متن کامل قانون جرائم رایانه ای

- **بخش یکم ـ جرائم و مجازات‌ها**

فصل یکم ـ جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

ماده (۱) هرکس به طور غیرمجاز به داده ها یا سیستم های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

مبحث دوم ـ شنود غیرمجاز

ماده (۲) هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ جاسوسی رایانه ای

ماده (۳) هرکس به طور غیرمجاز نسبت به داده ای سری در حال انتقال یا ذخیره شده در سیستم های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به مجازات های مقرر محکوم خواهد شد:

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

ب) در دسترس قرار دادن داده ای مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشا یا در دسترس قرار دادن داده ای مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره ۱ـ داده ای سری داده ای است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره ۲ـ آئین نامه نحوه تعیین و تشخیص داده ای سری و نحوه طبقه بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت دولت خواهد رسید.

ماده (۴) هرکس به قصد دسترسی به داده ای سری موضوع ماده (۳) این قانون، تدابیر امنیتی سیستم های رایانه ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۵) چنانچه مأموران دولتی که مسؤول حفظ داده ای سری مقرر در ماده (۳) این قانون یا سیستم های مربوط هستند و به آنها آموزش لازم داده شده است یا داده ها یا سیستم های مذکور در اختیار آنها قرار گرفته است بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده ها، حامل های داده یا سیستم های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم ـ جرائم علیه صحت و تمامیت داده ها و سیستم های رایانه ای و مخابراتی

مبحث یکم ـ جعل رایانه ای

ماده (۶) هرکس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر داده ای قابل استناد یا ایجاد یا وارد کردن متقلبانه داده ها،

ب) تغییر داده ها یا علایم موجود در کارت های حافظه یا قابل پردازش در سیستم های رایانه ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانه داده ها یا علایم به آنها.

ماده (۷) هرکس با علم به مجعول بودن داده ها یا کارت ها یا تراشه ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

مبحث دوم ـ تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی

ماده (۸) هرکس به طور غیرمجاز داده دیگری را از سیستم های رایانه ای یا مخابراتی یا حامل های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۹) هرکس به طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده ها یا امواج الکترومغناطیسی یا نوری، سیستم های رایانه ای 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۰) هرکس به طور غیرمجاز با انجام اعمالی از قبیل مخفی کردن داده ها، تغییر گذرواژه یا رمزنگاری داده ها مانع دسترسی اشخاص مجاز به داده ها یا سیستم های رایانه ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۱) هرکس به قصد به خطر انداختن امنیت یا آسایش عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سیستم های رایانه ای 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 خواهد شد.

فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده (۱۲) هرکس به طور غیرمجاز داده ای متعلق به دیگری را برباید، چنانچه عین داده ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۳) هرکس به طور غیرمجاز از سیستم های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سیستم 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 تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرایم علیه عفت و اخلاق عمومی

ماده (۱۴) هرکس به وسیله سیستم های رایانه ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ۱ ـ ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازات های فوق می شود. محتویات و آثار مبتذل به آثاری اطلاق می گردد که دارای صحنه ها و صور قبیحه باشد.

تبصره ۲ ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.

تبصره ۳ ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفه خود قرار داده باشد یا بطور سازمان یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره ۴ ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی اطلاق می شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده (۱۵) هرکس از طریق سیستم های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

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

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 ـ هتک حیثیت و نشر اکاذیب

ماده (۱۶) هرکس به وسیله سیستم های رایانه ای 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 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.

ماده (۱۷) هرکس به وسیله سیستم های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۸) هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ـ مسئولیت کیفری اشخاص

ماده (۱۹) در موارد زیر، چنانچه جرایم رایانه ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کند و جرم بوقوع پیوندد.

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

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یافته باشد.

تبصره ۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی را دارد.

تبصره ۲ـ مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

ماده (۲۰) 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 ۱ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

تبصره ۲ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. در صورتی که اموال شخص حقوقی به تنهایی تکافو نکند، مابه التفاوت از اموال مرتکب جبران خواهد شد.

