**به نام خدا**

**جزوه**

قانون جرایم رایانه ای

**تدوین**

**مدیریت حراست سازمان جهاد کشاورزی استان اصفهان**

**زمستان 1392**

****

**فهرست**

**فهرست صفحه**

**مقدم 4**

1. **بخش یکم ـ جرائم و مجازات‌ها 7**
   1. **فصل یکم ـ‌ جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی 7**
   2. **فصل دوم ـ جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی 8**
   3. **فصل سوم ـ‌ سرقت و کلاهبرداری مرتبط با رایانه 9**
   4. **فصل چهارم ـ جرایم علیه عفت و اخلاق عمومی 9**
   5. **فصل پنجم ـ هتک حیثیت و نشر اکاذیب 10**
   6. **فصل ششم ـ مسئولیت کیفری اشخاص 11**
   7. **فصل هفتم- سایر جرایم 13**
   8. **فصل هشتم- تشدید مجازات ها 13**

**2 - بخش دوم- آئین دادرسی 15**

**2-1- فصل یکم- صلاحیت 15**

**2-2- فصل دوم- جمع آوری ادله الکترونیکی 16**

**2-3- فصل سوم- استناد پذیری ادله الکترونیکی 19**

**3-بخش سوم- سایر مقررات 20**

**4- منابع 21**

**مقدمه:**

**محیط سایبر cyberspace محیطی است مجازی و غیر ملموس در فضای شبکه های بین المللی (این شبکه ها از طریق شاهراه های اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ ها، ملت ها، کشورها و به طور کلی هر آن چه در کره ی خاکی به صورت فیزیکی ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) بوده و در این محیط کاربران می توانند به هرگونه خدمات اطلاعاتی الکترونیکی دست پیدا کنند، بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه ای دنیا واقع شده است. محدوده ی 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 می تواند در هر زمانی و در هر مکانی با مردم در هر نقطه ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد.**

**از سوی دیگر امنیت ناکافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را جهت ارتکاب جرم های رایانه ای از جمله : از بین بردن، خراب کردن، دزدی اطلاعات، کلاه برداری های الکترونیکی، سوء استفاده از تجهیزات، جا زدن خود به جای کس دیگر و اخلال در سیستم ها در اختیار افرد شرور قرار می دهد.**

**یک عمل خلاف یارانه ای لزوماً وارد کردن خسارت فیزیکی به یک تجهیزات یا یک سیستم نیست، بلکه گاه فقط دسترسی به بعضی اطلاعات حساس یا محرمانه می تواند جرم باشد. این اطلاعات می تواند اطلاعات خصوصی یا فردی باشد که این روزها این گونه اعمال خلاف روبه افزایش است و تنوع آن هم روز به روز بیشتر می شود. نگران کننده ترین جنبه ی فضای سایبر انتشار سریع اطلاعات در آن می باشد، مثلاً در لحظه ی کوتاهی قسمتی از اطلاعاتی که می تواند به طور بالقوه مورد سوء استفاده قرار گیرد، کشف می شود.**

**جرایم رایانه ای عبارت است از استفاده غیر مجاز از فن آوری رایانه ای برای به دست گرفتن اطلاعات شخصی حساس و همین طور اطلاعات محرمانه سازمان ها. هر چند این جرم ها را با چشم نمی توان دید، ولی در بعضی موارد ممکن است خطرات بی شماری را به وجود آورند که ممکن است سالیان سال نتوان آنها را جبران کرد.**

**تاریخچه موضوع و سیر تحول آن:**

**در عرصه ی بین المللی در زمینه ی جرایم رایانه ای می توان به اقدامات زیر اشاره نمود:**

**-تصویب موافقت نامه جرایم یارانه ای در سال 1985-1986 توسط شورای اروپا.**

**- در سال 1989 کمیته ی تخصصی شورای اروپا برای تدوین و یکنواخت نمودن سیاست جنایی مربوط به جرایم رایانه ی پیشنهادهایی نمود، که مورد تصویب شورا قرار گرفت.**

**- در سال 1994 انجمن بین المللی حقوق جزا یک سری مسائل را به عنوان جرایم یارانه ای مستقل تدوین نمود.**

**- در سال 2001 میلادی شورای اروپا، موافقت نامه جرایم رایانه ای را تدوین نمود، که این موافقت نامه شامل 4 فصل و 48 گفتار می باشد.**

