جرایم رایانه ای و مقایسه ایران با سایر کشور ها‎

شبکه آموزشی پژوهشی ایران – مادسیج

madsg.com

چکیده

امروز بحث فناورى­اطلاعات­­­ و ­ارتباطات نوین، که تجلى روشن ­آن­ فضاى‏­ تبادل ­اطلاعات (فضاى­سایبر) ­است. مسئله­جدیدى را با عنوان پاسخگویى‏ به سوء استفاده‏هایى که از فضاى تبادل اطلاعات به عمل مى‏آید پیش روى‏ دانشمندان علوم جنائى قرار داده است. در این پایان نامه ­جرايم­ رایانه‏ای را ­در ابعاد خرد­ و کلان ­را مورد بررسى‏ قرار مى‏دهم، این بحث در قالب دو بخش دنبال مى‏شود. در بخش­اول، پس‏­از­توضیحاتي راجع به تاريخچه جرائم رایانه‏اى، به تعاريف و برداشت­هاي مختلف آن پرداخته ­و انواع و خصوصيات هركدام را بيان ميكنيم ودربخش دوم مقاله­ به محتواي اين نوع جرايم گوشه چشمي داريم سپس آثار مخرب جرايم رايانه­اي را به تفصيل توضيح داده و در ادامه. نحوه پيشگيري از اين ­جرايم و بالاخره در آخر از جرايم رايانه­اي در­كشورمان بحث خواهيم كرد. من در تلاش بودم که یک پایان نامه خوبی جمع­آوری ­کنم بخاطر همین پیگیرکارها و منابع خوبی بودم که در اول با کار پلیس فتا نیروی انتظامی آشنا شدم که خیلی بر اطلاعات ­خودم در ضمینه آشنایی با جرایم اینترنتی و دیگر مباحث آشنا شدم پس از آن به انقلاب رفتم که منابعی در این ضمینه پیدا کنم که بتواند در نگارش پایان نامه کمکم کند.

کلید واژه‏­ها:جرم رایانه‏اى- پیشگیرى جرايم رايانه­اي –آثار مخرب جرايم رايانه­اي

مقدمه

بشر در طول حیات خود اعصارگوناگونى را پشت سر­گذاشته و هریک از آنها را با الهام از تحول عظیمى که در آن عصر پدید آمده و گامى از رشد و تکامل بشرى را رقم زده نامگذارى کرده است، مانند: عصر آتش، عصر آهن‏ و عصر حاضرکه عصر فناورى اطلاعات و ارتباطات نام گرفته است.

هنوز نیم قرن از­ اختراع اولین رایانه نمی­گذرد، آن هم رایانه‏اى 30 تنى که‏ البته سرعت عمل آن از ابتدایى‏ترین ماشین­حساب‏هاى دیجیتال­امروزى نیز کمتر بود، اما به هرحال تحولى شگرف در دنیاى علم و فناورى محسوب‏ مى‏شد و از همین رو رایانه‏ها در این مدت کم به خوبى توانستند­ جاى­خود­را در تمامى شئون زندگى انسان باز کنند و به نوعى خود را درتمامى پیشرفت‏ها سهیم سازند. این اقبایل عمومى­­ بهره‏بردارى ­روزافزون از سیستم‏هاى‏ رایانه‏اى زمانى شتاب بیشترى به خود گرفت که در ابتداى دهه­ی نود میلادى‏ امکان متصل شدن آنها به یکدیگر در سراسر جهان فراهم شد. در این زمان‏ بود که مشاهده شد مرزها و موانع فیزیکى بى‏اثر شده و به نوعى رؤیاهاى‏ جهانى بشر واقعیت یافته است. اما از آنجا که این پدیده­ی شگفت‏انگیز از همان بدو تولد در دسترس‏ همگان قرار گرفت،هرکس مطابق اغراض و مقاصد خود از آن سود مى‏جست و نتیجه آن شد که بعضى از این بهره‏بردارى‏ها جنبه­ سوء­استفاده­ به‏­ خود گرفت­ و­ سیاستگذاران­ خرد­ و کلان را مجبور کرد که تدبیرى‏ بیاندیشند. این سوءاستفاده‏ها که در مجموع جرائم رایانه‏اى نام گرفته‏اند، طیف جدیدى­از جرائم هستند که به سبب ویژگى‏هاى متمایزى که با جرائم‏ سنتى دارند،تصمیم‏گیران جامعه را بر آن داشته‏اند تا در ابعاد مختلف‏ اقدامات متمایزى را طرح‏ریزى کنند. جرايم رايانه­اي جرايمي سازمان يافته­اند كه از طريق اشخاص حرفه­اي و باسواد انجام مي­شوند و هميشه قوانين رايانه­اي امروزه براي مجازات مجرمين كافي اما كامل نمي­باشد چون هر روز جرايم جديدي به وجود مي­آيد كه براي مجازات آنها نياز به قوانين جديد داريم همانگونه كه جرايم اينترنتي هميشه درحال روز شدن هستند بايستي تلاش كرد تابتوان با نو شدن جرايم هرساله قوانيني را كه در زمينه جرايم جديد قابل اعمال باشد ارائه كرد چون رايانه واينترنت هميشه وهميشه شكل­هاي مختلفي به خود   
مي­گيرند براي پيشگيري از اين جرايم باید همه دستگاه­ها تلاش كنند و مردم نيز توصيه­هاي مسئولين را در اين مورد جدي بگيرند ودر هنگام استفاده از اينترنت و رايانه مورد استفاده قرار دهند تا مورد سوء استفاده ديگران قرارنگيرند. همچنين اگر ديدند سايت يا وبلاگي برخلاف قوانين تعيين شده در حال­ارایه مطلب باشد موضوع راسريعا به دادستاني اطلاع تا نسبت به اعمال فيلتر درمورد آن سايت­اقدام شود قضات نيز مي­بايست به شدت با كساني كه اقدام به جرايم رايانه­اي مي­كنند برخود نمايند چون اين جرايم هم سبب بردن مال وهم سبب بردن ابروي اشخاص ميگردد برخورد قضات نيز در پيشگيري از وقوع جرم اهميت دارد بايست سعي شود در زمينه جرايم رايانه اي مجازات ها بازدارندگي بيشتري داشته باشد تا هم سبب ارعاب مردم وهم سبب عبرت گرفت مجرمين شود تا ديگر اقدام به چنين جرايمي ننمايند.

**فصل اول**

**تاریخچه جرایم رایانه­ای**

1-1تاريخچه­ جرايم رايانه­ای

 البته­ بايد ­ما­ بدانيم که ­هميشه در­ اعصار­ و قرون مختلف و در گذشته، هر زمان که پديده و­ علمي وارد   
­عرصه زندگی شده و داراي بعد مثبت بوده و استفاده­هاي مثبت از آن مي­شده و هم استفاده­هاي منفي و رايانه هم از اين قاعده مستثني نيست. رايانه در عين حال که داراي استفاده­هاي مثبت فراواني است، می­تواند بعنوان ابزار بزهکاری درجهت ­ضرر منافع مردم مورداستفاده قرار گیرد.

به دليل بهره­مند نبودن دولت ها و کشورها از فناوري ­و تکنولوژي تعيين تاريخ دقيق شروع جرم رايانه­اي سخت به نظرمي­رسد. چرا­که­ همان­طور که مي­دانيد برخي­ازکشورها مثل­آمريکا­ که­از­سطح تکنولوژي بالايي برخوردارند   
­به مراتب تاريخ وقوع جرم کلاهبرداري رايانه­اي بسيار زودتر از کشور ماست به هر عنوان تعيين دقيق اولين جرم رايانه­اي­کار دشواري ­است چرا که ­اگر ما حتي بگوييم مثلاً در قضيه الدون رويس اولين جرم رايانه­اي اتفاق افتاد باز هيچ دليل قاطعي وجود ندارد که قبل از آن جرم اتفاق نيفتاده باشد. شايد بتوان تاريخ اولين جرم رايانه­اي را به زماني نسبت دادکه چرتکه وارد محاسبات افراد بشر شد.

تعيين زمان واقعي ارتکاب اولين جرم کامپيوتري­کار دشواري­ است. کامپيوتر از زمان­چرتکه که ­از3500 سال­قبل ­از ميلاد در ­ژاپن، چين و هند وجود داشته، به نوعي مطرح بوده است. در سال 1801 انگيزه­هاي مالي باعث شد تا ژوزف ژاکارد يکي­از­صاحبان­کارخانه­هاي نساجي درفرانسه، اولين کارت کامپيوتري­را طراحي­کند. اين دستگاه امکان تکرار يک رشته مراحل پياپي­ ­را ­دریافت پارچه­هاي ­مخصوص­ فراهم ­مي­ساخت.

براساس نوشته­هاي «پروفسور الريش زيبر»­ درکتاب "پيدايش بين المللي­حقوق­کيفري­اطلاعات" اولين مواردي که جرم رايانه­اي ناميده شده ابتداعاً در مطبوعات عمومي و در­ادبيات­علمي دهة1960 ظاهرشد. اين­موارد ­شامل سوء استفاده­هاي ابتدايي ­از رايانه، سابوتاژ (خرابکاري) رايانه­اي، جاسوسي­رايانه­اي و استفاده ­غيرقانوني ­ازسيستم  
­رايانه­اي بود. البته چون اکثر گزارشات بر مبناي نوشته­هاي روزنامه­ها بود در مورد واقعيت يا خيالي بودن پديدة جديدجرم­ رايانه­اي بحث و­ترديد وجود داشت، از اواسط1970مطالعات تجربي در مورد جرم رايانه­اي با استفاده­ از متدهاي­ تحقيقاتي ­رشتة جرم­شناسي­ انجام­شد.­اين مطالعات ­ناظر­ به ­برخي از جرائم­رايانه­اي ­مي­شد.

**1-2انواع و ویژگی­های جرائم ­رایانه­ای**

جرایم­رایانه­ای امروز از­گستردگی زیادی برخوردار است، اما به طورخلاصه و براساس تقریبی دسته­بندی دهمین کنگره سازمان ملل متحد که در آوریل ۲۰۰۰ در زمینه جرم و رفتار مجرمان در وین برگزار شد،  
 می­توان آن را در چند دسته کلی بخش­بندی کرد:

"دسترسی غیرقانونی" که عبارت است از دسترسی به بخش یا کل یک سیستم کامپیوتری بدون داشتن حق و مجوز، جلوگیری غیرقانونی از دسترسی به داده­های شخصی با استفاده از ابزار تکنولوژیک و یا در داخل یک سیستم کامپیوتری؛ مداخلات اطلاعاتی همچون آسیب رساندن، حذف، جایگزینی، تخریب و یا سرکوب و توقیف داده­های کامپیوتری بدون مجوز؛ مداخله در سیستم­ها شامل انسداد و توقف جدی و بدون حق عملکرد سیستم­  
کامپیوتری با آسیب­رساندن، حذف، جایگزینی، تخریب و یا توقیف ­داده­های کامپیوتری؛ سوءاستفاده از دستگاه­ها جعل هویت و کلاه­ برداری الکترونیک.

جرایم را به سه دسته میتوان تقسیم کرد:

1-جرایم علیه اشخاص

2-جرایم علیه اموال

3- جرایم علیه دولت ها

**1-3 دسته بندی جرايم**

جرایم رايانه­اي را می­توان­ به 3 دهه تقسيم می­شود:

* دهة60 : پيدايش قضيةرويس، توجه ­مطبوعات و حقوقدانان، ايجاد مشکل دريافتن توصيف مجرمانه براي اعمال­ ارتکابي و ماهيت ­اين اعمال ­پيش­آمد.
* دهة 70: بروز قضيه هاي ژرمن هراشتات، امريکن اکويتي فالزينگ، شرکت سوئدي ولو، شروع مطالعات جزايي­به­صورت­محدود،­ تجزيه­و تحليل موارد ارتکابي و مباحث تئوريک در قالب دکترين­حقوق اقتصادي وکيفري­روي­داد.
* در دهة80: تفسير بنيادين ديدگاه عمومي و علمي ­در ­زمينه ­جرايم­رايانه­اي، افزايش سرقت برنامه­ها، تخلف صندوق­داران، سوء­استفاده هاي ­ارتباطات­ راه ­دور، پيدايش­چارچوب­هاي­ اولية  
   ­جامعه اطلاعاتي و قواعد­حاکم بر آن، افزايش وسعت جرائم ارتکابي و تبديل نوع جرايم از جرايم اقتصادي­ رايانه­اي به جرايم عليه­منافع­همه­جانبة­رايانه­اي،­­ ­ارائة اولين­ تعريف­جرايم­رايانه­اي­«سازمان  
  ­توسعه و همکاري اقتصادي». (هرگونه­رفتارغيرقانوني، غيراخلاقي وياغيرمجاز­ با­استفاده­از­فناوري  
  ­داده­پردازي­خودکار­ و ­يا­ انتقال­داده­ها)، شيوع انتقال­غير­قانوني سرمايه­ها با­استفاده از ابزار­الکترونيکي، خرابکاري، ويروس­ها و کرم­هاي ­رايانه­اي­ جعل اسناد و تغيير چارچوب بحث ها از دکترين حقوق اقتصادي، کيفري به حقوق اطلاعاتي، کيفري مطرح شد.

