دکتر الهام فریبرزی *
عضو هیأت علمی دانشگاه آزاداسلامی واحد مشهد

سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و جهان

چکیده

امروزه به کمک رایانه‌ها و اینترنت، اجرای بسیاری از کارها به طور قابل توجّهی آسان شده است. امّا این سرعت و توانایی راحت در انجام کارها، راه را برای ارتکاب جرم نیز گشوده است. در نتیجه با افزایش قوانین برای مجازات افرادی رو به رو هستیم که از این تکنولوژی سوء استفاده می‌کنند و تهدیدی علیه حریم خصوصی افراد و کسب و کارشان، امنیت عمومی و امنیت ملّی به شمار می‌روند.

تلاش این نوشتار بر آن است تا ضمن تبیین و تحلیل سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و دیگر کشورها، پیشنهادهایی برای قانون‌گذاران و کاربران رایانه و اینترنت ارایه کند.

واژگان کلیدی:
جرایم رایانه‌ای، جرایم اینترنتی، مجازات جرم‌های رایانه‌ای، جرایم مجازی، قانون جرایم رایانه‌ای

* Email: elhamfariborzi@gmail.com

دریافت: ۸۹/۱۱/۲۰ پذیرش: ۹۰/۳/۱

مقدمه

تحولات فن آوری، تأثیرات متفاوتی بر جوامع در کشورهای گوناگون داشته است. با توجّه به قرار گرفتن در فضای مجازی وگسترش استفاده از رایانه و اینترنت، مشکلات ناشی از آنها نیز رو به افزایش است. به دلیل این‌که امروزه افراد زیادی به اینترنت دسترسی دارند، جرایم رایانه‌ای تبدیل به یک مسأله‌ی اجتماعی شده است. امروزه همه‌ی افرادی که با اینترنت و رایانه سر و کار دارند، نگران هستند که مورد حمله‌ی مجازی افراد ناشناس قرار بگیرند.

جرایم رایانه‌ای ممکن است توسط هرکس با اهداف گوناگون رخ دهد؛ چه با هدف قانون شکنی و چه با هدف یادگیری درباره‌ی سیستم‌های اطلاعاتی یا نرم افزارها. برای نمونه؛ کلاهبرداری، ارتکاب تروریسم، قاچاق مواد مخدر، قاچاق انسان، سرقت اسرار تجاری، دزدی نرم افزار، جاسوسی اقتصادی، کلاهبرداری از مؤسسه‌های مالی، خراب‌کاری و وارد کردن خسارت به شرکت‌های زیادی از طریق برنامه‌های نرم افزاری مخرب (ویروس‌های رایانه‌ای) و موارد زیاد دیگری که در سراسر دنیا شاهد هستیم (Grabosky, 2006,p.42). طبق آمار منتشر شده در اینترنت[1] در سال ۲۰۰۹، ایالات متحده آمریکا با ۲۳٪، بیشترین جرایم رایانه‌ای را داشته است. چین با ۹٪ در رده‌ی دوم، آلمان با ۶٪ در رده‌ی سوم و بریتانیا با ۵٪ در رده‌ی چهارم قرار دارند. به هر حال وسعت رخداد جرایم رایانه‌ای در زمان کنونی به حدّی است که همه باید مراقب امنیت رایانه‌ای خود باشیم. امّا اگر مورد حمله‌ی این مجرمان قرار گرفتیم چگونه می‌توانیم از حق خود دفاع کنیم؟ آیا قوانینی حمایت کننده جهت برخورد با افراد مجرم و سودجو وجود دارد؟ بنابراین ضرورت پرداختن به این بحث هم اکنون بیشتر از گذشته احساس می‌شود. قوانین علیه جرم و جنایات رایانه‌ای از دولتی به دولت دیگر متفاوت است.

هدف اصلی این مقاله، تبیین و تحلیل سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و جهان است به گونه‌ای که بتوان درصد وقوع جرایم رایانه‌ای و اینترنتی را با اطلاع رسانی کاهش داد و از وقوع بسیاری از جرم‌ها پیشگیری کرد و خلاء قانونی احتمالی موجود در این زمینه را در کشور کاسته تا مانعی در انجام جرم شود.

---

[1].www.enigmasoftware.com

معنای جرم

امروزه توسط رایانه و شبکه‌ی اینترنت، افراد علاوه بر روش‌های قبلی انجام جرم، می‌توانند به حریم دیگران تجاوز و یا به مال او دست اندازی نماید. حوزه‌ی جرایم در زندگی امروز بشر، آن قدر پیچیده شده است که قانون گذاران مجبورند تحوّلات جرم را به صورت مداوم زیر نظر داشته باشند (دانش، ۱۳۸۸، ۱۸۲) و به تدوین قوانین درست گام بردارند. تعاریف مختلفی از جرم وجود دارد که در زیر چند نمونه آورده شده است:

- دورکیم (جامعه شناس فرانسوی) می‌نویسد: هر عملی که در خور مجازات باشد، جرم است. یعنی هر فعل یا ترک فعلی که نظم و آرامش اجتماعی را مختل سازد و قانون نیز برای آن مجازاتی تعیین کرده باشد، جرم محسوب می‌شود. از نظر حقوقی نیز جرم عملی است که بر خلاف یکی از موارد قانون مجازات عمومی هر کشور باشد و مجرم کسی است که در زمان معینی عمل او بر خلاف قانون رسمی کشور باشد (مرکز تحقیقات رایانه‌ای علوم اسلامی، ۱۳۸۹) بنا به این تعریف به بیان دیگر مقررات قانونی برای مجازات یک عمل است که نشان دهنده‌ی جرم بودن یا نبودن آن است.
- جرم، یک عمل خطا است که کنگره‌ی آمریکا از آن به عنوان جنایت و تخطی از قانون یاد کرده است (Balkin and et al., 2006,30).
- جرم به عنوان پدیده‌ای انسانی – اجتماعی، محصول تعامل انسان و اجتماع است و از آنجا که ویژگی فردی و شخصیتی افراد نیز خود به نوعی متأثر از محیط پیرامون آنهاست می‌توان محیط را به عنوان اساسی‌ترین عامل ایجاد زمینه‌های گرایش افراد به ارتکاب جرم دانست (دهقانی، ۱۳۸۹، ص ۲۰).

جرم رایانه‌ای

در زیر چند نمونه از تعاریف جرم رایانه‌ای آورده شده است:

- جرم رایانه‌ای اشاره دارد به هر جرم و جنایتی که از رایانه و شبکه به عنوان ابزاری جهت انجام آن جرم استفاده شده است (Moore, 2005,p.32).

- ارتکاب جرم در یک محیط الکترونیکی برای منافع اقتصادی یا آسیب رساندن به دیگران (Samuel, 2008, p.16).
- سوء استفاده از رایانه‌ها شامل هرنوع رفتار غیر قانونی، غیر اخلاقی، یا غیر مجاز که مربوط به پردازش و انتقال داده‌هاست (سازمان ملل، ۱۳۷۶، ص ۱۱۸).

معرفی تعدادی از جرم‌های رایانه‌ای

بحث جرایم رایانه‌ای در ایران ابتدا در اوایل دهه‌ی ۱۳۸۰ مطرح شد. آن زمان بیشتر حوزه‌هایی را در بر می‌گرفت که به جعل اسناد دولتی و شخصی مربوط می‌شد. چنان‌که اولین جرم رایانه‌ای در خرداد ۱۳۷۸ به ثبت رسید که در آن یک دانشجوی رایانه و یک کارگر چاپخانه در کرمان، چک‌های تضمینی را جعل می‌کردند. جعل اسکناس، بلیت شرکت‌های اتوبوس‌رانی، جعل اسناد دولتی هم‌چون؛ گواهینامه‌ی رانندگی، کارت پایان خدمت، مدرک تحصیلی، اوراق خرید و فروش خودرو و چک‌های مسافرتی از دیگر موارد جرم رایانه‌ای در اوایل دهه‌ی ۸۰ به حساب می‌آمد. پس از آن برخی از وبلاگ نویسان و روزنامه‌نگاران به اتهام نوشتن مطالب در وبلاگ‌ها و سایت‌ها دستگیر شدند و به اتهام‌هایی مانند توهین به افراد و مقدسات یا افشای اسرار و اسناد دولتی محاکمه و مجازات شدند و دولت با فیلترینگ گسترده‌ی سایت‌ها و کنترل سرعت اینترنت، به دنبال تعاریف و مصداق‌های تازه‌ای از جرایم رایانه‌ای و اینترنتی برآمد. هم‌چنین شکایت به خاطر اختلاف بر سر دامنه‌ی اینترنتی، اختلاف شرکت‌های اینترنتی با مخابرات، جعل سایت‌های اینترنتی، تعهد نداشتن شرکت‌های کامپیوتری و یا وب سایت‌ها، شکستن قفل نرم افزارها و هک ایمیل‌های شخصی نیز از موارد دیگر است که روز به روز بر تعداد این جرم‌ها افزوده می‌شود.

