بسم الله الرحمن الرحیم

عنوان : پیشگیری از وقوع جرایم رایانه ای

نویسنده : مهرداد بوستانچی دانشجوی کارشناسی ارشد حقوق جزا وجرم شناسی

منتشر شده در پایگاه نشر مقالات حقوقی،حق گستر

چکیده

. امروزه هیچ حوزه‌ای از تأثیر و مداخله رایانه مصون نیست و شاید گزافه نباشد که در جهان حاضر، هرکسی کار با رایانه را نیاموخته باشد، یک بیسواد نوین است. حال صحبت ما این است که چگونه و از طریق چه راههای می توان از اینگونه جرایم پیشگیری کرد وجلو انرا گرفت چون درصورت ارتکاب ان اثرات جبران ناپذیری برای مفعولین این جرم به همراه داردکه از جمله رفتن آبروی این اشخاص ودر خیلی از موارد بردن مال انها را در پی داردکه در این مقاله سعی شده راهکارهایی برای پیشگیری وپیش بینی وقوع این جرایم مطرح گردد تا بتوان از وقع آنها واثرات جبران ناپذیری که آنها دارن جلوگیری کرد چون به نظر میرسد کسانی که اقدام به ارتکاب این جرایم میکنند اشخاصی هستند که اطلاع کامل از اینترنت وکامپیوتر دارند واین جرایم هیچگاه نمیتوان با سهو وخطا اتفاق افتد

کلید واژگان: جرایم اینترنتی- پیشگیری از وقوع جرم – پیش بینی وقوع جرم

مقدمه

جرایم رایانه ای جرمی است وارداتی که با ورود کامپیوتر در استفاده از اینترنت در سطح گسترده در کشور رواج پیدا کرده است ورود اینترنت به کشور از سال ۱۳۷۰و آغاز شد ودر سال ۱۳۷۲ به تکامل رسد امادراین چند سال نبود قاونی مدون باعث گردید که بسیاری از مجرمین رایانه ای از زیر مجازات فرار کنند وبه جرایم خود ادامه دهند واستناد انها نیز به اصل برائت واصل قانونی بودن جرم ومجازات بود که استناد درستی هم بودبا تصویب قانون جرایم رایانه‌ای (۱۳۸۸)، مفاهیم وجرایم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشدوقتی در خصوص فناوری بحث می‌شود، نمی‌توان رایانه را نادیده گرفت. رایانه هم خود بزرگ ترین فناوری عصر حاضر است و هم سایر فناوری‌های نوین یا به وسیله آن و یا بر بستر آن شکل می‌گیرندالبته فناوری‌ها در کنار مزایای خود می‌توانند بسترساز سوءاستفاده‌هایی نیز باشند. به خصوص اگر این فناوری، رایانه باشد، دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه‌ای باشد، دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه‌ای طرف است. ماهیت و ویژگی این دسته از جرایم به نحوی اساسی با جرایم سنتی تفاوت دارد. امروزه، مجرمان رایانه‌ای در مکان‌هایی به غیر از نقاطی که آثار و نتایج اعمال

آنها ظاهر می‌شود، قرار دارند. در صورتی‌که کارایی قوانین جزایی موجود و متداول، منحصر به قلمرو خاصی است و به دلیل آنکه اجزای عنصر مادی کاملاً یا بعضاً تغییر یافته و برخی عناوین مجرمانه تازه هم به وجود آمده است، نمی‌توان مجرمان را با قوانین قبلی محاکمه کرد.

.

جرم رایانه ای چیست ؟

جرایم اینترنتی ورایانه ای نوعی جرایم جدید می باشدطیف گسترده افعال مجرمانه‌ای که ذیل این مفهوم جا دارند و ماهیت متغیر آنها که ناشی از پیشرفت لحظه به لحظه فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است ارائه تعریف جامع و مانع و خالی از مناقشه را مشکل و چه بسا غیرممکن می‌سازد؛ تا آنجا که در جدیدترین و جامع‌ترین سند بین‌المللی موجود در این زمینه (کنوانسیون جرایم سایبر ۲۰۰۱ بوداپست) تعریفی از این جرایم به عمل نیامده است. به نظر میرسد کامل ترین تعریف این باشد. تعریف بسیار موسع جرایم رایانه ای:

«هر جرمی که قانونگذار به صراحت رایانه را به منزله موضوع یا وسیله جرم جزءِ رکن مادی آن اعلام کرده باشد، یا عملاً رایانه به منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد».

