دومین کنفرانس ملی
راهکارهای توسعه و ترویج آموزش علوم در ایران
2nd National Conference
on Strategies for promoting science education in Iran
۱۸ تیرماه ۱۳۹۵
8 July 2016
Galedar - Iran
گله دار - ایران

مروری برجرایم سایبری (با تأکیدبرقوانین مجازات رایانه ای)

لیلا حقیقی

دانشجوی کارشناس ارشد حقوق،گرایش جزا وجرم شناسی دانشگاه آزاداسلامی واحد ابرکوه،یزد،ایران

Email: (Leilahaghighi77@yahoo.com)

چکیده

هدف ازنگارش این مقاله مروری بر جرایم رایانه ای یا جرایم سایبری می باشد. دراواسط دهه ۹۰با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم کامپیوتری، تحت عنوان جرایم سایبری(مجازی)یا جرایم در محیط سایبر شکل گرفته‌است .به این ترتیب جرایم اینترنتی را می‌توان مکمل جرایم کامپیوتری دانست، بخصوص اینکه جرایم نسل سوم کامپیوتری که به جرایم در محیط مجازی معروف است، غالباً از طریق این شبکه جهانی به وقوع می‌پیوندد. این مقاله که ابزار جمع آوری اطلاعات آن روش کتابخانه ای است به روش توصیفی - تحلیلی به بررسی جرایم سایری یا رایانه ای می پردازد وسعی شده است ابتدا مفاهیم ارائه شده و سپس تجزیه و تحلیل می‌شود و در پایان پیشنهادهایی به منظورامنیت بیشترکاربران ارائه می‌گردد.

کلمات کلیدی: جرایم سایبری،جرایم رایانه ای ،جرایم اینترنتی.،قوانین مجازات رایانه ای.

مقدمه

تعریف فضای سایبر[1]:فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. و بهترین معادل فارسی آن فضای مجازی است.

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح (سایبرنتیک) توسط ریاضیدانی به نام نوربرت وینر [2]در کتابی 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 سیستم‌های انسانی، ماشینی (و کامپیوتر ها) است.

سایبر پیشوندی است برای توصیف یک شخص، یک شی، 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 که به تعدادی از آنها اشاره می کنیم:

فضای سایبر(Cyberspace)، حقوق سایبری [3]، شهروند سایبر [4]، پول سایبر [5]، فرهنگ سایبر [6]، جرایم سایبری [7]، راهنمایی فضای [8]سایبر ، تجارت سایبر [9]، کانال سایبر [10]و ....

واژه فضای سایبر نخستین بار ویلیام گیبسون [11]نویسنده داستان علمی تخیلی در کتاب نورومنسر [12]در سال ۱۹۸۴ به کار برده است.

فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

یک سیستم آنلاین یا یک تلفن همراه یا یک دستگاه خودپرداز نمونه ای از فضای سایبر است که کاربران آن می‌توانند از طریق آن با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد.

این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهت‌های فضای سایبر با حالت های نا هشیاری، بخصوص حالت‌های ذهنی‌ای که در رویا ها ظاهر می‌شوند، بپردازند.

تعریف جرایم رایانه ای

پروفسور اولریش زیبر یکی از صاحب نظران معروف حقوق جزای رایانه معتقد است امروزه اجماع بین‌المللی براین است که جرم رایانه‌ای باید به طور کامل تعریف شود.

---

[1] Cyber space
[2] Norbert Wiener
[3] cyber law
[4] Cybercitizen
[5] Cyber cash
[6] Cyber culture
[7] cyber crime
[8] Cyber Coach
[9] Cyber business
[10] channel Cyber
[11] William Gibson
[12] Neuromancer

بنابراین تعریف کامل پذیرفته شده توسط گروه متخصصان oecd در سال ۱۹۸۳میلادی اصطلاح جرم رایانه‌ای بدین ترتیب تعریف شده: هرگونه رفتار غیرقانونی، غیراخلاقی یا غیرمجاز که مشتمل بر داده‌پردازی اتوماتیک یا انتقال داده‌ها باشد. مطالعات جدید مفاهیم وسیع‌تر و پیشرفته‌تری را از مجرمیت داده‌ها، یا جرم اطلاعاتی ارائه می‌کند.

پروفسورشیک یکی از حقوقدانان برجسته اتریشی در تعریف جرم رایانه‌ای چنین می‌گوید: جرم رایانه‌ای به هر عمل مجرمانه‌ای گفته می‌شود که در آن رایانه وسیله یا هدف ارتکاب جرم باشد.

برخی معتقدند گوناگونی تعاریف ارائه شده از جرم رایانه‌ای ناشی از اختلاف در دیدگاه‌هاست. برخی آن را ناشی از تفاوت در میزان دانش و آگاهی صاحب نظران می‌دانند؛ اما به نظر می‌رسد مشکلات موجود در تعریف جرم رایانه‌ای بیشتر از ماهیت این جرم ناشی می‌شود چگونه می‌توان تعریفی جامع و کامل از جرمی ارائه کرد که طیف وسیعی از اعمال، از نوشتن یک نامه توسط کارمند در رایانه‌ای گرفته تا بهره برداری از رایانه برای اختلاس میلیون‌ها دلار، را دربرگیرد.

هنوز این مجادلات پیرامون جرایم رایانه‌ای در میان صاحب نظران ادامه داشت. که با بروز اینترنت نوع دیگری از جرایم با عنوان جرایم اینترنتی مطرح گردید. و هنوز این واژه به بحث و مناظره در محافل علمی و تخصصی کشیده نشده بود که واژه جدیدی از جرایم رایانه‌ای تحت عنوان جرم سایبر در حال شکل گیری بود. پیدایش و شیوع جرایم تحت عنوان جرم سایبر بر پیچیدگی و دشواری ارائه تعریف کامل از جرم رایانه‌ای افزود و خود به مشکلی نو بدل شد.

تعریف گسترده جرایم رایانه ای و جرایم اینترنتی و جرایم سایبری

تا کنون تعاریف گوناگونی از جرم رایانه ای از سوی سازمان ها ومتخصصان ارائه شده که وجود تفاوت بیانگر ابهامات موجود درماهیت و تعریف این نوع از جرایم است. جرم رایانه ای یا جرم در فضای مجازی (سایبرکرایم) دارای دو معنی است.

جرم رایانه ای عبارت از جرایمی است که در فضای سایبر رخ می دهد . و در تعریف گسترده :

هر فعل یا ترک فعلی که در و یا از طریق یا به کمک رایانه یا از طریق اتصال به اینترنت ، چه به طور مستقیم یا غیرمستقیم رخ می دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده است ، جرم رایانه ای نامیده می شود.