برای نمونه برخی افراد حقیقی نسبت به ثبت دامنه‌های اینترنتی با نام مجموعه‌ها و مؤسسه‌ها و برندهای معتبر و شناخته شده اقدام می‌کنند که صاحبان اصلی این نام‌ها، مدعی باز پس گیری این دامنه‌ها می‌شوند. اختلاف کارمندان را با صاحبان این شرکت‌ها می‌توان نیز از دیگر موارد مطرح شده از این دست در شکایت‌های رایانه‌ای عنوان کرد.

همان‌گونه که مشخص شد جرایم گوناگونی می‌تواند در حوزه‌ی رایانه و اینترنت رخ دهد که تعدادی از آن‌ها عبارتند از:

- دسترسی غیر مجاز به داده‌ها یا سیستم رایانه‌ای یا مخابراتی
- شنود و دریافت غیر مجاز ارتباط خصوصی به وسیله‌ی سیستم رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی
- جرایم علیه امنیت سیستم‌های رایانه‌ای یا مخابراتی
- جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی
- جعل اینترنتی
- تخریب و ایجاد اختلال در داده‌ها
- اختلال در سیستم‌های رایانه‌ای
- کلاهبرداری اینترنتی که شامل هر گونه کلاهبرداری است که با وسیله‌ی برنامه‌های رایانه‌ای یا ارتباطات شبکه اینترنتی صورت می‌گیرد مثلاً از طریق وب سایت‌ها، پست الکترونیک و اتاق‌های گفتگو[1]. این جرم یکی از مهم‌ترین جرایم رایانه‌ای است که مانند جرم کلاهبرداری کلاسیک، ازجمله جرایم علیه اموال و مالکیت محسوب می‌شود (خرّم آبادی، ۱۳۸۶، ص ۱). کلاهبرداری رایانه‌ای شیوه‌های گوناگونی دارد، همچون سوء استفاده از شبکه‌ی تلفنی برای انجام مکالمه با هزینه‌ی مشترکان دیگر، سوء استفاده از صندوق‌های خودپرداز با دزدی کارت‌های بانکی، سوء استفاده از کارت‌های اعتباری با دزدی رمز این کارت‌ها.

بیشترین میزان شکایت‌های رایانه‌ای و اینترنتی از سال ۲۰۰۰ تا ۲۰۱۰ م در آمریکا به تجارت الکترونیکی مربوط می‌شود، شامل حراج آنلاین و کارت‌های اعتباری. هم‌چنین شکایت مربوط به دزدی هویت نیز در سال ۲۰۰۹ م به بعد افزایش داشته است (Richmond, 2011). البته برخی ادعا می‌کنند که آمار گزارش درباره‌ی جرایم رایانه‌ای، واقعی و قابل اعتماد نیست چون تعدادی از جرم‌ها به دلیل مشکلات مربوط به اثبات جرم گزارش نمی‌شوند.

از مهم‌ترین موارد جرم اینترنتی و رایانه‌ای در سال ۱۳۸۴ در ایران، ۳۲ مورد سوء استفاده از کارت‌های اعتباری ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از

[1]. E-mail and chat rooms

طریق اینترنت، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوع‌های متفرقه بوده است. هم‌چنین براساس اظهارات رئیس مبارزه با جرایم رایانه‌ای ناجا، در سال ۸۸ آمار پرونده‌های تشکیل شده، نشان می‌دهد که این جرایم رو به گسترش است (سایت علمی دانشجویان ایران، ۱۳۸۹)[1] و این نشان می‌دهد که افرادی که قرار است از خدمات دولت الکترونیکی استفاده کنند در معرض آسیب‌های جدّی قرار دارند.

خبرگزاری مهر(۱۳۸۸) نوشت که ناصر آبادی- رئیس همایش امنیت و دولت الکترونیکی در سال ۱۳۸۸- ناآشنایی کاربران با ویژگی‌های فضای مجازی، بی‌توجّهی و کم توجّهی به امنیت فناوری اطلاعات از سوی کاربران منفرد و مؤسسه‌های دولتی و خصوصی، افزایش میزان کاربری رایانه‌ای و بهره‌گیری از شبکه‌های رایانه‌ای، پیچیده‌تر شدن فعالیت‌های متخلفان و مجرمان فضای سایبر و فقدان همکاری‌های بین المللی در مقابله با جرایم رایانه‌ای را از علل وقوع جرایم رایانه‌ای در کشور می‌داند.

انتشار اخبار دروغ، ارسال مطالب، تصاویر و فیلم‌های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد، استفاده از فضای متعلق به دیگران، ارسال پیام‌های مخرب، اخلال در دسترسی به دیگران، نقض حق مالکیت، هک و ویروسی کردن سایت‌ها و شکستن حریم خصوصی افراد از طریق ایمیل افراد بخشی از جرم‌های اینترنت محسوب می‌شوند. به جرم‌های اینترنتی می‌توان کلاهبرداری، سوء استفاده از نام شرکت‌ها، دزدی اینترنتی و استفاده از علایم اینترنتی، نفوذ به سایت‌های دولتی و خصوصی و رزروکردن آدرس سایت‌ها بر اساس نام شرکت‌ها و افراد و باج خواهی از آنها طراحی برنامه‌های مخرب، دزدی، جنایت و سایر موارد از طریق ایمیل و چت را هم افزود.

مهم‌ترین جرم اینترنتی که هم اکنون برای کاربران به بحران تبدیل شده سرقت هویت است که آنها را مجبور به تغییر هویت به سمت هویت دیجیتالی کرده است. در مورد هک کردن هم، در برخی از کشورها طبق برخی قوانین، هکرها شناسایی و روانه زندان شده‌اند. در کشور ما برای هک کردن قانون خاصی نداریم فقط افرادی که از عمل دیگران متضرر می‌شوند می‌توانند با مراجعه به دادگاه و تنظیم شکایت برای رسیدگی اقدام کنند.

---

[1]. www.daneshju.ir/forum

مشکلات ناشی از جرایم رایانه‌ای

جرایم رایانه‌ای، بیلیون‌ها دلار به اقتصاد جهانی آسیب می‌رسانند و متخصصان معتقدند این مسأله، تهدیدی برای امنیت ملی و رفاه اجتماعی به شمار می‌آید. آمریکا در رأس تعداد جرم‌های رایانه‌ای قرار دارد، کره شمالی در مکان دوم، چین در مکان سوم و آلمان و فرانسه در مکان‌های بعدی قرار دارند (McQuade, 2009,61). این جرم‌ها می‌تواند مانع امنیت و آسایش فردی، آسایش عمومی، هتک حرمت خصوصی و عمومی و مانند آن شود که در زیر به نمونه‌هایی از اثرهای جرایم رایانه‌ای اشاره شده است (Ringwelski, 2011) :

- از دست دادن بازدهی: یکی از عمده‌ترین تأثیرهای جرایم رایانه‌ای بر روی یک شرکت، از دست دادن بازدهی است. این زیان می‌تواند از طرف شخص خارجی ایجاد شود، کسی که اطلاعات مالی حساسی را به دست می‌آورد و از آن برای برداشت بودجه سازمان استفاده می‌کند.
- زمان از دست رفته: یکی دیگر از پیامدهای بزرگ جرم رایانه‌ای، زمانی است که تلف می‌شود، هنگامی که کارکنان فناوری باید بخش زیادی از روز را به بررسی و مدیریت این اتفاقات اختصاص دهند.
- اعتبار آسیب دیده: در مواردی که رکوردهای مشتری به وسیله‌ی یک شکاف امنیتی مربوط به جرم رایانه‌ای به خطر می‌افتد، اعتبار و شهرت یک شرکت می‌تواند ضربه‌ای اساسی ببیند.

کاهش بهره‌وری: به علّت اقدام‌هایی که شرکت‌ها باید برای خنثی کردن جرایم رایانه‌ای انجام دهند، بیشتر تأثیرهای منفی بر روی بهره‌وری کارکنان دارد. دلیل آن است که به سبب اقدام‌های امنیتی، کارمندان باید رمزهای بیشتری وارد نمایند و عملیات وقت گیر دیگری را نیز برای انجام کارهایشان اجرا کنند. هر ثانیه که برای انجام این نمونه عملیات تلف می‌شود برابر است با هر ثانیه که برای کارهای سازنده مصرف نمی‌شود.