**فصل دوم**

**تعریف جرایم رایانه­ای**

2-1تعریف جرم رایانه­ای

1. جرم رایانه­ای چیست؟

جرایم اینترنتی­ و­ رایانه­ای نوعی­جرایم جدید است که طيف­ گسترده ­افعال ­مجرمانه‌اي ­كه اين­ مفهوم ­جا دارد و ماهيت­ متغير ­آن ­ ناشي ­از­ پيشرفت­ لحظه­ به­ لحظه فناوري­اطلاعات­ و­ شيوه‌هاي ­سوءاستفاده ­از آن است­.

تا آنجا­ كه­ در­ جديدترين­ و­ جامع‌ترين­ سند­ بين‌المللي­ در ­اين ­زمينه که در ­(کنوانسيون­ جرايم ­سايبر ­2001 بوداپست) تعريفي از اين­ جرايم ­به عمل نيامده­ است. به ­نظر­ می­رسد­کامل­ترین ­تعریف­ این ­باشد: «هر جرمي كه قانونگذار به صراحت ­رايانه را به منزله موضوع­ يا وسيله­ جرم ­جزء ­ركن ­مادي­ آن اعلام ­كرده باشد، يا­ عملاً ­رايانه  
 ­به ­منزله موضوع ­يا وسيله ­ارتكاب ­يا وسيله ­ذخيره يا ­پردازش يا ­انتقال­دلايل­جر­م ­در­آن ­نقش ­داشته ­باشد».   
 این تعریف هم علاوه بر جرايم ذكر شده در دو دسته قبل، جرايمي را نيز ‌كه صرفاً دلايل آنها يا اطلاعات مربوطه در رايانه ذخيره شده‌اند، به لحاظ تأمين بهتر اهداف تحقيق و تعقيب جرم با در نظر گرفتن قواعد خاص آيين دادرسي کيفري، جزء جرايم رايانه‌اي دانسته است.

برخي از نويسندگان، جرم رايانه­اي را مترادف جرم سايبري مي­دانند و آن دو را داراي دو معني ­و مفهوم  
 مي­دانند. «در تعريف دیگر، جرم کامپيوتري جرایمی است که در فضاي سايبر رخ مي­دهد از اين نظر جرايمي مثل هرزه نگاري، افترا، آزار و اذيت و سوء استفاده از پست الکترونيکي و ساير جرايمي که در آنها کامپيوتر به عنوان ابزار و وسيلة ارتکاب جرم بکار گرفته مي­شود، در زمرة جرم کامپيوتري قرار نمي­گيرد. در تعريف دیگری از جرم کامپيوتري هر فعل و ترک فعلي که «در» يا «از طريق» و يا «به کمک» اتصال به اينترنت، چه به طور مستقيم، يا بطور غیرمستقيم رخ مي­دهد و توسط قانون ممنوع گرديده و براي آن مجازات در نظر گرفته شده است جرم کامپيوتري ناميده مي­شود. و بر اين اساس جرايم کامپيوتري را مي­توان به سه دسته تقسيم بندی کرد:

**دسته بندی جرایم رایانه­ای**

* دستة اول: جرايمي هستند که در آنها رايانه و تجهيزات جانبي آن موضوع جرم واقع مي شوند مانند سرقت، تخريب­ و غيره.
* دستة دوم: جرايمي هستند که در آنها کامپيوتر به عنوان ابزار یا وسيله توسط مجرم براي ارتکاب جرم بکار گرفته مي­شود.
* دستة سوم: جرايمي هستند که مي توان آنها را جرايم کامپيوتري محض ناميد. اين نوع از جرايم کاملاً با جرايم کلاسيک تفاوت دارند و در دنياي مجازي به وقوع مي­پيوندند. اما آثار آنها در دنياي واقعي ظاهر مي شود، مانند دسترسي غير مجاز به سيستم هاي کامپيوتري، سازمان همکاري و توسعه اقتصادي جرم رايانه­اي را چنين تعريف مي­کند «سوء استفاده از کامپيوتر شامل هر رفتار غير قانوني غير اخلاقي يا غير مجاز مربوط به پردازش اتوماتيک و انتقال داده­هاست».

«کميتة اروپايي مسائل جنايي در شوراي اروپا در سال 1989 گزارشگری بيان کرد که در آن يکي از متخصصان چنين تعريفي ارائه کرده است : هر فعل مثبت غير قانوني که کامپيوتر، ابزار يا موضوع جرم باشد، يعني به عبارت ديگر هر جرمي که ابزار يا هدف آن تأثيرگذاري بر عملکرد کامپيوتر باشد».

پليس جنائي فدرال آلمان جرم کامپيوتري را چنين تعريف مي­کنند «جرم کامپيوتري در بر گيرندة همة اوضاع و احوال و کيفياتي است که در آن شکلهاي پردازش الکترونيک داده­ها، وسيلة ارتکاب و يا هدف يک جرم قرار گرفته است و مبنايي براي نشان دادن اين است که جرمي ارتکاب يافته است.»همچنين پليس ژاپن جرم کامپيوتري را چنين تعريف کرده است: «حوادثي که موجب تخريب عملکرد سيستم کامپيوتر يا استفاده غير قانوني از آن باشد، جرم کامپيوتري است.».

در مورد اين تعريف بايد گفت که پليس ژاپن حوادثي که موجب تخريب سيستم کامپيوتر شود را نيز جزء جرايم آورده­اند که به اطلاق حوادث در اين تعريف ايراد وارد است که چرا ما بايد بين زماني که فردي حادثه را ايجاد مي­کند و تخريب در عملکرد سيستم مي­آورد مرتکب جرم مي­شود و موجب ضرر مي­شود که در اين مورد ما نمي­توانيم آن را جرم بدانيم، چرا که به ­وجود عنصر اراده مختل شده و ما مي­دانيم که مسلوب اراده بودن باعث رفع مسئوليت کيفري است و در اين زمان ما نمي­توانيم فرد را مجرم بدانيم و اطلاق تعريف در حادثه شامل مورد دوم يعني حوادث قهري نيز مي­شود که صحيح به نظر نمي­رسد و بهتر بود حادثه را به شکلي   
مي­آورد که فقط شامل مورد دوم شود. همچنين وزارت دادگستري آمريکا «هر گونه عمل ناقض قانون کيفري که مستلزم آشنايي با دانش مربوط به تکنولوژي کامپيوتر جهت ارتکاب عمل، تعقيب و يا رسيدگي به آن باشد، جرم کامپيوتري است». اين تعريف نيز کامل به نظر نمي­رسد بدين توضيح که يک زمان رايانه وسيلة ارتکاب جرم مي شود يعني اينکه ما از کامپيوتر براي جعل و کلاهبرداري استفاده مي­کنيم با دانشي که از کامپيوتر داريم اقدام به عمل متقلبانه و بعد از فريب بزه ديده کلاهبرداري مي­کنيم که در اين صورت کلاهبرداري ما «کلاهبرداري کلاسيک رايانه­اي» است و با «کلاهبرداري رايانه­اي محض» فرق دارد و يک زمان ما با مداخله در سيستم بدون اينکه آن را وسيله قرار دهيم و بدون اينکه نياز به فريب باشد در جرم کلاهبرداري مثلاً ما اقدام به انتقال وجه به خود يا ديگران مي­کنيم که در اين حالت کامپيوتر وسيلة نيست که تعريف اين مسأله را شفاف بيان نکرده است و از تعريف اينگونه استنباط مي­شود­ که اين تعريف شامل مواردي مثل کلاهبرداري رايانه­اي محض­نمي­شود قبل از هر چيز بايد بيان شود که ما بايد بين جرم رايانه­اي به معناي اعم قائل به تفکيک شويم جرايم رايانه­اي­ به معناي اعم هم شامل جرايم عليه داده­ها و هم شامل جرايم محيط سايبر مي­شود ولي جرايم رايانه­اي شامل جرايم رايانه­اي نسل اول مي­شود.

2-2 قوانین جرایم رایانه­ای نسل اول:

1- ما بايد بين جرايم رايانه­اي با جرايم سايبر قائل به تفکيک شويم چرا که همان طور که در گفتار اول اشاره شد جرايم رايانه­اي جزء جرايم رايانه­اي نسل اول هستند و جرايم سايبر جزء جرايم رايانه­اي نسل سوم هستند که بين اينها فرق وجود دارد. حتي اگر جرايم رايانه­اي را نيز به طور اعم بگيريم جرايم رايانه­اي مترادف جرايم سايبر (جرايم محيط مجازي) نيست که برخي از نويسندگان به اشتباه اين دو را با هم مي­آورند. بلکه   
جرايم رايانه­اي به معناي اعم هم شامل جرايم رايانه­اي شامل جرايم عليه داده­ها و هم شامل جرايم سايبر   
مي­شود و شموليت دارد. که خود آن جزئي از جرايم فناوري اطلاعات است. و به نظر بنده جرايم اينترنتي نيز شامل جرايم رايانه­اي به معناي اعم مي­شود.

2- تعريفي که سازمان همکاري و توسعه اقتصادي ارايه داد نيز به نظر بنده جامع و کامل نيست و شامل جرايمي که عليه رايانه انجام مي­شود يا جرايمي که توسط رايانه انجام مي­شود و اين سازمان هر رفتار غير اخلاقي يا غير مجاز مربوط به پردازش اتوماتيک و انتقال داده­ها را جرم رايانه­اي گفته­اند که يک شکل از جرايم رايانه­اي است نه همه­ آن. و همچنين تعريف کميتة اروپايي که شامل مثلاً سرقت خود صرف کامپيوتر   
نمي­شود. به نظر بنده نياز جامعه بين المللي است که يک کنوانسيون جامع و کلي در مورد جرايم رايانه­اي به تصويب کشورها برسد که هم هماهنگ با سيستم­هاي حقوقي گوناگون باشد و هم جامع و کامل باشد و بعد به تبع آن يک سازمان بين المللي در مبارزه با جرايم رايانه­اي تشکيل شود که اولاً در جهت کمک به کشورهاي در حال توسعه براي محافظت از سيستم­هاي خود ثانياً کمک به کشورهاي در حال توسعه براي تضمين و قانونگذاري صحيح و در يک کلام مبارزه با اين پديده محرمانه به شکل منسجم و صحيح که پيشنهادهاي بنده در ادامه در مورد اين سازمان بين المللي بيان خواهد شد.

**3-2 تقسیم­بندی جرائم رایانه­ای**

**به دو دسته تقسیم می­شوند:**

1. جرايم رايانه‌اي محض: جرايمي كه ارتكاب آنها قبل از پيدايش رايانه و اجزاي فناوري اطلاعات امكان پذير نبوده‌اند؛ مانند دسترسي غيرمجاز.
2. جرايم رايانه‌اي سنتي: كه ارتكاب آنها وسيله رايانه داراي عواقبي بسيار شديدتر نسبت به ارتكاب سنتي آن است؛ مانند برخي جرايم مرتبط با محتوا مانند هرزه‌نگاري و يا تخريب فيزيكي نسبت به كامپيوتر.

**3-3تعریف موسع جرایم رایانه­ای:**

هر جرمي كه قانونگذار به صراحت رايانه را به منزله موضوع يا وسيله جرم جزء ركن مادي آن اعلام كرده باشد يا عملاً رايانه به منزله موضوع يا وسيله ارتكاب جرم در آن نقش داشته باشد. اين تعريف علاوه بر جرايم دسته قبل، آن دسته از جرايم سنتي را نيز كه با استفاده از رايانه و فناوري اطلاعات ارتكاب يابند را، بدون اينكه تغييري در عنصر مادي آنها صورت گرفته باشد، يا قانونگذار رايانه را جزء اين عنصر برشمرده باشد، مشمول اين عنوان مي‌داند؛مانند توهين به يك فرد كه از طريق پست الكترونيكي صورت پذيرفته باشد يا تخريب عمدي تجهيزات رايانه‌اي.

**فصل­سوم**

**انواع و ویژگی­های**

**جرایم رایانه­ای**

جرایم رایانه­ای امروز از گستردگی زیادی برخوردار است، اما به طور خلاصه و بر اساس تقریبی دسته­بندی دهمین کنگره سازمان ملل متحد در آوریل ۲۰۰۰ در زمینه جرم و رفتار مجرمان در وین می توان آن را در چند دسته کلی بخش­بندی کرده است.

* دسترسی غیرقانونی :که عبارت از دسترسی به بخش یا کل یک سیستم کامپیوتری بدون داشتن حق و مجوز این کار است؛ جلوگیری غیرقانونی از دسترسی به داده های شخصی با استفاده از ابزار تکنولوژیک از و یا در داخل­ یک ­سیستم­کامپیوتری، مداخلات اطلاعاتی همچون آسیب­رساندن­­­­­­­،حذف، جایگزینی، تخریب و یا سرکوب و توقیف داده­های کامپیوتری بدون مجوز، مداخله در سیستم­ها شامل انسداد و توقف جدی و بدون حق عملکرد سیستم­های­کامپیوتری­ با­ آسیب­رساندن، حذف، جایگزینی، تخریب ­و یا ­توقیف ­داده­های ­کامپیوتری، سوءاستفاده از دستگاه­ها، جعل هویت و کلاهبرداری الکترونیک.

