
بسم الله الرحمن الرحيم

دانشگاه پیام نور مرکز تهران
دانشکده حقوق
گرایش حقوق جزا و جرم شناسی

پایان نامه کارشناسی ارشد

تحت عنوان

بررسی سیاست جنایی ایران در قبال جرایم علیه صحت و تمامیت داده ها و سیستم های رایانه ای و مخابراتی

استاد محترم راهنما:
جناب آقای دکتر میلانی

استاد محترم مشاور:
سرکار خانم دکتر سوهانیان

دانشجو:
مهدی رزاقی نژاد

بهار ۱۳۹۳

تقدیم به؛

دو وجود پاک و مقدس:

پدر بزرگوارم...

که غیرت را در زخم دستانش...محبت را در

یک عمر زحمت بی منتش...و عشق به فرزند را

در جاذبه نگاهش می توان به نظاره نشست...

و مادر عزیزم...

که قلب پر عطوفتش،نهری است روان به نشانی کوثر،

و آفتاب مهرش در آستانه قلبم هرگز غروب نخواهد کرد...

و هر آنچه دارم از دعای خیر این دو فرشته مهربان است و دعای آنهاست

که ضامن پیشرفت و حرکت من است...

باشد که فرزند خوبی برایشان باشم و بتوانم گوشه ای از زحماتشان را

جبران کنم...

و تقدیم به؛

تمام کسانیکه صمیمانه دوستشان دارم و وامدار لطف بی

همتایشان هستم...

سپاس گذاری

"من لم یشکر المخلوق لم یشکر الخالق."

با سپاس فراوان از راهنمائی‌ها و زحمات جناب آقای دکتر میلانی و سر کار خانم دکتر سوهانیان اساتید محترم راهنما و مشاور، که از ابتدای راه و در طی انجام این تحقیق، با راهنمائی‌های خود مرا در نگارش این اثر یاری نمودند و جناب آقای دکتر نظیفی که زحمت داوری این اثر را برعهده گرفته اند.

چکیده

حفاظت از صحت و تمامیت داده ها و سیستم های رایانه ای از اهداف سیاست جنایی کشورها در وضع قوانین و جرم انگاری در حیطه فناوری اطلاعات می باشد زیرا که این دو اصل از اصول اساسی حاکم بر حمایت از داد ها و سیستم ها بوده و از اهمیت فوق العاده ای برخوردار است. جرائمی که ضد صحت و تمامیت در فضای الکترونیکی قابل وقوع هستند شامل چندین جرم می باشند. یکی از اینها جرم جعل رایانه ای ضد صحت داده ها می باشد که در قوانین متعدد چون قانون جرائم رایانه ای ، قانون تجارت الکترونیک و قانون جرائم نیروهای مسلح جرم انگاری گردیده و هدف مرتکب ایجاد یا تغییر در داده ها و برنامه های رایانه ای می باشد. قسم دیگر این جرائم عنوان عام خرابکاری رایانه ای می باشد که جرائم ضد تمامیت داده و سامانه ها را در بر می گیرد و چهار عنوان تخریب داده ، اخلال در سیستم ، ممانعت از دسترسی و تروریسم سایبری را شامل می شود که مرتکب آن با انجام اقداماتی بدون حق به داده های رایانه ای آسیب رسانده و یا کارکرد سیستم را مختل می نماید. آشنایی با مفاهیم اساسی هر یک از این جرائم و بررسی ارکان سه گانه و شناسایی انواع پاسخ های واکنشی و تدابیر کنشی در دو محور پیشگیری اجتماعی و وضعی وتبیین مدل سیاست جنایی کشور ایران در با مقابله با این قسم از جرائم به عنوان اهداف این پژوهش مد نظر قرار گرفته است. روش تحقیق توصیفی، تحلیلی و کتابخانه ای می باشد که محقق با بهره مندی از اسناد مختلف به بررسی جرائم در قوانین جاریه پرداخته و اقسام ضمانت اجراها را تبیین می نماید.یافته های این پژوهش حکایت از آن دارد که اولا این جرائم ماهیتی متفاوت از نوع سنتی داشته که در اثر فناوری نوین رایانه ای پدید آمده است ثانیا، مدل سیاست جنائی ایران در مقابله با این قسم از جرائم از الگوهای مدل های دولتی سیاست جنایی در مقابل مدل های جامعه ای آن تبعیت می کند که پاسخ ها با استفاده از نظام کیفری اعمال می شود، ثالثا ، سیاست جنایی تقنینی ایران به دلیل عدم حمایت مقررات حقوق جزای سنتی از داده ها و سامانه های رایانه ای و به موازات مقررات کنوانسیون جرائم سایبر اقدام به جرم انگاری این قسم از جرائم نموده و رابعا، پاسخ های تعیین شده در قوانین موضوعه اکثرا سرکوبگرایانه و همان مجازات های متداول حقوق جزای کلاسیک چون حبس و جزای نقدی می باشد.

