نشریه علمی تخصصی انجمن علمی
دانشجویی فقه و مبانی حقوق اسلامی

میزان

پاییز ۹۷
شماره ۱۲
قیمت: ۵۰۰ تومان

- قوانین جرایم سایبری در ایران
- جرایم علیه اشخاص
- جرایم سازمان‌یافته ارکان شرکت در جرم
- شرایط سازمان تامین اجتماعی برای تقسیط جرائم بیمه‌ای کارفرمایان

جرایم مجازی

فهرست

جرایم سازمان‌یافته ارکان شرکت در جرم ۲

جرایم مجازی ۵

جرایم علیه اشخاص ۱۲

شرایط سازمان تامین اجتماعی برای تقسیط جرائم بیمه‌ای کارفرمایان ۱۵

قوانین جرایم سایبری در ایران ۱۷

میزان

نشریه علمی تخصصی انجمن علمی دانشجویی فقه و مبانی حقوق اسلامی - پاییز ۹۷ - شماره ۱۲

صاحب امتیاز: انجمن علمی فقه و مبانی حقوق
زیر نظر: امور فرهنگی دانشگاه الزهرا(س)
استاد راهنما: زهرا سادات میر هاشمی
مدیر مسئول: فریناز سادات خطیبی
سردبیر: زینب خسروی فر
هیئت تحریریه: فریناز سادات خطیبی، زینب خسروی فر، مریم خدایی و فاطمه اسدی
کارشناس نشریات: سرکار خانم وزیری
چاپ: دامون
آدرس: ونک، میدان شیخ بهایی، دانشگاه الزهرا(س)-ساختمان خوارزمی

جرایم سازمان‌یافته
ارکان شرکت در جرم

رکن قانونی

همکاری و مشارکت فی‌نفسه جرم نیست مگر در فعلی که قانونگذار آن را جرم شناخته باشد و مطابق نظر قانونگذار برای آن مجازات تعیین گردیده است. در ماده ۴۲ قانون مجازات اسلامی چنین عنوان داشته است: «هر کس عالماً و عامداً با شخص یا اشخاص دیگر در یکی از جرائم قابل تعزیر یا مجازات‌های بازدارنده مشارکت نماید و جرم مستند به عمل همه آنها باشد خواه عمل هر یک به تنهایی برای وقوع جرم کافی باشد و خواه نباشد و خواه اثر کار آنها مساوی باشد، خواه متفاوت، شریک در جرم محسوب و مجازات او مجازات فاعل مستقل آن جرم خواهد بود...» و نیز در ماده ۲۱۴ همان قانون شرکت در قتل موجب قصاص را اینگونه تعریف می‌کند. «هرگاه دو یا چند نفر جراحتی را بر کسی وارد سازند که موجب قتل او شود چه در یک زمان یا زمان‌های متفاوت چنانکه قتل مستند به جنایت همگی باشد همه آنها قاتل محسوب می‌شوند...»

حال این سوال مطرح است که آیا در حدود و دیات شرکت در جرم معنی دارد یا خیر؟

و فی‌الواقع آیا شرکت در جرم در حدود و دیات قابل تحقق است یا خیر؟

در پاسخ به این سوال باید گفت در خصوص برخی از این جرائم شرکت در جرم معنی و مفهوم ندارد مثلاً درباره‌ی شرب‌خمر یا قذف نمی‌توان شرکت در جرم

را تعریف کرد و اگر جرم به اجتماع بیش از یک نفر باشد همگی فاعل مستقل شناخته می‌شوند.

اما شرکت در جرم در بزه‌هایی مانند سرقت و محاربه، امکان‌پذیر است، لیکن قانون در این موارد پیش‌بینی خاصی ننموده است. فلذا ما نباید به بهانه سکوت قانون از آن‌ها صرف‌نظر کنیم. چون در کتب فقهی معتبر امامیه هم درباره‌ی شرکت در جرم سرقت مستوجب حد اشاره کرده است.

عنصر مادی شرکت در جرم

عنصر مادی شرکت در جرم زمانی محقق می‌شود که عملیات مادی مجرمانه، که ضابطه جرم بودن است توسط بیش از یک نفر صورت گیرد و بتوان آن عمل مادی را به همه افراد نسبت داد.

در ماده ۴۲ قانون مجازات اسلامی مجازات شریک در جرم مجازات فاعل مستقل آورده است. یعنی در هر جرمی که شریک در جرم حضور داشته باشد و بتوان مرتکبی را شریک در جرم محسوب کرد. مجازات همان فاعل مستقل را بر آن (تحمیل می‌کنند) بار می‌کنند.

نکته مهم دیگر این است که ضابطه اصلی تحقق شرکت در جرم انتساب عملیات مادی جرم موردنظر است نه اعمالی که جنبه‌ی فرعی و مساعدتی در تحقق جرم دارد. به این ترتیب عبارت «جرم مستند به عمل همه آنها باشد» که در ماده ۴۲ قانون مجازات اسلامی آمده است اشاره به مستند بودن عملیات اجرایی به آنها دارد.

اگر در ماده مذکور به نحو روشن و صریح ذکر نگردیده است در این رابطه نظر مخالفی نیز وجود دارد که بیان می‌شود. قانونگذار مداخله در عملیات اجرایی را برای تحقق شرکت در جرم لازم و ضروری می‌داند به این معنی است که انجام عملیات اجرایی خواه مستند به عمل شرکاء باشد و یا یکی از آنها، یا اثر کار آنها به طور متفاوت باشد یا مساوی، شریک در جرم محسوب می‌شوند.

مطلب دیگری که در اینجا حائز اهمیت است میزان شدت یا ضعف عمل هر یک از شرکاء هیچ تاثیری در شرکت در جرم دانستن آنها ندارد. از این رو در ماده ۴۲ قانون مجازات اسلامی این‌گونه بیان کرده است: «... خواه عمل هر یک به تنهایی برای وقوع جرم کافی

باشد یا نباشد و خواه اثر کار آنها مساوی باشد یا متفاوت....»

