دانشگاه آزاد اسلامی

واحد شهرقدس

دانشکده علوم انسانی – گروه حقوق

پایان نامه برای دریافت درجه‌ی کارشناسی ارشد «M.A.»

گرایش جزا و جرم شناسی

عنوان:

بررسی جرم جاسوسی و خرابکاری در قوانین جزایی ایران با نگاهی به قانون جرایم رایانه ای

استاد راهنما:

آقای دکتر داود کرمی

نگارنده:

مصطفی کامرانی

خرداد ۱۳۹۷

صفحه تاییدیه هیئت داوران

سپاسگزاری

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمتهای او ندانند و کوشندگان، حق او را گزاردن نتوانند.سلام و دورد بر محمّد و خاندان پاک او، طاهران معصوم، هم آنآن‌که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

بدون شک جایگاه و منزلت معلم، اجّل از آن است که در مقام قدردانی از زحمات بی شائبه‌ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم.امّا ازآنجایی‌که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تأمین، و سلامت امانت‌هایی را که به دستش سپرده‌اند تضمین می‌کند، برحسب وظیفه و از باب «**من لم یشکر المنعم من المخلوقین لم یشکر اللّه عزّ و جلّ**» این دو معلم بزرگوارم که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از کنار غفلت‌هایم گذشته‌اند و در تمام عرصه‌های زندگی یار و یاوری بی‌چشم داشت برای من بوده‌اند؛ از اساتید با کمالات و شایسته، که در کمال سعه صدر، با حسن خلق و دقّت، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این رساله را بر عهده گرفتند، کمال تشکر و قدردانی را دارم.

تقدیم به

پدر و مادر عزیزم و همه ی کسانی که در راه تحصیل علم و دانش مرا یاری نموده اند.

فهرست مطالب

عنوان **صفحه**

فصل سوم : رکن شناسی جاسوسی رایانه ای

فصل چهارم: رکن شناسی خرابکاری های رایانه ای

چکیده

از گذشته تا به امروز یکی از دغدغه های اصلی حفظ امنیت و بقای دولت ها و ملت ها، سعی در ارتقای سطح توانایی برای کنترل، پیشگیری و مبارزه با پدیده های ضد امنیتی خصوصاً جاسوسی بوده است .
جاسوسی رایانه ای که خود چهره جدید و وسیعی از جاسوسی بشمار می رود- با توجه به وضعیت رایانه ای بودن اکثریت منابع اصلی اطلاعات و زیرساخت های حیاتی کشورها- یکی از مهمترین دغدغه های کشورها در این برهه از زمان می باشد که باید هر روز بیش از دیروز مدنظر و مورد توجه قرار گیرد .
پژوهش حاضر با روش توصیفی – تحلیلی به بررسی جرم جاسوسی و خرابکاری رایانه ای در قانون جرایم رایانه ای ایران پرداخته است. در این راستا به دنبال پاسخ به این سوالات است که جرم جاسوسی و خرابکاری در حقوق ایران چه جایگاهی دارند؟قانون جرایم رایانه ای برای جرم جاسوسی و خرابکاری چه مسئولیت کیفری و مجازاتی در نظر گرفته است؟میان جرم جاسوسی سنتی و رایانه ای چه تفاوت هایی وجود دارد؟آیا جرایم رایانه ای ایران جنبه ی بازدارندگی برای جرم جاسوسی و خرابکاری دارد؟ همچنین با توجه به اینکه قانون گذار جمهوری اسلامی ایران نیز در سال ۱۳۷۵ تحت عنوان تعزیرات و مجازات های بازدارنده مواد قانونی مختلفی را در مورد افشای اطلاعات ، در اختیار دیگران قرار دادن آنها ، انتقال آنها در شرایط جنگی و موارد دیگر مقرر داشته است که در این بین ماده ۵۰۵ قانون مجازات اسلامی(جاسوسی سنتی) را مورد بررسی قرار خواهیم داد و آن را با ماده ۳ جرایم رایانه ای (جاسوسی رایانه ای) مقایسه خواهیم نمود.
در خصوص جاسوسی رایانه ای در قوانین ایران باید گفت، در قوانین کیفری ایران تعریفی از جرم جاسوسی به عمل نیامده است. این رویکرد در قانون جرایم رایانه‌ای نیز مشاهده می‌شود. زیرا صرفاً مصادیق حصری واحکام آن طی سه ماده (۳، ۴ و ۵) در مبحث سوم فصل اول قانون مزبور، بیان شده است. با این وجود حقوقدانان تعاریف متعددی برای جاسوسی و جاسوس عرضه کرده اند از جمله: « جاسوس به شخصی اطلاق می‌شود که در پوشش متقلبانه یا مخفیانه وبه نفع دشمن در صدد تفحص پیرامون اسرار یا تحصیل اطلاعات یا اشیاء یا سایر مدارک و اسناد مربوط به استعداد و توانایی‌های نظامی، اقتصادی و فرهنگی مربوط به یک کشور دشمن باشد».