**انواع جرایم یارانه ای**

**جرایم رایانه ای را می توان به سه دسته تقسیم نمود:**

**دسته اول: جرایمی هستند که در آن ها رایانه و تجهیزات جانبی آن موضوع جرم واقعی می شوند. مانند سرقت، تخریب و غیره**

**دسته دوم: جرایمی هستند که در آن ها یارانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می شود.**

**دسته سوم: جرایمی هستند که می توان آن ها را جرایم رایانه ای محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند. آما آثار آن ها در دنیای واقعی ظاهر می شود. مانند دسترسی غیر مجاز به سیستم های رایانه ای.**

**در یک تقسیم بندی کلی می توان جرایم یارانه ای را به شرح ذیل احصاء نمود:**

**الف: جرایم سنتی شامل: جاسوسی، سابوتاژ، جعل یارانه ای، کلاهبرداری، تخریب، افتراء، پولشویی و قاچاق مواد مخدر**

**ب: جرایم ناظر به کپی رایت برنامه ها شامل: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش و استفاده ای غیر مجاز از برنامه های رایانه ای ( سرقت نرم افزار)**

**ج: جرایم علیه حمایت از داده ها**

**د: جرایم در تجارت الکترونیکی**

**ه: جرایم در بانکداری الکترونیک و جرایم مخابراتی و ماهواره ای**

**ز: جرایم اطفال و زنان**

**ح: ترور سایبر**

**جزوه حاضر جهت اطلاع از جرائم، مجازت ها و آئین دادرسی تخلفات ریانه ای تنظیم گردیده است، امید است همکاران گرامی با مطالعه و نظارت جهت رعایت این نکات اهتمام ورزیده و نسبت به اشاعه آن در محیط های کاری خود برای به حداقل رسانیدن آسیب ها و تهدیدات و افزایش فرصت ها و منافع ملی در زمینه جرایم رایانه ای اقدام نمایند.**

**بخش یکم ـ جرائم و مجازات‌ها**

**فصل یکم ـ‌ جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی**

‎‎‎**مبحث یکم ـ دسترسی غیرمجاز**

‎‎‎ماده (1) هرکس به طور غیرمجاز به داده‎ها یا سیستم‎های رایانه‎ای 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 (2) هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‎های رایانه‎ای 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 رایانه‎ای**

‎‎‎ماده (3) هرکس به طور غیرمجاز نسبت به داده‎های سری در حال انتقال یا ذخیره شده در سیستم‎های رایانه‎ای یا مخابراتی یا حامل‎های داده مرتکب اعمال زیر شود،‌ به مجازات‎های مقرر محکوم خواهد شد:  
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 تا شصت میلیون ریال یا هر دو مجازات.  
ب) در دسترس قرار دادن داده‎های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.  
ج) افشا یا در دسترس قرار دادن داده‎های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.  
تبصره 1ـ داده‎های سری داده‎هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‎زند.  
تبصره 2ـ آئین‎نامه نحوه تعیین و تشخیص داده‎های سری و نحوه طبقه‎بندی و حفاظت آن‌ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارت‎خانه‎های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت دولت خواهد رسید.

ماده (4) هرکس به قصد دسترسی به داده‎های سری موضوع ماده (3) این قانون،‌ تدابیر امنیتی سیستم‎های رایانه‎ای 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 (5) چنانچه مأموران دولتی که مسؤول حفظ داده‎های سری مقرر در ماده (3) این قانون یا سیستم‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سیستم‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‎احتیاطی، بی‎مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‎ها، حامل‎های داده یا سیستم‎های 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 داده‌ها و سیستم‌های رایانه‌ای و مخابراتی**

**مبحث یکم ـ جعل رایانه‎ای**

ماده (6) 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 داده‎های قابل استناد یا ایجاد یا وارد کردن متقلبانة داده‎ها،  
ب) تغییر داده‎ها یا علایم موجود در کارت‎های حافظه یا قابل پردازش در سیستم‌های رایانه‎ای یا مخابراتی یا تراشه‎ها یا ایجاد یا وارد کردن متقلبانة داده‎ها یا علایم به آنها.

ماده (7) هرکس با علم به مجعول بودن داده‎ها یا کارت‎ها یا تراشه‎ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