ماده (۲۱) ارائه دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیته تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه اعم از محتوای ناشی از جرایم رایانه ای و محتوایی که برای ارتکاب جرایم رایانه ای بکار می‌رود را پالایش کنند. در صورتی که عمداً از پالایش محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی احتیاطی و بی مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست تا یکصد میلیون ریال و در مرتبه دوم به جزای نقدی از یکصد میلیون تا یک میلیارد ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره «۱» چنانچه محتوای مجرمانه به وب سایت های مؤسسات عمومی شامل نهادهای زیر نظر ولی فقیه 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 شناخته شده 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 قضایی رسیدگی کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، وب سایت مزبور تا صدور حکم نهایی پالایش نخواهد شد.

تبصره «۲» پالایش محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضایی رسیدگی کننده به پرونده انجام خواهد شد.

ماده (۲۲) قوه قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کمیته تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نماینده وزارتخانه های 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 نماینده مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و قضایی و تأیید مجلس شورای اسلامی اعضای کمیته را تشکیل خواهند داد. ریاست کمیته به عهده دادستان کل کشور خواهد بود.

تبصره ۱- جلسات کمیته حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو دارای حق رأی رسمیت می‌یابد و تصمیمات کمیته با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره ۲- کمیته موظف است به شکایات راجع به مصادیق پالایش شده رسیدگی و نسبت به آنها تصمیم‌گیری کند. رأی کمیته قطعی است.

تبصره ۳- کمیته موظف است هر شش ماه گزارشی در خصوص روند پالایش محتوای مجرمانه را به رؤسای قوای سه‌گانه و شورای عالی امنیت ملی تقدیم کند.

ماده (۲۳) ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کمیته تعیین مصادیق مذکور در ماده فوق یا مقام قضایی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سیستم های رایانه ای خود از ادامه دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کمیته یا مقام قضایی 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 تا یکصد میلیون ریال و در مرتبه دوم به یکصد میلیون تا یک میلیارد ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ــ ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کمیته تعیین مصادیق اطلاع دهند.

ماده (۲۴) هرکس بدون مجوز قانونی از پهنای باند بین المللی 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 تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ــ سایر جرائم

ماده (۲۵) هرکس مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع یا معامله داده ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفاً بـه منظـور ارتکـاب جرائم رایانه ای به کار می روند.

ب) فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده ای که امکـان دسترسـی غیرمجـاز بـه داده هـا یـا سیستم های رایانه ای یا مخابراتی متعلق به دیگری را فراهم می کند.

ج) آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی.

تبصره ــ چنانچه مرتکب اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در ایـن مـاده محکوم خواهد شد.

فصل هشتم ــ تشدید مجازات‌ها

ماده (۲۶) در موارد زیر، حسب مورد مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها و یا شهرداری‌ها و موسسه‌ها و شرکت‌های دولتـی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی کـه زیـر نظـر ولـی فقیـه اداره مـی‌شـوند و دیـوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به طـور کلـی اعضـا و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه های رایانه ای یا مخابراتی که به مناسبت شغل خـود مرتکـب جـرم رایانـه ای شده باشد.

ج) داده ها یا سیستم های رایانه ای یا مخابراتی، متعلق به دولت یا نهادها و مراکـز ارایـه دهنـده خـدمات عمـومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

هـ) جرم در سطح گسترده ای ارتکاب یافته باشد.

ماده (۲۷) در صورت تکرار جرم برای بیش از دو بار دادگاه می‌توانـد مرتکـب را از خـدمات الکترونیکـی عمـومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک 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 ــ آیین دادرسی**

فصل یکم ــ صلاحیت

ماده (۲۸) علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیـر نیـز صـالح بـه رسـیدگی خواهند بود:

الف) داده های مجرمانه یا داده هایی که برای ارتکاب جرم به کار رفته‌اند به هر نحـو در سیسـتم هـای رایانـه ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیـره شـده باشد.

