هستی طهماسبی
کارشناس حقوقی

"هکر"ها در دام قانون

جامعه عاری از جرم تابحال وجود نداشته است و پس از این نیز مطمئناً وجود نخواهد داشت.

اما نکته‌ای که نباید فراموش کرد این است که با رشد و تحول در جوامع، جرایم نیز تغییر می‌کنند.

با پیشرفت جوامع، جرایم نیز گسترش می‌یابند. فن‌آوری‌های جدید، فرصت‌های جدیدی برای قانون گریزان پدید می‌آورد و پدید آمدن جرایم مرتبط با رایانه‌ها درست مانند پدید آمدن جرایم مرتبط با هر نوع پیشرفت دیگر بوده است.

ما در زندگی روزمره با انواع جرایم روبرو هستیم و مظاهر جرم، ابعاد زندگی، را تحت تاثیر قرار داده است.

اکثر ما از مجرمان بیزاریم و احساس می‌کنیم که در مقابل وقوع جرایم مختلف بسیار آسیب‌پذیر هستیم. وجود جرایم در خیابان‌های شهر نیز یادآور آسیب‌پذیری ما و در معرض خطر بودن آزادی و حقوق ماست. بطور کلی جرایم گوناگون یک مشکل اساسی در جوامع بشمار می‌رود. این در حالی است که هر روز با توسعه و گسترش جرایم از هر نظر بالاخص نوع جرم روبرو هستیم. و هر روز جرایم جدیدتری کشف شده و به لیست جرایم قبلی افزوده می‌شود.

به عنوان نمونه گسترش وسایل ارتباط جمعی و ابزارهای اطلاع‌رسانی که در سال‌های اخیر به اوج شکوفایی خود رسیده تحولاتی بس عظیم را در روابط انسان‌ها با یکدیگر موجب شده و در نتیجه تسهیل زندگی و رشد آن را در پی داشته است. شکی نیست که این تحولات در امر اطلاعات، تحولاتی در دیگر امور زندگی را نیز در پی داشته و آثار مثبت فراوانی به همراه آورده است.

اما چنانچه با دیدی منصفانه به موضوع بنگریم، قطعاً همه آن تحولات جدید ابعاد و آثار مثبت ندارند. به عبارت دیگر، در کنار محاسن ناشی از تحول مقوله اطلاعات و اطلاع‌رسانی و دگرگونی چشمگیر در عرصه ارتباطات معایب چندی نیز نهفته است که می‌تواند در صورت نادیده گرفته شدن، زیان‌های جبران ناپذیری را بر جامعه بشری وارد آورد.

تخلفات و جرایم رایانه‌ای از جمله این نقاط منفی ابزارهای نوین اطلاع‌رسانی است که علیرغم وضع مقررات و قوانین متعدد برای جلوگیری از وقوع آنها در کشورهای مختلف هنوز موفقیت چندانی حاصل نشده است.

هک و نفوذگری در رایانه‌های شخصی و دولتی نیز تا چند سال پیش همچون گوشه‌های تاریک یک تکنولوژی پیشرفته به شمار می‌آمد که تنها در فیلم‌های سینمایی و داستان‌های مهیج به تصویر کشیده می‌شد. اما اکنون با پیشرفت‌هایی که در زمینه توسعه اینترنت در کشور ما ایجاد شده، آمار جرایمی مانند: نفوذ غیرمجاز و حتی کلاهبرداری و دستکاری در اطلاعات به تدریج رو به افزایش است. این در حالی است که ما تا امروز قانون مصوب و خاصی برای اینگونه جرایم نداشته‌ایم و اکنون پس از گذشت سالها از ورود تکنولوژی کامپیوتر و اینترنت به ایران و همزمان با توجه عامه مردم و دولتمردان به تجهیز فن‌آوری اطلاعات و رونق دادن به فعالیت‌های آی تی (IT) در بخش‌های دولتی توسط نهادهایی چون شورای عالی اطلاع‌رسانی و در قالب طرح‌هایی مانند تکفا، برخورد با جرایم رایانه‌ای مراحل تدوین و تصویب خود را طی می‌کند.

