فصلنامه بین المللی قانون یار

License Number: 78864 Article Cod:Y5SH19A61115 ISSN-P: 2538-3701

عکس العمل های قانونی نسبت به جرائم رایانه ای در حقوق موضوعه

(تاریخ دریافت ۱۴۰۰/۰۴/۱۵، تاریخ تصویب ۱۴۰۰/۰۹/۱۸)

سارا داودی زاده جلگه

چکیده

امروزه با پیشرفت تکنولوژی و گسترش فضای مجازی شکل و ابزار ارتکاب جرم نیز تغییر کرده است. از سوی دیگر، نمی توان تاثیر استفاده از اینترنت و وسایل الکترونیکی از جمله رایانه و موبایل بر زندگی افراد را نادیده گرفت، به همین دلیل در سال های اخیر جرایم رایانه ای به مراتب افزایش پیدا کرده است. از این رو قانون گذار به منظور جلوگیری از ایجاد اختلال در این فضا، قوانینی را در این زمینه وضع کرده است. امروزه نمی توان تاثیر استفاده از اینترنت و وسایل الکترونیکی از جمله کامپیوتر ها و موبایل ها بر زندگی افراد نادیده گرفت. حضور افراد در فضای مجازی، ایجاد کسب و کار در این فضا، شکل گیری روابط اجتماعی در آن و همچنین انجام معاملات تجاری از طریق آن باعث شده است این فضا به عنوان یک محیط مجازی درآید که برخی از افراد از آن سود جویی می کنند. از این رو قانون گذار برای جلوگیری از ایجاد اختلال در این فضا و مشخص کردن قواعد استفاده کنندگان، قوانینی را در این زمینه وضع کرده است. در ایران سابقه جرم رایانه ای به جعل اسکناس توسط یک کارگر چاپخانه و یک دانشجو در سال ۱۳۷۸ بر می گردد. جرم رایانه ای نظیر جاسوسی رایانه ای و مجازات آن یعنی جرمی که با استفاده از فناری کامپیوتری رخ دهد. یعنی کسی با استفاده از کامپیوتر اقدام به انجام اعمال مجرمانه ای مانند بدست آوردن اطلاعات شخصی دیگران کند. در این مقاله قصد داریم به بررسی و شناخت عکس العمل های قانونی نسبت به جرائم رایانه ای در حقوق موضوعه بپردازیم و در این راستا خلاء تحقیقاتی موجود را رفع نماییم.

واژگان کلیدی: جرایم رایانه ای، فضای مجازی، داده های اینترنتی، رایانه، سایبر، حامل‌های داده

بخش اول: کلیات

در این بخش به تعریف و شناسایی برخی واژه های کلیدی مرتبط با جرایم رایانه ای می پردازیم.

بند اول: فضای سایبر[۱]

سایبر در فرهنگ های مختلف، از لحاظ لغوی به معنای مجازی و غیر ملموس است و در برخی فرهنگ های کامپیوتری به یک گروه کامپیوترهای بسیار بزرگ یا ابر کامپیوتر اطلاق شده است. اما واژه «سایبر »از لغت یونانی «kybernetes »به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضی دانی به نام نوربرت وینر[۲] درکتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم های انسانی، ماشینی (کامپیوترها) است. سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است بطورمثال شهروند سایبر[۳]. البته لازم به ذکر است ترجمه های فارسی از لفظ سایبر دقیق نیست هر چند بعضاً لفظ مجازی به عنوان معادل آن گرفته می شود اما چون سایبر بیانی است از موضوعات واقعی قابل مشاهده و لیکن غیر قابل لمس است نمی تواند بر لفظ مجاز که به موضوعات ذهنی و تصوری اشاره دارد، حمل شود. اما واژه فضای سایبر را نخستین بار ویلیام گیبسون [۴] نویسنده داستان علمی تخیلی در کتاب نورومنسر[۵] در سال ۱۹۸۴ بکار برده است. فضای سایبر در معنا به مجموعه ای از ارتباطات درونی انسانها از طریق کامپیوتر و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل[۱] با یکدیگر ارتباط بر قرار کنند. بر خلاف فضای واقعی، در فضای سایبری نیاز به جابجایی های فیزیکی نیست و

---

۱. cyber space

۲. norber wiener

۳. cybercitizen

۴.willian Gibson

۵. nwuromancer

۱. e-mail

کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس[۱] [۲] صورت می گیرد. همچنین باید گفته شود از حیث اصطلاحی فضای سایبر به گونه ای است که با جهان کنونی برابری می کند و به عنوان دنیای جدید معرفی می شود بنابراین دارای تعاریف فراوانی است. در مورد فضای سایبر تعاریف مختلفی صورت گرفته که هر یک از منظر خاصی به این اصطلاح نگریسته است در مجموع می توان گفت تعاریف ارائه شده یا متضمن این هستند که فضای سایبر در اصل جهان سایبر است که در عرض جهان فیزیکی مطرح شده است آن را همچون منبعی برای تبادل اطلاعات دانسته اند و یا اینکه فضای سایبر را با دید سخت افزارانه نگریسته و آن را تشکیل یافته از اتصال بیشماری از رایانه ها و سامانه ها می دانند.[۳]

بند دوم: اینترنت[۴] [۵]

اینترنت مجموعه ای از شبکه های کامپیوتری بزرگ و کوچک است. شبکه های مورد ذکر با روش های متفاوتی به یکدیگر متصل و موجودیت واحدی با نام « اینترنت» را به وجود آورده اند. نام در نظر گرفته شده برای شبکه های فوق از ترکیب واژه های [۶] (Inter connected) و (Net work)[۷] انتخاب شده است. لازم به ذکراست، اینترنت کار خود را از سال ۱۹۶۹ و با چهار دستگاه کامپیوتر میزبان[۸] آغاز و پس از رشد باور نکردنی خود، تعداد کامپیوترهای میزبان در شبکه به بیش از ده ها میلیون دستگاه رسیده است. اینترنت به هیچ سازمان و یا مؤسسه خاصی در جهان تعلق ندارد. عدم تعلق اینترنت به یک سازمان و یا مؤسسه بمنزله عدم وجود سازمانها و انجمن های مربوط برای استاندارد سازی نیست. یکی از این نوع انجمن ها « انجمن اینترنت» است که در سال ۱۹۹۲ با هدف تبیین سیاست ها و پروتکل های مورد نظر جهت اتصال به شبکه تاسیس شده است.

---

۱. Mouse

۲. موشواره

۳. http://www.rider.edu/suler/spycyber

۴. Internet

۵. جعفری، فرهاد، فرهنگ کامپیوتر، نشر تلاش، ۱۳۸۲، ص ۸۷

۶. ارتباط برقرار کردن

۷. شبکه ارتباطی

۸. host

بند سوم: رایانه[۱]

رایانه یا کامپیوتر[۲] ماشینی است که از آن برای پردازش اطلاعات استفاده می شود بر اساس «واژه نامه ریشه یابی»[۳] واژه کامپیوتر در سال ۱۶۴۶ به زبان انگلیسی وارد گردید که به معنی «شخصی که محاسبه می کند» بوده است و سپس از سال ۱۸۹۷ به ماشینی های محاسبه مکانیکی گفته می شد. در هنگام جنگ جهانی دوم «کامپیوتر» به زنان نظامی آمریکایی و انگلیسی که کارشان محاسبه مسیرهای شلیک توپ های بزرگ جنگی توسط ابزار مشابهی بوده گفته می شد. در اوایل دهه ۵۰ میلادی هنوز اصطلاح «ماشین حساب»[۴] برای معرفی این ماشین ها به کار می رفت. پس از آن عبارت کوتاهتر کامپیوتر به جای آن به کار برده شد. ورود این ماشین به ایران در اوایل دهه ۱۳۴۰ بود و در فارسی از آن زمان به آن«کامپیوتر» می گفتند واژه رایانه، در دو دهه اخیر در فارسی رایج شده و به تدریج جای «کامپیوتر» را گرفت.

