
بسم الله الرحمن الرحيم

دانشگاه پیام نور مرکز تهران

دانشکده علوم انسانی

گروه حقوق

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته حقوق جزا و جرم شناسی

عنوان:

مقایسه جرم جاسوسی درمحیط حقیقی ومجازی

استاد راهنما :

آقای دکترمهدی نقوی

استاد مشاور:

آقای دکتر نریمان فاخری

دانشجو:

سیده فهیمه طاهریان

تابستان ۱۳۹۰

تقدیم به:

روح پدرم که اصلی ترین مشوقم به آموختن بود

و

دستان پر مهر مادر مهربانم

سپاسگزاری:

سرآغاز کلام سپاسی است ویژه محضر استادگرانقدر جناب آقای دکتر مهدی نقوی که به عنوان استاد راهنما قبول زحمت نموده و اینجانب را در عین تواضع از گنجینه غنی معلومات خویش بهره مند ساختند.

همچنین از استاد بزرگوار مشاور، جناب آقای دکتر نریمان فاخری نیز کمال تشکر و تقدیر را دارم، بهره مندی از راهنمایی های علمی ایشان نقش مؤثری در تکمیل این پایان نامه داشته است.

و در آخر تقدیر و تشکر خاص خود را به مادر مهربان و خواهر عزیزم تقدیم می دارم که در همه حال یار و یاور و همراه و مشوقم در پایان دادن به این پایان نامه بوده اند.

چکیده

با تصویب قانون جرایم رایانه‌ای (۱۳۸۸)، مفاهیم وجرایم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشد.دراین میان،جرم جاسوسی اگرچه یکی ازجرایم قدیمی و کلاسیک حقوق جزابه شمار می‌رود، ولی درپرتو پیشرفت‌های فناوری، نحوه ارتکاب آن دستخوش تغییراتی می‌شود که در قانون جرایم رایانه‌ای تحت عنوان جاسوسی رایانه‌ای، جرم انگاری شده است.

هرچند که وقوع جرم جاسوسی به هرطریقی امکان پذیراست بعنوان مثال می توان اطلاعات راازطریق تلفن به شخص حقوقی یا حقیقی دیگر اطلاع داد وازحیث ابزاربکار برده شده تفاوتی دروقوع جرم ندارد.

اما جرم جاسوسی رایانه ای تفاوتهایی دارد که به همین لحاظ ازجلدجرم کلاسیک بیرون آمده وشکل نوینی ازاین جرم راپدیدآورده است.

ازآنجاییکه اکثرکشورها به وضع قوانین خاص درخصوص جرائم رایانه ای پرداخته اند لزوم وضع این قوانین درکشور مانیزبه چشم می خوردبه خصوص اینکه جرم جاسوسی کلاسیک درکشورما بیشتر ناظربه مسائل نظامی وسیاسی وامنیتی است ومسائل بازرگانی واقتصادی درآن نادیده انگاشته شده درحالیکه دراکثر کشورها جرم جاسوسی اقتصادی نیز درنظر گرفته شده است.

جاسوسی سایبری، واقعیتی سیاسی- اجتماعی و فنی- حقوقی است که شناخت آن و یافتن جایگاهش در نظام حقوقی داخلی و بین‌المللی، وابسته به انجام مطالعات میان رشته‌ای است.

علاوه بر جرم انگاری، رویارویی با اعمال جاسوسی سایبری، نیازمند پیشگیری و اتخاذ تدابیر شکلی افتراقی وخاص است.