حال باید گفت آنچه مهمترین مسئله در شرکت در جرم است؛ احراز رابطه علیت بین عملیات انجام شده توسط گروه و نتیجه حاصله می‌باشد که اگر مشخص شود بدون انجام عمل توسط این افراد نتیجه منفی می‌گشت، آنگاه شرکت در جرم افراد مورد نظر محرز و مشخص است.

عنصر روانی شرکت در جرم

در ماده ۴۲ قانون مجازات اسلامی با قید عالماً و عامداً، همکاری مجرمانه دو یا چند نفر از افراد را به شرط علم و اراده آنان موجب تحقق شرکت در جرم دانسته است. از این رو کسی که اثاثیه منزلی را از داخل خانه به خارج آن منتقل می‌کند و این فرد این عمل را ندانسته و ناآگاهانه از عمل سرقت توسط دوستانش و فقط به صرف کمک کردن برای نقل و انتقال اثاثیه که فکر می‌کند متعلق به دوستانش است انجام می‌دهد. اگر چه در این حالت مطابق بحث عنصر مادی، جرم شرکت است و عمل سرقت منتسب به عمل اوست، ولی به جهت عدم تحقق عنصر روانی که همان عالم بودن و علم داشتن به جرم بودن عمل و نتیجه مجرمانه حاصل از آن است، نمی‌توان چنین فردی را شریک در جرم نامید.

نکته دوم در این خصوص داشتن اراده و اختیار به علاوه عمد و قصد است. یعنی زمانی شخصی شریک در جرم است که بدون هیچ اکراه و اجباری و در حالت طبیعی و تسلط بر قوه‌ی عقل و سلامت کامل با علم به جرم بودن عمل موردنظر اقدام به مشارکت در آن نماید. علاوه بر موارد گفته شده در قبل باید این مطلب گفته شود که تبانی و توافق پیش از جرم برای تحقق شرکت در جرم لازم است و همین که فرد در یک مشاجره و درگیری از راه برسد و در یک نزاع دسته‌جمعی به نفع دوستانش شرکت کند و حاصل عمل همه آنها به نتیجه مشترکی ختم شود آن فرد نیز شریک در جرم است. با وجود آنکه از قبیل تبانی و توافق برای ارتکاب این فعل مجرمانه نداشته است.

در ماده ۴۲ قانون مجازات اسلامی چنین عنوان داشته است: «هر کس عالماً و عامداً با شخص یا اشخاص دیگر در یکی از جرائم قابل تعزیر یا مجازات‌های بازدارنده مشارکت نماید و جرم مستند به عمل همه آنها باشد خواه عمل هر یک به تنهایی برای وقوع جرم کافی باشد و خواه نباشد و خواه اثر کار آنها مساوی باشد، خواه متفاوت، شریک در جرم محسوب و مجازات او مجازات فاعل مستقل آن جرم خواهد بود...»

مجازات شرکت در جرم

در ماده ۴۲ قانون مجازات اسلامی مجازات شریک در جرم مجازات فاعل مستقل آورده است. یعنی در هر جرمی که شریک در جرم حضور داشته باشد و بتوان مرتکبی را شریک در جرم محسوب کرد. مجازات همان فاعل مستقل را بر آن (تحمیل می‌کنند) بار می‌کنند.

جرایم مجازی

جرایم سایبری، نوعی از جرایم اینترنتی می‌باشند که شامل جرم‌هایی هستند که در محیط سایبر بوجود می‌آیند، که در این مقاله ما به تعریف محیط سایبر که یک محیط مجازی می‌باشد و به ویژگی محیط سایبر، به‌طوری‌که کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی در سراسر دنیا دستیابی پیدا کنند و چگونگی ایجاد جرایم که در فضای سایبر کپی عین اصل می‌باشد و انواع مجرمین محیط سایبر شامل هکرها، کرکرها، فریک‌های تلفن و انواع جرم‌های ممکن بانام سایبرکرایم و در مورد جرم آینده با نام تروریسم سایبر که مانند تروریست‌های معمولی دارای انگیزه‌های سیاسی برای ارتکاب جرایم هستندو همچنین بحران سازهای سایبر شامل ویروسها، عنکبوتهای موتورهای جستجو و پالس‌های الکترومغناطیسی، کرم‌ها و بمب‌های منطقی و در مورد پلیس سایبر که مطابق با خاص بودن جرم‌های سایبر، نیاز به آموزش‌های خاص دارندو در آخر در مورد روش‌های

تاریخچهٔ جرایم سایبر

دراواسط دههٔ ۹۰با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم کامپیوتری، تحت عنوان جرایم سایبری (مجازی) یا جرایم در محیط سایبر شکل گرفته‌است. به این ترتیب جرایم اینترنتی را می‌توان مکمل جرایم

دراواسط دهۀ ۹۰با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم کامپیوتری، تحت عنوان جرایم سایبری (مجازی) یا جرایم در محیط سایبر شکل گرفته‌است.

کامپیوتری دانست، بخصوص اینکه جرایم نسل سوم کامپیوتری که به جرایم در محیط مجازی معروف است، غالباً از طریق این شبکه جهانی به وقوع می‌پیوندد.

ویژگی‌های فضای سایبری

کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون درنظرگرفتن اینکه این اطلاعات و خدمات در کدام نقطۀ دنیا واقع شده‌است. محیط سایبر زمینۀ فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیۀ معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده‌است. محدودۀ 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.

از بعد اقتصادی فضای سایبری را می‌توان یک بازار واحد جهانی دانست که از ثمره‌های موفق جامعه مبتنی بر تکنولوژی مدرن اطلاعاتی می‌باشد 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 می‌باشد، محیطی است مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگها، ملتها، کشورها و به‌طور کلی هرآنچه در کرۀ 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 می‌باشند و به طریق کامپیوتر، اجزا آن و شبکه‌های بین‌المللی بهم مرتبط می‌باشند.

