

شماره 16306/121

۱۳۸۸/۴/۳

قانون جرائم رایانه ای

جناب آقای دکتر محمود احمدی نژاد

ریاست محترم جمهوری اسلامی ایران

عطف به نامه شماره 21953/32871 مورخ 13/4/1384 در اجراء اصل یکصد و بیست و سوم (123) قانون اساسی جمهوری اسلامی ایران قانون جرائم رایانه ای که با عنوان لایحه به مجلس شورای اسلامی تقدیم گردیده بود با تصویب در جلسه علنی روز سه شنبه مورخ 5/3/1388 و تأیید شورای محترم نگهبان، به پیوست ابلاغ می گردد.

رئیس مجلس شورای اسلامی - علی لاریجانی

10/4/1388

شماره 71063

وزارت دادگستری

قانون جرایم رایانه ای که در جلسه علنی روز سه شنبه مورخ پنجم خرداد ماه یکهزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ 20/3/1388 به تأیید شورای نگهبان رسیده و طی نامه شماره 16306/121 مورخ 3/4/1388 مجلس شورای اسلامی واصل گردیده است، به پیوست جهت اجرا ابلاغ می گردد.

رئیس جمهور - محمود احمدی نژاد

قانون جرائم رایانه ای

بخش یکم - جرائم و مجازات ها

فصل یکم - جرائم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم - دسترسی غیرمجاز

ماده 1- هرکس به طور غیرمجاز به داده ها یا سامانه 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 میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

مبحث دوم - شنود غیرمجاز

ماده 2- هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم - جاسوسی رایانه ای

ماده 3- هر کس به طور غیرمجاز نسبت به داده های سری درحال انتقال یا ذخیره شده در سامانه های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به مجازات های مقرر محکوم خواهد شد:

الف) دسترسی به داده های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (20.000.000) ریال تا شصت میلیون (60.000.000) ریال یا هر دو مجازات.

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

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

تبصره 1- داده های سری داده هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می زند.

تبصره 2- آیین نامه نحوه تعیین و تشخیص داده های 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 هیأت وزیران خواهد رسید.

ماده 4- هرکس به قصد دسترسی به داده های سری موضوع ماده (3) این قانون، تدابیر امنیتی سامانه های رایانه ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 5- چنانچه مأموران دولتی که مسئول حفظ داده های سری مقرر در ماده (3) این قانون یا سامانه های مربوط هستند و به آنها آموزش لازم داده شده است یا داده ها یا سامانه 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 سامانه های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم - جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم - جعل رایانه ای

ماده 6- هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (20.000.000) ریال تا یکصد میلیون (100.000.000) ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر یا ایجاد داده های قابل استناد یا ایجاد یا واردکردن متقلبانة داده به آنها.

ب) تغییر داده ها یا علائم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانة داده ها یا علائم به آنها.

ماده 7- 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 - تخریب و اخلال در داده ها یا سامانه های رایانه ای و مخابراتی

ماده 8- هرکس به طور غیرمجاز داده های دیگری را از سامانه 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 میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 9- هر کس به طور غیرمجاز با اعمالی از قبیل واردکردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده ها یا امواج الکترومغناطیسی یا نوری، سامانه 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 میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 10- هرکس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده ها، تغییر گذر واژه یا رمزنگاری داده ها مانع دسترسی اشخاص مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 11- هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (8)، (9) و (10) این قانون را علیه سامانه های رایانه ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می روند، 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 - سرقت و کلاهبرداری مرتبط با رایانه

ماده 12. هرکس به طور غیرمجاز داده های متعلق به دیگری را برآید، چنانچه عین داده ها در اختیار صاحب آن باشد، به جرای نقدی از یک میلیون (1.000.000) ریال تا بیست میلیون (20.000.000) ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 13. هرکس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها 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 (20.000.000) ریال تا یکصد میلیون (100.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم - جرائم علیه عفت و اخلاق عمومی

ماده 14. هرکس به وسیله سامانه های رایانه ای یا مخابراتی یا حامل های 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 (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

تبصره 1. ارتکاب اعمال فوق درخصوص 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 و صور قبیحه باشد.

تبصره 2. هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون (1.000.000) ریال تا پنج میلیون (5.000.000) ریال جزای نقدی محکوم خواهد شد.

تبصره 3. چنانچه مرتکب اعمال مذکور در این ماده را حرفه خود قرار داده باشد یا به طور سازمان یافته مرتکب شود چنانچه مفسد فی الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره 4. محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده 15. هرکس از طریق سامانه 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، 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 (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون (2.000.000) ریال تا پنج میلیون (5.000.000) ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز 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 (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم می شود.

تبصره - مفاد این ماده و ماده (14) 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 می شود.

فصل پنجم - هتک حیثیت و نشر اکاذیب

ماده 16- هرکس به وسیله سامانه 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 میلیون (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

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

ماده 17- هر کس به وسیله سامانه های رایانه ای 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 (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

ماده 18- هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه ای 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 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 (در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم - مسؤولیت کیفری اشخاص

ماده 19. در موارد زیر، چنانچه جرائم 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 به وقوع بپیوندد.

