حقوق و جرایم سایبری

مقدمه

امروزه بسیاری از مردم از شبکه اینترنت یا اینترنت برای مبادله پیام یا فعالیت‌های دیگر استفاده می‌کنند. این شبکه‌ها فاصله زمانی و مکانی را از بین برده و قدرت زیادی در اختیار بشر قرار داده است. چون این فناوری فضای اشتراکی ایجاد کرده و مفاهیم جدیدی چون حاکمیت سایبری و غیره را به منصه ظهور رسانده است، برای استفاده از آن نیازمند تدوین قوانین جدیدی هستیم که حقوق سایبری نام دارد. از طرفی این فضا شرایط سوء استفاده را برای افراد بزهکار فراهم کرده است از این روی در این فضا نیز ممکن است انسان مرتکب جرم شود. چون چنین جرمی در فضای اینترنتی روی می دهد آن را جرم الکترونیکی یا سایبری نام می نهند.

ماهیت جرایم سایبری

چون جرایم کامپیوتری و سایبری ناشی از فناوری مدرن است از این روی آثار جالبی دارد که در ادامه بررسی می شود :

۱- جرایم کامپیوتری تصنعی هستند.

جرایم را به دو دسته طبیعی و تصنعی تقسیم می کنند که جرایم طبیعی بیشتر تحت سیطره قوانین مذهبی و شرعی است لکن جرایم تصنعی امور حادثند و تحت شمول مقررات جدید قرار می گیرند.

۲- تأثیر وجدانی اندکی برفاعل دارند.

فاعل بعضی از جرم ها نظیر سرقت یا قتل بعد از انجام جرم احساس سرزنش می کند (نوعا یا شخصا) اما فردی که چراغ قرمز را رد می کند و به مقررات راهنمایی و رانندگی در این خصوص توجه نمی نماید غالبا احساس شرمساری نمی کند. جرایم سایبری نیز جزو دسته دوم بوده و به علت ماهیت تکنولوژیک آن احساس غرور نیز در فاعل آن پدید می آید.

۳- عنصر مادی جرایم سایبری مشابه است(شکل یکسان ارتکاب).

به دلیل بسترهای متفاوت ارتکاب جرم های کلاسیک وشکل های متفاوت سناریوی مجرمانه طبعا عنصر مادی جرم ها با یکدیگر متفاوتند. لکن در اکثر جرایم کامپیوتری عنصر مادی یکسان بوده و امروزه بستر فناوری این جرم ها نیز یکی شده است. شکل یکسان ارتکاب از حیث اجزای عنصر مادی یا یکسانی به واسطه بستر فناوری است که موارد ذیل نمونه ای از آن است :

- ✓ قوانین ماهوی و شکل یکسان دارند.
- ✓ رویه های یکسان برای مبارزه وجود دارد.
- ✓ الزامات یکسان داخلی/ بین المللی دارند.
- ✓ پلیس واحد برای آن نیاز است.

٤- زمان ارتکاب جرم به حداقل رسیده است.

در حالت سنتی برای جرم مراحل ذیل تصور می شود :

- ✓ قصد مجرمانه
- ✓ تهیه مقدمات
- ✓ عملیات اجرایی جرم

درتمام مراحل فوق گذشت زمان مشهود است و ممکن است قصد تا عملیات اجرایی جرم از چند ثانیه تا چند ماه زمان نیاز داشته باشد. لکن در جرایم سایبری این زمان به چند ثانیه یا کسر ثانیه تبدیل می شود. فرد مرتکب از لحظه ارسال تا دریافت مطالب افتراآمیز در کل شبکه کمتر از چند ثانیه زمان نیاز دارد.

۵- مکان ارتکاب بین المللی شده است.

بعضی ازعواملی که تعدد مکان جرم را موجب می شود عبارتنداز :

- ✓ محل ارتکاب
- ✓ محل وقوع نتیجه
- ✓ محل وجود ادله
- ✓ محل فرار مرتکب

در جرایم سایبری به واسطه زیرساخت جهانی مکان ارتکاب جرم به تمام کره زمین توسعه یافته است. فردی که مطالب افتراآمیز در شبکه منشر می کند در زمان بسیار کوتاه پیام خود را به منطقه وسیعی از زمین می رساند. یا کسی که ویروسی نوشته و منتشر می کند چندین کامپیوتر را در کشورهای مختلف آلوده می کند. به دلیل ماهیت بین المللی جرایم سایبر مبارزه با آن نیز تشریک مساعی تمام کشورها را می طلبد.

٦- بزه دیده به جای انسان ماشین است.