کلید واژه: جرائم سایبر ، جرم رایانه ای ، تمامیت داده ، صحت داده ، سامانه رایانه ای ، جعل رایانه ای ، خرابکاری.

فهرست مطالب

عنوان صفحه

بخش اول

فرآیند جرم انگاری جرایم علیه صحت و تمامیت داده ها

بخش دوم

نظام پاسخ ها و ضمانت اجراهای مرتبط با جرائم علیه صحت و تمامیت داده ها

مقدمه

با پیدایش کامپیوتر ، جرائم کامپیوتری نیز پا به عرصه وجود نهاد ، بگونه ای که شیوع استفاده از رایانه در زندگی شخصی و روابط اجتماعی ، بزهکاری و تخلف استفاده از رایانه ، امری اجتناب پذیر می‌باشد[1].

فضای سایبری در دنیای اینترنتی و ارتباطات بسیار شنیده می شود[2]، در لغت فضای سایبر را به مجاز و مجازی ترجمه کرده اند که واژه مجاز در مقابل حقیقت بکار می رود ولی واژه محیط سایبر در عین اینکه بصورت شکل مادی قابل لمس نیست لکن محیطی است حقیقی و واقعی نه مجازی که از این محیط به محیط فن آوری اطلاعات (IT) یا محیط اطلاعات و ارتباطات نیز نام برده اند[3]. شاخه حقوق کیفری فن آوری اطلاعات ، رشته ای نوظهور و ناشی از فن آوری مدرن بوده که در دو دهه اخیر بوجود آمده و همانند برخی از رشته های نو چون حقوق کیفری محیط زیست یا حقوق کیفری اداری به بررسی جرائم رایانه ای در حوزه کامپیوتری می پردازد.

در خصوص جرائم رایانه ای تعاریف متعددی صورت پذیرفته و اولین مشکل در ارائه تعریف ، ماهیت جرائم سایبری می باشد که در تعریف آن الگوی یکسانی مورد تبعیت قرار نگرفته است بگونه ای که کشورها و سازمان های بین المللی تعاریف متعددی را ارائه نموده اند ، برای مثال سازمان ملل در نشریه بین المللی "سیاست جنایی" با یادآوری این نکته که در جرائم رایانه ای تعریف واحدی وجود ندارد، جرائم کامپیوتری را از یک طرف شامل فعالیت های مجرمانه با ماهیت سنتی مثل سرقت و جعل دانسته و از سوی دیگر شامل فعالیت های مجرمانه جدید می داند که از این منظر امکان سوء استفاده را برای کاربران فراهم می ساخته است[4]. کنوانسیون جرائم سایبر هرچند تعریفی ارائه نداده بلکه فقط به ذکر مصادیق بسنده کرده است. سازمان همکاری و توسعه اقتصادی (OECD) به عنوان یکی از سازمان های فعال و پیشرو در زمینه جرائم رایانه ای به ارائه تعریفی از سوء استفاده از رایانه پرداخته است. برابر با تعریف سازمان مذکور ، سوء استفاده از رایانه شامل هر رفتار غیرقانونی ، غیر اخلاقی یا غیر مجاز مربوط به پردازش خودکار و انتقال دادهاست[5].درایالت متحده آمریکا تعریف موسعی ازجرائم کامپیوتری به‌عمل

---

[1]- محیطی که اصطلاحا جرائم رایانه ای درحوزه آن به وقوع می پیوندد،محیط سایبر نامیده می شود.

[2]- فضای سایبر محیطی است مجازی و غیر ملموس که در فضای شبکه های بین المللی وجود داشته و در این محیط تمامی اطلاعات مربوز به روابط افراد و فرهنگ ها بصورت نوشته ، صوت ، و اسناد د یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس کاربران می باشد.

[3]- اصطلاح فضای سایبر برای اولین بار در سال ۱۹۸۲ در یک داستان علمی تخیلی بکار رفت و در سال ۱۹۹۰ پرفسور جان پری بارلو به هنگام صحبت در یک کنفرانس بر خط آن را بکار برد و بر سر زبانها انداخت.

[4]- دزیانی، محمد حسن، جرائم کامپیوتری، جلد اول، تهران، دبیرخانه شورای عالی انفورماتیک، چاپ محدود، ۱۳۷۶،ص۴۹

[5]-باستانی، برومند،جرائم رایانه‌ای واینترنتی جلوه‌ای نوین ازبزهکاری، تهران، انتشارات بهنامی، چاپ دوم، سال ۱۳۸۶،ص ۲۱