جرایم در سایبر اسپیس

فضای سایبر هنوز در مراحل اولیه است. طبیعت این جرایم و سوءاستفاده‌های مرتکب شده در این دنیای مجازی جدید هیچ‌گاه در دنیای حقیقی دیده نشده‌است. امنیت ناکافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران‌کننده‌ترین جنبۀ فضای سایبر انتشار سریع اطلاعات درآن می‌باشد، مثلاً در لحظۀ کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود. در فضای سایبر برای جستجو و پیداکردن این جرایم مشکلات پیچیده‌تر می‌شود. در دنیای واقعی دزدی از بانک کاملاً مشخص است چرا که بعد از سرقت در خزانه بانک پولی موجود نیست؛ ولی در تکنولوژی کامپیوتری شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان‌طورکه دقیقاً بوده باقی بگذارد. در فضای سایبر کپی عیناً عین اصل است با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب وبررسی مثل پاک کردن اثر انگشت تغییردهد.

نگران‌کننده‌ترین جنبهٔ فضای سایبر انتشار سریع اطلاعات درآن می‌باشد، مثلاً در لحظهٔ کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود.

مجرمین سایبر

هکر: دردههٔ ۱۹۷۰ واژهٔ هکر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر و باهوش باشد. بعدها دردههٔ ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید 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 قابل توجهی شوند، اما جستجو برای یافتن اطلاعات وآموزش، 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 سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایلها را پاک کنند یا بعضی انواع دیگر ویرانی را به‌بارآورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.

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 سیستم رایانه، یافتن راهی برای ورود مخفیانه به آن‌ها و پیداکردن سوراخ‌های امنیتی این سیستم هاست 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 جرایم رایانه‌ای رأفریک‌های تلفن " مرتکب می‌شوند. فریک‌ها به جای دسترسی به سیستم‌های رایانه‌ای، از طریق خطوط تلفن در دنیای سایبر گشت می‌زنند. فریک‌ها از میان اولین هکرها دردهه۱۹۷۰ پدید آمدند. یکی از حوادثی که توسط فریک‌ها بوجود آمده بود در سال ۱۹۷۷ مربوط به اداره پلیس شهر نیویورک می‌شد، فریک‌ها به سیستم 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 وفر صت جواب 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 سیستم‌های 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 سیستم 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 سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه، برای مثال 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 درراینه غیرفعال باقی می‌مانند و سپس با سررسیدن تاریخی که برنامهٔ آن‌ها مشخص شده‌است منفجر می‌شوند. اهداف این بمب‌ها متفاوت است.

انواع جرایم سایبری

تنوع انواع جرایم ارتکابی در سایبرسپیس شامل جرایم نسل اول کامپیوتری (البته به شکل نوین) و تعدادی جرایم بسیار جدید وبی سابقه می‌باشد.

جرایم 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 کامپیوتر به منظور مختل ساختن عملکرد عادی سیستم سابوتاژ رایانه‌ای گویند.

جعل کامپیوتری: واردکردن، تغییر، محو یا موقوف‌سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی واقتصادی صورت میگرد. جعل کامپیوتری جعل داده هاست. در جعل کامپیوتر ی 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 کامپیوتری 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 درآن 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 می‌باشد.

تطهیر نامشروع پول: بدست آوردن پول از طریق غیرقانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد، نحوهٔ ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ کونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را می‌نمایند و در تقاضای خود نحوهٔ ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف نوع و نحوهٔ تنظیمات لازم را اعلام می‌دارند و اصولاً درزمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب وبا هدف خود هماهنگ می‌نمایند لازم است ذکر شود غالب این درخواستها از افراد کشورهایی که از لحاظ تکنولوژی 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 سایبر 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 کامپیوتری 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 می‌باشد و ضریب اطمینان قاچاق موادمخدر از طریق ارتباطات کامپیوتری و شبکه‌ای بالاتر از نوع سنتی آن می‌باشد. جرایم ناظر به کپی رایت وبرنامه‌ها: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش واستفادهٔ غیرمجاز از برنامه‌های کامپیوتری سرقت نرم‌افزار گویند.