کلیدواژه: فضای سایبر،جرایم سایبری ،جاسوسی، جاسوسی اینترنتی ، جاسوسی کامپیوتری ، جاسوسی سنتی ، محیط حقیقی ، محیط مجازی

فهرست مطالب

عنوان صفحه

مقدمه

ورودبه اسرارمردم ازجمله اعمالی که موردمذمت ادیان الهی و اخلاق عمومی جوامع بوده،که متأسفانه با گسترش عرصه‌فن‌آوری اطلاعات وارتباطات[1] آفت‌های این پدیده شگرف نیزاز پیچیدگی‌های خود برخوردار است. مگر نه آن است که خواجه‌شیراز فرمود:

آنکسست اهل بشارت که اشارت داند

نکته هاهست بسی محرم اسرارکجاست

حافظ از باد خزان در چمن دهر مرنج

فکر معقول بفرما گل بی‌خار کجاست[2]

روزگاری فضای مجازی تنها منحصر به ذهن انسان بود. انسان از همان ابتدا در ذهن خود تخیلاتی داشت بیرون از مکان و متواری از زمان و در این فضا خود را از همه چیز رها می‌کرد.گاه به ماه می شتافت و گاه خورشید را به خانه اش می‌آورد. گاهی یاور همه مظلومان می‌شد و گاه بر سر خود تاج ثروت و مکنت می‌یافت. گاه خود را اندرون زیبایی‌ها می‌دید و گاه خود را سیراب از چشمه حیات جاودان می‌کرد.گاهی ریسمان محکم برگردن همه مشکلاتش می افکندوگاه قدرت شمارش پیروزی-هایش را از کف می داد؛ ولی همه اینها در فضای ذهنش بود. فضایی تنها که خود آن را مرور می کرد؛ نه می توانست ببیند و نه می‌توانست به دیگران نشان دهد.

فضای سایبر یا فضای مجازی که درگام اول با رادیووتلویزیون مطرح گردیدوسپس رایانه و مخابرات و از همه مهمتر اینترنت پایه‌هایش را بنا نهادند، دست کمی از ذهن آدمی ندارد. ولی این فضا هرچند همچون ذهن درگیر و دار زمان و مکان نیست و نمی توان در آن پا نهاد ولی می‌توان آن را دید و می‌توان به دیگران نیز نشان داد. این فضای خارق العاده تنها چهره دورنمای ذهنی دارد ولی در عمل با زندگی انسان عجین شده و معنای دیگری به آن داده است. دریک کلام با توجه به دارایی‌ها و

[1]. Information Technology

[2]. حافظ شیرازی، خواجه شمس الدین محمد، ۱۳۷۰، انتشارات حافظ نوین ، مصحح عبدالرحیم خلخالی، غزلیات ص۵۷

ویژگی‌های فضای سایبر باید پذیرفت که جهان جدیدی در برابر جهانی که تا کنون می شناختیم و می شناساندیم، ظهور کرده است. جرم جاسوسی متعلق به این جهان پراز تارنما[1] است.

برای دانستن بستری که در آن جاسوسی اینترنتی شکل می‌گیرد و خیره سرانه رشد می‌یابد، ابتدا باید بسترارتکاب یا همان فضای سایبر و ارزش‌ها و هنجارهایی که در آن حاکم است را شناخت. شاید بتوان گفت که امنیت این فضا در برابر جاسوسی اینترنتی مهمترین ارزش به شمار می‌رود.

با رایانه ای شدن اموروتجهیزمراکز حساس به رایانه واینترنت ، احتمال وقوع جاسوسی به نسبت گذشته افزایش یافته است،بااین تفاوت که درفضای سایبر هرلحظه حجم عظیمی از اطلاعات مبادله می شوند وهرکاربراینترنتی که خلاقیت نفوذ درسیستم داشته باشد، می تواند جاسوسی کند .

جاسوس رایانه ای نه منحصراً از طرف دولت یا شرکتی خاص مأموربه جاسوسی است ونه لزوماً قصد ابتدایی اش نفوذ به سیستم رایانه ای حاوی اطلاعات حساس یا طبقه بندی شده است ، بلکه دربرخی موارد کسب اطلاع درفضای سایبر بدون سوء نیت علیه امنیت ملی وصرفاً دراثر کنجکاوی انجام می شود ، امادرهرحال می تواند عواقب سوئی علیه امنیت ملی داشته باشد.