با توجه به این تعریف جرایم رایانه ای را می توان به سه دسته تقسیم کرد :

دسته اول : جرایمی هستند که در آنها کامپیوتر و تجهیزات جانبی آن موضوع جرم واقع می شود. مانند: سرقت ، تخریب و....

دسته دوم : جرایمی هستند که در آنها کامپیوتر به عنوان ابزار ارتکاب جرم به کارگرفته می شود که معمولا از طریق شبکه های رایانه ای و اینترنت رخ می دهد. مثل کلاهبرداری ، جعل و سرقت رایانه ای و ....

دسته سوم : جرایمی هستند که می توان آنها را جرایم سایبری نامید که در فضای مجازی به وقوع می پیونددادما آثار آنها در دنیای واقعی ظاهر می شود. مانند نفوذ غیر مجاز،شنود غیر مجاز، انتشار ویروس ،کرم های رایانه ای و ...

سیر تیپیک اصطلاحات حقوق رایانه ای ، حقوق اینترنتی و حقوق سایبر

۱-اصطلاح حقوق رایانه [1] و جرایم رایانه ای

در دهه های ۱۹۶۰ و ۱۹۷۰ میلادی که سال های تولید ابر کامپیوتر ها و ورود آنها در شرکتهای بزرگ بمنظور انجام امور حسابداری ، توزیع کالا و نگهداری حسابها بود .اولین جرم رایانه ای در این دهه توسط رویس که حسابدار یک شرکت عمده فروش میوه و سبزی بود رخ داد.

[1] computer law

او با نوشتن یک برنامه و تغییر در داده ها مبالغی را در حسابی جدا واریز می کرد و در زمانهای خاص با صدور چک مبلغ را به نفع خود از حساب شرکت خارج می نمود.

در این دهه کامپیوترهای کوچکتر با توان محاسباتی بیشتر تولید شد و علم برنامه نویسی پیشرفته تر شد و در این دهه اکثر شرکتها کلیه برنامه ها ومحاسبات مالی خود را با رایانه انجام می دادند.

در دهه ۱۹۷۰ جرایم کلاهبرداری ، جعل و جاسوسی رایانه ای اتفاق افتاد و حقوق جزا به سمت رشته جدید حقوق کیفری اطلاعاتی رفت و اصطلاح حقوق رایانه ، حقوق تکنولوژی اطلاعات [1] و تبعا جرایم رایانه ای و جرایم علیه تکنولوژی اطلاعات از اواخر همین دهه مطرح شد.

۲-اصطلاح جدید حقوق شبکه [2] و حقوق اینترنت [3]

در این دهه ۱۹۸۰ نرم افزارها تولید شدند و کلیه پرداختهای الکترونیکی و امور اداری ادارات توسط رایانه به شکل ساده انجام می شد. در این دهه سازمان توسعه اقتصادی اروپا OECD برای اولین بار لیستی ۵ گانه از جرایم رایانه ای ارائه کرد.

همچنین این دهه آغاز شروع به کار شبکه ها، پایگاههای داده و تا حدودی اینترنت بود و جرایمی مانند کپی رایت نرم افزار، نفوذ به حریم خصوصی، مالکیت اطلاعات و... مورد بحث قرار گرفت. در این دهه دو اصطلاح جدید حقوق شبکه و حقوق اینترنت و در پی آن جرایم شبکه ای و جرایم اینترنتی مورد توجه حقوقدانان قرار گرفت.

۳-اصطلاح حقوق سایبر و جرایم سایبری

در دهه ۱۹۹۰ تکنولوژی اطلاعات در زمینه بانکداری ، امور اداری و مالی به صورت پیشرفته و همچنین امور تولید و آموزش و... به شدت افزایش یافت. و در سال ۱۹۹۴ اصطلاح سایبر و فضای مجازی یا سایبر اسپیس و حقوق سایبر و جرایم سایبری [4] مطرح شد.

شورای اروپا می گوید : منظور از فضای سایبر در مباحث حقوقی ترکیبی از عناصر زیر می باشد.
کامپیوتر + مودم + مخابرات (ماهواره) با ویژگی شبیه سازی و مجازی

تاریخچه جرایم رایانه ای در ایران

در خصوص تاریخ وقوع جرم رایانه ای در ایران، نمی توان وقوع آنرا با سال ۱۳۴۱ که رایانه وارد ایران شد همزمان دانست. کار برد رایانه در سالهای اولیه بسیار محدود بوده و در دهه ۵۰ و ۶۰ کم کم بر تعداد رایانه های موجود در ایران و همچنین وسعت برنامه های رایانه ای افزوده شد به دلیل عدم وجود قانون مدون و آمار دقیق از جرائم و سوء استفاده از رایانه نمی توان تاریخچه ای مشخص بیان نمود.

با توجه به گسترش رایانه و تکنولوژی اطلاعات در ایران با گسترش تخلفات مرتبط با کپی و تکثیر غیر مجاز نرم افزارها و برنامه هایرایانه ای سرانجام پس از سالها بحث و بررسی قانون حمایت از پدید آورندگان نرم افزارهای رایانه ای » در دی ماه ۱۳۷۹ تصویب شد که آئین نامه اول آن نیز در ۷۰ ماده تهیه و در اواخر سال ۱۳۸۰ جهت بررسی و تصویب به هیات وزیران ارسال شد.

---

[1] IT law
[2] network law
[3] internet law
[4] cyber crime

و در سال ۱۳۸۱ نیز طرح قانون تجارت الکترونیکی تهیه که نهایتاً متن آن در سال ۱۳۸۲ به تصویب نهایی مجلس شورای اسلامی رسید. از جمله موارد مهمی که می‌توان به آنها شاره نمود عبارتند از: جرم انگاری جعل، کلاهبرداری کامپیوتری، حمایت کیفری از حقوق مصرف کننده، حمایت از داده‌ها و کپی رایت.

براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. که در آن یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک های تضمینی مسافرتی کردند و چون تفاوت و تمایز چندانی بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آنها به عنوان جرم اینترنتی محسوب می شود.

بعد از این بود که گروه های هکر جرم های دیگری را مرتکب می شدند، مواردی چون جعل اسکناس، اسناد و بلیطهای شرکت های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک های مسافرتی و عادی بخشی از این جرایم اینترنتی هستند.

قانون مجازات جرایم رایانه ای

بخش اول: تعاریف

ماده ۱- در این قانون اصطلاحات در معانی ذیل بکار رفته‌اند:

الف- سیستم رایانه‌ای (Computer System)

هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری ـ نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده عمل می‌کند.

ب- سیستم مخابراتی (Communication System)

هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات بین یک منبع (فرستنده, منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی بوسیله پروتکل‌هایی که برای گیرنده قابل فهم و تفسیر باشد .

ج- داده رایانه‌ای (Computer Data)

هر نمادی از وقایع، اطلاعات یا مفاهیم به شکلی مطلوب برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب است و باعث می‌شود که سیستم رایانه‌ای عملکرد خود را به مرحله اجرا گذارد. داده دارای ارزش مالی است.

