لایحه قانون جرایم رایانه‌ای مصوب هیات دولت – تیرماه ۱۳۸٤

ارائه شده به مجلس شورای اسلامی

بخش نخست: کلیات

ماده ۱- تعریف‌ها:

الف) داده رایانه‌ای

هر نمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای پردازش در یک سیستم رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا گذارند.

ب) داده محتوا

هر نمادی از موضوع‌ها، مفهوم‌ها یا دستورالعمل‌ها نظیر متن، صوت یا تصویر، چه به صورت در جریان یا ذخیره شده که به‌منظور برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای بکار گرفته شده و بوسیلهٔ سیستم رایانه‌ای ایجاد شود.

ج) داده حاصل از مبادله داده محتوا

هرگونه داده‌ای که توسط رایانه ها در زنجیره ارتباطات تولید می‌شود تا ارتباطی را از مبدأ تا مقصد مسیریابی کند و شامل مبدأ ارتباط، مقصد ، مسیر، زمان، تاریخ، اندازه، مدت زمان و نوع خدمات اصلی و نظایرِ آن خواهد بود.

د) اطلاعات

عبارت است از داده های پردازش شده قابل فهم برای انسان یا سیستم های رایانه ای یا مخابراتی.

هـ) اطلاعات کاربر

هر گونه اطلاعاتی که در اختیار ارائه‌کننده خدمات باشد و مربوط به مشترک آن خدمات بوده و شامل نوع خدمات ارتباطی و پیش‌نیازهای فنی و دوره استفاده از آن خدمات، هویت مشترک، آدرس جغرافیایی یا پستی یا IP ، شماره تلفن و سایر مشخصات شخصی وی می باشد.

و) سیستم رایانه‌ای

هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت افزاری – نرم‌ا فزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده عمل می‌کند.

ز) سیستم مخابراتی

هرنوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد.

ح) ارائه دهنده خدمات دسترسی

هرشخص حقیقی یا حقوقی است که امکان ارتباط یا اتصال به اینترنت را برای کاربران فراهم می‌کند و عبارتند از :

۱- ایجاد کننده نقطه تماس بین‌المللی: ارائه دهنده خدمات دسترسی است که امکان ارتباط یا اتصال پر ظرفیت به اینترنت را از طریق سیستم‌های ارتباطی برای کاربران فراهم می‌کند.

۲- ارائه دهنده خدمات دسترسی کم‌ظرفیت: ارائه دهنده خدمات دسترسی است که به عنوان واسط میان ایجاد کننده نقطه تماس بین‌المللی و کاربران عمل می‌کند و امکان ارتباط یا اتصال به اینترنت را برای آنان فراهم می‌نماید.

۳- ارائه دهنده خدمات دسترسی حضوری: ارائه دهنده خدمات دسترسی است که امکان استفاده کاربران از اینترنت را به صورت حضوری در محلی معین فراهم می‌کند.

ط) ارائه دهنده خدمات میزبانی

هر شخص حقیقی یا حقوقی است که فضای لازم را برای ذخیره داده کابران فراهم می‌کند. ذخیرهٔ‌گذرای اطلاعات یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی ، خدمات میزبانی محسوب نمی‌شود.

ی) تدبیرهای حفاظتی:

عبارت است از به کارگیری روش های نرم افزاری یا سخت افزاری یا ترکیبی از آن دو، متناسب با نوع و اهمیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، به منظور جلوگیری از دسترسی بدون مجوز به آنها.

بخش دوم : جرایم ومجازاتها

فصل اول- جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث اول - دسترسی بدون مجوز

ماده ۲- هرکس به‌طور عمدی و بدون مجوز با نقض تدبیرهای حفاظتی داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی ، به آنها دسترسی یابد به جزای نقدی از پنج میلیون ریال تا پنجاه میلیون ریال محکوم خواهد شد.

مبحث دوم- شنود و دریافت بدون مجوز

ماده ۳- هرکس به‌طور عمدی و بدون مجوز داده‌های در حال انتقال در یک ارتباط خصوصی را در سیستم‌های رایانه‌ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری شنود یا دریافت نماید به جزای نقدی از پنج میلیون ریال تا سی میلیون ریال محکوم خواهد شد.