بند چهارم: داده های سری

بر اساس تعاریف موجود در منابع می توان «داده»[۵]را چنین تعریف نمود. داده ها گروهی از نمادها، کلمات، اعداد، نمودارها و حقایق گسسته و بی مفهومی هستند که رخدادها را نشان می دهند.داده ها حقایقی هستند که از طریق مشاهده و تحقیق به دست می آیند. موارد خامی که هنوز پردازش نشده اند، مانند تاریخ و مقدار یک صورتحساب.

بند پنجم: حامل های داده

حامل های داده عبارتند از مجموعه ای گوناگون از وسایل ذخیره سازی اطلاعات که قابل حملند و می توان به سادگی آنها را از یک رایانه به رایانه دیگر منتقل کرد مانند دیسک نرم[۱]، دیسک سخت[۱]،

---

۱. جعفری، فرهاد، همان، ص ۳۹.

۲.computer

۳.barnhart concise

۴. computing machines

۵.Data

۱.Floppy Disk

لوح فشرده [۲]، نوار مغناطیسی [۳]، دیسک ویدئویی دیجیتال [۴]، حافظه فلش [۵]، این حامل ها هر یک ظرفیت های متعددی برای ذخیره سازی اطلاعات دارند که برای سنجش این ظرفیت معمولاً از اصطلاحاتی نظیر مگابایت [۶] یا گیگا بایت [۷] استفاده می شود که هر قدر بالاتر باشد اطلاعات بیشتری را می توان ذخیره کرد.

بند ششم: سیستم های رایانه ای و مخابراتی [۸]

سیستم های رایانه ای شامل هر نوع دستگاه یا مجموعه ای از دستگاه های متصل سخت افزاری، نرم افزاری است که از طریق اجرای برنامه های پردازش خودکار داده، عمل می کند. سیستم های مخابراتی شامل هر نوع دستگاه با مجموعه ای از دستگاه ها برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکار ساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قرار دادهایی که برای گیرنده قابل فهم و تفسیر باشد.

بند هفتم: جرم رایانه ای

جرم رایانه ای بر۲ نوع است: در تعریف محدود (مضیق) جرمی که در فضای مجازی رخ می دهد، جرم رایانه ای است و بر اساس این دیدگاه، اگر رایانه ابزار و وسیله ارتکاب جرم باشد آن جرم را می توان در زمره جرایم رایانه ای قلمداد کرد.در تعریف گسترده (موسع) هر فعل یا ترک فعلی که «در» یا «از طریق» یا «به کمک سیستم های رایانه ای» رخ می دهند جرم رایانه ای قلمداد می شود. از این دیدگاه جرایم به ۳ دسته تقسیم می شوند:

---

۱. hard Disk

۲.compact Disk

۳. Magnetic Tape

۴. Digital Video Disk (DVD)

۵. Flash memory

۶. Megabyte

۷. Gigabyte

۸. همان، ص ۱۲۸.

۱- رایانه موضوع جرم: در این دسته از جرائم رایانه و تجهیزات رایانه ای، موضوع جرائم سنتی (کلاسیک) مثل سرقت، تخریب، تجهیزات و.... می شوند.

۲- رایانه واسطه جرم: رایانه وسیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک و... استفاده می شود.

۳- جرائم محض رایانه ای: دسته سوم جرایم محض جرائمی مثل هک یا ویروسی کردن که صرفاً در فضای سایبر اتفاق می افتد.

در کنفرانس بین الملل بوداسپت(۲۰۰۱) چیزی تحت عنوان جرم رایانه ای مطرح نشده بلکه در فضای مجازی از جرم سایبری[۱] نام برده شده که در فارسی به جرم مجازی تعبیر می شود. در اسناد و کنوانسیون های بین المللی پیرامون جرائم رایانه ای رویکرد دوگانه ای وجود دارد. به این معنا که هم ارتکاب جرایم رایانه ای محض مثل هک کردن و هم ارتکاب برخی جرایم مانند جرائم سنتی با استفاده از سیستم های رایانه ای مانند نقض حقوق مالکیت معنوی جرم انگاری شده است[۲].با توجه به تعاریف بیان شده به نظر نگارنده بجاست در متن اصلی قانون جرائم رایانه ای برخی ازاین اصطلاحات برای روشن تر شدن نص قانون و جلوگیری از ابهامات بطور صریح و آشکار تعریف بشود.

بخش دوم: بررسی ابعاد حقوقی عکس العمل های قانونی درخصوص جرائم رایانه ای

قبل از دهه ۱۹۷۰ کشورها در چهارچوب قوانین سنتی با جرائم رایانه ای برخورد می کردند اما با پیشرفت فن آوری اطلاعات و تنوع و کثرت سوء استفاده هایی که از این فناوری می شد، حقوق جزای سنتی دیگر جوابگوی کافی نبود.از این رو کشورها سعی کردند با توجه خاص به این گونه جرائم نو ظهور راهکارهایی را برای کنترل جرائم مرتبط با فن آوری اطلاعات ارائه دهند.

بند اول: واکنش قانونگذار ایران به جرائم رایانه ای

---

۱. cyber crime

۲. اسماعیل بیگی، مهر، جرائم کامپیوتری، ۱۳۸۹.

از آنجا که جرم رایانه ای مرتبط با ورود کامپیوتر است ابتدا مختصری در خصوص ورود رایانه به ایران صحبت می کنیم.رایانه که از اوایل سال ۱۳۴۰ وارد ایران شده بود فقط از سوی نهادهای دولتی خاص مورد استقبال قرار گرفت تا سال ۱۳۴۵ جمعاً ۹ رایانه در ایران وجود داشت. اما در سال ۱۳۴۹ این تعداد به ۷۸ دستگاه رسید که اغلب این رایانه ها اجاره ای بودند در سال ۱۳۵۶ تعداد رایانه های نصب شده به ۶۱۶ دستگاه رسید.بعد از انقلاب نهادهایی برای امور انفورماتیک ایجاد شد که با فعالیت این نهادها رشد فناوری در سالهای اخیر نسبتاً خوب بوده است. در حال حاضر تمام سازمانها و نهادها برای انجام امور خود از رایانه استفاده می کند. اما در خصوص واکنش های تقنینی در خصوص جرائم رایانه ای می توان قانون حمایت از مؤلفان مصوب ۱۳۴۸ را اولین واکنش تقنینی ایران در این زمینه دانست و دومین واکنش «قانون ترجمه یا تکثیر کتب و نشریات و آثار صوتی» مصوب ۱۳۵۲ می باشد.

ماده ۲۳ قانون حمایت از مؤلفان: «هر کس تمام یا قسمتی از اثر دیگران که مورد حمایت این قانون است به نام خود یا به نام پدید آورنده بدون اجازه او و یا عالماً به نام شخص دیگری غیر از پدید آورنده نشر یا پخش یا عرضه کند به حبس تأدیبی از ۶ تا ۳ سال محکوم خواهد شد».