امنیت ملی ، پیوند محکمی با مرزهای سرزمینی ورابطه دیرینه ای با وضعیت داخلی کشور دارد . اما درفضای سایبر که مرزهای مشخصی برای آن ترسیم نشده ودنیای کوچک است که همه دنیای بزرگ را بهم پیوند می دهد ، نمی توان از اقدامات سنتی برای پاسبانی امنیت ملی درفضای سایبر سود جست ، زیرا به قول جناب رنو، دادستان آمریکایی، درفضای سایبر یک هکر نیازی به گذرنامه ندارد ، زیرا درهیچ معبری بازرسی نمی شود .

ویژگی جهانی وبدون مرز بودن این فضا که مهمترین مشخصه اش نورافکنی درهر تاریک خانه بی خبر واسرارآمیز با توسل به فناوری تبادل اطلاعات است ، امنیت ملی رابا چالشی جدید وجدی مواجه کرده است . اگرچه این فضاراهکارهای نوینی مانند اطلاع رسانی ، رمزنگاری وخبرگیری رابرای تأمین امنیت ملی پیش رو نهاده است ، امادرمقابل تهدیداتی راوارد این حوزه کرده که ماهیتاً با نظایر فیزیکی متفاوت است .

---

[1]. وب سایت یاوب‌گاه (به انگلیسی: SiteWebیاWebsite) مجموعه‌ای از صفحات وب است که دارای یک دامنه اینترنتی یا زیردامنه اینترنتی مشترک‌اند.

ارتکاب دوجرم مشهور جاسوسی رایانه ای واقدامات تروریستی سایبری ، اگر درحدی بود که رایانه برای تحقق آنهافقط نقش وسیله را داشت ،هردوراجرم سنتی فرض می کردیم وباقوانین وراهکارهای غیرسایبری موجود به پیشگیری ازآنها می شتافتیم .اما دراین دو جرم ، اولاً موضوع مستقیم، امنیت ملی نیست تا ادعا کنیم همان موضوع سنتی جرایم علیه امنیت است . موضوع جرم درجاسوسی محرمانگی داده وسیستم ها ودراقدامات تروریستی سایبری ،امنیت اطلاعات وشبکه است که به دلیل پیوند امنیت ملی با آنها ، از جاسوسی رایانه ای واقدامات تروریستی سایبری نهایتاً به عنوان جرایم علیه امنیت ملی یادمی کنیم .ثانیاً درهر دو جرم ، وسیله بابستر درهم آمیخته ودرزمانی بسیار کوتاه ودرمکان های متکثر مورد نظر مرتکب تحقق می یابد، کیفیتی که نمی توان درجرایم سنتی سراغ گرفت .

مع الوصف به زودی با دنیای کاملاً رایانه ای واینترنتی مواجه خواهیم شد که اگر برخورد مناسبی باآن نکنیم ، به پدیده ای مخوف وکنترل ناپذیر علیه همه چیز ، اعم از امنیت ملی ، اخلاق ، دین وروابط اجتماعی وخانوادگی تبدیل خواهد شد.

۱.بیان مسأله

در یک تعریف عام، جاسوسی رایانه‌ای یا سایبری عبارت است از « جستجوی غیرمجاز برای آزمودن وضعیت اهداف رایانه‌ای یا ارزیابی سیستم دفاعی رایانه یا رؤیت اطلاعات یا کپی برداری غیر قانونی از داده های فایل است.»[۱] جاسوسی سایبری شامل وارسی غیرمجازجهت کشف پیکربندی کامپیوتر مورد هدف، یا ارزیابی حفاظت‌های سیستمی آن یا مرور و کپی برداری غیرمجاز از فایل های داده‌ای است.