- نگرانی‌هایی در زمینه‌ی امنیت و حریم شخصی واجتماعی پیش آورد.

چگونگی کشف جرایم رایانه‌ای

هر دستگاهی که در اینترنت وجود دارد یا به آن متصل است یک شماره شناسایی منحصر به فرد دارد که به آن آدرس IP یا شماره‌ی IP گفته می‌شود.[۱] در بسیاری از جرایم نیاز به دانستن این مطلب است که آدرس IP در چه تاریخ، مکان و چه ساعتی، در اختیار چه کسی بوده که این بسیار به کشف جرم و تشخیص آن کمک می‌کند زیرا جعل هویت، کار خیلی دشواری نیست و می‌توان هویت و آدرس جعلی داد. اما شماره تلفنی که به یک ISP وصل می‌شود و از طریق آن خدمات می‌دهد را نمی‌توان جعل کرد؛ بنابراین برای کشف دقیق جرم به آن اطلاعات نیاز است که با این وجود با یک بررسی سریع و با کمک متخصص فناوری اطلاعات، می‌توان اطلاعات لازم را جهت شناسایی جرایم رایانه‌ای به دست آورد (کانون وکلای دادگستری منطقه اصفهان، ۱۳۸۹)[۲].

روند قانون‌گذاری بر جرایم رایانه‌ای و اینترنتی در ایران و کشورهای دیگر

در کشورهای گوناگون برای مدیریت جرایم رایانه‌ای راهکارهای متفاوتی به کار گرفته می‌شود. بیشتر کشورها سعی دارند تا با تصویب قوانین و مقررات، آسیب‌های ناشی از جرایم رایانه‌ای را به کمترین مورد برسانند. اما علاوه بر این قوانین بازدارنده، باید مراجعی نیز وجود داشته باشند تا مشکلات مرتبط در این زمینه کاهش یابند. در ادامه به چند نمونه از این موارد پرداخته می‌شود:

ایران

تصویب قوانین و مقررات کیفری، لازمه‌ی ایجاد امنیت و فراهم آورنده‌ی شرایط توسعه در هر حوزه‌ی فناوری محسوب می‌شود و حوزه‌ی فناوری اطلاعات و ارتباطات نیز از این قاعده جدا نیست. اما برای تهیه‌ی قانونی مناسب که حقوق و تکالیف همکاران این حوزه را تعیین کند، ایجاد زبان مشترک میان حقوق‌دانان و متخصّصان فناوری

---

[۱]. یک آدرس IP چیزی مثل این است: ۲۱۶.۲۷.۵۵.۱۲۷

[2].www.isfahanbar.org

اطلاعات و ارتباطات و نگاه قانون‌گذار به موضوعات متفاوت از زاویه‌ی دید متخصّصان و کاربران آن حوزه، ضرورتی انکارناپذیر است.

نکته‌ی قابل تأمل درباره‌ی جرایم اینترنتی این است که در سال‌های گذشته بنا بر نظر و تصمیم مجلس شورای اسلامی و اظهار نظر مسؤولان قضایی، مبنای فعالیت سایت‌ها اینترنتی و مرجع رسیدگی به جرایمی را که به واسطه‌ی اینترنت رخ می‌دهد، می‌توان در قلمرو قانون مطبوعات جستجو کرد و دلیل تصمیم این بود که شبکه‌های اینترنتی که اقدام به نشر مطلب می‌کنند نوعی نشریه محسوب می‌شوند. برای اثبات درستی این نظر می‌توان به تبصره‌ی ۳ ماده‌ی یک فصل اول قانون مطبوعات کشورمان اصلاحیه‌ی مصوب سال ۱۳۷۹[1] استناد کرد؛ براساس این تبصره، تمام نشریات الکترونیک، مشمول مواد این قانون « قانون مطبوعات » است (فیروزمنش، ۱۳۸۸).[2] بنابراین با جرایم اینترنتی و جرایمی که از طریق نشریات الکترونیکی رخ می‌دهد می‌توان بر اساس مجازات‌های پیش بینی شده در قانون مطبوعات برخورد کرد. به گزارش خبرنگار مهر، اولین بار در دی ماه ۱۳۷۹، قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای به تصویب رسید که آیین‌نامه آن نیز در ۷۰ ماده به تصویب هیأت وزیران رسیده است (مدیر وب سایت آگهی سارا، ۱۳۸۹)[3].

پس از آن، پیش نویس قانون جرایم رایانه‌ای ایران توسط کمیته‌ی مبارزه با جرایم رایانه‌ای قوه‌ی قضاییه تهیه شد و لایحه‌ی آن پس از گذشت چند سال از تهیه پیش نویس با اعمال نظر کارشناسان، توسط مجلس شورای اسلامی به تصویب رسید. این لایحه شامل سه بخش جرایم و مجازات، آیین دادرسی و سایر مقررات است. هر یک، فصول و مباحث مربوطه را در قالب مواد و تبصره‌های گوناگون بیان می‌کند و بسیاری از مشکلات مجازی (سایبر) را رسیدگی خواهد کرد. سپس قانون گذار در ایران در تاریخ ۱۳۸۲/۱۰/۱۷ قانون تجارت الکترونیک را برای از بین بردن خلاء موجود در قوانین در این زمینه و تجارت الکترونیک به تصویب رسید. قانون تجارت الکترونیک مشتمل بر ۸۱ ماده است که در بخش‌ها و فصل‌های متفاوت به مباحثی در زمینه‌های کلیات و تعاریف

---

[1]. (الحاقی ۱۳۷۹/۱/۳۰)

[2].www.infoage.ir

[3].www.agahisara.ir

و تفسیر قانون، اعتبار قرار دادهای خصوصی، پذیرش ارزش اثباتی امضای الکترونیکی، مبادله‌ی داده پیام، حمایت انحصاری در بستر مبادله‌های الکترونیکی، حمایت از داده پیام‌های شخصی، حفاظت از داده و پیام در بستر مبادلات الکترونیکی، حمایت از علایم تجاری جرایم و مجازات آن و کلاهبرداری رایانه‌ای، جعل رایانه‌ای نقص حقوق انحصاری در بستر مبادلات الکترونیک، جبران خسارت و دیگر مسائل متفرقه پرداخته است.

در باب چهارم این قانون، اولین گفتار در رابطه با کلاهبرداری رایانه‌ای است که نشانگر میزان اهمیت و درجه‌ی آن در نظر قانون گذار است زیرا همان‌گونه که مشخص شد بیشتر جرایمی که در حوزه‌ی جرایم رایانه‌ای اتفاق می‌افتد، کلاهبرداری رایانه‌ای است. ماده‌ی ۶۷ و هم چنین تبصره‌ی آن در قانون تجارت الکترونیک در باب چهارم از جرایم و مجازات‌ها و گفتار اول کلاهبرداری رایانه‌ای تنها ماده در این زمینه است به عبارت دیگر تنها عنصر قانونی ما در این زمینه محسوب می‌شود. ماده‌ی ۶۷ قانون تجارت الکترونیک مقرر داشته است :هر کس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده‌ی غیر مجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی هم‌چون ورود، محو، توقف داده پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و ... ، دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و مانند آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند، اموال دیگران را ببرد، مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود. هم چنین تبصره‌ی این ماده مقرر می‌دارد: شروع به این جرم نیز جرم محسوب و مجازات آن، کمترین مجازات مقرر در این ماده است.

سپس کمیته‌ی مبارزه با جرایم رایانه‌ای که از طرف شورای عالی توسعه‌ی قضایی، وظیفه‌ی تدوین پیش‌نویس قانون مجازات جرایم رایانه‌ای را عهده دار شد، در خرداد ماه ۸۳، پیش‌نویس تهیه شده را با برگزاری نشست «ابعاد حقوقی فناوری اطلاعات» در معرض نقد و ارزیابی صاحب‌نظران قرار داد که تضمین کننده سلامت فضای مجازی آینده‌ی کشور بود. سپس قانونی مشتمل بر ۵۶ ماده و ۲۵ تبصره در تاریخ ۱۳۸۸/۳/۲۰ به تأیید شورای نگهبان رسید. به موجب مواد تصویب شده، جرایمی هم‌چون؛ دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، جعل رایانه‌ای، تخریب و اخلال در داده‌ها یا

سیستم‌های رایانه‌ای و مخابراتی، سرقت و کلاهبرداری مرتبط با رایانه، جرایم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب، مسؤولیت کیفری اشخاص جرم انگاری شد. فصل پنجم از این متن به شرح زیر است:

هتک حیثیت و نشر اکاذیب

ماده‌ی (۱۶): هرکس به وسیله‌ی سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به گونه‌ای که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. تبصره ـ چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد .

ماده‌ی (۱۷): هرکس به وسیله‌ی سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به گونه‌ای که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد .

ماده‌ی (۱۸): هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقام‌های رسمی به وسیله‌ی سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به طور صریح یا تلویحی نسبت دهد، شامل این‌که از طریق یاد شده به گونه‌ای از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده‌ی حیثیت به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد .

ماده‌ی (۵): چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده‌ی (۳) این قانون یا سیستم‌های مربوط هستند و به آنها آموزش لازم داده شده یا داده‌ها یا سیستم‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا

رعایت نکردن تدابیر امنیتی، موجب دسترسی اشخاص بدون صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد و یا در ماده‌ی (۱۹) در موارد زیر، چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در زمینه‌ی منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف- هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب- هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع پیوندد.

ج- هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر نظارت نکردن وی مرتکب جرم رایانه‌ای شود.

د- هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

تبصره‌ی ۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره‌ی ۲ـ مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

ماده‌ی (۲۴): هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یک‌صد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

ماده‌ی (۲۱): ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیته‌ی تعیین مصادیق موضوع ماده‌ی زیر محتوای مجرمانه شامل محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود را پالایش کنند. در صورتی که عمداً از پالایش محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه‌ی دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه‌ی نخست به جزای نقدی از بیست تا یکصد

میلیون ریال و در مرتبه‌ی دوم به جزای نقدی از یک‌صد میلیون تا یک میلیارد ریال و در مرتبه‌ی سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

در فصل هشتم (تشدید مجازات‌ها) آمده است:

ماده‌ی (۲۷): در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی هم‌چون؛ اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف- چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب- چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج- چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

در فصل دوم یعنی جمع‌آوری ادله‌ی الکترونیکی در رابطه با نگهداری داده‌ها آمده است:

ماده‌ی (۳۲): ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را دست‌کم تا شش ماه پس از ایجاد و اطلاعات کاربران را دست‌کم تا شش ماه پس از خاتمه‌ی اشتراک نگهداری کنند.

تبصره‌ی ۱ـ داده ترافیک هرگونه داده‌ای است که سیستم‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدا تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی هم‌چون؛ مبدا، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره‌ی ۲ـ اطلاعات کاربر هرگونه اطلاعات درباره‌ی کاربر خدمات دسترسی هم‌چون؛ نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا IP، شماره تلفن و سایر مشخصات فردی اوست.

ماده‌ی (۳۳): ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را دست‌کم تا شش ماه پس از خاتمه‌ی اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را دست‌کم تا پانزده روز نگهداری کنند.

این قانون که پس‌از رفع مشکلات شرعی و قانونی به تصویب شورای نگهبان رسید، مجازات‌های حبس و جریمه‌ی نقدی را برای دسترسی غیرقانونی به اطلاعات خصوصی و محرمانه پیش‌بینی کرده است. بر اساس قانون جرایم رایانه‌ای، هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی را در سامانه‌های رایانه‌ای، مخابراتی، امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ۱۰میلیون ریال تا ۴۰میلیون ریال یا هر دو مجازات محکوم خواهد شد.

هم‌چنین هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از ۹ روز تا یک سال یا جزای نقدی از ۵ میلیون ریال تا ۲۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد. در ماده‌ی ۳ این قانون آمده است: "هر کس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد".

به گزارش خبرگزاری مهر، دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، حبس از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات در دسترس قرار دادن داده‌های مذکور برای اشخاص بدون صلاحیت، به حبس از دو تا ده سال افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

بر اساس قانون، داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند. آیین‌نامه نحوه‌ی تعیین و تشخیص داده‌های سری و نحوه‌ی طبقه‌بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارت‌خانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهد رسید.

سرانجام، با توجه به گسترش تخلفات و تعریف جرایم جدید در فضای مجازی قانون جرایم رایانه‌ای در ۳ بخش (۱- جرایم و مجازات‌ها ۲- آیین دادرسی ۳- سایر مقررات) و پنج فصل و ۵۶ ماده و ۲۵ تبصره تنظیم شده‌است. حبس و جریمه‌ی نقدی یا هر دو مجازات‌هایی است که برای مرتکبان این جرایم وضع شده‌است. این قانون در ۷ تیر

۱۳۸۸ قانون جرایم رایانه‌ای به تأیید شورای نگهبان رسید و رئیس‌جمهور ۱۰ تیر آن را برای اجرا ابلاغ کرد (مدیر وب سایت لینک‌های مفید، ۱۳۸۹)[1]. در قانون مجازات جرایم رایانه‌ای که شامل چهار بخش است، در بخش اول یعنی تعاریف به توضیح اصطلاحات به کار رفته در ماده‌های قانون پرداخته شده و در بخش دوم به جرایم و مجازات‌ها اشاره شده است.

اعضای کارگروه تعیین مصادیق محتوای مجرمانه "موضوع ماده‌ی ۲۲ قانون جرایم رایانه‌ای" در زمینه‌ی وظایف و مأموریت‌های ذاتی خود مکلف به ایجاد سامانه رصد فضای مجازی در دستگاه متبوع خود بوده و هم چنین تمام ارایه 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 اعلام کند.[2] این کارگروه فهرست مصادیق محتوای مجرمانه "موضوع ماده‌ی ۲۲ قانون جرایم رایانه‌ای" را در پنج فصل مشتمل بر موارد زیر منتشر کرد.:

الف- محتوای علیه عفت و اخلاق عمومی

ب- محتوای علیه مقدسات اسلامی

ج- محتوای علیه امنیت و آسایش عمومی

د- محتوای علیه مقامات و نهادهای دولتی و عمومی

هـ- محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم به کار می‌رود.

رعایت مقررات فهرست مصادیق محتوای مجرمانه برای ارایه دهندگان خدمات دسترسی و میزبانی و تمام کاربران در فضای مجازی لازم است و در صورت تخطی طبق مقررات برخورد خواهد شد. ولی با توجه به تعریف کلمات به کار رفته در تعدادی از موارد آن کلی گویی است در حالی که در قوانین جزایی نباید به صورتی کلی جرم را تعریف کرد تا قابل تعمیم به هر موردی باشد که قاضی تعریف می‌نماید که مشکل زاست.

---

[1].www.mofidlinks.ir

[2]. www.dadsetani.ir and E-mail:dadsetani@dadsetani.ir

چگونگی رسیدگی به جرایم رایانه‌ای در ایران

اما پرسش مهّم این است که ضمانت اجرایی قانون جرایم رایانه‌ای کشور چیست؟ در ایران دادگستری مجتمع ۳۴ تهران برای رسیدگی به جرایم رایانه‌ای اختصاص یافته است. شرح وظایف و احکامی که برای مجتمع قضایی رسیدگی به جرایم رایانه‌ای (متشکل از سه عضو اصلی و سه عضو علی‌البدل) این است که می‌تواند برای افراد و اشخاص حکم قضایی صادر کند و نیروی انتظامی به عنوان بازوی اجرایی در این زمینه فعالیت می‌کند، اما شورای انتظامی نظام صنفی رایانه‌ای ماهیت صنفی دارد و وظایف و اختیاراتش با این مجتمع متفاوت است.

با توجّه به این‌که شورای انتظامی سازمان نظام صنفی رایانه‌ای حق جلب و توقیف و صدور رأی و حکم قضایی را مانند مجتمع قضایی ندارد، شورای انتظامی سازمان نظام صنفی رایانه‌ای، ماهیت قضایی ندارد. مجتمع قضایی رسیدگی به جرایم رایانه‌ای می‌تواند پروانه صادره توسط شورای انتظامی سازمان نظام صنفی رایانه‌ای را توقیف و از صدور پروانه جلوگیری کند و یا از ادامه‌ی کسب و فعالیت آن شرکت مربوطه یا سازمان به عنوان اتحادیه جلوگیری نماید. نیروی انتظامی ملزم به انجام احکام صادره از مجتمع قضایی است. پیگیری جرایم رایانه‌ای از طریق مراجع قضایی زمان بر است ولی از طریق شورای انتظامی سازمان سریع‌تر به شکایات رسیدگی می‌شود. طبق ماده‌ی ۴۴، تخلفات دو نوع صنفی و جزایی هستند؛ رسیدگی شورای انتظامی به شکایات بعد از یک نوبت دو هفته، آغاز شده و بسته به نوع پرونده، اعلام حکم زمان می‌برد. طی جلسه رسیدگی دو طرف حاضر می‌شوند که ممکن است با توافق طرفین حل اختلاف صورت بگیرد و حکم به مراجع قضایی اعلام نشود.