ماده ۳ قانون ترجمه یا تکثیر کتب و نشریات و آثار صوتی: «نسخه برداری یا ضبط یا تکثیر آثار صوتی که بر روی صفحه یا نوار یا هر وسیله دیگر ضبط شده است بدون اجازه صاحبان حق یا تولید کنندگان انحصاری یا قائم مقام قانونی آن ها برای فروش ممنوع است. حکم مذکور در این ماده شامل نسخه برداری یا ضبط یا تکثیر از برنامه رادیو تلویزیون یا هر گونه پخش دیگر نیز خواهند بود». از اواسط دهه ۱۳۷۰ به ویژه ابتدای دهه ۱۳۸۰ که استفاده از رایانه های شخصی توسط افراد حقیقی و حقوقی گسترش یافت ارتکاب جرائم رایانه ای هم رشد نسبتاً سریعی داشت. از آنجا که پس از همگانی شدن استفاده از اینترنت زمینه جرائمی که جنبه اخلاقی داشت رونق بیشتری یافت و از این طریق نظم و عفت عمومی به خطر افتاد، قانونگذار در سال ۱۳۷۹ در برابر برخی جرائم واکنش نشان داد و با الحاق تبصره سوم به ماده اول قانون مطبوعات مقرر داشت: «کلیه نشریات الکترونیکی مشمول مواد این قانون است». چهارمین واکنش قانونگذار ما «قانون حمایت از پدید آروندگان نرم افزارهای رایانه ای» مصوب ۱۳۷۹ می باشد که در ماده سیزدهم قانون مذکور نقض حقوق پدید آورندگان نرم افزارهای رایانه ای مورد حمایت این قانون جرم تلقی شده است. موارد نقض حقوق مورد حمایت این قانون ممکن است به شکل استفاده غیر مجاز، کپی برداری غیر مجاز، تکثیر یا توزیع و یا هر عملی باشد که منجر به تعرض

به حقوق مادی و معنوی پدید آورندگان این آثار می شود. در سال ۱۳۸۲ واکنش دیگری از سوی قانونگذار در مقابل جرائم رایانه ای با تصویب قانون مجازات نیروهای مسلح انجام گرفت. به موجب ماده ۱۳۱ قانون مجازات نیروهای مسلح، جعل اطلاعات و داده های رایانه ای، تسلیم و افشای غیر مجاز اطلاعات و داده ها به افرادی که صلاحیت دسترسی به آن را ندارند، (جاسوسی رایانه ای) سرقت و یا تخریب حامل های داده و سوء استفاده مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می شود. ششمین واکنش قانونی مرتبط با جرائم رایانه ای از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ توسط مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۶۶ تا ۶۹ و ۷۴ تا ۷۷ این قانون کلاهبرداری، جعل و دستیابی و افشای غیر مجاز اسرار تجاری نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و غیره که از طریق رایانه در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین گردیده است. بعد از تصویب قانون تجارت الکترونیکی باز هم برای مقابله با سایر سوء استفاده های رایانه ای مانند سوء استفاده از رایانه به منظور نفوذ به حریم خصوصی افراد، تخریب، سرقت، توقف و تغییر داده هایی که فاقد شرایط مقرر در قانون حمایت از پدید آورندگان نرم افزارهای رایانه ای هستند، استفاده های مالی رایانه ای خارج از بستر تجارت الکترونیک و سایر جرائم نیاز به یک قانون پیشرفته و جامع احساس می شد. بنابراین شورای عالی و توسعه قضائی قوه قضائیه پیش نویس قانون جرائم رایانه ای و آئین دادرسی آن را در سال ۱۳۸۲ تهیه و طی جلساتی متعدد از دی ماه تا اوایل خرداد ماه با حضور حقوقدانان و متخصصان امور رایانه ای آن را بررسی کردند تا پس از تصویب رئیس قوه قضائیه به عنوان لایحه جرائم رایانه ای از طریق هیئت دولت به مجلس شورای اسلامی تقدیم شود[۱].

بند دوم: چالشهای تصویب قانون جرائم رایانه ای با تأکید بر جرم جاسوسی رایانه‌ای

در تیرماه ۱۳۸۴ لایحه جرائم رایانه ای به شرح زیر تقدیم مجلس شورای اسلامی شد:

بخش اول (ماده ۱) کلیات

بخش دوم (ماده ۲ تا ۱۹) جرائم و مجازات ها

---

[۱]. باستانی، برومند، جرائم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، نشر بهنامی، ۱۳۹۰، ص ۱۲۱

بخش سوم (مواد ۲۰ تا ۳۸) آئین دادرسی جرائم رایانه ای

بخش چهارم(ماده ۳۹) همکاری های بین المللی

بخش پنجم (مواد ۴۰ تا ۴۲) سایر مقررات

در ماده ۴ لایحه فوق الذکر تحت عنوان جرائم علیه امنیت مقرر شده بود:

«هر کس بطور عمدی و بدون مجوز مرجع قانونی به داده های رایانه ای به کلی سری و سری موجود در سیستم های رایانه ای یا مخابراتی یا حامل های داده دسترسی یابد یا داده های رایانه ای به کلی سری و سری در حال انتقال را شنود یا دریافت کند به جزای نقدی از ده میلیون ریال تا یک میلیاد ریال متناسب با جرم اتفاق افتاده محکوم خواهد شد». از آنجا که این لایحه با هدف حبس زدایی تنظیم شده بود، برای جرمی مانند جاسوسی رایانه ای نیز مجازات نقدی تعیین و مقرر گردیده بود. این امر نقدی بر لایحه مزبور است، زیرا ماهیت جرمی نظیر جاسوسی و خسارت ناشی از آن، چه در محیط معمولی و چه فضای رایانه ای و سایبر با اندکی دقت از یک درجه اهمیت برخوردار است. درنتیجه تعیین مجازات نقدی نه تنها اهمیت آن را می کاهد، بلکه تناسبی با مجازاتهای مقرر قانون مجازات اسلامی و قانون مجازات جرایم نیروهای مسلح نیز ندارد. با وجود اشکال فوق، عیناً در جلسه مورخ ۸۷/۵/۷ کمیسیون قضائی و حقوقی مجلس با حضور کارشناسان ذیربط تصویب و به همراه سایر مواد، گزارش شور اول آن به مجلس ارسال شد. نتایج شور دوم این لایحه درتاریخ ۸۷/۹/۲۶ به مجلس ارائه شد که طی آن ماده ۴ لایحه دولت مورد اصلاحات عمده ای قرار گرفت، به نحوی که ایرادات مذکور بر طرف و سه ماده (مواد ۳، ۴، ۵) تحت عنوان جاسوسی رایانه ای جایگزین ماده قبلی شد. لایحه مذکور در تاریخ ۸۷/۱۰/۱۵ در مجلس به تصویب رسید و در مورخ ۸۷/۱۲/۵ در اجرای اصل ۹۴ قانون اساسی به شورای نگهبان ارسال شد. شورای نگهبان در مجلس مورخ ۸۷/۱۲/۲۱، لایحه را بررسی کرده و در تاریخ ۸۷/۱۲/۲۶ مواد خلاف شرع و خلاف قانون اساسی را به مجلس اعلام کرده و گفتنی است شورای نگهبان هیچ ایرادی را نسبت به نقایص مواد مربوط به جاسوسی رایانه ای ابراز نکرد. از جمله این ایرادات می توان به این نکته اشاره کرد که، در مقدمه ماده ۳ که جایگزین ماده قبلی شد اصطلاحاتی وجود دارد که تعریفی از آنها به عمل نیامده است. اصطلاحاتی مانند، داده، سامانه های رایانه ای و مخابراتی که شایسته بود با توجه به ورود این مفاهیم برای نخستین بار به ادبیات

