
بسم الله الرحمن الرحيم

دانشگاه اصفهان

دانشکده علوم اداری و اقتصاد

گروه حقوق

پایان نامه ی کارشناسی ارشد رشته ی حقوق

گرایش جزا و جرم شناسی

تحلیل خرابکاری رایانه ای در قانون جرایم رایانه ای ایران

استاد راهنما:

دکتر قدرت اله خسروشاهی

استاد مشاور:

دکتر حسن عالی پور

پژوهشگر:

مریم عطوان

اردیبهشت۱۳۹۱

دانشگاه اصفهان

دانشکده علوم اداری و اقتصاد

گروه حقوق

پایان نامه ی کارشناسی ارشد رشته ی حقوق گرایش جزا و جرم شناسی خانم مریم عطوان

تحت عنوان

تحلیل خرابکاری رایانه ای در قانون جرایم رایانه ای ایران

در تاریخ ۱۳۹۱/۲/۱۹ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد راهنمای پایان نامه دکتر قدرت اله خسرو شاهی با مرتبه ی علمی استادیار امضا

۲- استاد مشاور پایان نامه دکتر حسن عالی پور با مرتبه ی علمی استادیار امضا

۳- استاد داور داخل گروه دکتر حسن عالی پور با مرتبه ی علمی استادیار امضا

۴- استاد داور خارج از گروه دکتر بهروز ترک لادانی با مرتبه ی علمی دانشیار امضا

امضای مدیر گروه

تقدیم به:

لطف بی انتهای پروردگارم

قلب مهربان مادرم

دستان گرم پدرم

و عشق بیکران همسرم

باقدردانی و تشکر فراوان از استاد گرامی

جناب آقای دکتر خسروشاهی

و استاد عزیز

جناب آقای دکتر حسن عالی پور

چکیده

خرابکاری سایبری عنوان مجموعه ای از جرایم رایانه ای است که علیه تمامیت داده و سامانه های رایانه ای صورت می گیرند و در فضای سایبر خسارات فراوانی ایجاد می کنند. ارزش تمامیت داده و سامانه های رایانه ای یکی از مهم ترین اصول امنیت رایانه به شمار می آید که به حفظ موجودیت و یکپارچگی داده ها و سامانه های رایانه ای اشاره دارد. قانون جرایم رایانه ای ایران در جهت حمایت از این ارزش، موادی را به جرم انگاری جرایم علیه تمامیت داده و سامانه های رایانه ای اختصاص داده است. این مواد در دو عنوان تخریب داده ها و اخلال سامانه ای قابل جمع اند؛ تخریب داده ناظر به هر گونه ایراد آسیب غیر مجاز به داده های رایانه ای می باشد و اخلال سامانه ای ایجاد اختلال یا از کار انداختن سامانه ها را مورد مجازات قرار می دهد. بنابراین تخریب داده ها، اخلال سامانه ای، ممانعت از دسترسی و تروریسم سایبری از گونه های خرابکاری رایانه ای محسوب می گردند. با بررسی هایی که در این تحقیق صورت می گیرد محقق می گردد که تخریب سایبری ماهیتی متفاوت از تخریب سنتی دارد و این نکته با بررسی ارکان تشکیل دهنده ی این جرم و تبیین متفاوت بودن رکن مادی و سایر ویژگی ها روشن می گردد. بنابراین در این تحقیق در پی آنیم که با تبیین صحیح و روشن ارکان تشکیل دهنده ی این جرایم، روشنگر ابهامات پیرامون این موضوعات باشیم و برای این مهم، اسناد و قوانین بین المللی که مهم ترین آنها کنوانسیون جرایم سایبر می باشد راهگشاست.

واژگان کلیدی: جرم رایانه ای، خرابکاری سایبری، تمامیت داده، تخریب داده، اخلال سامانه، داده، سامانه.

