جرایم سایبری

لحن یا سبک این مقاله بازتاب‌دهندهٔ لحن دانشنامه‌ای استفاده‌شده در ویکی‌پدیا نیست.

بیشتر بدانید

این مقاله نیازمند ویکی‌سازی است. لطفاً با توجه به راهنمای ویرایش و شیوه‌نامه، محتوای آن را بهبود بخشید.

بیشتر بدانید

جرائم سایبری گونه‌ای از جرائم اینترنتی و شامل جرم‌هایی است که در محیط سایبری رخ می‌دهد. محیط سایبری محیطی مجازی است که کاربران آن می‌توانند به هرگونه خدمات و اطلاعات الکترونیکی در سراسر دنیا دستیابی پیدا کنند. مجرمین محیط سایبری شامل هکرها، کرکرها، فریک‌های تلفن بوده و انواع جرم‌های ممکن در این فضا، سایبرکرایم و تروریسم سایبر خوانده می‌شوند. سایبرتروریسم مانند تروریست‌های معمولی ممکن است دارای انگیزه‌های سیاسی برای ارتکاب جرائم باشند. بحران‌سازهای سایبر شامل ویروس‌ها، عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیسی، کرم‌ها و بمب‌های منطقی است. پلیس سایبر براساس نوع جرم‌های سایبری، نیاز به آموزش‌های خاص دارد.[۱]

تاریخچهٔ جرائم سایبر

دراواسط دههٔ ۹۰با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرائم رایانه‌ای، تحت عنوان جرائم سایبری (مجازی) یا جرائم در محیط سایبری شکل گرفته‌است. به این ترتیب جرائم اینترنتی را می‌توان مکمل جرائم رایانه‌ای دانست، بخصوص اینکه جرائم نسل سوم رایانه‌ای که به جرائم در محیط مجازی معروف است، بیشتر از طریق این شبکه جهانی به وقوع می‌پیوندد.[۲]

ویژگی‌های فضای سایبری

کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون درنظرگرفتن اینکه این اطلاعات و خدمات در کدام نقطهٔ دنیا واقع شده‌است. محیط سایبری زمینهٔ فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیهٔ معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده‌است. محدودهٔ فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و در یک سطح کم هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد.[۳]

از بعد اقتصادی فضای سایبری را می‌توان یک بازار واحد جهانی دانست که از ثمره‌های موفق جامعه مبتنی بر فناوری مدرن اطلاعاتی است که با روند توسعه آن روابط اجتماعی سنتی و فرهنگی حاکم بر روابط افراد را در سطح ملی دچار تحول نماید.

تعریف محیط سایبر

از لحاظ لغوی در فرهنگ‌های مختلف سایبر به معنی مجازی و غیرملموس است، محیطی است مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مانند اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هرآنچه در کرهٔ خاکی به صورت فیزیکی ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) دریک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران هستند و از طریق رایانه، اجزا آن و شبکه‌های بین‌المللی بهم مرتبط هستند.

جرائم در سایبر اسپیس

طبیعت این جرائم و سوءاستفاده‌های مرتکب شده در این دنیای مجازی تازه هیچ‌گاه در دنیای حقیقی دیده نشده‌است. امنیت نا کافی فناوری همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران‌کننده‌ترین جنبهٔ فضای سایبری انتشار سریع اطلاعات در آن است، برای نمونه در لحظهٔ کوتاهی بخشی از اطلاعاتی که می‌تواند به‌طور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود. در فضای سایبری برای جستجو و پیدا کردن این جرائم مشکلات پیچیده‌تر می‌شود. در دنیای واقعی دزدی از بانک کاملاً مشخص است چرا که پس از سرقت در خزانه بانک پولی موجود نیست؛ ولی در فناوری رایانه‌ای شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

برای نمونه سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان‌طور که دقیقاً بوده باقی بگذارد. در فضای سایبری کپی عیناً عین اصل است با کمی کار روی سامانه، سارق می‌تواند امکان هرگونه تعقیب و بررسی مانند پاک کردن اثر انگشت تغییر دهد.

مجرمین سایبر

- هکر: دردهٔ ۱۹۷۰ واژهٔ هکر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر و باهوش باشد. بعدها دردهٔ ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سامانه‌های نو به صورت ناشناس تبحر داشته باشد. امروزه بیشتر با هدف

ترساندن هکرها، رسانه‌ها و مقامات مسئول مانند آژانس‌های دولتی وادارات پلیس، این واژه به هر شخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند. این درست است که هکرهای کنجکاو می‌توانند سهواً باعث زیان‌های چشمگیری شوند، اما جستجو برای یافتن اطلاعات و آموزش، نه انتقام‌گیری یا صدمه زدن به دیگران، عاملی است که باعث می‌شود اکثر هکرها سرگرمی خود را به نحوی بیرحمانه دنبال کنند.