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

تبصره 2. مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسئول خواهد بود.

ماده 20. اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و احوال جرم ارتكابی، میزان درآمد و نتایج حاصله از ارتكاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتكابی، 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 سه 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 - 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 دیگر را نخواهد داشت.

ماده 21. ارائه دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل

محتوای مجرمانه که در چارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه ای و محتوایی که برای ارتکاب جرائم رایانه ای به کار می رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی احتیاطی و بی مبالاتی زمینه دسترسی به محتوای غیر قانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون (20.000.000) ریال تا یکصد میلیون (100.000.000) ریال و در مرتبه دوم به جزای نقدی از یکصد میلیون (100.000.000) ریال تا یک میلیارد (1.000.000.000) ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره 1- چنانچه محتوای مجرمانه به تارنماهای (وب سایت های) مؤسسات عمومی شامل نهادهای زیر نظر ولی فقیه و قوای سه گانه مقننه، مجریه و قضاییه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب 19/4/1373 و الحاقات بعدی آن یا به احزاب، جمعیت ها، انجمن های سیاسی و صنفی و انجمن های اسلامی یا اقلیت های 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، تارنما (وب سایت) مزبور تا صدور حکم نهایی پالایش (فیلتر) نخواهد شد.

تبصره 2- پالایش (فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضایی رسیدگی کننده به پرونده انجام خواهد گرفت.

ماده 22- 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 وزارتخانه های آموزش و پرورش، ارتباطات و فناوری 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 قضایی و حقوقی به انتخاب کمیسیون قضایی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه (کمیته) را تشکیل خواهند داد. ریاست کارگروه (کمیته) به عهده دادستان کل کشور خواهد بود.

تبصره 1- جلسات کارگروه (کمیته) حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو رسمیت می یابد و تصمیمات کارگروه (کمیته) با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره 2- کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آنها تصمیم گیری کند.

تبصره 3- کارگروه (کمیته) موظف است هر شش ماه گزارشی در خصوص روند پالایش (فیلتر) محتوای مجرمانه را به رؤسای قوای سه گانه و شورای عالی امنیت ملی تقدیم کند.

ماده 23- ارائه دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در ماده فوق یا مقام قضایی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه های رایانه ای خود از ادامه دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای

دستور کارگروه (کمیته) یا مقام قضایی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی احتیاطی و بی مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخست به جزای نقدی از بیست میلیون (20.000.000) ریال تا یکصد میلیون (100.000.000) ریال و در مرتبه دوم به یکصد میلیون (100.000.000) ریال تا یک میلیارد (1.000.000.000) ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره - ارائه دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه (کمیته) تعیین مصادیق اطلاع دهند.

ماده 24. 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 (100.000.000) ریال تا یک میلیارد (1.000.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم - سایر جرائم

ماده 25. هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه ای به کار می رود.

ب) فروش یا انتشار یا در دسترس قراردادن گذر واژه یا هر داده ای که امکان دسترسی غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می کند.

ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای و تخریب و اخلاف در داده ها یا سیستم های رایانه ای و مخابراتی.

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

فصل هشتم - تشدید مجازات ها

ماده 26. 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 اداره ها و سازمان ها یا شوراها و یا شهرداری ها و موسسه ها و شرکت های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه هایی که زیر نظر ولی فقیه اداره می شوند و دیوان محاسبات و مؤسسه هایی که با کمک مستمر دولت اداره می شوند و یا دارندگان پایه قضایی و به طور کلی اعضاء و کارکنان قوای سه گانه 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 خود مرتکب جرم رایانه ای شده باشد.

ج) داده ها یا سامانه های رایانه ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

ه) جرم در سطح گسترده ای ارتکاب یافته باشد.

ماده 27. در صورت تکرار جرم برای بیش از دو بار دادگاه می تواند 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 - آیین دادرسی

فصل یکم - صلاحیت

ماده 28. علاوه بر موارد پیش بینی شده در دیگر قوانین، دادگاه های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده های مجرمانه یا داده هایی که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه های رایانه ای و مخابراتی یا حامل های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنماهای (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 سامانه های رایانه ای و مخابراتی و تارنماهای (وب سایت های) مورد استفاده یا تحت کنترل قوای سه گانه یا نهاد رهبری یا نمایندگی های رسمی دولت یا هر نهاد یا مؤسسه ای که خدمات عمومی ارائه می دهد یا علیه تارنماهای (وب سایت های) دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیرایرانی باشد.

ماده 29. چنانچه جرم رایانه ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادرای پس از اتمام تحقیقات مبادرت به صدور قرار می کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده 30. قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادرایها، دادگاه های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.

تبصره - قضات دادرایها و دادگاه های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد.

ماده 31 - در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی دادگاه های عمومی و انقلاب در امور مدنی خواهد بود.

فصل دوم - جمع آوری ادله الکترونیکی

مبحث اول - نگهداری داده ها

ماده 32. ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره 1. داده ترافیک هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

تبصره 2. 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.