د- داده محتوا (Content Data)

هر نمادی از موضوعات، مفاهیم یا دستورالعمل‌ها نظیر متن، صوت یا تصویر، چه به صورت در جریان یا ذخیره شده که جهت برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای بکار گرفته شده و بوسیلهٔ سیستم رایانه‌ای ایجاد شود.

هـ - داده حاصل از تبادل داده محتوا (traffic data)

هرگونه داده‌ای که توسط رایانه ها در زنجیره ارتباطات تولید می‌شود تا ارتباطی را از مبدأ تا مقصد مسیریابی کند و شامل مبدأ ارتباط، مقصد ، مسیر، زمان، تاریخ، اندازه، مدت زمان و نوع خدمات اصلی و غیره خواهد بود.

و- اطلاعات (information)

داده، متن، تصویر، صدا، کد، برنامه رایانه‌ای، نرم‌افزار و پایگاه داده یا مایکروفیلم یا مایکروفیش ایجاد شده رایانه‌ای می‌باشد.

ز- اطلاعات مشترک (Subscriber information)

هر گونه اطلاعاتی که در دست تأمین کننده خدمات وجود داشته و مربوط به مشترک آن خدمات بوده و شامل نوع خدمات ارتباطی و پیش‌نیازهای فنی و دوره استفاده از آن خدمات، هویت مشترک، آدرس IP یا پستی یا جغرافیایی، شماره تلفن و سایر مشخصات شخصی وی می شود.

ح- ارائه‌کننده خدمات (Service Provider)

هر شخص حقیقی یا حقوقی است که برای کاربر خدماتش امکان برقراری ارتباط با سیستم کامپیوتری را فراهم آورده یا داده رایانه‌ای را به جای ارائه دهنده خدمات ارتباطی یا کاربران آن پردازش یا ذخیره می‌کند.

بخش دوم : جرایم و مجازاتها

ماده۲- هر کس عمداً و بدون مجوز، با نقض تدابیر حفاظتی داده ها یا سیستم‌های رایانه‌ای یا مخابراتی، به آنها دسترسی یابد به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم خواهد شد.

ماده۳- هر کس عمداً و بدون مجوز داده‌های در حال انتقال غیر عمومی در یک ارتباط خصوصی به، یا از یک یا چند سیستم رایانه ای یا مخابراتی یا امواج الکترو مغناطیسی را شنود یا دریافت نماید به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم خواهد شد.

ماده ۴- هرکس عمداً و بدون مجوز نسبت به داده‌های سری در حال انتقال یا موجود در سیستم‌های رایانه‌ای یا مخابراتی یا در حامل های داده که واجد ارزش برای امنیت داخلی یا خارجی کشور باشد، مرتکب اعمال زیر شود به مجازات‌های زیر محکوم می‌گردد:

الف ـ دسترسی به داده‌های موضوع این ماده یا تحصیل آنها به حبس از یک سال تا سه سال و پرداخت جزای نقدی از ده میلیون تا سی میلیون ریال

ب ـ قرار دادن داده‌های مذکور در دسترس اشخاص فاقد صلاحیت دسترسی به حبس از دو سال تا ده سال

ج ـ افشا و یا قرار دادن داده‌های مذکور در دسترس دولت، سازمان، شرکت، قدرت و یا گروه بیگانه یا عاملین آنها به حبس از پنج تا پانزده سال

تبصره۱ـ داده‌های سری، داده‌هایی هستند که افشای آنها به امنیت کشور و یا منافع ملی صدمه وارد سازد.

تبصره ۲ـ آیین نامه طرز تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری و با همکاری وزارتخانه‌های کشور، اطلاعات، ارتباطات و فن‌آوری اطلاعات و دفاع وپشتیبانی نیروهای مسلح تهیه و به تصویب هیئت وزیران خواهد رسید.

ماده ۵ - هر کس به قصد دسترسی به داده‌های سری موضوع ماده ۴ با نقض تدابیر امنیتی، به سیستم‌های رایانه‌ای و مخابراتی مربوط دست یابد به حبس از شش ماه تا دو سال یا پرداخت جزای نقدی از پنج میلیون تا بیست میلیون ریال محکوم خواهد شد.

ماده ۶ - هر یک از مأمورین دولتی که به‌نحوی امین، مسئول حفظ امنیت و یا حفاظت فنی داده‌های موضوع ماده ۴ این قانون و یا سیستم‌های مربوط باشند و در اثر بی‌احتیاطی، بی‌مبالاتی و یا عدم رعایت اصول حفاظتی سبب دسترسی اشخاص فاقد صلاحیت دسترسی به داده‌ها، حامل داده‌ها و یا سیستم‌های مذکور در ماده فوق گردند، به حبس از شش ماه تا دو سال یا پرداخت جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال و محرومیت از خدمات دولتی تا پنج سال محکوم می گردد.

ماده ۷- هر کس به قصد تقلب، داده های رایانه ای و مخابراتی دارای ارزش اثباتی را تغییر داده یا ایجاد ، محو یا متوقف نماید، مرتکب جعل رایانه ای بوده و علاوه بر جبران خسارت وارده، به حبس از یک سال تا هفت سال یا پرداخت جزای نقدی از ده میلیون تا هفتاد میلیون ریال محکوم خواهد شد.

ماده ۸- هرکس داده‌های مذکور در ماده ۷ را با علم به مجعول بودن آنها، مورد استفاده قرار دهد، علاوه بر جبران خسارات وارده به حبس از یک‌سال تا پنج سال و یا پرداخت جزای نقدی از ده میلیون تا پنجاه میلیون ریال محکوم خواهد شد.

ماده ۹- هر کس به قصد تقلب با ایجاد، تغییر، متوقف کردن یا از بین بردن داده‌ها یا سایر علایم و کدهای قابل پردازش در سیستم رایانه‌ای یا مخابراتی، کارت‌های اعتباری یا مغناطیسی یا سایر کارت‌های قابل پردازش یا مورد استفاده در سیستم‌های مزبور را جعل نماید یا با اعمال فوق نسبت به آنها مرتکب تقلب گردد به حبس از نود و یک روز تا سه سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار ریال تا سی میلیون ریال محکوم خواهد شد.

ماده ۱۰- هر کس به قصد اضرار، داده‌های دیگری را از سیستم رایانه‌ای یا مخابراتی یا ازحامل‌های داده پاک نماید یا صدمه بزند یا دستکاری کند یا غیر قابل استفاده نماید و یا به هر نحو تخریب یا مختل نماید به طوریکه منتهی به ضرر غیر شود به حبس از شش ماه تا دو سال و یا پرداخت جزای نقدی از پنج میلیون تا بیست میلیون ریال محکوم می‌گردد.

