فهرست مطالب

مقدمه

جرایم رایانه‌ای از رایج ترین،گسترده ترین و پیشرفته ترین جرایم در عصر حاضر می‌باشند.
این جرایم به دلیل راحتی در ارتکاب و گستردگی بیش از اندازه و هم چنین داشتن جنبه‌ی فرا ملی می‌بایست بیشتر مورد توجه قرار گیرند.
این دسته از جرایم به راحتی حریم خصوصی افراد را مورد تعرض قرار می‌دهند و علاوه بر جنبه‌ی مالی، به حیثیت افراد نیز تعرض می‌کنند.
با در نظر گرفتن این مسئله که زندگی اجتماعی افراد در جامعه هر روز بیش از پیش با فضای مجازی آمیخته می‌شود و این آمیختگی سبب گستردگی این محیط و در نتیجه افزایش جرایم در این محیط می‌شود،قوانین ما نیز لازم است که سرعت هماهنگی خود را افزایش دهند و به نحوی مورد استفاده و اجرا قرار گیرند که بتوانند تا حدودی جلوی رشد بی رویه آمار جرایم رایانه‌ای را بگیرند.
این مهم نیز تا حدودی با تجزیه و تحلیل قوانین و رویه قضایی امکان پذیر است اما برای به دست آوردن نتیجه‌ی مطلوب تر باید حمایت و حفاظت از این محیط را به طور جدی تر انجام دهیم و هم چنین قانون گذاری در این موارد را با جامعه‌ی بین المللی هماهنگ تر نماییم.
در راستای موارد ذکر شده، در این پایان نامه سعی شده است که با توجه اصول اساسی حقوق جزا و هم چنین نظر اساتید و حقوق دانان و رویه‌ی قضایی، به تحلیلی درست و کارآمد از ماده‌ی ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تحت عنوان دسترسی غیر مجاز دست پیدا کنیم تا حتی اندکی به هدف کلی ما که امنیت هرچه بیشتر فضای مجازی است نزدیک تر شویم.

الف) بیان مسئله:

رایانه یکی از بزرگ ترین و عمومی ترین دستاوردهای علمی – صنعتی بشر در نیم قرن اخیر است و به موازات پیدایش و گسترش کمی و کیفی خود پرسش‌های بسیاری را پیش رو گذاشته است. گسترش شبکه‌های جهانی و محلی اینترنت و فضای مجازی ابعاد بسی گسترده از مباحث و مسائل حقوقی در همین فاصله زمانی کوتاه را پدید آورده است.

رایانه به موازات خدمات بی شمار خود همچون دیگر دستاوردهای علمی – صنعتی امکان بهره برداری نادرست از آن و تبدیل به ابزاری برای جرم و بزه را دارد. این جرایم اقسام مختلفی دارد و به شیوه‌های مختلف واقع می‌شوند به عبارتی، امروزه رایانه و تجهیزات رایانه‌ای امکان بیش از پیش رفتارهای ضداجتماعی را به وجود آورده است. جرایمی که تا پیش از این به هیچ وجه امکان پذیر نبوده است و نیز فرصت‌های تازه و پیشرفت‌های بسیاری برای قانون شکنان در اختیار انسان قرار داده، ومی توان گفت به صورت بالقوه ارتکاب گونه‌های مرسوم و کلاسیک جرایم را به شیوه‌های غیر مرسوم و بسیار جدید سوق می‌دهد. منظور از جرایم رایانه‌ای جرایمی می‌باشند که یا مستقیما رایانه را مورد هدف قرار داده اند و به عبارتی جرایم علیه رایانه محسوب می‌شوند مثل؛ ایجاد خسارت در داده‌ها و اختلال در داده ها، اختلال در سیستم و شبکه تولید و انتشار برنامه‌های مخرب و موجد اختلال و..... و یا اینکه جرایمی سنتی هستند که رایانه فقط به عنوان وسیله ارتکاب جرم می‌باشند و به عبارتی می‌توان گفت که جرایم از طریق رایانه می‌باشند مثل: کلاهبرداری، جعل، پولشویی، توهین، افترا و...

رایانه‌ها در این مدت کم به خوبی توانستند جای خود را در تمامی شئون زندگی انسان باز کنند و به نوعی خود را در تمامی پیشرفت‌ها سهیم سازند. این اقبال عمومی بهره برداری روزافزون از سیستم‌های رایانه‌ای زمانی شتاب بیشتری به خود گرفت که در ابتدای دهه‌ی نود میلادی امکان متصل شدن آنها به یکدیگر در سراسر جهان فراهم شد. در این زمان بود که مشاهده شد مرزها و موانع فیزیکی بی اثر شده و به نوعی رویاهای جهانی بشر واقعیت یافته است. اما از آنجا که این پدیده‌ی شگفت انگیز از همان بدو تولد در دسترس همگان قرار گرفت، هر کس مطابق اغراض و مقاصد خود از آن سود می‌جست و نتیجه آن شد که بعضی از این بهره برداری‌ها جنبه سوء استفاده به خود گرفت و سیاستگذاران خرد و کلان را مجبور کرد که تدبیری بیاندیشند. این سوء استفاده‌ها که در مجموع

جرائم رایانه‌ای نام گرفته اند، طیف جدیدی از جرائم هستند که به سبب ویژگی‌های متمایزی که با جرائم سنتی دارندتصمیم گیران جامعه را بر آن داشته اند تا در ابعاد مختلف اقدامات متمایزی را طرح ریزی کنند.