درحالت سنتی بزه دیده یا که هدف جرم است انسان می باشد و در جرایم علیه اشخاص، تمامیت جهانی و معنوی فرد هدف ارتکاب جرم است. در جرایم علیه اموال جرم علیه مال متعلق به انسان است. شکل اولیه بزه دیده در جرایم سایبری رابطه انسان و ماشین بود. در کلاه برداری کامپیوتری اولیه و کلاسیک فرد مرتکب، با دادن دستورالعمل اضافی بدون این که آنان را بفریبد یا حتی دیده باشد وجوه دیگران را به خود اختصاص می داد. در شکل جدید و اخیر این **شکل از بزه دیده به صورت ماشین- ماشین تغییر یافته است که بیشترین مورد تحقق آن در جرایم تجارت الکترونیکی و جرایم بانکداری الکترونیکی است.**

تاريخچه جرائم كامپيوتري

- با پيدايش كامپيوتر، جرائم كامپيوتري نيز بوجود آمد. تاريخچة جرائم كامپيوتري را مي‌توان به سه نسل طبقه بندي نمود
- نسل اول : **جرايم رايانه اى** كه تا اواخر دهة 1980 مي‌باشد شامل سرقت و كپي برداري از برنامه‌ها و جرائم عليه حريم خصوصي اشخاص مانند سرقت از آثار و تحقيقات افراد بود.
- نسل دوم: كه تحت عنوان **جرائم داده‌ها**ناميده مي‌شود تا اواخر دهه 1990 ادامه داشته است .در اين دهه تمامي جرائم عليه تكنولوژي اطلاعاتي، ارتباطاتي، كامپيوتري، ماهواره اي و شبكه‌هاي بين المللي تحت عنوان جرائم عليه داده‌ها اطلاق مي‌شود
- نسل سوم كه از اواسط دهة 1990 شروع مي‌شود جرائم كامپيوتري تحت عنوان **جرائم سايبريا جرائم در محيط سايبر**معروف گرديد

- **حقوق فضای سایبر(حقوق فناوری اطلاعات)** : کلیه ابعاد مدنی , تجارت جزایی , بین الملل و فنی را شامل می شود .
- از حیث ابعاد حقوقی یعنی بعد حقوق خصوصی در حقوق سایبری دو بحث عمده مطرح است , **یکی بعد مدنی** و **دیگر بعد تجاری** .

1- بعد مدنی :

- الف **قراردادهای انفورماتیک:** از حیث نوع شناسی ، قرارداد ، بسته به خرید ، توزیع ، سفارش و پشتیبانی تفاوت می کند.نوع شناسی قراردادهای انفور ماتیک کاملا برگرفته از منطق برنامه نویسی و مراحل ان است .شامل
- 1- طراحی و ظهور در برنامه ، پیاده سازی سیستم و نرم افزار ، پشتیبانی سیستم یا برنامه ، راه اندازی سیستم و برنامه
- 2-خرید بسته های نرم افزاری ، مراحل ازمون (الفا)و استفاده موقت (بتا)و بکارگیری دائم و نهایی(فینال)
- 3-مالکیت فکری ، که بیشتر در بحث مالکیت کپی رایت مطرح میشود.

- ب **مسئولیت مدنی قراردادی** : مسئولیت ناشی از قرارداد که بسته به نوع تعهد و تخلف قراردادی به وجود می آید.این نوع مسئولیت می تواند در امور مختلف بروز کندو نتایج گوناگونی بوجود آورد.مانند مسئولیت ناشی از **نرم افزارهای معیوب** در امور بیمارستانی برای درمان بیماران که موجب مرگ بیمار می شود .
- **دکترین مراقبت** مانند اینکه فرد داده ها و اطلاعاتی را روی شبکه می گذارد که گاهی نادرست است (مانند استفاده از قارچ های خوراکی ، اطلاعاتی ارائه می شود که و یک کاربراینترنت از ان استفاده می کند و مسموم میشود)در اینجا به نوعی مسئولیت مدنی بروز و تحقق می یابد .
- **استانداردها** : برای اینکه بتوان بگونه ا ی عادلانه مسئولیت را بر افرادمستقر کرد ، باید در ابتدا استاندارد های مختلفی برای انواع کالا ها و خدمات و.. اعلام شود . و اگراین استانداردها موحود بود آنگاه باید میزان مراقبت را سنحید
- ج **ادله ا ثبات دبجیتالی:** نکته مهم برشمردن دلایل است . کلا به **اقرار ،اسناد کتبی ،شهادت ،امارات وقسم** تقسیم می شود. ویژگی دلیل در امور مدنی احصا شدن است و بسته به نوع دلیل قواعدی بر آن حاکم است.در اسناد مهم ترین مسئله فرایند حاکم بر ایجاد سند است . **سند رسمی باید برابر قانون ثبت اسناد تشکیل شود تا بتواند رسمی تلقی شود .**
- **کتبی نبودن دادها و اطلاعات و راحتی اصلاح و محو شدن فایل ها موجب می شود که بقا به معنی فیزیکی ومعمولی وجود نداشته باشد بنابراین اصالت مرسوم اسناد رسمی وجود ندارد.**

- **حقوق مالکیت فکری** : خود شامل چند نوع است که مهم ترین آنها شامل حق اختراع طرح های صنعتی و علایم تجاری و حق طبع یا کپی رایت است.
- ه **پایگا داده ها:** پایگاه داده ها به دلیل نوع ارایه و انتخاب و نیز ارزش اقتصادی و ماهیت خود ماهیتی جدا از نظام مالکیت فکری و به ویژه کپی رایت را می طلبد.