فهرست مطالب

عنوان **صفحه**

عنوان **صفحه**

فصل سوم: ارکان خرابکاری رایانه ای

عنوان **صفحه**

عنوان **صفحه**

مخفف ها:

ق.آ.د.د.ع.ا ..... قانون آیین دادرسی دادگاه های عمومی و انقلاب

ق.ج.ر..... قانون جرایم رایانه ای

ق.م.ا.....قانون مجازات اسلامی

فصل یکم:

کلیات

همزمان با تولد رایانه و پیشرفت آن، دنیای رایانه ها و به تعبیر صحیح تر فضای سایبر شکل گرفت. با گذشت زمان پیشرفت هر کدامشان از دیگری متأثر بود و هر دوی آنها بر زندگی بشر تأثیرگذار بود. فضای سایبر و رایانه زندگی بشری را با قوانین خود هماهنگ ساخته و جامعه ای نوین را برپا کرده است. جامعه ای که در آن پول الکترونیکی در قراردادهای الکترونیکی تنها در سامانه بانک های الکترونیکی رد و بدل می گردد و تجارت الکترونیکی را سرعت می بخشد.

مؤثرترین چیزی که در این فضا نقش ایفا می کند، اطلاعات و داده است. در واقع داده و اطلاعات جان فضای سایبر محسوب می گردند که بدون آنها سخن گفتن از فضای سایبر، سخن گفتن از جسم بی روح است. این ویژگی مهم ترین تفاوت فضای سایبر از دنیای واقعی به شمار می آید. فضایی که در آن زمان و مکان اهمیت خود را از دست می دهند و به قولی بی معنی می گردند، فضایی که حضور فیزیکی در آن بی ارزش می گردد؛ و این هاست که باعث می گردد فضای سایبر ماهیتی مستقل و متفاوت از فضای واقعی به خود بگیرد. متناسب با این فضا ارزش هایی نیز متفاوت از ارزش های حاکم بر دنیای واقعی، بر فضای سایبر و عناصر تشکیل دهنده آن حکم فرماست.

به این دلیل که فضای سایبر شکل گرفته از رایانه و شبکه به هم پیوسته از رایانه هاست که شالوده اصلی آن را داده تشکیل می دهد، مهم ترین ارزش های این فضا نیز در جهت حمایت از این داده ها و اطلاعات شکل گرفته اند.

برجسته ترین این ارزش ها که در جهت حمایت حفظ امنیت رایانه به وجود آمده اند؛ عبارتند از: ارزش تمامیت داده و سیستم، حفظ محرمانگی داده و سیستم و دسترس پذیری داده و خدمات.

ارزش تمامیت داده و سیستم، ناظر به موجودیت و یکپارچگی داده و سیستم می باشد و محرمانگی داده بیانگر این نکته است که هیچ کس این اجازه را ندارد که بدون مجوز به داده یا سامانه دیگری دست پیدا کند و از اطلاعات او بهره مند گردد و دسترس پذیری به قابلیت دسترسی مستمر به داده و سامانه و خدمات آن برای کاربران و صاحبان آنها اشاره دارد.

همان گونه که هر جامعه ای برای خود دارای ارزش ها و اصولی است که از اعضا خود خواستار حفظ و رعایت آنها می باشد و نقض هریک از این ارزش ها و اصول را تعرض به جامعه و اعضای آن محسوب می کند و در برابر آن واکنش نشان می دهد، در فضای سایبر نیز همین گونه است. به عبارتی، همانند دنیای واقعی هر گاه در فضای سایبر یکی از ارزش های پیش گفته نقض گردد، ضرری صورت می گیرد که امنیت رایانه و فضای سایبر را زیر سؤال می برد و در این حالت جرمی صورت گرفته که نیازمند واکنش است. به عبارتی معیار جرم انگاری در جرایم رایانه ای، نقض هر یک از این ارزش ها می باشد و حمایت کیفری از آنها نمود می یابد. در راستای این حمایت، در کنوانسیون های بین المللی و در تقسیم بندی هایی که از جرایم رایانه ای صورت گرفت، مهم ترین و فنی ترین دسته بندی، دسته بندی جرایم رایانه ای بر اساس نقض معیار های امنیت فضای سایبر می باشد، که رفتارهای مجرمانه که این معیارها را نقض می کنند در سه دسته جای می دهند: دسته نخست:جرایم علیه صحت و تمامیت داده یا سیستم، دسته دوم: جرایم علیه محرمانگی داده یا سیستم و دسته سوم: جرایم علیه قابلیت دسترسی داده یا سیستم.