جاسوسی رایانه‌ای اساساً با جاسوسی سنتی تفاوتی ندارد و در هر دو، مرتکب در جستجوی اطلاعات است. حتی انگیزه های ارتکاب این دو گونه از جاسوسی نیز می تواند شبیه هم باشد.[۲] به همین دلیل

---

[۱] . CRS report for congress: **Botnets, Cybercrime, and Cyberterrorism**: Vulnerabilities and Policy issues for Congress, January ۲۰۰۸,P.۱۲

[۲] . برای دیدن برخی ار مهمترین انگیزه های جاسوسی ر.ک میرمحمد صادقی، حسین؛ جرایم علیه امنیت و آسایش عمومی، ص ۷۹ به بعد

می توان گفت که در جاسوسی رایانه ای، رایانه تنها در حد وسیله است و به جهت الکترونیکی شدن اطلاعات و رایانه ای شدن فعالیت های امنیتی، اهمیت یافته است.

جاسوسی در معنای دقیق کلمه، همان تجسس وکنکاش است و عموماً مرحله ای پس ازحمله سایبری را در بر می گیرد. در واقع حمله کننده پس از دسترسی به رایانه، اقدام به جستجوی اطلاعات می نماید. این نوع حمله نیز مقدمه‌ای برای کسب اطلاعات و انجام حمله‌های سایبری مخرب و مختل-کننده است و با انجام آن محرمانگی سیستم و داده‌ها نقض می‌شود.جاسوسی سایبری بسیار خطرناک است؛ زیرا با در نظر گرفتن این که شکاف امنیتی پس از کشف متجاوز قابل اصلاح است، نقاط ضعف نا آشکار امنیتی این امکان را می دهد تا از آنها نه برای یک بار، بلکه برای مدت زمانی طولانی بهره برداری کند.

در عمل قانونگذاران کشورهاواز جمله ایران، جاسوسی را تنها به معنای تجسس و وارسی تلقی نکرده و قبل و بعد از این رفتار را نیز لحاظ کرده‌اند. به سخن دیگر جاسوسی شامل **سه رفتار ورود به مواضع یا مکان حاوی اطلاعات طبقه‌بندی شده، تجسس و تحصیل اطلاعات و در نهایت افشاء یا ارایه اطلاعات است.** به جهت حساسیت اطلاعات طبقه‌بندی شده و ارتباط آنها با امنیت کشور، زمینه جاسوسی که همان ورود به مواضع یا مکان مربوطه است نیز جرم دانسته شده است.[1]

جاسوسی رایانه ای بر خلاف جاسوسی سنتی که جایگاه مبهمی در قانون مجازات اسلامی دارد، با شفافیت در ماده ۳ قانون جرایم رایانه ای(ماده ۷۳۱ قانون مجازات اسلامی) پیش بینی شده است. طبق این ماده«هرکس به طورغیرمجاز نسبت به داده‌های سری درحال انتقال یاذخیره‌شده درسامانه‌های رایانه‌ای یا مخابراتی یاحاملهای داده مرتکب اعمال ذکرشده درقانون شود،به مجازاتهای مقرر محکوم خواهدشد.»

جاسوسی رایانه ای در حقوق کیفری ایران در سه مرحله تحقق می یابد که هر سه مرحله به طور مجزّا جرم تلقی می شود. **مرحله نخست**، دسترسی به داده‌های سری یا تحصیل آنها یا شنود محتوای سری در حال انتقال که با جاسوسی سنتی از حیث ورود به مواضع ممنوعه که اطلاعات در آن واقع شده اند برابری می‌کند. مرحله نخست جاسوسی رایانه ای در واقع همان دسترسی غیرمجاز است و

---

[1]. بتول ، پاکزاد ،۱۳۸۸ ،**تروریسم سایبری** ، پایان نامه دکتری حقوق کیفری وجرم شناسی ، دانشگاه شهید بهشتی ، تهران ، ص ۱۸۲ به بعد

به لحاظ رفتاری با هم تفاوتی ندارند ولی از جهت قصد مرتکب، در دسترسی غیرمجاز مرتکب صرفاً در صدد نقض تدابیر امنیتی و ورود به سیستم است در حالی که در جاسوسی، مرتکب به قصد به دست آوردن اطلاعات به سیستم رایانه ای دیگری رخنه می کند. از این رو ماده ۴ قانون جرایم رایانه ای، با تکرار ماده یک این قانون که درباره دسترسی غیرمجاز است، تنها موضوع جرم را تغییر داده است. در ماده ۴، موضوع جرم، داده های سری است.