**3-1 انواع جرم­هاي رايانه­اي**

"هك كردن" عبارتست از نفوذ به يك سيستم كامپيوتري بدون داشتن مجوز، مالكيت يا صلاحيت لازم. هك كردن يعني غلبه كردن بر سيستم­هاي امنيتي يك سيستم كامپيوتري براي دسترسي غير قانوني به اطلاعات ذخيره شده. لو رفتن رمز عبور به قصد دسترسي به اطلاعات خصوصي افراد يك سازمان يكي از  
رايج­ترين تخلفات رايانه­اي است. يكي از خطرناك­ترين خلاف كاري­هاي رايانه­اي عبارتست از هك كردن آدرس IP تا بدين وسيله خلافكار خود را به جاي شخص ديگری جا بزند و افكار شوم يا جنايات مورد نظر خود را اجرا كند.

فيشينگ[[1]](#footnote-1) : عبارتست از تلاش براي بدست آوردن اطلاعاتي مانند رمز عبور، شناسه عبور و جزئيات كارت اعتباري با جا زدن خود به عنوان يك منبع قابل اعتماد.

فيشينگ از طريق سرويس­هاي ايميل يا با وعده هاي دروغ انجام مي گيرد يا با ايجاد برخي جذابيت ها كاربران اينترنتي را ترغيب مي­كنند اطلاعات خود را در سايت­هايي كه توسط كلاه برداران ساخته شده است وارد كنند. اين خلاف كاران معمولاً وب سايت هايي طراحي مي­كنند كه در كاربر احساس اعتماد و وارد شدن در يك سايت امن را مي دهد و معمولاً هم موفق مي­شوند يعني كاربر در دام آن­ها افتاده و اطلاعات خود را وارد می­کند.

**حمله فيشينگ چيست؟**

فیشینگ نوع بسیار خاصی از جرائم رایانه­ای است که برای فریب دادن شما در زمینه افشای جزئیات مالی و شخصی شما، طراحی شده است. مجرمان رایانه­ای، یک وب سایت جعلی ایجاد می­کنند که بسیار شبیه به وب سایت بانک (یا هر وب سایت دیگری که تراکنش­های مالی در آن انجام می­شود سپس تلاش می­کنند تا شما را به منظور بازدید از این سایت و تایپ کردن اطلاعات محرمانه خود نظیر اطلاعات شخصی و ورود به سایت، و گرفتن کلمه عبور فریب دهند. نوعاً مجرمان رایانه­ای تعداد زیادی نامه­های الکترونیکی ارسال می­کنند که حاوی یک فراپیوند به سایت جعلی است.

حمله فیشینگ نوعی دیگر از جرایم سایبری است که در آن، مجرم یک کپی تقریباً ۱۰۰ درصد شبیه یک وب سایت بنگاه تجاری، ایجاد می­کند. و تلاش می­کند تا کاربران را برای افشای جزئیات شخصی خود نام کاربری، کلمه عبور[[2]](#footnote-2)، و غیره از طریق یک فرم در سایتی جعلی فریب دهد که این اجازه را به مجرم می­دهد با استفاده از این اطلاعات پول به دست آورد.

فیشرها یا مجرمان فیشینگ از تکنیک­های متعددی برای فریب دادن کاربران به منظور دسترسی به سایت جعلی استفاده می­کنند. مثلاً، ارسال ایمیل­هایی که به نظر می­آید از یک بانک باشد. این ایمیل­ها اغلب از لوگوهای قانونی و یک سبک تجاری خوب استفاده می­کنند و سربرگ نامه را به گونه­ای طراحی می­کنند که شبیه این به نظر برسد که به بانکی قانونی تعلق دارند. به طورکلی، این نامه­ها به دریافت­کنندگان اطلاع   
می­دهند که بانک، زیرساخت IT خود را تغییر داده و از تمامی مشتریان می­خواهد که اطلاعات کاربری خود را مجدداً تصدیق کنند هنگامی­که دریافت کننده، روی لینک موجود در ایمیل کلیک می­کند، به سایتی جعلی هدایت می­شود که از او می­خواهد اطلاعات شخصی خود را وارد کند.

**گروه ويروس­هاي كامپيوتري:**

دسته­ ويروس­هاي كامپيوتري (شامل ويروس­ها، كرم­ها، نرم­افزار­هاي جاسوسي و غیره) در حقيقت نرم افزارهايي هستند كه خود را تكثير و منتشر مي­كنند و كامپيوترهاي موجود در يك شبكه را بدون اطلاع كاربران آلوده كرده و به آنها صدمه مي­زند. ويروس­ها از طريق فايل­هاي سيستم يك شبكه كامپيوتري، اينترنت يا هر وسيله نقل انتقال اطلاعات مانند حافظه فلش، و غیره وارد كامپيوترهاي ديگر مي­شوند. ويروس­هاي كامپيوتري كدهايي هستند كه با هدف ضربه زدن به يك سيستم رايانه­اي يا از بين بردن اطلاعات نوشته شده­اند. نوشتن ويروس كامپيوتري در همه جاي دنيا يك جرم است به گونه­اي كه نويسنده ويروس در برابر تمام خسارت­هاي وارده به همه كامپيوترهاي آلوده شده مسئول است.

**3-2وسایل سایبری[[3]](#footnote-3):**

عبارت­ است از استفاده از فناوري ­ارتباطات به خصوص اينترنت براي آزار و اذيت افراد. تهمت، ارسال  
 نرم افزارهاي مخرب و تخريب اطلاعات­و تجهيزات كامپيوتري دراين گروه قرار­ مي­گيرند. اين خلافكاران اغلب كاربران را از طريق چت­روم ها، تالارهاي تبادل نظر و اجتماعات اينترنتي شكار مي كنند سپس اطلاعات آنها را بدست مي­آورند (مثلاً شماره تلفن و آدرس، محل كار و غیره) و با استفاده از اين اطلاعات قربانيان خود را مورد اذيت و آزار قرار مي­دهند. ايميل­هاي تهديد آميز، مزاحمت تلفني و مانند اين­ها انجام مي­دهند و اين مورد يكي از جرم­هاي رايانه­اي خطرناك است كه در سراسر دنيا مجازات سنگيني برايش قرار مي­گيرد.

هويت جعلي: هويت جعلي يا خود را به جاي كس ديگر جا زدن يكي از جديدترين كلاه برداري­هايي است كه به كمك آن پول­هاي زيادي ربوده شده و سودهاي كلاني نصيب كلاه برداران مي­شود. در اين شيوه كلاه بردار خود را به جاي مالك جا مي­زند. يا از هويت شخص ديگري براي بدست آوردن كالا يا خدمات مورد نياز خود استفاده مي­كنند. مهاجرت غير قانوني، تروريسم و ايميل­هاي سياه در زمره اين جرائم قرار مي­گيرد.

در انواع جرائم رايانه­اي همه جرایم در يك چيز مشترك است و آن هم بهره برداري غير قانوني از فناوري جديد رايانه­اي و ارتباطات براي فعاليت­هاي خلاف كارانه است. همان طور كه فناوري جديد راهي براي مقابله ارائه  
 مي دهد از آن سو هم جنايتكاران از آخرين فناوري­ها سود مي­برند. و هميشه يك قدم از سيستم­هاي امنيتي جلوتر هستند. و هيچ راهي امن تر از احتياط نيست پس مراقب ايميل هاي ناشناس، چت روم­ها، حافظه­هاي فلش، وب سايت­هاي مشكوك و غیره باشيد و سعي كنيد اطلاعات بيشتري درباره امنيت در اينترنت پيدا كنید.

**3-3ویژگی های جرایم رایانه­ای**

این گونه جرایم را می­توان به سه دسته تقسیم کرد:

1- جرایم علیه اشخاص : جرایم علیه اشخاص را می­توان اذیت و آزارهای اینترنتی دانست که می­تواند به اشکال جنسی، نژادی، مذهبی و غیره رخ دهد. این جنبه معمولاً با حوزه دیگری به نام حریم خصوصی شهروندان تداخل پیدا می­کند که خود حوزه بسیار گسترده و قابل توجه دیگری است. از دیگر جرایم این دسته می توان به جرایمی مانند پورنوگرافی کودکان و آزار و اذیت­ها با استفاده از رایانه اشاره کرد که یکی از گسترده­ترین و شایع ترین جرایم موجود است.

2- دسته دوم شامل خرابکاری های کامپیوتری و تبادل برنامه های خطرناک است. جرایم علیه اموال   
 3-جرایم علیه دولت­ها : شایع ترین نمونه این جرایم، سرقت اطلاعات یا آسیب رساندن به رایانه­ها و سیستم است. این در حالی است که در برخی سیستم های حقوقی، اموال غیرعینی و غیرملموس قابل سرقت نبوده و آسیب وارده باید حتماً دیده شود. مشکل دیگر موجود در این عرصه، ارایه نشدن تعریف­های لازم درباره جوانب مختلف این تکنولوژی و جرایم محتمل در درون آن است.

نقض قوانین کپی رایت (حق مؤلف) را نیز می توان یکی دیگر از جرایم شایعی دانست که امروزه از طریق رایانه و شبکه جهانی اینترنت به شدت در حال انجام است. یک مورد از موارد ثبت شده حمله به برنامه «یاهو مسنجر» در ساعت ۱۰:۳۰ دقیقه هفتم فوریه ۲۰۰۰ بود که سه ساعت طول کشید و در این زمان، «پینگ» یاهو به یک گیگابایت درثانیه کاهش یافت.

کلاه برداری و ایجاد اختلال در سیستم­های مالی و بانکی برای انتقال وجوه و پول به حساب مجرم یکی از جرایم مهمی است که تا کنون خسارات زیادی را در کشورهای مختلف جهان به همراه داشته است. انتشار ویروس «ملیسا» در سال ۱۹۹۹ یک نمونه مشهود دیگر است. این ویروس در مارس ۹۹ برای نخستین بار در اینترنت ظاهر شده و با سرعت زیادی در سیستم­های کامپیوتری آمریکا و اروپا منتشر شد. برآورد شده که انتشار این ویروس در سراسر جهان، خسارتی هشتاد میلیونی از خود بر جای گذاشت. این ویروس تنها در آمریکا ۲ / ۱ میلیون کامپیوتر متعلق به یک پنجم بزرگ ترین تجارت­های این کشور را آلوده کرد.

«دیوید اسمیت»، طراح این ویروس، در نهم دسامبر ۱۹۹۹ به علت طراحی و انتشار این ویروس به ارتکاب جرایم ایالتی و فدرال متهم شد. تروریسم رایانه­ای، آخرین موج جرایم به وجود آمده در این عرصه است که نگرانی­های گوناگونی را در میان کشورها پدید آورده است. استفاده تروریست ها از شبکه به صورت های گوناگون برای تبادل اطلاعات به صورت رمزی و کد شده و حتی در قالب پورنوگرافی کودکان و استخدام نیرو از این راه، معضلی است که در آینده ای نه چندان دور، می تواند به مهم ترین چالش بین المللی برای کشورها تبدیل شود.

در عین حال، معاملات مواد مخدر از طریق اینترنت و سرویس­های پست الکترونیکی نیز زمینه دیگری است که باندهای قاچاق مواد مخدر به راحتی از آن برای انجام معاملات و ردیابی محموله های غیرقانونی قرص ها و تبلیغ محصولات خود از آن استفاده می­کنند.

پلیس فدرال آمریکا هم اکنون دارای یک شاخه جرایم اینترنتی و رایانه­ای بوده که چهار زمینه عمده را به عنوان هدف خود بیان کرده است که در درجه نخست، مبارزه با جرایم جدی رایانه­ای و گسترش آن است.

1) شناسایی و دستگیری مجرمان جنسی که از اینترنت برای توزیع و تولید پورنوگرافی کودکان استفاده می­کنند.

2) مبارزه با فعالیت­های مجرمانه­ای که مالکیت معنوی کشور آمریکا را هدف قرار می­دهد.

3) امنیت ملی و بازار رقابت را به خطر می­اندازد.

4) سرکوب شبکه­های مجرمانه بین المللی سازمان یافته که در فعالیت­های جعل و سرقت هویت اینترنتی فعالیت دارند.

از جرایم شایع دیگر در محیط اینترنت می­توان به پورنوگرافی اینترنتی کودکان اشاره کرد که در همه جهان جرم به شمار رفته و مرتکبین آن به شدت از سوی کشورها و پلیس بین الملل تحت تعقیب قرار می­گیرند. اینترپل چند ماه پیش موفق شد با بازسازی چهره فیلتر شده یک مجرم جنسی کودک آزار با استفاده از   
روش­های پیچیده کامپیوتری و پیگیری­های دقیق وی را شناسایی کرده و سرانجام با همکاری پلیس تایلند موفق به دستگیری این مجرم فراری شود که عکس اعمال مجرمانه خود را در شبکه اینترنت منتشر کرده بود.