در نتیجه‌ی این پیشرفت علم و فراگیر شدن استفاده از فضای مجازی سبب ایجاد بستری مناسب برای سودجویی و انجام جرایم جدید شده است که با تصویب قانون مبارزه با جرایم رایانه‌ای در سال ۱۳۸۸ و جرم انگاری آن توسط مقنن سعی در پیشگیری از ارتکاب این نوع جرایم شده است. ماده‌ی ۱ قانون جرایم رایانه‌ای در باب جرم دسترسی غیر مجاز می‌باشد که با توجه به اینکه بیشتر بزه‌های رایانه‌ای از رهگذر دسترسی غیر مجاز انجام می‌یابند می‌توان گفت که دسترسی مقدمه‌ی لازم دیگر بزه هاست. دسترسی غیر مجاز عبارت است از:رخنه غیر قانونی به سیستم یا شبکه رایانه‌ای حفاظت شده یک شخص حقیقی یا حقوقی، از دسترسی غیرمجاز گاه به عنوان نفوذ غیر مجاز و هک یاد می‌شود که به نظر می‌رسد استفاده این دو واژه مترادف به جای دسترسی غیر مجاز صحیح نباشد. حال با بررسی ماده ۱ قانون جرایم رایانه‌ای که راجع به همین جرم دسترسی غیر مجاز به اطلاعات افراد است در می‌یابیم که برخی از نواقص و ابهام و کلی گویی در این ماده وجود دارد که این نواقص شامل:

۱) عدم تبیین و ابهام کلمه غیر مجاز و تدابیر امنیتی مذکور در صدر ماده.

۲) عدم پیش بینی تحقق این جرم در صورت ترک فعل.

۳) عدم بازدارندگی مجازات

٤) عدم همخوانی ضرر وارده از این جرم برای جامعه و افراد نسبت به مجازات.

۵) از لحاظ غیر عمدی بودن تحقق این جرم هیچ سخنی به میان نیامده است.

هم چنین باید گفت که پس از تصویب قانون مجازات اسلامی در سال ۱۳۹۲ هیچگونه بررسی تطبیقی با قانون جرایم رایانه‌ای در زمینه‌ی معاونت و مشارکت و مواردی از این دست صورت نگرفته است.

با توجه به موارد ذکر شده و از آنجا که جوامع انسانی همواره پویا هستند و قوانین به بیان اصول و قواعد کلی بسنده می‌کنند رویه قضایی در نقش تفسیری و تکمیلی می‌توانند تفاسیری منطبق با واقعیات و ضروریات اجتماعی از قانون ارائه بدهد.قانون نظم ناقص است و نمی‌توانیم همه‌ی راه حل‌ها را در آن بیابیم و این قدرت رویه قضایی است که می‌تواند به کمک نص قانون به ارائه

استنتاجی منطبق با واقعیت‌ها بپردازد و آنگاهی که قانون از این تحولات عقب می‌ماند سیستم قضایی به عنوان مکمل وارد می‌شود تا بتواند به این خلاها پاسخ گوید.

ب) ضرورت انجام پژوهش:

با توجه به ضرورت استفاده از فضای مجازی و گستردگی استفاده‌ی تمامی اقشار جامعه از آن بدون هیچگونه محدودیت سنی و مکانی و زمانی و...ایجاب میکند که ابهام زدایی هایی از متن قانون در راستای کمک به حفظ حریم خصوصی افراد وسلامت جامعه صورت گیرد و از آنجایی که به نسبت اهمیت و گستردگی جرم دسترسی غیرمجاز به این جرم پرداخته نشده است سعی بر آن داشتم که با بررسی کاربردی و رویه‌ای این جرم تا حدودی به رفع ابهامات قانونی در این جرم بپردازم تا بتوان به راهکارهایی برای امنیت هرچه بیشتر در فضای مجازی دست پیدا کرد.

پ) سؤال‌های پژوهش:

۱)رویه قضایی دادگاه‌های ایران در زمینه‌ی جرم دسترسی غیرمجاز چگونه است؟

۲) منظور از تدابیر امنیتی ذکر شده در ماده ۱ قانون جرایم رایانه‌ای چیست ؟

۳) منظور از واژه‌ی غیر مجاز در این ماده چیست ؟

ت) فرضیات پژوهش:

۱) تفاوت بسیاری در هک و دسترسی غیرمجاز وجود دارد اما قانون گذار هر دو واژه را مترادف گرفته است.

۲)مجازات تعیین شده در ماده ۱ قانون جرایم رایانه‌ای بازدارندگی و کارایی لازم را ندارد.

۳) جرم انگاری ماده ۱ قانون جرایم رایانه‌ای مشمول حامل‌های داده نیز می‌شود.

ث) اهداف پژوهش:

۱) بررسی از منظر معاونت و مشارکت در رویه قضایی

۲) بررسی از منظر مقید و یا مطلق بودن در رویه قضایی

۳) بررسی از منظر شروع به جرم در رویه قضایی

٤) بررسی ادله اثبات در رویه قضایی

۵) بررسی ابهام گویی‌های قانون و بررسی آن موارد در رویه قضایی

ج) سابقه انجام پژوهش:

با توجه به جستجوهای به عمل آمده، تألیفات مختلفی در موضوع بحث یافت شد که عبارتند از:
کتب‌های کار شده: جرایم رایانه‌ای نوشته اولریش زیبر،بررسی فقهی حقوقی جرایم رایانه‌ای تألیف حسینعلی بای و بابک پورقهرمانی، تحقیقات مقدماتی در جرایم سایبر نوشته محمدرضا زندی، مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات گردآوری شده توسط امیر حسین جلالی فراهانی، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین الملل و... که بسیاری از اینها به تازگی به چاپ رسیده‌اند. همچنین یک رساله دکتری با موضوع «جرایم فناوری اطلاعات» به نگارش عبدالصمد خرم آبادی و نیز پایان نامه کارشناسی ارشد با عنوان بررسی راهکارهای مبارزه با جرایم رایانه‌ای با توجه به مقررات داخلی و بین المللی» نوشته سجاد آقا خانی و «کلاهبرداری کامپیوتری در حقوق ایران و ایالات متحده آمریکا» به قلم مصطفی عباسی حسین آبادی، « استنادپذیری ادله دیجیتال در حقوق کیفری» به نگارش افشار خسروی زاده، «دادرسی جرایم رایانه‌ای در حقوق کیفری ایران» نوشته همت الله انصاری، تاکنون در زمینه‌ی بزه دسترسی غیر مجاز هیچ گونه تحلیل رویه‌ای صورت نگرفته است اما در رابطه با دسترسی غیر مجاز پایان نامه هایی تحت عنوان«دسترسی غیرمجاز در فضای. سایبر »به نگارش مهدی قاسمی خواه و راهنمایی شهرام ابراهیمی و «دسترسی غیر مجاز افراد در فضای مجازی » به نگارش کبری میرزاده سرند و راهنمایی عسل عظیمیان نگارش شده است.