ماده ۱۱- هر کس عمدا با انجام اعمالی از قبیل وارد کردن، انتقال دادن، ارسال، پخش، صدمه زدن، پاک کردن، ایجاد وقفه، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی، سیستم رایانه‌ای یا مخابراتی دیگری را غیر قابل استفاده کرده یا عملکرد آنها را مختل نماید به حبس از شش ماه تا دو سال و یا پرداخت جزای نقدی از پنج میلیون تا بیست میلیون ریال محکوم می‌گردد.

ماده ۱۲- هر کس عمدا از طریق سیستم رایانه‌ای یا مخابراتی یا بوسیله امواج الکترومغناطیسی و با انجام اعمالی از قبیل مخفی کردن داده‌ها، تغییر رمز ورود ویا رمزنگاری داده‌ها، مانع دستیابی اشخاص مجاز به داده‌ها یا سیستم رایانه‌ای یا مخابراتی گردد به حبس از نود و یک روز تا یک سال و یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم می‌گردد.

ماده ۱۳- هر کس با انجام اعمالی نظیر وارد کردن ، تغییر ، محو ،ایجاد، توقف داده‌ها یا مداخله در عملکرد سیستم و نظایر آن، از سیستم رایانه‌ای یا مخابراتی سوء استفاده نماید و از این طریق وجه یا مال یا منفعت یا خدمات مالی یا امتیازات مالی برای خود یا دیگری تصاحب یا تحصیل کند در حکم کلاهبردار محسوب و به حبس از یک سال تا هفت سال و پرداخت جزای نقدی معادل وجه یا مال یا قیمت منفعت یا خدمات مالی یا امتیازات مالی که تحصیل کرده است، محکوم می‌شود.

تبصره: مجازت شروع به این جرم ، حداقل مجازات حبس مقرر خواهد بود

ماده ۱۴- هر کس از کارت‌های موضوع ماده ۹ این قانون سوء استفاده نماید و از این طریق مال یا وجه یا مزایای مالی یا خدمات مالی تحصیل یا تصاحب کند، علاوه بر جبران خسارات وارده به حبس از یک تا سه سال و پرداخت جزای نقدی معادل وجه یا مال یا قیمت منفعت یا خدمات مالی یا امتیازات مالی که تحصیل کرده است، محکوم می‌گردد.

ماده ۱۵- هر کس از طریق سیستم رایانه‌ای یا مخابراتی محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش یا عمل جنسی انسان یا انسان با حیوان را تولید کند یا منتشر سازد یا مورد هر قسم معامله قرار دهد، به حبس از نودو یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال و یا به هر دو مجازات محکوم خواهد شد.

تبصره۱: چنانچه محتویات موضوع این ماده در دسترس اشخاص زیر ۱۸ سال تمام قرار داده شود یا برای آنها منتشر یا ارائه گردد مرتکبین به حداکثر یک یا هر دو مجازات مقرر محکوم خواهند شد.

تبصره۲: تولید محتویات غیرواقعی (از طریق پویا نمایی، طراحی و نقاشی) با قصد انتشار یا معامله مشمول مقررات این ماده است.

ماده ۱۶- هر کس از طریق سیستم رایانه‌ای یا مخابراتی مرتکب اعمال زیر شود، در مورد جرایم موضوع بند الف به حبس از یک سال تا سه سال یا پرداخت جزای نقدی از سه میلیون تا پانزده میلیون ریال یا به هر دو مجازات و در مورد جرایم موضوع

بند ب و ج به حبس از نود و یک روز تا یک سال یا جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال یا به هر دو مجازات محکوم خواهد شد.

الف) محتویات مستهجن از قبیل نمایش اندام جنسی یا نمایش آمیزش یا عمل جنسی اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال تمام تولید یا ارایه یا منتشر یا ذخیره‌سازی یا تهیه یا در دسترس دیگران قرار دهد.

ب) به منظور دستیابی اشخاص زیر ۱۸ سال تمام به محتویات موضوع بند الف این ماده یا ماده قبل، مبادرت به تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید آنها نموده یا طریق دستیابی به محتویات مذکور را تسهیل نموده یا آموزش دهد.

ج) به منظور ارتکاب جرایم و انحرافات جنسی یا سایر جرایم یا خودکشی یا استعمال مواد روانگردان اشخاص زیر ۱۸ سال تمام را آموزش داده یا تبلیغ یا تحریک یا تهدید یا تشویق یا دعوت نموده یا فریب دهد یا طریق ارتکاب یا استعمال آنها را تسهیل نماید یا آموزش دهد.

تبصره ۱: تولید یا ذخیره‌سازی یا تهیه محتویات غیر واقعی چنانچه به قصد ارایه یا انتشار یا قرار دادن در دسترس دیگران نباشد از شمول این ماده مستثنی است.

تبصره۲: مفاد دو ماده فوق شامل آن دسته از محتویاتی که برای استفاده متعارف علمی یا هر مصلحت عقلایی دیگر ارایه می‌گردد، نخواهد بود.

ماده ۱۷- هر کس از طریق سیستم رایانه‌ای یا مخابراتی فیلم یا تصویر یا صوت دیگری را تغییر دهد یا تحریف نماید و منتشر سازد یا با علم به تحریف یا تغییر، انتشار دهد، به نحوی که منجر به هتک حرمت یا ضرر غیر گردد به حبس از نود ویک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا پنج میلیون ریال محکوم خواهد شد.

تبصره: ارتکاب جرم موضوع این ماده نسبت به مقام رهبری یا روسای قوای سه گانه مستوجب حداکثر حبس یا جزای نقدی مقرر در این ماده خواهد بود.

ماده ۱۸- هر کس از طریق سیستم رایانه‌ای یا مخابراتی فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی دیگری را بدون رضایت وی منتشر نماید یا در دسترس دیگران قرار دهد، به نحویکه منجر به ضرر غیر گردد یا عرفاً موجب هتک حیثیت وی شود به حبس از نود و یک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا پنج میلیون ریال محکوم خواهد شد.

ماده ۱۹- هر کس از طریق سیستم رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا اعمالی را بر خلاف حقیقت راساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی نسبت دهد به نحویکه موجب تشویش اذهان عمومی یا مقامات رسمی یا ضرر غیر شود، علاوه بر اعاده حیثیت به حبس از سه ماه و یک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا پنج میلیون ریال محکوم خواهد شد.

تبصره: جرایم موضوع مواد ۱۷ (به استثنای تبصره این ماده) ۱۸ و ۱۹ (به استثنای نشر یا در دسترس قرار دادن اکاذیب یا نسبت دادن اعمال خلاف حقیقت که موجب تشویق اذهان عمومی یا مقامات رسمی گردد) جز با شکایت شاکی خصوصی تعقیب نمی‌شود و با گذشت وی تعقیب موقوف خواهد شد.