سازمان­های بین المللی گوناگون دیگری نیز در این زمینه جرایم الکترونیکی فعالیت دارند که مهم­ترین آن­ها عبارتند از: شورای اروپایی، سازمان ملل متحد، اتحادیه اروپا، سازمان کشورهای آمریکایی، گروه ۸، سازمان همکاری­های اقتصادی آسیای­شرقی، اتحادیه­کشورهای جنوب شرق آسیا، سازمان همکاری ها و توسعه اقتصادی، ناتو، اتحادیه آفریقا، اتحادیه عرب و سازمان همکاری­های شانگ­های، اما شاید بهترین مرجع بین المللی در این زمینه برای الگو گرفتن دیگر کشورها و ایجاد روندی مشابه، کنوانسیون جرایم رایانه­ای و­ اینترنتی، شورای اروپایی باشد که شمار بسیاری از کشورهای اروپایی به آن پیوسته و عضویت برای کشورهای غیر عضو این شورا نیز آزاد است. هدف اصلی این معاهده که همه کشورها امکان پیوستن به آن را دارند همان گونه که در مقدمه آن نیز ذکر شده، ایجاد سیاست کیفری واحد با هدف حمایت از جامعه در برابر جرایم رایانه­ای و اینترنتی با در پیش گرفتن قانون­گذاری­ها و تقویت­همکاری بین­المللی­است. این کنوانسیون نتیجه چهارسال فعالیت کارشناسان شورای اروپایی و کشورهای دیگر بوده و دارای یک پروتکل الحاقی با موضوع تبلیغات نژادپرستانه و تبلیغ تنفر از طریق شبکه­های کامپیوتری مصوب مارس ۲۰۰۶ بوده و هم اکنون نیز بحث تروریسم رایانه­ای و اینترنتی در دستور کار این کنوانسیون قرار دارد .

[[4]](#footnote-4)

**فصل­چهارم**

**محتوای­ جرایم ­رایانه­ای**

**4-1محتوا علیه عفت واخلاق**

 اولین مورد از این گروه ‌بندی هفتگانه به محتواهای علیه عفت و اخلاق عمومی مربوط می‌شود و مواردی چون اشاعه فحشاء و منکرات، تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی، انتشار، توزیع و معامله محتوای خلاف عفت عمومی (مبتذل و مستهجن)، تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل و استفاده ابزاری از افراد در تصاویر و محتوا و تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیرقانونی به عنوان مصادیقی از جرایم رایانه‌ای معرفی شده‌اند و تمامی افرادی که نسبت به انتشار چنین مواردی اقدام کرده باشند طبق قوانین مورد مجازات قرار خواهد گرفت.

**4-2محتوا علیه مقدسات اسلام**

 در گروه دوم جرایم رایانه‌ای که به محتوا علیه مقدسات اسلامی مربوط می‌شود، ارائه محتوایی که مخالف موازین اسلامی، اهانت به دین اسلام و مقدسات آن، اهانت به هر یک از انبیاء یا ائمه طاهرین (ع)، تبلیغ به نفع حزب گروه یا فرقه منحرف و مخالف اسلام، نقل مطالب از نشریات و رسانه‌ها و احزاب و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آن‌ها باشد.

**4-3محتوا علیه امنیت وآسایش عمومی**

  اما دسته سوم جرایم رایانه‌ای به محتواهای علیه امنیت و آسایش عمومی برمی­گردد و مواردی چون تشکیل جمعیت، دسته، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور، هرگونه تهدید به بمب گذاری، انتشار محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند، انتشار محتوا علیه اصول قانون اسلامی، تبلیغ علیه نظام جمهوری اسلامی ایران، اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی، تحریک یا اغوای مردم به جنگ و کشتار یکدیگر، تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحا در خدمت نیروهای مسلح هستند به عصیان، فرار، تسلم یا عدم اجرای وظایف نظامی، تحریص و تشویق افراد و گروه­ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور، تبلیع به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران، فاش کردن و انتشار غیرمجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی یا اسرار نیروهای مسلح، فاش کردن و انتشار غیرمجاز نقشه و استحکامات نظامی،انتشار غیرمجاز مذاکرات غیرعلنی مجلس شورای اسلامی، انتشار بدون مجوز مذاکرات محاکم غیرعلنی دادگستری و تحقیقات مراجع قضایی و انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد را شامل می­شود.

**4-4 محتوا علیه مقامات ونهادهای دولتی**

  اما در گروه چهارم که به محتوا علیه مقامات و نهادهای دولتی و عمومی برمی گردد: اهانت و هجو نسبت به مقامات، نهادها و سازمانهای حکومتی و عمومی، افترا به مقامات، نهادها و سازمانهای حکومتی و عمومی، نشر اکاذیب و تشویش اذهان عمومی علیه مقامات، نهادها و سازمانهای حکومتی، جعل پایگاه‌های اینترنتی بانک ها، سازمان­ها و نهادهای دولتی و عمومی جرم محسوب می‌شود.

**4-5 محتوا برای ارتکاب جرایم رایانه‌ای**

به گزارش ایسنا، در گروه پنجم که به محتواهایی که برای ارتکاب جرایم رایانه‌ای به کار می‌روند مربوط می‌شود، و مواردی از قبیل انتشار یا توزیع و یا در دسترس قرار دادن، معامله داده‌ها یا نرم افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می­رود، فروش انتشار یا در دسترس قرار دادن غیرمجاز گذرواژه­ها و داده­هایی که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می­کند، انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز، افترا به مقامات، نهادها و سازمان­های حکومتی، شنود غیرمجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم­های رایانه‌ای و مخابراتی، آموزش و تسهیل سایر جرایم رایانه‌ای، انتشار فیلترشکن­ها و آموزش روشهای عبور از سامانه‌های فیلترینگ، انجام هرگونه فعالیت تجاری و اقتصادی رایانه‌ای مجرمانه مانند شرکتهای هرمی، ایجاد مراکز قمار در فضای مجازی جزو جرایم رایانه‌ای تعریف می­شوند.

**4-6 امور سمعی و بصری و مالکیت معنوی**

  بخشی دیگر از محتواهای مجرمانه فضای مجازی دسترسی به امور سمعی و بصری و مالکیت معنوی مربوط می­شود و بر همین اساس انتشار و سرویس دهی بازی­های رایانه‌­ای دارای محتوای مجرمانه، معرفی آثار سمعی و بصری غیرمجاز به جای آثار مجاز، عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ­ارشاد  
 ­اسلامی و تشویق و ترغیب به نقض حقوق مالکیت معنوی برخی از این موارد جرم محسوب می‌شوند.

**4- 7محتوای دعوت کننده به جرم**

  اما در گروه دیگر محتواهایی که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کنند از جمله انتشار محتوای حاوی تحریک، ترغیب، یا دعوت به اعمال خشونت آمیز و خودکشی، تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار، باز انتشار و ارتباط به محتوای مجرمانه تارنماها و نشانی‌های اینترنتی مسدود شده، نشریات توقیف شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیر قانونی، تشویق تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم،‌ تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره، تبلیغ و ترویج اسراف و تبذیر، فروش، تبلیغ، توزیع و آموزش استفاده از تجهیزات دریافت از ماهواره جزو نمونه‌های این دسته از جرایم رایانه‌­ای به شمار  
 می­روند.

**4-8 جرایم رایانه­ای از زبان نوتورن**

سالانه گزارش­های زیادی درباره آمار و ارقام جرایم رایانه­ای و قربانیان آنها می شنویم. یکی از این   
گزارش­ها در مورد ارقام و آمار جرایم رایانه­ای از شرکت امنیتی نورتون منتشر می­شود. بر اساس این گزارش 431 میلیون نفر در سال قربانی جرایم رایانه­اي می­شوند. از طرفی این جرایم حدود 400 میلیون دلار هزینه در بر داشته است. حال این جرایم از خالی کردن حساب دیگران تا دزدی اطلاعات مردم نام برده می­شود.

**4-9درصدهای مبتلایان به جرائم رایانه­ای**

96% از افراد آنلاین در طول عمر خود قربانی جرایم رایانه­ای شده است.

از هر 14 نفر دو نفر قربانی جرایم رایانه­ای می­شوند که در نتیجه هر روز بیش از 1 میلیون نفر طعمه این جرایم می­شوند.

10%افراد آنلاین جرایم رایانه­ای را در تلفن های همراه خود نیز داشته اند.

آسیب پذیری های تلفن همراه نسبت به سال 2009، 42% بیشتر بوده است.

این گزارش همچنین بیان کرده است که علاوه بر افزایش تهدیدات نسبت به کاربران تلفن همراه، شبکه های اجتماعی نیز در معرض خطر این جرایم قرار دارند. بر اساس گزارشات نورتون، ۸۰% از مردان سنین ۱۸ تا ۳۱ سال که از طریق تلفن همراه خود به اینترنت متصل می شوند قربانی جرایم رایانه­ای شده­اند. شایع ترین جرایم رایانه­ای، ویروس ها و نرم افزارهای مخرب هستند که حدود 54% از کاربران اینترنت را طعمه خود قرار داده­اند. کلاهبرداری آنلاین نیز 11% از کاربران را قربانی کرده است. پس این قربانیان جرایم رایانه­ای برای محافظت از خود چکاری می­توانند انجام دهند؟ پاسخ های بسیاری وجود دارد. 41% از افراد می­گویند. که نرم افزارهای امنیتی آنها منسوخ شده است در حالیکه فقط 47% هر روز میزان اعتبار کارت­های اعتباری خود را بررسی می­کنند و61% همچنان رمزهای عبور مناسب را نادیده گرفته و هرگز از رمزهای پیچیده و غیرقابل تشخیص است و گاهی رمزهای عبور خود را تغییر نمی­دهند.

**4-10حمله بدافزاری به رایانه‌های شرکت‌های تجاری هر ۳ دقیقه یک‌ بار**

شرکت های تجاری مختلف هر سه دقیقه یک بار مورد حملات بدافزاری قرار می­گیرند؛ امری که نشان می­دهد خطرات سایبری تا چه حد گسترش یافته است. از جمله حملات متداولی که هر سه دقیقه یک بار صورت می­گیرد می توان به ارسال ایمیل­های آلوده اشاره کرد که حاوی لینک­های مشکوک هستند و کاربران با کلیک کردن بر روی آنها به سمت سایت­های آلوده هدایت می­شوند.