واژه های کلیدی: جاسوسی رایانه ای، خرابکاری رایانه ای، جرایم رایانه ای، دسترسی غیر مجاز

فصل اول

کلیات تحقیق

۱-۱-مقدمه

جرایم رایانه ای جاسوسی و خیانت به کشور از دیرباز موجب نکوهش و سرافکندگی بوده است و قوانین کشورهای مختلف هم به جرم انگاری این عمل خیانتکارانه و مذموم پرداخته اند ، قانون گذار جمهوری اسلامی ایران نیز در سال ۱۳۷۵ تحت عنوان تعزیرات و مجازات های بازدارنده مواد قانونی مختلفی را در مورد افشای اطلاعات ، در اختیار دیگران قرار دادن آنها ، انتقال آنها در شرایط جنگی و موارد دیگر مقرر داشته است.

که در این بین ماده ۵۰۵ قانون مجازات اسلامی(جاسوسی سنتی) را مورد بررسی قرار خواهیم داد و آن را با ماده ۳ جرایم رایانه ای (جاسوسی رایانه ای) مقایسه خواهیم نمود . برای تعریف جاسوسی سنتی میتوان به همان ماده ۵۰۵ قانون مجازات اسلامی اشاره داشت که چنین مقرر میدارد «هرکس با هدف برهم زدن امنیت کشور به هر وسیله اطلاعات طبقه بندی شده را با پوشش مسئولین نظام یا مامورین دولت یا به نحو دیگر جمع آوری کند چنانچه بخواهد آن را در اختیار دیگران قرار دهد و موفق به انجام آن شود به حبس از دو تا ده سال و در غیر این صورت به حبس از یک تا پنج سال محکوم میشود» . بدین ترتیب جمع آوری اطلاعات طبقه بندی شده (سری ، به کلی سری ، محرمانه ، خیلی محرمانه) و در اختیار دیگران قرار دادن این اطلاعات تحت عنوان جاسوسی در قوانین ما پیش بینی شده است و تاکنون پاسخگوی جرائم احتمالی در این حوزه بوده است اما با رشد روز افزون کاربران رایانه و رشد شبکه های اجتماعی مجازی ، افزایش وبلاگ ها و سایت ها با موضوعات متنوع و هم چنین امکان انتقال داده ها توسط ایمیل یا چت و ... سبب شد تا این مجموعه عظیم نوین مجازی مورد توجه بیگانگان و طمع اطلاعاتی آنان قرار بگیرد و سرویس های اطلاعاتی بیگانه نیز در همین راستا سعی در فعالیت های جاسوسی در این فضای مجازی نمودند. قانون گذار جمهوری اسلامی در ماده ۷۳۲ قانون