2 - بعد تجاری:

- حقوق تجارت دارای دو بعد داخلی و خارجی است که باپیدایش و تکامل شبکه های رایانه ای بین المللی این تفکیک از بین رفت. ابتدا بحث تبادل الکترونیک داده های بسته , مبنا و معیار تجارت بود و سپس جای خود را به تبادل داده های باز داد و امروزه بعد تجارت فضای سایبر به تجارت الکترونیکی , تبادلات الکترونیکی و مانند ان پرداخته است

- **ابعادعمومی (حقوق اساسی - اداری) سایبر** : از بعد حقوق عمومی در سایبرلا دو بحث عمده حمایت از داده ها و جریان آزاد اطلاعات مطرح است که هم حقوق اساسی و هم حقوق اداری را شامل می شود .
- **الف- حمایت از داده ها** :داده های شخصی ناظر برداده های هویتی شخص است . که موجب تمایز انسان و حریم خصوصی شخص از دیگری می شود حمایت از داده هاناظر برحمایت از افراد در قبال پردازش داده های شخصی در حالت اتوماتیک , نیمه اتوماتیک یا غیراتوماتیک است.این داده ها با داده های عمومی ،داده های احتماعی - اعم از پزشکی ،سوابق کیفری و قضایی- داده های علمی و آماری تفاوت دارد.
- هرگونه دسترسی , افشا , در اختیار داشتن , نشر,توزیع و پردازش غیرقانونی جرم است و بسته به سیستم قضایی و قانونی مورد نظر در یک یا دو دسته از جرایم اداری و جرایم کیفری به طور مجزا مشخص می شود.

- **ب -جریان آزاد اطلاعات** : در محیط دیجیتالی و شبکه های رایانه ای اصل بر آزاد بودن جریان اطلاعات و دسترسی افراد به اطلاعات است . اما این آزادی بی حد و مرز نیست . در مسایل امنیتی , حریم خصوصی افراد , اسرار دولتی مهم و مسایل بهداشتی این آزادی نفی می شود.
- شاخه های جریان آزاد اطلاعات با گسترش و پیشرفت رایانه ، محدوده و وسعت بیشتری یافته ومباحثی مانند دموکراسی الکترونیکی ، دولت الکترونیکی ،پارلمان الکترونیکی و رای گیری الکترونیکی نیز مطرح شده.
- **ابعاد بین المللی حقوق سایبر** : در فضای سایبر مرزی به آن معنا در داخل کشورها وجود ندارد . اصل حاکمیت دولت و اصل استقلال عدم مداخله در حاکمیت در فضای سایبر به شدت دچار تنش شده است , فضای سایبرفضای واحد جهانی الکترونیکی محض است . به همین دلیل باید این فضا نظامند و قاعده مند شود.

انواع جرايم اينترنتي

جرايم اينترنتي شامل انواع مختلفي مي شوند از جمله:

1- جرايم عليه محرمانه بودن و تماميت و در دسترس بودن داده ها.

2- جرايم عليه سيستم هاي رايانه اي و اينترنتي مانند اخلال در سيستم ها.

3- جرايم عليه اموال مانند كلاهبرداري اينترنتي.

4- جرايم عليه امنيت و آسايش عمومي مانند توهين به مقدسات و اصول كلي يك كشور.

5- جرايم عليه مالكيت فكري.

6- جرايم عليه محتوي مانند پرنوگرافي (تصاوير و فيلم هاي مستهجن جنسي).

به طور كلي اين شش دسته در تمام كشورها جرم شناخته شده و به طور كلي آن چه مبنا و محور اين نوع تقسيم بندي قرار گرفته است ارزش هايي هستند كه مورد حمايت قانونگذار بوده و مورد تجاوز و تعدي مجرمان قرار گرفته است و شايد ارزش ها از كشوري تا كشور ديگري متفاوت باشند.