- کراکرها: ازسوی دیگر کرکرها هکرهای بدخواهی هستند. آن‌ها به سامانه‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایل‌ها را پاک کنند یا بعضی گونه‌های دیگر ویرانی را به‌بارآورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها است.
  - تفاوت هکرها و کرکرها: هکرها دریک مورد مهم با کرکرها تفاوت دارند، کارهایی که آن‌ها انجام می‌دهند معمولاً از روی بدخواهی نیست. انگیزه بیشتر هکرها برای این کار، تمایل شدید به یادگیری نحوه کار سامانه رایانه، یافتن راهی برای ورود مخفیانه به آن‌ها و پیدا کردن سوراخ‌های امنیتی این سامانه‌ها است هیجان خواندن اطلاعاتی که می‌دانند اجازه دیدن آنهارا ندارند یا انجام کاری که می‌دانند قانونی نیست به لذت دست زدن به چنین تجاربی توسط هکرها به عنوان سرگرمی می‌افزاید. آن‌ها در فعالیت‌های خود معتقد به نگرش ببین اما دست نزن هستند.

- فریک‌های تلفن: شکل دیگر از جرائم رایانه‌ای رأفریک‌های تلفن " مرتکب می‌شوند. فریک‌ها به جای دسترسی به سامانه‌های رایانه‌ای، از طریق خطوط تلفن در دنیای سایبر گشت می‌زنند. فریک‌ها از میان نخستین هکرها دردهه۱۹۷۰ پدید آمدند. یکی از حوادثی که توسط فریک‌ها به وجود آمده بود در سال ۱۹۷۷ مربوط به اداره پلیس شهر نیویورک می‌شد، فریک‌ها به سامانه تلفن این اداره نفوذ کرده بودند و متن ضبط شده‌ای را که به تماس گیرندگان خوشامد می‌گفت تغییر داده بودند، در متن ضبط شدهٔ جدید گفته می‌شد که افسران پلیس مشغول خوردن نان شیرینی و نوشیدن قهوه هستند و فرصت پاسخ دادن به تلفن‌ها را ندارند، این پیام به تماس گیرندگان توجه می‌کرد که در موارد اورژانس با شماره ۱۱۹ تماس بگیرند.

بحران سازهای سایبر

- ویروس: ویروس‌ها یا برنامه‌های خود همانندساز، برنامه‌هایی هستندکه با هدف آلوده کردن سامانه‌های دیگر نوشته می‌شوند و معمولاً از طریق یک دیسکت و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند. بعضی ویروس‌ها ممکن است قادر به حمله به فایل‌های سامانه و ذوب کردن مادربورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت و ازکارانداختن رایانه باشند.

- عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیس:که می‌توانند دسک سخت یک رایانه را ذوب کنند.

- کرم‌ها:می‌توانند به یک سامانه دسترسی پیدا کنندااما نمی‌توانند در خارج از شبکه، برای نمونه از طریق یک دیسکت، گسترش پیدا کنند. کرم‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه رایانه کند شود یا از کار بیفتد.

- بمب‌های منطقی:آن‌ها تعمداً زیانبار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند. آن‌ها طوری طراحی شده‌اند که طی یک دورهٔ زمانی دررایانه غیرفعال باقی می‌مانند و سپس با سررسیدن تاریخی که برنامهٔ آن‌ها مشخص شده‌است منفجر می‌شوند. اهداف این بمب‌ها متفاوت است.

گونه‌های جرائم سایبری

گوناگونی جرائم ارتکابی در سایبرسپیس شامل جرائم نسل یکم رایانه‌ای (البته به شکل نوین) و تعدادی جرائم بسیار نو و بی‌سابقه است.