هر زمان که فردی در حوزه‌ی اینترنت مشکلی داشته باشد، می‌تواند به شکل حضوری و یا به صورت رونوشت اعتراض خود را به صورت اینترنتی[1] اعلام کند. هم‌چنین، طرح راه اندازی وب سایت رسیدگی به جرایم رایانه‌ای به واسطه‌ی پشتیبانی

[1].E-mail: shora@isp.ir

نکردن مالی و کارشناسی مسکوت مانده است. با ایمیلی که شورای حل اختلاف دارد بعضی از موارد رسیدگی می‌شود، اما کافی نیست (وب سایت وکالت، ۱۳۸۸)[1].

آمریکا

در سال ۲۰۰۶ در آمریکا بیش از ۲۰۰ هزار شکایت شد. بیش از ۸۶ هزار از این شکایت‌ها پردازش شدند و بیش از ۱۹۴ میلیون دلار ادعای خسارت مالی شد. ایمیل (۷۴٪)، صفحه‌ی وب (۳۶٪) و تلفن (۱۸٪) از سه مکانیزم اصلی برای تماس مجرمان به قربانیان گزارش شد[2]. بنابراین بین سال‌های ۲۰۰۶ و ۲۰۰۷ م، افزایش خالص در بودجه فناوری اطلاعات در مورد امنیت صرف شده در آمریکا وجود دارد که اعلان شد متأسفانه رقم کمی به آموزش مرتبط به آن اختصاص یافت. رتبه‌بندی انجام شده بر اساس میزان ضرر مالی و غیر مالی، عبارت بودند از:

- کلاهبرداری مالی (۲۱،۱۰۰،۰۰۰ دلار)
- ویروس / کرم / تروجان (۸،۴۰۰،۰۰۰ دلار)
- نفوذ سیستم‌های خارجی (۶،۸۰۰،۰۰۰ دلار)
- تعداد فزایندهای از بچه‌های ناخواسته که حاصل تعاملات سکسی آنلاین بودند
- تهاجم جنسی به جوانان و آزار و اذیت‌های آنلاین آنان.

در کنگره قوانین فدرال در آمریکا قوانین جرایم رایانه‌ای در سال ۱۹۸۴ تصویب شد (Williams, 2006,14) که شامل قوانینی جهت کلاه برداری و سوء استفاده رایانه‌ای بود که به واسطه‌ی این قوانین رابرت موریس، دانشجوی کارشناسی ارشد در دانشگاه کرنل، برای انتشار اولین "کرم" بر روی اینترنت تحت پیگرد قانونی قرار گرفت. البته پیش از این، قوانیتی در سال ۱۹۶۱ دررابطه با رایانه بررسی شده بود که از سال ۱۹۸۷ به اجرا در آمد. مثلاً در رابطه با کلاه برداری با کمک رایانه در بند516 - D. آمده است: شخصی مرتکب جرم کلاه برداری رایانه‌ای است که او آگاهانه دسترسی و یا باعث امکان دسترسی به رایانه یا هر قسمت از آن شود؛ یا یک برنامه یا داده‌هایی را به منظور گول زدن یا به عنوان بخشی از فریب افراد ایجاد کند؛یا باعث خسارت رایانه یا هر قسمت آن

[1].www.vekalat.org
[2].www.Computer- forensics

یا مخدوش کردن و حذف هر برنامه یا اطلاعات مندرج در آن رایانه شود؛ یا باعث دسترسی فردی به رایانه و یا هر قسمت آن شود تا بتوان کنترل بر پول، دارایی یا به خدمات دیگر داشت. با این حکم کسی که مرتکب جرم کلاهبرداری رایانه‌ای می‌شود با توجه به سطح مالی کلاهبرداری شده مجازات می‌شود(InfoTech, 2010).

در سال ۱۹۸۶، قانون حریم خصوصی ارتباطات الکترونیکی تصویب شد. در قانون زیرساخت اطلاعات ملی[1] که در سال ۱۹۹۶ ساخته شد که هر فردی به صورت غیر مجاز به دیدن اطلاعات بر روی رایانه خاصی بپردازد مجرم است و عمل وی غیر قانونی است. در دیگری که قانون امنیت داخلی (قانون پاتریوت ایالات متحده آمریکا)[2] بود و در ۲۶ اکتبر۲۰۰۱ به تصویب رسید درباره‌ی قانون محافظت در اینترنت بود. به عنوان نمونه؛ قانونی در سال ۱۹۹۶ به تصویب رسید که افراد و سازمان‌ها را در برابر دزدی اسرار تجاری محافظت کند(Wesley, 2010).[3]

به علاوه، قانون کمیسیون تجارت فدرال[4]، مجموعه‌ای از قوانین برای تبلیغات آنلاین تحت اختیار این کمیسیون به عنوان اولین آژانس حمایت کننده از مصرف کنندگان ایجاد شده است. طبق FTCA تبلیغات آنلاین به عنوان دیگر تبلیغات مکتوب و رسانه‌ای باید قابل اعتماد باشد ونباید مصرف کنندگان را گمراه کند. علاوه بر این FTCA علیه تبلیغ کنندگان آنلاین که در کارهای فریب دهنده شرکت می‌کنند، پرونده‌ی حقوقی تشکیل می‌دهد. هم‌چنین FTCA بیان می‌کند ضمانت نامه‌ی کتبی برای فروش آنلاین محصولات باید دقیقاً در محل خرید محصول در سایت مورد نظر، قرار گرفته باشد (ماده‌ی ۱۶ از قانون فدرال قسمت ۷۰۲).

مرکز شکایت جرایم اینترنتی[5] برای مشارکت دفتر تحقیقات فدرال[6] و مرکز ملی جرایم یقه سفیدها[7] تاسیس شد. هدف این مرکز، دریافت شکایت‌های مرتبط با جرایم

---

1. NIIA= The National Information Infrastructure Act
2. The Homeland Security Act-(USA Patriot Act)
3. www.ehow.com
4. FTCA= The Federal Trade Commission ACt
5. IC3=The Internet Crime Complaint Center
6. FBI= Federal Bureau of Investigation
7. NW3C =National White Collar Crime Center

اینترنتی، تحقیقات بیشتر و توسعه آن و سپس ارجاع آن به دفترهای فدرال، ایالتی، محلی و یا دفترهای اجرای قوانین بین المللی برای رسیدگی‌های لازم.

یکی از آژانس‌های ایالتی که به جرایم رایانه‌ای می‌پردازد، آژانس گشت زنی کالیفرنیا[1] است. طبق قوانین این آژانس، جرم‌هایی هستند که نیازمند توجه فوری می‌باشند که در زیر چند نمونه از آنها آورده شده است:

- اگر شخصی آگاهانه و بدون مجوز اقدام به آسیب رساندن، پاک کردن، تغییر دادن و استفاده از داده‌ها یا رایانه نماید.
- اگر شخصی آگاهانه و بدون اجازه به سیستم رایانه‌ای یا شبکه رایانه‌ای دسترسی یابد و یا شرایط دسترسی به آن را فراهم آورد.
- اگر شخصی آگاهانه و بدون اجازه از نام دامنه‌ی اینترنتی فرد دیگری استفاده کرده و اقدام به ارسال ایمیل و در نتیجه آسیب و خرابی یک سیستم رایانه‌ای شود.

دادگستری ایالات متحده آمریکا برای تسهیل گزارش جرایم رایانه ای، اقدام به دسته بندی این جرم‌ها و معرفی آژانس‌های مناسب برای هر دسته کرده که در زیر به نمونه‌ای از آن جرم‌ها اشاره شده است: نفوذ رایانه‌ای، خرید و فروش رمزها،[2] پورنوگرافی کودکان و بهره‌کشی، کلاهبرداری اینترنتی و هرزنامه‌ها، آزار و اذیت اینترنتی و قاچاق مواد منفجره یا سلاح گرم از طریق اینترنت.

برای نمونه تعدادی از جرم‌های انجام شده بین سال‌های ۲۰۰۸ تا ۲۰۱۱ م در ایالات متحده عبارتند از:

- یک مرد ۳۷ ساله از نیوهمشایر در آمریکا به خاطر هک کردن رایانه‌های بین المللی به ۸۲ ماه زندان محکوم شد. هم‌چنین وی باید تقریباً حدود ده میلیون مالیات عقب مانده‌ای را که مربوط به فایل درآمد مالیاتی وی در زمان زندگیش در ماساچوست است و وی آن را هک کرده بود، بپردازد.