تعیین مصادیق محتوای مجرمانه :

- **الف) محتوای علیه عفت و اخلاق عمومی**
- ۱- اشاعه فحشاء و منکرات (بند ۲ ماده ۶ قانون مطبوعات)
- ۲- تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی (بند ب ماده ۱۵ قانون جرایم رایانه‌ای و ماده ۶۴۹ قانون مجازات اسلامی)
- ۳- انتشار، توزیع و معامله محتوای خلاف عفت عمومی (مبتذل و مستهجن) بند ۲ ماده ۶ قانون مطبوعات و ماده ۱۴ قانون جرایم رایانه‌ای)
- ۴- تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل (ماده ۱۵ قانون جرایم رایانه‌ای)
- ۵- استفاده ابزاری از افراد (اعم از زن و مرد) در تصاویر و محتوی، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیر قانونی (بند ۱۰ ماده ۶ قانون مطبوعات)

ب) محتوای علیه مقدسات اسلامی

- ۱- محتوای الحادی و مخالف موازین اسلامی (بند ۱ ماده ۶ قانون مجازات اسلامی)
- ۲- اهانت به دین مبین اسلام و مقدسات آن (بند ۷ ماده ماده ۶ قانون مجازات اسلامی و ماده ۵۱۳ قانون مجازات اسلامی)
- ۳- اهانت به هر یک از انبیاء عظام یا ائمه طاهرین (ع) یا حضرت صدیقه طاهره (س) (ماده ۵۱۳ قانون مجازات اسلامی)
- ۴- تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام (بند ۹ ماده ۶ قانون مطبوعات)
- ۵- تبلیغ مطالب از نشریات و رسانه‌ها و احزاب و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آنها باشد (بند ۹ ماده ۶ قانون مطبوعات)
- ۶- اهانت به امام خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)
- ۷- اهانت به مقام معظم رهبری (امام خامنه‌ای) و سایر مراجع مسلم تقلید (بند ۷ ماده ۶ قانون مطبوعات)

ج) محتوای علیه امنیت و آسایش عمومی

- 1ـ تشکیل جمعیت، دسته، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور (ماده ۴۹۸ قانون مجازات اسلامی)
- 2ـ هر گونه تهدید به بمب گذاری (ماده ۵۱۱ قانون مجازات اسلامی)
- 3ـ محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند (بند ۱ ماده ۶ قانون مطبوعات)
- 4ـ انتشار محتوی علیه اصول قانون اساسی (بند ۱۲ ماده ۶ قانون مطبوعات)
- 5ـ تبلیغ علیه نظام جمهوری اسلامی ایران (ماده ۵۰۰ قانون مجازات اسلامی)
- ۶- اخلال در وحدت ملی و ایجاد اختلاف ما بین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی (بند ۴ ماده ۶ قانون مطبوعات)
- ۷- تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحاء در خدمت نیروهای مسلح هستند به عصیان، فرار، تسلیم یا عدم اجرای وظایف نظامی (ماده ۵۰۴ قانون مجازات اسلامی)

- ۸- تحریص و تشویق افراد و گروه‌ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور (بند ۵ ماده ۶ قانون مطبوعات)
- ۹- تبلیغ به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران (ماده ۵۰۰ قانون مجازات اسلامی)
- ۱۰- فاش کردن و انتشار غیر مجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی (بند ۶ ماده قانون مطبوعات و مواد ۲ و ۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرایم رایانه‌ای)
- ۱۱ـ فاش کردن و انتشار غیر مجاز اسرار نیروهای مسلح (بند ۶ ماده قانون مطبوعات)
- ۱۲ـ فاش کردن و انتشار غیر مجاز نقشه و استحکامات نظامی (بند ۶ ماده ۶ قانون مطبوعات)
- ۱۳ـ انتشار غیر مجاز مذاکرات غیر علنی مجلس شورای اسلامی (بند ۶ ماده ۶ قانون مطبوعات)
- ۱۴ـ انتشار بدون مجوز مذاکرات محاکم غیر علنی دادگستری و تحقیقات مراجع قضایی (بند ۶ ماده ۶ قانون مطبوعات)

د) محتوای علیه مقامات و نهادهای دولتی و عمومی

- ۱- اهانت و هجو نسبت به مقامات، نهادها و سازمان حکومتی و عمومی (بند 8 ماده 6 قانون مطبوعات و مواد ۶۰۹ و ۷۰۰ قانون مجازات اسلامی)
- ۲- افترا به مقامات، نهادها و سازمان حکومتی و عمومی (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)
- ۳- نشر اکاذیب و تشویش اذهان عمومی علیه مقامات، نهادها و سازمان‌های حکومتی (بند ۱۱ ماده ۶ قانون مطبوعات و ۶۹۸ قانون مجازات اسلامی)