این تعریف هم علاوه بر جرایم ذکر شده در دو دسته قبل، جرایمی را نیزکه صرفاً دلایل آنها یا اطلاعات مربوطه در رایانه ذخیره شده‌اند، به لحاظ تأمین بهتر اهداف تحقیق و تعقیب جرم با در نظر گرفتن قواعد خاص آیین دادرسی کیفری، جزء جرایم رایانه‌ای دانسته است

۱- جرایم رایانه‌ای محض: جرایمی که ارتکاب آنها قبل از پیدایش رایانه و اجزای فناوری اطلاعات امکان پذیر نبوده‌اند؛ مانند دسترسی غیرمجاز.

۲- جرایم رایانه‌ای سنتی: که ارتکاب آنها وسیله رایانه دارای عواقبی بسیار شدیدتر نسبت به ارتکاب سنتی آن است؛ مانند برخی جرایم مرتبط با محتوا مانند هرزه‌نگاری و یا تخریب فیزیکی نسبت به کامپیوتر

قانون جرایم رایانه ای: مصوب ۱۳۸۸/۳/۵مجلس شورای اسلامی

لازم الاجراء از ۱۳۸۸/۵/۱ حاوی ۵۶ ماده

۲۹ عنوان مجرمانه

مبحث اول :دسترسی غیر مجاز مبحث دوم : شنود غیر مجاز مبحث سوم :جاسوسی رایانه ای

فصل دوم:جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی

مبحث اول:جعل رایانه ای

مبحث دوم: تخریب و اختلال در داده ها یا سامانه های رایانه ای و مخابراتی

فصل سوم:سرقت و کلاهبرداری مرتبط با رایانه فصل چهارم:جرائم علیه عفت و اخلاق عمومی

فصل پنجم:هتک حیثیت و نشر اکاذیب

فهرست مصادیق محتوای مجرمانه موضوع ماده ۲۱ قانون جرایم رایانه ای

۱-محتوا علیه عفت و اخلاق عمومی ۲- محتوا علیه مقدسات اسلامی ۳- محتوا علیه امنیت و آسایش عمومی

۴-محتوا علیه مقامات و نهادهای دولتی و عمومی ۵- محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی

۶- محتوای که تحریک ، ترغیب ، یا دعوت به ارتکاب جرم می کند (محتوای مرتبط با سایر جرایم)

دکتر فیضی چکاب استاد دانشگاه علامه طباطبایی اینتر نت و رایانه رابطه مساوی با یکدیگر ندارند. زمانیکه بحث از جرایم اینترنتی شود مسلما در عرصه فراتر از مرزها صحبت به میان می آید

بر اساس قانون، اعضای کارگروه مرکب از وزارتخانه های ارتباطات و فناوری اطلاعات ـ اطلاعات ـ فرهنگ و ارشاد اسلامی ـ آموزش و پرورش ـ سازمان تبلیغات ـ ناجا ـ صدا و سیما و...) در راستای وظایف و مأموریتهای ذاتی خود مکلف به ایجاد سامانه رصد فضای مجازی در دستگاه متبوع خود بوده و همچنین کلیه ارائه دهندگان خدمات دسترسی و میزبانی نیز مکلف خواهند بود چنانچه با یکی از مصادیق مصرحه در این فهرست مواجه شدند، بلافاصله مراتب را به دبیرخانه مستقر در دادستانی کل کشور از طریق سایت دادستانی به آدرس www.dadsetani.ir یا آدرس الکترونیکی dadsetani@dadsetani.ir اعلام نمایند.»

وی در ادامه افزود: «رعایت مقررات فهرست مصادیق محتوای مجرمانه برای ارائه دهندگان خدمات دسترسی و میزبانی و کلیه کاربران در فضای مجازی لازم است و در صورت تخطی طبق مقررات برخورد خواهد شد.»