مجازات اسلامی یا همان ماده ۳ جرایم رایانه ای توانست با تدبیری موفق ، این نوع جدید از جاسوسی را که تحت عنوان جاسوسی رایانه ای شناخته میشود پوشش دهد ، طبق این ماده «هر کس به طور غیر مجاز نسبت به داده های سری در حال انتقال یا ذخیره شده در سامانه های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود به مجازات های مقرر محکوم خواهد شد : الف) دسترسی به داده های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات ب) در دسترس قرار دادن داده های 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 .«بدین ترتیب جاسوسی رایانه ای در سه مرحله به صورت کامل جرم انگاری شده و مجازات آن مقرر شده است ، اما سوال اساسی این است که چرا با وجود اینکه قانون مجازات اسلامی پیش از این و در ماده ۵۰۵ فوق الذکر در مورد جرم جاسوسی ، جرم انگاری نموده بود یک بار دیگر و در یک ماده قانونی جدید باز هم به جرم انگاری جاسوسی پرداخته است ؟ به عبارت دیگر مگر این جرایم چه تفاوت هایی با یکدیگر دارند که مقنن تحت عنوان دو ماده قانونی به شرح آن پرداخته است ؟ آیا ماده ۳ جرایم رایانه ای ماده ۵۰۵ را نسخ کرده است ؟ آیا رایانه به عنوان ابزار جرم سبب این تفاوت بین دو ماده شده است یا موارد دیگری نیز وجود دارد؟در پاسخ به این سوالات باید گفت اولاً ماده ۳ جرایم رایانه ای ماده ۵۰۵ را نسخ صریح یا ضمنی نکرده است و هر دو ماده قانونی در دادگاه ها قابل اعمال است و ثانیاً طبیعتاً صرف ارتکاب جرم توسط رایانه نمیتواند موجب تصویب قانون جدیدی باشد زیرا در همان ماده ۵۰۵ قانون مجازات اسلامی نیز عنوان «به هر نحو دیگر» یا «به هر وسیله» وجود دارد که شامل رایانه هم میشود ، پس تفاوتهای دیگری وجود دارد که اینک به بیان آن خواهیم پرداخت .

۱)در ماده ۵۰۵ قانون مجازات اسلامی بحث از اطلاعات طبقه بندی شده به طور عام است و شامل هر چهار طبقه اطلاعات میشود اما در ماده ۳ جرایم رایانه ای صرفاً از اطلاعات سری و به کلی سری نام برده شده و اطلاعات محرمانه و خیلی محرمانه را از تعریف خود خارج نموده است . همان طور که میدانیم اطلاعات سری

اطلاعاتی است که افشای آن به منافع ملی و امنیت کشور لطمه وارد میکند و اطلاعات به کلی سری اطلاعاتی است که افشای آنها به امنیت کشور و منافع ملی صدمات جبران ناپذیر وارد میکند . بدین ترتیب چون ماده ۳ جرایم رایانه ای اختصاصاً به اطلاعات سری و به کلی سری اختصاص دارد در موارد جرایم احتمالی در حال حاضر قاضی به این ماده استناد مینماید نه ماده ۵۰۵ قانون مجازات اسلامی .

۲)در ماده ۵۰۵ آمده است که «اطلاعات را جمع آوری کند» اما در ماده ۳ جرایم رایانه ای مقرر شده است که «دسترسی به داده ها» . بدین ترتیب متوجه خواهیم شد که محدوده ماده ۳ جرایم رایانه ای بیشتر است و صرف دسترسی به این اطلاعات را جرم انگاری کرده است اما از طرفی هم این ماده ضعف دارد زیرا جمع آوری اطلاعات را مورد اشاره قرار نداده است . حال در فرضی که فردی به اطلاعات طبقه بندی شده دسترسی پیدا کرده و این اطلاعات را جمع آوری نموده باشد قبل از در اختیار قرار دادن ، جرم متعدد انجام داده است اما قاضی ماده ۵۰۵ قانون مجازات اسلامی را اعمال خواهد نمود زیرا جمع آوری اطلاعات مستلزم دسترسی به آن اطلاعات بوده است و مجازاتش هم اشد است .

۳)در ماده ۵۰۵ بیان شده است که اطلاعات طبقه بندی شده را «در اختیار دیگران قرار دهد» . مفهوم دیگران کلی و مبهم است و ممکن است منظور مقنن کشور بیگانه یا فرد بیگانه یا فرد غیر صالح و ... باشد ولی ماده ۳ جرایم رایانه ای این نقص را جبران نموده و باز هم با تعریفی بازتر نسبت به ماده قبلی بیان داشته است برای افراد فاقد صلاحیت یا دولت ، سازمان ، شرکت یا گروه بیگانه یا عاملان آنها .