آمده است:«هراقدام غیر قانونی که با یک کامپیوتریا سیستم کامپیوتری یا بکارگیری آن مرتبط باشدجرم کامپیوتری است و نیزهر اقدام عمومی که به هر ترتیب با کامپیوتر مرتبط بوده و موجب ایراد خسارت به بزه دیده شده و مرتکب از این طریق منافعی را تحصیل کند،جرم کامپیوتری است». در ایران در یک تعریف ارائه شده هر فعل یا ترک فعلی که علیه کامپیوتر یا شبکه های کامپیوتری صورت گرفته یا بواسطه کامپیوتر یا شبکه های کامپیوتری محقق شود، جرم کامپیوتری نام گرفته است[1].بیشتر حقوق دانان در تعیین اولین جرم رایانه ای ، اختلاف نظر دارند ولی نظر غالب بر این است که "قضیه الدون رویس" بعنوان اولین جرم رایانه ای ثبت گردیده است[2].بحث جرائم رایانه ای در ایران ابتدا در اوایل دهه ۸۰ مطرح شد. آن زمان بیشتر حوزه هایی را در بر می گرفت که به جعل اسناد دولتی و شخصی مربوط می-شد. در خصوص اولین جرم رایانه ای در ایران به نظر می رسد در خرداد ماه سال ۷۸ به ثبت رسیده باشد به این توضیح که یک دانشجوی کامپیوتر با یک کارگر کارخانه در کرمان ، چک های تضمینی را جعل می کردند. جعل اسکناس،بلیط شرکت های اتوبوسرانی،جعل اسناد دولتی،کارت پایان خدمت و چک های مسافرتی، از دیگر اشکال جرائم رایانه ای در اوایل دهه ۸۰ است ، پس از آن برخی وبلاگ نویسان به اتهام نوشتن مطالب در سایت های دیگر و همچنین به اتهام هایی چون توهین به افراد یا مقدسات یا افشای اسرار و اسناد دولتی محاکمه گردیدند و دولت با فیلترینگ گسترده سایت ها و کنترل سرعت اینترنت به دنبال توسعه مصداق های جرائم رایانه ای برآمد.همچنین شکایت به خاطر اختلاف بر سر دامنه های اینترنتی ، اختلاف شرکت های کامپیوتری، اینترنت وب سایت ها، شکستن قفل نرم افزارها و هک ای میل های شخصی از دیگر مواردی است که روز به روز بر تعدا این جرائم افزوده است[3].

برخی نویسندگان بر اساس دسته بندی تلفیقی بزه های رایانه ای را به چهار دسته ذیل طبقه بندی می نمایند[4]:

۱- بزه های ضد صحت و تمامیت داده و سیستم مانند جعل و خرابکاری رایانه ای

۲- بزه های ضد محرمانگی یا خلوت داده یا سیستم مانند شنود غیر مجاز

۳- بزه های ضد قابلیت دسترسی داده یا سیتم مانند دسترسی غیرقانونی و غیر مجاز

۴- بزه های قابل ارتکاب از طریق رایانه که خود بر دو دسته بزه های ضد شخصیت معنوی افراد و بزه های مالی تقسیم بندی می شود مانند هتک حیثیت، نشر اکاذیب و کلاهبرداری.

---

[1]- بای، حسینعلی، پورقهرمانی، بابک، بررسی فقهی حقوقی جرائم رایانه‌ای، قم، پژوهش‌های علوم و فرهنگ اسلامی، چاپ اول، پاییز ۱۳۸۸،ص۳۸

[2]- بدین توضیح که وی بعد از بی مهری مسئولان شرکت عمده فروشی میوه و سبزی بعنوان حسابدار آنجا انتخاب می شود که مبالغی از مرجع آن را کاهش و به حساب دیگری واریز می نماید.

[3]- فریبرزی، الهام، سیر تحول قوانین مربوط به جرائم رایانه‌ای در ایران و جهان، فصلنامه تخصصی فقه و تاریخ تمدن، سال هشتم، شماره ۲۷، بهار ۱۳۹۰،ص۶۰

[4] - Walden, Lan, Computer Crimes and Digital Investigations, Axford University press, Frist Publish, 2007.

دسته بندی فوق همان تقسیم بندی بر مبنای نقش رایانه است.کنوانسیون بزه های محیط سایبر از شیوه تلفیقی استفاده نموده است. علاوه بر کنوانسیون مزبور این شیوه از سوی قانون جرائم رایانه ای مصوب ۱۳۸۸ نیز گزینش گردیده است:

الف– بیان مسئله و سوالات تحقیق

به موازات گسترش فعالیت های ارتباطی در فضای سایبر ، بخشی از بزهکاران ،فعالیت های مجرمانه و تبهکارانه خود را به این فضا منتقل نموده اند و در سطح گسترده مرتکب جرائم متعددی گردیده اند. عده ای از بزهکاران با ظهور فضای مجازی ، نه تنها فرصت ها و ابزارهای جدیدی در جهت ارتکاب جرم کشف نموده اند ، بلکه مبدع اقسام بزهکاری در قالب فناوری های رایانه ای نیز گردیده اند[۱].

از اینرو، نه تنها شاهد جرائم متعارفی چون سرقت،کلاهبرداری، جاسوسی، نشر اکاذیب هستیم، که همانند فضای واقعی در محیط پرزرق و برق در گستره اینترنت ارتکاب می یابند بلکه جرائم جدیدی نیز در حال شکل گیری است که موضوع آن اقدام علیه امنیت سامانه ها و شبکه های رایانه ای است که از جمله آن می توان جرائم علیه محرمانگی ، صحت و تمامیت و در دسترس پذیری سامانه ها و داده ها را نام برد که در مجموعه جرائم سایبر در معنای مضیق قلمداد می گردد.