ماده ۲۰- ایجادکنندگان نقطه تماس بین‌المللی موظفند امکان دستیابی به محتویات موضوع ماده ۱۵ وبند الف ماده ۱۶ را متوقف سازند، در غیر اینصورت به مجازات مقرر در مادهٔ ۲۵ همین قانون محکوم خواهند شد، سایر ارائه‌کنندگان خدمات اینترنتی نیز که با علم به تخلف اشخاص فوق، خدماتی را دریافت و امکان دستیابی به این محتویات را فراهم نمایند به مجازات فوق محکوم خواهند شد.

ماده ۲۱- به منظور جلوگیری از ادامهٔ ارائه یا انتشار محتویات موضوع مواد ۱۵ و بند الف ماده ۱۶ ارائه‌کنندگان خدمات میزبانی موظفند:

الف ـ نسبت به محتوای موجود درسایت‌های تحت میزبانی خود نظارت نمایند، چنانچه عدم نظارت یا بی مبالاتی وی در نظارت منجر به ادامهٔ ارائه یا انتشار محتویات فوق گردد به مجازات مقرر در ماده ۲۵ همین قانون محکوم خواهند شد.
ب ـ به محض اطلاع از وجود محتویات فوق در هر یک از سیستم‌های تحت میزبانی خود مراجع قضایی یا انتظامی را مطلع نموده و اقدامات لازم را در جهت توقف و در صورت امکان حفاظت از داده‌های مربوطه به عمل آورند. در غیر این صورت به مجازات مقرر در ماده ۲۵ همین قانون محکوم خواهند شد.

تبصره: تعیین مقررات نظارتی موضوع این ماده بر اساس آئین‌نامه‌ای است که توسط وزارت ارتباطات و فناوری اطلاعات ظرف سه ماه از تاریخ تصویب این قانون تهیه شده و به تصویب هیأت دولت خواهد رسید.

ماده ۲۲- هر کس مرتکب اعمال ذیل گردد، به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم می‌گردد.

الف ـ تولید، انتشار، توزیع، یا مورد معامله قرار دادن داده‌ها یا نرم‌افزارها یا هر نوع وسایل الکترونیکی که به منظور ارتکاب یکی از جرایم رایانه‌ای مورد استفاده قرار می‌گیرند.
ب ـ فروش، انتشار رمز عبور، کد دستیابی یا داده‌های رایانه‌ای به طور غیرمجاز به نحوی که به وسیلهٔ آن سیستم رایانه‌ای یا مخابراتی یا داده‌های مربوطه قابل دستیابی باشد.

تبصره: چنانچه مرتکب اعمال فوق را حرفهٔ خود قرار داده باشد، به هر دو مجازات محکوم خواهد شد.

ماده ۲۳- در موارد زیر، چنانچه جرایم رایانه‌ای مندرج در این قانون، تحت نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف ـ هرگاه مدیر شخص حقوقی مرتکب یکی از جرایم مندرج در این قانون شود.
ب ـ هرگاه مدیر شخص حقوقی دستور ارتکاب یکی از جرایم مندرج در این قانون را صادر نماید و جرم بوقوع پیوندد.
ج ـ هرگاه یکی از کارمندان شخص حقوقی، با اطلاع مدیر یا در اثر عدم نظارت وی، مرتکب یکی از جرایم مندرج در این قانون شود.
د ـ هرگاه مدیر، در ارتکاب یکی از جرایم مندرج در این قانون معاونت نماید.
هـ ـ هرگاه تمام یا قسمتی از موضوع فعالیت عملی شخص حقوقی، به ارتکاب یکی از جرایم موضوع این قانون اختصاص یافته باشد.

تبصره ۱- منظور از مدیر در این ماده هر شخصی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارا می‌باشد.

تبصره ۲- مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

تبصره ۳- کلیهٔ فعالیت‌های نهادهای دولتی که در راستای اعمال حاکمیت می‌باشد، از شمول این ماده مستثنی خواهد بود.

ماده ۲۴- اشخاص حقوقی موضوع مادهٔ فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، به ترتیب ذیل محکوم خواهند شد:

الف ـ سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی؛
ب ـ چنانچه حداکثر مجازات حبس آن جرم تا پنج سال باشد، تعطیلی موقت شخص حقوقی از یک تا ۹ ماه
ج ـ چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال باشد تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم منحل خواهد شد.

تبصره۱ـ مدیر شخص حقوقی که مطابق بند ۳ این ماده منحل می‌شود تا پنج سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت.

تبصره ۲ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. در صورتی که اموال شخص حقوقی به تنهایی تکافو نکند، مابه‌التفاوت از اموال مرتکب جبران خواهد شد.

ماده ۲۵- متخلفین از بند ب ماده ۲۱ و مواد ۳۰، ۳۱ و۳۲ این قانون به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از ده میلیون تا صد میلیون ریال محکوم خواهند شد.

ماده ۲۶- هر گاه مرتکبین جرایم موضوع این قانون قبل از کشف جرم یا دستگیری، مامورین تعقیب را از وقوع جرم مطلع نمایند یا به نحو موثری در کشف جرم کمک و راهنمایی کنند یا موجبات تعقیب سایر مرتکبین را فراهم آورند و یا در جبران خسارت وارده مساعدت کنند در مجازات آنان تخفیف داده خواهد شد یا مجازات حبس حسب مورد معلق خواهد شد و در جرایم موضوع ممانعت در دسترسی، دسترسی غیرمجاز ، شنود غیرمجاز ، تخریب داده‌ها یا اختلال در سیستم و جعل کامپیوتری دادگاه می‌تواند مرتکب را از مجازات مقرر معاف نماید.

ماده ۲۷- چنانچه هر یک از مستخدمین و مأمورین دولتی اعم از قضایی و اداری یا شوراها یا شهرداری‌ها یا نهادهای انقلابی و به طور کلی قوای سه گانه و همچنین نیروهای مسلح یا شرکت‌های دولتی یا سازمان‌های دولتی وابسته به دولت و یا مأمورین به خدمات عمومی خواه رسمی یا غیر رسمی به مناسب انجام وظیفه مرتکب یکی از جرایم موضوع این قانون شود و یا جرم بر اثر تبانی بیش از دو نفر واقع شود، مرتکب به بیش از دو سوم حداکثر مجازات حبس یا جزای نقدی مقررمحکوم خواهد گردید.

تبصره- چنانچه عمل مرتکب معاونت باشد به نصف حداکثر مجازات مقرر قانونی محکوم خواهد شد.

بخش سوم: آیین دادرسی

ماده ۲۸- در هر حوزه قضایی به تشخیص رئیس قوه قضاییه به تعداد مورد نیاز، شعبی از دادسراها و دادگاه‌های عمومی و انقلاب و تجدیدنظر و کیفری استان برای رسیدگی به جرایم رایانه‌ای اختصاص می‌یابد.

