استفاده خواهد بود آشکار کرده و آن چه منظور ما از آن بوده است را بیان کنیم. مشخص ساختن تعاریف و ارائه معانی و مفاهیم براساس تعاریف ذکر شده، منجر به انتقال معنای مورد نظر پژوهشگر به خواننده می گردد؛ چرا که ممکن است هر شخصی بر اساس برداشت خاص خود، واژگان مهم تحقیق را تعریف نماید و احیاناً هماهنگ با محقق نباشد و سرانجام، در دستاوردهای تحقیق به تفاهم نرسند؛ بنابراین، در ذیل به تبیین مفاهیم پرداخته می شود.

### **گفتار اول: جاسوسی رایانه ای**

جاسوسی قدرت دانستن است. قدرتی که با آن می توان فهمید چگونه حوادث به امتیازاتی برای کشورها تبدیل میشود. بدین سبب کشورهای مختلف به طور معمول اجازه این امر را به خود می دهند که برای حفظ موقعیت، حراست از مرزهای جغرافیایی و تقویت پیروزیهای خویش در مقابل رقیب، به اطلاعاتی در زمینه های اقتصادی، سیاسی، فرهنگی، نظامی و غیره دسترسی پیدا نمایند و برای حصول به این مقصود همواره در صدد پیدا کردن و اجیر نمودن نیروهایی هستند که از هر طریق و به هر قیمت ممکن اطلاعات را در اختیار آنها قرار دهد. اگر در گذشته جاسوسی در قالب کلاسیک و منحصر به نوع نظامی بود و پیروزی در این بعد موفقیت محسوب میشد، با ورود بشر به عصر فناوری اطلاعات، جاسوسان بدون بکارگیری ابزارهای قاهرانه فیزیکی، با استفاده از فرصت ها و ابزارهای رایانه ای فنی و نرم افزاری، فارغ از مرزهای



جغرافیایی اطلاعات اقتصادی سیاسی نظامی و... کشورهای مختلف در اقصا نقاط جهان را، بدون حضور فیزیکی در محل وجود اطلاعات، بدست آورده و خسارات سنگین و جبران ناپذیری را بر پیکره امنیت این کشورها وارد می کنند(بابایی، ۱۳۸۸، ۱۱). پیشرفت تکنولوژی موجب گردید که فضای مجازی و قابلیت های آن برای نگهداری اطلاعات، جایگزین فضای مادی شوند. شیوع استفاده از این فضا در راستای نگهداری اطلاعات، آن را به آماج مناسب برای جاسوسان تبدیل کرد تا با ورود به آن، اطلاعات مورد نیاز خود را گردآوری نمایند. توجه جاسوسان به این فضای جدید به عنوان آماج جرم جاسوسی توجه قانونگذاران را نیز جهت حمایت بیشتر از آن، به این مقوله جلب کرده و جاسوسی رایانه ای در عالم حقوق کیفری پا به عرصه وجود نهاد.

### ۱. مفهوم لغوی جاسوسی رایانه ای

از نظر لغوی جاسوسی رایانه ای از دو لفظ جاسوسی و رایانه ای تشکیل شده است. به همین دلیل هر کدام از کلمات جاسوسی و رایانه ای را به طور جداگانه بررسی می کنیم

ممکن است تصور شود که معنا و مفهوم جاسوسی به سبب روشن بودن آن، نیازی به بررسی و بیان نداشته باشد لکن با توجه به معانی مختلفی که این واژه دارد بهترین معنای عبارت است از: کنجکاوی کردن، بررسی کردن، خبرجستن از امور مردم، اموری که مردم می خواهند پنهان بماند.

جاسوسی مشتقات ماده «س م ع» در لغت به معنای مترادف با جاسوس استعمال شده است. سماعون: به معنای جاسوسان و خبر جویان. (سیاح، ۲، ۱۳۷۶/۷۳۲)

جاسوسی در لغت به معنای تفتیش و تحقیق و تفحص از امور و اخبار و اطلاع دادن از آنها و هم خانواده تجسس و اجتسس آمده است و جاسوس کسی است که اخبار و اسرار کسی یا اداره یا مملکتی را به دست بیاورد و به دیگری اطلاع دهد. (عمید، ۱۳۸۴، ۶۴۰)

دهخدا در مورد جاسوسی می گوید: «جاسوس جستجو کننده خبر برای بدی شخصی باشد که از ملکی برای ملک دیگر خبر برد.» (محمدی، ۱۳۸۷، ۱۲)

در ترمینولوژی حقوق، جاسوسی این گونه بیان شده است: (بین الملل عمومی) «کسی که محرمانه یا تحت عنوانهای نادرست بنفع خصم در صدد تحصیل اطلاعاتی از نقشه و قوای طرف و مقاصد او برآید.» (جزایی) «اشخاص ذیل جاسوسند: الف - هر کس که برای بدست آوردن اسناد یا اطلاعاتی بنفع دشمن به یک قلعه یا مکان مستحکم یا پاسگاه یا هر بنگاه نظامی یا استحکامات و اردوگاههای ارتش داخل شده باشد. ب - هر کس که برای دشمن اسناد یا اطلاعاتی بدست