‎‎‎**مبحث دوم ـ تخریب و اخلال در داده‎ها یا سیستم‎های رایانه‎ای و مخابراتی**

ماده (8) هر کس به طور غیرمجاز داده‎های دیگری را از سیستم‎های 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (9) هر کس به طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‎ها یا امواج الکترومغناطیسی یا نوری، سیستم‎های 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (10) هرکس به طور غیرمجاز با انجام اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‎ها یا سیستم‎های رایانه‎ای 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 (11) هرکس به قصد به خطر انداختن امنیت یا آسایش عمومی اعمال مذکور در مواد (8)، (9) و (10) این قانون را علیه سیستم‌های رایانه‌ای و مخابراتی که برای ارائة 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 (12) هرکس به طور غیرمجاز داده‎های متعلق به دیگری را برباید، چنانچه عین داده‌ها 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 (١٣) هرکس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‎ها 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 (١٤) هرکس به وسیله سیستم‎های رایانه‎ای 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 1 ـ ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازات های فوق می شود. محتویات وآثار مبتذل به آثاری اطلاق می گردد که دارای صحنه ها وصور قبیحه باشد.  
تبصره 2 ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.  
تبصره 3 ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفة خود قرار داده باشد یا بطور سازمان‌یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.  
تبصره 4 ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی اطلاق می‎شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده (١٥) هرکس از طریق سیستم‎های 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 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 خشونت‎آمیز 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 (١٤) 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 (16) هرکس به وسیله سیستم‎های 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 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 (17) هرکس به وسیله سیستم‎های رایانه‎ای 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 (18) هر کس 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 (١٩) در موارد زیر، چنانچه جرایم رایانه‎ای 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 رایانه‎ای شود.  
ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‎ای 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 رایانه‎ای شود.  
د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‎ای اختصاص یافته باشد.  
تبصره ١ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‎گیری یا نظارت بر شخص حقوقی را دارد.  
تبصره ٢ـ مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

ماده (٢٠) 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 ١ـ 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 دیگری را نخواهد داشت.  
تبصره ٢ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. در صورتی که اموال شخص حقوقی به تنهایی تکافو نکند، مابه‎التفاوت از اموال مرتکب جبران خواهد شد.

ماده (٢١) ارائه‎دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیتة تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای بکار می‌رود را پالایش کنند. در صورتی که عمداً از پالایش محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‎احتیاطی و بی‎مبالاتی زمینة دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبة نخست به جزای نقدی از بیست تا یکصد میلیون ریال و در مرتبة دوم به جزای نقدی از یکصد میلیون تا یک میلیارد ریال و در مرتبة سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره 1 – چنانچه محتوای محرمانه به کارنمای ( وب سایت های ) موسسات عمومی شامل نهادهای زیر نظر ولی فقیه و قوای سه گانه مقننه، مجریه و قضائیه و موسسات عمومی غیر دولتی موضوع قانون فهرست نهادها و موسسات عمومی غیر دولتی مصوب 19/4/73 والحاقات بعدی آن یا به احزاب، جمعیتها، انجمن های سیاسی صنفی و انجمن های اسلامی یا اقلیتهای دینی شناخته شده یا به سایر اشخاص حقیقی یا حقوقی حاضر در ایران که اماکن احراز هویت و ارتباط با آنها وجود دارد تعلق داشته باشد.

**بادستور مقام قضائی رسیدگی کننده به پرونده و رفع اثر فوری محتوای محرمانه از سوی دارندگان تارنما (وب سایت) مزبور تا صدور حکم نهایی پالایش فیلتر نخواهد شد.**

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

**ماده 22- قوه قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کارگروه (کمیته) تعیین مصادیق محتوای محرمانه را در محل دادستای 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 از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تائید 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 یکبار 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 محرمانه را به روسای قوای سه گانه وشورای عالی امنیت ملی تقدیم کند.**

**ماده 23- ارائه دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در ماده فوق با مقام قضائی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه های رایانه ای خود از ادامه دسترسی به آن ممانعت به عمل آوردند چنانچه عمداً از اجرای دستور کار گروه (کمیته) یا مقام قضائی خودداری کنند منحل خواهند شد در غیر این صورت چننچه در اثر بی احتیاطی وبی مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند در مرتبه نخست به جزای نقدی از بیست میلیون (000/000/200) ریال تا یکصد میلیون (000/000/100) ریال و در مرتبه دوم به یکصد میلیون (000/000/100) ریال تا یک میلیارد (000/000/000/1) 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 با اجزای نقدی از یکصد میلیون (000/000/100) ریال تا یک میلیارد (000/000/000/1) ریال با هر دو مجازت محکوم خواهد شد.**

**فصل هفتم- سایر جرایم**

**ماده 25- هرشخصی که مرتکب اعمال زیر شود به حبس از نود یک روز تا یکسال با جزای نقدی از پنج میلیون (000/00/5) ریال تا بیست میلیون (000/00/20) ریال با هر دو مجازت محکوم خواهد شد.**

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

**ب- فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده ای که امکان دسترسی غیر مجاز به دادها 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 دسترسیغیر مجاز شوند غیر مجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی.**

**تبصره- چنانچه مرتکب اعمال یاد شده را حرفه خود قرارداده باشد به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد.**