۵) محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم به‌کار می‌رود

- ۱- انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم افزارهای که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌رود (ماده ۲۵ قانون جرایم رایانه‌ای)
- ۲- فروش، انتشار یا در دسترس قرار دادن غیر مجاز گذر واژه‌ها و داده‌هایی که امکان دسترسی غیر مجاز به داده‌ها با سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می‌کند (ماده ۲۵ قانون جرایم رایانه‌ای)
- ۳ـ انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی (ماده ۲۵ قانون جرایم رایانه‌ای)
- ۴- آموزش و تسهیل سایر جرایم رایانه‌ای (ماده ۲۱ قانون جرایم رایانه‌ای)

- ۵- انجام هر گونه فعالیت تجاری و اقتصادی رایانه‌ای مجرمانه مانند شرکت‌های هرمی (قانون اخلال در نظام اقتصادی کشور و سایر قوانین)
- ۶- انتشار ویروس دهی بازی‌های رایانه‌ای دارای محتوای مجرمانه (مواد مختلف قانون مجازات اسلامی و قانون جرایم رایانه‌ای)
- ۷- انتشار فیلتر شکن‌ها و آموزش روش‌های عبور از سامانه‌های فیلترینگ (بند ج ماده ۲۵ قانون جرایم رایانه ای)
- ۸- تبلیغ و ترویج اسراف و تبذیر (بند ۳ ماده ۶ قانون مطبوعات)
- ۹- انتشار محتوای حاوی تحریک، ترغیب، یا دعوت به اعمال خشونت آمیز و خودکشی (ماده ۱۵ قانون جرایم رایانه‌ای)
- ۱۰- تبلیغ و ترویج مصرف موادمخدر، مواد روان گردان و سیگار (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵)

- ۱۱- باز انتشار و ارتباط (لینک) به محتوای مجرمانه تارنماها و نشانی‌های اینترنتی مسدود شده، نشریات توقیف شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیر قانونی
- ۱۲- تشویق، تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق موادمخدر، قاچاق مشروبات الکلی و غیره (ماده ۴۳ قانون مجازات اسلامی)
- ۱۳- انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد
- ۱۴- تشویق و ترغیب مردم به نقض حقوق مالکیت معنوی (ماده ۱ قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه ای و ماده ۷۴ قانون تجارت الکترونیکی)
- ۱۵-معرفی آثار سمعی و بصری غیر مجاز به جای آثار مجاز (ماده ۱ قانون نحوه مجازات. اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)
- ۱۶ـ عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی (ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)

جرايم اينترنتي از نظر نوع تاثير به سه طبقه كلي تقسيم مي شوند:

1- جرايم اينترنتي فرهنگي

الف جرايم بر ضد ارزش هاي فرهنگي چون توهين و اهانت به دين مبين اسلام و مقدسات

ب) جرايم محتوا (Content Crime) چون هتك عفت عمومي

ج) افشاي اسرار خصوصي افراد.

2- جرايم اينترنتي امنيتي چون ايجاد اخلال در امنيت داده ها.

3- جرايم اينترنتي مالي چون سرقت و كلاهبرداري اينترنتي.

الف) جرايم برضد ارزش ها

حفظ ارزش هاي موجود در جامعه موجب ماندگاري و ثبات فرهنگ و اخلاق آن جامعه مي شود. به همين جهت، هر جامعه اي در جلوگيري از محو يا كم رنگ شدن آن ها مي كوشد. فرهنگ ايراني اسلامي نيز داراي ارزش هايي است كه بايد به طرق مختلف از جمله قرار دادن ضمانت اجرا و برخورد با مهاجمان به ارزشها در صيانت آن كوشيد.

علاوه بر ماده 513 قانون مجازات اسلامي كه قانوني عام و شامل برخي جرايم اينترنتي نيز مي شود، در قانون مطبوعات كه طبق تبصره 3 ماده 1 شامل كليه نشريات الكترونيكي ثبت شده بر اساس اين قانون مي شود، به جرم توهين به اسلام و مقدسات اشاره شده است. البته قانون مطبوعات را نمي توان شامل برخي مصاديقي دانست كه خارج از اين قانون هستند. چرا كه صفحات وب، داده ها و نشريات الكترونيكي ثبت نشده يا خارج از ايران را شامل نمي شود.

ب) جرايم محتوا (Content Crime)

يكي از ارزش هاي مترقي جوامع اسلامي حفظ عفت عمومي و اخلاق حسنه است. حفظ عفت عمومي، اقدامي پيشگيرانه از وقوع جرايم بسياري است كه ناشي از ايجاد هرج و مرج در رفتارهاي افراد جامعه مي شود. به عنوان نمونه، يكي از عوامل اصلي وقوع جرم زنا، همجنس بازي، مساحقه و قوادي به هيجان در آوردن شهوت مجرمان است كه در اثر ترويج مطالب مستهجن افزايش خواهد يافت. از اين رو، قانون جرايم رايانه اي، فصل چهارم خود را به جرايم مرتبط با محتوا اختصاص داده است.