خرابکاری رایانه ای عنوان مجموعه ای از جرایم رایانه ای است که علیه تمامیت داده یا سامانه صورت می گیرند و ارزش تمامیت داده و سیستم را نقض می کند و امنیت رایانه و فضای سایبر را از بین می برد. این دسته از جرایم در مبحث دوم فصل دوم جرایم رایانه ای ایران، با عنوان «تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی» جرم انگاری شده است: تخریب داده، اخلال سامانه ای، ممانعت از دسترسی و تروریسم سایبری. این جرایم در دو عنوان تخریب داده ها و اخلال سامانه ای قابل جمع اند؛ تخریب داده ناظر به هر گونه ایرادِ آسیب غیر مجاز به داده های رایانه ای می باشد و اخلال سامانه ای ایجاد اختلال یا از کار انداختن سامانه ها را مورد مجازات قرار می دهد. هر دوی این عناوین مجرمانه، زیر واژه خرابکاری رایانه ای قابل بحث هستند. به عبارتی خرابکاری رایانه ای، عنوان عامی است که هم تخریب را دربر می گیرد و هم اخلال را. استفاده از این عنوان در این پایان نامه برای این است تا بتواند همه ی

چهار عنوان مجرمانه ی پیش گفته را در برگیرد. هر چند این عنوان در قانون جرایم رایانه ای به کار نرفته است ولی جایگاه روشنی در عرف دارد و همین عنوان را می توان برای همه گونه های رفتاری که عرف، فاعل آن را خرابکار می نامد، به کار برد.

به کارگیری واژه خرابکاری در قانون ایران پیشینه داشته و مقنن بدون اینکه منظور خود را از این واژه بیان کند و بیشتر با تکیه بر روشن بودن مفهوم این واژه در عرف و جامعه، از آن در چند قانون بهره برده است؛ نمونه روشن این گفته، قانون مجازات اخلال کنندگان در امنیت پرواز هواپیما و خرابکاری در وسایل و تأسیسات هواپیمایی مصوب ۱۳۴۹ و هم چنین ماده ۶۸۷ قانون مجازات اسلامی مصوب ۱۳۷۵ می باشد. در قانون پیش گفتهٔ ۱۳۴۹ مقنن اعمالی مانند آسیب رساندن به هواپیما یا مسافرین یا گروه پرواز و اموال موجود درآن، ایجاد مانع درکار تأسیسات ناوبری هوایی، خارج ساختن کار دستگاه‌های ناوبری از مجرای صحیح خود و... و معاونت در این اعمال را جرم انگاری نموده و تمامی این جرایم را تحت عنوان «خرابکاری در وسائل و تأسیسات هواپیمایی» قرار داده است. در ماده ۶۸۷ ق.م.ا نیز مقنن، تخریب یا ایجاد حریق یا از کار انداختن را از زیر مجموعه های واژه ی خرابکاری قرار داده است و این گونه بیان می کند: « هر کس ...، مرتکب تخریب یا ایجاد حریق یا از کارانداختن یا هر نوع خرابکاری دیگر شود... ». در همین راستا می باشد که در این تحقیق تصمیم گرفته شد که از عنوان «خرابکاری رایانه ای» برای تحت شمول قرار دادن جرایم علیه تمامیت داده استفاده گردد.

۱-۱- شرح و بیان مسأله پژوهشی

امروزه با عنایت به اینکه داده های حاصل از تلاش فکری و علمی متخصصان امور رایانه ای بعضاً با تلاش فراوان و صرف هزینه های مالی و زمانی بسیاری تولید می شود و با توجه به اینکه با ارزش ترین دستاورد جامعه ما گندم، فولاد یا حتی فناوری نیست بلکه اطلاعات است(دی آنجلیز، ۱۷:۱۳۸۲) و نیز در راستای حمایت از داده هایی که دولت، موسسات خصوصی و سایر افراد در فعالیت های خود از آن بهره مند می شوند ضرورت حمایت کیفری از داده ها احساس می شود و این خرابکاری رایانه ای است که تمامیت و در دسترس بودن داده ها، برنامه ها و سامانه های رایانه ای را به خطر می اندازد.