۴)یکی از دلایلی که با وجود یک ماده قانونی ، ماده دیگری تصویب میگردد افزایش مقدار مجازات مقرر در ماده پیشین است ، در اینجا هم همان طور که در متن مواد فوق الذکر مشخص است در ماده ۵۰۵ ، مجازات فرد در صورتی که موفق به انتقال اطلاعات گردد ۲ الی ۱۰سال حبس مقرر شده است و در صورت عدم موفقیت ۱ الی ۵ سال حبس اما در ماده ۳ جرایم رایانه ای برای انتقال اطلاعات به افراد فاقد صلاحیت ۲ الی ۱۰ سال حبس مقرر شده است و برای انتقال اطلاعات به گروه ، دولت و سازمان بیگانه بین ۵ الی ۱۵ سال حبس تعزیری مقرر شده است که شدید تر محسوب میشود.

۱-۲-بیان مسئله

جرم جاسوسی از جمله جرایمی است که در طبقه اول جرایم علیه امنیت و آسایش عمومی قرار دارد، چرا که استقلال و امنیت و تمامیت ارضی کشور و اساس حکومت را به خطر می‌اندازد و موجب فاش شدن اسرار و اطلاعات میشود.[۱] گرچه برخی معتقدند (سان تزو) جاسوسی خوب مقدمه پیروزی است. هیچ زمانی در طول تاریخ نام کشوری به افتخار برده نشده است که بدون سرویسهای جاسوسی و اطلاعاتی قوی.) توانسته باشد کاری انجام دهد .[۲]

برخی از علمای علم حقوق در تفکیک جرم جاسوسی و خیانت به کشور دچار اشکال شده اند و اظهار میدارند که در حال حاضر تفکیک جرایم فوق عملی نیست و عده ای نیز، ممیز اساسی این دو جرم را تابعیت و ملیت مرتکب قرار داده اند.[۳]

برخی از متون قانونی کشورهای اروپایی فرق اصلی جرم جاسوسی و خیانت به کشور را عنصر تابعیت مرتکب می‌دانند. یعنی اگر مرتکب جرم از اتباع کشوری باشد و جرم بر ضد آن کشور وقوع یافته باشد، عمل ارتکابی خیانت به کشور محسوب میشود و در صورتیکه مرتکب خارجی باشد، عمل او جاسوسی خواهد بود. از طرف دیگر قانونگذاران و محاکم نیز معیار مناسبی برای تمایز جرایم جاسوسی و خیانت به کشور مشخص نکرده اند به طوری که گاهی عمل واحد، هم جاسوسی و هم خیانت محسوب میشود. به هر حال بنابر اصل تفکیک بین معنا و مفهوم خیانت و جاسوسی در فقه، بدون ملاحظه جنبه های کاربردی آن در صحنه سیاست و حکومت ،جاسوس لزوما باید کافر حربی باشد و الا مسلمانان و کافر ذمی اگر مرتکب عمل مشابهی شوند ، خائن محسوب میشوند. در نظام اسلامی در شرایط کنونی، کافر یا مسلمان بودن چندان دخالتی در این موضوع ندارد و عملا تابعیت سیاسی است که تعیین کننده است .[۴]

---

[۱] شجوده، ۱۳۸۸ ش، ص . ۱۲

[۲] اندلمن، دمارانش، ۱۳۸۰ ش، ص ۱۶۲ و. ۱۶۳

[۳] شامبیاتی، ۱۳۷۶ ش، ج ۳ ص ۱۰۲

[۴] زینلی، ۱۳۷۸ ش، ص ۲۴۴

۱-۳- سوالات تحقیق

۱-۳-۱-سوال اصلی

۱-جرم جاسوسی و خرابکاری در حقوق ایران چه جایگاهی دارند؟

۱-۳-۲- سوال فرعی

۱-قانون جرایم رایانه ای برای جرم جاسوسی و خرابکاری چه مسئولیت کیفری و مجازاتی در نظر گرفته است؟

۲-میان جرم جاسوسی سنتی و رایانه ای چه تفاوت هایی وجود دارد؟

۱-۴-فرضیه‌ها

قوانین موضوعه کشور در خصوص برخورد با جرایم رایانه‌ای دارای نواقصی است.

جاسوسی رایانه‌ای ماهیتاً جدا از جاسوسی سنتی است.