انواع جرائم رايانه‌اي

تقسيم بندي جرائم كامپيوتري

1- جرائم كامپيوتري عليه اشخاص

2- جرائم كامپيوتري عليه اموال و مالكيت

3- جرائم كامپيوتری عليه دولتها يا وظايف دولت‌ها

انواع جرائم رايانه‌اي

تقسيم بندي جرائم كامپيوتري

1- جرائم كامپيوتري عليه اشخاص

الف: نوشته‌ها و عكسهاي شهوت انگيز

ب: اذيت و آزار كردن

ج: تهديد به قتل

د: كلاهبرداري

2- جرائم كامپيوتري عليه اموال و مالكيت (كپی رايت)

الف: سرقت و تكثير غير مجاز برنامه‌هاي كامپيوتري حمايت شده

ب: سابوتاژ (خرابكاري) و اخاذي كامپيوتري

ج: كلاهبرداري كامپيوتري از طريق كارت اعتباري د: قاچاق مواد مخدر از طريق اينترنت

ه: پولشوئي كامپيوتری

3- جرائم كامپيوتری عليه دولتها يا وظائف دولتها

الف: تهديد به گروگان گيری، اخاذي و كشتن مسئولين و يا اعضاي خانوادة آنها

ب: جاسوسي كامپيوتري

ج: ترور

1- جرائم کامپیوتری علیه اشخاص جرائم کامپیوتری علیه اشخاص عبارتند از:

الف: نوشته‌ها و عكسهاي شهوت انگيز (pornography) فروش يا به تصوير كشاندن عكسهاي مبتذل جهت تحريك كردن نوجوانان و يا پيدا نمودن اشخاص از طريق چات(گپ زدن) جهت به نمايش گذاشتن عكسهاي آنها در اينترنت و معرفي آنها به ديگر اشخاص جهت داشتن ارتباط نامشروع.

ب: اذيت و آزار كردن (Harassment) اين نوع جرم ممكن است به صورت ارتباطات و دست انداختن و متلك گفتن ، بي حرمتي به مقدسات و مطالبه كردن وجه از ديگران باشد.

ج: تهديد به قتل يكي از جرائمي كه ممكن است از طريق اينترنت و يا ارسال پيغام به ايميل اشخاص صورت پذيرد تهديد به قتل مي‌باشد.

د: كلاهبرداري

كلاهبرداري كامپيوتري از جمله جرائم اصلي سوء استفاده های كامپيوتري عليه اشخاص و يا دارائي افراد محسوب مي‌گردد.

دارائي عيني غير ملموس در قالب داده‌هاي كامپيوتري مانند وجوه سپرده و پس انداز ، تغيير و دست كاري كردن در ساعات كاري، متداولترين راههاي كلاهبرداري كامپيوتري مي‌باشد. در تجارت الكترونيك نقل و انتقال پول نقد و خريد و فروش كالاهاي تجاري، به سرعت جاي خود را به انتقال سپرده‌ها از طريق سيستمهاي كامپيوتري داده‌است كه نتيجتاً موجبات سوء استفاده كردن افراد سودجو و فرصت طلب را فراهم كرده است.

كلاهبرداري كامپيوتري از **طريق وارد كردن رمزها به خودپردازها و سوء استفاده كردن از كارتهاي اعتباري ديگران معمول ترين شيوة ارتكاب در كلاهبرداري كامپيوتري مي‌باشد**

در ذيل به نمونه‌هائي از كلاهبرداريهاي كامپيوتري اشاره مي‌شود:

1- سوء استفاده از شبكة تلفني امروزه بعضي از افراد سودجو با استفاده از تكنيكهائي وارد خطوط تلفني مي‌شوند كه آنها می توانند مكالمات تلفني خود را با هزينه‌هاي مشتركين ديگر انجام دهند. نوع ديگر سوء استفاده از شبكة تلفني، از طريق تجارت با شماره‌هاي كارت تلفن انجام مي‌شود كه از طريق كامپيوتر مورد نفوذ يافتگي قرار مي‌گيرد.

2- **سوء استفاده از صندوقهاي خود پرداز** در گذشته، سوء استفاده از صندوقهاي خود پرداز با استفاده از كارت بانكهائي كه به سرقت مي‌رفت صورت مي‌گرفت ولي امروزه، با استفاده از سخت افزار و نرم افزار ويژة كامپيوتري، اطلاعات الكترونيكي غير واقعی به صورت كد روي كارتهاي بانك ثبت شده مورد سوء استفاده قرار مي‌گيرد.