آورد که ممکن است نسبت به عملیات ارتش یا نسبت به تأمین قلاع یا امکانه مستحکم یا پاسگاهها یا بنگاههای نظامی مضر باشد. ج - هر کس که جاسوسان یا افراد دشمن را که برای اکتشاف مأمور شده باشند عمداً مخفی نموده یا سبب اختفاء آنها گردد. هر کس که اسرارنواحی یا سیاسی یا مفاتیح رمز را بر خلاف مصالح کشور به اجنبی تسلیم کند» (لنگرودی، ۱۳۸۵، ۱۸۹). رایانه هم معادل فارسی لفظ کامپیوتر در زبان انگلیسی است، و وسیله یا دستگاهی است که میتواند اطلاعات و برنامه های کار را در حافظه اش نگهداری کند و طبق دستور موجود در برنامه های مزبور اطلاعات را بپذیرد و پس از پردازش به صورت اطلاعات و گزارش های خروجی مشخص ارائه کند و تمام انواع رایانه ها، از رایانه های کیفی و رایانه های خانگی مد نظر است. (آریا، ۱۳۷۲: ۳۲)

کار جاسوس یک پازل دائمی است که از شکل ها و رنگ های مختلفی ساخته شده است و این رنگ ها و شکل ها مدام شکل می گیرند و از شکل می افتند. جاسوسی شامل جستجوی پایان ناپذیر برای یافتن قطعات جدا از هم است که تحلیل گران سرویس های مخفی آن ها را برای پازل خود جمع می کنند. جاسوسی رایانه ای شکل مدرن و توسعه یافته همان جاسوسی سنتی است که با همان اهداف انجام می شود.

## ۲- مفهوم اصطلاحی جاسوسی رایانه ای

با وجود اهمیت جاسوسی، در هیچ کدام از قوانین کیفری تعریفی صریح و روشنی از جاسوسی ارائه نشده است، فقط در برخی از قوانین آن هم با عباراتی پیچیده و مبهم، تعریفی از جاسوسی ارائه شده است. به نظر دلیل این امر رعایت امنیت و مصالح کشورهاست؛ چرا که در صورت تعریفی روشن و صریح امکان سوءاستفاده زیاد میباشد.

علیرغم این سکوت قوانین و یا ارائه تعاریف کشدار از جاسوسی که مقتضای حفظ ارزش های مورد حمایت در امنیت ملی کشورهاست، حقوقدانان متعددی بنا به اقتضاء، به بحث در مورد جاسوسی و ارائه تعاریفی از آن پرداخته اند.

در یک تعریف عام، جاسوسی رایانه ای یا سایبری عبارت است از:

وضعیت اهداف رایانه ای یا ارزیابی سیستم دفاعی رایانه، رویت اطلاعات و کپی برداری غیرقانونی از داده های فایل. است چنانکه پروفیسور گارو نیز منظور از جاسوسی را ارتکاب اعمالی میداند که مرتکب به صورت محرمانه و با لباس مبدل و تغییر شکل، اسرار ملی را تحصیل کنند و به نیروهای خارجی تسلیم نمایند. (گارو، ۱۳۸۱، ۶۷۶)

در حقوق بین الملل کلاسیک تعریفی که از جاسوسی ارائه شده بحث جاسوسی در مخاصمات مسلحانه است که از دیرباز مطرح بوده است و عبارت است از «کسب اطلاعات و اخبار نظامی از دشمن» (بابائی، ۱۳۸۸، ۱۸)

از نظر حقوق بین الملل عمومی جاسوس به کسی گفته می شود که تحت عنوان های نادرست و جعلی به نفع خصم در مورد تحصیل اطلاعاتی، از نقشه، قوای طرف و مقصد او برآید. جاسوس فردی است که اخبار و اطلاعات کسی یا موسسه ای و یا کشوری را مخفیانه گردآورده و به شخص یا موسسه یا کشوری دهد. (جعفری لنگرودی، ۱۳۸۵، ۱۸۹)