- جرائم سنتی درمحیط دیجیتال
  - جاسوسی رایانه‌ای :جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشا و انتقال و استفاده از اسرار است، فرد مرتکب جرم با دستیابی وفاش کردن این اسرار، ضرر سیاسی، نظامی، مالی، تجاری می‌کند. این جرم امنیت ملی را با مخاطره مواجه می‌کند.
  - سابوتاژ رایانه‌ای :این جرم با جرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی واقتصادی یک کشور و بالطبع اخلال در امر حکومت است. در واقع اصلاح، موقوف سازی، پاک کردن غیرمجاز داده‌ها یا عملیات رایانه به منظور مختل ساختن عملکرد عادی سامانه سابوتاژ رایانه‌ای گویند.
  - جعل رایانه‌ای: واردکردن، تغییر، محو یا موقوف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای به منظور و اهداف سیاسی واقتصادی صورت می‌گیرد. جعل رایانه‌ای جعل داده‌ها است. در جعل رایانه‌ای عمل ارتکابی بر داده‌ها اثر می‌گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.
  - افترا و نشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین و گسترده‌ترین سرویس شبکه‌های رایانه‌ای و بین المللی است، هر کاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی در آن تقلب کرد. این قالبیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعات برای تهیه‌کننده کاملاً مشکل است و در عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی و گسترده امنیتی مشکل بوده و تنها برای بخش کوچکی از داده‌ها میسر است.
  - تطهیر نامشروع پول: بدست آوردن پول از طریق غیرقانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرائم کلاسیک بوده که در محیط سایبری به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد، شیوه ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ گونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را می‌نمایند و در تقاضای خود شیوه ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف نوع و شیوه تنظیمات لازم را اعلام می‌دارند و اصولاً در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب وبا هدف خود هماهنگ می‌نمایند لازم است ذکر شود بیشتراین درخواستها از افراد کشورهایی که از لحاظ فناوری اطلاعاتی و ارتباطی و هماهنگی پلیسی در سطح بین‌المللی در درجهٔ پایین‌تری قراردارند انتخاب می‌شود.
  - قاچاق موادمخدر: با توجه به گسترش ارتباطات شبکه‌ای و در محیط سایبری و دسترسی آسان افراد به هم از طریق پست الکترونیک و اینترنت هرگونه قاچاق مواد مخدر اعم از خرید، فروش، پخش، توزیع یافتن واسطه‌ها و مصرف‌کنندگان از طریق شبکه‌های رایانه‌ای انجام می‌شود. از ویژگی‌های آن حذف و کمتر نمودن واسطه‌ها وتوزیع کنندگان، گسترش دامنهٔ فعالیت قاچاق چیان تا سطح بین‌المللی، اقدامات پلیس در خصوص کشف فروشندگان و خریداران موادمخدر به سختی و در مواردی غیرممکن است و ضریب اطمینان قاچاق موادمخدر از طریق ارتباطات رایانه‌ای و شبکه‌ای بالاتر از نوع سنتی آن است.

- جرائم ناظر به کپی رایت وبرنامه‌ها: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش واستفادهٔ غیرمجاز از برنامه‌های رایانه‌ای سرقت نرم‌افزار گویند.

- جرائم در تجارت الکترونیک: شامل کلاهبرداری در تجارت، تعریف کلی و کلاسیک کلاهبرداری عبارت تست از"تحصیل مال دیگری بااستفاده از وسایل متقلبانه"شخصی در نقطه‌ای نامعلوم با واردشدن به شبکهٔ بین‌المللی (مانند اینترنت)و معرفی خود به عنوان تاجر و صاحب یک شرکت معتبر در یک سایت تجاری و ارائهٔ "نهادی مشابه ادارهٔ ثبت اسناد که این نهاد عهده‌دار ثبت داده‌های تجاری وتجاراست تا بدین ترتیب تاجر مجوز ورود به عرصهٔ تبادلات الکترونیک را کسب نماید "وهم چنین نهادی که در تجارت الکترونیک به معنای زیرساخت کلید عمومی است. اساس تجارت الکترونیک و از محورهای عمده و مهم آن داشتن این نهاد برای تجار است "(تماماً غیرواقع و کذب)، اظهار می‌دارد که کالایی را با قیمت معین، نوع و تعداد مشخص در اختیار داشته و قابل عرضه به مشتریان است از طرفی خریدارانی که در فضای شبکه‌ها مشغول تجارت الکترونیک (خریدوفروش) هستند پس از دریافت پیام، نسبت به برقراری ارتباط شبکه‌ای (که بیشتر به صورت پست الکترونیک یا ارسال درخواست هز طریق شبکه است قبول (خرید) خودرا اعلام و مقداری از کالای موردنظر را درخواست می‌کنند. شخص فروشنده پس از جلب اعتماد طرف مقابل، نسبت به اعلام شماره حساب یا شماره کارت اعتباری خود برای دریافت وجه اقدام می‌نماید. خریدار نیز پس از پرداخت وجه (بیشتر به صورت پرداختهای الکترونیکی)منتظر دریافت کالا است در صورتی‌که شخص فروشنده قبلاً با عملیات‌های متقلبانه و نفوذ توانسته بوده که نهادهای نامبرده را به صورت غیرواقع برای خود اختیار نماید و بدین وسیله مبلغی را من غیرحق کسب نماید.