چ) نوآوری پژوهش:

نوآوری در این پژوهش بررسی رویه مراجع قضایی در زمینه‌ی دسترسی غیرمجاز(ماده ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸) می‌باشد که تاکنون مورد پژوهش قرار نگرفته است، همچنین بررسی‌ها شامل اصلاحات انجام شده در مواد عمومی قانون مجازات اسلامی مصوب ۱۳۹۲ و هم چنین اصلاحات انجام شده در قانون آیین دادرسی کیفری در سال ۱۳۹٤ که مرتبط با مبحث دسترسی غیرمجاز می‌باشند انجام گرفته است.

ح) روش پژوهش:

روش تحقیق در پژوهش حاضر توصیفی- تحلیلی است که یافتههای این پژوهش بر اساس منابع کتابخانهای (استفاده از کتب و مقالات فارسی و انگلیسی) و همچنین مراجعه به دادگاه و دادسرا و بررسی آرا مرتبط و هم چنین صحبت با قضات به دست آمده است.

خ) موانع و محدودیتهای پژوهش:

از جمله موانع در انجام این پژوهش منابع بسیار اندک در زمینهی جرایم رایانهای به خصوص دسترسی غیر مجاز و هم چنین تعداد آرا قضایی بسیار محدود در زمینهی دسترسی غیر مجاز و عدم همکاری پژوهشکدهی منابع انسانی قوهی قضاییه در خصوص در اختیار قرار دادن آرا قضایی میباشد.

د)ساختار پژوهش:

موضوع این پژوهش در دو فصل کلی مورد بررسی و تحقیق قرار گرفته است که در فصل نخست و در مبحث اول تلاش بر این بوده است که تاریخچهای مختصر از جرایم رایانهای و چگونگی تغییر و رشد این جرایم را بررسی نماییم و سپس در مبحث دوم و سوم به بیان تعاریفی از واژگان تخصصی و تعاریف بین المللی از جرایم رایانهای پرداخته شده است و در مبحث چهارم از این فصل که مبحث آخر است به جرم دسترسی غیرمجاز که محور اصلی این پژوهش است ورود کرده ایم و سعی کرده ایم که مبانی اصلی و نظری این جرم را بررسی کرده و به تعدادی از اختلافات رویهای و نظرات مختلف در جرم دسترسی غیرمجاز بپردازیم و هم چنین در این مبحث به دو عنوان مهم و بحث برانگیز که فروش و استفاده از فیلتر شکن است پرداخته شده و از نظر رویهای بررسی انجام گرفته است.

فصل دوم نیز به چهار مبحث اختصاص داده شده است که مبحث اول آن به بررسی جرم دسترسی غیرمجاز به عنوان جرم مقدمه برای جرایم دیگر و بررسی قواعد تعدد در این موارد و هم چنین رویهی قضایی در اعمال این مقررات در جرایم مختلف رایانهای به صورت موردی پرداخته شده است و سپس به بررسی مقررات تکرار جرم، شروع به جرم و شرکت و معاونت پرداخته شده است.

در ادامه‌ی فصل دوم نیز به مباحث ادله‌ی الکترونیکی و صلاحیت‌ها و تفتیش و توقیف و رویه‌ی قضایی در پذیرش ادله در جرایم رایانه‌ای پرداخته شده است، در مبحث تفتیش و توقیف سعی بر آن شده است که حدود اختیارات ضابطان به طور دقیق بررسی شود، زیرا از نظر نگارنده خروج از این حدود نیز می‌تواند مشمول دسترسی غیرمجاز بشود که در این مبحث به بحث و بررسی این نظریه پرداخته شده است.

در مبحث صلاحیت نیز سعی بر آن شده است که تمامی فروض را مورد بررسی قرار بدهیم و به نتیجه گیری کلی در این مبحث برسیم.

فصل اول

تاریخچه، مفاهیم، کلیات دسترسی غیر مجاز

مبحث اول:تاریخچه‌ای از جرائم رایانه‌ای در دنیا

فناوری همواره در حال پیشرفت است و این بدان معناست که مجرمان اینترنتی به طور مداوم حملات جدیدی را متناسب با روند جدید آغاز می‌نمایند، برای درک چگونگی تکامل جرایم رایانه‌ای در آینده نیاز است که به گذشته نگاهی کنیم تا بفهمیم این جرایم چگونه در گذشته به وجود آمده و تکامل یافته‌اند.

گفتار اول:معروف ترین حملات سایبری تاریخ

ریشه‌ی اصلی جرایم رایانه‌ای در ارتباطات از راه دور می‌باشد و عنوان هکر ناشی از ایجاد تلفن و سیستم‌های مخابراتی است که در دهه ۱۹۷۰ به اوج خود رسید به گونه‌ای که افرادی با توجه به ویژگی‌های سخت افزاری و فرکانسی شبکه‌های تلفنی و با بررسی نقاط ضعف آنها و استفاده از همان ضعف‌ها قادر به دریافت نرخ تلفن رایگان شده بودند.

اما جرایم رایانه‌ای و اینترنتی در سال ۱۹۸۸ هنگامی که شخصی به نام رابرت تپن موریس[۱]، ویروسی را به نام موریس در جهان آزاد کرد آغاز شد، موریس به درستی نمی‌دانست که این ویروس قادر به چه چیزی می‌باشد،زیرا قبلا این ویروس را به طور کامل در آزمایشگاه مورد بررسی قرار نگرفته بود، در نهایت آزاد سازی این ویروس سبب شد که کامپیوترها در سراسر جهان تحت تاثیر این ویروس قرار گرفته و سرورهای اصلی دچار اختلال شده و متوقف شوند، با وجود اینکه موریس به سرعت دستورالعمل‌های خاموش کردن این ویروس را منتشر کرد اما خسارات بسیار زیادی در سراسر جهان به وارد شده بود و در سال ۱۹۸۹ موریس اولین شخصی بود که تحت عنوان سو استفاده رایانه‌ای تحت پیگرد قانونی قرار گرفت [۲].