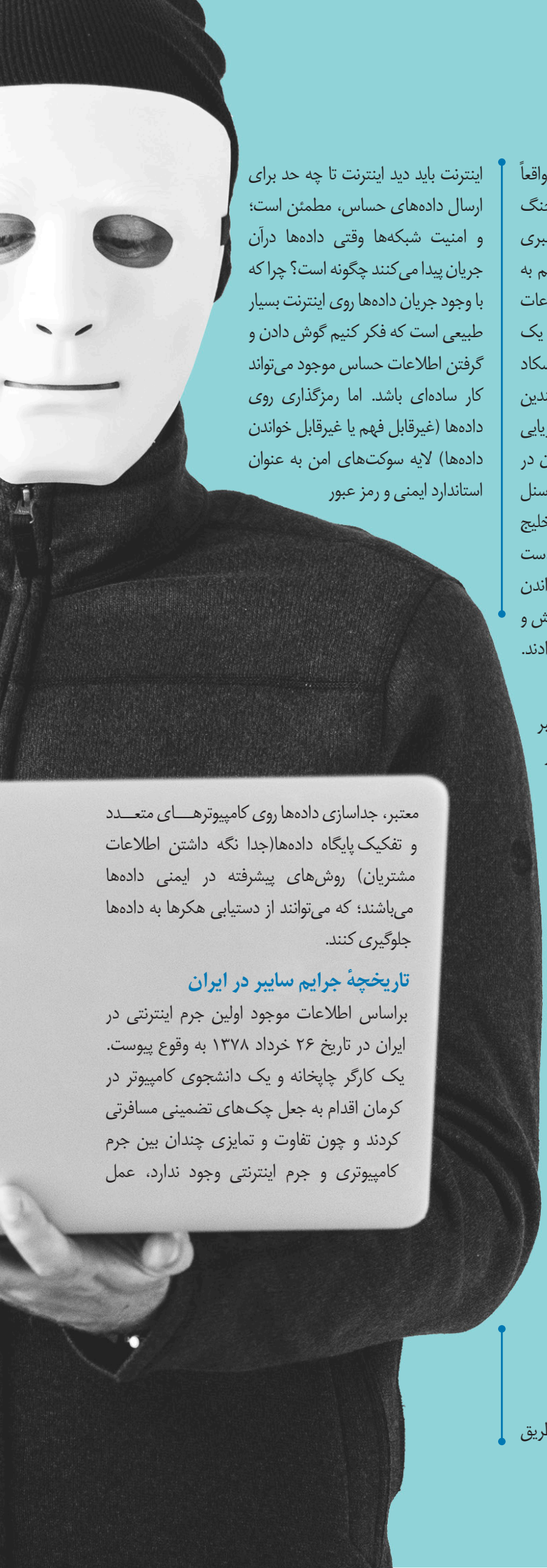
جرایم در تجارت الکترونیک: شامل کلاهبرداری در تجارت، تعریف کلی و کلاسیک کلاهبرداری عبارتست از"تحصیل مال دیگری بااستفاده از وسایل متقلبانه"شخصی در نقطه‌ای نامعلوم با واردشدن به شبکهٔ بین‌المللی (مثل اینترنت)و معرفی خود به عنوان تاجر و صاحب یک شرکت معتبر در یک سایت تجاری و ارائهٔ "نهادی مشابه ادارهٔ ثبت 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 می‌باشد "(تماماً غیرواقع و کذب)، اظهار می‌دارد که کالایی را با قیمت معین، نوع و تعداد مشخص در اختیار داشته و قابل عرضه به مشتریان می‌باشد از طرفی خریدارانی که در فضای شبکه‌ها مشغول تجارت الکترونیک (خریدوفروش) می‌باشند پس از دریافت پیام، نسبت به برقراری ارتباط شبکه‌ای (که غالباً به صورت پست الکترونیک یا ارسال درخواست هز طریق شبکه می‌باشد 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

بدست آوردن پول از طریق غیرقانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد

وجه اقدام می‌نماید. خریدار نیز پس از پرداخت وجه (غالباً به صورت پرداختهای الکترونیکی)منتظر دریافت کالا می‌باشد 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، گروگان گیری 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 می‌باشد. اما آیا واقعاً تروریسم سایبر امکان‌پذیر است؟ در سال ۱۹۹۱ 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 سیستم‌های 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.

پلیس سایبر

بعضی از افسران پلیس از دهه۱۹۷۰ در زمینه جرایم سایبر آموزش دیده‌اند و تخصص پیدا کرده‌اند. جرایم سایبر ممکن است در هر جایی اتفاق بیفتد و غالباً قابل ردیابی نیستند. بیشتر ادارات پلیس محلی فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرایم 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 جرایم سایبر خواهد بود؟ علاوه برآنچه پلیس رایانه‌ای نامیده می‌شود، شهروندانی نیز وجود دارند که به صورت شخصی به جلوگیری از جرایم سایبر و شناسایی مجرمان کمک می‌کند. هنوز هم مباحثات زیادی درمورد روش‌های مورد استفاده توسط مقامات رسمی، دراجرای قوانین مبارزه با جرایم 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 و یا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس، مطمئن است؛ و امنیت شبکه‌ها وقتی داده‌ها درآن 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 و رمز عبور معتبر، جداسازی داده‌ها روی کامپیوترهـــای متعـــدد و تفکیک پایگاه داده‌ها(جدا نگه داشتن اطلاعات مشتریان) روش‌های پیشرفته در ایمنی داده‌ها می‌باشند؛ که می‌توانند از دستیابی هکرها به داده‌ها جلوگیری کنند.

تاریخچهٔ جرایم سایبر در ایران

براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل

آن‌ها به عنوان جرم اینترنتی محسوب می‌شود.

بعد 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 جرایم اینترنتی هستند.

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

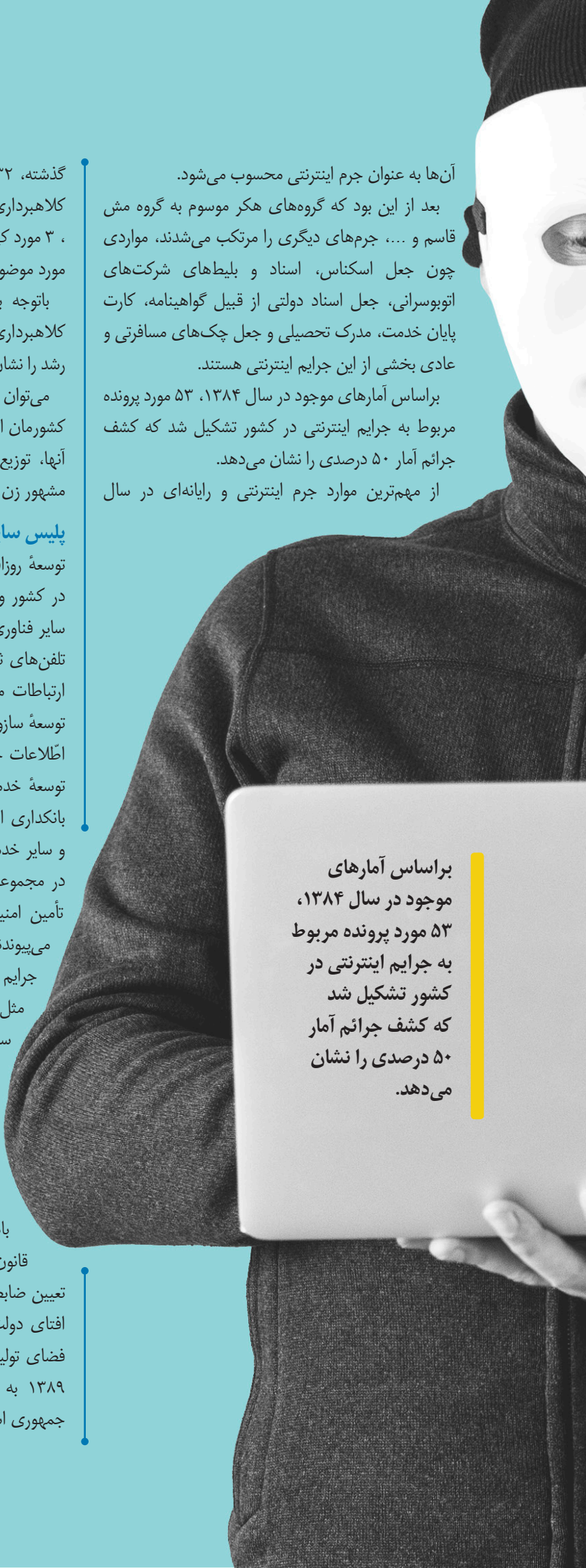
از مهم‌ترین موارد جرم اینترنتی و رایانه‌ای در سال گذشته، ۳۲ مورد سوء استفاده از کارت‌های اعتباری ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت ، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده‌است.