- جرم آینده، تروریسم سایبر: والتر لاکور یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌المللی اشاره می‌کند که یک مقام رسمی سیا ادعا کرده‌است که می‌تواند "با یک میلیارد دلار و ۲۰ هکر قابل، ایالت متحده را فلج کند."لاکور یادآوری می‌کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی، گروگان‌گیری یا بعضاً حمله ناگهانی به تسهیلات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیلهٔ حمله الکترونیکی به شبکه‌های رایانه‌ای وارد آید می‌تواند"بسیار غم انگیزتر باشد و اثرات آن تا مدت‌ها باقی بماند."لاکور معتقد است که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران‌کننده تر از جنگ‌های بیولوژیک یا شیمیایی باشد. از اقدامات سایبر ترور ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از ویژگی‌های این نوع ارتباط عدم توانایی پلیس در کنترل و شنود این ارتباطات است. اما آیا واقعاً تروریسم سایبر امکان‌پذیر است؟ در سال ۱۹۹۱میلادی حین جنگ خلیج فارس که میان عراق و ائتلافی از چند کشور به رهبری ایالت متحده درگرفت، یک جوان ۱۸ ساله فلسطینی، متهم به نفوذ به رایانه‌های پنتاگون شد. این مرد جوان ظاهراً به اطلاعات سری مربوط به موشک پیتریوت دسترسی پیدا کرده بود که یک سلاح کلیدی آمریکا برای دفاع در مقابل حمله موشک‌های اسکاد عراق محسوب می‌شد. در نفوذ دیگری در همان جنگ چندین نوجوان هلندی به رایانه‌های نظامی، زمینی، هوایی و دریایی ایالت متحده در۳۴ سایت مختلف نفوذ کردند، نفوذکنندگان در یکی از حملات خود به داده‌های بسیار حساسی دربارهٔ پرسنل نظامی، نوع و میزان تجهیزات نظامی فرستاده شده به خلیج فارس، اهداف موشک‌ها و توسعهٔ سامانه‌های تسلیحاتی دست یافتند، در واقع این نوجوانان کرکرهایی بودند که تنها به خواندن این فایل‌ها اکتفا نکردند بلکه اطلاعات مربوط به تحرکات ارتش و توانایی موشک‌ها را سرقت کردند و در اختیار عراقی‌ها قراردادند.

بعضی از افسران پلیس از دهه۱۹۷۰ در زمینه جرائم سایبر آموزش دیده‌اند و تخصص پیدا کرده‌اند. جرائم سایبر ممکن است در هر جایی اتفاق بیفتند و بیشتر آنها قابل ردیابی نیستند. بیشتر ادارات پلیس محلی فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرائم سایبر هستند به ویژه به این دلیل که این پرونده‌ها ممکن است در آن واحد به حوزه‌های قضایی متعددی مربوط شوند؛ بنابراین چه کسی مسئول مبارزه با جرائم سایبر خواهد بود؟ علاوه برآنچه پلیس رایانه‌ای نامیده می‌شود،

شهروندانی نیز وجود دارند که به صورت شخصی به جلوگیری از جرائم سایبر و شناسایی مجرمان کمک می‌کند. هنوز هم مباحثات زیادی در مورد روش‌های مورد استفاده توسط مقامات رسمی، دراجرای قوانین مبارزه با جرائم سایبر وجود دارد. پلیس تا چه حد مجاز است که در تحت پیگرد قراردادن و دستگیری مجرمان سایبر به ویژه هکرها پیش رود؟ پلیس تا چه حد اجازه دارد که به حریم خصوصی الکترونیک شهروندان پا بگذارد؟ چگونه باید میان حقوق افراد و نیاز مقامات دولتی برای تحقیقات و تشکیل پرونده تعادل برقرار کرد؟ ولی با این وجود پلیس توانسته بسیاری از هکرهای بدخواه را شناسایی کند و در یافتن مجرمان سایبر موفق باشد.