فصل پنجم

آثارمخرب جرایم رایانه­ای

|  |
| --- |
| **5-1آثار مخرب جرایم رایانه­ای**   * الف. آثار و آسیب­های روانی * **اعتیاد مجازی** * اعتیاد مجازی، استفاده بیش از حد از اینترنت است تا آنجا که بدون استفاده از آن فرد احساس کمبود می­کند و روابط او با محیط متأثر از استفاده مکرر و دیوانه وار فرد شده از حالت عادی خارج می­شود.این اختلال روانی در کشورهایی که استفاه از اینترنت آسان و ارزان است، بسیار چالش زا بوده و تا آنجا که نهادهای مختلف را درگیر کرده است. در کشوری، مثل آمریکا تعداد معتادان به اینترنت از سایر معتادان بیشتر است، تا جایی که برخی معتادان 18 ساعت از وقت روزانه خود را در اینترنت صرف می­کنند. در آمریکا به قدری فاجعه بار است که کلیساها، پیشوایان مذهبی با فریادهای کمک خواهی زن و شوهر، یا یکی از آنها، برای رهایی از این نوع اعتیاد مواجه هستند و مؤسسه های مشاوره ای مسیحی در حال تدوین مشاوره­های اعتیاد به اینترنت می­باشند. پیامدهای اعتیاد به اینترنت و حتی کار زیاد با اینترنت، که در حدّ اعتیاد نباشد، نتایج و پیامدهای زیان بخشی برای فرد و جامعه در پی داشته و آسیب­های شدید جسمانی، مالی، خانوادگی، اجتماعی و روانی را به همراه دارد.   یکی از پیامدهای فردی و اجتماعی اعتیاد و کار زیاد با اینترنت، انزوا و کناره­گیری اجتماعی است.  پوت نام (1991م) معتقد است در طی 35 سال گذشته کاهش چشم گیری در ارتباطات اجتماعی افراد در آمریکا رخ داده است. مردم کمتر به رأی گیری و کلیسا می روند، به ندرت موضوعات سیاسی را با همسایه­ها در میان گذاشته یا عضویت گروه­های داوطلبانه را قبول می­کنند، مهمانی شام کمتری دارند و کمتر به منظور اجتماعی دور هم جمع می­شوند. این موضوع پیامدهای عمده­ای برای جامعه و فرد دارد، زیرا وقتی مردم از نظر اجتماعی درگیر باشند، سالم­تر و خوشبخت تر زندگی می­کنند.  از دیگر پیامدهای اعتیاد اینترنتی مشکلات خانوادگی و تأثیر آن بر روابط زناشویی، والدین و فرزندان است. امروزه اصطلاح «بیوه اینترنتی» برای همسر معتاد به اینترنت اطلاق می­شود. آمار نشان می­دهد که اعتیاد به اینترنت ممکن است به فروپاشی خانواده و طلاق منجر شود. شاید باور کردن اینکه شخصی همسر خود را فقط به علت ارتباط با فرد دیگر در اینترنت ترک می­کند، برای کسانی که به اینترنت اعتیاد پیدا نکرده­اند، وحشتناک به نظر برسد؛ ولی این مسئله هر روز در دنیای اینترنت اتفاق می­افتد.  دکتر یانگ معتقد است: اگرچه زمان تنها عامل تعیین کننده در تعریف اعتیاد به اینترنت نیست، ولی عموماً معتادان بین 40 تا 80 درصد از وقت خود را با جلساتی که ممکن است هر کدام حتی تا 20 ساعت طول بکشد، صرف می­کنند و این کار باعث می­شود تا اختلالاتی در میزان و زمان خواب کاربر به وجود آید. در موارد شدید، حتی  قرص­های کافئین برای تسهیل زمان طولانی­تری در اینترنت بودن مصرف می­شود.  این اختلال، خستگی بیش از اندازه ای در بدن ایجاد می­کند، که کارکرد درسی و شغلی را تحت تأثیر قرار می­دهد و ممکن است نظام ایمنی بدن را ضعف کند و فرد، آسیب پذیری بیشتری به بیماری­ها پیدا کند. افزون بر این، به علّت عدم ورزش و حرکات مناسب، مشکلات عصب­های مچ و درد پشت، چشم درد و مانند آن به وجود می­آید.  5**-2 بحران هویت**   * هویت، واجد و دارای سه عنصر است: شخصی، فرهنگی و اجتماعی، که هریک در تکوین شخصیت فرد نقش مهمی را ایفا می­کند. در مقایسه­ها، هویت شخصی، ویژگی بی همتای فرد را تشکیل می­دهد و هویت اجتماعی در پیوند با گروه ها و اجتماعات مختلف قرار می­گیرد. * اینترنت صحنه فرهنگی و اجتماعی است، که فرد خود را در موقعیت های متنوع نقش ها و سبک های زندگی قرار می­دهد و این خود زمینه­ای برای آسیب پذیری شخصیت کاربر و موجب چند شخصیتی شدن کاربر می­شود.   از این روست که ساختار و چینش پایگاه های شخصی (WebLoge) به گفته میلر (Miler) نشان از شخصیت آن کاربر است. جوانان در این محیط از آسیب پذیری بیشتری برخوردارند، به ویژه در دورانی که هویت ایشان شکل می­گیرد، این خطر پررنگ تر می شود. دکتر محمد عطاران معتقد است: با امکانات و گزینه­های فراوانی که رسانه های عمومی، از جمله اینترنت در اختیار جوانان می­گذارند، آنان دائماً با محرک­های جدید و انواع مختلف رفتار آشنا می­شوند. چنین فضایی هویت نامشخص و پیوسته متحولی را می­آفریند، خصوصاً برای نسلی که در مقایسه با نسل قبل با  محرک­های فراوانی مواجه است. همچنین از طریق رسانه­های جمعی، افراد، خطّ مفروضی میان فضای عمومی و خصوصی را تجدید سازمان می­کنند و این امکانی است که جوانان فعالانه از آن استفاده می­کنند. جوان، به خصوص در دوران بلوغ که مرحله شکل گیری هویت اوست و همواره به دنبال کشف ارزش­ها و درونی کردن آنها می­باشد، با اینترنت و حجم گسترده، حیرت انگیز و گوناگون اطلاعات مواجه می­شود و ناچار که در این دنیای مجازی، هویت خویش را از طریق جستجو پیدا کند و بدین سان، ممکن است برخی و شاید تعداد زیادی از نوجوانان راه را در اینترنت گم کنند و دوران هویت یابی خویش را بیش از پیش با بحران سپری کنند. از سوی دیگر، گاهی برخی از ویژگی­های شخصیتی، مانند سن، تحصیلات، محل سکونت و حتی جنسیت در اینترنت از بین می­رود، به عنوان نمونه، بسیاری از افرادی که در اتاق­های چت مشغول گفتگو با یکدیگر می­باشند. با مشخصیاتی غیرواقعی ظاهر شده و از زبان شخصیتی دروغین که از خود ساخته­اند و آن را به مخاطب یا مخاطبان خود معرفی کرده­اند، صحبت می­کنند و با این حال، چه تأثیراتی که همین شخصیتهای ناشناس بر یکدیگر دارند. از جمله نتایج بحران هویت نیز کم رنگ شدن علایق کاربران به وطن خویش است، که نتایج خطرناکی چون خیانت به کشور و خودکم بینی و وابستگی فرهنگی و شخصیتی به کشورهای بیگانه خواهد بود. یکی از ریشه­های وقوع جرایم امنیتی، وجود بحران هویت است که در جرایم جاسوسی و خیانت به کشور بیشتر رخ می­نماید.  **5-3­­ انحرافات جنسی**   * از جمله آثار مخرّب جرایم رایانه­ای، به ویژه جرایم مرتبط با محتوا (به قول قانون مجازات جرایم رایانه­ای) به وجود آمدن انحرافات جنسی و اختلالات جنسی است. اینترنت به دلیل رویکرد آزاد اندیشی در روابط جنسی از سوی گردانندگان اصلی آن (یعنی غرب و به ویژه آمریکا) و نگرش تجاری نسبت به مسائل جنسی موجب پدید آمدن پدیده کثیفی به نام هرزه نگاری و هنر پلید شهوانی و رواج سرسام آور آن گردید، که مرزهای اخلاقی را درهم می­شکند و تهدیدی برای فرهنگ­ها، به ویژه فرهنگ­های دینی، چون فرهنگ اسلامی است.   اصولاً، پورنوگرافی به عنوان نمایش تصویری و یا کلامی، رفتارهای جنسی است که با هدف ارضای خواسته های جنسی دیگران تعریف می­شود. این گونه مطالب و تصاویر که در پی تحریک جنسی دیگران عرضه  می­گردد، معمولاً به ارضای غیرطبیعی جنسی مراجعه کنندگان آن می انجامد.  نکته دیگر اینکه رجوع به اینترنت برای دسترسی به مطالب مستهجن[[5]](#footnote-5)، صرفاً به افراد نابهنجار خلاصه نمی­شود و حجم قابل توجهی از مراجعان را افراد طبیعی تشکیل می­دهند. اصولاً اینترنت به جوی دامن زده که در سایه ویژگی های خاص خود به تدریج به شکل گیری ناهنجاری­های جنسی در کاربران خود می­انجامد و منشأ به وجود آمدن بسیاری از جرایم رایانه­ای (به ویژه محتوایی) و مقمه­ای برای جرایم جنسی می­گردد.  **5-4 دلایل رجوع مردم**  **دلال رجوع و اقبال مردم به این گونه مطالب را در عرصه اینترنت می توان در این موارد خلاصه نمود:**  **الف. گمنامی:**   * ناشناخته ماندن مراجعان در عرصه اینترنت، به نوعی اعتماد به نفس در افراد را دامن می زند و این حالت، نوعی رفتار غیرمسئولانه را در فرد شکل می­دهد. مراجعان درچنین شرایطی است که به خود اجازه  می­دهند تا برخلاف رفتارهای طبیعی به راحتی از دسترس زوج اینترنتی خود دور شوند و یا بلافاصله به فرد دیگری روی آورند. اصولاً در چنین فضایی است که فرد می­تواند در معرفی خود هرگونه که می­خواهد عمل کند و همین ویژگی، خود محرکی است تا کاربران اینترنتی به استفاده از هویت جعلی روی آورند و این را می­توان از جمله ویژگی­های فرهنگ فضای مجازی برشمرد، که این خود زمینه­ای برای ارتکاب جرایم فضای سایبر نیز هست.   **ب. سهولت:**   * مطالب شهوانی و تصاویر سکسی به آسانی در دسترس همگان قرار دارند. عرضه گسترده این مطالب و وجود تعداد بی­شمار اتاق­های گفت­وگوی سکسی، هر کاربری را به داشتن اولین تجربه در این حوزه تحریک می­کند. یک زن یا شوهر کنجکاو به راحتی و دور از دیدگان همسرش وارد این فضاها می­شود و گفت وگوهای سکسی با دیگران را تجربه می­کند چنین سهولتی است که بسیاری را به تجربه رفتارهای ناهنجاری جنسی نه در فضای فیزیکی، بلکه در فضای مجازی هدایت می­کند. به ویژه اگر نظارت نهادهای مسئول در کشورها در این زمینه کم رنگ و ناتوان باشند.   **ب. آثار اجتماعی و فرهنگی**  **1- تزلزل در ارکان خانواده**  یکی از آثار جرایم مربوط به محتوا، همچون هرزه نگاری و ترویج مطالب مستهجن، تزلزل در روابط زناشویی است؛ چرا که از آثار هرزه نگاری اعتیاد جنسی است، که در جوامعی که اینترنت ارزان در اختیار افراد قرار دارد، شیوع بسیاری دارد. در این موارد زنان از همسران خود شکایت دارند که به ایشان بی توجهی کرده و بیش از آنکه از بودن در کانون خانواده و در کنار همسر لذت ببرند از صرف وقت در اینتنت و فضای مجازی و لذت­های منحرف جنسی و غیر آن لذت می­برند. بخشی از عوامل طلاق در این قبیل کشورها اعتیاد به اینترنت، به ویژه اعتیاد جنسی مجازی است. کسانی که به خاطر سودی کثیف رو به ترویج تجارت جنسی مجازی آورده­اند و نهادهایی که بی تفاوت یا کم تفاوت از کنار این قبیل مسائل می­گذرند، خواسته یا ناخواسته یکی از مهم­ترین گروه­های اجتماعی؛ یعنی خانواده را رو به انحیاط و نابودی و یا حداقل ضعف می­کشانند. دیگر، زن و شوهر از کنار یکدیگر بودن کمتر لذت می­برند و بیشتر وقت خود را صرف لذت­های رنگارنگ، اما پلید در فضای مجازی می­کنند. در نتیجه محبت به عنوان رکن اصلی و اساسی خانواده روبه سستی می­رود. فرزندانی که در این محیط بار می­آیند، دچار انحراف اخلاقی شده و سلات روانی و روابط جنسی پاک از بین می­رود. از این روست که نتیجه اباحه گری جنسی به افزایش پدیده­هایی، مثل فرزندان تک والدینی، زنان و مردانی که تنها زندگی می­کنند، بچه های نامشروع وغیره خواهد انجامید. بنابراین لزوم نظارت سخت گیرانه و دقیق در فضای مجازی از سوی نهادهای مسئول و والدین رخ می­نماید. وظیفه نهادهای فرهنگی نیز در فرهنگ سازی در جهت بهره ­برداری صحیح از اینترنت بسیار مهم و تأثیرگذار است.  **5-5 کاهش امنیت و احساس آرامش، به ویژه در کاربران اینترنتی**  یکی از آثار جرایمی؛ از قبیل دسترسی غیرمجاز، شنود و دریافت غیرمجاز، جعل داده ها، تخریب و ایجاد اختلال در داده­ها، اختلال در سیستم، ممانعت از دستیابی، سرقت داده ها؛ کاهش امنیت شهروندان جامعه و به خطر افتادن حریم خصوصی ایشان است. شاید بعضی وقت­ها در مجاورات خصوصی، چیزی را بگوییم که امید داشته باشیم که خوانندگان آن را به فراموشی بسپارند یا چیزی را بنویسیم که بعدها از آن پشیمان گشته و امیدوار باشیم که خوانندگان برگه­های ما را در لابه لای دیگر برگه­های متعدّد و متفرق بایگانی خویش گم کنند و دیگر به خواندن آنها مبادرت نورزند؛ ولی فناوری اطلاعات به همه این امکان را می­دهد، که همه اطلاعات حال و گذشته را به  گونه­ای سامان مند بایگانی و ذخیره نموده و هر وقت که آن را لازم داشتند، فورا بیابند. از این جهت، اگر  حریم­خصوصی شما در زمان و مکانی خاص افشا گردد. امید نداشته باشید که کاربران رایانه­ها آن را فراموش کنند، چرا که فناوری اطلاعات این امکان را سلب کرده است. اینکه شما چه چیزهایی خریده­اید و از کجا آنها را تهیه کرده­اید، پولش را از کجا آورده­اید و چقدر به چه کسی اهدا کرده­اید و از چه کسی چه انتظاراتی دارید و با چه کسانی نامه پراکنی می­کنید، همه و همه در دنیای رایانه­ای، درون بلندگوهایی پخش می­شود، که اوّلاً: امکان شنیدن آن برای همگان وجود دارد و ثانیاً: هرگز آوای مکرر و باقی آنها خاموش نمی­شود و همواره با هرعملیات الکترونیکی شما، بر حجم آنها اضافه می­شود.  امروزه حریم خصوصی اشخاص در معرض خطراتی است، که قبل از فناوری اطلاعات هرگز وجود نداشت، همان طور که قبل از پیدایش فناوری الکتریسیته هیچ کس درمعرض خطر برق گرفتی نبود، حال باید مواظب بود که توسعه فناوری، حریم خصوصی افراد را به آتش نکشد. اینکه چه کسانی در قبال این خطرات پیش آمده مسئولیت دارند؟ و یا با چه تدابیری باید این احساس عدم امنیت را کاهش داد؟ سؤال­هایی است که در این باره مطرح است. البته مقابله با جرایم رایانه­ای و حفاظت دقیق از داده­ها، هم از طریق دولت و هم از طریق سازمان های خدمت رسان و هم از طریق خود افراد، در کاهش این ناامنی بسیار مؤثر خواهد بود. در این مسر کارشناسان واگذاری IP و استفاده از پروکسی[[6]](#footnote-6)، نصب دیوار آتشین، نصب ضد ویروس و ضد جاسوس اینترنت و کار فرهنگی را توصیه می­کنند.  **5-6 کاهش علایق و ارزش های ملی نزد کاربر**  یکی از ویژگی­های اینترنت، جهانی بودن آن است، که با وجود فوایدی که دارد، اثرات مخربی نیز بر فرهنگ­های ملی جوامع می­گذارد؛ چرا که کاربران با استفاده از اینترنت ضمن این که با زبان انگلیسی حاکم بر آن درگیر هستند، از زبان ملی خود دور می­شوند، به عنوان مثال در چت های اینترنتی، فارسی زبانان بیشتر از الفبای انگلیسی به جای الفبای فارسی استفاده می­کنند (که یکی از دلایل آن کمبود نرم افزارهای قدرتمند فارسی است). گسترش این کاربرد خود موجب تضعیف الفبای فارسی خواهد شد.  **5-7تغییر هنجارهای فرهنگی**  با توجه به تفاوت هنجارها از جامعه­ای نسبت به جامعه دیگر، امکانات الکترونیکی از جمله فضای مجازی تبادل و تأثر فرهنگی را رونق می­دهد. در این بین فرهنگ­های ضعیف یا صاحبان فرهنگ­های قدرتمند، اما کم تلاش متأثر از فرهنگ مهاجم قرار خواهند گرفت. فرهنگ اسلامی نیز در این تبادل گرچه فرهنگی با پشتوانه است، اما در صورتی که مسلمین در شناخت و شناساندن آن نکوشند در برابر فرهنگ مهاجم غرب دچار التقاط و تغییر خواهند شد.  **5-8 ناامنی مالی و سرمایه گذاری**  یکی از اساسی­ترین باورهای مورد قبول اغلب جوامع، مالکیت بر اموال است. در فضای مجازی، با مطرح شدن مال الکترونیکی، که به شکل پول الکترونیکی، داده­ها و اسناد با ارزش و غیره است، لزوم حفظ امنیت مالی و مراقبت از آن برعهده حکومت خواهد بود. از این رو یکی از آثار کلاهبرداری و سرقت الکترونیکی، ناامنی سرمایه گذاری درحوزه اموال الکترونیکی است.  **5-9کم رنگ شدن ارزش های مترقی**  هرجامعه، صاحب ارزش­هایی است که ناشی از فرهنگ آن است، اما برخی ارزش­های مترقی در جوامع اسلامی است، که در اثر تأثیر از فرهنگ بی بندبار غرب در حال کم رنگ شدن است. ارزش­هایی مثل حیا و عفت زن، اهمیت داشتن شخصیت انسان نه جنسیت آن، قبح عریان نمایی بدن به ویژه شرمگاه وغیره که در نتیجه رواج استفاده از مطالب مستهجن و ملاک شدن بولالهوسی در روابط انسانی در حال کم رنگ شدن است. دین چابنر در مقاله­ای، چنین پیامدهایی را ناشی از رواج اباحه گری جنسی و هرزه نگاری دانسته و می­گوید: «مطالعات دقیق و گسترده­ای در طول این سال ها در این باره صورت نگرفته است، در نتیجه رواج بوالهوسی است که بلوتوث و ارسال تصاویر مستهجن در میان جوامع اسلامی رشد می­یابد، روابط آزاد دختر و پسر ترویج می­شود، کم پوشی و عریان پوشی در میهمانی­ها و عروسی ها، به ویژه در میان جوانان گسترش می­یابد.  ج. آثار سیاسی**(تزلزل در حاکمیت و اقتدار سیاسی)**  بارزترین ویژگی اینترنت، انباشت اطلاعات متنوع در آن است و این ویژگی آن را به بزرگ­ترین انبار اطلاعاتی جهان تبدیل کرده است، به نحوی که خوب و بد، حقّ و باطل به شیوه­های رنگارنگ به ارائه خواسته­ها و دانسته­های خود می­پردازند.  از این رو این کاربران هستند که در برابر حجم وسیعی از اطلاعات سردرگم می­مانند و باید انتخاب کنند. برخی بر این عقیده­اند که این آزادی اطلاعات گامی است در طریق دموکراسی؛ چرا که کاربران دسترسی به همه نوع اطلاعات دارند و لذا می­توانند از میان آنها، آنچه به نظرشان درست تر می­نماید، برگزینند و دنباله بهترین اندیشه در زمینه­های مختلف سیاسی، فرهنگی و غیره است. اما آیا کاربران در انتخاب اطلاعات آزادی کامل دارند؟ آیا اطلاعات همانگونه که هست در اختیار کاربران قرار می­گیرد، اینها سؤالاتی است که تأمّل در آن، نظر طرفداران آزادی اطلاعات را متزلزل می­کند. به عنوان نمونه وقتی یک کاربر بخواهد از طریق جستجوگرهای قدرتمندی، چون گوگل و یاهو به دنبال موضوعی، مثلاً درباره ایران (کلمه Iranرا تایپ کند) بگردد، آیا این موتورهای جستجو صادقانه مهم ترین و دقیق ترین اطلاعات را در این باره ارائه می­دهند؟ اما حقیقت جز این است، چرا که مطالعات نشان می­دهد، فضای حاکم بر اینترنت و ساختار تشکیل دهنده آن، همه براساس اهداف و سیاست­های گرداننده اصلی اینترنت؛ یعنی آمریکا و از طریق شرکت­های محوری، طرح ریزی شده است.  به عنوان نمونه می­توان به دو مورد اشاره کرد:  1. وب سایت مشهور گوگل و بسیاری از موتورهای جستجوی مشهور اینترنت. براساس برخی از سیاست های سانسوری که در فوق به آن اشاره شد، اقدام به ارائه اطلاعاتی از پیش تعیین شده براساس کلید واژه­های کاربر می­کنند، که معمولاً شمار زیادی از کاربران، این نتایج را که در ردیف­های اول تا 50 نتایج جستجو قرار دارد، مورد استفاده نهایی خود قرار داده و استنباط های نهایی و برداشت های کلّی خود را براساس این موارد، کسب و معرفی می­کنند. به عنوان مثال کلید واژه هایی، مانند ایران، عراق، کره، هنگامی که در باکس جستجو تایپ شده و جستجو می­شود، در بالاترین فهرست نتایج جستجو، صفحات وبی نشان داده می­شود که به نوعی تعلّق مستقیم و یا غیرمستقیم آشکار به بخش های اطلاعاتی و امنیتی آمریکا دارد. مثلاً در مورد عراق، عراقی که از نگاه اسناد سازمان جاسوسی آمریکا و بخش­های اطلاع رسانی دیگر داخل و خارج از آمریکا مورد بررسی و مطالعه قرار گرفته است، به کاربران جستجوگر کلید واژه عراق، معرفی می­شود.  سرچشمه اصلی این امر تلاش گسترده آمریکائیان مبنی بر تسلّط بلامنازع بر شاهراه جهانی اطلاع­رسانی و ارائه تصویری از جهان براساس نگاه آمریکا و سیاست جهانی آن به هر شهرند دهکده جهانی است، که از طریق مکانی به نام اینترنت، جهان را زیرکاوش خود قرار می­دهند.  2. از دیگر مواردی که می­توان از آن به عنوان نوعی از دیپلماسی انحصارطلبی آمریکا در اینترنت به شمار آورد و آن را زمینه ساز بستر شعار: «جهان یا اینترنت را از نگاه آمریکا بنگرید»، دانست، ایجاد پایگاه­های خبری متعدد در اینترنت توسط سازمان­هایی است که توسط ایالات متحده مورد حمایت معنوی و مادی قرار می­گیرند تا حجم قابل توجهی از اطلاعات خبری و رسانه­ای که در اینترنت منتشر و در اختیار اکثر کاربران شبکه در اقصی نقاط جهان قرار می­گیرد، به گونه­ای مرتبط با آنچه آن را می توان دیپلماسی انحصارطلبی رسانه­ای آمریکا خواند قرارگیرد. به عنوان مثال، شبکه اینترنتی ورلدنیوز، که دارای بیش از پانصد سایت اینترنتی خبری و اطلاعاتی به بیش از 10 زبان زنده دنیا می­باشد و همواره اخبار منتشر شده توسط سایت­های خبری مختلف این شبکه عظیم خبری در فهرست های بالایی نتایج جستجو قرار می­گیرد، با روزآوری مرتب و مکرر خود و انتشار حجم قابل ملاحظه­ای از اخبار و اطلاعات متنوع در اینترنت، تفسیر خبری و اطلاعاتی خاصی را به کاربران وب ارائه می­کند که در ورای آن نوعی خط دهی مبتنی بر سایبر آمریکایی قرار دارد. نوعی نسخه پیچی خودخواهانه و انحصارطلبی برای فضای اطلاعاتی شناور در اینترنت که روزانه مورد استفاده حجم عظیمی از شهروندان دهکده جهانی قرار می­گیرد. به هر حال دیپلماسی نوین واشنگتن که بر محور اطلاعات، ارتباطات و تلاش برای مونوپول کردن این روند در رسانه­ای اثرگذار و فراگیر بنام اینترنت، بنیانگذاری شده است، بیش از پیش یافتن راه­های امنیتی مطمئن با ضریب اثرگذاری بیشتر و اثرپذیری مخرب کمتر را جستجو می­کند که در نهایت، راه اندازی پلیس اینترنتی به مرکزیت آمریکا و به اختیار درآوردن رسانه وب را در سال­های آینده هدف قرار داده است.  امری که شدیداً مغایر با اصول فراگیری است، که اینترنت را شاهراهی برای تسریع ارتباطات و انتشار بهینه و غیرسانسوری اطلاعات توسط هر شخص و در هر مکان با رعایت حقوق مادی و معنوی مربوط تصور می­کند. قطعاً هرکاربری که بداند برای وی برنامه­های از پیش تعیین شده­ای در رسانه سایبر تهیه شده و حقّ انتخاب و عمل بیشتر و بهتری را ندارد و همواره پلیسی مخفی و غیرتأیید شده توسط کشورهای حاضر در اینترنت، پست الکترونیک، وبلاگ، سایت اینترنتی و عملکردهای مختلف او را زیرنظر خواهد داشت، همواره دیسکانکت بودن را بر آنلاین بودن، ترجیح خواهد داد. همچنان­که می­دانیم، اطلاعات در تصمیم گیری­های سیاسی مردم بزگ ترین نقش را دارند، لذا اطلاعات انبوه در انباری به نام اینترنت می تواند نقش پررنگی در هدایت افکار عمومی و گزینش­های سیاسی کاربران داشته باشد. در این شرایط نحوه ارائه اطلاعات در انتخابات یک کشور بسیار تاثیرگذار خواهد بود و خواهد توانست در نحوه چینش مهره­های هیئت حاکمه کشورها مؤثر باشد. از این رو اینترنت می­تواند تهدیدی علیه حاکمیّت کشورها باشد و با ارائه اطلاعات هدفمند و همسو با رسانه­های آمریکایی هرصدای مخالف دیدگاه­های آمریکا را منزوی و کم اثر کند. در نتیجه با کار هماهنگ رسانه­ای، انتخابات کشورها را به جهتی که آمریکا و همدستانش می­خواهند، سوق دهد. بدین سبب است که عمده کرده و برای مقابله با این روند تدابیری، چون فیلتر و مسدود کردن سایت­هایی که در جهت تزلزل حاکمیت ایشان اطلاعات ارائه می­کنند، اتخاذ می­نمایند.  به همین ترتیب تقریباً در تمام کشورهای عربی حاشیه خلیج فارس، کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترل­ها به علل مذهبی، سیاسی و فشارهای داخلی صورت می­گیرد. روش اصلی کنترل اطلاعات الکترونیک در این کشورها انحصار مخابرات در شرکت­های دولت است. اسرائیل نیز در میان کشورهای خاورمیانه تلاش بسیاری در جهت دستیابی به امنیت کرد، تا آنجا که با صرف هزینه کلانی به تولید Checkpoint با پیشنیه و ریشه در کاربردهای نظامی - بعنوان یکی از قابل اطمینان ترین و پرفروش­ترین فایروال­های جهان که کشورهای عربی نیز به آن متکی هستند، در جهت سیاست­های اینترنتی خود اقدام کرد. |