مرحله دوم ، در دسترس قراردادن داده‌های سری برای اشخاص فاقد صلاحیت و **مرحله سوم** که مشابه با مرحله دوم بوده ولی متضمن اقدام خطرناک تری است افشایا در دسترس قرار دادن داده‌های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها است. بدیهی است که درجاسوسی، موضوع جرم حالتی کاملاً امنیتی دارد و آنچه که ماده۳ قانون جرایم رایانه ای پیش بینی کرده، جاسوسی سیاسی است زیرا طبق تبصره۱ ماده۳ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

در کنار این نوع جاسوسی باید ازجاسوسی تجاری، صنعتی و اقتصادی نیز یاد کرد که می تواند مورد توجه تروریست ها قرار بگیرد. از این رو برخی کشورها، جاسوسی صنعتی که متضمن افشای اسرارتجاری و صنعتی است را، مقوله ای امنیتی می‌دانند؛ برای نمونه، قانون جاسوسی اقتصادی ۱۹۹۶ ایالات متحده، ربودن، شروع به ربودن و تبانی برای ربودن اطلاعات را جاسوسی اقتصادی دانسته است.[۱] البته این قانون شرط قصد رساندن منفعت به یک عامل بیگانه را نیز ذکر کرده که این امر جاسوسی صنعتی را به جاسوسی سیاسی نزدیک می کند.

ماده ۵ قانون جرایم رایانه‌ای نیز به تقلیداز قانون مجازات اسلامی(ماده ۵۰۶)، رفتارهای غیرعمدی مأمورین مربوطه که منجر به تخلیه اطلاعاتی می شود را نیزجرم دانسته است. طبق این ماده چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده۳ این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است براثربی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حاملهای داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای

---

[۱]. Ryan,Robin.D; **The criminalization of trade secret theft under the Economic Espionage Act OF ۱۹۹۶: An evaluation of United States v Hsu**, ۴۰ F. SUPP. ۲D ۶۲۳; University of Dayton law review, volume ۲۵, ۱۹۹۹-۲۰۰۰, p. ۲۴۴

نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهندشد.

بررسی مقوله جاسوسی سایبری به عنوان شکل نوین از جاسوسی ،نیازجامعه دانشگاهی و نهادهای تصمیم‌گیر است تا از طریق آن با پدیده‌های جدید روز که در دیگر نقاط جهان طرح گردیده آشنا گردند. همین آشنایی نه تنها محققان و دست اندرکاران قانونی، قضایی و اجرایی ما را به قافله تحقیقات جدید، نزدیک می کند؛ بلکه راهی است برای درک میزان خطری که می تواند جاسوسی سایبری برای جامعه اطلاعاتی ایجاد کند و درک راه هایی که از همین الان باید به فکر پیمودن آنها بود.

۲. سؤالات و فرضیات

پیرامون جرم جاسوسی اینترنتی ومقایسه آن با جرم جاسوسی سنتی سؤالات بسیاری مطرح است و اگر این دسته از جرایم از نگاه‌های متفاوت مانند جنبه‌های حقوقی، جرم‌شناسی و سیاسی بررسی گردند، تعداد سؤالات عدیده و متنوع خواهند بود. اما سؤالاتی که در این تحقیق در پی پاسخ به آنها هستیم در رده سؤالات فرضیه بردار هستند تا بتوان در پرتو آنها سخن ازپایان نامه گفت و درنهایت از آنها دفاع کرد یا بر پایه دلایل قانع کننده ای آنها را رد نمود. سؤالات اصلی تحقیق حاضر عبارتند از:

۱-آیا باتوجه به ویژگی‌های فضای سایبر پدیده ای به نام جاسوسی سایبری وجوددارد؟

۲- درحقوق کیفری، جاسوسی سایبری چه ماهیتی دارد؟

۳- در سیاست تقنینی ایران جاسوسی سایبری وسنتی چه جایگاهی دارند؟

۴- آیاسیاست جنایی درررویارویی با جرم جاسوسی نیازمند اتخاذتدابیر کیفری پیشگیرانه خاصی است؟

فرضیه‌های تحقیق به شکل خبری و در قالب پاسخ به سؤالات فوق به شرح زیر است:

۱- هم ازجهت رخ داده‌های عینی وهم ازحیث ضوابط هنجاری و مقرره های پیش بینی شده، جاسوسی سایبری واقعیت وجودی دارد.