جرائم سایبری دارای ویژگی متمایزی از سایر جرائم کلاسیک می باشد چرا که ماهیت این گونه جرائم به دلیل تکنولوژی پیچیده و گسترده ، خصوصیات منحصر بفرد را دارد و باعث می گردد قوانین موجود پاسخگوی مسائل نباشند. از جمله مهمترین خصوصیات می توان به تنوع مرتکبان و گستردگی حجم خسارات وارده ، عدم وابستگی به محل ارتکاب جرم و فرا ملی بودن آن ، سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان، سهولت از بین بردن آثار وقوع جرم و بالا بودن رقم سیاه آن اشاره نمود[۲].

برای درک شناخت مناسب از جرائم رایانه ای منجمله جرائم مورد بحث بدوا نیازمند شناخت ارزش های مورد حمایت در محیط سایبر می باشیم.

در باب سیاست جنایی جرائم سایبری منجمله جرائم مورد بحث در نوشتار حاضر ، علاوه بر جرم انگاری مصادیق مجرمانه از طریق وضع ضمانت اجراهای کیفری توسل به اقدامات کنشی اعم از پیشگیری اجتماعی و وضعی در قالب آموزش کاربران اینترنتی در فضای سایبر و همچنین ارتقای

---

[۱]–پیکا، جورج، جرم شناسی، ترجمه نجفی ابرندآبادی، علی حسین، تهران، نشر میزان، چاپ اول، زمستان ۱۳۸۹،ص ۱۱

[۲]–جاویدنیا، جواد، جرائم تجارت الکترونیکی (جرائم رایانه‌ای در بستر تجارت الکترونیکی)، تهران، انتشارات خرسندی، چاپ اول، سال ۱۳۸۸،ص ۹۸

راهکارهای فنی امنیت سیستم ها و گوشزد نمودن استفاده از تدابیر حفاظتی و نظارتی از اهمیت ویژه ای برخوردار است.

ازجمله اصول حاکم برفناوری اطلاعات وامنیت رایانه،اصل جریان آزاد اطلاعات است که رعایت این اصل در پرتوی احترام و حمایت از محرمانگی ، تمامیت و دسترس پذیری داده ها و اطلاعات ممکن خواهد بود ، لذا داده های رایانه ای در فضای سایبر می بایست در معیت این اصل مورد حمایت واقع گردند.از اینرو،هیچکس نمی تواند بدون حق در جریان آزاد اطلاعات خلل وارد نماید لیکن لازم به ذکر است که محدوده این اصل تا حدی لازم الرعایه است که به حریم خصوصی و ارتباطی سایر افراد من جمله داده های شخصی ، امنیتی و اسرار مهم دولتی لطمه ای وارد نسازد.

محرمانگی[۱] داده ها و اطلاعات و دسترس پذیری[۲] آنها از اصول با اهمیت دیگر ناظر بر حمایت از داده هاست. محرمانگی ویژگی برجسته بخشی از زندگی انسانهاست که نمی خواهد دیگران از اطلاعات شخصی افراد آگاه شوند و تعرض به این اصل زمانی تحقق می یابد که یک معترض (هکر) اطلاعات کاربر رایانه ای را بدون اجازه مشاهده،نسخه برداری یا استفاده می نماید.ارزش این اصل به حدی است که مقنن ایران در یک فصل مستقل به جرم انگاری بزه های ضد مرحمانگی پرداخته است.

حفظ عملکرد سیستم و در دسترس نگه داشتن آن برای افراد و جامعه نیازمند حمایت ویژه بوده و در پرتوی اصل دسترس پذیری تحقق می یابد زیرا که تحصیل اطلاعات و برنامه های مرتبط برای کاربران در هر زمانی امری ضروری و حیاتی جلوه می نماید.نقض این عامل زمانی محقق می گردد که کاربر برای مدت طولانی یا کوتاه از ارتباط و دستیابی به سیستم رایانه ای و اطلاعاتی خویش باز می ماند و مشاهده آن برای وی غیر ممکن می گردد. نمونه معمول حملات، حملات گسترده**Dos**[۳] و **DDos**[۴] می باشد که مهاجمان با استفاده از آنها و بکارگیری روش های متعدد می کوشند که کاربران مجاز را از دستیابی و استفاده از یک سرویس خاص دچار مشکل نموده و به نوعی در سرویس های یک شبکه اخلال ایجاد نمایند[۵].

یکی دیگر از اقسام جرائم رایانه ای ، جرائم علیه صحت و تمامیت داده های رایا نه ای و مخابراتی می باشد، تمامیت به معنای حفظ اصالت در برابر تحریفات است که در معنای عام صحت را نیز در بر می گیرد و این اطمینان را بوجود می آورد که هیچکس نمی تواند اطلاعات دیگری را تغییر،تحریف یا تخریب نماید.