مبحث سوم: جرایم علیه امنیت

ماده ۴- هرکس به‌طور عمدی وبدون مجوز به داده‌های رایانه‌ای سرّی موجود در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده دسترسی یابد یا داده‌های رایانه‌ای سرّی در حال انتقال را شنود یا دریافت نماید به جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال محکوم خواهد شد.

تبصره ۱: داده‌های رایانه‌ای سرّی، داده هایی هستند که افشای بدون مجوز آنها می‌تواند به اساس و مبانی حکومت ضرر جبران‌ناپذیری وارد نماید و یا منافع عمومی و امنیت ملی را دچار مخاطره کند.

تبصره ۲: آئین‌نامه شیوه‌ی حفاظت وانتقال داده‌های رایانه‌ای سرّی ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری و با همکاری وزارتخانه‌های کشور ، اطلاعات ، ارتباطات وفناوری اطلاعات و دفاع وپشتیبانی نیروهای مسلح تهیه گشته و به تصویب هیأت وزیران خواهد رسید.

فصل دوم: جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث نخست: جعل

ماده ۵ – هرکس با قصد تقلب ، داده‌های رایانه‌ای قابل استناد یا داده‌های موجود در کارت‌های اعتباری یا مغناطیسی یا سایر علایم یا کدهای کارت‌های قابل پردازش و یا مورد استفاده در سیستم‌های رایانه‌ای یا مخابراتی را تغییر داده یا ایجاد یا حذف یا متوقف نماید جاعل محسوب وبه مجازات مقرر برای جعل محکوم خواهد شد و همچنین هرکس با علم به جعل و تزویر از آنها استفاده کند، به مجازات مقرر برای استفاده کننده محکوم خواهد شد.

مبحث دوم: تخریب وایجاد اختلال در داده‌ها

ماده ۶ – هرکس به‌طور عمدی داده‌های رایانه‌ای متعلق به دیگری را از حامل‌های داده یا سیستم‌های رایانه‌ای یا مخابراتی پاک نماید یا صدمه بزند یا غیر قابل استفاده کند یا به هر نحو بطور کلی یا جزیی تخریب یا مختل نماید به جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال محکوم خواهد شد.

مبحث سوم: اختلال در سیستم

ماده ۷ – هرکس به‌طور عمدی با انجام اعمالی از قبیل وارد کردن ، انتقال دادن ، ارسال ، پخش ، صدمه زدن ، پاک کردن ، ایجاد وقفه ، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری ، سیستم های رایانه‌ای یا مخابراتی متعلق به دیگری را از کار بیندازد یا کارکرد آنها را مختل نماید به جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال محکوم خواهد شد و چنانچه عمل وی به قصد اخلال در نظم و امنیت عمومی باشد و در قوانین دیگر مجازات شدیدتری پیش‌بینی شده باشد ، به مجازات مندرج در همان قانون محکوم خواهد شد.

فصل سوم: کلاهبرداری

ماده ۸ – هرکس از سیستم های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن ، تغییر، محو، ایجاد، توقف داده‌ها یا اختلال در عملکرد سیستم ، سوء استفاده نماید و از این طریق وجه یا مال یا منفعت یا خدمات مالی و یا امتیازات مالی برای خود یا دیگری تحصیل کند کلاهبردار محسوب و به مجازات مقرر برای کلاهبرداری محکوم خواهد شد.

فصل چهارم: جرایم مرتبط با محتوا

ماده۹- هرکس بوسیله سیستم های رایانه‌ای یا مخابراتی محتویات مستهجن را ارائه یا منتشر نماید و یا مورد هر قسم معامله قرار دهد و یا به منظور انتشار یا تجارت تولید نماید به مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

ماده ۱۰- اشخاصی که بوسیله حامل‌های داده یا سیستم رایانه‌ای یا مخابراتی مرتکب یکی از اعمال زیر شوندبه ترتیب زیر مجازات خواهند شد:

الف) هرکس محتویات مستهجن را به اشخاص زیر ۱۸ سال تمام ارائه نماید یا محتویات مستهجن اشخاص زیر ۱۸ سال تمام را تولید یا ارائه یا منتشر نماید و یا مورد هر قسم معامله قرار دهد و یا آنها را تهیه یا نگهداری یا ذخیره نماید، به حداکثر مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

ب) هرکس به منظور دست‌یابی اشخاص زیر ۱۸ سال تمام به محتویات مستهجن یا به منظور ارتکاب جرایم، مبادرت به تحریک یا ترغیب یا تهدید یا تطمیع یا فریب آنها نموده و یا شیوه دست‌یابی یا ارتکاب موارد ذکر شده را برای آنها تسهیل نموده یا آموزش دهد به مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

ج) هرکس محتویات مستهجن غیر واقعی (از قبیل پویا نمایی یا طراحی یا نقاشی) را به قصد ارائه یا انتشار، تهیه یا تولید یا ذخیره یا نگهداری نمایدبه حداقل مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

تبصره۱: محتویات مستهجن به محتویاتی گفته می‌شود که شامل نمایش برهنگی کامل زن و مرد یا اندام تناسلی یا نمایش آمیزش و یا عمل جنسی انسان و حیوان باشد.

تبصره۲: مفاد دو ماده پیشین شامل آن دسته از محتویاتی نخواهد بود که با رعایت موازین شرعی و برای مقاصد علمی یا هر مصلحت حلال عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا انتشار یا ذخیره شده یا مورد معامله قرار می‌گیرد.

ماده ۱۱- هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سیستم رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا بعنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به‌طور 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 مجازات مقرر برای جرم نشر اکاذیب محکوم خواهد شد.

ماده ۱۲- هرکس بوسیله سیستم رایانه‌ای یا مخابراتی فیلم یا صوت دیگری را تغییردهد یا تحریف نماید و منتشر سازد یا با علم به تغییر یا تحریف، انتشار دهد به نحوی که منجر به هتک حرمت یا ضرر وی گردد، به مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

تبصره:چنانچه عمل مرتکب از مصادیق تعرض به نوامیس مردم باشد به حداکثر هر سه مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد.

فصل پنجم : افشای سر

ماده۱۳- هرکس بوسیله سیستم رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی و خانوادگی یا اسرار دیگری را، به جز موارد قانونی، بدون رضایت او منتشر نماید یا در دسترس دیگران قرار دهد به گونه‌ای که منجر به ضرر وی گردد یا بطور عرفی موجب هتک حیثیت او تلقی شود به مجازات مقرر برای افشاء سر محکوم خواهد شد.

فصل ششم: مسئولیت کیفری ارائه دهندگان خدمات

ماده ۱۴- ایجاد کنندگان نقطه تماس بین‌المللی موظفند با بکارگیری تدبیرها و تجهیزات فنی متعارف محتویات مستهجن موضوع ماده ۹و بند الف ماده۱۰ این قانون را پالایش نمایند در غیر این صورت فرد

متخلف برای بار نخست به پرداخت جزای نقدی از مبلغ ده میلیون ریال تا یکصد میلیون ریال و درصورت تکرار به تعطیل موقت از یک هفته تا یک ماه و برای بار سوم به لغودائم مجوز و محرومیت دائم از تصدی این حرفه محکوم خواهد شد.

سایر ارائه کنندگان خدمات دسترسی نیزکه با علم به تخلف ایجادکنندگان نقطه تماس بین‌المللی، محتویات مستهجن ذکر شده را به کاربران ارائه دهند به مجازات مقرر در این ماده محکوم خواهند شد.

ماده ۱۵- ارائه کنندگان خدمات میزبانی موظفند پس از اطلاع از وجود محتویات مستهجن موضوع ماده ۹ و بند الف ماده ۱۰ این قانون در فضای واگذار شده توسط آنها، به سرعت محتویات ذکر شده را غیرقابل دسترس نموده و مراتب را به مراجع قضایی یا انتظامی محل اعلام و براساس دستور مقام قضایی اقدام نمایند. در غیر اینصورت فرد متخلف برای بار نخست به پرداخت جزای نقدی از مبلغ ده میلیون ریال تا پنجاه میلیون ریال و درصورت تکرار به پرداخت جزای نقدی از مبلغ پنجاه میلیون ریال تا یکصد میلیون ریال و محرومیت دائم از حرفه ذکر شده محکوم خواهد شد.