«صحت و تمامیت داده و سامانه های رایانه ای در کنار محرمانگی داده ها و سامانه های رایانه ای از اصول بنیادی امنیت رایانه است. برجستگی این اصل حتی از محرمانگی نیز بیشتر است؛ زیرا صحت و تمامیت داده، نشانگر پیکره فضای سایبر و استواری آن است؛ و نبود آن به آشفتگی و پریشانی افزارهایی است که فضای سایبر را پدید آورده اند.

برجستگی دیگر اصل صحت و تمامیت داده ها و سامانه ها، در این است که اصل دسترس پذیری که سومین اصل از اصل های بنیادی امنیت رایانه به شمار می رود را در بر می گیرد. رفتارهایی که سبب می شود تا دارنده ی داده نتواند به طور قانونی به داده هایش دست یابد یا به سامانه اش دسترسی داشته باشد، گونه ای از اخلال در داده ها یا سامانه های رایانه ای است. از این رو قانون جرایم رایانه ای، بزه ممانعت از دسترسی به داده یا سامانه را در زیر بزه های ضد صحت و تمامیت داده و سامانه آورده است(عالی پور، ۱۳۸۸ :۱).

اخلال یا از کارانداختن در برگیرنده پدیدآوردن ناتوانی و نارسایی در انجام بهینه و متعارف یک مال است. هر چند اخلال رایانه ای نسبت به داده ها و سامانه های رایانه ای و آن هم درفضای سایبر صورت می گیرد و چنانچه کسی به قصد از میان بردن داده های دیگری ، رایانه اش را از بلندی پرت کند یا آن را بسوزاند یا لوح فشرده را به دو نیم کند یا آن را بخراشد یا سنگ، بر روی داده بر(حامل داده) بزند، هیچ یک تخریب یا اخلال رایانه ای نیست و بر حسب مورد درذیل دو ماده ۶۷۶ و ۶۷۷ ق.م.ا(تخریب سنتی) جای می گیرند. اما با توجه به عمل مرتکب در بزه اخلال رایانه ای که عبارت است از : حذف، تخریب، مختل و غیر قابل پردازش کردن در بزه اخلال داده های رایانه ای- که این ۴ رفتار روی هم رفته در زیر دو رفتار تخریب و اخلال گرد می آیند- و مقایسه آن با عمل مرتکب در تخریب سنتی(ماده ۶۷۷ قانون مجازات اسلامی)؛ این سوال مطرح می گردد که: آیا بزه تخریب داده های رایانه ای ماهیتاً متفاوت از جرم تخریب سنتی به شمار می آید؟

از طرف دیگر موضوع بزه اخلال داده های رایانه ای در ماده ۸ ق.ج.ر (۷۳۶ ق.م.ا) «داده های دیگری» می باشد؛ صرف نظر از اینکه مالیت داشته باشد یا نداشته باشد، استناد پذیر باشد یا نباشد. «با توجه به اینکه اصطلاح داده یک عبارت نسبی است یعنی اگر موجب درک و فهم لازم و کامل در این مرحله شده باشد به عنوان آگاهی یا اطلاعات از آن نام می برند و چنانچه موجب درک و فهم کامل نگردد به عنوان همان داده به شمار می آیند(عالی پور ،۱۳۸۸:۲۵)»، و لحاظ اینکه بند «۲» ماده«۴» کنوانسیون جرایم سایبر مصوب ۲۰۰۱- که این کنوانسیون مخصوص شورای اروپاست اما قانون جرایم رایانه ای ایران برگرفته از این کنوانسیون می باشد- به اعضاء اجازه داده نسبت به این جرم [مختل کردن داده ها] حق شرط قائل شوند و مقررکنند این رفتار به زیان شدید منجر شود و تفسیر آنچه «زیان شدید» را تشکیل می دهد به قانونگذار ملی واگذار شده است . این تردید را در ذهن ایجاد می کند که: آیا بهتر نبود مقنن ما نیز معیار این چنینی برای جلوگیری از گستردگی دامنه ی شمول این ماده در نظر می گرفت. یا اینکه اقدام مقنن صحیح بوده است؛ چراکه همان گونه که در گزارش توجیهی کنوانسیون جرایم سایبر درمورد فلسفه ی جرم انگاری اخلال در