---

۱ - Confidentiality

۲ - Availability

۳ - Denial of Service

۴ - Distributed Denial of Service

۵-مقنن ایران بزه ممانعت از دسترسی را که ضد اصل دسترس پذیری است،در زیر مجموعه جرائم علیه صحت و تمامیت داده ها مورد مطالعه خویش قرار می دهد که بعنوان بخشی از این رساله از نظر خواهد گذشت.

حقوق کیفری اطلاعات در این زمینه مکلف است حفاظت دو فاکتور تمامیت داده ها و صحت آنرا تضمین نماید.درکنوانسیون جرائم سایبر، جرائم بر ضد محرمانگی،تمامیت و در دسترس بودن داده ها و سامانه‌های رایانه ای،تحت یک طبقه وبا هم آمده است وجرائمی که دراین دسته قرار می گیرند،عبارتند از: دستیابی عمدی و من غیر حق به سامانه های رایانه ای ،شنود عمدی و من غیرحق، ایجاد اخلال من غیر حق در داده ها و ایجاد اخلال عمدی در سامانه های رایانه ای، سوء استفاده از وسایل رمز عبور و کد دستیابی یا داده یا برنامه های رایانه ای[1].

اولین جرمی که در طبقه بندی این دسته از جرائم واقع می گردد،جعل رایانه ای و استفاده از سند مجعول می باشد. جعل در حقوق جزای سنتی از جمله جرائم علیه آسایش عمومی بوده که باعث سلب روابط مردم در صحنه اجتماعی با یکدیگر می گردد. این جرم وفق مواد قانون مجازات اسلامی و به روش سنتی در اسناد و نوشته ها قابل تعقیب و مجازات می باشد.همانگونه که حقوق جزا با بکارگیری مقررات لازم ، حمایت از صحت و اصالت ارزش های غیر الکترونیکی و اسناد عادی را تضمین می نماید، همین نقش را باید در خصوص حفظ صحت و در نتیجه مجازات جاعلان اسناد رایانه ای ایفاء نماید.به همین خاطر با پیشرفت فناوری اطلاعات ارتکاب این جرم در فضای مجازی آنهم نسبت به داده ها و اسناد الکترونیکی قابل تعقیب و مجازات می باشد.هدف جرم انگاری جعل رایانه ای این است تا خلاء های قانون جزا را در جعل سنتی که منوط به خواندنی بودن نوشته ها یا اظهارات موجود در سند است و داده های الکترونیکی را در بر نمی گیرد برطرف نماید.قوانین جرائم قبل از سال ۸۲ درباره جعل رایانه ای ساکت بود تا اینکه با تصویب قانون تجارت الکترونیکی مصوب۸۲/۴/۲۴ ماده ۶۸ این قانون به جعل کامپیوتری اختصاص یافت و مصادیق جعل رایانه ای را مشخص نمود اما با عنایت به تنوع جعل و محدودیت شمول قانون مزبور به مبادلات تجاری ،الکترونیکی، مقنن ماده ای را در قانون جدید به جعل رایانه ای اختصاص داده که درکنار قانون تجارت الکترونیک به عنوان قانون خاص مرتکبین را تحت پیگرد قانونی قرار خواهد داد ضمن آنکه قانون مجازات جرائم نیروهای مسلح نیز جعل رایانه ای را برای نظامیان جرم انگاری نموده است. قانونگذار درماده ۶ قانون جرائم رایانه ای(ماده ۷۳۴ قانون مجازات اسلامی)، هرگونه تغییر داده ها و علائم موجود درکارت های حافظه و وارد کردن متقلبانه آنها را تحت عنوان جعل و استفاده از سند مجعول کامپیوتری جرم انگاری نموده است[2].

---

[1]- بزه جعل رایانه ای نیز در یک ماده مستقل و جداگانه در کنوانسیون مزبور مورد جرم انگاری واقع گردیده است.

[2]-لازم به ذکر است که کنوانسیون جرائم سایبری نیز درماده ۷ خود جعل رایانه ای را بعنوان بخشی ازجرائم پیش بینی نموده است لذا محقق در صدد آن است تا ضمن ارائه تعریفی از جعل رایانه ای این جرم را با عناصر اختصاصی آن در قوانین جاریه و بررسی مبانی جرم انگاری مورد تجزی و تحلیل خویش قرار دهد.