۲- جاسوسی سایبری ماهیتاً گونه ای جدا از مصادیق سنتی جاسوسی است.

۳- سیاست تقنینی ایران، از جهت محتوا و ویژگی های انطباقی، جرم جاسوسی سایبری وسنتی را پذیرفته و پیش بینی کرده است.

۴- رویارویی با جاسوسی سایبری نیازمند اتخاذ تدابیری افتراقی است.

۳.روش تحقیق

با توجه به ماهیت و گستره ی موضوعی طرح بحث روش تحقیق تحلیلی توصیفی و در مواردی تطبیقی است.

۴. ضرورت تحقیق

ضرورت تحقیق امری است مرتبط با مقتضیات زمانی و مکانی. از حیث مقتضیات زمانی باید گفت ضرورت تحقیق برپایه یکی ازسه زمان گذشته، حال وآینده متجلی می‌شود. از حیث گذشته، ضرورت تحقیق ازنقطه نظرتاریخی دیده می شود تاتجربه والگویی برای آینده باشد؛بررسی تاریخی موضوعات حقوقی معمولاً به صورت تبعی است و در کنار بررسی حال این موضوعات صورت می گیرد مگر اینکه کلاً چهره ی تاریخی به خود بگیرد مانند بررسی محاکم کیفری پیش از دوره مشروطه یا تفحص درباره قوانین کیفری دوره هخامنشیان.

از جهت حال، ضرورت تحقیق به جهت مشکلات، چالش‌ها، نیازها و ابعاد موضوعی است که در جامعه حضور دارد. نسبت به یک موضوع حقوقی عموماً، تحقیق و پژوهش ازنگاه زمان حاضر بررسی می‌شود؛ برای نمونه، تحقیق پیرامون یک جرم یا یک نهاد کیفری یا یک مقوله جرم شناختی از آن جهت ضرورت دارد که مقتضیات کنونی جامعه آن را ایجاب کرده است.

از جهت آینده، ضرورت تحقیق از آن رو به چشم می‌آید که پدیده‌ای نوظهور دغدغه آینده ما شود. این قبیل موضوعات در دنیایی که سراسر بر فناوری و صنعت مبتنی است کاملاً بدیهی می باشد. در واقع حقوق کیفری امروزه نه تنها باید نگران گذشته و حالش باشد، بلکه باید به آینده نیز نگاهی عمیق داشته باشد. ضرورت انجام تحقیق در رابطه با جاسوسی سایبری دست کم در ایران از منظر آینده نگری توجیه می‌شود.

۵. اهداف تحقیق

مهمترین هدف در نگارش این پایان نامه، هشدار درباره شکل گیری و رسوخِ خیره کننده یک پدیده ویرانگر سایبری است. مقابله در برابر تهدید سهمگین جاسوسی در فضای سایبر در جامعه ای که روز به روز رایانه ای و اطلاعاتی می شود، جز با شناسایی درست و کامل آن امکانپذیر نیست. پس

هدف هشدار دادن برای پیشگیری از جاسوسی سایبری سبب می‌گردد تا از همین الان دست به تحقیقاتی گسترده در این زمینه زد.

هدف هشداردهی متوجه قانونگذارونهادهای مربوطه است تابابهره‌گیری ازتحقیقات دانشگاهی، مقررات وتدابیر شایسته اتخاذ کند. درکنار این هدف عمده اهداف دیگری نیز انگیزه نگارش این پایان نامه بوده اندکه عبارتنداز: تهیه یک مجموعه تحقیقی جامع و درخورتوجه جهت استفاده پژوهشگران و دانشگاهیان، فراهم کردن زمینه بررسی موضوعات بسیار جدید در حقوق کیفری ایران، بیان نواقص حقوق کیفری در مبارزه با این پدیده.