داده هاآمده است: «هدف از جرم انگاری اخلال در داده ها، حمایت از داده ها و برنامه های رایانه ای همانند اشیاء مادی در برابر آسیب های عمدی است. منافع قانونی حمایت شده در اینجا تمامیت و اجرا یا کاربری مناسب از داده های ذخیره شده و برنامه های رایانه ای است». این بحث در مورد بزه اخلال سامانه ای نیز مطرح است.

در ماده ی ۱۰ ق.ج.ر(ماده ۷۳۸ ق.م.ا)، ممانعت از دسترسی هم نسبت به داده، بزه به شمار می آید و هم سامانه. از آنجا که این ماده به سامانه مخابراتی هم پرداخته و نیز چون داده و سامانه را به طور جمع به کار برده است، این پرسش مطرح می گردد که آیا موضوع بزه ممانعت، خود داده یا سامانه است یا خدمات و کارکرد آن و آیا ممانعت از دسترسی به اینترنت یا خدمات ارتباطی می تواند در ذیل این ماده جای بگیرد؟ اگر بزه اخلال سامانه ای ازطریق بزه تخریب داده صورت گیرد مصداق تعدد است؟ مختل کردن کارکرد در بزه اخلال سامانه ای عمل مرتکب محسوب می گردد یا نتیجه ی رفتار او؟آیا مجازات های مقرر شده متناسب، مؤثرو بازدارنده می باشند؟و... .

در این پایان نامه سعی بر این است که با شناسایی ارکان تشکیل دهنده ی این بزه ها، به سوالات وشبهات موجود پاسخ دهیم و در نتیجه پیشنهاداتی برای کامل تر شدن قوانین در این زمینه مطرح کنیم.

۱-۲- سؤالات و فرضیات

سؤالاتی که در پی پاسخ به آنها هستیم در رده سؤالات فرضیه بردار هستند تا بتوان در پرتو آنها سخن از پایان نامه گفت و در نهایت از آنها دفاع کرد یا بر پایه دلایل قانع کننده ای آنها را رد نمود. سؤالات اصلی تحقیق حاضر عبارتند از:

- آیا لازم است که داده های موضوع بزه تخریب واخلال داده های رایانه ای دارای ارزش مالی یا استناد پذیر باشند؟
- با توجه به قانون جرایم رایانه ای آیا برای تحقق جرایم مشمول خرابکاری رایانه ای وقوع ضرر لازم است؟
- آیا مجازات های حبس و جزای نقدی که در قانون جرایم رایانه ای برای جرایم مشمول عنوان خرابکاری رایانه ای مقرر شده، مؤثر وبازدارنده هستند؟

فرضیه های تحقیق در قالب پاسخ به سؤالات فوق به شرح زیر است:

فرضیه یکم: لازم نیست که داده های موضوع بزه تخریب واخلال داده دارای ارزش مالی یا استنادپذیر باشند.

فرضیه دوم: برای تحقق جرایم مشمول خرابکاری رایانه ای لازم نیست ضرری صورت گیرد.

فرضیه سوم: با توجه به نوین بودن جرایم رایانه ای و شرایط ارتکاب آنها این مجازات ها نمی تواند مؤثر و بازدارنده باشد.

۱-۳- روش تحقیق

روش تحقیق در این پایان نامه در مقام توصیف و تحلیل مباحث مرتبط با خرابکاری سایبری است که گرد آوری اطلاعات از طریق روش کتابخانه ای، به عبارتی مراجعه به منابع مکتوب و مستندات کتابخانه ای، فیش برداری و استفاده از منابع اینترنتی می باشد. این تحقیق که متضمن بررسی مباحث و مطالب گفته شده پیشینیان و ارزیابی اعتبار و صحت آنهاست غالباً به طریق کتابخانه ای صورت می گیرد. ابزار تجزیه و تحلیل در این تحقیق بر مبنای استفاده از روش عقلانی و بهره گیری از استدلال های منطقی و بکارگیری اصول مسلم حقوقی (به ویژه اصول تفسیر قوانین کیفری) می باشد.