3- **سوء استفاده از كارتهاي اعتباري** در حال حاضر ، بيشتر معاملات از طريق اينترنت صورت مي‌گيرد. مثلاً پرداخت قبوض برق، آب، تلفن و همچنين خريد كالا، شركت در همايشهاي بين المللي و غيره معمولاً با استفاده از كرديت كارت (كارت اعتباري) استفاده مي‌شود و معمولا مشتري مي‌بايستي رمز كارت خود و ديگر جزئيات را قيد نمايد. بدين جهت بعضي از افراد سودجو با فاش شدن رمز كارت اعتباري مشتريان سوء استفاده مي‌نمايند

جرائم كامپيوتري عليه اموال و مالكيت جرائم اقتصادي كه از طريق كامپيوتر يا شبكة جهاني (اينترنت) صورت مي‌پذيرد عبارتند از:

الف: سرقت و تكثير غير مجاز برنامه‌هاي كامپيوتري حمايت شده از آنجائيكه براي ساخت و توليد يك برنامة كامپيوتري يا سينمايی هزينه‌هاي زيادي اعم از مالي و زماني صرف مي‌شود لذا تكثير و استفاده غير مجاز از آن براي صاحبان قانوني زيانهاي بسيار زيادي را به بار خواهد داشت.

ب: سابوتاژ (خرابكاري) و اخاذي كامپيوتري

سابوتاژ كامپيوتري يعني اصلاح، موقوف سازي و يا پاك كردن غير مجاز داده‌ها و يا عمليات كامپيوتري به منظور مختل ساختن عملكرد عادي سيستم. سابوتاژ كامپيوتري ممكن است وسيله‌اي براي تحصيل مزاياي اقتصادي بيشتر نسبت به رقيبان يا براي پيش‌برد فعاليتهاي غير قانوني تروريست براي سرقت داده‌ها و برنامه‌ها به منظور اخاذي باشد.

ج: كلاهبرداري كامپيوتري

از طريق كارت اعتباري در تحقيقاتي كه توسط ديويد كارتر استاد دانشگاه ميشيگان آمريكا صورت پذيرفته است متداولترين جرم كامپيوتري كه در سالهاي اخير گزارش شده كلاهبرداري با كارت اعتباري بود. كلاهبرداري كارتهاي اعتباري به اين علت وسوسه انگيز است كه خدشه زنندگان در زمان بسيار كوتاهي تنها با وصل شدن به اينترنت بدون نياز به مهارت خاصي از كارتهاي اعتباري سوء استفاده مي‌كنند

د: قاچاق مواد مخدر از طريق اينترنت

با توجه به دسترسي آسان افراد به همديگر از طريق اينترنت و ارسال ايميل هرگونه خريد و فروش و پخش مواد مخدر از طريق شبكه‌هاي كامپيوتري انجام مي‌شود. ضريب اطمينان قاچاق كنندگان مواد مخدر از طريق كامپيوتر نسبت به نوع سنتي آن بالاتر مي‌باشد. زيرا پليس به راحتي نمي‌تواند از برنامه‌هاي قاچاق كنندگان مطلع شود و لذا اقدامات پليس در خصوص كشف فروشندگان و خريداران مواد مخدر غير ممكن است.

ه: پولشوئي كامپيوتري

پولشوئي و غارت يكي از جرائم كلاسيك بوده كه داراي سابقه طولاني است كه با پيشرفت تكنولوژي اين جرم از طريق كامپيوتر و اينترنت صورت مي‌پذيرد. نحوة ارتكاب بدين صورت است كه باندهاي بزرگ نامشروع با ارسال ايميل پيشنهاد انجام يك كار تجاري را به شخصي‌ـ مي‌نمايند و بدون اينكه اثر و نشاني از خود بجاي بگذارند پيشنهاد ارسال مبالغي پول به حساب شخصي را كه براي او ايميل فرستاده‌اند مي‌نمايند و در تقاضاي خود نحوة ارسال و سهم هريك از طرفين را بيان نموده و در صورت توافق طرف مقابل (گيرندة ايميل) نوع و نحوة تضمينات لازم را اعلام مي‌كنند و اصولاً در زمان استرداد پول يك عنوان مشروع در تجارت الكترونيك را با منشأ تجاري انتخاب و با هدف خود هماهنگ مي‌نمايند