در حالی که برخی از هکرها و ویروس‌ها به خاطر چیزهای غیرعادی یا خنده دار به یاد آورده می‌شوند، یک ویروس مخرب رایانه‌ای که اولین بار در سال ۲۰۱۰ کشف شد، به دلیلی کاملاً متفاوت در تاریخ ثبت خواهد شد. کرم استاکس نت [۳]را اولین سلاح دیجیتالی جهان لقب داده‌اند. به نظر می‌رسد برخلاف ویروس‌های دیگر، این کرم برای آسیب فیزیکی به تجهیزات کنترل شده توسط

---

[۱] Robert Tappan Morris

[۲] https://peoplepill.com/people/robert-tappan-morris/

[۳] Stuxnet

رایانه‌ها طراحی شده است. این اولین مورد شناخته شده‌ای بود که هکرها می‌توانستند به تجهیزات دنیای واقعی صدمه جسمی وارد کنند، و این کار آنها را بسیار پیچیده و نسبتاً ترسناک می‌کند. این کرم برای هدف قرار دادن سیستم

های کنترلی مورد استفاده برای نظارت بر تأسیسات صنعتی طراحی شده بود و اولین بار پس از شکستن غیرمنتظره تعداد زیادی سانتریفیوژ اورانیوم در نیروگاه‌های هسته‌ای در ایران کشف شدکه هیچ کس مسئولیت آن را بر عهده نگرفت. استاکس نت به طور خاص کنترل کننده‌های قابل برنامه ریزی منطقی را هدف قرار می‌دهد، که به شما امکان می‌دهد فرآیندهای الکترومکانیکی مانند مواردی که برای کنترل ماشین آلات و فرآیندهای صنعتی از جمله سانتریفیوژهای گاز برای جداسازی مواد هسته‌ای استفاده می‌شود کند. گزارش شده استاکس نت تقریباً یک پنجم سانتریفیوژهای هسته‌ای ایران را خراب کرده است[۱]. به دنبال حمله استاکس نت به برنامه هسته‌ای ایران در سال ۲۰۱۰، ایران به سرعت شروع به سرمایه گذاری و بهبود قابلیت‌های تهاجمی جنگ سایبری خود کرد، که حملات پیچیده تری را به دنبال داشت.

عملیات cleaver یک عملیات مخفی جنگ سایبری بود که سازمان‌های مهم زیرساختی در سراسر جهان را هدف قرار می‌داد که بر اساس گزارش‌ها بیش از ۵۰ کشور مورد حمله‌ی سایبری قرار گرفته بودند و این گزارش همچنین نشان می‌دهد که فرودگاه‌ها، شرکت‌های هواپیمایی اصلی، آژانس‌های دولتی، شرکت‌های حمل و نقل، اپراتورهای ارتباط از راه دور، پیمانکاران دفاعی و موسسات آموزشی از جمله این مراکز هستند اما نوع دسترسی هکرها در سازمان‌های مختلف و داده‌های سرقت شده آنها بسیار متفاوت بود. در مورد دانشگاه‌ها، آنها داده‌های تحقیقاتی، اطلاعات دانشجویی، خانه دانشجویی و همچنین شناسایی اطلاعات، تصاویر و گذرنامه را هدف قرار دادند، در مورد شرکتهای زیرساختی حیاتی، آنها اطلاعات مهمی را سرقت کردند که می‌تواند به آنها یا سازمانهای وابسته امکان خرابکاری در سیستمهای کنترل صنعتی،کنترل نظارت و دستیابی به داده‌ها را بدهد.این حمله در جهان به نام هکرهای ایرانی شناخته می‌شود[۲] اما ایران هیچ وقت مسئولیت این حمله را برعهده نگرفت، از نظر

[۱] Eric j. sinrod (۲۰۱۴), when does cybercrime become internet warfare?

[۲] https://www.computerworld.com/article/۲۸۵۴۰۸۴/iranian-hackers-compromised-airlines-airports-critical-infrastructure-firms.html

برخی از سیاست مداران این حمله توسط ایران و در پاسخ به ویروس استاکس نت صورت گرفته است اما صحت آن هیچ وقت تایید نشد.

همانطور که هر سال قدرتهای نظامی به طور تصاعدی رشد میکند، قابلیتهای سایبری نیز میتواند رشد کند اما آنچه واضح است پس از حملات استاکس نت ایران به سرعت در زمینهی سایبری پیشرفت کرد به گونهای که شاید بتوان گفت جزو قدرتهای برتر در این زمینه پس از روسیه و چین قرار دارد.

در نتیجه میتوان بیان داشت که از آنجا که سیستمهای رایانهای از زندگی روزمره، مشاغل، سازمانها، دولتها و اشخاص جدایی ناپذیرند، ما یاد گرفته ایم که اعتماد فوق العاده زیادی به این سیستمها داشته باشیم.

در نتیجه، ما اطلاعات فوق العاده مهم و ارزشمندی را روی آنها قرار داده ایم. تاریخ نشان داده است که چیزهای با ارزش همیشه هدف یک مجرم قرار میگیرند. همانطور که افراد از دادههای ارزشمند رایانههای شخصی، تلفنها و غیره خود را پر میکنند، اطلاعاتی را برای هدف قرار گرفتن توسط مجرمین قرار میدهند. که همین موضوع سبب گسترش جرایم رایانهای از مقیاسهای کوچک یعنی اشخاص تا کشورها را درگیر کند که نشان میدهد جرایم سایبری از مهم ترین مواردی است که باید به آنها توجه ویژهای شود.

الف) نسل اول جرائم رایانه ای

در راستای بررسی تاریخچه جرایم رایانهای ابتدا به نسل نخست این جرایم بر میخوریم که در مقایسه با جرایم کلاسیک تافتهی جدابافتهای محسوب نخواهند شد و با توجه به اولین نسل از این جرایم که در دههی ۱۹۶۰ صورت گرفت میتوان گفت که اساسا حریم خصوصی افراد را مورد حمله قرار میداد اما با رشد روزافزون تکنولوژی و ورود رایانه به فعالیتهای اقتصادی و شغلهای صنعتی در دههی ۱۹۷۰، گرایش بزه کاران سایبری نسبت به بحث حریم خصوصی کاهش یافته و به سمت جرایم اقتصادی منحرف شد، جرایمی که همچنان در بطن جامعه گستردگی زیادی دارد و حجم زیادی از پروندههای قضایی را شامل میشوند همانند کلاهبرداری رایانه ای،سرقت رایانه ای، جاسوسی و...، نسل نخست به جرایم رایانهای در معنای خاص آن اشاره دارد،که در دههای ۶۰ و ۷۰

میلادی به مرحله‌ی ظهور رسیدند[۱]. در این مقطع زمانی تاکید بر رایانه به عنوان یک وسیله نوین برای ارتکاب جرایم سنتی همانند کلاهبرداری و جعل نگریسته می‌شد.در واقع می‌توان گفت نسل اول جرایم سایبری از رایانه برای فعالیت مجرمانه استفاده می‌کرد[۲].