تبصره- قضات دادسراها و دادگاه‌های مذکور ترجیحا از بین قضاتی که آشنایی لازم به امور رایانه‌ای دارند، انتخاب خواهند شد.

ماده ۲۹- در صورت حدوث اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی مدنی دادگاههای عمومی و انقلاب خواهد بود.

ماده ۳۰- کلیه ایجادکنندگان نقاط تماس بین‌المللی و ارائه‌کنندگان خدمات اطلاع رسانی و اینترنتی موظفند داده‌های حاصل از تبادل داده محتوا را حداقل تا سه ماه پس از ایجاد و داده‌های مشترک را حداقل تا سه ماه پس از خاتمه اشتراک نگهداری نمایند.
تبصره: مراجع مذکور موظفند آدرس‌های IP خود را به اداره کل مبارزه با جرایم رایانه‌ای نیروی انتظامی اعلام نمایند.

ماده ۳۱- هر گاه حفظ داده‌های ذخیره شده برای تحقیق یا دادرسی لازم باشد مقام قضایی می‌تواند دستور حفاظت از داده‌های ذخیره شده را به اشخاصی که داده‌های مذکور به نحوی تحت تصرف یا کنترل آنها قرار دارد، صادر نماید و در موارد فوری ضابطین دادگستری می‌توانند دستور حفاظت را صادر و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضایی برسانند. چنانچه هریک از مقامات دولتی از اجرای دستور مذکور خودداری نمایند علاوه بر مجازات مقرر در خصوص سایر افراد به انفصال از خدمات دولتی از یک تا پنج سال محکوم خواهند شد.

تبصره ـ مدت زمان حفاظت حداکثر سه ماه می باشدو با نظر مقام قضایی قابل تمدید است.

ماده ۳۲ ـ مقامات قضایی می‌توانند دستور افشای داده‌های حفاظت شده مذکور درماده ۳۳ را به اشخاصی که داده‌های مذکور را در تصرف و یا کنترل دارند صادر تا در اختیار ضابطین قرار گیرد .

ماده ۳۳- تفتیش و توقیف داده‌ها و یا سیستم‌های رایانه‌ای در مواردی بعمل می‌آید که حسب دلایل ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم در آنها وجود داشته باشد.

ماده ۳۴- تفتیش و توقیف داده‌ها و یا سیستم‌های رایانه‌ای با دستور مقام قضایی صورت می‌گیرد و در جرائم مشهود و فوریت امر ضابطین دادگستری می‌توانند بدون دستور قضایی اقدام و ظرف ۲۴ ساعت مراتب را به مقام قضایی اعلام نمایند.

ماده ۳۵-دستور قضایی جهت تفتیش و توقیف باید شامل اطلاعاتی نظیر مکان و محدوده تفتیش و توقیف، نوع داده‌های مورد نظر، مشخصات احتمالی فایل‌ها و سخت افزارها و نرم‌افزارها، تعداد آنها ، مدت زمان مورد نیاز ، نحوه دستیابی به فایل‌های رمزگذاری شده، اجرای دستور در داخل یا خارج از محل باشد. تفتیش مشتمل بر موارد زیر خواهد بود:

- تفتیش از تمام یا بخشی از سیستم رایانه‌ای
- تفتیش داده‌های رایانه‌ای ذخیره شده

- تفتیش حامل‌های داده از قبیل: دیسکت و سی‌دی
- دستیابی به فایل‌های حذف شده یا رمزنگاری شده

ماده ۳۶- داده‌ها، حامل‌های داده و سیستم‌های رایانه‌ای یا مخابراتی که دلیل یا وسیله ارتکاب جرم بوده و یا از جرم تحصیل شده قابل توقیف می باشند.

ماده ۳۷- در جمع‌آوری داده‌ها با رعایت تناسب و توجه به نوع و اهمیت و نقش داده‌ها در ارتکاب جرم به روش‌هایی از قبیل موارد ذیل عمل می شود:

الف - غیر قابل دسترس نمودن داده ها با روشهایی چون تغییر گذر واژه و رمزنگاری
ب - تهیه پرینت از فایلهای متنی
ج - تهیه کپی یا تصویر از تمام یا بخشی از داده ها
د - ضبط حاملهای داده

ماده ۳۸- توقیف سیستم‌های رایانه‌ای و یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل موارد ذیل صورت می‌گیرد:

الف- تغییر گذر واژه به منظور عدم دسترسی به سیستم
ب - خاموش نمودن سیستم
ج - پلمپ سیستم در محل استقرار
د – ضبط سیستم

ماده ۳۹- در موارد ذیل سیستم‌های رایانه‌ای و مخابراتی توقیف خواهند شد:

الف- داده‌های ذخیره شده به سهولت قابل دسترس نبوده و یا حجم زیادی داشته باشند.
ب – بهره‌برداری وتجزیه وتحلیل داده‌ها بدون وجود سیستم سخت افزاری امکان‌پذیر نباشد.
ج - مالک یا مسئول یا متصرف قانونی سیستم به توقیف رضایت داده باشد.
د - تهیه کپی از داده‌ها به لحاظ فنی امکان‌پذیر نباشد.
هـ - تفتیش در محل سبب ایراد صدمه به داده‌ها گردد.
و - سایر موارد با تصمیم مقام قضایی.

ماده ۴۰- توقیف حامل‌های داده غیر متصل به سیستم رایانه‌ای و مخابراتی مانند ضبط آلات و ادوات جرم انجام خواهد گرفت.

ماده ۴۱ـ چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سیستم‌های رایانه‌ای که تحت کنترل و یا تصرف متهم قرار دارند ضروری باشد، ضابطین می‌توانند دامنه تفتیش و توقیف را به سیستم‌های دیگر گسترش داده و داده‌های مورد نظر را تفتیش و یا توقیف نمایند.

ماده ۴۲- در موارد توقیف داده ها، چنانچه به روند تحقیقات لطمه‌ای وارد نیاید با تقاضا و هزینه مالک یا دارنده حق دسترسی به داده‌ها و دستور مقام قضایی، کپی داده‌های توقیف شده به ایشان تحویل می‌شود، مگر آنکه داده‌ها غیر قانونی باشد.

ماده ۴۳ـ در مواردی که با تشخیص مقام قضایی توقیف سیستم یا داده‌ها سبب ایراد لطمات جانی به افراد یا اخلال در برنامه‌های خدمات عمومی گشته و یا مخل امنیت کشور باشد از روش‌های مناسبتری به جای توقیف استفاده خواهد شد.