دبیرخانه کارگروه با بررسی گزارشات واصله نسبت به مجرمانه بودن یا نبودن، تصمیم نهایی را اتخاذ و در صورت احراز محتوای مجرمانه نسبت به پالایش (فیلتر) اقدام خواهد نمود و مراتب از سوی دبیرخانه به مراجع قضائی ذیربط جهت تعقیب کیفری مقتضی اطلاع داده خواهد شد.» در این راستا شورای عالی اطلاع‌رسانی ـ شورای عالی انقلاب فرهنگی ـ شورای عالی فن‌آوری اطلاعات، وزارت ارتباطات و فناوری اطلاعات و دفتر اینترنت دادستانی تهران، برنامه‌ریزی‌های مشترکی را برای مدیریت اینترنت و شبکه‌های اطلاع‌رسانی به انجام رسانیده‌اند.

از آنجا که امروزه یکی از راههای کنترل تخلفات اینترنتی و اعمال نظارت، ایجاد دیواره آتشین و بحث فیلترینگ است و این روش در بسیاری از کشورها با امعان نظر به مصالح عمومی و منافع ملی از طریق نرم افزارهای مناسب معمول می‌شود و کشورها خود را در برابر پیامدهای امنیتی ـ فرهنگی و اخلاقی و سیاسی فضای سایبر واکسینه می‌کنند. (ولو به‌صورت تسکینی و موقت) ما

نیز باید با دیدی وسیع و آینده‌نگرانه برای این مسأله تدبیر کنیم و تهدیدها را به فرصت مغتنمی برای رشد و توسعه و بالندگی و تبیین و تبلیغ آرمان‌های نظام اسلامی مبدل کنیم.مجموعه مقررات پالایش و فیلترینگ مراکز اینترنتی مصوب سال ۱۳۸۱ شورای عالی انقلاب فرهنگی نیز در راستای اعمال کنترل و نظارت دقیقتر بر مراکز اینترنتی و اعطای مجوز به مراکز مذکور در چارچوب ضوابط نظارتی توسط وزارت ارتباطات و فن‌آوری اطلاعات از جمله اقدام‌هایی است که در سال‌های گذشته انجام شده است.

پیشگیری از وقوع جرایم رایانه ای

۱- نقش دادستان برای پیشگیری از وقوع جرایم رایانه ای: واقعبینانه باید در نظر داشت که استفاده از بسیاری اهرم‌های اعمال روش‌های پیشگیرانه در دسترس ما نیست چرا که اساساً این فن‌آوری، یک فن‌آوری وارداتی است و ما در برابر جریان یکطرفه‌ای قرار گرفته‌ایم که از خیلی جهات دست ما را برای اعمال اراده بسته است، اما در عین حال از روش کنترل و نظارتی فیلترینگ می‌توان به عنوان یک اقدام پدافندی تا حدودی بازدارنده استفاده کرد؛ چنانچه بموجب مصوبه شورای عالی انقلاب فرهنگی، شماره ۵۹ مورخ ۱۰دی سال ۸۱، کمیته‌ای تحت عنوان «کمیته تعیین مصادیق پایگاه‌های اطلاع‌رسانی رایانه‌ای غیرمجاز» مرکب از نمایندگان وزارت اطلاعات، وزارت فرهنگ و ارشاد اسلامی، سازمان صدا و سیما، نماینده دبیرخانه شورای عالی انقلاب فرهنگی و نماینده سازمان تبلیغات اسلامی با مسئولیت نماینده وزارت اطلاعات و برای بررسی و احراز مصادیق فعالیت‌های غیرمجاز در عرصه سایبر تشکیل شد تا اعمال فیلترینگ با توجه به جمیع جهات فرهنگی، امنیتی و غیره مورد بهره‌برداری قرار داده شود.

اگرچه بنظر می‌رسد این کمیته از آنجا که ماهیت غیرقضایی دارد، نمی‌تواند موجب اعطا یا سلب حق از اشخاص باشد، چرا که فیلتر کردن یا رفع فیلترینگ سایت، باید صرفاً با مجوز مقام ذیصلاح قضایی انجام شود.

بنابراین نظارت استصوابی مقام ذیصلاح قضایی بر تصمیمات کمیته مذکور ضروری می‌کند تا در صورت تأیید تشریفات قانونی و رعایت ضوابط، نظر کمیته را تنفیذ و تأیید کند.