ب) نسل دوم جرائم رایانه ای

در نسل دوم تمرکز بر محتوا بیشتر شد. به دیگر سخن در نسل دوم تاکید بر داده‌های رایانه‌ای بود. در این مرحله تنها به رایانه به مثابه وسیله و یا واسط ارتکاب جرایم سنتی نگریسته نمی‌شد. بلکه هر نوع جرمی که علیه داده چه در خود رایانه و چه در حامل‌های داده و یا سایر واسط‌های انتقال صورت می‌گرفت را جرم

رایانه‌ای تلقی می‌نمودند. این نسل از جرایم رایانه‌ای در دهه ۸۰ میلادی آغاز شده و تا اوایل دهه ۹۰ میلادی نیز ادامه یافت. اما در نهایت تجمع رایانه و مخابرات الکترونیکی محض، فضای خاصی را تحت عنوان فضای رایانه‌ای بوجود آورد که مسائل جزایی آن به گونه‌ای متفاوت و متکامل نسبت به جرایم رایانه‌ای در دهه‌های ٦۰ و ۸۰ میلادی است.

پ) نسل سوم جرائم رایانه‌ای

مسلماً آنچه که جرایم رایانه‌ای دهه‌های گذشته را دگرگون نمود، پیدایش فضای سایبر بوده است. فضای سایبر تاریخچه جرایم رایانه‌ای را تحت تاثیر کامل خود قرار داده است. این فضا مولد جرایم نوینی شد که امروزه به جرایم سایبر (Cyber Crime) معروف هستند. که تا به امروز، آنها را به عنوان آخرین نسل از جرایم رایانه‌ای می‌شناسند. نسل سوم از جرایم رایانه‌ای را باید سرآغاز مرحله نوینی در جرایم رایانه‌ای به حساب آورد که از اوایل دهه ۹۰ میلادی با ورود و بسط فضای مجازی و بالاخص اینترنت پا به عرصه وجود نهاد. در پی افزایش ورود تکنولوژی به زندگی شهروندان و ورود کاربران متعدد به شبکه هاب اجتماعی و شناخته شدن و گسترش وب در دهه‌ی ۹۰ میلادی راه برای آن دسته از بزه کارانی که به هرزه نگاری کودکان، قمار، فعالیت‌های تروریستی و... علاقه مند بودند باز شد و همزمان با همه گیر شدن فعالیت‌های رایانه‌ای در جامعه، این گونه بزه‌ها نیز گسترس پیدا کرد به

---

[۱] لطفی ، سمانه ، حیدری ، علی مراد ، شناخت جرایم رایانه ای از منظر اسناد بین المللی و قوانین داخلی ،فقه و حقوق ارتیاطات ، تابستان ۱۳۸۹ ، صفحه ۸

[۲] https://www.knowbe۴.com/resources/five-generations-of-cybercrime

گونهای که در اواخر ۱۹۹۰ میلادی فضایی در وب تحت عنوان دارک وب [۱]ایجاد شد که صرفا به فعالیت هایی از قبیل موارد ذکر شده میپردازد. در این میان هر چیزی در دنیای واقعی به دنبال الکترونیکی کردن خود بود. حتی مبادلات تجاری نیز از این قافله عقب نماندند و شبکههای رایانهای و الکترونیکی توانستند تجار را قانع کنند تا به فضای سایبر اعتماد کرده و معاملات خود را در این فضا منعقد سازند و بدین وسیله دست و پای خود را از قید و بندهای فضای حقیقی برهانند. این رویکرد منجر به شکل گیری تجارت الکترونیک گردید.

گفتار دوم: تاریخچهای از جرائم علیه محرمانگی دادهها از طریق سامانهها در ایران

پیدایش رایانه به سال ۱۳۲۰ هجری شمسی بر میگردد اما اولین ورود این تکنولوژی به کشورمان از سال ۱۳٤۰ به بعد به واسطهی نهادهای مهمی همچون دانشگاه تهران و بانک ملی صورت پذیرفت به گونهای که تا اواخر دههی ٤۰ تعداد این رایانهها به ۱۰۰ عدد نیز نمیرسید اما با مرور زمان تعداد این دستگاهها افزایش یافته و اکثر نهادها و ارگانهای مهم را تحت پوشش قرار داد و در دههی ۷۰ در دسترس عموم مردم بود، با گسترش اینترنت در دههی ۸۰ استقبال زیادی از سوی جامعه برای استفاده از این تکنولوژی صورت گرفت، این علاقه و گسترش تکنولوژی تا جایی به پیش رفته است که اکنون بخش عمدهای از زندگی جامعهی مدرن را در برگرفته است، با توجه به سابقهی تاریخی اندک این تکنولوژی در کشور و تصویب قانون در زمینهی این جرایم در سال ۱۳۸۸ واضح است که آمار دقیق و درستی از جرایمی که در اوایل ورود رایانه انجام گرفته است در دست نیست و پس از گسترش جرایمی مانند انتشار فساد و فحشا، اهانت به مقدسات، توهین، سرقت ادبی و...که از رهنمود رایانه و سیستمهای مخابراتی و حاملهای داده صورت میپذیرفت نیاز به نهادهای تخصصی برای مقابله با این جرایم همچون پلیس فتا حس شد که با تصویب قانون در خصوص این جرایم این نهادها نیز به مرور

[۱] Dark Web به شبکهای گفته میشود که در دسترس عموم نبوده و بیشتر برای مقاصد غیرقانونی مورد استفاده قرار میگیرد. ردیابی فعالیتهای آن و شناسایی افراد در آن دشوار یا غیرممکن است. در این شبکه اطلاعات جامعی نهفته شده که افراد ناشناس آنها را مدیریت میکنند. فروشندگان مواد مخدر، هکرها، تروریستها ،قاتل ها و افراد سودجو غالباً این دسته از افراد را تشکیل میدهند. دارک وب بخش کوچکی از دیپ وب یا وب پنهان است.