---

[1]. CHP=The California Highway Patrol
[2]. Passwords

• یک مرد ۲۶ - ساله تگزاسی، محکوم به هک کردن سرورهای رایانه‌ای ازشرکت‌های محلی و ناسا شد. وزارت دادگستری اعلان کرد که وی از اکتبر ۲۰۱۰ تحت پیگرد قانونی جرایم اینترنتی است.

• با توجه به گزارش سالانه جنایت سایبر توسط اف بی آی آنها اعلان کردن که جرم‌های رایانه‌ای و اینترنتی در سال ۲۰۰۹، ۲۲.۳ درصد بیشتر از سال ۲۰۰۸ شده و بیشترین موارد شکایت در رابطه با فضای سایبر در رابطه با از دست دادن پول به هر نوعی برای افراد/سازما ن‌ها و یا دولت بوده است. این رقم نیز در ۲۰۰۹ نسبت به ۲۰۰۸ نیز دو برابر شده است. در ۲۰۰۸ معادل ۲۶۴،۴۰۰،۰۰۰دلار و در ۲۰۰۹ معادل ۵۵۹،۷۰۰،۰۰۰، بنابراین آنها مردم را توصیه کرده‌اند تا برای اطلاعات بیشتر و محافظت بیشتر در فضای مجازی به آدرس وب سایتی در اینترنت زیر مراجعه کنند.[۱]

• مالک ۶۱ ساله پیشین شرکت والترمن در ایالت آیوا به بیش از ۱۲ سال زندان به اتهام کلاه برداری پستی و پول شویی از طریق اینترنت محکوم شد.• دادستان منطقه‌ای از نیویورک در ایالات متحده آمریکا به خاطر این‌که وب سایت‌های زیر اخبار زنده ورزشی را غیر قانونی و توسط قانون " برای تماشا کلیک کن و پولش را بپرداز و سپس مشاهده کن" پخش می‌کردند، آنها را توقیف کرد.[۲] دادستانی از منطقه‌ی منهتن آمریکا گفت: "غیر قانونی پخش کردن جریان رویدادهای ورزش حرفه‌ای توسط پرداخت به ازای هر مشاهده از طریق وب سایت‌هایی که هیچ تعهدی به آنها ندارند، سرقت از کسب و کار محسوب می‌شود و جرم است. "

• یک مرد روسی ساکن مسکو متهم با ارسال هزاران ایمیل هرزنامه یا اسپم شد. وی زمانی که در ماه نوامبر ۲۰۱۰ به لاس وگاس در ایالت نوادا برگشت محاکمه شد. بیشترین مجازات ممکن برای این جرم، زندان است و نه بیش از سه سال.

---

[1].www.justice.gov/criminal/cybercrime/index.html

[۲]. این وب سایت‌ها عبارتند از: ATDHE.NET, CHANNELSURFING.NET, HQ-STREAMS.COM, HQSTREAMS.NET, FIRSTROW.NET, ILEMI.COM, IILEMI.COM, IILEMII.COM,ROJADIRECTA.ORG and ROJADIRECTA.COM.

• یک مرد میامی با اتهام خرید، فروش و استفاده از کارت‌های اعتباری دزدیده شده دستگیر شد. وی شماره‌های ذخیره شده بیش از ۲۶،۰۰۰ کارت اعتباری را بر روی رایانه داشت و از طریق اینترنت و کارت جعلی خرید و فروش می‌کرد.

• یک زن دوبلین متهم به هک کردن ایمیل و تغییر رمز ورود ایمیل شد. وی که در پی قانون حمایت از کودکان درگیر اختلافات با پدر بچه اش است و پدربزرگ و مادربزرگ در سال ۲۰۰۸ بود. بدون مجوز، وارد ایمیل متعلق به مادر بزرگ کودک شد و تغییر رمز عبور داد. بنابراین، قربانی قادر به دسترسی به حساب خود نشد. هنگامی که او بار دیگر به تنظیم رمز عبور پرداخت، کشف کرد که این فرد ایمیل‌های بین او و وکیلشان در رابطه با حضانت کودک، حذف شده بود.

• یک مرد نبراسکایی، اتهام خود را درباره‌ی حمله به وب سایت کلیسای ساینتولوژی در ژانویه سال ۲۰۰۸ که باعث از کارافتادن و تعطیلی وب سایت شد، پذیرفت و به یک سال زندان محکوم شد. وی با استفاده از نرم افزاری که در آن مقدار زیادی از ترافیک اینترنت را با اطلاعات مخرب جایگزین می‌کند، به گونه‌ای که وب سایت مورد حمله، قادر به رسیدگی به حجم بالایی از ترافیک اینترنت دیگر نخواهد بود، دست به این جرم زد و باعث شد کاربران قانونی نتوانند به دلیل ترافیک ساختگی بالا برای سایت، به اطلاعات سایت دست پیدا کنند.

• دو مرد اروپایی به اتهام حمله‌ی مجازی علیه سایت‌های اینترنتی دو شرکت‌های آمریکایی محکوم شدند. آنها به عمد باعث صدمه به رایانه‌های این دو شرکت‌های مستقر در ایالات متحده که کارشان راه اندازی ماهواره‌ای بود، شدند. هریک از آنها به ۱۵ سال زندان محکوم شدند. هم‌چنین چهار نفر شاغل در همین شرکت به خاطر کمک و توطئه در انجام این جرم، هر یک به دو سال زندان محکوم شدند.

• مردی ابتدا مظنون به هک رایانه‌ای شد و وی را بازداشت کردند و سپس دولت فدرال وی را متهم کرد که وی درخواست‌هایی جنسی صریح برای دیدن فیلم از زنان و دختران نوجوان لس آنجلس توسط اینترنت داشته است. این مرد با یک باند زیر زمینی وابسته بود که کارشان هک رایانه‌ها و به دست آوردن اطلاعات

شخصی آنان و سپس خواستار صریح فیلم سکسی از قربانیان زن در ازای نگه داشتن اطلاعات شخصی و خصوصی آنان می‌شدند. این گروه به بیش از ۱۰۰ رایانه توسط هک دسترسی یافته و حدود ۲۳۰ نفر را درگیر کرده بودند که دست‌کم ۴۴ نفر از آنها نوجوان بودند و سرانجام آنها متهم به سوء استفاده ازتکنولوژی برای اعمال کنترل بر زنان جوان و قربانیان بی‌خبر شدند.

• بخش جرم‌های رایانه‌ای و مالکیت معنوی[1] مسؤول اجرای استراتژی‌های ملی در مبارزه‌ی گروهی با جرایم رایانه‌ای و مالکیت معنوی در سراسر جهان است که در آمریکا می‌باشد.

درآمریکا به شهروندان توصیه شده تا با کسب آگاهی، جنایات رایانه‌ای و جنایات مالکیت معنوی را به دولت فدرال گزارش کنند. برخی از آژانس‌های اجرای قانون که مناسب برای انواع خاصی از گزارش جرم و جنایت رایانه‌ای است به صورت زیر است :

• جرم هک کردن و دزدی رمز عبور(دفتر محلی اف بی آی- سرویس مخفی آمریکا- مرکز شکایت جرم‌های اینترنتی (IC3)

• پورنوگرافی یا بهره برداری از کودکان (مرکز شکایت جرم‌های اینترنتی – اداره‌ی مهاجرت و گمرک آمریکا)

• استثمار از کودکان و کلاه برداری از آنان (مرکز شکایت جرم‌های اینترنتی - خدمات بازرسی پستی ایالات متحده)

• کلاه‌برداری اینترنتی و هرزنامه‌ها یا اسپم (دفتر محلی اف بی آی- سرویس مخفی ایالات متحده - بخش جرایم مالی) - کمیسیون تجارت فدرال (شکایت آنلاین) در صورت تقلب در اوراق بهادار و سرمایه گذاری‌های مربوط به اِسپَم ایمیل‌ها، بورس و اوراق بهادار کمیسیون شکایت آنلاین) - مرکز شکایت جرم‌های اینترنتی

• آزار و اذیت اینترنتی (دفتر محلی اف بی آی)

• تهدید بمب از طریق اینترنت (دفتر محلی اف بی آی)

[1].The Computer Crime and Intellectual Property Section =CCIPS

- قاچاق مواد منفجره یا آتش زا و یا سلاح گرم توسط اینترنت (دفتر محلی اف بی آی- دفتر محلی ای تی اف)