۱-٤- اهمیت و ارزش تحقیق

در جامعه امروزی با توجه به اینکه محصولات فکری اندیشمندان ومتخصصان به صورت داده وارد فضای سایبر می گردد وبا توجه به اینکه جامعه به سمت الکترونیکی شدن، چه در بخش خصوصی چه در بخش دولتی، گام برمی دارد. و از سوی دیگر داده های حاصل از تفکرات اندیشمندان بعضاً با تلاش فراوان و صرف هزینه های مالی و زمانی بسیار تولید می گردد، ضرورت حمایت کیفری هر چه بیشتر از داده ها و سامانه های رایانه ای احساس می گردد. این خرابکاری رایانه ای است که صحت و تمامیت داده و سامانه را و به دنبال آن اصل دسترس پذیری را نقض می کند. بنابراین با توجه به جدیدالتصویب بودن قانون جرایم رایانه ای نیاز به تحقیقات جامع در این زمینه احساس می گردد تا جامعه دانشگاهی و نهادهای تصمیم گیراز طریق آن به طور کامل با ویژگی ها و ارکان این بزه هاکه جامعه اطلاعاتی را تهدید می کند؛ آشنا گردند. این تحقیق می تواند با نمایاندن ضعف و کاستی های این قانون در حمایت از داده ها و سامانه های رایانه ای، مقنن را در تصویب قوانین کامل تر راهنما گردد. باید اضافه نمود که از این جهت نیز که خرابکاری رایانه ای از ارکان مادی بزه تروریسم سایبری به شمار می رود، این تحقیق در این زمینه نیز می تواند حائز اهمیت محسوب گردد و زوایایی از این قضیه را روشن گرداند.

۱-۵- اهداف تحقیق

با توجه به سؤالات و فرضیات تحقیق، اهداف را می توان این گونه بیان کرد:

- شناسایی جایگاه خرابکاری رایانه ای از منظر حقوقی
- تبیین ارکان تشکیل دهنده جرایم مشمول عنوان خرابکاری رایانه ای
- ارزیابی ضمانت اجراهای خرابکاری رایانه ای
- تقویت نقاط قوت و یافتن راهکارهایی برای نقاط ضعف قانون جرایم رایانه ای در زمینه خرابکاری رایانه ای

۱-٦- سابقه تحقیق

با تحقیقاتی که در این زمینه صورت گرفت کتاب و پایان نامه ای با این عنوان و موضوع یافت نشد. با این وجود در مقالات و پایان نامه ای به مناسبت و به صورت گذرا به این موضوع پرداخته شده است:

پاکزاد(۱۳۹۰) در کتاب تروریسم سایبری: تهدیدی نوین علیه امینت ملی، پس از پرداختن به سنخ شناسی، طبقه بندی انواع تروریسم و بیان سیاست جنایی تقنینی جمهوری اسلامی ایران در قبال تروریسم به ویژه تروریسم سایبری، به خرابکاری سایبری پرداخته است. خرابکاری سایبری در این رساله مفهومی دربرگیرنده ی اتلاف داده، تحریف اطلاعات، دست اندازی به نام دامنه و... در نظر گرفته شده است. باید در نظر داشت که در این رساله به بزه های تخریب، اخلال و ممانعت از دسترسی به عنوان رکن مادی بزه تروریسم سایبری پرداخته شده است نه به عنوان یک جرم مستقل. به همین دلیل ارکان تشکیل دهنده ی این بزه ها را به طور مفصل بیان نمی کند.

بای و پورقهرمانی(۱۳۸۸) در کتاب بررسی فقهی حقوقی جرائم رایانه ای، بیشتر به مبانی فقهی و تاریخچه ی جرائم رایانه ای پرداخته اند. این کتاب ناظر به جرائم مندرج در قانون تجارت الکترونیکی و با تکیه بر قوانین بین المللی نگارش یافته است. باید در نظر داشت که چاپ این کتاب قبل از تصویب قانون جرائم رایانه ای می باشد.