شایان ذکر است در مجموعه مقررات پالایش و فیلترینگ ۱۴ عنوان مجرمانه از جمله توهین به مقدسات، اشاعه فحشا و نشر اکاذیب و توهین به علما و مسئولان قید شده است.

علاوه بر این، عناوین مجرمانه‌ای در قوانین جاری از جمله مواد ۶۳۹ و ۶۴۰ قانون مجازات اسلامی آمده است.

اگرچه اعمال کنترل و نظارت قضایی ـ امنیتی و پلیسی در گستره کشوری، هر یک تعریف و مبنای قانونی خاص خود را دارد ، اما بنظر می‌رسد این کنترل و نظارت از حیث قضایی در وهله نخست متوجه دادسرا است؛ چرا که دادسرا باید به عنوان نهاد کشف و تعقیب، مترصد به انجام اقدامهای لازم برآید و در برابر جرایم مشهود توسط ضابطان یا گزارش ثالث یا حتی اخذ نظر از کارشناس، مبادرت به انجام روند قضایی مقتضی کند.

همچنین در مواردی که جرم دارای جنبه عمومی است و از جمله جرایم فضای سایبر که در معرض دید میلیون‌ها انسان قرار دارد و از مختصات و ویژگی‌های جرم عمومی برخوردار است به نیابت از جامعه از حقوق ایشان صیانت و نقش مدعی‌العمومی خود را در این پروسه ایفا کند.

البته این موضوع چون کاملاً ماهیتی مرکب (اعم از فنی و حقوقی و قضایی) دارد باید توسط اشخاص صاحب صلاحیت در حوزه‌های مذکور مورد توجه قرار گیرد، اما بنظر می‌رسد نقش دادستان به عنوان مرجع صیانت از حقوق عمومی و مقام تعقیب، کلیدی و محوری است.

با عنایت به این‌که رسالت پیشگیری از وقوع جرم نیز از جمله وظایف مقرر در بند ۵ اصل ۱۵۶ قانون اساسی است و بطور خاص براساس رویه قضایی و اختیارات مفوضه رئیس قوه قضاییه، متوجه دادستان کل کشور است، بنظر می‌رسد دادستان کل که مدعی‌العموم با صلاحیت کشوری است، مقام ذیصلاح برای ورود به مسأله سالم کردن فضای سایبر و پیشگیری از بروز جرایم در این فضا است.

علاوه بر این، موضوع نظارت دادستان بر حسن جریان امور و از جمله مفاد اصل ۱۶۱ قانون اساسی و ماده ۱۷ قانون اصلاح پاره‌ای از قوانین دادگستری دال بر ایفای وظیفه ذاتی نظارت دادستان کل بر دادسراهای سراسر کشور، مقوم و مؤید این نظریه است.

بر همین اساس دادستانی کل کشور طرح تشکیل ستادی تحت عنوان «ستاد پیشگیری و مبارزه با جرایم فن‌آوری اطلاعات»را محضر ریاست قوه قضائیه ارائه کرد که بموجب آن، این ستاد در گستره کشوری مبادرت به ایجاد وحدت رویه قضایی در مواجهه با موارد مجرمامه مذکور کرده است و همچنین در زمینه پیشگیری از وقوع جرایم در فضای سایبر ارائه طریق خواهد کرد

۲– پلیس فتا پلیس فضای تولید و تبادل اطلاعات ایران با نام مختصر فتا، یک واحد تخصصی نیروی انتظامی جمهوری اسلامی ایران است که وظیفه آن مقابله با جرایم اینترنتی، کلاهبرداری و جعل در فضای سایبر و حفاظت از اسرار ملی بر روی شبکه اینترنت است. این واحد در ۳ بهمن ۱۳۸۹ (۲۳ ژانویه ۲۰۱۱) به فرمان اسماعیل احمدی مقدم فرمانده نیروی انتظامی ایران شروع به کار کرداین اقدام را می‌توان واکنش پلیس به انتشار کرم رایانه‌ای استاکس نت و همچنین مقابله با کنترل فضای سایبر توسط مخالفان حکومت ایران (بعد از ناآرامی ایران پس از اعلام نتایج انتخابات ۱۳۸۸) دانست. و ایجاد آن در مراکز استان ها برنامه