پلیس آمریکا در سال ۲۰۰۳ به خاطر رشد زیاد جرایم رایانه‌ای افزود که یک سیستم کلی و کارآمد ضروری و مورد نیاز می‌باشد تا به کنترل جرایم اینترنتی بپردازد (Walden, 2007,47). پس از آن دولت فدارل آمریکا کتاب راهنمایی[۱] در رابطه با جعل، نقض حقوق مولف و سرقت اسرار تجاری از اکتبر ۲۰۰۴ منتشر کرده است. مثلاً در آن نوشته شده چنانچه اسرار تجاری به سرقت رفتند و یا حقوق مولف نقض شد، چگونه و به چه واحدی و چه مطالبی را در گزارش‌شان ارسال کنند. هم‌چنین طرح‌های دیگری نیز دولت برای مبارزه با جرم‌های رایانه‌ای ارائه داده است.[۲]

کانادا

کانادا اولین کشوری بود که در سال ۱۹۸۳ در قانون فدرال خود، به طور مشخص به جرم رایانه‌ای اشاره کرد و قوانینی برای آن به تصویب رساند (Casey, 2004,26) که شامل سه مورد بود: استفاده غیرمجاز از رایانه، خرابی داده و نقض حق چاپ. (Carroll, 1996,38). در کانادا قوه مقننه، حقوق جزا برای مقابله با جرم و جنایت رایانه‌ای را در چهارم دسامبر ۱۹۸۵ به اجرا در آورد، به گونه‌ای که استفاده غیر مجاز از رایانه در موارد ممنوعه زیر جرم است:

۱. هر کس که با استفاده از دستگاه الکترو مغناطیسی، صوتی، مکانیکی و یا دیگر وسایل به طور مستقیم یا غیر مستقیم، به رایانه‌ای دیگر دست‌یابی یابد و باعث جرم شود، جرم وی قابل تعقیب و موجب حبس برای مدّت حداکثر ده سال خواهد شد. جرم‌هایی هم‌چون: از بین بردن و یا مخدوش کردن داده‌ها؛ ارائه اطلاعات بی‌معنی، بی‌فایده و یا بی‌اثر؛ مانع، قطع و یا تداخل با استفاده از داده‌ها، یا مانع، قطع و یا تداخل با هر شخص در استفاده از داده‌ها شود. در سال ۱۹۸۸، قانون اصلاح قانون کپی رایت

---

[1]. With pdf format electronic

[۲]. مانند وب سایت.www.stopfakes.gov که اطلاعاتی را برای کسب و کار و مالکیت معنوی فراهم می‌کند (TheInternational Trade Administration, U.S. Department of Commerce, 2011).

خواستار افزایش مجازات برای آن جرم به حداکثر یک میلیون دلار و یا پنج سال زندان برای محکومیت در کیفر خواست شد.[۱]

کد جنایی کانادا شامل مجموعه‌ای از قوانین برای برخورد با مسائل جرم و جنایت رایانه‌ای است. نسخه‌ی کنوانسیون جرم رایانه‌ای (۲۰۰۱ نوامبر ۲۳) شامل جرم‌هایی به صورت زیر است: دسترسی غیر مجاز/ استراق سمع غیرقانونی/ تداخل داده‌ها/ تداخل سیستم/ سوء استفاده از دستگاه/ کاربرد رایانه جهت جعل اسناد/کربرد رایانه جهت تقلب / کاربرد رایانه جهت پورنوگرافی کودکان/ نقض کپی رایت و حقوق مرتبط/ تلاش و کمک و یا معاونت در جرم / ارتباطات با گروه‌های نژادپرستانه از طریق سیستم‌های رایانه‌ای/ ارتباطات نژادپرستانه و تهدید آمیز / توهین‌های نژادپرستانه با انگیزه/ کاربرد رایانه در توجیه نسل کشی یا جنایات علیه بشریت/ کمک و معاونت در جرم /معاملات با سرقت، جعل و استفاده از کارت‌های اعتباری غیر مجاز از رایانه / شکستن حریم خصوصی افراد توسط رایانه (Kim ،1997).

چین، دانمارک و سوئیس

از سال ۱۹۹۴، چین قوانین و آیین نامه‌های زیادی را برای نظارت بر اینترنت به تصویب رسانده است که می‌توان به چند مورد اشاره کرد. محاکمات توسط نیروی نظامی قانونی برگزار می‌شود و اعمال مجازات‌ها سنگین هستند و حتی مجازات اعدام را هم برای این جرم‌ها دارند. تعدادی از این قوانین مرتبط می‌شود به امنیت سیستم‌های اطلاعاتی رایانه‌ای، قانون کپی رایت، نظارت بر سرویس‌های اطلاعاتی اینترنتی و حفاظت از حق انتشار آنلاین اطلاعات.

در ژانویه سال ۱۹۹۰، دو پسر دبیرستانی دانمارکی بودند که به عنوان اولین هکرهای دانمارکی شناخته شدند. این در حالی بود که دانمارک قانونی به صراحت

---

[۱]. در کشور کانادا با مراجعه به سایت www.antifraudcentre-centreantifraude.ca می‌توان اطلاعاتی درباره‌ی جرایم اینترنتی به دست آورد. در صورتی که اطلاعات سایت کافی نباشد، می‌توانند با آدرس اینترنتی info@antifraudcentre.ca مکاتبه کنند و سؤال‌های خود را مطرح نمایید. هم‌چنین می‌توان به صورت آنلاین، تخلف صورت گرفته را گزارش کرد.

درباره‌ی منع هک کردن رایانه را در همان زمان داشت. پس از محاکمه، برای آنها حکم دو سال تعلیقی خورد و به شدّت از هک هر رایانه‌ای منع شدند و اگر دوباره تکرار کنند، به آنها هشدار داده شد که حکم بازداشت خواهند داشت.

در سوئیس، در سال ۱۹۹۳ قانون ممنوعیت هک کردن به تصویب رسید، اگر چه تنها دو هک قبل از تصویب این قانون انجام شد که به صورت غیر قانونی هم حل و فصل شد (دانشجو، ۱۳۸۹). واحد هماهنگی سوئیس برای کنترل جرایم رایانه‌ای[1] یک اداره‌ی مرکزی است که افراد می‌توانند موضوعات مشکوک اینترنتی را که شامل موارد زیر می‌شود را گزارش دهند: پورنوگرافی، خشونت، افراط گرایی، نژادپرستی، ورود غیرمجاز به سیستم‌های فناوری، تکثیر ویروس‌های رایانه‌ای، تخریب داده‌ها، و سوء استفاده از کارت‌های اعتباری (کارت مالی).

نتیجه

با توجّه به رشد و توسعه فن آوری اطلاعات و ارتباطات و تأثیر آن بر تعاملات اجتماعی از یک سو و گسترش و تنوع جرایم رایانه‌ای و کثرت بزه دیدگان بالقوه در ایران و جهان از سوی دیگر، ایجاد قوانین قضایی جدید مرتبط و به روز ضرورت دارد تا بتواند پیامدهای منفی فناوری اطلاعات را پیشگیری کرده و یا کاهش دهد. تصویب قانون جرایم رایانه‌ای در ایران، گام مثبتی در جهت مقابله با مجرمان و کمک به توسعه‌ی فناوری اطلاعات بود.

نباید فراموش کنیم که اکنون با قوانینی در رابطه با جرم‌های رایانه‌ای روبه‌رو هستیم که تمامی کاربران رایانه و اینترنت کشور را در بر گرفته و تکلیف‌هایی را بر عهده‌مان گذارده است. برای آگاهی از حقوق و تکالیفی که این قانون برایمان تعیین کرده، ساده‌ترین راه، می‌تواند مطالعه متن قانون و درک جوانب آن می‌باشد (فیروزمنش، ۱۳۸۸).

از آنجایی که جرایم رایانه‌ای هر روز بیشتر و با شیوه‌های متفاوتی رخ می‌دهند، باید ابتدا به فکر راه‌های پیشگیری باشیم. با تصویب قوانین بازدارنده می‌توان از رخداد این جرایم جلوگیری کرد. همان‌گونه که در متن مقاله ملاحظه شد در بسیاری از کشورها

[1].(CYCO=Coordination Unit for Cybercrime Control)

قوانین سختی وجود دارد که باعث می‌شود این گونه جرایم کمتر رخ دهند. هم‌چنین جریمه‌های مالی سنگین و زمان بیشتر محکومیت در زندان برای مجرمان بر اساس قانون جرم‌های اینترنتی در ایالات متحده، وجود داشت.

در ایران نیز از آنجا که دولت الکترونیک در دستور کار قرار گرفته است، باید قوانین لازم را برای کاهش هرچه بیشتر این دسته مشکلات و جرم‌های رایانه‌ای، تصویب شود تا بتوانیم در بخش‌های گوناگون هم‌چون؛ تجارت الکترونیک هم گام‌های خوبی برداشته شود. هم‌چنین باید از اجرای کامل و صحیح این قوانین نیز اطمینان حاصل کرد. بدون شک، انجام کارهای مطالعاتی و تحقیقاتی در زمینه‌ی موضوعات مهّم، حساس و مبتلا به جامعه یکی از ضروریات حوزه‌های دانشگاهی است. بنابراین پیشنهاد می‌شود تا بتوانیم با آگاهی از خطرهای بالقوه جرم‌های رایانه‌ای، راه پیشگیری و مقابله با آن‌ها را به دست آوریم.