امنیت سایبر

با وجود تبادل عظیم اطلاعات حیاتی ویا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس، مطمئن است؛ و امنیت شبکه‌ها وقتی داده‌ها در آن جریان پیدا می‌کنند چگونه است؟ چرا که با وجود جریان داده‌ها روی اینترنت بسیار طبیعی است که فکر کنیم گوش دادن و گرفتن اطلاعات حساس موجود می‌تواند کار ساده‌ای باشد. اما رمزگذاری روی داده‌ها (غیرقابل فهم یا غیرقابل خواندن داده‌ها) لایه سوکت‌های امن به عنوان استاندارد ایمنی ورمز عبور معتبر، جداسازی داده‌ها روی رایانههای متعدد و تفکیک پایگاه داده‌ها (جدا نگه داشتن اطلاعات مشتریان) روش‌های پیشرفته در ایمنی داده‌ها هستند؛ که می‌توانند از دستیابی هکرها به داده‌ها جلوگیری کنند.

تاریخچهٔ جرائم سایبر در ایران

براساس اطلاعات موجود نخستین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی رایانه در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم رایانه‌ای و جرم اینترنتی وجود ندارد، عمل آن‌ها به عنوان جرم اینترنتی محسوب می‌شود.

پس از این بود که گروه‌های هکر موسوم به گروه مش قاسم و ...، جرم‌های دیگری را مرتکب می‌شدند، مواردی چون جعل اسکناس، اسناد و بلیط‌های شرکت‌های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرائم اینترنتی هستند.

براساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرائم اینترنتی در کشور تشکیل شد که کشف جرائم آمار ۵۰ درصدی را نشان می‌دهد.

به طور کلی جرایم سایبری در ایران دامنه گسترده ای را در بر میگیرد. برخی از این جرایم به شرح زیر اند:

- دسترسی و شنود غیر مجاز (گذرواژه یا هر داده‌ی خصوصی دیگری که مربوط به شخص حقیقی یا حقوقی باشد)
- انتشار مطالب و محتوای مبتذل و مستهجن
- جاسوسی رایانه‌ای
- جرایم علیه صحت داده‌ها و سیستم‌های رایانه‌ای از جمله تخریب، جعل و اخلال در سیستم‌های رایانه‌ای و مخابراتی و کلاهبرداری در فضای سایبری (که در این صورت نیاز به وجود یک وکیل کلاهبرداری دیده می‌شود)

- جرم در عفت و اخلاق عمومی
- نشر اکاذیب و داده‌های ناصحیح
- انتشار و در دسترس قرار دادن معاملات فروش و انتشار آن‌ها
- انتشار و پخش آموزه‌های نادرست در فضای سایبری
- هک، فیشینگ و بدافزارها و گسترش ویروس‌های سایبری

از مهم‌ترین موارد جرم اینترنتی و رایانه‌ای در سال گذشته، ۳۲ مورد سوء استفاده از کارت‌های اعتباری ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده‌است.

باتوجه به آمارهای سال ۸۴ میزان کشفیات مربوط به کلاهبرداری، جعل و دیگر جرائم رایانه‌ای و اینترنتی ۱۱ درصد رشد را نشان می‌دهد.

می‌توان گفت امسال هم جرائم رایانه‌ای و اینترنتی در کشورمان اتفاق افتاده که شاید یکی از مهم‌ترین و خبرسازترین آنها، توزیع سی دی مستهجن منسوب به یکی از بازیگران مشهور زن بود و از مصادیق بارز جرم رایانه‌ای است.

پلیس سایبری در ایران

توسعهٔ روزافزون زیرساخت‌های فناوری اطّلاعات و ارتباطات در کشور و افزایش کاربران و استفاده کنندگان از اینترنت و دیگر فناوری‌های اطّلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلّی، ارتباطات ماهواره‌ای از جملهٔ دلایلی است که لزوم ایجاد و توسعهٔ سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطّلاعات جمهوری اسلامی ایران را توجیه می‌کند. همچنین توسعهٔ خدمات الکترونیک در کشور نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و دیگر خدمات از این دست، نیز لزوم ایجاد پلیسی تخصّصی در مجموعهٔ نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرائمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند. از سوی دیگر، رشد قارچ‌گونه جرائم در حوزهٔ فضای تولید و تبادل اطّلاعات کشور (فتا) مانند کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطّلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرائم اخلاقی و برخی جرائم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصّصی که توان پی‌جویی و رسیدگی به جرائم سطح بالای فنّاورانه داشته باشد، به وجود آید. از سوی دیگر با توجّه به تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوّبات کمیسیون افتای دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطّلاعات، این پلیس در بهمن‌ماه سال ۱۳۸۹ به دستور سردار فرماندهی محترم نیروی انتظامی جمهوری اسلامی ایران، تشکیل گردید.