ب) جرم از طریق وب سایت های دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سیستم های رایانـه ای و مخـابراتی و وب سـایت هـای مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا موسسه ای که خدمات عمومی ارائه می‌دهد یا علیه وب سایت های دارای دامنه مرتبه بالای کد کشوری ایـران در سـطح گسـترده ارتکاب یافته باشد.

د) جرایم رایانه ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکـه مرتکـب یـا بـزه دیـده ایرانـی یـا غیرایرانی باشد.

ماده (۲۹) چنانچه جرم رایانه ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محـل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشـخص نشـود، دادسـرا پـس از اتمـام تحقیقات مبادرت به صدور قرار می کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده (۳۰) قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگـاه هـای عمـومی و انقـلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.

تبصره ــ قضات دادسراها و دادگاه های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخـاب خواهنـد شد.

ماده (۳۱) در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهد بود.

فصل دوم ــ جمع آوری ادله الکترونیکی

مبحث اول ــ نگهداری داده ها

ماده (۳۲) ارائه دهندگان خدمات دسترسی موظفند داده ای ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعـات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره ۱ــ داده ترافیک هرگونه داده ای است که سیستم های رایانه ای در زنجیره ارتباطـات رایانـه ای و مخـابراتی تولید می‌کنند تا امکان ردیابی آنها از مبداء تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیـل مبـداء، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

تبصره ۲ــ 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 IP، شماره تلفن و سایر مشخصات فردی اوست.

ماده (۳۳) 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 ــ حفظ فوری داده های رایانه ای ذخیره شده

ماده (۳۴) هرگاه حفظ داده ای رایانه ای ذخیره شده برای تحقیق یا دادرسی لازم باشـد، مقـام قضـایی مـی‌توانـد دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیـر

خطر آسیب دیدن یا تغییر یا از بین رفتن داده ها، ضابطان قضایی می توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضایی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضایی یا سایر اشخاص از اجرای این دستور خودداری یا داده ای حفاظت شده را افشا کنند یا اشخاصی که داده ای مزبور به آنها مربوط می شود را از مفاد دستور صادره آگاه کنند، ضابطان قضایی و کارکنان دولت به مجازات امتناع از دستور مقام قضایی و سایر اشخاص به حبس از نود و یک روز تا شش ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات محکوم خواهند شد.

تبصره ۱ـ حفظ داده ها به منزله ارائه یا افشای آنها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره ۲ـ مدت زمان حفاظت از داده ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضایی قابل تمدید است.

مبحث سوم ـ ارائه داده ها

ماده (۳۵) مقام قضایی می‌تواند دستور ارائه داده ای حفاظت شده مذکور در مواد (۳۲)، (۳۳) و (۳۴) فوق را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. مستنکف از اجرای این دستور به مجازات مقرر در ماده (۳۴) محکوم خواهد شد.

مبحث چهارم ـ تفتیش و توقیف داده ها و سیستم های رایانه ای و مخابراتی

ماده (۳۶) تفتیش و توقیف داده ها یا سیستم های رایانه ای و مخابراتی به موجب دستور قضایی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده (۳۷) تفتیش و توقیف داده ها یا سیستم های رایانه ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سیستم‌ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده (۳۸) دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجرای صحیح آن کمک می کند، از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده ای مورد نظر، نوع و تعداد سخت افزارها و نرم افزارها، نحوه دستیابی به داده ای رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده (۳۹) تفتیش داده ها یا سیستم های رایانه ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف) دسترسی به تمام یا بخشی از سیستم های رایانه ای یا مخابراتی.

ب) دسترسی به حامل های داده از قبیل دیسکت ها یا لوح های فشرده یا کارت‌های حافظه.

ج) دستیابی به داده ای حذف یا رمزنگاری شده.

ماده (۴۰) در توقیف داده ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده ها، کپی برداری یا تصویربرداری از تمام یا بخشی از داده ها، غیرقابل دسترس کردن داده ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل های داده عمل می‌شود.