پیش‌نویس این قانون که توسط کمیته مبارزه با جرایم رایانه‌ای قوه قضاییه در ۷۳ ماده تهیه گردیده، به مراحل نهایی خود نزدیک شده و جهت اجرا باید به تصویب مجلس شورای اسلامی برسد.

تا این مرحله این پیش‌نویس بازخوردهای فکری واندیشه‌ای مختلفی را در جامعه ایجاد کرده است. برخی مخالف و برخی موافق و برخی نیز خواستار اصلاح این پیش‌نویس هستند.

اما واقعیت این است که وجود یک قانون برای جرایم اینترنتی لازم است، همانطور که وجود قوانین راهنمایی و رانندگی برای جامعه‌ای که مردمش از اتومبیل استفاده می‌کنند لازم و ضروری است. در تمام کشورهای دنیا هم قوانینی برای جرائم اینترنتی در نظر گرفته شده است، به عنوان مثال: درایالات متحده، انتشار عکس‌های جنسی کودکان ممنوع است و کسانی که از این قانون تخطی کنند، به شدت مجازات می‌شوند. همچنین انتشار ویروس، یا نفوذ به کامپیوتر شخصی دیگران، از دیگر مواردی است که تخطی از آن مجازات سنگینی در پی دارد. این قوانین برای محدود کردن کاربران یا جلوگیری از سلب آزادی اشخاص نیست و می‌تواند راه‌حل‌های مفید و موثری را برای ضابطه مند کردن فعالیت شرکت‌های بخش خصوصی و برخورد قانونمند با جرایمی که در این حوزه اتفاق می‌افتد را پیش رو قرار دهد.

مفهوم جرایم کامپیوتری

مباحث زیادی در بین کارشناسان درباره آنچه تشکیل دهنده جرایم کامپیوتری است و یا جرایم مربوط به کامپیوتر در جریان است. و پس از گذشت سال‌ها هنوز، یک تعریف رسمی بین‌المللی برای این اصطلاحات وجود ندارد. مولفان و کارشناسانی که در پی یافتن تعریفی برای جرایم کامپیوتری هستند، تردیدی در موجودیت این پدیده ندارند، اما تعاریف ارائه شده از سوی آنان در حیطه تخصص مطالعاتی آنها می‌باشد.

طرح مبارزه با جرایم رایانه‌ای با وجود برخی کاستی‌ها، نخستین حرکت در عرصه رایانه‌ای کشور به شمار می‌رود

در کنگره دهم سازمان ملل متحد در مورد پیشگیری از جرم و اعمال مجرمین، جرم کامپیوتری با دو تعریف طبقه‌بندی شده است.

اولین تعریف به نام جرم سایبر در مفهوم جزیی (جرم کامپیوتری) می‌باشد که به شرح زیر است:

"هرگونه رفتار مستقیم غیرقانونی به وسیله عملیات الکترونیکی که امنیت سیستم های کامپیوتری و داده‌های پردازش شده به وسیله آنها را هدف قرار دهد."

دومین تعریف که جرم کامپیوتری در مفهوم کلی (جرم مرتبط با کامپیوتر) نام دارد؛ بدین معناست:

"هرگونه رفتار غیرقانونی که به وسیله یا در ارتباط با یک سیستم یا شبکه کامپیوتری ارتکاب یافته و تملک ارائه یا توزیع غیرقانونی داده‌ها به وسیله یک سیستم یا شبکه کامپیوتری."

راهنمای سازمان ملل نیز جرایم کامپیوتری را اینگونه تعریف کرده است:

"جرایم کامپیوتری می‌تواند شامل فعالیت‌های محرمانه باشد که ماهیتی سنتی دارند از جمله سرقت، کلاهبرداری، جعل و سوء استفاده که همگی به طور معمول در همه جا مشمول ضمانت اجراهای کیفری است و کامپیوتر نیز فرصت‌های تازه‌ای برای سوء استفاده به وجود آورده است که می‌توانند و یا باید جرم انگاری شوند".