از دیگر جرائمی که مقن آنرا در دسته جرائم علیه تمامیت داده های رایانه ای قرار داده تخریب و اخلال در داده ای رایانه ای و همچنین سابوتاژ رایانه ای می باشد[1].این نوع از جرائم بدلیل نوظهور بودن از اهمیت بیشتری نسبت به سایرین برخوردار می باشد.سابقا در اکثر نظامهای حقوقی تمامیت داده های ذخیره شده در رایانه تحت مقررات کلی مربوط به تخریب، قرار می گرفت اما با عنایت به اینکه مقررات قبلی به منظور حمایت از اشیاء ملموس مادی و ضع گردیده بود در حیطه فناوری اطلاعات قابل اجرا نبود.ایجاد شبکه های اطلاع رسانه ای رایانه ای در سطح جهانی، فعالیت تخریب و اخلال را درباره داده ها و کارکرد سیستم های رایانه ای تسهیل نموده و باعث گردیده تا عده ای فعالیت خود را در راه ایجاد و تولید برنامه های مخرب معطوف نمایند. این امر باعث گردیده تا بسیاری از کشورها در حوزه تخریب و اخلال در داده های رایانه ای اقدام به وضع قوانین کیفری نمایند. ایجاد اختلال از شیوه هایی است که امروزه امر دسترسی افراد به اطلاعات را با مشکل روبه رو می نماید زیرا اختلال ممکن است از طریق سیستم های رایانه ای، امواج یا برنامه های مخربی نظیر ویروس یا کرم های رایانه ای را وارد سیستم نماید. با عنایت به اینکه نرم افزار های رایانه ای حالت غیرملموس دارند، و جزء اموال مادی محسوب نمی شوند، لذا نمی توان مرتکبین آنرا تحت عنوان تخریب کیفری مجازات نمود لذا عناوین تخریب رایانه ای و سابوتاژ رایانه ای در قوانین پیش بینی گردیده است. منافع قانونی مورد حمایت، تمامیت داده ها و برنامه های رایانه ای می باشد.

عمل تخریب نرم افزارها جزء جرائمی است که با ابداع کامپیوترپدید آمده است. تخریب،اخلال و غیرقابل استفاده کردن داده ها، اعمالی است که دسترسی به داده ها را به خطر افکنده و باعث گردیده کشورها در خصوص حمایت از داده ها جرم انگاری نمایند،کشور ما نیز از این قاعده مستثنا نبوده و همانندکنوانسیون جرائم سایبر درکنار جعل رایانه ای، عمل تخریب و اخلال در داده ها را نیز جرم انگاری نموده است[2].

۱- با وجود قانون تجارت الکترونیک زوایای مورد نیاز در جرائم الکترونیکی کدام است؟

۲- اهداف سیاست جنایی کشور ما از جرم انگاری جرائم الکترونیکی چه می باشد؟

[1]- سابوتاژ رایانه ای نیز نوعی خرابکاری رایانه ای بوده که هدف مجرم اخلال در امنیت اقتصادی، سیاسی و اجتماعی می باشد.

[2]-برآنیم تا این قسم از جرائم را که به علت ارتکاب از طریق کامپیوتر نوظهور می باشند را باعناصر اختصاصی مورد بررسی و مطالعه خویش قرار داده و جهت حمایت از اصول حاکم بر داده ها و سامانه ها و پیشگیری و حفاظت موثر توام با آموزش های لازم در استفاده از سامانه ها و برنامه های شخصی و حساس، پاسخ ها و واکنش مقنن در پرتوی ضمانت اجراهای کیفری و غیرکیفری در غالب سیاست جنایی مورد مداقه خویش واقع نماییم.

ب– فرضیات تحقیق

۱- به نظر می رسد که با عنایت به تنوع مصادیق و محدودیت شمول قانون مزبور به مبادلات تجاری جرم انگاری جرائم جدید دائما در حال وقوع باشد.

۲- به نظر می رسد سیاست جنایی از جرم انگاری این قسم از جرائم اهدافی از قبیل حمایت از داده ها و برنامه های رایانه ای در برابر آسیب های عمدی و پر کردن خلاء حقوق جزای سنتی نسبت به داده های الکترونیکی داشته باشد.

ج– پیشینه و سابقه تحقیق

مطالب متعدد و متنوعی در این خصوص وجود دارد که نگارنده از آنها استفاده کاملی نموده و اساس این تحقیق قطعا بر مبنای تحقیق پیشینیان بوده است لکن در خصوص عنوان خاص پایان نامه تحقیقات جامعی وجود نداشته است. صرفا برخی منابع از قبیل پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی با عنوان سیاست جنایی ایران در قلمرو کلاهبرداری رایانه ای در دانشکده حقوق دانشگاه آزاد مشهد نوشته آقای خالقی و برخی مقالات کوتاه به بررسی نمونه ای از مصادیق جرائم رایانه ای پرداخته و سایر منابع به برسی اجمالی و کلی جرائم رایانه ای اشاره دارد.

د– ضرورت تحقیق

امروزه ارتباطات و تعاملات افراد صرفا به دنیای واقعی محدود نمی گردد بلکه حجم گسترده ای از این روابط به فضای سایبر منتقل گردیده که تنظیم این روابط و انسجام بخشی به آن مقررات خاصی را می طلبد. فناوری اطلاعات در قلمرو حقوق کیفری تحولات عدیده ای را موجب گردیده است به گونه ای که امروزه رایانه و تجهیزات مرتبط امکان رفتارهای ضد اجتماعی بی شماری را پدید آورده، بخشی از این جرائم همان جرائم سنتی چون جعل است که در محیط رایانه و با استفاده از تکنولوژی رایانه ای نمود پیدا نموده است و بخشی دیگر رفتارهایی با ماهیت جدید بوده که بر اثر تکنولوژی نوپای رایانه ای پدید آمده و فرصت های قانونی را برای مجرمین فراهم نموده است.