قوانین جزایی ایران، جرم جاسوسی رایانه‌ای را پذیرفته و پیش بینی کرده است.

۱-۵-اهداف تحقیق

جرم جاسوسی رایانه‌ای در قوانین جزایی ایران با توجه به قوانین جرائم رایانه‌ای.

شیوه‌های تحقق جرم رایانه‌ای در قوانین ایران.

مقایسه جرم جاسوسی رایانه‌ای با جاسوسی سنتی در قوانین جزایی ایران.

۱-۶-ضرورت‌های تحقیق

با تصویب قانون جرایم رایانه‌ای (۱۳۸۸)، مفاهیم وجرایم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشد. در این میان، جرم جاسوسی اگرچه یکی از جرایم قدیمی و کلاسیک حقوق جزابه شمار می‌رود، ولی در پرتو پیشرفت‌های فناوری، نحوه ارتکاب آن دستخوش تغییراتی

می‌شود که در قانون جرایم رایانه‌ای تحت عنوان جاسوسی رایانه‌ای، جرم انگاری شده است.[1] 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

۱-۷- ساماندهی تحقیق

پایان نامه دارای ۵ فصل ، فصل اول کلیات تحقیق ، فصل دوم ماهیت و تعاریف و مبانی نظری ، فصل سوم رکن شناسی جاسوسی رایانه ای ، فصل چهارم رکن شناسی خرابکاری های رایانه ای و فصل پنجم نتیجه گیری و پیشنهادات می باشد .

۱-۸- نو آوری

تا کنون پژوهشی در قالب یک پایان نامه کارشناسی ارشد در خصوص جرم جاسوسی و خرابکاری در قوانین رایانه ای ایران صورت نگرفته است و پژوهش از نظر موضوع دارای نوآوری می باشد.

۱-۹-پیشینه تحقیق

کامرانلو (۱۳۹۴) در پژوهشی با عنوان جاسوسی رایانه‌ای و تفاوت آن با جاسوسی‌های سنتی به بررسی جاسوسی رایانه‌ای و ابعاد آن پرداخته و سوالاتی مطرح نموده است که چرا با وجود اینکه قانون مجازات اسلامی پیش از این و در ماده ۵۰۵ فوق الذکر در مورد جرم جاسوسی، جرم انگاری نموده بود یک بار دیگر و در یک ماده قانونی جدید باز هم به جرم انگاری جاسوسی پرداخته است؟ به عبارت دیگر مگر این جرایم چه تقاوت هایی با یکدیگر دارند که مقنن تحت عنوان دو ماده قانونی به شرح آن پرداخته است؟ آیا ماده ۳ جرایم رایانه‌ای ماده ۵۰۵ را نسخ کرده است ؟ آیا رایانه به عنوان ابزار جرم سبب این تفاوت بین دو ماده شده است یا موارد دیگری نیز وجود دارد؟ در پاسخ به این سوالات باید گفت اولاً ماده ۳ جرایم رایانه‌ای ماده ۵۰۵ را نسخ صریح یا

[1] گارو: استاد مطالعات نظری و عملی در حقوق جزا ترجمه دکتر ضیاء الدین نقابت ۱۳۸۹، ص ۸۲

ضمنی نکرده است و هر دو ماده قانونی در دادگاه‌ها قابل اعمال است و ثانیاً طبیعتاً صرف ارتکاب جرم توسط رایانه نمیتواند موجب تصویب قانون جدیدی باشد زیرا در همان ماده ۵۰۵ قانون مجازات اسلامی نیز عنوان «به هر نحو دیگر» یا «به هر وسیله» وجود دارد که شامل رایانه هم می‌شود[۱].