همچنین در رهنمود شورای اروپا برای تعریف جرم کامپیوتری نظرات مختلفی با اهداف مطالعاتی و موضوعی مطرح شده و یکی از آنها جرم کامپیوتری را اینگونه تعریف کرده است:

"هر عمل غیرقانونی که کامپیوتر ابزار یا موضوع جرم باشد و به عبارت دیگر هر جرمی که ابزار یا هدف آن تاثیرگذاری بر عملکرد کامپیوتر باشد."

نباید از نظر دور داشت که تعریف جرم کامپیوتری در هر کشور متفاوت است. قانونگذاران فنلاند جرم کامپیوتری را به این ترتیب تعریف کرده‌اند:

"جرمی است که در برگیرنده سیستم‌ها و داده‌ها یا واحدهای نرم‌افزار و سخت‌افزار به عنوان یک هدف و یا یک ابزار یا یک رکن عمل مجرمانه است.

در ایالات متحده تعریف موسعی از جرم کامپیوتری به عمل آمده است به این صورت که: "هر اقدام غیرقانونی که با یک کامپیوتر یا سیستم کامپیوتری یا به کارگیری آن مرتبط باشد را جرم کامپیوتری می‌گویند و هر اقدام عمومی که به هر ترتیب با کامپیوتر مرتبط بوده و موجب ایجاد خسارت به بزه دیده شده و مرتکب از این طریق منافعی را تحصیل کند جرم کامپیوتری است."

وزارت دادگستری آمریکا نیز هر اقدام غیرقانونی که برای ارتکاب، پی جویی یا پیگرد قضایی آن بهره‌برداری از دانش فن‌آوری کامپیوتر ضروری باشد را جرم کامپیوتری دانسته است.

نقش کامپیوترها و شبکه‌های در ارتکاب جرایم:

۱- کامپیوتر و شبکه می‌تواند به عنوان وسیله‌ای برای ارتکاب جرم محسوب شود.

۲- کامپیوتر و شبکه می‌تواند هدف جرم باشد

(بزه دیده).

۳- از کامپیوتر ها و شبکه‌ها می‌توان برای مقاصد مرتبط با جرم استفاده کرد. به عنوان مثال نگهداری سوابق فعالیت‌های قاچاقچیان.

بنابراین جرم کامپیوتری را از دو نظر می‌توان تعریف کرد:

الف: در تعریف مضیق، جرم کامپیوتری اساساً منحصر و محدود به نفوذ غیرمجاز، تحریف یا تخریب از طریق کدهای کامپیوتری، جاسوسی کامپیوتری، جعل و کلاهبرداری کامپیوتری خواهد بود و همچنین آزار و اذیت، سوء استفاده از پست الکترونیک، سرقت و... از طریق سیستم‌های کامپیوتری جرم نخواهد بود.

ب: در تعریف موسع از جرم کامپیوتری، هرفعل و ترک فعلی که از طریق یا به کمک کامپیوتر و یا از طریق شبکه‌های کامپیوتری یا از طریق اینترنت، چه بطور مستقیم یا غیرمستقیم انجام می‌شود که توسط قانون ممنوع گردیده و برای آنها مجازات مالی یا جسمی در نظر گرفته شده است را شامل می‌شود.

قانون فن آوری اطلاعات سال ۲۰۰۰ هندوستان از تعریف مضیق استفاده کرده و فقط نفوذ غیرمجاز، تخریب کامپیوتری و پورنوگرافی در فضای مجازی را به عنوان جرم کامپیوتری محسوب کرده و مطابق این قانون نمی‌توان مرتکبین کلاهبرداری کامپیوتری را تحت تعقیب قرار داد و فقط می‌توان براساس ماده ۴۲۰ قانون جزای هندوستان در خصوص دروغگویی و فریب، شخص مرتکب را مجازات نمود.

قانونگذارانی که از تعریف مضیق پیروی می‌کنند معتقدند که قوانین سنتی پاسخگوی نیازهای قانونی دوران معاصر می‌باشد و برای مبارزه با اشکال جدید جرم نیازی به وضع قوانین جدید و ایجاد تورم کیفری نیست.

ایران نیز جزء آن دسته کشورهایی است که باید تعریفی از جرم کامپیوتری داشته باشد زیرا به اعتقاد بسیاری از حقوق‌دانان ایرانی قوانین دیگر همه شمول جرایم کامپیوتری را در بر نمی‌گیرد.