این جرائم به لحاظ ویژگی های متمایز از جرائم سنتی خسارات هنگفتی را به جامعه وارد می آورد که در جهت حفظ و تداوم اعتماد مردم به جامعه مجازی و در جهت حفاظت از داده ها و اطلاعات علمی متخصصان رایانه ای از حملات مخرب مقنن ،دست به جرم انگاری زده است.نبود تحقیقی توصیفی و تحلیلی در این موضوع ضرورت انجام پژوهش های مرتبط با این حیطه را بیشتر کرده است.

ه– اهداف تحقیق

هدف تحقیق حاضر بررسی جرائم علیه صحت و تمامیت رایانه ای ، از قبیل جعل، تخریب، و اخلال در داده ها و برنامه های رایانه ای و قوانین مرتبط بوده تا با نشان دادن نواقص موجود و فهم مناسب از آن و ارائه راه حل کاربردی برای مشکلات موجود بتوان ارائه طریق نمود تا نسبت به شفاف سازی و یکسان سازی قوانین اقدام گردد.مضافا آنکه ارائه راهکارهای پیشگیرانه در جهت مقابله با این قسم از جرائم و تقویت قوانین و در صورت لزوم اصلاح آن از جمله دیگر اهداف این پژوهش است.

و– کاربرد های متصور از تحقیق

امید است این تحقیق برای قوه مقننه در وضع قوانین جامع وکامل و یا اصلاح و تکمیل قوانین موجود در خصوص کلیه ابعاد جرائم علیه صحت و تمامیت داده ها و برای قوه قضائیه در جهت توجه به مصادیق جدید این قسم از جرائم و ارائه لوایح برای کامل کردن قانون جرائم رایانه ای و برای استفاده قضات،وکلا و دانشکده های حقوق و همچنین برای استفاده ی پلیس مخصوص این جرائم راهگشا و موثر واقع گردد.

ز– روش تحقیق

روش تحقیق، توصیفی، مقایسه ای و تحلیلی بوده که با بهره مندی از منابع کتابخانه ای و اسنادی محقق بخش عمده ای از منابع مورد نیاز خود را از مطالعه کتب، مقالات و فیش برداری کسب نموده و به تجزیه تحلیل جرائم مورد بحث می پرداخته ، از طرف دیگر با بررسی اسناد موجود تک تک جرائم را در قوانین جاریه با عناصر اختصاصی آن مورد تجزیه و تحلیل خویش قرار می دهد.

ی– ساختار تحقیق

تحقیق حاضر در دو بخش مورد بررسی و مطالعه قرار خواهد گرفت بدین توضیح که در بحث نخست مرحله جرم انگاری به همراه تعاریف، سیر تاریخی و مصادیق جرائم به همراه عناصر آن مورد مطالعه واقع می شود و در بخش دوم نیز پاسخ ها اعم از پاسخ های کیفری، غیرکیفری به همراه کیفیات مشدده و مخففه مجازات ها و مراجع اعمال پاسخ مورد تجزیه و تحلیل واقع خواهند گشت.

بخش اول
فرآيند جرم انگاري

فصل اول؛بررسی مفاهیم اولیه

نوظهور بودن بزه‌های رایانه‌ای بدلیل نوین بودن بستر ارتکاب این جرائم وابسته به اجزای جدیدی است که شناخت اجزای سازنده این بستر و سایر موضوعات تخصصی داخل در حیطه حقوق کیفری اطلاعاتی امری ضروری جلوه می‌نماید. شناخت ارکان تشکیل دهنده بزه‌های رایانه‌ای من جمله بزه علیه صحت وتمامیت داده و سامانه و متعاقبا فهم بهتر این جرائم و تفسیر درست و منطقی از مواد قانونی مستلزم شناخت مفاهیم و واژگان متعددی است که بارها در مواد قانونی مورد بحث تکرار گردیده است. لذا برآنیم تا در این فصل مفاهیم و واژگان تخصصی داخل در این حوزه را مورد مطالعه خویش قرار دهیم.

مبحث اول؛ داده،قابلیت استناد و تمامیت داده پیام

داده در لغت به معنای اطلاعات، مفروضات، داشته‌ها و سوابق آمده است[۱].مطابق تعریف فرهنگ کامپیوتر مایکروسافت داده عبارت از فقره یا فقراتی از اطلاعات است و بنا به دانشنامه جهانی آکسفورد داده به اطلاعاتی اطلاق می‌شود که غالبا در قالب خاص و برای اهداف مشخص تهیه شده است[۲]. علیرغم اینکه داده در موارد متعدد و تحت عناوینی از قبیل حمایت از داده پیام، در قانون تجارت الکترونیک بکار رفته، لیکن این قانون تعریفی از آن ارائه نداده است.