فصل ششم

راهکارهای پیشگیرانه

برای جرائم رایانه­ای

**6-1جرائم رایانه­ای و ­راهکارهای­پیشگیرانه**

"جرایم رایانه­ای"، جرائمی است وارداتی که با ورود کامپیوتر و استفاده از اینترنت در سطح گسترده در کشور رواج پیدا کرده است. از ورود اینترنت به کشور از سال­1370آغاز شد و در سال­1372به تکامل رسید. اما در این چند سال نبود قانونی مدون باعث گردید که  بسیاری از مجرمین رایانه­ای از زیر مجازات فرار کنند وبه جرایم خود ادامه دهند و استناد آنها نیز به اصل برائت و اصل قانونی بودن جرم و مجازات بود که استناد درستی هم بود. با تصويب قانون جرايم رايانه‌اي (1388)، مفاهيم وجرايم تازه‌اي در حقوق كيفري ايران خلق شد كه هريك نيازمند بررسي‌هاي دقيق وكارشناسانه مي‌باشد. وقتي درخصوص فناوري بحث مي‌شود، نمي‌توان رايانه را ناديده گرفت. رايانه هم خود بزرگ ترين فناوري عصر حاضر است و هم ساير فناوري‌هاي نوين يا به وسيله آن و يا بر بستر آن شكل مي‌گيرند. حقوق كيفري نوين، امروزه با جرايم و مجرمان ‌رايانه‌اي طرف است . ماهيت و ويژگي اين دسته از جرايم به نحوي اساسي با جرايم سنتي تفاوت دارد. امروزه، مجرمان ‌رايانه‌اي در مكان‌هايي به غير از نقاطي‌كه آثار و نتايج اعمال آنها ظاهر مي‌شود، قرار دارند. در صورتي‌كه كارايي قوانين جزايي موجود و متداول، منحصر به قلمرو خاصي است و به دليل آنكه اجزاي عنصر مادي كاملاً يا بعضاً تغيير يافته و برخي عناوين مجرمانه تازه هم به وجود آمده است، نمي‌توان مجرمان را با قوانين قبلي محاكمه كرد. جرایم اینترنتی و رایانه­ای نوعی جرایم جدید می­باشد. طيف گسترده افعال مجرمانه‌اي كه ذيل اين مفهوم جا دارند و ماهيت متغير آنها كه ناشي از پيشرفت لحظه به لحظه فناوري اطلاعات و شيوه‌هاي سوءاستفاده از آن است ارائه تعريف جامع و مانع و خالي از مناقشه را مشكل و چه بسا غيرممكن مي‌سازد؛ تا آنجا كه در جديدترين و جامع‌ترين سند بين‌المللي موجود در اين زمينه (کنوانسيون جرايم سايبر 2001 بوداپست) تعريفي از اين جرايم به عمل نيامده است. به نظر می­رسد کامل ترین تعریف این باشد: «هر جرمي كه قانونگذار به صراحت رايانه را به منزله موضوع يا وسيله جرم جزء ركن مادي آن اعلام كرده باشد، يا عملاً رايانه به منزله موضوع يا وسيله ارتكاب يا وسيله ذخيره يا پردازش يا انتقال دلايل جرم در آن نقش داشته باشد». این تعریف هم علاوه بر جرايم ذكر شده در دو دسته قبل، جرايمي را نيز‌كه صرفاً دلايل آنها يا اطلاعات مربوطه در رايانه ذخيره شده‌اند، به لحاظ تأمين بهتر اهداف تحقيق و تعقيب جرم با در نظر گرفتن قواعد خاص آيين دادرسي کيفري، جزء جرايم رايانه‌اي دانسته است.

**6-2 نقش اشخاص حقیقی و حقوقی در جهت نظارت و پیشگیری از وقوع جرایم رایانه­ای:**

1. نقش دادستان برای پیشگیری از وقوع جرایم رایانه­ای:

* واقع بينانه بايد در نظر داشت كه استفاده از بسياري اهرم‌هاي اعمال روش‌هاي پيشگيرانه در دسترس ما نيست ؛چرا كه اساساً اين فن‌آوري، يك فن‌آوري وارداتي است و ما در برابر جريان يك طرفه‌اي قرار گرفته‌ايم كه از خيلي جهات دست ما را براي اعمال اراده بسته است، اما در عين حال از روش كنترل و نظارتي فيلترينگ مي‌توان به عنوان يك اقدام پدافندي تا حدودي بازدارنده استفاده كرد، چنانچه بموجب مصوبه شوراي عالي انقلاب فرهنگي، شماره 59 مورخ 10دي سال 81،كميته‌اي تحت عنوان «كميته‌ تعيين مصاديق پايگاه‌هاي اطلاع‌رساني رايانه‌اي غيرمجاز» براي بررسي و احراز مصاديق فعاليت‌هاي غيرمجاز در عرصه سايبر تشكيل تا اعمال فيلترينگ با توجه به جميع جهات فرهنگي، امنيتي و غيره مورد بهره‌ برداري قرار داده شود.

2- نقش مردم در پیشگیری از وقوع جرایم رایانه­ای:

* مردم خودشان اطلاعات خود را در فضاي مجازي فاش مي‌كنند. به عبارتی اشخاصی هستند که از اینترنت اطلاع کافی ندارند و بدون اطلاع ، اقدام به چت کردن با افراد ناآشنا می­نمایند. این اشخاص اطلاعات شخصی خودشان را در معرض دسترس این افراد قرار می­دهند. به این گونه که توسط افراد متخصص هک شده و اطلاعات شخصی شان در اختیار آنها قرار می­گیرد. 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 می­شوند که از کارت آنها پول برداشت شود که می­بایست پس از اقدام به پرداخت­های 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.

3 - نصب آنتی ویروس­ها و نرم افزارهایی که وظیفه حذف یا جلوگیری از ورود کرم­های اینترنتی دارند:

* برای جلوگیری از دزدی اطلاعات، خیلی از ویروس­ها و کرم­های اینترنتی هنگامی که وارد کامپیوتر می­شوند سیستم امنیتی را از کار می­اندازند و اقدام به دادن اطلاعات شخص دریافت کننده  به شخص فرستنده ویروس می نمایند که از طریق آنتی ویروس­ها و ضدکرم­های اینترنتی که به روز شده­اند  
   می­توان از ورود آن ها و سرقت داده­ها جلوگیری کرد.

4- اقدامی که جدیداً توسط وزارت بازگانی صورت گرفته:

* به منظور کنترل و نظارت بر روی سایت­های اینترنتی که در امور بازرگانی فعال بوده و خدمات اینترنتی به کاربران ارائه می­دهند ، جلساتی میان پلیس فتا و وزارت بازرگانی برگزار شد و شرکت­های ارائه دهنده خدمات اینترنتی و فعال در امور بازرگانی تحت نظارت پلیس قرار گرفته و ساماندهی شوند.

5- ارتش سایبری ایران:

* (هک کردن سایت­هایی که برخلاف قانون جرایم رایانه­ای 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 فکرمی­کندکه دارد اینترنت را با دسترسی‎اش کنترل و مدیریت می‎کند، اما این طور نیست؛ این ما هستیم که اینترنت را با قدرت‌ 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.

**6- هشدار:**

شما می­توانید با انجام چند دستورالعمل مؤثر، از رایانه خود در برابر تهدید­های سایبری [محافظت](http://www.iranvij.ir/%d9%85%d9%87%d9%85-%d8%aa%d8%b1%db%8c%d9%86-%d8%aa%d9%87%d8%af%db%8c%d8%af-%d9%87%d8%a7%db%8c-%d8%b1%d8%a7%db%8c%d8%a7%d9%86%d9%87-%d8%a7%db%8c-%d8%a7%d9%85%d8%b1%d9%88%d8%b2%db%8c-%d9%88-%d8%b1%d8%a7.html)کنید. پیروی از رهنمودهای ساده زیر کمک خواهد کرد تا خطر حمله را به حداقل برسانید.

▪ مراقب ایمیل­هایی باشید که از شما اطلاعات شخصی می­خواهند. 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 می­خواهد، فرم مربوطه را پر نکنید. چنین اطلاعاتی را تنها با استفاده از یک سایت ایمن وارد کنید.

▪ هر مورد مشکوکی را فوراً به بانک گزارش دهید.

▪ هرگز از لینک­های 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 سایت­های فیشینگ را مسدود می­کند یا نه و آیا نوار ابزاری را نصب   
می­کند که هنگام حملات شناخته شده فیشینگ، هشدار بدهد؟

▪ به طور منظم حساب های بانکی خود (شامل کارت­های پیش پرداخت و اعتباری، لیست گردش مالی حساب بانکی و غیره) را کنترل کنید تا مطمئن شوید تراکنش­های فهرست شده، قانونی و درست هستند.

مطمئن شوید که از آخرین نسخه مرورگر وب نصب شده در رایانه­تان، استفاده می­کنید و هرگونه وصله امنیتی نصب شده است.

فصل هفتم

جرایم­ رایانه­ای درکشور

**7-1جرایم رایانه­ای مهم در کشور**

آمار کاربران اینترنتی ایران بیش از 36 میلیون و 500 هزار نفر است‌ 26 میلیون نفر از کاربران اینترنتی کشور را جوانان تشکیل می‌دهند که بخش زیادی از آنها دانشجو هستند و در واقع 22 درصد فضای اینترنتی کشور توسط دانشجویان استفاده می‌شود. سردار سید کمال هادیانفر رئیس پلیس فتا در حاشیه ششمین اجلاس معاونان فرهنگی و اجتماعی و نمایندگان وزیر در هیأت‌های نظارت بر تشکل‌های اسلامی دانشگاه‌ها که در شهر مشهد مقدس برگزار شد، با اشاره به اینکه فضای مجازی، فضای جدیدی است که به موازات فضای فیزیکی و واقعی شکل گرفته است، گفت: این فضا فرصت‌های بی‌نظیری را به بسیاری از کشورها می‌دهد و لیکن باید به آسیب‌های جنگ نرمی که از این فضا متوجه جامعه هست توجه شود، وی ادامه داد: دانشگاه‌ها باید در این عرصه فعال باشند و به شناسایی فرصت‌ها، تهدیدات وآسیب‌های این حوزه بپردازند، 8 میلیون و 500 هزار جرم اینترنتی در 20 کشور جهان در سال 2009 به ثبت رسیده که یک میلیون و 900 هزار مورد آن مربوط به کشور آمریکا است و کشور کره با 164 هزار فقره جرم اینترنتی در رتبه چهارم جرایم اینترنتی قرار دارد. رئیس پلیس فتا به رشد 3.8 برابری آمار جرایم سایبری ایران در سال 90 نسبت به سال 89 اشاره کرد و گفت: در سال 89 تعداد هزار و 35 فقره جرم اینترنتی در ایران به ثبت رسید که این آمار در سال گذشته به چهار هزار مورد افزایش یافت. وی یادآورشد: در صورت ادامه روند کنونی رشد جرایم سایبری در ایران، میزان این جرایم در سال جاری به 8 تا 10هزار فقره افزایش می­یابد. وی ادامه داد:‌ چه بخواهیم و چه نخواهیم مردم وارد فضای مجازی می‌شوند و کسی نمی‌تواند از آن جلوگیری کند؛ هم اکنون استفاده از اینترنت در دنیا به عنوان یکی از حقوق بشر در سازمان ملل مطرح است.به اعتقاد وی باید به دنبال مدیریت فضای مجازی با آگاهی بر زوایای پنهان باشیم نه تقابل با این فضا چراکه با توجه به کاهش هزینه‌ها و سرعت انجام کار مجبور به استفاده از این فضا هستیم، رئیس پلیس فتا ادامه داد: ساختارهای کسب و کار سنتی با ساختار تجارت الکترونیک 8 تا 25 درصد صرفه‌جویی در پی دارد؛ در سال 2010، 3 هزار و 750 میلیارد چرخش فناوری در قالب 12.8 تریلیون دلار سهم تجارت صورت گرفت.

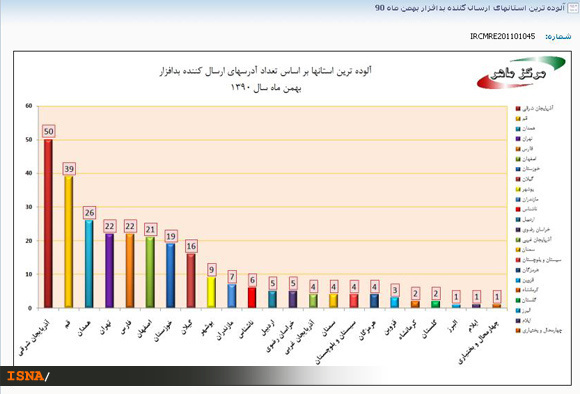
**7-2درآمدهای ناشی از جرایم سایبری**

وی (سردار هادیانفر) درآمدهای ناشی از جرایم سایبری را 388 میلیارد دلار و تفاوت 8 تا 25 درصدی تجارت الکترونیک را 105 میلیارد دلار دانست و افزود: کشورها مجبورند که به این سمت گام بردارند؛ کشورهای توسعه یافته به جهت انتقال ساختارها و بستر‌ها شتابان‌تر به این سمت می‌روند به همین جهت از آسیب پذیری‌ بعدی آن در امان نیستند. هادیانفر افزود: کشورهای در حال توسعه مانند ایران به جهت تهدیدات زیاد فضای سایبری سعی کرده با حوصله وارد این فضا شود، برهمین اساس خیلی از کشورهای دیگر در استفاده از این فناوری عقب‌تر است. وی درخصوص وضعیت دانشگاه‌ها در استفاده از فضای مجازی تصریح کرد: دانشگاه‌ها هنوز هم حضورشان در فضای مجازی کم است و خیلی جای کار دارند؛ البته پلیس نیز وظیفه دارد به دانشجویان آسیب‌ها، چالش‌ها، تهدیدات و جرایم را بشناساند تا آسیب‌ها کاهش یابد.