۶. سابقه تحقیق

تحقیق ونگارش پایان نامه پیرامون جرایم رایانه ای دارای سابقه‌ای بیشتر ازیک دهه است.اگرچه درخصوص جاسوسی سنتی مقالاتی نوشته شده همچنین پایان نامه هایی درخصوص جرایم سایبری به رشته تحریردرآمده است لیکن ازآنجا که درحوزه جرایم سایبردربستردانشگاهی امروزی یکی از موضوعاتی که همواره ناب و بی‌سابقه است موضوعاتی است که در حوزه فناوری اطلاعات و فناوری‌های نوین قرار دارد. در مجموع جاسوسی سایبر به جهت به روزبودن حوزه فناوری جدید و بکر می نماید.

۷. ساختار تحقیق

این تحقیق شامل کلیات ،۳ فصل وهر فصل شامل چندین بخش ودرصورت نیاز بندهای متعدد وقسمت نتیجه گیری می باشد .

درقسمت کلیات به بیان مسأله ، سؤالات وفرضیات ، روش تحقیق ، ضرورت تحقیق ، اهداف تحقیق و سابقه تحقیق پرداخته شده است . فصل اول که شامل ۴ بخش می باشد به تعریف جاسوسی وجرایم سایبری وویژگیها وسابقه تاریخی جرایم سایبری ازجمله جرم جاسوسی پرداخته شده است . درفصل دوم که شامل ۷ بخش می باشد به شناخت جرم جاسوسی سایبری وسنتی ،شیوه جاسوسی ،مراحل جاسوسی ،مصادیق جرم جاسوسی ،ارکان مرتبط به جاسوسی رایانه ای وتطبیق جرم جاسوسی کلاسیک وسایبری پرداخته شده ودرفصل سوم که شامل ۶ بخش می باشد به راه های

پیشگیری از جرایم سایبری،مشکلات تعقیب ورسیدگی جرایم رایانه ای ،ادله اثبات دعاوی رایانه ای، صلاحیت قضایی درمحیط مجازی ودرآخر به بررسی سیاست جنایی درایران پرداخته شده است .

فصل اول

ویژگیها و تحولات جرایم سایبری و جاسوسی

بخش اول : جاسوسی

۱-۱-۱ تعریف لغوی جاسوسی

ممکن است تصورشود که معناومفهوم جاسوسی به سبب روشن بودن آن، نیازی به بررسی وبیان نداشته باشد لکن باتوجه به معانی مختلفی که این واژه داردبهترین معناعبارت است از: کنجکاوی کردن، بررسی کردن،خبرجستن ازامورمردم، اموری که مردم می خواهند پنهان بماند.[۱]

در مورد لغت جاسوسی در فرهنگ معین اینگونه بیان شده «جاسوس آن که اخبار و اطلاعات کسی یا مؤسسه‌ای و یا کشوری را مخفیانه گردآورد و به شخص یا مؤسسه و یا کشوری دهد.»[۲]

۱-۱-۲تعریف فقهی جاسوسی

اکثرفقهای عظام جاسوسی راتعریف نکرده اندوممکن است این امربه سبب روشن بودن معنای جاسوسی از دیدگاه آنان بوده باشد ، درابواب فقهی نیز بابی رابه این بحث اختصاص نداده اند، بلکه درجاهای مختلف به طورپراکنده وگذرا از جاسوسی سخن به میان آمده است . درکتب فقه برای این منظور غالباً ازتعبیر عین وعیون استفاده شده است .[۳]