ماده ۴۴ـ متضرر می‌تواند در خصوص عملیات و اقدامات مأمورین درتوقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل به مرجع قضایی دستور دهنده تسلیم نماید، به درخواست مذکور خارج از نوبت رسیدگی شده و تصمیم متخذه قابل اعتراض است.

ماده ۴۵ـ شنود داده محتوا ممنوع است، جز در مواردی که به امنیت کشور مربوط است و یا برای احقاق حقوق اشخاص به نظر قاضی ضروری تشخیص داده شود. مدت زمان شنود باید توسط مقام قضایی تعیین شود.

ماده ۴۶- داده‌های رایانه‌ای و مخابراتی در صورتی که مطابق این قانون جمع‌آوری و نگهداری شده باشند می‌توانند در اثبات جرم مورد استناد قرار گیرند.

ماده ۴۷- به منظور جلوگیری از بروز هرگونه تغییر، تحریف یا آسیب و حفظ وضعیت اصلی داده‌های رایانه‌ای و مخابراتی، لازم است تا زمانی که مرجع قضایی مربوط ضروری می‌داند، از آن نگهداری و مراقبت به عمل آید.

تبصره- آئین نامه نحوه جمع آوری، نگهداری و مراقبت از داده‌های رایانه‌ای و مخابراتی توسط وزارت دادگستری با همکاری نیروی انتظامی و وزارت ارتباطات و فناوری اطلاعات ظرف سه ماه از تاریخ تصویب این قانون تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.

بخش چهارم: معاضدت بین‌المللی

ماده ۴۸- معاضدت بین‌المللی، هرگونه تبادل اطلاعات و انجام امور اداری و پلیسی و قضایی که دولت ایران و سایر دول را قادر به کشف، پیگیری، تعقیب،رسیدگی و اجرای حکم نماید، در بر خواهد گرفت.

تبصره- چگونگی پیگیری و انجام امور مذکور در ماده ۴۸ و تشکیلات سازمانی مورد نیاز برای اجرای آن به موجب آئین نامه ای خواهد بود که ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با کسب نظر از مراجع ذیربط تهیه و به تصویب رئیس قوه قضاییه خواهد رسید.

ماده ۴۹- قبول همکاری بین‌المللی در موارد ذیل ممنوع می‌باشد:

الف ـ انجام درخواست با شرع و قوانین داخلی مغایرت داشته باشد.
ب ـ انجام درخواست مستلزم اقدام علیه حاکمیت، امنیت و یا دیگر منافع اساسی کشور ایران یا کشورهای دیگر باشد.

ماده ۵۰- مرتکبین جرایم غیر مندرج در این قانون که از طریق سیستم‌های رایانه‌ای و یا مخابراتی ارتکاب می‌یابند، طبق قانون مربوط مجازات خواهند شد، لیکن از نظر مقررات شکلی از قبیل مرجع رسیدگی و نحوه تفتیش و توقیف تابع ضوابط مقرر در این قانون می‌باشند.

ماده ۵۱- کلیه قوانین و مقررات مغایر از تاریخ تصویب این قانون ملغی می‌باشند.

جرائم رایانه ای و راهکارهای پیشگیرانه

جرایم اینترنتی و رایانه ای نوعی جرایم جدید می باشد. طیف 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 می رسد کامل ترین تعریف این باشد: «هر جرمی که قانونگذار به صراحت رایانه را به منزله موضوع یا وسیله جرم جزء 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.

نقش اشخاص حقیقی و حقوقی در جهت نظارت و پیشگیری از وقوع جرایم رایانه ای:

۱. نقش دادستان برای پیشگیری از وقوع جرایم رایانه ای:

واقع بینانه 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 یک طرفه‌ای 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» برای بررسی و احراز مصادیق فعالیت‌های غیرمجاز در عرصه سایبر تشکیل 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. 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 و ... 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 مجرمانه مذکور کرده است و همچنین در زمینه پیشگیری از وقوع جرایم در فضای سایبر ارائه طریق خواهد کرد.

۲- پلیس فضای تولید و تبادل اطلاعات ایران:

نام مختصر فتا، یک واحد تخصصی نیروی انتظامی جمهوری اسلامی ایران است که در ۳ بهمن ۱۳۸۹ (۲۳ ژانویه ۲۰۱۱) شروع به کار کرد و وظیفه آن مقابله با جرایم اینترنتی، کلاهبرداری و جعل در فضای سایبر و حفاظت از اسرار ملی بر روی شبکه اینترنت است. تشکیل 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. این 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. حوزه فعالیت این پلیس برخورد با جرائم سایبری نظیر مسایل اخلاقی، اقتصادی و حتی تروریسم است.

۳- نقش مردم در پیشگیری از وقوع جرایم رایانه ای:

مردم خودشان اطلاعات خود را در فضای مجازی فاش می‌کنند. به عبارتی اشخاصی هستند که از اینترنت اطلاع کافی ندارند و بدون اطلاع ، اقدام به چت کردن با افراد ناآشنا می نمایند. این اشخاص ، اطلاعات شخصی خودشان را در معرض دسترس این افراد قرار می دهند. به این گونه که توسط افراد متخصص هک شده و اطلاعات شخصی شان در اختیار آنها قرار می گیرد. همچنین گاهی اوقات اشخاص برای خرید یک محصول از یک سایت ، رمز عبور کارت شتاب خود را در اختیار متصدیان سایت قرار داده و سبب می شوند که از کارت آنها پول برداشت شود که می بایست پس از اقدام به پرداخت های اینترنتی از جمله شهریه و قبوض ، رمز خود را بر روی سیستم قرار نداده و یا حذف نماییم که مورد سوء استفاده دیگران قرار نگیرد .

۴ - نصب آنتی ویروسها و نرم افزارهایی که وظیفه حذف یا جلوگیری از ورود کرم های اینترنتی دارند:

برای جلوگیری از دزدی اطلاعات، خیلی از ویروس ها و کرم های اینترنتی هنگامی که وارد کامپیوتر می شوند سیستم امنیتی را از کار می اندازند و اقدام به دادن اطلاعات شخص دریافت کننده به شخص فرستنده ویروس می نمایند که از طریق آنتی ویروس ها و ضدکرم های اینترنتی که به روز شده اند می توان از ورود آن ها و سرقت داده ها جلو گیری کرد.

۵- اقدامی که جدیداً توسط وزارت بازرگانی صورت گرفته:

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 و شرکت های ارائه دهنده خدمات اینترنتی و فعال در امور بازرگانی تحت نظارت پلیس قرار گرفته و ساماندهی شوند.

۶- ارتش سایبری ایران: (هک کردن سایت هایی که برخلاف قانون جرایم رایانه ای عمل می کنند).

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. ارتش سایبری ایران 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 و برخی چانه‌زنی‌ها از ارتباط مرکز مبارزه با جرائم سازمان یافته سپاه با این گروه خبر می‌دهد . در اردیبهشت ۱۳۸۸ نیز خبرگزاری فارس گزارش داد مؤسسه «Tech Defense» 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 .