**7-3جرایم­ بانکی بیشترین آمار جرایم رایانه­ای درکشور**

وی در خصوص بیشترین جرایم اینترنتی درکشور گفت: 48.5 درصد از جرائم برداشت از حساب بانکی است که این به جهت بی‌موالاتی مالکین در نگهداری رمزهایشان، سوء استفاده اینترنتی از حساب‌هایشان یا نفوذ هکر به شبکه بانکی و برداشت پول بوده است. هتک حیثیت دومین جرم اینترنتی در کشور است که هادیانفر نمونه آن را ارائه اطلاعات غلط از اساتید دانشگاه، دزدیدن عکس‌ها با استفاده از ایمیل‌های ایجاد شده و انتشار آن در سایت‌ها دانست. رئیس پلیس فتا کلاهبرداری اینترنتی با استفاده از فیشینگ و فارمینگ را سومین جرم سایبری در کشور تلقی کرد و در توضیح فیشینگ باید گفت: پایه فیشینگ در آنطرف مرزها بسته شده است.

**7-4آلوده­ترین استان­های کشور در ضمینه ارسال بدافزار**



شکل 7-1

آلوده­ترین استان­های ارسال کننده بد افزار اینترنتی در کل کشور

دراین میان استان آذریجان شرقی با بیشترین (50درصد) و استان چهارمحال بختیاری و البرز و ایلام با کمترین میزان (1 درصد) جز کمترین و بیشترین ارسال کننده­های آدرس­های بدافزار در ایران به شمار میروند.

فصل هشتم

سوالات مهم در زمینه

جرایم رایانه­ای­

8-1سوالات ذیل از جمله مهمترین مسائل مربوط به جرایم رایانه است:

**1- منظور از جرم دسترسی غیرمجاز چیست؟**

بر اساس قانون اشاره شده هركس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی كه به‌ وسیله تدابیر امنیتی حفاظت ‌شده ‌است دسترسی یابد، مرتكب دسترسی غیر مجاز محسوب می­شود. در برخی جرایم مثل كلاهبرداری یا جعل مجازات ماموران دولتی تشدید می­شود در جرایم رایانه­ای نیز همینطور است و چنانچه مأموران دولتی كه مسئول حفظ داده‌های سری مقرر در ماده (3) قانون جرایم رایانه­ای یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذكور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل­های داده یا سامانه‌های مذكور شوند مجازات شدیدتری خواهند داشت.

**2-مجازات جرم دسترسی غیرمجاز چیست؟**

بر اساس قانون اشاره شده مرتكب دسترسی غیر مجاز به حبس از نود و یك روز تا یك‌سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محكوم خواهدشد.

1. **منظور از شنود غیرمجاز چیست؟**

بر اساس قانون اشاره شده هر كس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌‌های رایانه‌ای یا مخابراتی یا امواج الكترومغناطیسی یا نوری را شنود كند، مرتكب شنود غیرمجاز تلقی   
می­شود.

1. **مجازات جرم شنود غیرمجاز چیست ؟**

مرتكب جرم شنود غیرمجاز به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محكوم خواهدشد.

**5-جاسوس رایانه‌ای كیست ؟**

هركس به طور غیرمجاز نسبت به داده‌های سری درحال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده مرتكب اعمال زیر شود جاسوس رایانه­ای تلقی می‌گردد.

**6- مصداق اول جاسوس رایانه­ای؟**

کسی كه به داده‌ها یا تحصیل آنها یا شنود محتوای سری در حال انتقال دسترسی پیدا كند.

**7- مصداق دوم جاسوس رایانه­ای؟**

کسی كه داده‌های ر برای اشخاص فاقد صلاحیت در دسترس قراردهد.

**8- مصداق سوم جاسوس رایانه­ای؟**

كسی كه داده‌های برای دولت، سازمان، شركت یا گروه بیگانه یا عاملان آنها افشاء یا در دسترس قرار دهد.

**9- مجازات­های جاسوس رایانه­ای چه خواهد بود؟**

  الف) مجازات مصداق اول جاسوس رایانه­ای عبارت است از:

 بیست میلیون (20.000.000) ریال تا شصت میلیون (60.000.000) ریال یا هر دو مجازات.

  ب) مجازات مصداق دوم جاسوس رایانه­ای عبارت است از حبس از دو تا ده سال

ج) مجازات مصداق سوم جاسوس رایانه­ای عبارت است از حبس از پنج تا پانزده سال

**1-8 تشدید مجازات ماموران دولتی در این جرایم**

در برخی جرایم مثل كلاهبرداری یا جعل مجازات ماموران دولتی تشدید می­شود در جرایم رایانه­ای نیز همینطور است و چنانچه مأموران دولتی كه مسئول حفظ داده‌های سری مقرر در ماده (3) این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذكور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل­های داده یا سامانه‌های مذكور شوند مجازات شدیدتری خواهند داشت.

**\*قانون جرایم رایانه­ای:**

بر اساس ماده 5 قانون جرایم رایانه­ای این اشخاص به مجازات زیر محكوم می­شوند:

* حبس­ از91 روز تا 2 سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات. بعلاوه این اشخاص به انفصال از خدمت از شش ماه تا دو سال

نیز محكوم خواهندشد.

**نتیجه گیری**

جرایم­رایانه­ای یکی از پدیده­های نوظهوری ­است که گرچه برخی از جرایم آن شباهت­هایی با جرایم سنتی دارد، اما تفاوت­هایی در روش و ماهیت و نوع­ جرم دارد که از لحاظ جرم­شناسی و کیفرشناسی و حقوق کیفری پژوهش­های نوی را می­طلبد. جرایم­رایانه­ای به ­دلیل تأثیرات ناگواری که برجامعه­اطلاعاتی وکاربران دارد، برخورد جدی­تری را از سوی دولت مردان سیاسی و قضایی می­طلبد. نظارت و فیلترکردن دقیق تر و جدی­تری، چه برای جلوگیری از آسیب امنیتی و چه آسیب­های فرهنگی را می­طلبد.

حقوق ایران در زمینه جرایم­ رایانه­ای گرچه تلاش های مفیدی داشته، ولی همنان نیاز به کار و پژوهش در زمینه ابعاد مختلف آن دارد. ضمن اینکه در عرصه قانونگذاری کاستی­هایی نیز وجود دارد که امید است با تصویب قانون مجازات جرایم رایانه­ای که سال­هاست در فراموشخانه مجلس مورد بی مهری است، گامی در این راه برداشته شود متخصصان معتقدند جرم جاسوسي ‌رايانه‌اي، با شدت و پيچيدگي بيشتري در سطح وسيع جهاني ادامه پيدا خواهد كرد). رفته رفته جاسوسي اينترنتي به عنوان ابزاري براي حصول برتري در رقابت بي‌پايان كشورها در زمينه‌هاي صنعتي، اقتصادي، نظامي ‌وغیره تبديل خواهد شد وكشورهاي بيشتري وارد صحنه بازارکار ‌رايانه‌اي مي‌شوند. اين جنگي است كه در آن نيازي به استفاده از پياده نظام، هواپيما جنگنده و موشك نيست. كليد موفقيت در اين جنگ اطلاعات است، عوامل جاسوسي ‌رايانه‌اي و اينترنتي نقش پياده نظام اين جنگ پسامدرن را بازي مي‌كنند.

در حال حاضر با عنايت به پيشرفت‌هاي لحظه‌اي در عرصه رايانه و فضاي سايبر ضرورت آموزش‌ بيش از پيش مشخص شده و براي اجراي يك سياست كيفري مؤثر جهت پيشگيري از جرايم ‌رايانه‌اي به‌خصوص جاسوسي رايانه­اي و اينترنتي، اين آموزش‌ها بايد در مقاطع مختلف زماني تكرار و روزآمد شوند.

**\*آموزش هایی برای کشف جرایم رایانه­ای:**

1- از آنجاكه پليس به عنوان ضابط دادگستري وظيفه كشف جرايم را بر عهده دارد، در كنار آموزش قضات وساير مقدمات قضايي، آموزش پليس نيز بايد در سرفصل برنامه‌ريزي‌ها قرار گيرد.

2-آموزش‌هاي عمومي ‌در سطح كارمندان دولت و نظاميان.

3- تا حد ممكن عدم ذخيره سازي داده‌ها و اطلاعات طبقه بندي شده به شبكه‌هاي ‌رايانه‌اي به‌خصوص شبكه جهاني اينترنت.

5- تشكيل هرچه سريع تر مراجع تخصصي قضايي وپليس با عنايت به الزام قانوني ماده 30 ق.ج. رو تقويت آنها.

6- مسدود كردن درگاه‌هاي رايانه‌هاي حساس در ادارات به عنوان راهكاري سريع وكم هزينه و در عين حال مؤثر. در اين روش تمامي ‌درگاه‌هاي سيستم‌هاي ‌رايانه‌اي از قبيل درايورها، پورت‌هاي USB وغیره از طريق سرور (شبكه) بسته شده و به اين ترتيب كاربر رايانه نمي‌تواند هيچ داده و اطلاعاتي را وارد رايانه كرده و يا از آن خارج كند. در اين حالت كاربر تنها به داده‌هاي مجازي‌ كه از سوي مسئولان و به منظور انجام وظيفه روي سيستم او قرار داده شده، دسترسي خواهد داشت. اما واقعیت این است که مبارزه و کشف اینگونه جرایم کاری بس دشوار است، چرا که به واسطه ویژگی­های فضای مجازی که ظرفیت سوء استفاده از آن را بالا می برد. ویژگی­هایی؛ چون بدون مرز بودن فضای مجازی، کم هزینگی و پرثمری و پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات بالا بدون آسیب جسمانی مجرم، آسان بودن تهیه و امکانات و عوامل مورد نیاز جرم، بازتاب جهانی موفقیت، به ویژه در ملات تروریستی و مکتوم ماندن شکست، امکان هماهنگی یکدیگر در جرایم سازمان یافته، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پول­شویی آسان تر و هرگونه انجام فعالیت­های مالی الکترونیکی در جهت اهداف مجرمانه و غیره.

**جدول راهکارهای ایران و کشورهای دیگر برای مقابله با جرائم رایانه­ای:**

|  |  |
| --- | --- |
| **نام کشور** | **راهکار مقابله** |
| **آمریکا** | **کنترل کاربران اینترنتی خود از طریق جاسوسی  (در سطح جهانی)** |
| **انگلیس** | **شورای امنیت و مقابله با جرایم اینترنتی**  **(اعزام بالن به آسمان و تجهیز این بالن­ها به تجهیزات کنترل کننده ارتباطی)** |
| **ایران** | **پلیس فتا و ستاد مبارزه با جرائم اینترنتی** |

جدول 8-1

گفتنی است که به غیر از ایران هم تلفن و هم اینترنت کاربران توسط استخدام هکرهای حرفه­­ای با نفوذ به اطلاعات شخصی کاربران و کنترل و بررسی روزمره کارهای کاربران در ایترنت از برخی جرائم رایانه­ای جلوگیری می­کنند ولی اینکار نقض حقوق بشریت است و خود به نوعی بدتر از جرم رایانه­ای است.

مراجع

1- عاطفه زاهدی "قوانین ومقررات ناظر بر جرایم رایانه­ای(اینترنتی)".

2- گروه علمی موسسه آموزش عالی آزاد چتر دانش.ناشر,آراسبز.نوبت وسال چاپ,اول-1391"مجموعه قوانین ومقررات کاربردی جزایی"

3- رضوي.محمد.(جرايم سايبري ونقش پليس در پيشگيري ازاين جرايم وكشف آنها)فصل نامه دانش انتظامي.سالن نهم.ش يك.قانون جرايم سايبري مصوب 1388

4- پلیس فتا – نیروی انتظامی جمهوری اسلامی ایران

[1]: policing cybercrime BY: petter Gottschalk for www.bookboon.com

1. Phishing [↑](#footnote-ref-1)
2. PIN [↑](#footnote-ref-2)
3. Cyber stalking [↑](#footnote-ref-3)
4. کنوانسیون جرایم رایانه­ای [↑](#footnote-ref-4)
5. Obscenity [↑](#footnote-ref-5)
6. Proxy [↑](#footnote-ref-6)