حقوق کیفری، تعریف جامع و مانعی از آنها ارائه می شد. البته در لایحه تقدیمی دولت برخی از این اصطلاحات تعریف شده بود اما به دلایل نامعلومی در مجلس حذف شد. ایرادات وارد شده از سوی شورای نگهبان از سوی مجلس بر طرف و در جلسه علنی مورخ ۸۸/۱/۳۰ به تصویب رسیده و در تاریخ ۸۸/۲/۲ به شورا ارسال شد. شورای نگهبان در جلسه ۸۸/۲/۱۶ مجداً ایراداتی را به لایحه وارد دانسته و در مورخ ۸۸/۲/۱۹ نظریه خود را به مجلس ارسال کرد. مجلس پس از رفع موارد مغایرت، لایحه را در جلسه علنی مورخ ۸۸/۳/۵ به تصویب رساند و برای تأیید نهایی در تاریخ ۸۸/۳/۱۰ به شورا ارسال کرد، و در نهایت شورای محترم نگهبان در جلسه ۸۸/۳/۲۰ با توجه به اصلاحات به عمل آمده، لایحه مزبور را مغایر با موازین شرعی و قانون اساسی نشناخته در همان تاریخ به مجلس اعلام کرد. دولت محترم جمهوری اسلامی ایران نیز قانون مزبور را در تاریخ ۸۸/۴/۱۰ برای اجرا به وزارت دادگستری ابلاغ کرد. قانون جرائم رایانه ای را می توان آخرین واکنش تقنینی قانونگذار کشورمان در خصوص جرائم رایانه ای تا به حال اعلام کرد.[۱]

بخش سوم: تحولات تقنینی کشورها در جرائم رایانه ای

همانطور که می دانیم قبل از دهه ۱۹۷۰ به علت خلاء قانون مرتبط با جرائم رایانه ای، قوانین کلاسیک مستمسکی برای برخورد با این گونه جرائم بودند، اما پیشرفت فن آوری اطلاعات و تنوع و کثرت جرائمی که با استفاده از این فن آوری به عمل می آمد حقوق جزای کلاسیک را به چالش کشید. علت این چالش ها این بود که قوانین کشورها تا قبل از شروع جرائم رایانه ای غالباً به حمایت از اهداف و موضوعات مملوس می پرداختند اما اطلاعات رایانه ای یک موضوع غیر مملوس هستند. حقوق جزای ماهوی که حمایت از ارزش ها را به عهده دارد، در برابر تجاوز و تعدی به این ارزشها با نگرشی جدید واکنش نشان داد. این نگرش طی مراحلی موجب اصلاح سیستم های قضایی گردید[۱]. از دهه ۷۰ میلادی به بعد به صورت ۵ مرحله این اصلاحات را می توان مشاهده کرد.

---

[۱]. عالی پور حسن، حقوق کیفری فناوری اطلاعات، نشر خرسندی، ۱۳۹۰، ص ۳۸۰-۳۶۸.

[۱]. خرم آبادی، عبدالصمد، تاریخچه و تعریف و طبقه بندی جرایم رایانه ای، مجموعه مقالات همایش بررسی ابعاد حقوقی فن آوری اطلاعات، انتشارات سلسبیل، تهران، ۱۳۸۲، ص ۱۹

مرحله اول: حمایت از اطلاعات خصوصی بود که در دهه های ۱۹۷۰ و ۱۹۸۰ به علت مشکلات ناشی از حفاظت اطلاعات خصوصی آغاز شد. این تقنین واکنشی در برابر چالشهای جدید مربوط به حقوق فردی و خصوصی بود که به واسطه امکانات جمع آوری، ذخیره سازی و انتقال دادهها از طریق تکنولوژی های جدید با مسائل جدید مواجه شده بود. در این مرحله کشورهای مختلفی قوانینی را در راستای حمایت از داده ها، در حمایت از حقوق خصوصی و فردی شهروندان از جنبه اداری، مدنی، و کیفری تصویب کردند. از جمله کانادا و استرالیا در ۱۹۷۲، سوئد در ۱۹۷۳، آمریکا در ۱۹۷۴، آلمان در ۱۹۷۷، بریتانیا در ۱۹۸۴، لوگز امبورگ در ۱۹۷۹، ایسلند در ۱۹۸۱، اتریش، دانمارک و فرانسه و نروژ ۱۹۷۸، ایرلند، ژاپن و هلند در ۱۹۸۸ قوانینی را در این راستا تصویب کردند. مرحله بعدی ایجاد و اصلاح قوانین ناظر به جرائم رایانه ای در دهه ۱۹۸۰ بود. در این مرحله حقوق جزا با اشیا و موضوعات ناملموس مانند برنامه ریزی رایانه ای و طرق جدید ارتکاب مانند سوء استفاده از کامپیوتر به جای سرقت از شخص و روشهای جدید دستکاری مواجه شد. این قوانین جدید ناظر به جرائم اقتصادی کامپیوتری در کشورهای مختلف بدینگونه تصویب شده اند که برخی از این قوانین تاکنون چندین بار اصلاح شده اند. آمریکا از سال ۱۹۷۶ (در سطح ایالتی)، ایتالیا ۱۹۸۷، استرالیا ۱۹۷۹، بریتانیا ۱۹۸۱، ایالات متحده آمریکا از سال ۱۹۸۴، (در سطح فدرال)، دانمارک و کانادا ۱۹۸۵، آلمان ۱۹۸۶، سوئد و شیلی ۱۹۸۷، اتریش ژاپن و نروژ ۱۹۸۷، فرانسه و یونان ۱۹۸۸، فنلاند و بریتانیا ۱۹۹۰. مرحله سوم وضع قوانینی در جهت حمایت از مالکیت معنوی بود. بعد از اینکه برنامه های کامپیوتری در دهه ۱۹۷۰ از شمول حق اختراع و امتیاز ثبت خارج شد قوانین اصلاحی بطور صریح حمایت کپی رایت از برنامه های کامپیوتری را در دهه ۱۹۸۰ مقرر کردند و آنها تحت سیطره فراتر از حقوق کیفری قرار گرفتند و در سال ۱۹۸۴ حمایت از محصولات رسانه ای از اقدامات این مرحله بود. قوانین تصویب شده در کشورها بدین شرح است:

۱۹۷۲ در فیلیپین، ۱۹۸۰ در ایالت متحده آمریکا، ۱۹۸۳ در مجارستان، ۱۹۸۴ در استرالیا، هند و مکزیک، ۱۹۸۵ در شیلی، آلمان فدرال، فرانسه، ژاپن و بریتانیای کبیر، ۱۹۸۷ در برزیل، کانادا و اسپانیا، ۱۹۸۸ در کانادا و دانمارک ؛ ۱۹۸۹ در کلمبیا و سوئد، ۱۹۹۰ در نروژ و ۱۹۹۱ در فنلاند. مرحله چهارم اقداماتی در زمینه آئین دادرسی بود. این قوانین در زمینه بازرسی محیط های داده پردازی، تکوین دکترین های جدید مسئولیت کیفری، پیدایش و تکوین مقررات ناظر به جرایم رایانه ای،