شکل گرفت و گسترش پیدا کرد به گونه‌ای که روز به روز نیاز به جود این نهادها بیشتر حس می‌شود[۱].

مبحث دوم:مفاهیم و مبانی

باتوجه به فنی و تخصصی بودن موضوع ابتدا ضروری است واژگان و اصطلاحات فنی شناسایی شوند که در ذیل به آنها اشاره می‌گردد.

گفتار اول: جرم و تعریف آن

در زمان‌های گذشته هر عملی توسط شخص یا حتی حیوانی صورت می‌گرفت که موجب آسیب به شخص دیگری می‌شد را جرم و قابل مجازات می‌دانستند. مجازات‌ها نیز در زمان‌های قدیم بسیار متفاوت بوده است به گونه‌ای که افراد بزه کار ممکن بود سر بریده شوند یا از کشور به بیرون انداخته شوند، برای تنبیه حیوانات به سمت آنها سنگ پرتاب می‌کرده اند، همانگونه که مشخص است جرم یک مفهوم متغیر و وابسته به رشد اجتماعی افراد جامعه می‌باشد که به منافع و هم چنین ارزش‌ها و باورهای مشترک آنها وابسته است. اما هرچه زمان می‌گذرد ماهیت و تعریف جرم نیز روشن تر می‌شود. بلکبرن[۲] جرم را اینگونه تعریف می‌کند:اعمالی که موجب مجازات قانونی می‌شوند، آنها جرایمی علیه جامعه هستند، جرایم منجر به عواقبی می‌شود که به نوعی به بفراد جامعه صدمه می‌زند، این عواقب می‌تواند بسیار بی اهمیت یا بسیار مهم باشند، از دیدگاه بلکبرن جنایات به طور کلی توسط جامعه تایید نمی‌شوند زیرا غالبا شامل نقض قوانین اخلاقی هستند که توسط جامعه رعایت می‌شوند[۳].اما نکته‌ی مورد توجه این است که ماهیت جرم به دلیل تحولات موجود در جامعه و محیط در حال تغییر است و نمی‌توان آن را صرفا بر اساس ارزش‌های جامعه تعریف کرد، غالبا جرم انگاری جرایم بر اساس سیاست‌های دولت است که با توجه به ارزش‌های جامعه و در راستای این سیاست‌ها صورت می‌گیرد، اما آنچه واضح است اینکه مردم نقش مهمی در ممنوعیت و جرم انگاری رفتارها دارند.بنابراین اینکه یک جرم چیست به این

---

[۱] برای مطالعه ی بیشتر رجوع کنید به : فریبرزی ، الهام ، سیر تحول قوانین مرتبط با جرایم رایانه ای در ایران و جهان ، فصلنامه تخصصی فقه و تاریخ تمدن ، سال هفتم ، شماره بیست و هفتم ، بهار ۱۳۹۰

[۲] blackburn

[۳] برای مطالعه ی بیشتر رجوع کنید به Blackburn, R. (۱۹۹۳). *Wiley series in clinical psychology. The psychology of criminal conduct: Theory, research and practice.* John Wiley & Sons

بستگی دارد که از دیدگاه قانونی یا هنجاری به آن نگاه شود، به بیان دیگر آنچه ما به عنوان یک جرم در نظر میگیریم به زمان، جامعه، فرهنگ، سیاست و نوع نگاه به جرم بستگی دارد زیرا جامعه به طور مداوم همراه با ارزشها، اعتقادات و هنجارهای اجتماعی در حال تکامل و تغییر است و این روند به طور قطع بر آنچه بر آنچه که جرم را تشکیل میدهد و به طور کلی جرم تعریف میشود تاثیر خواهد داشت اگرچه مشکلات زیادی در تعریف جرم وجود دارد.

در قانون مجازات اسلامی مصوب ۱۳۹۲ در تعریف جرم آمده است که هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است، بر اساس این ماده مفهوم جرم باید محدود به رفتاری باشد که در قوانین تعریف شده است اما آنچه واضح است این است که هیچ وقت نمیتوان به تعریف دقیق و درست قانون گذار و تمامی مصداق هایی که مشمول این جرم انگاریها در قوانین شده اند پی برد مگر با کمک رویهی قضایی حاکم بر قوانین، در بیان کلی میتوان گفت رویهی قضایی مصادیق مورد نظر قانون گذار را با کمک دکترین و آرا وحدت رویه و نظریههای مشورتی و هم چنین مبانی اصلی حقوق جزا مشخص خواهد کرد.

گفتار دوم: رویه قضایی و مفاهیم مرتبط

رویهی قضایی را میتوان راه و روش یکسان قضات در تصمیم گیری در خصوص دعاوی مشابه نامید، در نظام حقوقی ما رویه قضایی به دو صورت عام و خاص تعریف میشود،رویهی قضایی به معنای عام به مجموعه آرا قضایی صادر شده از دادگاهها در تمامی سطوح گفته میشود که برای سایر محاکم در دعاوی مشابه الزام آور نخواهد بود و منبع حقوقی محسوب نمیشوند، اما رویه قضایی به معنای خاص به آرایی اطلاق میگردد که نسبت به دعاوی مشابه آرا متعارض صادر شده و هیت عمومی دیوان در مقام رفع تعارض اقدام به صدور رای وحدت رویه کرده که اینگونه آرا برای دیگر محاکم الزام آور بوده و به عنوان منبع حقوق محسوب میشوند، نکتهای که در خصوص رویه قضایی مطرح است این است که دادگاهها میدانند که رویه قضایی در معنای عام آن برای آنها الزام آور نخواهد بود اما اکثر قضات به طور اختیاری از این رویهها پیروی میکنند.