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

می‌توان گفت امسال هم جرایم 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 سایر 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 سایر خدمات از این دست، نیز لزوم ایجاد پلیسی تخصّصی در مجموعهٔ نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند. از سوی دیگر، رشد قارچ‌گونه جرایم در حوزهٔ فضای تولید و تبادل اطّلاعات کشور (فتا) مثل 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 جرایم اخلاقی و برخی جرایم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصّصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فنّاورانه داشته باشد، به وجود آید. از سوی دیگر با توجّه به تصویب قانون جرایم 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.



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

جرایم علیه اشخاص

نویسنده : محمدحسین طارمی

به طور کلی در حقوق کیفری اختصاصی، هر جرمی به صورت جداگانه تعریف و عناصر و شرایط تشکیل دهنده آن بررسی می‌شود که این امر سبب تمییز و تفکیک جرایم از یکدیگر می‌شود. حقوق‌دانان غالبا در تقسیم بندی‌های خود از جرایم، به آثار زیان بار فعل مجرمانه توجه کرده، جرایمی را که خسارات حاصل از آن‌ها به طور کلی دارای جهت مشترکی است، در یک گروه جای داده اند. به عنوان مثال، جرایم سرقت، کلاهبرداری، خیانت در امانت و... را که همگی تعرض به اموال و مالکیت است، در یک طبقه با عنوان جرایم علیه اموال و مالکیت مورد بحث و بررسی قرار می‌دهند. جرایمی از قبیل قتل را به عنوان جرایم علیه اشخاص و جرایم دیگری مانند: جعل، جاسوسی، و... را تحت عنوان جرایم علیه امنیت و آسایش عمومی قرار داده‌اند.

تقسیم بندی مباحث

جرایم علیه اشخاص، بر خلاف جرایم علیه اموال و جرایم علیه امنیت، به جرایمی که بر ضد خود شخص و فردی است که جامعه را تشکیل می‌دهد؛ می‌پردازد. از آن جا که هر شخصی دارای دو بعد مادی و معنوی، یا جسمانی و روانی است، جرایم علیه نیز به دو بخش عمده تقسیم شده است.

بخش اول: جرایم علیه تمامیت جسمانی

جرایم علیه تمامیت جسمانی اشخاص که در فقه جزایی به عنوان «جنایات» مورد بحث قرار گرفته است؛ از مهمترین جرائمی است که حق حیات آدمی و اصل مصونیت از تعدی و تعرض را هدف قرار داده و همواره در قوانین جزایی شدید ترین واکنش کیفری را برای آن پیش بینی شده است.

ایراد صدمات بدنی گاه منتهی به حدوث مرگ (قتل) که سنگین ترین نتیجه مجرمانه است، می‌شود. گاه نیز نتایج خفیف تری را به صورت قطع یا نقص عضو و زایل شدن منافع آن است،تحت عنوان جنایت بر اطراف، در پی دارد. جنایت در لسان اغلب فقها به سه بخش تقسیم شده است. اما ایشان ضمن مباحث مختلف در ابواب مربوطه، انواع دیگری از جنایت را یادآور شده‌اند. با عنایت بر اقوال ایشان، مجموعه جنایات مذبور در گروه‌های زیر بررسی شده است:

۱. جنایت عمد
۲. شبه عمد
۳. خطایی محض
۴. در حکم شبه عمد
۵. در حکم خطایی محض.

قانون مجازات اسلامی نیز به تبعیت از فقه به صورت پراکنده این اقسام را بیان داشته است.

منابع حقوقی جنایات علیه تمامیت جسمانی را در دو گروه عمده جای داده و مورد بحث قرار داده‌اند:

الف ـ جنایات عمدی

جنایات عمدی آن دسته از جرایم عمدی است که بر ضد شخص واقع می‌شود. این جنایات بر دو قسم است:

۱. جنایت بر نفس (قتل عمد)

قانون مجازات اسلامی بدون تعریف جامع و مانع از قتل عمد، در ماده ۲۰۶ به شرح مصادیق قتل عمد می‌پردازد:

«قتل در موارد زیر عمدی است:

الف- مواردی که قاتل با انجام کاری قصد کشتن شخص معین یا فرد یا افرادی غیر معین از یک جمع را دارد،خواه آن کار نوعا کشنده باشد،خواه نباشد، ولی در عمل سبب قتل شود.

ب- مواردی که قاتل عمدا کاری انجام دهد که نوعا کشنده باشد، هر چند قصد کشتن را نداشته باشد.