تصویب کنوانسیون اروپایی و مطالعاتی در مورد طرح سازمان ملل (کنوانسیون مبارزه با سایبر کرایم) می باشد. در این خصوص می توان به تدوین قوانین انگلیس ۱۹۸۴، دانمارک ۱۹۸۵، آمریکا ۱۹۸۶، هلند ۱۹۹۲، اشاره نمود[۱،۲]. مرحله آخر اصلاح قوانین در مورد جرائم مربوط به محتواست. در این مرحله بسیاری از کشورها قوانینی وضع کردند که تهیه و توزیع، عرضه و نگهداری پورنوگرافی (هرزه نگاری) کودکان از طریق سیستم ها و شبکه های رایانه ای را جرم تلقی می کرد. در سال ۲۰۰۰ مؤسسه بین المللی مک کانل[۳] مطالعه ای در مورد وضعیت قوانین وضع شده در باره جرائم رایانه ای در چهار گوشه جهان به عمل آورد بر اساس این مطالعه، از کشورها خواسته شد چنانچه قوانین و یا پیش نویس قوانینی در این خصوص دارند، ارسال و در غیر این صورت اعلام کنند که هیچ اقدام مثبتی انجام نداده اند. مشخص شد بیش از ۵۰ کشور با ارسال تازه ترین اقدامات خود در این زمینه به استعلام مؤسسه بین المللی «مک کانل» پاسخ دادند. کشور ایران جز این ۵۰ کشور بود. پس از بررسی های به عمل آمده مشخص شد ۳۳ کشور از بین ۵۰ کشور تا کنون نسبت به روز آمد کردن قوانین خود در برخورد با انواع جرائم رایانه ای هیچ اقدامی انجام نداده اند با وجود این، بیشتر آن کشورها در حال تهیه پیش نویس قوانین بودند که از آن جمله می توان از ایران، آلبانی، بلغارستان، بورندی، کوبا، دو مینیکن، مصر، اتیوپی، فیجی، مجارستان، اردن، رومانی، زیمباوه، ویتنام، یوگسلاوی و لبنان نام برد.

از باقی کشورها، ده کشور برای برخورد با حداکثر پنج جرم کامپیوتری قانون وضع کرده اند که عبارتند از: برزیل، کانادا، شیلی، چین، چک، دانمارک، مالزی، لهستان، اسپانیا و فرانسه.

نه کشور آمریکا، انگلیس، استرالیا، پرو، ژاپن، موریس، استونی و هند نیز قوانین خود را برای برخورد با حداقل شش نوع از ده جرم کامپیوتری مورد نظر روزآمد ساخته بودند.از میان این کشورها تنها

---

[۱]. زیبر، اولریش، پیدایش حقوق اطلاعاتی کیفری ۱۹۹۲ – ترجمه محمد حسن ذریانی سازمان برنامه و بودجه کشور ۱۳۷۶، ص۲۹

[۲]. ابراهیم حسن بیگی، حقوق و امنیت فضای سایبر نشر ابرار، تهران ۱۳۸۴ -۱۸۹-۱۸۸ و عبدالصمد خرم آبادی، همان ص ۱۹-۲۰ و برومند باستانی همان ص ۱۰۵-۱۰۷

[۳].MC’ Connell

فیلپین نشان داده بود که قوانین خود را به منظور تعقیب آتی مرتکبان هر ۱۰ نوع جرم کامپیوتری ذکر شده روزآمد کرده است.[۱]

بخش چهارم: فعالیتهای بین المللی در خصوص جرائم رایانه ای

همانگونه که میدانیم مباحث جرائم رایانه ای بسیار متنوع است و موضوعاتی خاص را در بر می گیرد. کشورهای مختلف نیز درهمین ارتباط بنابر ارزش های اخلاقی خود سعی کرده اند ترکیبی از فاکتورهای تکنیکی و حقوقی را مد نظر قرار بدهند. آخرین و مهمترین گردهمایی بین المللی و مصوبه راجع به این گونه جرائم به کنفرانس بوداپست در اواخر سال ۲۰۰۱ میلادی بر میگردد. که درآن بیشتر کشورهای اروپایی همراه کانادا، ژاپن، آفریقای جنوبی و آمریکا مصوبه ای به نام «کنوانسیون جرائم سایبر» امضاء کردند. در مجموع بیش از ۳۲ کشور بر این مصوبات صحه گذاشتند اما روسیه، اسلواکی، ترکیه، لیتوانی، لوکز امبورگ، چک، دانمارک، و بوسنی هنوز بدان نپیوسته اند. همچنین سازمانهای بین المللی و منطقه ای از جمله سازمان ملل[۲]، شورای اروپا[۳]، سازمان همکاری توسعه اقتصادی[۴]، و انجمن بین المللی حقوق و جزا[۵] گامهای بزرگی را در قالب توصیه نامه ها، پیشنهادات، و ارائه همکارها، برای تدوین قوانین مرتبط با جرائم کامپیوتری برای کشورهای عضو برداشته اند که به عنوان نمونه می توان به موافقتنامه جرایم کامپیوتری شورای اروپا در تقسیم بندی، تعریف و شناسایی جرایم کامپیوتری در سال ۲۰۰۱، اشاره نمود و یا انجمن بین المللی حقوق کیفری در گردهمایی خود در سال ۱۹۹۲ در ورستبورگ به کشورها توصیه نمود تا در هنگام اصلاح قوانین موجود یا وضع قوانین نوین به مواردی همچون دقت و وضوح مقررات، عدم تورم کیفری بخصوص با تحدید مسئولیت کیفری به جرایم عمدی و تطابق این قوانین با نسل حقوقی و فرهنگی کشور خود

---

۱. محمدخیام روحانی، جرایم کامپیوتری و مجازات، خبرنامه انفورماتیک شورای عالی انفورماتیک شماره۷۷ فروردین ۱۳۸۰ص۳۹-۳۸
WWW.MCCONNELL INTERNATIONAL.COM

۲. United Nations organization.

۳. (CE):council of Europe

۴. (O.E.C.D): organizationa for economic co-operation and development

۵. (AIDP): Association Internationale de droit penal/international association of penal law

توجه لازم را مبذول دارند.[۱] در سال ۱۹۹۹ گروه هشت (آمریکا، انگلستان، فرانسه، آلمان، ژاپن، کانادا، ایتالیا، و روسیه) درباره جرایم سایبر کنفرانس سه روزه ای برگزار کردند. گروه هشت از مشاغل خصوصی درخواست کرد در راستای مبارزه با جرایم رایانه ای با دولت همکاری کنند و از دولتها درخواست کرد که قوانین مربوط به اینترنت خود را هماهنگ کنند، رویه قضایی را سرعت بخشند و موانع متعدد را (مثل زبان و فرهنگ) در قوانین کشورهای مختلف کاهش دهند.[۲]

بخش پنجم: اقدامات سازمانهای بین المللی و رویه برخی از کشورها در خصوص جرم جاسوسی رایانه ای به عنوان یک جرم مهم بین المللی

همانطور که میدانیم فناوری اطلاعات یکی از بزرگ ترین دستاوردهای علوم بشری است که تأثیرعمیقی بر کشور ها گذاشته است.از بدو پیدایش و همزمان با توسعه این تکنولوژی سوء استفاده از آن توسط مجرمان آغاز و توسعه یافته است، به نحوی که امروزه اشکال متنوع جرائم مرتبط با رایانه و تکنولوژی اطلاعات، تهدیدی جدی برای کشورها و با توجه به بین المللی بودن این تکنولوژی تهدیدی علیه جامعه بین المللی است. همین امر نیز موجب واکنش سازمان های بین المللی و منطقه ای به این جرائم شده است.