با توضیحات فوق جرایم کامپیوتری را می‌توان به سه دسته به شرح زیر تقسیم کرد:

دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند مانند سرقت، تخریب و غیره.

در کشورهای مختلف جهان، مجازات‌هایی برای جرایم کامپیوتری در نظر گرفته شده است

دسته دوم: جرایمی هستند که در آنها کامپیوتر به عنوان ابزار و وسیله، توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود.

دسته سوم: جرایمی هستند که می‌توان آنها را جرایم کامپیوتری محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود، مانند دسترسی غیرمجاز به سیستم‌های کامپیوتری.

در حال حاضر تشریح حقوقی جرایم کامپیوتری یا جرایم مرتبط با کامپیوتر ضروری به نظر می‌رسد که در ادامه این نوشتار بررسی می‌شود.

کلاهبرداری کامپیوتری

جرم کلاهبرداری کامپیوتری با بحث ورود دستورالعمل‌های اضافی شروع شد. طبعاً در طول زمان، این جرم راه تکامل خود را پیمود. زیرا در قوانین ناظر بر کلاهبرداری کشورهای گروه سیویل و از جمله ایران، لازم است که شخص، انسان دیگری را بطور مستقیم بفریبد ولی کلاهبرداری کامپیوتری چنین الزام‌هایی را دارا نمی‌باشد. از این رو خلاء تقنینی پیش می‌آید که در برخی کشورها با وضع قانون جرم کلاهبرداری کامپیوتری، خلاء موجود پر شده است.

در جرم کلاهبرداری و دیگر جرایم علیه اموال، مسیر حرکت مجرم متفاوت است. در سرقت، سارق سراغ صاحب مال می‌رود و مال وی را می‌رباید. در کلاهبرداری، اگر چه ظاهراً صاحب مال سراغ مجرم می‌رود، اما در واقع مانور متقلبانه مجرم موجب رجوع صاحب مال به اوست و تسلیم مال به مجرم نیز براساس رضایت مال باخته است. در خیانت در امانت نیز، مجرم مال را به رسم امانت دریافت می‌کند، اما از امانت تخطی می‌کند.

اما در کلاهبرداری کامپیوتری، فرد با اعمال خاص نرم‌افزاری دست به ارتکاب جرم می‌زند.

مجرم بطور مستقیم هیچ کس را نمی‌فریبد، بلکه فریب نسبت است، وی چه دارای سمت باشد(وکیل، نماینده پارلمان و...) یا خیر، بصورت غیرمجاز، به سیستم کامپیوتری دست می‌یابد به هدف خود نائل می‌شود.

هیچ مالی به رسم امانت به وی سپرده نشده است و فقط به واسطه برنامه‌ریزی، سوء استفاده از ورودی.

خروجی و داده‌پردازی و .. به اموال دست می‌یابد.

در حقیقت کلاهبرداری از شکل ساده و سنتی، کلاهبرداری و تقلب در پست و تمبرهای پستی، وجوه رایج، روند شرکت‌سازی کذب، استفاده از شگردهای اقتصادی و تجاری، سوء استفاده از بیمه، سوء استفاده از سیستم بانکداری، کارت‌های اعتباری و اسناد اعتباری هر روز بیشتر پیچیده‌تر می‌شود و بتدریج در جامعه اطلاعاتی و عصر اطلاعات وارد شکل جدید خود می‌شود.

کلاهبرداری کامپیوتری در ابتدا بصورت تقلب در مرحله برنامه نویسی و دادن دستورالعمل‌های اضافی خلاصه می‌شد.

هر جا سیستم کامپیوتری وجود داشته باشد هکرها هم هستند

این دستورالعمل‌ها و برنامه‌های تقلبی، یا مستقیم هدف مالی داشت یا دادن ظاهر واقعی به یک امر کذب بود و همین موجب تسلیم و تسلم ناروای مال می‌شد.