به بیان دیگر منظور از رویه قضایی به معنای عام آن روش یکسان و ثابت صاحب منصبان قضایی (قضات) در حل و فصل دعاوی مشابه از جمله در مقام تفسیر قانون در موارد سکوت، تناقض یا اجمال قانون است، این رویه بر دیگر مراجع و مقامات مانند وکلا و نیروهای انتظامی و امنیتی و...نیز

تاثیر دارد [۱]. از آنجایی که در جرایم رایانه‌ای سرعت رشد جرایم بسیار زیاد است و هر روزه شکلی جدید به خود می‌گیرند قانون نمی‌تواند تمام این ابعاد را پیش بینی کرده و قاعده تعیین کند و این امکان نیز جود ندارد که قوانین را به سرعت اصلاح کرد،در نتیجه استفاده از تجربه‌ی گذشته‌ی قضات در رویه قضایی به کمک می‌آید و این ابهامات قانونی را پاسخ می‌گوید.

گفتار سوم: رایانه و مفاهیم مرتبط

در دنیای امروز ما برای همه کارهای خود از رایانه استفاده می‌کنیم. فعالیت‌های روزمره ما: پرداخت قبض، خرید مواد غذایی، استفاده از شبکه‌های اجتماعی، سرگرمی، کار در خانه، برقراری ارتباط با دوست و... همه با استفاده از رایانه[۲] انجام می‌شود. بنابراین نه تنها دانستن چگونگی استفاده از رایانه بلکه شناختن اجزای سازنده رایانه و کار آنها نیز مهم است.رایانه یک وسیله الکترونیکی است که داده‌های کاربر را می‌پذیرد، آنها را پردازش می‌کند، نتایج تولید می‌کند، آنها را برای کاربران نمایش می‌دهد و نتایج را برای استفاده در آینده ذخیره می‌کند.

عملکردهای رایانه‌ها عبارت است از:

دریافت ورودی:داده‌ها از طریق دستگاه‌های ورودی مختلف مانند صفحه کلید، ماوس، قلم‌های دیجیتال و غیره به کامپیوتر وارد می‌شوند. ورودی می‌تواند از طریق دستگاه هایی مانند cd-rom، درایو قلم، اسکنر و غیره نیز تغذیه شود.

پردازش اطلاعات:عملیات بر روی داده‌های ورودی بر اساس دستورالعمل‌های ارائه شده در برنامه‌ها انجام می‌شود.

ذخیره اطلاعات:پس از پردازش، اطلاعات در منطقه ذخیره سازی اولیه یا ثانویه ذخیره می‌شود.

تولید خروجی:اطلاعات پردازش شده و سایر جزئیات از طریق دستگاه‌های خروجی مانند مانیتور، چاپگر و غیره به جهان خارج منتقل می‌شوند.[۳]

---

[۱] کاظمی افشار ، هاجر ،دانشنامه جهان اسلام ، شماره ۲۰ ،رویه قضایی ، ۱۳۹۴ ، صفحه ۸۵۰

[۲] https://techterms.com/definition/computer

[۳] https://revisionworld.com/gcse-revision/ict/computers-data-and-information

الف) داده و حامل‌های داده:

داده‌های رایانه ای[۱] اطلاعاتی است که توسط رایانه پردازش یا ذخیره می‌شود. این اطلاعات ممکن است به صورت اسناد متنی، تصاویر، کلیپ‌های صوتی، برنامه‌های نرم افزاری یا انواع دیگر داده‌ها باشد. داده‌های رایانه ممکن است توسط پردازنده مرکزی رایانه پردازش شده و در پرونده‌ها و پوشه‌ها بر روی دیسک [۲]سخت کامپیوتر ذخیره شود. داده‌های رایانه‌ای در ابتدایی ترین سطح خود دسته‌ای از صفرها هستند که به داده‌های باینری[۳] معروف هستند. از آنجا که تمام داده‌های رایانه در قالب باینری هستند[٤]، می‌توانند به صورت دیجیتالی ایجاد، پردازش و ذخیره شوند. این ویژگی اجازه می‌دهد تا داده‌ها از یک رایانه به رایانه دیگر با استفاده از اتصال شبکه یا دستگاه‌های مختلف رسانه‌ای منتقل شوند. همچنین بعد از چندین بار استفاده، به مرور زمان خراب نمی‌شود یا کیفیت آن از بین نمی‌رود[۵]. هر رسانه‌ای است که توانایی نگهداری داده را داشته باشد، یک حامل داده [٦]محسوب می‌شود، از مصادیق حامل‌های داده می‌توان به سی دی، فلش، هارد، رم اشاره کرد.

ب) سیستم‌های مخابراتی:

ارتباطات از راه دور اصطلاحی جهانی است که برای طیف وسیعی از فناوری‌های انتقال اطلاعات مانند تلفن‌های همراه، خطوط زمینی و شبکه‌های پخش استفاده می‌شود. در ارتباطات از راه دور، داده‌ها به صورت سیگنال‌های الکتریکی معروف به امواج حامل منتقل می‌شوند، که برای انتقال اطلاعات به سیگنال‌های آنالوگ یا دیجیتال تبدیل می‌شوند.مخابرات و پخش از طریق آژانس ملل متحد به نام اتحادیه بین المللی مخابرات (ITU)[۷] در سراسر جهان اداره می‌شوند. اکثر کشورها کمپانی‌های خود را برای اجرای مقررات ارتباط از راه دور دارند. ارتباطات از راه دور به تبادل

---

[۱] Computer data

[۲] Hard disc

[۳] binary

[٤] یک سیستم عددی است که فقط از دو رقم استفاده می‌کند - ۰ و ۱. کامپیوترها به صورت باینری کار می‌کنند ، به این معنی که آنها داده ها را ذخیره می‌کنند و فقط با استفاده از صفر و یک محاسبات را انجام می‌دهند.