بند اول: سازمانهای بین المللی و منطقه ای

جرائم کامپیوتری و اینترنتی با توجه به خصیصه فرا ملی و فرا سرزمینی بودن خود لازمه تعاون و همکاری بین المللی را ایجاد میکنند، چنین پدیده هایی به دلیل شرایط خاص و ماهیت بین المللی شان، نوعی سیاست جنایی متحد الشکل را به دنبال می آورند. در کشورهای پیشرفته قانونگذاران آنها با توجه به نیاز جامعه، انواع مختلفی از اعمال مجرمانه کامپیوتری را شناسایی و در قالب قوانین کیفری خود گنجانده اند. همزمان با این اقدامات پراکنده، مراجع بین الملل نیز فعالیت خود را در این زمینه

---

[۱]. سازمان ملل – نشریه بین الملل سیاست جنایی (ش ۴۳-۱۹۹۴/۴۴) ترجمه دبیرخانه شورای عالی انفورماتیک سازمان برنامه و بودجه کشور جلداول ۱۳۷۶ ص ۴۹.۵۰

[۲]. مرادی، جعفر، جرائم دیجیتال در محیط سایبر، خبرنامه انفورماتیک، شورای عالی انفورماتیک، کشور شماره ۷۹ شهریور و مهر ۸۰ ص ۵۳.

آغاز و با دسته بندی جرائم شناخته شده لیستهایی از این گونه جرایم را به عنوان الگوی واحد و راهنما برای تدوین قوانین ملی کشورها ارائه نمودند.

الف) سازمان همکاری و توسعه اقتصادی (OECD)[1].

تا پیش از اقدام (O. E. C. D) تقسیم بندی دقیقی از جرائم کامپیوتری ارائه نشده بود. بالاخره در سال ۱۹۸۶ (O. E. C. D) بر اساس تجزیه و تحلیل تطبیقی قوانین ماهوی موجود و پیشنهادهای اصلاحی چند کشور عضو، اولین طبقه بندی را ارائه نمود وطی آن پنج دسته از اعمال را مجرمانه تلقی کرد.[2] اما در این تقسیم بندی جرائم کامپیوتری با عنوان خاصی مطرح نشدند و فقط مصداقی از آنها ذکر شد.

ب) اقدامات شورای اروپا (CE)[3]

کمیته منتخب جرائم کامپیوتری پس از بررسی نظرات O ,E ,C ,D و نیز بررسی های حقوقی– فنی دو لیست تحت عنوان «لیست حداقل» و «لیست اختیاری» را در مورد جرائم کامپیوتری به کمیته وزرا پیشنهاد داد که مورد تصویب آنها قرار گرفت. در توصیه نامه شماره (۸۹) R(۹)[4] درج شده است: «کمیته رهنمودهایی ارائه داده است که مختص کشورهای عضو نیست و سیاست جنایی مطرح شده در این رهنمودها به علت توجه به یافته های O, E, C, D و دیگر محققان می تواند برای همه کشورها مطرح باشد». در بند (ب) لیست اختیاری جاسوسی رایانه ای به عنوان یکی از انواع جرائم رایانه ای شناخته شده و اینگونه تعریف شده است:

«بازرسی و تفتیش به وسیله ابزارهای لازم برای افشا انتقال یا استفاده از اسرار تجاری یا بازرگانی بدون داشتن حق یا بدون هیچ توجیه قانونی دیگری خواه با قصد ایجاد ضرر اقتصادی به شخص محقق اسرار و خواه به قصد کسب یک منفعت اقتصادی غیر قانونی برای خود یا دیگری است».

---

[1]. organization for Economie co-operation& Development

[2].بتول پاکزاد، پایان نامه کارشناسی ارشد، جرایم کامپیوتری دانشگاه بهشتی ۱۳۷۵

[3]. (CE): COUNCIL OF EUROPE

[4]. استراسبورگ ۱۹۹۰

ج) سازمان ملل متحد (UN) [۱]

سازمان ملل متحد ضمن تاکید بر تقسیم بندی شورای اروپا (O, E, C D) (فهرستی از انواع مشترک و عمومی جرائم کامپیوتری از دیدگاه خود بیان کرد. این سازمان نیز مثل (O, E, C, D) جاسوسی رایانه ای را در زمره جرائم شمرده شده نیاورده است اما در بند (د) دسته بندی خود دستیابی غیر مجاز به سیستم ها و خدمات کامپیوتری را آورده که شاید بتوان آن را به نوعی بیانگر جاسوسی رایانه ای دانست. این سازمان تعریف دستیابی غیر مجاز[۲] به سیستم ها و خدمات کامپیوتری این گونه بیان می کند: «دستیابی غیر موجه فرد به سیستم کامپیوتری از طریق یافتن راههای گریز سیستم امنیتی، معرفی خود به جای کاربران مجاز سیستم کشف رمز، دستیابی به سیستم می باشد».

د) انجمن بین المللی حقوق جزاء (AIDP)[۳]

انجمن بین المللی حقوق جزا در طول سالهای ۱۹۹۲ و ۱۹۹۴ میلادی در نشستهای خود در ورتسبورگ آلمان و ریودوژانیرو بر کار شورای اروپا، صحه گذاشت و تقسیم بندی آنها را پذیرفت. اما با پیشرفت های حاصل در تکنولوژی اطلاعات و افزایش جرائم مربوط از زمان تصویب قطعنامه سال ۱۹۸۹ میلادی شورای اروپا توصیه می کند که کشورها باید مطابق با سنن حقوقی و فرهنگی خود و با توجه به قابلیت اعمال قوانین موجودشان، رفتارهای ذکر شده در فهرست اختیاری بویژه «تغییر داده های کامپیوتری» و «جاسوسی کامپیوتری» را مورد مجازات قرار بدهند. متوجه می شویم که انجمن بین المللی حقوق جزا «جاسوسی کامپیوتری» را رسماً به عنوان یک جرم رایانه ای تلقی کرده و از کشورها خواسته تا آن را جرم انگاری نمایند.

بند دوم: رویه برخی کشورها[۱]

---

۱. UNITED NATIONS ORGANIZATION

۲. UNAUTHORIZED ACCESS

۳. ASSO CIATION INTERNATION DE DROIT PENAL

۱. بتول پاکزاد، همان.

جرائم کامپیوتری زاییده تکنولوژی پیشرفته اند بنابراین محل نشو و نمایشان نیز در جایی است که این تکنولوژی مدرن بیشتر زمینه طرح دارد. آلمان و آمریکا، از اولین جوامعی هستند که به علت صنعتی بودن برای جرائم کامپیوتری مجازات خاص قرار داده اند.