نتیجه گیری

در این مقاله ما در مورد مفهوم سه واژه جرایم رایانه ای ، جرایم اینترنتی و جرایم سایبری ، چگونگی بوجود آمدن این جرمها، تعاریف و سیرتیپیک مباحث حقوق رایانه، حقوق شبکه و اینترنت و حقوق سایبر بحث کردیم.

هدف ما از طرح این مباحث آشنایی با مفهوم حقیقی این واژه ها بود. چون در اکثر محافل علمی علی الخصوص حقوق دانان هنوز تفاوتی برای این واژگان قائل نبوده و به اشتباه هر سه مورد را در جاهای مختلف بصورت یکسان بکار می گیرند.

با تعاریفی که از جرایم رایانه ای، اینترنتی و سایبری مطرح شد. مشخص گردید این سه واژه به نوعی با هم متفاوت هستند و وجه مشترک هر سه وجود نقش سیستم های رایانه ای می باشد. و فقط ارتباط این واژگان در کاربرد رایانه در همه موارد است اما در نوع جرایم و ادله دیجیتال متفاوت هستند و به نوعی جرایم اینترنتی و سایبری نوع تکامل یافته جرایم رایانه ای هستند.

علی ایحال با تعریفی که از جرم رایانه ای داریم به آن دسته از اعمال مجرمانه ای که صرفا در رایانه های غیر متصل به شبکه ها صورت می گیرد جرایم رایانه ای و به جرایمی که از طریق اتصال رایانه ها به هم و از طریق اتصال به شبکه های رایانه ای و اینترنت صورت می گیرد.

جرایم رایانه ای و در نهایت به عمده جرایمی که به وسیله ابزارهای الکترونیکی و سیستم های رایانه ای مبتنی بر زیر ساخت مخابراتی با قابلیت شبیه سازی مجازی رخ می دهند جرایم سایبری گفته می شود.

و به احتمال زیاد منشا انتخاب عنوان قانون جرایم رایانه ای برای قانون مصوب مجلس در سال ۱۳۸۸ همین مساله بوده است. که با توجه به وجود جرایم سایبری و اینترنتی در این قانون ، عنوان انتخابی قانون جرایم رایانه ای می باشد. همین مسئله است که رایانه وجه مشترک و منشا هر سه نسل جرایم بوده است.

پیشنهادمی گردد سامانه های اطلاع رسانی قوانین ایران به منظور آشنانمودن کاربران ومراجعین اینترنتی راه اندازی گردد ومفاد قوانین مجازات جرایم رایانه ای یا سایبری دراختیارکاربران قرارگیرد.درصورت آشنا بودن کاربران باقوانین ،احتمال وقوع جرایم ناخواسته وناآگاهانه کاهش می یابد.

شما می توانید با انجام چند دستورالعمل مؤثر، از رایانه خود در برابر تهدید های سایبری محافظت کنید. پیروی از رهنمودهای ساده زیر کمک خواهد کرد تا خطر حمله را به حداقل برسانید.

- مراقب ایمیل هایی باشید که از شما اطلاعات شخصی می خواهند. بسیار بعید است که بانک شما چنین اطلاعاتی را توسط ایمیل از شما بخواهد. اگر تردید دارید با آن تماس بگیرید تا موضوع را بررسی کنند.
- در ایمیلی که از شما اطلاعات شخصی می خواهد، فرم مربوطه را پر نکنید. چنین اطلاعاتی را تنها با استفاده از یک سایت ایمن وارد کنید. بررسی کنید که آدرس اینترنتی با &۰۳۹;https&۰۳۹;// شروع می شود یا به طور معمول با &۰۳۹;http&۰۳۹;//. به دنبال علامت قفل در گوشه پایین و سمت راست مرورگر وب باشید و روی آن دو کلیک (دابل کلیک) کنید تا اعتبار گواهی دیجیتال را بررسی کنید و یا از تلفن برای انجام امور بانکی خود استفاده کنید.
- هر مورد مشکوکی را فوراً به بانک گزارش دهید.
- هرگز از لینک های داخل ایمیل برای بارگذاری یک صفحه وب استفاده نکنید. در عوض، آدرس اینترنتی را در مرورگر تایپ کنید.
- کنترل کنید که آیا آنتی ویروس شما سایت های فیشینگ را مسدود می کند یا نه و آیا نوار ابزاری را نصب می کند که هنگام حملات شناخته شده فیشینگ، هشدار بدهد؟
- به طور منظم حساب های بانکی خود (شامل کارت های پیش پرداخت و اعتباری، لیست گردش مالی حساب بانکی و غیره) را کنترل کنید تا مطمئن شوید تراکنش های فهرست شده، قانونی و درست هستند.

مطمئن شوید که از آخرین نسخه مرورگر وب نصب شده در رایانه تان، استفاده می کنید و هرگونه وصله امنیتی نصب شده است.

مراجع

۱. حسن بیگی، ابراهیم ،حقوق و امنیت در فضای سایبر،موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران،۱۳۸۴

۲. شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، نشر بهینه فراگیر، چاپ اول، تهران ۱۳۸۸

۳. مجموعه قوانین ومقررات کاربردی جزایی، مولف،گروه علمی موسسه آموزش عالی آزاد چتر دانش.ناشر,آراسبز.نوبت وسال چاپ,اول-۱۳۹۱

۴. انصاری، باقر، حقوق حریم خصوصی، انتشارات سمت، چاپ اول، تهران ۱۳۸۶

۵. پاکزاد، بتول، جرایم رایانه، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی، ۱۳۸۰

۶ -جلالی فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، انتشارات خرسندی، چاپ اول، تهران ۱۳۸۹

۷. تننباوم، آندرو اس، شبکه های کامپیوتری، ترجمه عین الله جعفر نژاد قمی، انتشارات علوم رایانه، چاپ سوم، تهران ۱۳۸۳

۸. دزیانی، محمد حسن، ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، شماره ۵۸، دی و اسفند ۱۳۷۳

۱۰ -شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۷۹

۱۱. جاویدنیا، جواد، جرایم تجارت الکترونیکی، انتشارات خرسندی، چاپ دوم، تهران ۱۳۸۸

۱۲. برومند باستانی«جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران،۱۳۸۳

۱۳. رضوی.محمد.(جرایم سایبری ونقش پلیس در پیشگیری ازاین جرایم وکشف آنها)فصل نامه دانش انتظامی.سالن نهم.ش یک.قانون جرایم سایبری مصوب ۱۳۸۸

14. policing cyber crime BY:petter Gottschalk for www.bookboon.com

15.Frankel, David S., *Model Driven Architecture: Applying MDA to Enterprise Computing*, OMG Press, Wiley Publishing, 2003.