قوانین جرائم سایبری در ایران

قانون جرائم رایانه‌ای

بخش یکم

جرائم و مجازاتها

فصل یکم

جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

- مبحث یکم ـ دسترسی غیرمجاز

ماده۱ـ هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت‌شده‌است دسترسی یابد، به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهدشد.

- مبحث دوم ـ شنود غیرمجاز

ماده۲ـ هر کس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به زندان از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

- مبحث سوم ـ جاسوسی رایانه‌ای

ماده۳ـ هر کس به‌طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهدشد:

الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به زندان از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات.

ب) در دسترس قراردادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به زندان از دو تا ده سال.

ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به زندان از پنج تا پانزده سال.

تبصره۱ـ داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره۲ـ آئین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آن‌ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت وزیران خواهدرسید.

ماده۴ـ هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به زندان از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۵ـ چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوط هستند و به آن‌ها آموزش لازم داده شده‌است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرار گرفته‌است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند، به زندان از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهندشد.

فصل دوم

جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

- مبحث یکم ـ جعل رایانه‌ای

ماده۶ ـ هر کس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به زندان از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهدشد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آنها.

ب) تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آنها.

ماده۷ـ هرکس با علم به مجعول بودن داده‌ها یا کارت‌ها یا تراشه‌ها از آن‌ها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهدشد.

- مبحث دوم ـ تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی

ماده۸ ـ هرکس به‌طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به زندان از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۹ـ هر کس به‌طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آن‌ها را مختل کند، به زندان از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۱۰ـ هرکس به‌طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذر واژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۱ـ هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، از قبیل خدمات درمانی، آب،

برق، گاز، مخابرات، ترابری و بانکداری مرتکب شود، به زندان از سه تا ده سال محکوم خواهدشد.

فصل سوم

سرقت و کلاهبرداری مرتبط با رایانه

ماده۱۲ـ هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون ریال تا بیست میلیون ریال و در غیر این صورت به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۳ـ هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به زندان از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم

جرائم علیه عفت و اخلاق عمومی

ماده۱۴ـ هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به زندان از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره۱ـ ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به دستکم یکی از مجازات‌های فوق می‌شود. محتویات و آثار مبتذل به آثاری اطلاق می‌گردد که دارای صحنه و صور قبیحه باشد.

تبصره۲ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون ریال تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.

تبصره۳ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفه خود قرار داده باشد یا به‌طور سازمان یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره۴ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده۱۵ـ هرکس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن، آن‌ها را تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آن‌ها را تسهیل نموده یا آموزش دهد، به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد. ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون ریال تا پنج میلیون ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آن‌ها را تسهیل کند یا آموزش دهد، به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم می‌شود. تبصره ـ مفاد این ماده و ماده (۱۴) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.

فصل پنجم

هتک حیثیت و نشر اکاذیب

ماده۱۶ـ هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به زندان از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده۱۷ـ هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به زندان از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

ماده۱۸ـ هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی به‌طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یادشده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان)، به زندان از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهدشد.

فصل ششم

مسؤولیت کیفری اشخاص

ماده۱۹ـ در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهدبود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

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

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

د) هرگاه تمام یا بخشی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته‌باشد.

تبصره۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره۲ـ مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهدبود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهدبود.

ماده۲۰ـ اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات زندان آن جرم تا پنج سال زندان باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات زندان آن جرم بیش از پنج سال زندان باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت.

ماده۲۱ـ ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده‌است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبه دوم به جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره۱ـ چنانچه محتوای مجرمانه به تارنماهای (وب سایتهای) مؤسسات عمومی شامل نهادهای زیر نظر ولی‌فقیه و قوای سه‌گانه مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب ۱۹/۴/۱۳۷۳ و الحاقات بعدی آن یا به احزاب، جمعیتها، انجمن‌های سیاسی و صنفی و انجمن‌های اسلامی یا اقلیتهای دینی شناخته‌شده یا به دیگر اشخاص حقیقی یا حقوقی حاضر در ایران که امکان احراز هویت و ارتباط با آن‌ها وجود دارد تعلق داشته باشد، با دستور مقام قضائی رسیدگی‌کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، تارنما (وب سایت) مزبور تا صدور حکم نهایی پالایش (فیلتر) نخواهد شد.

تبصره۲ـ پالایش (فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضائی رسیدگی‌کننده به پرونده انجام خواهد گرفت. برای اطلاع از مصادیق محتوای مجرمانه اینجا کلیک کنید.