ماده (۴۱) در شرایط زیر سیستم های رایانه ای یا مخابراتی توقیف خواهند شد:

الف) داده ای ذخیره شده به سهولت در دسترسی نبوده یا حجم زیادی داشته باشد،

ب) تفتیش و تجزیه و تحلیل داده ها بدون سیستم سخت افزاری امکان‌پذیر نباشد،

ج) متصرف قانونی سیستم رضایت داده باشد،

د) کپی برداری از داده ها به لحاظ فنی امکان‌پذیر نباشد،

هـ) تفتیش در محل باعث آسیب داده ها شود،

و) سایر شرایطی که قاضی تشخیص دهد.

ماده (۴۲) توقیف سیستم های رایانه ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل تغییر گذرواژه به منظور عدم دسترسی به سیستم، پلمپ سیستم در محل استقرار و ضبط سیستم صورت می‌گیرد.

ماده (۴۳) چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده های مرتبط با جرم ارتکابی در سایر سیستم های رایانه ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سیستم های دیگر گسترش خواهند داد و داده های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده (۴۴) توقیف داده ها یا سیستم های رایانه ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی می شود ممنوع است.

ماده (۴۵) در جایی که اصل داده ها توقیف می شود، ذی‌نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده ای توقیف شده منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه ای وارد نسازد و داده ها مجرمانه نباشند.

ماده (۴۶) در مواردی که اصل داده ها یا سیستم های رایانه ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده ها و نوع و تعداد سخت افزارها و نرم افزارهای مورد نظر و نقش آنها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

ماده (۴۷) متضرر می‌تواند در مورد عملیات و اقدام‌های مأموران در توقیف داده ها و سیستم های رایانه ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستور دهنده تسلیم نماید. به درخواست یاد شده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

مبحث پنجم ـ شنود محتوای ارتباطات رایانه ای

ماده (۴۸) شنود محتوای در حال انتقال ارتباطات غیرعمومی در سیستم های رایانه ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

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

فصل سوم ـ استنادپذیری ادله الکترونیکی

ماده (۴۹) به منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع آوری شده، لازم است مطابق آیین‌نامه مربوط از آنها نگهداری و مراقبت به عمل آید.

ماده (۵۰) چنانچه داده ای رایانه ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سیستم رایانه ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده ها خدشه وارد نشده باشد، قابل استناد خواهند بود.

ماده (۵۱) کلیه مقررات مندرج در فصل های دوم و سوم این بخش، علاوه بر جرایم رایانه ای شامل سایر جرایمی که ادله الکترونیکی در آنها مورد استناد قرار می‌گیرند نیز می شود.

- **بخش سوم ـ سایر مقررات**

ماده (۵۲) به منظور ارتقای همکاری‌های بین المللی در زمینه جرائم رایانه ای، وزارت دادگستری موظف است با همکاری وزارت ارتباطات و فناوری اطلاعات اقدامات لازم را در زمینه تدوین لوایح و پیگیری امور مربوط جهت پیوستن ایران به اسناد بین المللی و منطقه‌ای و معاهدات راجع به همکاری و معاضدت دوجانبه یا چندجانبه قضایی انجام دهد.

ماده (۵۳) در مواردی که سیستم رایانه ای یا مخابراتی به عنوان وسیله ارتکاب جرم بکار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد.

تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرایم رایانه ای مقررات خاصی از جهت آیین دادرسی پیش‌بینی نشده است طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد.

ماده (۵۴) میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضاییه و تصویب هیأت وزیران قابل تغییر است.

ماده (۵۵) وزارت دادگستری موظف است ظرف شش ماه از تاریخ تصویب این قانون با همکاری وزارت ارتباطات و فناوری اطلاعات آئین نامه های مربوط به جمع آوری و استنادپذیری ادله الکترونیکی را تهیه کند و به تصویب رئیس قوه قضائیه خواهد رسید.

ماده (۵۶) قوانین و مقررات مغایر با این قانون ملغی است.

تاریخ تصویب: ۱۱/۱۱/۱۳۸۸