ماده 33. ارائه دهندگان 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 - حفظ فوری داده های رایانه ای ذخیره شده

ماده 34. هرگاه حفظ داده های رایانه ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر 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 24 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 های حفاظت شده را افشاء کنند یا اشخاصی که داده های 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 نودویک روز تا شش ماه یا جزای نقدی از پنج میلیون (5.000.000) ریال تا ده میلیون (10.000.000) ریال یا هر دو مجازات محکوم خواهند شد.

تبصره 1 - حفظ داده ها به منزله ارائه یا افشاء آنها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره 2. مدت زمان حفاظت از داده ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضایی قابل تمدید است.

مبحث سوم - ارائه داده ها

ماده 35. مقام قضایی می تواند دستور ارائه داده های حفاظت شده مذکور در مواد (32)، (33) و (34) فوق را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرارگیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (34) این قانون محکوم خواهد شد.

مبحث چهارم - تفتیش و توقیف داده ها و سامانه های رایانه ای و مخابراتی

ماده 36. تفتیش و توقیف داده ها یا سامانه های رایانه ای و مخابراتی به موجب دستور قضایی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده 37. تفتیش و توقیف داده ها یا سامانه های رایانه ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده 38. دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجراء صحیح آن کمک می کند، از جمله اجراء دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده های مورد نظر، نوع و تعداد سخت افزارها و نرم افزارها، نحوه دستیابی به داده های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده 39. تفتیش داده ها یا سامانه های رایانه ای و مخابراتی شامل اقدامات ذیل می شود:

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

ب) دسترسی به حامل های داده از قبیل دیسکت ها یا لوحه ای فشرده یا کارت های حافظه.

ج) دستیابی به داده های حذف یا رمزنگاری شده.

ماده 40. در توقیف داده ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش هایی از قبیل چاپ داده ها، کپی برداری یا تصویربرداری از تمام یا بخشی از داده ها، غیر قابل دسترس کردن داده ها با روش هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل های داده عمل می شود.

ماده 41. در هریک از موارد زیر سامانه های رایانه ای یا مخابراتی توقیف خواهد شد:

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

ب) تفتیش و تجزیه و تحلیل داده ها بدون سامانه سخت افزاری امکان پذیر نباشد،

ج) متصرف قانونی سامانه رضایت داده باشد،

د) تصویربرداری (کپی برداری) از داده ها به لحاظ فنی امکان پذیر نباشد،

ه) تفتیش در محل باعث آسیب داده ها شود،

ماده 42- توقیف سامانه های رایانه ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش هایی از تغییر گذرواژه به منظور عدم دسترسی به سامانه، پلمپ سامانه در محل استقرار و ضبط سامانه صورت می گیرد.

ماده 43- چنانچه در حین اجراء دستور تفتیش و توقیف، تفتیش داده های مرتبط با جرم ارتكابی در سایر سامانه های رایانه ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارد ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سامانه های مذکور گسترش داده و داده های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده 44- چنانچه توقیف داده ها یا سامانه های رایانه ای یا مخابراتی موجب ایراد لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلاف در ارائه خدمات عمومی شود ممنوع است.

ماده 45- در مواردی که اصل داده ها توقیف می شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به این که ارائه داده های توقیف شده مجرمانه یا منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه ای وارد نشود.

ماده 46- در مواردی که اصل داده ها یا سامانه های رایانه ای یا مخابراتی توقیف می شود، قاضی موظف است با لحاظ نوع و میزان داده ها و نوع و تعداد سخت افزار ها و نرم افزار های مورد نظر و نقش آنها در جرم ارتكابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

ماده 47- متضرر می تواند در مورد عملیات و اقدام های مأموران در توقیف داده ها و سامانه های رایانه ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستوردهنده تسلیم نماید. به درخواست یاد شده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

مبحث پنجم - شنود محتوای ارتباطات رایانه ای

ماده 48- شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

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

فصل سوم - استناد پذیری ادله الکترونیکی

ماده 49 - به منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع آوری شده، لازم است مطابق آیین نامه مربوط از آنها نگهداری و مراقبت به عمل آید.

ماده 50 - چنانچه داده های رایانه ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سامانه 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 خواهد بود.

ماده 51 - کلیه مقررات مندرج در فصل های دوم و سوم این بخش، علاوه بر جرائم رایانه ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می گیرد نیز می شود.

بخش سوم - سایر مقررات

ماده 52 - در مواردی که سامانه رایانه ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد.

تبصره - در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه ای مقررات خاصی از جهت آیین دادرسی پیش بینی نشده است طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد.

ماده 53 - میزان جزا های 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 54 - آیین نامه های مربوط به جمع آوری 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 قضاییه خواهد رسید.

ماده 55 - شماره مواد (1) تا (54) این قانون به عنوان مواد (729) تا (782) قانون مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرائم رایانه ای منظور و شماره ماده (729) قانون مجازات اسلامی به شماره (783) اصلاح گردد.

ماده 56 - قوانین و مقررات مغایر با این قانون ملغی است.

قانون فوق مشتمل بر 56 ماده و 25 تبصره در جلسه علنی روز سه شنبه مورخ پنجم خرداد ماه یک هزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ 20/3/1388 به تأیید شورای نگهبان رسید.

رئیس مجلس شورای اسلامی - علی لاریجانی