در حقوق بین الملل نوین با برداشته شدن مرزهای جغرافیایی و کمرنگ شدن حاکمیت ها و تبدیل و ارتقاء موضوعات داخلی همچون حقوق بشر به موضوعات بین المللی پیشرفت های چشمگیر صنعتی در زمینه های مختلف به خصوص در امور فضایی سبب آن شده است که دیگر موضوع حقوق بین الملل و جاسوسی منحصر به مخاصمات مسلحانه نگردد و در شاخه های مختلف حقوق بین الملل همچون حقوق بشر دیپلماسی، حقوق بین الملل فضا و... نیز ظهور و بروز جاسوسی را ملاحظه کنیم. فارغ از گستردگی مفهوم جاسوسی، غالباً قانونگذاران جرم را صرفاً به دو رفتار جمع آوری اطلاعات و دادن آن به دشمن منحصر ندانسته و دریافته اند که مراحل تحقق جاسوسی دلیلی بر استمرار پنداشتن این جرم نمی شود؛ به عبارت دیگر مراحل سه گانه جاسوسی که عبارتند از شناسایی و تعیین اطلاعات مورد نیاز، جمع آوری اطلاعات و بالاخره تجزیه اطلاعات جمع آوری شده که نهایتاً منجر به هدف اصلی جاسوسی یعنی ارایه اطلاعات به مسوولان یک دولت یا شرکت بیگانه جهت اتخاذتصمیم است موجب نشده تا قانونگذاران در جرم انگاری این جرم منتظر حصول نتیجه شوند، بلکه بدون توجه به مراحل مزبور، هر رفتار فیزیکی مرتبط با جاسوسی را به عنوان جرمی جداگانه تلقی کرده اند. (بابایی، ۲۲، ۱۳۸۸)

ماده ۱۹ قطعنامه بروکسل مصوب ۱۸۷۴ می گوید: «جاسوس کسی است که به طور مخفیانه و با وسایل و بهانه های مجعول اطلاعات را جمع آوری یا برای تحصیل اطلاعات در نقاط اشغال شده به وسیله ی نیروی دشمن با قصد اینکه آن ها را به طرف مقابل تسلیم نماید، تجسس می کند.» (محمدی، ۱۳۸۷، ۱۴)

با توجه به توضیحات فوق ممکن است دو برداشت از معنای جاسوسی رایانه ای به ذهن متبادر شود:

اولاً ممکن است این برداشت شود که جاسوسی رایانه ای، جاسوسی است که به وسیله رایانه انجام می شود. یعنی جاسوسی رایانه ای یکی از انواع جاسوسی کلاسیک است و به بیان دیگر هر گاه جاسوسی کلاسیک به وسیله رایانه محقق شود آن را جاسوسی رایانه ای می گویند .

ثانیا ممکن است این برداشت شود که جاسوسی رایانه ای، جاسوسی است جدای از جاسوسی کلاسیک و جرمی است مستقل از آن که در فضای سایبر (مجازی) صورت میگیرد و کاملاً از جاسوسی کلاسیک مستقل و جدا است؛ که به نظر ما برداشت دوم صحیح تر به نظر می رسد؛ زیرا از نظر ما جاسوسی به دو دسته کلی جاسوسی رایانه ای و جاسوسی کلاسیک تقسیم می شود و جاسوسی کلاسیک به وسیله رایانه هم (برداشت اول از جاسوسی رایانه ای) جزئی از جاسوسی کلاسیک است و یک از مصادیق و راههای انجام جاسوسی کلاسیک است و با جاسوسی رایانه ای مد نظر ما فرق دارد .

در بیان خلاصه جاسوسی رایانه ای را می توان اینگونه تعریف کرد:

دسترسی، در دسترس قرار دادن و افشای غیرمجاز داده های سری دارای ارزش اطلاعاتی، اعم از در حال انتقال یا ذخیره شده، از هر طریقی در رایانه و فضای سایبر.

در مورد این تعریف نکاتی را باید بیان کرد :

۱ - منظور از اطلاعات اعم است از اطلاعات مالی و غیرمالی و اطلاعات نوشتاری، غیرنوشتاری و سمعی و بصری و به طور کلی هر نوع اطلاعاتی .

۲. «دارای ارزش اطلاعاتی» منظور آن اطلاعاتی است که دارای ارزش باشد و به اصطلاح اخبار و خبرهای سوخته نباشد؛ چرا که ممکن است فردی به اطلاعاتی غیرمجاز دسترسی یابد که ارزش اطلاعاتی ندارد و به نظر ما از شمول جرم جاسوسی رایانه ای خارج میشود .

۳. «از هر طریقی» منظور هر روشی که فرد و اطلاعات دارای ارزش اطلاعاتی را در محیط رایانه کسب کند را باید شامل این جرم دانست و تمام راههای مد نظر این تعریف است .

۴. «در محیط رایانه» اعم است از هر محیط رایانه ای چه رایانه های بزرگ چه رایانه های کیفی و چه شبکه های رایانه ای مدنظر است.

۵ - «فضای سایبر» نیز بستر ارتکاب این جرم را معین می کند.

### گفتار دوم تحولات تاریخی جاسوسی:

جاسوسی از زمره جرایم قدیمی است که همواره مورد برخوردهای سخت و خشن قرار گرفته است برخی قدمت تاریخی این جرم را حداقل به زمان حضرت موسی «علیه اسلام» برمی گردانند.