بعدها با پیشرفت برنامه‌نویسی و ارتقای نحوه دستیابی کلاهبرداری کامپیوتری شکل جدیدی به خود گرفت. با بحث آن لاین (on Line) شدن داده‌ها، و در کنار آن بسته‌های نرم‌افزاری، ویروس‌ها، کرم‌ها، بمب‌های زمانی منطقه‌ای و... موجب شد مجرم بتواند هم به سهولت به کدهای محرمانه اشخاص دست یابد و هم بتواند اموال آنان را برباید و به خود اختصاص دهد.

جعل کامپیوتری

جعل مرسوم و کلاسیک ناظر به جعل چیزی است که قابلیت استناد داشته باشد و بتوان آن را ارائه کرد و اثر حقوقی بر آن مترتب باشد. موضوع این جرم ساختن نوشته، سند و هر چیز دیگر برخلاف حقیقت است و ساختن به شکل به وجود آوردن سند و ایجاد نوشته و سند، خراشیدن، تراشیدن، محو، اثبات می‌شود.

اما در محیط دیجیتال، تراشیدن، خراشیدن، محو، اثبات به شکل فیزیکی اصلاً وجود ندارد و به شکل دیجیتال یعنی ورود، تغییر، محو، متوقف سازی داده‌ها و مداخله در داده‌ها (به انضمام ارتباطات راه دور) ارتکاب می‌یابد.

با توجه به تحول کاربرد سند و شکل آن و گسترش تدریجی کاربرد اسناد الکترونیکی و تفاوت این اسناد با سندهای کاغذی از حیث فیزیکی و تشابه از حیث اصول اثباتی و استنادی، با توجه به تحول مصادیق جعل در محیط دیجیتال از شکل مادر و عمده و ظهور مصادیق جدید در کارت اعتباری، بانکداری الکترونیکی، پرداخت الکترونیکی و در نهایت تجارت الکترونیکی، یادآوری این نکته ضروری به نظر می‌رسد که مفهوم سند در قانون مدنی بایستی که اصلاح شود و اسناد دیجیتال نیز اثر قانونی برابر اسناد دیگر (اسناد مرسوم) را دارا شوند.

جاسوسی کامپیوتری

مقررات جاسوسی در قانون تعزیرات و قوانین دیگر فقط ناظر به جاسوسی سیاسی است.

جاسوسی در قوانین و مقررات نیروهای مسلح نیز تنها شامل جاسوسی نظامی می‌باشد و نحوه اطلاع جاسوسی نیز معمولاً سنتی است از قبیل ورود به مکان‌های حاوی اطلاعات سیاسی محرمانه و... . اما جاسوسی کامپیوتری ناظر بر کسب و افشاء اطلاعات و داده‌های سیاسی، نظامی، مالی، اقتصادی، تجاری و صنعتی چه در بخش دولتی و چه در بخش خصوصی است.

به عبارت ساده‌تر جاسوسی مرسوم در طول زمان تکامل یافته و از صرف اطلاعات سیاسی و نظامی فراتر رفته و اطلاعات مهم و محرمانه اقتصادی، صنعتی، مالی و تجاری را شامل شده و نیز پس از استقرار اقتصاد بازار و آزاد هم شامل اطلاعات دولتی و هم غیردولتی شده است.

این در حالی است که مقررات کشور ما هنوز به شکل سنتی و فاقد کارآیی وجود دارد که جوابگوی نیازمندی‌های کشور نیست.

سابوتاژ کامپیوتری

سابوتاژ یا خرابکاری، تخریب اموال دولتی، اخلال در نظم امور، اعمال تخریبی در خطوط نفت و انتقال نیرو و ... به منظور مبارزه و معارضه با نظام سیاسی کشور است.

مقررات سابوتاژ مرسوم در کشور ما به صورت متفرق و از جمله جرایم علیه خطوط نفت، راه آهن، هواپیمایی و... می‌باشد و مصادیق مذکور در مقررات یاد شده ناظر به اهداف فیزیکی است.

در سابوتاژ کامپیوتری، ورود، تغییر، محو، متوقف‌سازی و مداخله در داده‌ها و اطلاعات و سیستم کامپیوتری و مخابراتی ارگان‌های دولتی صورت می‌گیرد تا با اخلال در روند کار آن ارگان، نوعی اخلال در نظام سیاسی کشور پیش آید.