[۵] https://techterms.com/definition/data

[٦] Data carriers

[۷] International Telecommunication Union

اطلاعات از طریق ابزارهای الکترونیکی و الکتریکی در مسافت قابل توجهی گفته می‌شود. یک آرایش کامل ارتباط از راه دور از دو یا چند ایستگاه مجهز به دستگاه‌های فرستنده و گیرنده تشکیل شده است. یک تنظیم مشترک از فرستنده‌ها و گیرنده‌ها، به نام فرستنده و گیرنده، همچنین ممکن است در بسیاری از ایستگاه‌های ارتباط از راه دور استفاده شود. دستگاه‌های مخابراتی شامل تلفن، تلگراف، رادیو، تنظیمات ارتباط ریز موج ها[۱]، فیبر نوری، ماهواره و اینترنت هستند.

مبحث سوم: تعریف جرائم رایانه ای

در حال حاضر، اکثر مردم از مفهوم جرایم رایانه‌ای آگاه هستند، اما ممکن است تبعات کامل یا اهمیت زیاد جرایم اینترنتی را درک نکنند. هک به منظور سرقت اطلاعات مالی یا شخصی احتمالاً یکی از شناخته شده ترین انواع جرایم اینترنتی است، هک در واقع زیر مجموعه‌ای از جرم دسترسی غیرمجاز است زیرا هک تنها با استفاده از روش‌های تخصصی و توسط افراد آموزش دیده صورت می‌گیرد در حالی که دسترسی غیرمجاز مفهومی بسیار گسترده دارد که در ادامه به آن پرداخته خواهد شد. حال به یک بررسی اجمالی از جرایم رایانه‌ای پردازیم. به طور خلاصه، جرایم رایانه‌ای هر نوع فعالیت غیرقانونی است که از طریق یا بر روی فناوری‌های رایانه‌ای یا مخابراتی انجام می‌شود. دسترسی غیر مجاز و کلاهبرداری رایانه‌ای از متداول ترین انواع جرایم رایانه‌ای هستند، اما جرایم رایانه‌ای شامل طیف گسترده‌ای از فعالیت‌های مخرب نیز می‌شود، مانند آزار و اذیت اینترنتی یا وارد کردن کرم یا ویروس. جرایم اینترنتی را می‌توان به دو دسته مجزا تقسیم کرد: مواردی که باعث آسیب عمدی می‌شوند و مواردی که باعث آسیب ناخواسته می‌شوند. در بیشتر موارد، این جرایم با ایجاد خسارت مالی همراه هستند اما مواردی نیز وجود دارند که هیچ گونه خسارت مالی به بزه دیده وارد نمی‌گردد بعنوان مثال آزار و اذیت رایانه‌ای و یا دسترسی غیرمجاز بدون هیچ گونه آسیب و یا سو استفاده ای، در این صورت هیگ گونه خسارت مالی وجود ندارد، اما همچنان یک جرم است.در مواردی نیز این خسارت مالی ممکن است در طول زمان ایجاد باشد شود برای مثال شخصی یک ویروس "بی ضرر" را وارد سیستم‌های مرکزی یک شرکت می‌کند و به مرور تجارت را به هر طریقی مختل می‌کند. اگرچه ممکن است همانند سرقت اطلاعات انحصاری یا مالی خسارت مالی فوری نداشته باشد. با

[۱] microwave communication arrangements

توجه به تمامی توضیحات ارائه شده باید ذکر کرد که ارائه‌ی تعریفی دقیق و درست از جـرم رایانـه‌ای در عمل ممکن نمی‌باشد و حتی کنوانسیون جرایم سایبر نیز نتوانسته است تعریفی ارائه دهد و تنها بـه ذکر مصادیق بسنده کرده است، آنچه مشخص است اینکه اختلافات زیادی در تعریف این جرم وجود دارد که این اختلافات نیز به سبب تفاوت‌های زیر ساخت‌های فنی و حقوقی و نظام‌هـای حقـوقی در کشورهای مختلف می‌باشد، همانگونه که مشخص است قانون گذار ما نیز در قـانون جـرایم رایانـه‌ای مصوب ۱۳۸۸ تعریفی از این جرایم ارائه نکرده است و تنها به ذکر مصادیق اکتفا کرده، رویه‌ی قضـایی با کمک دکترین و قوانین بین المللی در زمینه‌ی جرایم رایانه‌ای به رویه‌ی تقریبا واحدی در هر یـک از جرایم رایانه‌ای جرم انگاری شده در این قانون رسیده اند که می‌توان گفت این رویـه قضـایی حـداقل در زمینه‌ی دسترسی غیر مجاز در مصادیق آن هماهنگی زیادی با قوانین کشورهای دیگر داشته کـه در آینده بررسی خواهد شد.

گفتار اول) روش‌های تخصصی منجر به دسترسی غیرمجاز:

هک کردن: هک کردن به بیان ساده هر دسترسی غیرمجاز به یک سیستم رایانه‌ای است. گاهی اوقات، هک کردن می‌تواند نسبتاً بی ضرر باشد، مانند بازنویسی بخش هایی از یک برنامه نرم افزاری موجـود، برای دسترسی به ویژگی هایی که طراح اصلی بـه آنهـا توجـه نداشـته اسـت. هـک کـردن یکـی از پرکاربردترین موارد جرایم اینترنتی است، اما همه هکرها مجرم نیستند. برخی از هکرهـا کـه اغلـب از آنها به عنوان هکرهای "کلاه سفید"[۱] یاد می‌شود، توسط شرکت‌های نرم افزاری استخدام می‌شـوند تـا ایراداتی را در سیستم خود پیدا کنند تا قبل از "کلاه سیاه"[۲] یا هکرهای جنایتکار بتوانند آنها را برطـرف کنند.

ویروس‌ها، کرم‌ها، بدافزارها: انواع مختلفی از نرم افزارهای مخرب را می‌توان از طریق طیـف وسـیعی تحویل داد. در مورد بیشتر ویروس‌ها، آنها باید به نوعی روی یک هـارد دیسـک بـارگیری شـوند. در حملات هدفمند، یک قربانی ممکن است ایمیلی با ظاهری ساده و بدون ایراد دریافت کند که ظاهراً از یک همکار یا فرد معتمد حاوی پیوندی برای کلیک کردن یـا بـارگیری اسـت. در مـوارد دیگـر، وب سایت‌ها ممکن است حاوی پیوندهای آلوده باشند که با کلیـک روی آنهـا کـرم‌هـا یـا ویـروس‌هـا را

[۱] White Hat Hacker

[۲] Black Hat Hacker