امسال ناجا است.گسترش پلیس فتا در شهرهای بزرگ کشور نیز از برنامه های سال آینده ناجا است. حوزه فعالیت این پلیس برخورد با جرائم سایبری نظیر مسایل اخلاقی، اقتصادی و حتی تروریسم است. ایجاد پلیس «فتا» به معنای ایجاد محدودیت برای مردم و ایجاد مداخله در حریم خصوصی آنها نیست بلکه پیش‌بینی جرایم جدید در حوزه‌های جدید اینترنتی و پیشگیری اجتماعی است. پلیس فتا ابتدا در تهران راه‌اندازی شد، اما آمایش سرزمینی پلیس فتا در سراسر کشور در سال ۹۰ اجرا می‌شود و در ۳۲ استان کشور پلیس فتا رونمایی خواهد شد.

۳- **نقش مردم در پیشگیری از وقوع جرایم رایانه ای**: مردم خودشان اطلاعات خود را در فضای مجازی فاش می کنند به عبارتی اشخاصی هستند که از اینترنت اطلاع کافی ندارن وبدون اطلاع اقدام به چت کردن با افراد نا آشنا می نمایند این اشخاص اطلاعات شخصی خودشان را در معرض دسترسی این افراد قرار میدهند به این گونه که توسط افراد متخصص هک شده واطلاعات شخصیشان در اختیار انها قرار میگیرد پس در فضای مجازی باید بسیار حواسمان را جمع کنیم همچنین گاهی اوقات برای خرید یک محصول از یک سایت رمز عبور کارت شتاب خود را در اختیار متصدیان سایت قرار داده وسبب میشوند که از کارت انها پول برداشت شود همچنین میبایست پس از اقدام به پرداخت های اینترنتی از جمله شهریه وقبوض رمز خودرا بر روی سیستم قرار نداده ویا حذف نماییم که مورد سوء استفاده دیگران قرار نگیرد .

۴– نصب آنتی ویروسها ونرم افراز هایی که وظیفه حذف یا جلوگیری از ورود کرمهای اینترنتی دارند برای جلوگیری از دزدی اطلاعاتخیلی از ویروسها و کرم های اینترنتی هنگامی که وارد کامپوتر میشوند سیست امنیتی را از کار میاندازند واقدام به دادن اطلاعات شخص دریافت کننده به شخص فرستنده ویروس مینمایند که از طریق آنتی ویروس ها وضد کرم هایاینترنتی که به روز شده اند میتوان از ورود آنها وسرقت دادها جلو گیری کرد

۵- **اقدامی که جدیدا توسط وزارت بازگانی صورت گرفته** سایت های اینترنتی امور بازرگانی ساماندهی شده و تحت نظارت پلیس فضای تولید و تبادل اطلاعات ناجا (فتا) قرار می گیرند.

، به منظور کنترل و نظارت بر روی سایت های اینترنتی که در امور بازرگانی فعال بوده و خدمات اینترنتی به کاربران ارائه می دهند، جلساتی میان پلیس فتا و وزارت بازرگانی برگزار شد. شرکت های ارائه دهنده خدمات اینترنتی و فعال در امور بازرگانی تحت نظارت پلیس قرار گرفته و ساماندهی شوند.

همچنین سایت هایی که اقدام به فروش دامنه های فارسی می کنند، ازسوی پلیس فتا مجاز شناخته شدند، اما باید کاربران از مدیریت سایت و نحوه فعالیت آنها اطمینان حاصل کنند. این گونه سایت ها نیز به زودی تحت نظارت و پوشش پلیس قرار می گیرند.

۶– ارتش سایبری ایران(هک کردن سایت های که برخلاف قانون جرایم رایانه ای عمل میکنند) نام ارتش سایبری ایران زمانی بر سر زبان‌ها افتاد که در اولین حمله سایت توئیتر را مورد حمله قرار داد و در پیامی که در سایت قرار داده بود، از حمایت از اغتشاش در ایران توسط توئیتر انتقاد کرده بود. در پیام هکرها آمده بود: «آمریکا فکر می‌کند که دارد اینترنت را با دسترسی‌اش کنترل و مدیریت می‌کند، اما این طور نیست؛ این ما هستیم که اینترنت را با قدرت‌مان کنترل و مدیریت می‌کنیم. بنابراین، سعی نکنید مردم ایران را تحریک کنید نامی است که افراد نامشخصی برای فعالیت‌های غیرمتعارف خود روی