ماده۲۲ـ قوه قضاییه موظف است ظرف یک ماه از تاریخ تصویب این قانون کارگروه (کمیته) تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نماینده وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه (کمیته) را تشکیل خواهند داد. ریاست کارگروه (کمیته) به عهده دادستان کل کشور خواهد بود.

تبصره۱ جلسات کارگروه (کمیته) دستکم هر پانزده روز یک بار و با حضور هفت نفر عضو رسمیت می‌یابد و تصمیمات کارگروه (کمیته) با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره۲ـ کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آن‌ها تصمیم‌گیری کند.

تبصره۳ـ کارگروه (کمیته) موظف است هر شش ماه گزارشی در خصوص روند پالایش (فیلتر) محتوای مجرمانه را به رؤسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند.

ماده۲۳ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در ماده فوق یا مقام قضائی رسیدگی‌کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامه دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کارگروه (کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبه دوم به یکصد میلیون ریال تا یک میلیارد ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهندشد. تبصره ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه (کمیته) تعیین مصادیق اطلاع دهند.

ماده۲۴ـ هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به زندان از یک تا سه سال یا جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم

دیگر جرائم

ماده۲۵ـ هر شخصی که مرتکب اعمال زیر شود، به زندان از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهدشد:

الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود.

ب) فروش یا انتشار یا در دسترس قراردادن گذر واژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند.

ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی. تبصره ـ چنانچه مرتکب، اعمال یادشده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

فصل هشتم

تشدید مجازاتها

ماده۲۶ـ در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها یا شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی‌فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند یا دارندگان پایه قضائی و به‌طور کلی اعضاء و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه‌دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

ه(جرم در سطح گسترده‌ای ارتکاب یافته باشد.

ماده۲۷ـ در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات زندان آن جرم نودویک روز تا دو سال زندان باشد، محرومیت از یک ماه تا یک سال.

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

ج) چنانچه مجازات زندان آن جرم بیش از پنج سال زندان باشد، محرومیت از سه تا پنج سال.

بخش دوم

آئین دادرسی

فصل یکم

صلاحیت

ماده۲۸ـ علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته‌است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنماهای (وب‌سایتهای) دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایتهای) مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای (وب‌سایتهای) دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد.

ماده۲۹ـ چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده۳۰ـ قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد. تبصره ـ قضات دادسراها و دادگاه‌های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد.

ماده۳۱ ـ در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آئین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهدبود.

فصل دوم

گردآوری ادله الکترونیکی

- مبحث یکم ـ نگهداری داده‌ها

ماده۳۲ـ ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را دستکم تا شش ماه پس از ایجاد و اطلاعات کاربران را دستکم تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره۱ـ داده ترافیک هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آن‌ها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره۲ـ اطلاعات کاربر هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی (IP)، شماره تلفن و دیگر مشخصات فردی اوست.

ماده۳۳ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را دستکم تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را دستکم تا پانزده روز نگهداری کنند.

- مبحث دوم ـ حفظ فوری داده‌های رایانه‌ای ذخیره شده

ماده۳۴ـ هرگاه حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضائی می‌تواند دستور حفاظت از آن‌ها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب‌دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی یا دیگر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشاء کنند یا اشخاصی که داده‌های مزبور به آن‌ها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و دیگر اشخاص به زندان از نودویک روز تا شش ماه یا جزای نقدی از پنج‌میلیون ریال تا ده‌میلیون ریال یا هر دو مجازات محکوم خواهند شد.

تبصره۱ـ حفظ داده‌ها به منزله ارائه یا افشاء آن‌ها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.

- مبحث سوم ـ ارائه داده‌ها

ماده۳۵ـ مقام قضائی می‌تواند دستور ارائه داده‌های حفاظت‌شده مذکور در مواد (۳۲)، (۳۳) و (۳۴) فوق را به اشخاص یادشده بدهد تا در اختیار ضابطان قرارگیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (۳۴) این قانون محکوم خواهد شد.

- مبحث چهارم ـ تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

ماده۳۶ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده۳۷ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آن‌ها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه‌ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده۳۸ـ دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجراء صحیح آن کمک می‌کند، از جمله اجراء دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های مورد نظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده۳۹ـ تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف) دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای یا مخابراتی.

ب) دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوحهای فشرده یا کارت‌های حافظه.

ج) دستیابی به داده‌های حذف یا رمزنگاری شده.

ماده۴۰ ـ در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود.