با توجه به نحوه ارتکاب و نیز موضوع جرم سابوتاژ مرسوم متفاوت است و نیازمند مقررات جداگانه و جدید است.

این جرم به صورت کدبندی و در اینترپول، کنوانسیون اروپایی "سایبرکرایم" ذکر شده است.

تخریب کامپیوتری

بررسی جرایم تخریب در قانون مجازات اسلامی حاکی از اتلاف، از بین بردن و نابود کردن اموال منقول و غیرمنقول از جمله اشجار، باغ‌ها، اسناد، املاک و... است.

تخریب کامپیوتری جرمی است که از لحاظ عنصر معنوی و هدف جرم مانند تخریب مرسوم است. اما به دلیل نوع رفتار مرتکب و نحوه ارتکاب و موضوع جرم با تخریب مرسوم تفاوت دارد.

مرتکب تخریب کامپیوتری هیچ فعل فیزیکی در عالم واقع انجام نمی‌دهد بلکه در محیط دیجیتال با ورود، محو، تغییر، اثبات و... داده‌ها یا اطلاعات به دیگری ضرر می‌رساند. داده‌هایی که برای دیگران ارزشمند محسوب می‌شود و ایجاد مسائل یاد شده در آنها موجب ضرر مالی به وی می‌شود.

وجه تمایز تخریب و سابوتاژ

۱- تفاوت در نیت مرتکب: سابوتاژ مبارزه با نظام سیاسی است اما هدف تخریب نابودی اموال دیگری و ایجاد ضرر مالی می‌باشد.

۲- تفاوت در موضوع جرم: در سابوتاژ، ارگان‌ها، نهادها و وزارت‌خانه‌های دولتی هدف قرار می‌گیرند. و در حالی که در تخریب داده‌های شخصی دیگران مورد هدف واقع می‌شوند.

دستیابی غیرمجاز

دستیابی غیرمجاز جزء جرایم صرفاً کامپیوتری و جدید است و ماهیت و طبعی صرفاً فنی دارد.

در اکثر کشورها همگام با دکترین‌های حقوق کیفری اطلاعاتی، کنوانسیون اروپایی سایبرکرایم، دستورالعمل کدبندی جرایم کامپیوتری اینترپول، توصیه‌نامه AIDP ، انجمن بین‌المللی حقوق جزاء، توصیه‌نامه OECD ، جرم مستقلی تحت این عنوان تصویب و در مقررات جزایی گنجانده شده است.

این جرم، جرم صرف دستیابی است و با مفاهیم مجرمانه دیگر یعنی نفوذیابی، شنود، افشاء که همه از جرایم ناقض حمایت از داده‌ها می‌باشند، تفاوت دارد.

این جرم می‌تواند به عنوان جزیی از عنصر مادی جرایم مهمتر به کار رود. آنگاه تنها جرمی مستقل نخواهد بود بلکه جزیی از جرم مهمتر می‌باشد. و به دلیل ماهیت و طبع ساده این جرم، جرم مادر و عمده محسوب می‌شود.