الف) آلمان

آلمان در روند علمی و تقنینی خود مسیر جالبی را طی کرده و شاید بیش از ۱۰ سال جرائم کامپیوتری و حقوق کیفری اطلاعاتی فقط در عرصه دانشگاه ها و آکادمی ها طرح می شد تا اینکه بالاخره به وسیله شیوع و نیز ایجاد مشکلات تجاری، اقتصادی شگرف برای جامعه آلمان مقنن این کشور برای حل این معضل همت گماشت بنابراین در اصلاحات گذشته در مجموعه قوانین جزایی (S. T. B. B.) و دیگر قوانین ساختار لازم را بنا نهاد.در طبقه بندی قبلی جرائم از سوی مقنن آلمان «جاسوسی کامپیوتری داده ها و یا تسلیم اطلاعات» احصاء شده است.در آخرین طبقه بندی که بر مبنای واقعیت موجود قوانین کیفری کنونی تنظیم شده است و البته در قالب یک مقاله به وسیله دکتر «مورنشلاگر» در گردهمایی و رتسبورگ به سال ۱۹۹۲ میلادی ارائه شده جاسوسی رایانه ای اینگونه احصا شده است:

۱- دستیابی غیر قانوی به سیستمهای پردازش الکترونیک داده ها

- جاسوسی کامپیوتری داده ها

- جاسوسی و تسلیم داده ها

- تخلف از اسرار تجاری و صنعتی

- نفوذ کردن [۱]

ب) آمریکا

همانطور که ملاحظه شد اولین جرائم کامپیوتری در آمریکا واقع شد و هر روز نیز بر دامنه و اشکال مختلف این نحوه عمل مجرمانه در این کشور افزوده می شود این امر منجر به واکنش هایی از سوی

[۱]. Hacking

قانونگذار علیه این جرائم هم در سطح فدرال و هم در سطح ایالت ها شده است که در اینجا قوانین جرائم کامپیوتری دو ایالت تگزاس و ویسکونسین آمریکا مورد بررسی قرار می گیرد.

۱) در قانون جرائم کامپیوتری ایالت ویسکونسین آمریکا[۱]

قبل از هر صحبتی باید توجه داشت که با توجه به سیستم قضایی آمریکا (کامن لاو) [۲]شکل تنظیم قوانین در این کشور با کشورهای پیرو سیستم حقوق نوشته (سیویل لاو) [۳]تا حدی متفاوت است. بیشتر کشورهای عضو سیستم کامن لاو قانون جرایم کامپیوتری را تصویب کرده اند بر خلاف کشورهایی که جرائم کامپیوتری را زیر عنوان کلاسیک آن جرم درج کرده اند (کانادا و آمریکا) یا در فصلی ملحق به کد جزایی کشورشان ذکر کرده اند. (فرانسه) [۴] در قانون این ایالت انواع جرائم کامپیوتری تحت دو عنوان کلی بیان شده اند:

الف) جرائم علیه داده ها وبرنامه های کامپیوتری

ب) جرائم علیه کامپیوتر، تجهیزات یا منابع کامپیوتری

که در قمست الف با اشاره به دستیابی غیر مجاز به داده ها می توان ردپایی از عنوان جاسوسی رایانه ای پیدا کرد.

در متن قانون جرائم کامپیوتری در بخش جرائم علیه داده های ایالت ویسکونسین آمده:

«هر کس عمداً، عالماً و بدون مجوز هر یک از اعمال زیر انجام دهد به مجازات مقرر در همین قانون محکوم می شود:

---

[۱]. فصل ۲۹۳ قوانین ۱۹۸۱، جرائم کامپیوتری، قوانین ایالت ویسکونسین آمریکا، دریافتی از اینترنت دبیرخانه شورای عالی انفورماتیک کشور

[۲]. Common LAW

[۳].Civil LAW

[۴]. بتول پاکزاد، همان و بای، حسینعلی وپور قهرمانی، بابک، بررسی فقهی حقوقی جرائم رایانه ای، ناشر پژوهشگاه علوم وفرهنگ اسلامی، ۱۳۸۸، ص۱۰۶

۱- داده ها، برنامه های کامپیوتری یا مستندات حمایتی را تغییر دهد.

۲- داده ها، برنامه های کامپیوتری یا مستندات حمایتی را تخریب و نابود کند.

۳- به داده ها وبرنامه های کامپیوتری یا مستندات حمایتی دست پیدا کند.

۴- به تصرف داده ها و برنامه های کامپیوتری یا مستندات حمایتی اقدام کند.

۵- داده ها و برنامه های کامپیوتری یا مستندات حمایتی را کپی کند.

۶- کدهای دستیابی محدود یا دیگر اطلاعات برای دستیابی محدود را برای شخص غیر مجاز افشاء کند.

با توجه به بندهای ۳و ۴و ۵و ۶ این ماده در می یابیم رابطه بسیار نزدیکی بین اقدامات صورت گرفته با جاسوسی کامپیوتری به دیده اغماض وجود دارد.

ب) قانون جرائم کامپیوتری ایالت تگزاس آمریکا[1]

در قانون جرائم کامپیوتری تگزاس انواع جرائم تحت دو عنوان کلی «نقض امنیت کامپیوتر» و «دستیابی مضر» بیان شده اند.

که در عنوان کلی «نقص امنیت کامپیوتر» ما با جرائمی از این دست روبرو هستیم:

- استفاده غیر مجاز از کامپیوتر
- دستیابی غیر مجاز به کامپیوتر
- دستیابی غیر مجاز به داده های کامپیوتر
- افشاء اطلاعات محرمانه مربوط به سیستم امنیتی کامپیوتر

[1]. فصل ۳۳ بخش عنوان ۷، قوانین ایالت تگزاس آمریکا، دریافتی از اینترنت دبیرخانه شورای عالی انفورماتیک

در دو عنوان اخیر «دستیابی غیر مجاز به داده ها» و «افشاء اطلاعات محرمانه» موجود در این قانون جرائم رایانه ای، جرم انگاری جاسوسی رایانه ای به خوبی مشهود است هر چند ضمنی و نه تحت عنوان خاص.[1] در اینجا لازم به ذکر است که هر چند در مطالب گذشته شاهد تلاش های کشور ها و مجامع بین المللی در خصوص جرم انگاری جرائم رایانه ای علی الخصوص جاسوسی رایانه ای بودیم. اما به نظر نویسنده تداوم و جامعیت بخشیدن به این اقدامات بصورت روزآمد بسیار واجب بوده و سایر کشورها هم که در این راستا کوتاهی کرده اند، باید از سوی نهاد های بین الملل تحت فشار قرار بگیرند تا هر چه سریعتر اقدامات لازم را انجام بدهند.

نتیجه گیری

در گذشته گفتیم اختراع کامپیوتر و پس از آن دستیابی انسان به فضای سایبر سبب تغییراتی عظیم در زندگی ما از جهات گوناگون شده است. بیشتر جرائم در گذشته محدود به زمان و مکان معینی بودند و بیشتر مجرمین، بزه دیدگان و جرائم به راحتی قابل شناسایی بودند و از ماهیت پیچیده ای برخوردار نبودند، اما کامپیوتر و اینترنت تحولات شگرفی را موجب شدند به تبع دستیابی بشر به کامپیوتر و اینترنت در ماهیت جرائم تغییرات بس شگرف به وجود آمد. برای مثال جرائمی مثل سرقت، جعل، جاسوسی و... همگی در شکل کلاسیک آن در فضای مادی و محسوس اتفاق می افتادند. در این میان جرم جاسوسی در شکل کلاسیک، که شاید بتوان آن را مهم تر از سایر جرائم دانست با تحولات دنیای علم در زمینه رایانه شکل تازه ای برای ارتکاب به دست آورد که این تهدیدی جدی و نوین علیه امنیت برای زمان حال یا خطری بزرگ برای آینده ای بسیار نزدیک می تواند باشد. زیرا که متخصصان معتقدند جرم جاسوسی رایانه ای، با شدت و پیچیدگی بیشتری از سایر جرائم در سطح وسیع جهانی ادامه پیدا خواهد کرد. همچنین در راستای پیشگیری از جرایم اینترنتی همچون کلاهبرداری و جاسوسی اینترنتی باید گفت از آنجا که پلیس به عنوان ضابط دادگستری وظیفه کشف جرایم را به عهده دارد، در کنار آموزش قضات و سایر مقامات قضایی، آموزش پلیس نیز باید در سر فصل برنامه ریزی ها قرار گیرد. همچنین مورد دیگری که پیشنهاد می گردد آموزش عمومی در سطح کارمندان دولت و نظامیان برای جلوگیری از بی احتیاطی، بی مبالاتی این افراد در خصوص داده های