ماده۴۱ ـ در هریک از موارد زیر سامانه‌های رایانه‌ای یا مخابراتی توقیف خواهد شد:

الف) داده‌های ذخیره شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد،

ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت‌افزاری امکان‌پذیر نباشد،

ج) متصرف قانونی سامانه رضایت داده باشد،

د) تصویربرداری (کپی‌برداری) از داده‌ها به لحاظ فنی امکان‌پذیر نباشد،

هـ) تفتیش در محل باعث آسیب داده‌ها شود،

ماده۴۲ ـ توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آن‌ها در ارتکاب جرم با روش‌هایی از تغییر گذرواژه به منظور عدم دسترسی به سامانه، پلمپ سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده۴۳ ـ چنانچه در حین اجراء دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در دیگر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارد ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به سامانه‌های مذکور گسترش داده و داده‌های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده۴۴ـ چنانچه توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی موجب ایراد لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی‌شود ممنوع است.

ماده۴۵ـ در مواردی که اصل داده‌ها توقیف می‌شود، ذی‌نفع حق دارد پس از پرداخت هزینه از آن‌ها کپی دریافت کند، مشروط به این که ارائه داده‌های توقیف‌شده مجرمانه یا منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه‌ای وارد نشود.

ماده۴۶ـ در مواردی که اصل داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت‌افزارها و نرم‌افزارهای مورد نظر و نقش آن‌ها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آن‌ها تعیین تکلیف کند.

ماده۴۷ـ متضرر می‌تواند در مورد عملیات و اقدام‌های مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

- مبحث پنجم ـ شنود محتوای ارتباطات رایانه‌ای

ماده۴۸ـ شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.

فصل سوم

استنادپذیری ادله الکترونیکی

ماده۴۹ـ به منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی گردآوری شده، لازم است مطابق آئین‌نامه مربوط از آن‌ها نگهداری و مراقبت به عمل آید.

ماده۵۰ـ چنانچه داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهد بود.

ماده۵۱ـ کلیه مقررات مندرج در فصل‌های دوم و سوم این بخش، علاوه بر جرائم رایانه‌ای شامل دیگر جرائمی که ادله الکترونیکی در آن‌ها مورد استناد قرار می‌گیرد نیز می‌شود.

بخش سوم

دیگر مقررات

ماده۵۲ ـ در مواردی که سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده‌است، مطابق قوانین جزائی مربوط عمل خواهد شد. تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آئین دادرسی پیش‌بینی نشده‌است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.

ماده۵۳ـ میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیئت وزیران قابل تغییر است.

ماده۵۴ـ آیین‌نامه‌های مربوط به گردآوری و استنادپذیری ادله الکترونیکی ظرف مدت شش ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.

ماده۵۵ـ شماره مواد (۱) تا (۵۴) این قانون به عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرائم رایانه‌ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد.

ماده۵۶ـ قوانین و مقررات مغایر با این قانون ملغی است.

قانون فوق مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی روز سه شنبه مورخ پنجم خردادماه یکهزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ ۲۰/۳/۱۳۸۸ به تأیید شورای نگهبان رسید.

منابع

https://web.archive.org/web/20150207065446/http://www.cyberpolice.ir/page/2431

https://divansalar.org/blog/%D9%88%DA%A9%DB%8C%D9%84-/%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C

1. *cybercrime | Definition, Statistics, & Examples | Britannica" (https://www.britannica.com/topi"* *c/cybercrime). www.britannica.com* *(به انگلیسی). Retrieved 2022-01-10.*
2. *«جرایم سایبری چیست | امنیت سایبری چیست» (/https://techlife.ir/cybercrime)* . تکولایف. ۰۸-۰۵-۲۰۲۰ . *دریافت‌شده در ۱۰-۰۱-۲۰۲۲* .
3. *Warren Buffett: 'Cyber poses real risks to humanity' » (https://finance.yahoo.com/news/warre»* *n-buffett-cyber-attacks-131445079.html). finance.yahoo.com* *(به انگلیسی). دریافت‌شده در ۱۰-۰۱-۲۰۲۲* .
1. برومند باستانی «جرائم رایانه‌ای و اینترنتی» انتشارات بهنامی، تهران، ۱۳۸۳
2. Gina.De.Angelis،Cyber Crimes،Chelsea House Publisher.۲۰۰۰
3. دکتر ابراهیم حسن بیگی «حقوق و امنیت در فضای سایبر» مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران، ۱۳۸۴

آخرین ویرایش ۶ ماه پیش توسط **Lordmsdos** انجام شده