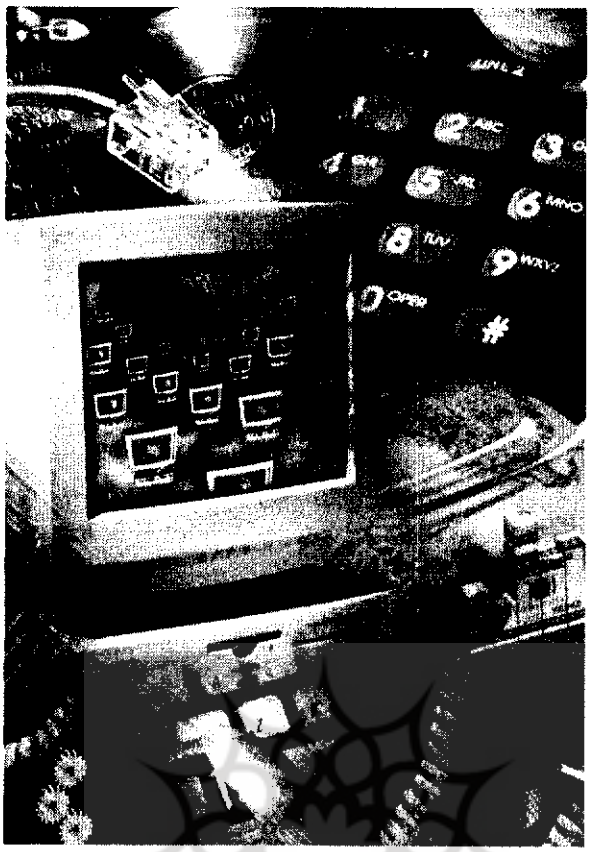
شنود غیرقانونی

شنود غیرقانونی از جمله جرایم مهم کامپیوتری است که به دلیل اهمیت آن در کنوانسیون اروپایی سایبرکرایم، توصیه‌نامه AIDP ، توصیه‌نامه OECD ، کد جرایم اینترپول و... ذکر شده است.

شنود معادل Interception پدیده‌های الکترونیکی است که با استراق سمع تفاوت دارد و استراق سمع به صورت شنیداری و در مخابرات (مکالمات تلفنی) صورت می‌گیرد. اما شنود کامپیوتری به صورت دسترسی به داده‌ها و توقف انتقال داده‌ها صورت می‌گیرد که خاص محیط سایبر است.

هک

در تصور عمومی مردم و جوامع هک یا نفوذگری همان از میان رفتن یک وب سایت و اطلاعات موجود در آن است.



رضا پرویزی دبیر کمیته مبارزه با جرایم اینترنتی در این باره معتقد است: دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای یا همان haking از نظر مفهومی و مصداقی کاملاً از تخریب و ایجاد اختلال در داده‌ها و سیستم‌ها جدا است. اما به خاطر اینکه

در کنگره دهم سازمان ملل دو تعریف از جرایم کامپیوتری ارائه شده است

این دو جرم اغلب همزمان یا توام با هم ارتکاب می‌یابند و بیشتر موارد تخریب و ایجاد اختلال مستلزم دسترسی غیرمجاز به داده‌ها و سیستم‌ها است مردم عادی آن دو را یکی تلقی می‌کنند.

هکرها خود دو نوع هستند:

۱. هکرها

۲. کرکرها

که با یکدیگر متفاوت هستند.

هکرها

کارهایی که هکرها انجام می‌دهند معمولاً از روی بدخواهی نیست. انگیزه بیشتر هکرها برای این کار، تمایل شدید به یادگیری نحوه کار سیستم رایانه، یافتن راهی برای ورود مخفیانه به آنها و پیدا کردن سوراخ‌های امنیتی این سیستم‌ها است.

در دهه ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر باشد.

بعدها در دهه ۱۹۸۰ این واژه به معنی شخصی بود که در "نفوذ" به سیستم های جدید به صورت ناشناس تبحر داشته باشد.

اما امروزه این واژه مفهوم یک جرم را می‌رساند.

کرکرها

کرکرها، هکرهایی بدخواه هستند. آنها به سیستم ها رخنه می کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایل ها را پاک کنند یا بعضی انواع دیگر ویرانی را بار آورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت و اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.

برخی معتقدند کشورهایی که مهد کامپیوتر و اینترنت هستند باید بیشتر باموضوع هک و نفوذگری درگیر باشند و به عکس عده‌ای دیگر معتقدند که این یک ادعا بیش نیست. چون هیچ آمار رسمی‌ای این موضوع را تاکید نمی‌کند

چنانکه پرویزی عنوان می‌کند: "در هر جا که سیستم یا شبکه رایانه‌ای وجود داشته باشد، هکرها نیز وجود خواهند داشت. شاید فقدان قوانین جزایی مرتبط با این جرایم و فقدان سیاست جزایی مناسب در یک جامعه و عدم توجه به اهمیت و امنیت سیستم‌ها و شبکه‌های رایانه‌ای و نادیده گرفتن اقدامات پیشگیرانه زمینه‌ساز رشد هکرها باشد.

نفوذگری به معنای خاص و قانونی آن ذاتاً با جرایمی مثل ورود غیرمجاز و ورود به عنف اماکن سنخیت بیشتری دارد."