بشیری(۱۳۹۲) پژوهشی با عنوان بررسی حقوقی جرایم رایانه ای در حقوق جزای عمومی انجام داد. در حال حاضر جرایم اینترنتی با اشکال مختلفی صورت می پذیرد که عبارتند از : کلاهبرداری اینترنتی، جاسوسی اینترنتی، سوء استفاده از شبکه های تلفنی، سوءاستفاده از کارتهای اعتباری، وارد کردن ویروس به کامپیوترهای دیگر، پولشویی و ... در این تحقیق، پس از مقدمه به بررسی تاریخچه جرایم کامپیوتری، تبیین مفهوم و ماهیت جرایم اینترنتی، بررسی انواع مختلف جرایم اینترنتی، بررسی نقاط قوت و ضعف قوانین و ارائه راهکارهای مناسب برای پیشگیری از وقوع جرایم کامپیوتری پرداخته است

سلیمی(۱۳۹۲) در پایان نامه کارشناسی ارشد خود به تجزیه و تحلیل حقوقی جرم جاسوسی در فضای مجازی پرداخته است.

در پژوهش فوق 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 درخطرافتادن دادوستد افراد با یکدیگر و یا ازبین رفتن اموال و خدمات آنها می‌شود، که درصورت برهم‌زدن امنیت کشور، خود نوعی جاسوسی امنیتی تلقی می‌شود. 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 رایانه‌ای و قانون تجارت الکترونیک مورد بررسی قرار گرفته است. آنگاه به تفاوت انواع جاسوسی در فضای مجازی و سنتی از جنبه‌های مختلف پرداخته شده است. بدین ترتیب با توجه به تاکید قانون‌گذار بر حفظ حاکمیت ملی،

[۱] کامرانلو؛ ۱۳۹۴، جرایم رایانه ای ، ص ۳۳

جاسوسی در فضای مجازی نه تنها از بعد امنیتی بلکه از بعد صنعتی نیز، در زمره جرایم علیه امنیت کشور قلمداد می‌شود .

رهامی و پرویزی(۱۳۹۱) در پژوهشی به بررسی جاسوسی رایانه‌ای در حقوق ایران ووضعیت بین المللی آن پرداخته است. در این پژوهش آمده است که این جرم از جرایمی است که ارتکاب آن قبل از پیدایش رایانه امکان پذیر نبوده است؛ به همین خاطر اکثر کشورها اخیرا اقدام به تصویب مقرراتی در این باره کرده اند. در حقوق داخلی ایران نیز اقداماتی نظیر دسترسی غیرمجاز به داده‌های محرمانه که افشای آنها باعث لطمه به امنیت کشور و منافع ملی شود؛ با عنوان جاسوسی رایانه‌ای جرم انگاری شده است. مقاله حاضر حول این موضوع بحث و بررسی کرده است که منظور از جاسوسی رایانه‌ای چیست و نیز نقش و اهمیت رایانه در وقوع جاسوسی رایانه‌ای و اعمالی که مشمول جرم جاسوسی رایانه‌ای می‌شود .

محمدباقرگرایلی (۱۳۹۰) پژوهشی با عنوان بررسی جعل و تخریب و اخلال رایانه‌ای انجام داد. ایشان در این پژوهش بیان کردند که در کنار فواید بسیار رایانه که در عصر ارتباطات به وجود آمد، این پدیده همچون هر پدیده دیگر موجبات سوء استفاده برخی را نیز فراهم نموده است. در چنین شرایطی عده‌ای سودجود درصدد سوء استفاده از این فناوری در راستای اهداف پلید خویش برآمدند که باتوجه به مزایا و امتیازات رایانه جلوه‌های نوینی از بزهکاری پا به عرصه وجود گذاشت. باتوجه به قانون جرایم رایانه‌ای[1] این مقاله پس از بررسی کلی جرایم رایانه‌ای، جرم جعل رایانه‌ای و تخریب و اختلال در داده‌ها را از منظر فقه و حقوق بررسی می‌کند.

عرب پور(۱۳۹۰) در پایان نامه کارشناسی ارشد خود با به بررسی جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای در نظام حقوقی ایران و اسناد بین المللی پرداخته است. جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای به عنوان جرایمی که حریم خصوصی اشخاص را مورد تعرض قرار داده و سبب از بین رفتن محرمانگی داده‌ها و سامانه‌های رایانه‌ای می‌گردند، به موازات طرح در حقوق داخلی در قلمرو اسناد بین‌المللی نیز قابل بررسی می‌باشند. این دسته از جرایم تهدیدی جدی برای اشخاص حقیقی و حقوقی همه کشورها،

[1] مصوب ۱۳۸۸/۳/۵