ج- مواردی که قاتل قصد کشتن را ندارد و کاری را که انجام می‌دهد، نوعا کشنده نیست. ولی نسبت به طرف بر اثر بیماری یا پیری یا ناتوانی یا کودکی و امثال آن‌ها نوعا کشنده باشد و قاتل نیز به آن آگاه باشد.»

۲. جنایت بر اعضا

ماده ۲۷۱ قانون مجازات اسلامی مشابه ماده ۲۰۶ مصادیق جنایت عمدی بر اعضا را بیان داشته است.

رکن مادی جنایات عمدی

رکن مادی جنایات عمدی وجود شخص زنده، که این شخص شرعا مستحق کشته شدن نباشد. (م ۲۲۶ ق.م.ا.)، فعلیت یافتن قصد ارتکاب جرم به صورت مباشرت یا تسبیب عمدی و وقوع نتیجه (مرگ) و وجود رابطه استناد است.

رکن روانی جنایات عمدی

عمد یا قصد جزائی عبارت است از انصراف ارادی جانی به وقوع فعل و عنوان مجرمانه با علم به ممنوعیت آن. لذا رکن روانی متشکل از عمد در فعل و عمد در نتیجه است.

مجازات جنایات عمدی

حکم اولی در مجازات مرتکب جنایت عمدی قصاص است. شرایط ثبوت قصاص عبارتست از: تساوی در دین (منطوق و مفهوم مواد ۲۰۷، ۲۰۹ و ۲۱۰ ق.م.ا.) تساوی در عقل (م۲۲۲) و انتفاء ابوّت است. شرایط اجرای آن نیز عبارتند از: تقضای اولیاء دم، اذن ولی امر، اذن ولی دم، پرداخت دیه مازاد بر استحقاق و ممنوعیت ایذاء جانی. البته قصاص عضو دارای شرایط ویژه ی دیگری است که عبارتست از: تساوی اعضا در سالم بودن (م۲۷۴)،تساوی در اصلی بودن (م ۲۹۳)، تشاوی در محل جنایت (م ۲۷۵)، تساوی در جنایت (م ۲۷۶)، عدم تغریر (مواد ۲۷۷ و ۲۸۱).

ب ـ جنایات غیر عمدی

جنایات غیر عمدی اعم از قتل و جنایات مادون نفس، به چهار صورت واقع می‌شود:

۱. جنایت شبه عمد

ملاک اصلی آن وجود قصد فعل و عدم قصد نتیجه است. با توجه به ماده ۲۹۵ بند ب می‌توان آن را چنین تعریف کرد: « شبه عمد، جنایت غیر مقصودی است که از فعل غالبا غیر کشنده ای که بر مجنی علیه اعمال شده حاصل آمده است.

۲. جنایت خطایی محض

ملاک اصلی آن فقدان قصد فعل و نتیجه است (بند الف ماده ۲۹۵).

۳. جنایت در حکم خطای محض

گاه ممکن است جنایت ارتکابی به وسیله جانی، طاهرا به صورت عمد یا شبه عمد واقع شده باشد یا تصور عمد و خطا در مورد آن غیر قابل پذیرش باشد، در این موارد قانونگذار آثار خطای محض

را بر آن مترتب ساخته و به عنوان جنایت در حکم خطای محض از ان یاد کرده است. چنان که ارتکاب جنایت به وسیله مجنون و صغیر (تبصره م ۲۹۵) شخص خواب(م ۳۲۳) را در زمره خطای محض آورده است.

۴. جنایت در حکم شبه عمد

جنایتی که ماهیت آن عمد یا خطای محض است، لکن به دلیل وجود عناصر یا شرایطی خاص ،آثار جنایت شبیه عمد بر آن مترتب می‌گردد. لذا در صورتی که جانی در شخصیت مجنی علیه دچار اشتباه شده و بدون قصد مجرمانه مرتکب قتل عمد شود (تبصره ۲ ماده ۲۹۵) یا با وجود قصد مجرمانه اشتباه در هویت کند (رای اصراری ۱۳۷۱/۷/۷) و یا جنایت خطای محض همراه با خطای جزایی (بی احتیاطی، بی مبالاتی، عدم مهارت، عدم رعایت نظامات) باشد (تبصره ۳ م ۲۹۵)، جنایت در حکم شبه عمد خواهد بود.

بخش دوم: جرایم علیه شخصیت معنوی اشخاص

این جرایم به پنج بخش کلی قابل تقسیم است:

۱. توهین

عبارت است از رفتار عمدی خلاف قانون که به موجب عرف نسبت به طرف موهن باشد. رکن مادی این جرم رفتار مادی موهن نسبت به فرد معین است. رکن معنوی آن قصد و علم به اهانت آمیز بودن رفتار است. رکن قانونی عبارت است از مواد ۵۱۳ و ۵۱۴ (اهانت به مقدسات و شخصیت‌های مذهبی) م۵۱۷ق.م.ا (اهانت به رئیس کشور خارجی) م۶۰۸ ق.م.ا (توهین ساده)، م۶۰۹ ق.م.ا (توهین مشدد)، م۶۱۹ ق.م.ا و....

۲. افترا

افترا به معنای عام که شامل جرایم ذیل است:

أ. افترا

عبارتست از نسبت دادن عمدی و آگاهانه امری مجرمانه و زشت به شخص. ماده ۶۹۸ ناظر به افترای ساده و ماده ۶۹۹ ق.م.ا. ناظر به افترای عملی است. البته اشاعه فحشا (م ۶۹۷) اتهام در جرایم مواد مخدر (ماده ۲۸ ق. مواد مخدر) انتشار حکم(م ۱۸۸ ق.آد.ک.) از دیگر مصادیق قانونی افتراست.

ب. قذف

که عبارتست از «نسبت دادن زنا یا لواط به دیگری» مواد ۱۳۹ - ۱۶۴ ق.م.ا.