اینترنت به کار می‌برند. درباره این گروه اطلاعات چندانی در دسترس نیست، اما برخی منابع احتمال وابستگی آن به دولت ایران را مطرح کرده‌اند. این گروه به چندین وب سایت آمریکایی و چینی و همچنین وب‌گاه‌های حامی جنبش سبز و مخالف دولت جمهوری اسلامی ایران، حمله کرده‌است. طرح تشکیل ارتش سایبری ایران از سال ۸۴ در سپاه مطرح شد، اما با افزایش تبلیغات علیه دولت نهم در اجرای آن تسریع به عمل آمد. مدتی بعد گروهی بسیار وسیع تشکیل شد که تعداد اعضای آن از چند نام بسیار فراتر می‌رفت برخی گانه‌زنی‌ها از ارتباط مرکز مبارزه با جرائم سازمان یافته سپاه با این گروه خبر می‌دهد. در اردیبهشت ۱۳۸۸ نیز خبرگزاری فارس گزارش داد مؤسسه «Defense Tech» که از مؤسسات نظامی و امنیتی ایالات متحده آمریکا است، با استناد به آمار دریافتی از سازمان اطلاعات آمریکا، ایران را جزء پنج کشور دارای قوی‌ترین نیروی سایبری معرفی کرده‌است. این مؤسسه با تاکید بر اینکه ارتش سایبری ایران زیرمجموعه تیم رصد سایبری سپاه است، بودجه آن را ۷۶ میلیون دلار اعلام کرده بود.[۴] این موسسه همچنین تعداد نیروهای این ارتش را بیش از ۲۴۰۰ نفر و ۱۲۰۰۰ نفر ذخیره برآورد کرده بود.

اقدامات ارتش سایبری ایران

روز ۲۵ آذر ۱۳۸۸ وب‌گاه موج سبز آزادی هک شد

صبح روز جمعه، ۲۷ آذر ۱۳۸۸ به وقت ایران امکان دسترسی به وب‌گاه توییتر در برخی از نقاط دنیا قطع شد

روز ۱۰ بهمن ۱۳۸۸ ارتش سایبری ایران وب‌سایت رادیو زمانه را هک کرده،

ارتش سایبری ایران در پیامی در رادیو زمانه که وابسته به دولت هلند است، آورده:« ارتش سایبری ایران به تمام مزدوران وطن فروش هشدار می‌دهد که در دامان اربابان خود نیز آن‌ها را راحت نمی‌گذارد

اطلاعات دریافتی حاکی از آن است که این حمله از ابعاد گسترده‌ای برخوردار بوده و ظاهراً باعث شده که کلیه اطلاعات این وب‌سایت از روی سرور آن پاک شود

. در ۲۳ بهمن ۱۳۸۸ سایت جرس نیوز که اخبار جنبش سبز را منتشر می‌کند توسط ارتش سایبری هک شد

در آبان ۱۳۸۹ ارتش سایبری ایران وبسایت تلویزیون فارسی ۱ را به همراه تعداد زیادی از وبسایت های مرتبط با گروه موبی از جمله تلویزیون طلوع، تلویزیون لمر، رادیو آرمان و .. را هک کرد.پس از حک سایت شبکه تلویزیونی فارسی ۱ این پیام در صفحه اول سایت این شبکه توسط ارتش سایبری ایران قرارگرفت رابرت مرداک وشرکای صیهونیستش بدانندکه ارزوی تخریب بنیان خانواده هارا در ایران به گور میبرند.