گفتار اول؛ داده پیام،صحت و اصالت داده

با توجه به اینکه داده ها در واقع همان اطلاعات مورد نظر افراد می باشند لذا بحث صحت و اصالت داده ها نیز مهم و مقابل توجه می باشد که در دو بند این موضوع بررسی می گردد.

بند اول؛ داده[۳]، داده پیام[۴] و اطلاعات[۵]

در قانون جرائم رایانه‌ای داده دارای ارقام مختلفی از قبیل داده‌های رایانه‌ای و مخابراتی بکار برده شده است که در بخش جرائم علیه صحت و تمامیت داده و سامانه بدان اشاره گردیده است که عملا با درآمیختن سیستمهای مخابراتی و رایانه‌ای تفکیک میان آن دو میسر نمی‌باشد.

---

[۱]–موسسه لغت نامه دهخدا، لوح فشرده لغت نامه دهخدا، روایت سوم، تهران، موسسه انتشارات چاپ دانشگاه تهران، ۱۳۸۳،ص۱۲۵

[۲] – نوری، محمدعلی، نخجوانی، رضا، حقوق حمایت داده‌ها، تهران، انتشارات گنج دانش، چاپ اول سال ۸۲،ص۵۹

[۳] - Data

[۴] - Data Massage

[۵] - Information

کنوانسیون جرائم سایبر در بند ب ماده ۱ خود داده رایانه‌ای را بشرح ذیل تعریف نموده است :

« هر نوع ارائه وقایع، اطلاعات، حقایق یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است که شامل برنامه‌ای می‌شود که برای کارکرد یک سیستم رایانه‌ای مناسب است».

تعریف فوق از تعریف موسسه بین‌المللی استاندارد از داده‌ها اقتباس شده است. این تعریف حاوی عبارت مناسب برای پردازش است یعنی داده‌ها به شکلی وارد شوند که بتوان آنها را مستقیما بوسیله سیستم رایانه‌ای پردازش نمود[۱].

در پیش‌نویس لایحه جرائم رایانه‌ای که در جلسه مورخ ۸۷/۵/۷ با حضور کارشناسان ذیربط مطرح گردید و مورد تصویب قرار گرفت تعریف مزبور در بند ج ماده اول پیش‌نویس لایحه با اندکی تغییر به شرح ذیل بیان گردیده است:

«داده رایانه‌ای هرنمادی از واقعه، اطلاعات یا مفهوم به شکل مطلوب برای پردازش در یک سیستم رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا گذارند».

مرکز پژوهش‌های مجلس با این توجیه که با توجه به پیشرفت فن‌آوری تعاریف قابلیت خود را از دست داده و باعث تفاسیر قضایی متعددی می گردد پیشنهاد حذف ماده ۱ لایحه جرائم رایانه‌ای را در قالب تعاریف ارائه نموده که نهایتا بخش کلیات در تصمیم نهایی این لایحه حذف گردید. در اظهار نظر کارشناسی صورت پذیرفته آمده است فارغ از اینکه بکار بردن لفظ عام کلیات در مورد تعاریف بدون ذکر مقرره دیگر که عمومات و کلیات لایحه را بیان کند، نامناسب بود. در این قسمت از لایحه که شامل یک ماده و مشتمل بر ۱۳ تعریف از واژگان می‌باشد حذف گردیده و بخش نخست جایگزین آن شده است. وفق نظر کارشناسان چون کلیه واژگان دارای جنبه فنی بوده و بطور کامل نمی‌توان از آنها تعریف ارائه نمود زیرا با توجه به توسعه فضای سایبر واژگان فنی داخل در این حوزه نیز در حال تغییر و تحول می‌باشد[۲]..

هر چند عدم ارائه تعریف از واژگان مزبور این حسن را داردکه مقنن بدون محدود کردن اصطلاحات در قالب الفاظ مبهم که تفاسیر متعددی را توسط قضات در برداشته باشد قاضی را با ارجاع امر به کارشناسی یاری خواهد کرد تا تعریف اصطلاحات را درک نماید اما از دیگر سو، حقوقدانان و قضات ناآشنا به مبانی علم کامپیوتر را در فهم بهتر مواد قانونی و عناصر مجرمانه جرائم داخل در حیطه فن‌آوری اطلاعات با مشکل مواجه می‌سازد، چرا که در وهله اول قاضی تحقیق در دادسرا می‌بایست

---

[۱]- جلال فراهانی،امیرحسین،کنوانسیون جرائم سایبر و پروتوکل الحاق آن،معاونت حقوقی و توسعه قضایی قوه قضائیه،تهران،نشر خرسندی،۱۳۸۸،ص ۲۰

[۲]-مجلس شورای اسلامی، مرکز پژوهش‌ها، اظهار نظر کارشناسی درباره لایحه جرائم رایانه‌ای، کد موضوعی ۲۰۰، شماره مسلسل ۷۵۵۲، آبانماه ۸۴،ص۳