ج. نشر اکاذیب

طبق ماده ۶۹۸ ق.م.ا. اظهار اکلذیب و انتساب اعمال خلاف حقیقت از مصادیق بارز این جرم است.

۳. جرایم علیه آزادی رفت و آمد

که شامل جرایم ذیل است:

أ. جرایم علیه آزادی تن

شامل جرایم توقیف و اخفاء غیر قانونی توسط افراد عادی (م ۵۸۳ ق.م.ا.)

ب. دستور بازداشت غیر قانونی

صدور دستور بازداشت غیر قانونی توسط قضات(۵۷۵ ق.م.ا.)؛

ج. بازداشت غیر قانونی

بازداشت غیر قانونی توسط مامورین(۵۷۰)

د. آدم ربایی(م ۶۲۱ ق.م.ا.)

ه. قاچاق انسان(ق.مبارزه با قاچاق انسان مصوب۸۳)

۴. تهدید واکراه

تهدید واکراه که شامل

أ. اخذ سند یا نوشته به عنف (م ۶۶۸ ق.م.ا.)

ب. تهدید به قتل و مانند آن (م ۶۶۹ ق.م.ا.)

۵. جرایم علیه جریم خصوصی

شامل هتک حرمت منزل(مواد ۶۹۴، ۵۸۰ ق.م.ا.) هتک حرمت املاک غیر (م ۶۹۱ ق.م.ا.) هتک حرمت مراسلات یا مخبرات یا مکالمات تلفنی(م ۵۸۲ ق.م.ا.) مزاحمت تلفنی (م ۶۴۱ ق.م.ا.)

شرایط سازمان تامین اجتماعی برای تقسیط جرائم بیمه‌ای کارفرمایان

مدیر کل وصول حق بیمه سازمان تامین اجتماعی اعلام کرد: به منظور مساعدت با کارفرمایان بدهی های بیمه به صورت تقسیط تا ۶۰ قسط امکان پذیر خواهد بود.

به گزارش خبرگزاری صدا و سیما به نقل از اداره کل روابط عمومی سازمان تامین اجتماعی، مهرداد قریب در برنامه گفتگوی روز ۱۸,۳۰ شبکه خبر گفت: کارفرمایانی که به هر علتی تاکنون موفق نشده‌اند برای ارائه درخواست خود برای بهره‌مندی از قانون بخشودگی جرایم بیمه‌ای به شعب تأمین اجتماعی مراجعه کنند، فقط امروز را برای تعیین تکلیف بدهی خود به این سازمان مهلت دارند.

وی افزود: با توجه به اینکه بخشی از کارفرمایان نتوانستند در سال ۹۶ از بخشودگی جرایم استفاده کنند در سال ۹۷ سازمان تامین اجتماعی برای بالا بردن توان کارفرمایان به هیئت وزیران پیشنهادی داد که در تاریخ نهم اردیبهشت ۹۷ مصوبه به سازمان اعلام و در تاریخ ۱۰/۲/۹۷ این بخشنامه صادر شد و تا امشب (۱۰/۴/۹۷) فرصت داده شده تا از این بخشودگی جرائم استفاده کنند. تمام کارگاه های تولیدی، صنعتی، معدنی، پیمانکاری اعم از اشخاص حقیقی، حقوقی، دولتی و غیر دولتی می توانند از قانون بخشودگی جرائم بیمه ای استفاده کنند.

مدیرکل وصول حق بیمه سازمان تامین اجتماعی گفت: برخی کارفرمایان با مشکلاتی مواجه می شوند مثل نوسانات ارزی، تحریم، رکود، سیل و زلزله که کارفرمایان نمی توانند در مهلت مقرر قانونی حق بیمه را پرداخت کنند بنابراین سازمان تامین اجتماعی برای حمایت از کارفرمایان خوش حساب گذشته این بخشنامه را صادر کرد تا بتوانند از تسهیلات بخشودگی استفاده کنند.

وی افزود: بررسی های لازم در کمیته های مخصوص انجام می شود و با تایید نهایی و در صورت تائید خوش حساب بودن کارفرمایان می توان از بخشودگی استفاده کرد.

قریب گفت: افرادی که مراجعه و گواهی های لازم را ارسال می کنند بررسی ها انجام می شود و اگر از تاریخ اعلام دلایل ابرازی ظرف ۱۸ ماه قبل از آن حق بیمه ۴ ماه را به صورت کامل پرداخت کرده باشند می توانند از بخشودگی ها استفاده کنند.

وی اظهار داشت: کارفرمایان می توانند به شعب سازمان تامین اجتماعی مراجعه کنند و درخواست را یا به سازمان ارجاع دهند یا در سیستم ثبت کنند بعد با مراجعه می توانند سایر مدارک را ارائه دهند.

قریب افزود: صد و چهل شعبه در کشور تا ساعت ۲۰ امشب فعال هستند تا درخواست ها را دریافت کنند.

سال گذشته ۱۲۳ هزار کارفرما

مراجعه کردنـــــدو درخواست‌های خود را ارائه دادند و تا شب گذشته نیز ۶۰ هزار کارفرما درخواست خود را ثبت کرده اند و کمیته های مستقر در شعب مشغول بررسی درخواست ها هستند.

وی درباره برآورد بدهی گفت: کل بدهی کارفرمایان بخش خصوصی به سازمان تامین اجتماعی ۱۸ هزار میلیارد تومان است که تعدادی که بدهکار هستند می‌توانند از امکان تقسیط نیز استفاده کنند.برخی از کارفرمایان که توان پرداخت دارند می توانند با پرداخت اصل بیمه از بخشودگی صد درصدی جرایم استفاده کنند، اگر در ۱۲ قسط پرداخت کنند نیز می توانند از بخشودگی ۱۰۰ درصدی و در صورت ۱۸ قسط از ۸۵ درصد و در صورت پرداخت ۲۴ قسط از ۷۵ درصد، در صورت استفاده از ۳۰ قسط از ۶۰ درصد و صورت ۳۶ قسط از پنجاه درصد بخشودگی جرائم استفاده خواهند کرد.