۷–اطلاع رسانی به مردم در رابطه با جرایم رایانه ای: بایستی سعی کرد درجامعه آگاهی مردم رادرموردجرایمی که توسط رایانه اتفاق میافتد افزایش داد چون بسیاری از کسانی که مورد سوءاستفاده رایانه ای قرار میگیرند اشخاصی بی اطلاع هستند که فکر میکنند محیط اینتر نت فضای امن میباشد می بایست طی برنامه هایی که از تلویزون پخش می شود وجود این جرایم ونحوه انجام آن به مردم گوشزد شود تا در فضای اینترنت به هیچ شخص حقیقی ویا هیچ سایتی اطمینان نکنندو همیشه بر روی اینترنت مواظب اطلاعات شخصی که روی کامپیوتر خود دارند باشند به نظر خود من کاربردی ترین راه برای پیشگیری از

وقوع جرایم رایانه ای اطلاع رسانی ومصاحبه با مال باختگان رایانه می باشد کسانی که یا مال یا دادهایشان بر روی اینترنت به سرقت رفته است یا مورد سوءاستفاده واقع شده اند این باعث آگاهی برای مردم شده وسبب پیشگیر ی از وقوع جرایم رایانه ای میگردد

نتیجه گیری

جرایم رایانه ای جرایمی سازمان یافته می باشند که از طریق اشخاص حرفه ای وبا سواد انجام میشوند و همیشه قصد آنها سوء استفاده از اشخاص دیگر می باشد با توجه به طیف گسترده جرایم واصل قانونی بودن جرایم ومجازات ها قوانین رایانه ای امروزه برای مجازات مجرمین کافی اما کامل نمی باشد چون هر روز جرایم جدیدی به وجود می آید که برای مجازات آنها نیاز به قوانین جدید داریم همانگونه که جرایم اینترنتی همیشه درحال روز شدن هستند بایستی تلاش کرد تابتوان با نو شدن جرایم هرساله قوانینی را که در زمینه جرایم جدید قابل اعمال باشد ارائه کرد چون رایانه واینترنت همیشه وهمیشه شکل ها ی مختلفی به خود می گیرند برای پیشگیری از این جرایم می بایست همه دستگاهها تلاش کنند ومردم نیز توصیه های مسئولین را در این مورد جدی بگیرند ودر هنگام استفاده از اینترنت و رایانه مورد استفاده قرار دهند تا مورد سوء استفاده دیگران قرار نگیرند .همچنین اگر دیدند سایت یا وبلاگی برخلاف قوانین تعیین شده در حال ارائه مطلب می باشد موضوع راسریعا به دادستانی اطلاع تا نسبت به اعمال فیلتر درمورد آن سایت اقدام شود قضات نیز می بایست به شدت با کسانی که اقدام به جرایم رایانه ای می کنند برخود نمایند چون این جرایم هم سبب بردن مال وهم سبب بردن ابروی اشخاص میگردد برخورد قضات نیز درپیش گیری از وقوع جرم اهمیت دارد بایست سعی شود در زمینه جرایم رایانه ای مجازات ها بازدارندگی بیشتری داشته باشد تا هم سبب ارعاب مردم وهم سبب عبرت گرفت مجرمین شود تا دیگر اقدام به به چنین جرایمی ننمایند .

در بعضی از مواد مربوط به جرایم رایانه ای حبس های ۹۱ روز پیش بینی شده که به نظر من این نشان دهنده میل قانون گذار به حبس اشخاصی می باشد که اقدام به جرایم رایانه ای می نمایند .

چون جرایم رایانه ای توسط اشخاص با سواد وهمیشه با آگاهی انجام می شودپس میبایست در محاکمه مجرمین نهایت سعی وتلاش را بنماییم تا نتوانند از چنگال قانون فرار کنند چون این افراد کسانی هستند که یا خیلی زیرک

میباشند یا اینکه وکلای کار کشته ای برا دفاع از خود انتخاب می کنند که در بیشتر موارد با توجه به نبود قانون خود را ازچنگال قانون ومجازات فراری دهند.

منابع وماخذ

رضوی، محمد، « جرایم سایبری ونقش پلیس در پیشگیری از این جرایم وکشف آنها »، فصلنامه دانش انتظامی، سالن نهم، ش ۱، ، قانون جرایم رایانه‌ای مصوب۱۳۸۸

طارمی‌محمد حسین، گذری بر جرایم رایانه‌ای ۱۳۸۷، به نقل ازPegahhawze.com

سایت های اینترنتی

www.gerdab.ir
www.hamshahrionline.com
www.jamejamonline.com
www.wikipedia.com
http://hodarayaneh.org
www.melatonline.com
www.iclub.ir
www.farsnews.com
www. saleh.ruhollah.org