[1].پاکزاد، بتول، همان و بای حسینعلی و پور قهرمانی، بابک، همان، ص۱۰۷

سری است.مورد دیگری که در راستای جلوگیری از جرایم اینترنتی می توان ب هآن اشاره داشت مسدود کردن درگاه های رایانه های حساس در ادارات به عنوان راهکاری سریع و کم هزینه در عین حال موثر می باشد. در این روش تمامی درگاه های سیستم های رایانه ای از قبیل درایوهای CD و DVD، پورت های USB و... از طریق سرور (شبکه) بسته شده، به این ترتیب کاربر رایانه نمی تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند تا بدین سان جرم جاسوسی یا کلاهبرداری اینترنتی و یا حتی سرقت اینترنتی صورت گیرد و محقق شود.. در این حالت کاربر تنها به داده های مجاز که از سوی مسئولان و به منظور انجام وظیفه روی سیستم او قرار داده شده، دسترسی خواهد داشت.

منابع و مأخذ

الف)کتاب ها

۱. آریا، ناصر، فرهنگ اصطلاحات کامپیوتر و شبکه های کامپیوتری، نشر جنگل، ۱۳۸۹.

۲. آشوری، محمد، آئین دادرسی کیفری، دوره دو جلدی، انتشارات سمت، ۱۳۸۵.

۳. اردبیلی، محمد علی، حقوق جزای عمومی، دوره دو جلدی، نشر میزان، ۱۳۸۳.

۴. بابایی، حسن، جاسوسی از دیدگاه حقوق بین الملل، کتابخانه گنج دانش، ۱۳۸۸.

۵. بای، حسینعلی و پور قهرمانی، بابک، بررسی فقهی حقوقی جرائم رایانه ای، نشر پژوهشگاه علوم و فرهنگ اسلامی، ۱۳۸۸.

۶. جعفری، فرهاد و بناء پور، هاشم، فرهنگ کامپیوتر، انتشارات تلاش، ۱۳۸۲.

۷. جلالی فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، انتشارات خرسندی، ۱۳۸۹.

۸. جلالی فراهانی، امیرحسین، درآمدی بر آئین دادرسی کیفری جرایم سایبر، انتشارات خرسندی، ۱۳۸۹.

۹. حسن بیگی، ابراهیم، حقوق و امنیت فضای سایبر، نشر ابرار، ۱۳۸۴.

۱۰. خرم آبادی، عبدالصمد، مجموعه مقالات همایش بررسی ابعاد حقوقی فن آوری اطلاعات، انتشارات سلسبیل، ۱۳۸۲.

۱۱. شامبیاتی، هوشنگ، حقوق جزای عمومی، دوره دو جلدی، انتشارات مجد، ۱۳۸۸.

۱۲. شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، نشر بهینه فراگیر، ۱۳۸۸.

۱۳. صادقی، محمد هادی، جرائم علیه اشخاص، نشر میزان، ۱۳۸۴.

۱۴. ضرابی، غلامرضا، آئین دادرسی کیفری، کتابخانه گنج دانش، ۱۳۷۲.

۱۵. عالی پور، حسن، جرائم ضد امنیت ملی، انتشارات خرسندی، ۱۳۸۹.

۱۶. عالی پور، حسن، حقوق کیفری فناوری اطلاعات، انتشارات خرسندی، ۱۳۹۰.

۱۷. فضلی، مهدی، مسئولیت کیفری در فضای سایبر، انتشارات خرسندی، ۱۳۸۹.

ب)مقالات

۱. اسماعیل بیگدلی، مجید، تاریخچه جرائم سایبر، دریافتی از اینترنت، ۱۳۸۹.

۲. باقری پور، سید محمد، آشنایی با جرائم رایانه ای، دریافتی از اینترنت، ۱۳۹۰.

۳. بیات، سمیرا، جرائم رایانه ای، اینترنت، ۱۳۹۰.

۴. پیرزمان، حسن، تاریخچه جرائم اینترنتی، اینترنت، ۱۳۸۷.

۵. جعفری، رضا ودکتر فیض چکاب، بررسی جرائم رایانه ای و اینترنتی، میزگرد، ۱۳۹۰.

۶. جاویدنیا، جواد، جرم رایانه ای چیست؟ اینترنت، ۱۳۸۹.

۷. جلالی فراهانی، امیرحسین، صلاحیت در فضای سایبر، فصلنامه فقه و حقوق شماره ۱۳۸۶، ۱۱.

۸. خاتمی نژاد، سید حسین و حسین پور، ابوالفضل، بررسی جرائم کامپیوتری، اینترنت، ۱۳۸۹.

۹. خانزاده، حمید، تحلیل قانون مدنی جرائم رایانه ای، اینترنت، ۱۳۸۸.

۱۰. دوست مهدیان و ترابی، رضا، جرائم و مقررات ادله الکترونیکی امنیت مجازی، اینترنت، ۱۳۸۷.

۱۱. روحانی، محمد خیام، جرایم کامپیوتری و مجازات، خبرنامه انفورماتیک، شورای عالی انفورماتیک، شماره ۷۷ فروردین ۱۳۸۰.

د)پایان نامه ها

۱. ابراهیمی، فرشاد، هتک حیثیت افراد از طریق افشای سر در محیط مجازی، پایان نامه کارشناسی ارشد، دانشگاه شیراز، ۱۳۹۱.

۲. البوعلی، امیر، صلاحیت مراجع قضایی در رسیدگی به جرائم ارتکابی در فضای سایبر، پایان نامه کارشناسی ارشد، دانشگاه شیراز، ۱۳۸۸.

۳. آل محمد، فاطمه، سیاست جنایی ایران در قبال جرائم رایانه ای، پایان نامه کارشناسی ارشد، دانشگاه شیراز، ۱۳۹۰.

۴. پاکزاد، بتول، جرائم کامپیوتری، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی، ۱۳۷۵.

۵. رحیمی سکه روانی، محمد، پیشگیری غیرکیفری از جرائم در فضای سایبر، پایان نامه کارشناسی ارشد، دانشگاه شیراز، ۱۳۸۹.

۶. علمداری، علی، مبانی و معیار جرم انگاری جرایم سایبر (مطالعه تطبیقی در حقوق ایران و آلمان)، پایان نامه کارشناسی ارشد، دانشگاه شیراز، ۱۳۸۹.

۷. عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه ای از دیدگاه فقه و حقوق کیفری ایران، دانشگاه آزاد واحد تهران مرکز، پایان نامه کارشناسی ارشد، ۱۳۸۷.