مدیر کل وصول حق بیمه سازمان تامین اجتماعی درباره اجرای قانون حمایت از تولید ملی گفت: در این فرصت کارفرمایان می توانند از نقدینگی در بخش تولید و اشتغال استفاده کنند و توان مالی کارفرمایان بالا می رود و بخشودگی بیشتری شامل حال آنها می شود تا بتوانند از همه تعهدات سازمان تامین اجتماعی استفاده کنند.

وی درباره دیگر سیاست‌های تشویقی گفت: سازمان اجتماعی اخیرا بخشنامه‌ای تحت عنوان مشوق های بیمه‌ای برای فارغ التحصیلان دانشگاهی در نظر گرفته است که در صورت جذب فارغ التحصیلان دانشگاهی کارفرمایان می‌توانند از معافیت بیمه ای سهم کارفرما استفاده کنند و از خدمات سازمان تامین اجتماعی بدون پرداخت حق بیمه کارفرما استفاده کنند.

قریب درباره پرداخت نکردن حق بیمه‌ای کارفرمایان نیز گفت: در صورت پرداخت نکردن بدهی بیمه بازهم فرصت دیگری داده خواهد شد که به این منظور بدهی کارفرمایان به صورت تقسیط تا ۶۰ قسط امکان پذیر خواهد بود اما وقتی سازمان اجتماعی جرائم را بخشید بنابراین کارفرمایان نیز باید اقساط را به موقع پرداخت کنند تا مجدد مشمول جریمه نشوند.

وی درباره خدمات غیر حضوری و تسهیل در پرداخت‌ها نیز گفت: سازمان تامین اجتماعی در سال‌های اخیر اقدامات موثری انجام داده است؛ اولین اقدام این است که پرداخت و ارسال لیست بیمه از طریق اینترنت صورت می گیرد. ما یک میلیون و ۴۰۰ کارفرما داریم که ۹۹ درصد ارسال لیست و پرداخت حق بیمه به صورت اینترنتی صورت می گیرد. سازمان تامین اجتماعی با این کار هزینه ها را کاهش داد و بهره وری را بالا برد. در صدور دفترچه خدمات درمانی نیز بر اساس کد ملی می توانند خدمات دریافت کنند و به مرور در مراکز دولتی نیز استفاده از دفترچه درمانی از بین می رود و می توانند از این خدمات استفاده کنند. میز خدمت برای پاسخ گویی به مستمری بگیران و بیمه شدگان به جهت تکریم عملی ارباب رجوع ایجاد شده است.

قریب درباره بازرسی الکترونیکی از کارگاهها نیز گفت: بازرسی ها قبلا به صورت دستی صورت می گرفت . در حال حاضر از آذرماه سال ۹۶ بازرسی‌ها هم به صورت آنلاین و آفلاین صورت می‌گیرد و بازرسان از طریق تبلتی که در دست دارند بازرسی را انجام می‌دهند که این امر بهره وری را افزایش داده است که با این کار کلیه کارگرانی که مشغول کار هستند تحت پوشش خدمات بیمه‌ای قرار دهیم و به صورت انلاین بتوانند از خدمات تامین اجتماعی بهره‌مند شوند.

قوانین جرایم سایبری در ایران

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 حبس 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 حبس 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 درحال 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 حبس 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 حبس 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 حبس 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 توسطوزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویبهیئت 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 حبس 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 حبس 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

ماده۶ـ هر کس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس 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 حبس 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 حبس 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 حبس 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، حمل و نقل و بانکداری مرتکب شود، به حبس 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 حبس 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 حبس 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 حبس 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 درخصوص محتویات مبتذل موجب محکومیت به حداقل 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 فی‌الارضشناخته 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 حبس 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 حبس 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 حبس 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 حبس 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 براعاده حیثیت (در صورت امکان)، به حبس 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 قسمتی 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 حبس آن جرم تا پنج سال حبس 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 حبس آن جرم بیش از پنج سال

حبس 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 ۱۳۷۳/۴/۱۹ و الحاقات بعدی آن یا به احزاب، جمعیتها، انجمن‌های سیاسی و صنفی و انجمن‌های اسلامی یا اقلیتهای دینی شناخته‌شده یا به سایر 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 محلدادستانی 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.

تبصره۱۱ - جلسات کارگروه (کمیته) حداقل 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 وشورای 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 بی احتیاطی 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 حبس 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: سایر جرائم

ماده۲۵ـ هر شخصی که مرتکب اعمال زیر شود، به حبس 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 سیستم‌های 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.

هـ)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 حبس آن جرم نودویک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

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

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

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: جمع‌آوری ادله الکترونیکی

مبحث اول ـ نگهداری داده‌ها

ماده۳۲ـ ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل 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 سایر مشخصات فردی اوست.

ماده۳۳ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل 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 سایر 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 سایر اشخاص به حبس 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.

ماده۴۱ـ 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،

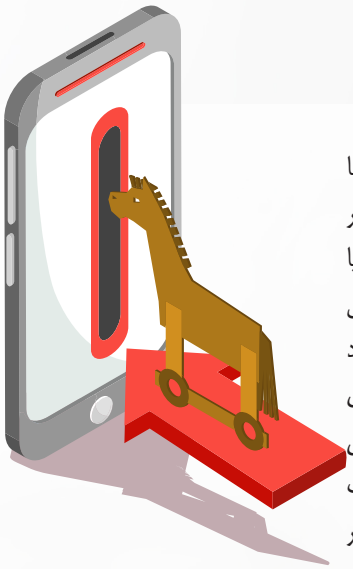
ج) متصرف قانونی سامانه رضایت داده باشد،

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 سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرارداد 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 عمومی شود 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.