۱-۱-۳ تعریف جاسوسی ازنظرحقوق بین الملل

به طورکلی درحقوق بین الملل سعی شده قوانینی که وضع می گردد باعث ایجاد وحدت گردد . مثلاً درموردجاسوسی تعریفی ارائه شود که به لحاظ رعایت حقوق افراد جامعه وضمانت آزادی های فردی ، دولت ها مجازنباشندکه عملی راجاسوسی تلقی نموده ومرتکب راتعقیب نمایند.ماده ۱۲ قطعنامه بروکسل ۱۸۷۴ می گوید :«جاسوس کسی است که به طور مخفیانه وبا وسایل وبهانه های مجهول اطلاعات راجمع آوری یابرای تحصیل اطلاعات درنقاط اشغال شده بوسیله نیروی دشمن باقصداین که آن هارابه طرف مقابل تسلیم نماید ، تجسس می کند.»

---

[۱] .محمدقریب، تبیین الغات لتبیان الآیات **یا فرهنگ لغات قرآن** ، ج۱، ص۲۷۴و۲۷۵

[۲] .معین، محمد، ۱۳۸۶ ،**فرهنگ معین**،یک جلدی فارسی، انتشارات زرین، ص۴۹۹

[۳] .ساریخانی، عادل، ۱۳۷۸، **جاسوسی وخیانت به کشور**،مرکز انتشارات دفتر تبلیغات اسلامی، ص۳۰ ص۳۱

ماده ۲۹ آیین نامه ضمیمه قرارداد لاهه مورخه ۱۸ اکتبر۱۹۰۷ مقرر می کند : « کسی رانمی توان جاسوس دانست مگر اینکه به طورمخفیانه یابه بهانه های مجهول به نفع یکی ازمتخاصمین درصدد تحصیل اطلاعات یاجمع آوری اشیائی برآید.»[۱]

۱-۱-۴تعریف قانونی جاسوسی

قانون گذارنیز درهیچ یک از نصوص قانونی ، جرم جاسوسی راتعریف نکرده وتنها دربرخی ازمواد قانونی به کلمه جاسوسی وجرایم مرتبط باآن اشاره نموده است .

اینک باتوجه به معنا ومفهوم لغوی جاسوسی وباتوجه به طبع وماهیت عمل مذکور وبا استناد به مواد قانونی درتعریف جاسوسی می توان گفت : « جاسوسی به عمل شخصی گفته می شود که با عناوین غیرواقعی ومتقلبانه ، اقدام به کسب اطلاعات یا نقشه ها یا مدارک واسناد مخفی ومحرمانه مربوط به اسرارنظامی ، اقتصادی ، سیاسی و تسلیم آنها به کشور بیگانه نماید.»[۲]

بخش دوم : فضای سایبر

خلاقیت انسان ، فضای سایبر رابه ما هدیه کرده است ، فضایی که منافع وقابلیت های بسیاری دارد.اما هدایای بزرگ بهای گزافی نیز دارند . پیش از اینکه فضای سایبر به عنوان یک فناوری ظاهر شود، تعدادی ازفلاسفه درارتباط با امکان وجود «حقیقت مجازی»[۳] اظهارنظرکرده بودند.برای نمونه، افلاطون درکتاب جمهوریت خود به تمثیل غار می پردازد ومی گوید « آنچه حقیقت واقعی است دربیرون غار است وماسایه های آن بردیوار غار هستیم . او می گوید ، ما حقیقت مجازی هستیم واین یک فریب است که فکر می کنیم حقیقت واقعی هستیم.» درهرحال فضای سایبرعبارتی است که دردنیای اینترنتی ، رسانه وارتباطات بسیارشنیده می شود به نظر می رسد به کارگیری این اصطلاح دراین زمینه وبرای ارجاع به آن رنگ وبویی صرفاً فنی ومکانیکی داده باشد.ملاحظه دقیق تراین اصطلاح نشان می دهد که این واقعیت وجوه وجنبه های متنوعی از جمله خصلت های روان شناختی

---

[۱] .شامبیاتی، هوشنگ،۱۳۷۷،حقوق کیفری اقتصادی ،جلدسوم،چاپ آینده،ص ۱۰۱

[۲] .ساریخانی، عادل، پیشین ،ص۳۱

[۳].Virtual Reality