با مطالعه‌ی قانون جرایم رایانه‌ای، متوجه می‌شویم تنها دو شکل از انواع ضمانت-اجراها یا همان مجازات وجود دارد: جریمه‌ی نقدی و زندان. امّا در قوانین کشوری مانند ایالات متحده، گمان می‌رود سخت‌گیری بیشتری صورت می‌گیرد و مجازات‌هایی هم‌چون تعلیق، حبس خانگی، کار عام‌المنفعه، جبران مالی خسارت‌های وارده و حبس در نظر گرفته می‌شود.

گمان می‌رود تصویب قوانین سخت، اِعمال دقیق و بدون رعایت مصالح شخصی قوانین و تنوع در ضمانت‌اجراهای به کار گرفته شده، شرایط مناسب‌تری را برای رشد و توسعه فناوری اطلاعات و ارتباطات فراهم آورد.

دولت باید آسیب‌های بخش جرایم رایانه‌ای و اینترنتی را در کشور کاهش داده و با آموزش جوانان در چگونگی استفاده از اینترنت و توضیح اخلاق مجازی[1] که اشاره به یک سری از رفتارهای سالم و مسؤولانه در جامعه افراد حاضر در اینترنت است، خطاهای کمتری را شاهد باشیم.

با آموزش اخلاق مجازی به درک خطر رفتارهای مضر و غیر قانونی آنلاین و یادگیری این‌که چگونه از خودمان محافظت کنیم دست می‌یابیم. هم‌چنین مناسب است

[1].cyber ethics

دولت تمرکز بر افزایش همکاری‌های بین المللی در این زمینه را در دستور کار خود قرار دهیم و کنوانسیونی درباره‌ی قوانین مبارزه با جرم و جنایت رایانه‌ای را توسعه بدهیم تا بتوانیم در دنیای بدون مرز اینترنت با ایجاد مجموعه‌ای از قوانینی با استاندارد بین المللی در رابطه با جرم و جنایت رایانه ای، از میزان این جرم‌ها بکاهیم و در فضای مجازی، احساس امنیت بیشتری داشته باشیم.

در پایان، شایان ذکر است که در کشورهای دیگر با ایجاد مجازات‌های سنگین در نفوذ با رایانه‌ها، به امنیت اطلاعات فردی و حریم شخصی توجّه زیادی شده که این مسأله تا حدودی در قوانین جرایم رایانه‌ای ما کم رنگ‌تر است و یا مجازات‌های سبک‌تری که راه را برای متخلّفان و سودجویان باز خواهد کرد و هم‌چنین فرد باید ابتدا در یک جامعه‌ی سالم و بانشاط احساس امنیت کند که بتواند این حس خوب را نیز به دیگران در خانواده و محیط کارش منتقل کند تا این که جامعه‌ای داشته باشیم که حس امنیت در آن موج می‌زند.

هم‌چنین، به کاربران اینترنتی پیشنهاد می‌شود که بدون شناخت نسبت به ارتباط ایمیل، چت و وب کم در فضای مجازی اقدام نکنند تا مورد سوء استفاده‌های موجود در این حوزه قرار نگیرند. یکی از مسایلی که هر کاربر اینترنتی دارای وبلاگ یا سایت باید به آن توجّه نماید، قوانین و مقررات حاکم بر فضای مجازی می‌باشد تا با آموزش پیشگیری از جرم، به کاهش آن کمک نمایند.

به پژوهش‌گران نیز پیشنهاد می‌شود به بررسی و تحلیل علمی و انجام مطالعات مقایسه‌ای به منظور درک بهتر مفاهیم و شناخت کاستی‌ها، نواقص و نوآوری‌های قوانین مصوب مرتبط با جرایم رایانه‌ای بپردازند.

🕮 کتاب‌نامه:

۱. خبرگزاری مهر، **میزان و انواع جرائم رایانه‌ای در ایران**، ۱۳۸۸، دسترسی از وب سایت: http://qom.iran-tejarat.com/News/Cat21/News31028.html

۲. خرّم آبادی، عبدالصمد، **کلاهبرداری رایانه‌ای از دیدگاه بین المللی و وضعیت ایران**، نشریه فصلنامه حقوق، دوره۲ شماره ۱، ۱۳۸۶.

۳. دانش، تاج زمان، **مجرم کیست؟ جرم شناسی چیست؟** تهران، نشر کیهان، ۱۳۸۸.

۴. دهقانی، محمود، **پیش گیری از وقوع جرم و نقش سازمان‌های مسؤول در قوانین ایران**، تهران، نشر جنگل، ۱۳۸۹.

۵. سایت علمی دانشجویان ایران، **جرایم رایانه‌ای**، ۱۳۸۹، دسترسی از وب سایت: http://www.daneshju.ir/forum/f780/t93795.html

۶. سازمان ملل، **نشریه بین المللی سیاست جنائی**، ترجمه‌ی دبیرخانهٔ شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور، ۱۳۷۶.

۷. صناعی، محمود، **مرکز تحقیقات رایانه‌ای علوم اسلامی**، تحلیل ناکامی، ماهنامه سخن، ۱۳۸۹.

۸. فیروزمنش، افشین، **قانون مطبوعات و نشریات االکترونیکی**، ماهنامه تحلیلگران عصر اطلاعات، ۱۳۸۸، دسترسی از وب سایت :www.infoage.ir

۹. کانون وکلای دادگستری منطقه اصفهان، **جزئیات جرایم رایانه‌ای در ایران**، ۱۳۸۹، دسترسی از وب سایت: http://isfahanbar.org/?part=news&inc=news&id=52

۱۰. مدیر وب سایت آگهی سارا، **نگاهی به تعریف و مبانی جرم رایانه‌ای و کامپیوتری در فضای سایبر و اینترنت**، ۱۳۸۹، دسترسی از وب سایت: http://www.agahisara.ir/cms/archives/162259

۱۱. مدیر وب سایت لینک‌های مفید، **متن کامل قانون جرایم رایانه‌ای**، ۱۳۸۹، دسترسی از وب سایت: http://mofidlinks.ir/0-8.htm

۱۲. وب سایت وکالت، **گذشت ۷ سال از تدوین لایحه جرائم رایانه‌ای و میزان تطابق با فناوری روز**، ۱۳۸۸، دسترسی از وب سایت: http://www.vekalat.org/public.php?cat=2&newsnum=1242852

13. Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (eds) Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York, 2006.

14. Casey, E, Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet (2nd ed.). Amsterdam: Elsevier Academic Press, 2004.
15. Carroll, J. M, Computer security. USA: Butterworth-Heinemann Press, 1996.
16. Computer forensics, Cyber Crime Statistics. Access on: http://www.computer-

orensics recruiter.com/home/cyber_crime_statistics.html, 2010.

17. enigmasoftwar, Top 20 Countries Found to Have the Most Cybercrime. Accessed on 16 April 2011, from http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime, 2009.
18. Grabosky, P, Electronic Crime, New Jersey: Prentice Hall, 2006.
19. InfoTech, Computer Crime Prevention Law, 2010, Access on:

http://infotech.siuc.edu/docs/pages/prevent.htm. Kim, M. W. (1997). How countries handle

computer crime. Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier,

Fall 1997.

20. McQuade, S. The Encyclopedia of Cybercrime, Westport, CT: Greenwood Press, 2009.
21. Moore, R, Cybercrime; investigating high-technology computer crime, 2005. Publisher: Anderson Publishing Co.
22. Ringwelski, M, Effects of Cyber Crime, 2011, Access on: http://www.ehow.com/about_5052659_effects-cyber-crime.html
23. Richmond, R, Internet Fraud Declined in 2010. The New York Times, 2011.
24. Samuel, M, Computer Crime and Information Technology Misuse. Publisher: Commonwealth Publishers, 2008.
25. The International Trade Administration, U.S. Department of Commerce. (2011). Protecting intellectual property rights. Access on: http://www.stopfakes.gov/
26. Walden, I, Computer Crimes and Digital Investigations, Oxford: Oxford University Press, 2007.
27. Wesley, W, Laws on Computer Crime, 2010, Access on:

http://www.ehow.com/about_5414732_laws-computer-crime.html.

28. Williams, M, Virtually Criminal: Crime, Deviance and Regulation Online, Routledge, London, 2006.