نامی(۱۳۸۶) در مقاله ی تخریب نرم افزارهای رایانه ای با نگرشی نوین به جرم تخریب کیفری، پس از بیان ارکان جرم تخریب سنتی، با توجه به لایحه ی قضایی مجازات جرائم رایانه ای، به تخریب و ایجاد اخلال در داده و سامانه ی رایانه ای پرداخته است. ایشان داده را معادل نرم افزارهای رایانه ای دانسته اند، برای نرم افزارهای رایانه ای ویژگی مالی برشمرده اند؛ در حالی که نه تنها در قانون جرائم رایانه ای بلکه در لایحه ی قضایی مجازات جرائم رایانه ای چنین قیدی وجود ندارد. باید در نظر داشت که تغییرات عمده و مهمی در لایحه ی قانون جرائم رایانه ای به منظور تصویب صورت گرفته است.

فضلی(۱۳۸۴) در مقاله ی تخریب و اخلال در داده ها و سیستم های رایانه ای، که در اولین همایش بررسی ابعاد حقوقی فناوری اطلاعات ارائه نموده اند، جرم اخلال یا تخریب داده ها را از جرائم رایانه ای محض نمی دانند و معتقدند که تخریب از قدیم وجود داشته و اکنون نسبت به داده نیز اعمال می گردد. در حالی که باید گفت مبنای بزه های رایانه ای محض، موضوعات سایبری می باشد. در واقع بزه هایی، بزه رایانه ای محض به شمار می آیند که علیه داده یا سیستم صورت گیرند و در فضای سایبر واقع شوند و در بزه اخلال یا تخریب داده ها نیز همین گونه است. نکته ی دیگر اینکه، این مقاله با توجه به قوانین و کنوانسیون های بین المللی نگارش یافته است.

دی آنجلیز(۱۳۸۲) در کتاب جرایم رایانه ای، پس از بیان چگونگی پیدایش جرائم ریانه ای و گزارشات مرتبط با آن، به ویژگی های کلی فضای سایبر و مجرمین سایبری پرداخته است. به بیان این که خطر تروریسم سایبری جامعه ی اطلاعاتی را تهدید می سازد و شواهدی از این خطر، بسنده می کند. و در آخر از پلیس سایبر و هکرها و کرکرها سخن می گوید. در این کتاب توجه چندانی به قوانین و کنوانسیون های بین المللی ناظر به جرائم رایانه ای ندارد.

بنابر مطالب فوق و با توجه به جدیدالتصویب بودن قانون جرایم رایانه ای، مشخص می گردد که هنوز تحقیق جامعی در این زمینه صورت نگرفته است و به منظور شفافیت هرچه بیشتر این موضوع، نیاز به تحقیقات بیشتر در این زمینه احساس می گردد.

۱-۷- کاربرد نتایج تحقیق

از این جهت که جامعه و اعضای آن هر روز بیش از پیش به فضای سایبر، داده وسامانه های رایانه ای وابسته می گردند و از سوی دیگر هر روز خطرات بیشتری از جمله انتشارکرم ها و ویروس های رایانه ای این نیازها را تهدید می کند و قانون جرایم رایانه ای اولین قانونی است که از صحت و تمامیت آنها حمایت می کند. بنابراین، این تحقیق می تواند منبع مطالعاتی مناسبی به منظور شناساندن هرچه بهتر خرابکاری رایانه ای به جامعه دانشگاهی و نهادهای تصمیم گیر به شمار آید؛ قضات را در اجرای هرچه بهتر عدالت کیفری یاری رساند و نمایانگر نقاط ضعف و قوت قانون جرایم رایانه ای در این زمینه باشد. درنتیجه مقنن را درجهت تصویب نمودن قوانین کامل تر در این زمینه رهنمون گردد. همچنین از این لحاظ که طبق قانون جرایم رایانه ای، خرابکاری رایانه ای از ارکان مادی بزه تروریسم سایبری محسوب می گردد، این تحقیق منبع مطالعاتی مناسبی برای تحقیقات در این زمینه محسوب می گردد.

۱-۸- سامان دهی تحقیق