**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 سازمانه ساشوراها و یا شهرداریها و موسسه ها و شرکتهای دولتی و یا وابسته به دولت یا نهاده های انقلابی و بنیادها و موسسه هایی که زیر نظر ولی فقیه اداره می شوند و دیوان محاسبات و موسسه 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 ماموران به خدمت عمومی اعم از رسمی و غیر رسمی 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 یارانه ای شده باشد.**

**ج- داده ها با سامانه های یارانهای یا مخابراتی، متعلق به دولت یا نهادها و رماکز ارائه دهنده خدمات عمومی باشد.**

**د- جرم به صورت سازمان یافته ارتکاب یافته باشد.**

**ه- جریم در سطح گسترده ای ارتکاب یافته باشد.**

**ماده 27- در صورتیکه تکرار جرم برای بیش از دوبار 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 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 سال تا پنج سال.**

**بخش دوم- آئین 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 بکاررفته است به هر نحو درسامانه های رایانه ای و مخابراتی با حاملهای داده موجود قلمرو حاکمیت زمینی دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.**

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

**د- جرائم رایانه ای متضمن سوء استفاده از اشخاص کمتر از هیجده سال، اعم از آنکه مرتکب یابزه دیده ایرانی یا غیر ایرانی باشد.**

**ماده 29- چنانچه جرم رایانه ای 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 می کند و دادگاه مربوط نیز رای مقتضی را صادر خواهد کرد.**

**ماده 30- قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاههای عمومی و انقلاب، نظامی و تجدید نظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.**

**تبصره- قضات دادسراها و دادگاههای 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 آئین 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 ها ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.**

**تبصره1- داده ترافیک هر گونه 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 مربوط می شود.**

**تبصره2- 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 کابران 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، ظابطان قضایی می توانند راسأ دستور حفاظت را صادر کنند و مراتب را حداکثر تا 24 ساعت به اطلاع مقام قضایی برسانند چنانچه هریک 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 صادر 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 میلیون (000/000/5) ریال تا ده میلیون (000/000/10) ریال با هر دو مجازات محکوم خواهند شد.**

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

**تبصره 2- مدت زمان حفاظت از داده ها حداکثر سه ماه است و در صورت لزوم دستور مقام قضائی 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 قرار گیرد مستنکف از اجزاء 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 با 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 یا 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 لوح فشرده یا کارتهای حافظه**

**ج- دستیابی به داده های حذف با 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 غیرقابل دسترس کردن داده ها با روشهایی از قبیل تغییر گذر واژه یا رمز نگاری و ضبط حاملهای 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 با حجم زیادی داشته باشد.**

**ب- تفتیش و تجزیه وتحلیل داده ها بدون سامانه سخت افزاری امکان پذیر نباشد.**

**ج- متصرف قانونی سامانه رضایت داده شده**

**د- تصویربرداری (کپی برداری) از داده ها به لحاظ فنی امکان پذیر نباشد.**

**ه- تفتیش در محل باعث آسیب داده 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 گذر واژه 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 جرم ارتکابی 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 اخلال در ارائه خدمات عمومی شود ممنوع است.**

**ماده 45- در مواردی که اصل داده ها توقیف می شود ذینفع 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 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 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 47- متضرر می تواند در مورد عملیات و اقدامهای ماموران در توقیف داده ها و امانه 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 نوب رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.**

**مبحث پنجم- شنود محتوای ارتباطات رایانه ای**

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

**تبصره- دسترسی به محتوای ارتباطات غیر عمومی ذخیره شده نظیر پست الکترونیکی با 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 انکار ناپذیری ادله الکترونیکی جمع آوری شده لازم است مطابق آئین 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 انکار پذیری 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 درآنها مورد استناد قرار می گیرد نیز می شود.**

**بخش سوم- سایر مقررات**

**ماده 52- در مواردی که سامانه ریانه 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 آئین دادرسی پیش بینی نشده است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.**

**ماده 53- میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است.**

**ماده 54- آئین نامه های مربوط به جمع آوری و استناد پذیری ادله الکترونیکی ظرف مدت شش ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.**

**ماده 55- شماره مواد (1) تا 54 این قانون به عنوان مواد 729 تا 782 قانون مجازات اسلامی (بخش تعزیزات) 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 خردادماه یک هزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ 20/3/88 به تائید شورای نگهبان رسید.**

**منابع:**

1. **سایت کارگروه تعیین مصادیق محتوای مجرمانه( internet.ir)**
2. **جزوه آموزشی جرایم رایانه ای اداره کل حراست وزارت جهاد کشاورزی**