جرائم كامپيوتري عليه دولتها

- الف: تهديد به گروگان گيری، اخاذي و كشتن مسئولين و يا اعضاي خانوادة آنها يكي از جرائم مدرن كامپيوتري كه معمولاً قاچاق چيان و يا افراد سياسي براي رسيدن به اهداف خود از آنها استفاده مي‌نمايند تهديد مقامات كشور و يا خانوادة آنها به گروگان گرفتن و يا كشتن است. معمولاً جرائمي كه توسط افراد سياسي صورت مي‌گيرد با قاچاق چيان متفاوت است. قاچاق چيان معمولاً از طريق تهديد به گروگان‌گيري و همچنين تهديد به كشتن و اخاذي از مسئولين اقدام مي‌نمايند ولي افراد سياسي از طريق اعلام در اينترنت دولت را تهديد به جنگ مسلحانه و براندازی حكومت مي‌نمايند بدون آنكه اثر و آثاري از خود بجاي بگذارند

ب: جاسوسي كامپيوتري

جاسوسي كامپيوتري به عملي گفته مي‌شود كه شخصي يا گروهي براي دولت يك كشوري اطلاعات مخفيانه از دولت ديگر در ازاي دريافت پول انجام مي‌دهد بعنوان مثال مي‌توان به موارد زير اشاره نمود: در آلمان سازمان اطلاعاتي ك.گ.ب روسيه به شخصي پول داده بود تا اطلاعات مخفيانه ارتش آمريكا را بدست آورد. يا در مورد ديگر مي‌توان به قضيه لوس آلماس دانشمند هسته‌اي اشاره نمود كه اطلاعات بسيار محرمانة هسته‌اي خود را در اختيار دولت چين قرار داده بود

ج: ترور

امروزه برخي اقدامات تروريستي با دسترسي به اطلاعات حفاظت شده صورت مي‌پذيرد. تروريستهاي اطلاعاتي فقط با استفاده از يك كامپيوتر مي‌توانند بصورت غير مجاز وارد سيستم‌هاي كامپيوتري امنيتي شوند مثلاً با تداخل در سيستم ناوبري هوائي باعث سقوط هواپيما شده يا باعث قطع برق سراسري شوند

طبقه بندی جرایم سایبری

یکی از مشکلات برخورد قضایی و پلیسی با جرم های سایبر چگونگی طبقه بندی آن ها است. کشورهای مختلف به علت سنت های حقوقی متفاوت، رویه های مختلفی را به رویکردها فنی، حقوقی در ارتباط با جرم کامپیوتری دنبال کرده اند. از این روی طبقه بندی های متفاوتی نیز ارائه داده اند که بعضی از آن ها عبارتند از :

۱- طبقه بندی OECD

این طبقه بندی در سال ۱۹۸۳پنج دسته اعمال را در حوزه سایبر جرم تلقی کرده است. که به شرح زیر است :

الف- ورود، تغییر، پاک کردن و یا متوقف سازی داده های کامپیوتری که به طور ارادی و با قصد غیرقانونی در مورد وجوه یا هرچیز با ارزش دیگر صورت گرفته باشد.

- ب- ورود، تغییر، پاک کردن و یا متوقف سازی داده های کامپیوتری و یا برنامه های کامپیوتری که به صورت عمدی و با قصد ارتکاب جعل صورت گرفته باشد.
- ج- ورود، تغییر، پاک کردن و یا متوقف سازی داده های کامپیوتری و یا برنامه های کامپیوتری یا هرگونه مداخله دیگر در سیستم های کامپیوتری که به صورت عمدی و با قصد جلوگیری از عملکرد سیستم کامپیوتری و یا ارتباطات صورت گرفته است.
- د- تجاوز به حقوق انحصاری مالک یا برنامه کامپیوتری حفاظت شده با قصد بهره برداری تجاری از آن برنامه ها و ارائه آن به بازار.
- هـ - دستیابی یا شنود در یک سیستم کامپیوتری و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسؤول سیستم مزبور چه با تخطی از تدابیر امنیتی و چه با هدف غیر شرافتمندانه و یا مضر صورت گرفته باشد.
- طبقه بندی OECD به علت تفکیک جرایم و ابهام در ماهیت هر جرم استفاده نشد.

۲- طبقه بندی شورای اروپا

شورای اروپا دو لیست حداقل و اختیاری به شرح زیر برای جرایم کامپیوتری ارایه داد :

الف- لیست حداقل شامل موارد زیر :

- ✓ کلاه برداری کامپیوتری
- ✓ جعل کامپیوتری
- ✓ خسارت به داده ها یا برنامه های کامپیوتری
- ✓ سابوتاژ (خرابکاری) کامپیوتری
- ✓ دستیابی غیرمجاز
- ✓ تکثیر غیرمجاز یک برنامه کامپیوتری حمایت شده
- ✓ تکثیر غیرمجاز

ب- لیست اختیاری شامل موارد زیر :

- ✓ تغییر داده های کامپیوتری یا برنامه های کامپیوتری
- ✓ جاسوسی کامپیوتری
- ✓ استفاده غیرمجاز از کامپیوتر
- ✓ استفاده غیرمجاز از برنامه کامپیوتری حمایت شده