فصل هفتم : سایر جرایم

ماده ۱۶- اشخاص زیر به جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال محکوم خواهند شد.

الف) هرکس با علم و عمد اقدام به تولید یا انتشار یا توزیع یا معامله داده‌ها یا نرم‌افزارها ویا هر نوع وسایل الکترونیکی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌روند، نماید.

ب) هرکس با علم و عمد رمز عبور یا کد دست‌یابی یا داده‌های رایانه‌ای را بدون مجوز به دیگران ارائه کرده یا مورد معامله قرار دهد یا منتشر نماید به گونه‌ای که امکان دسترسی بدون مجوز به داده‌ها یا سیستم‌های رایانه‌ای و یا مخابراتی دیگری را فراهم آورد.

تبصره: درصورتی که مرتکب، اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر مجازات محکوم خواهد شد.

فصل هشتم: تخفیف و تشدید مجازات

ماده ۱۷ – اشخاصی که مرتکب جرایم ذکر شده در مواد ۵-۴-۳-۲ این قانون شده‌اند هرگاه پیش از کشف جرم مأموران تعقیب را از ارتکاب جرم مطلع نمایند یا به هنگام تعقیب موجب تسهیل تعقیب سایر

مرتکبان را فراهم آورند یا مأموران دولت را به گونه مؤثری در کشف جرم کمک و راهنمایی کنند و یا ضرر و زیان ناشی از جرم را در مرحله تحقیق جبران نمایند بنا به پیشنهاد دادستان مربوط و موافقت دادگاه ویا با تشخیص دادگاه در مجازات آنان تخفیف متناسب داده می‌شود و دادگاه می‌تواند مجازات مرتکب را معلق و یا او را از مجازات معاف نماید.

ماده ۱۸ – هریک از کارمندان و کارکنان اداره‌ها و سازمانها یا شوراها و یا شهرداریها و مؤسسه‌ها و شرکتهای دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که به کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به طور کلی اعضاء و کارکنان قوای سه‌گانه و هم‌چنین نیروهای مسلح و مأموران به خدمات عمومی اعم از رسمی و غیر رسمی به مناسبت انجام وظیفه مرتکب جرایم رایانه‌ای موضوع این قانون شوند حسب مورد به بیش از دو سوم حداکثر مجازات مقرر محکوم خواهند شد.

تبصره: هرگاه عمل مرتکب مشمول عنوان معاونت در جرم باشد به نصف حداکثر مجازات قانونی محکوم خواهد شد.

بخش سوم: آیین دادرسی

فصل اول: صلاحیت

ماده ۱۹- در هر حوزه قضایی، در صورت ضرورت، به تشخیص رئیس قوه قضاییه به تعداد مورد نیاز، شعبی از دادسراها و دادگاه‌های عمومی و انقلاب و تجدیدنظر برای رسیدگی به جرایم رایانه‌ای اختصاص می‌یابد.

تبصره- *قضات دادسراها و دادگاه‌های ذکر شده از میان قضاتی که آشنایی لازم به امور رایانه دارند، انتخاب خواهند شد.*

ماده ۲۰- در صورت اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی دادگاههای عمومی و انقلاب در امور مدنی خواهد بود.

فصل دوم: جمع آوری ادله الکترونیکی

مبحث اول: نگهداری داده ها

ماده ۲۱- کلیه ایجادکنندگان نقاط تماس بین‌المللی و ارائه‌کنندگان خدمات دسترسی موظفند داده‌های حاصل از مبادله داده محتوا را حداقل تا سه ماه پس از ایجاد و اطلاعات کاربران را حداقل تا سه ماه پس از خاتمه اشتراک نگهداری نمایند.

تبصره: *مراجع ذکر شده موظفند آدرس‌های IP خود را به وزارت ارتباطات و فناوری اطلاعات اعلام نمایند.*

مبحث دوم : حفظ فوری داده‌ها

ماده ۲۲- هر گاه حفظ داده‌های ذخیره شده برای تحقیق یا دادرسی لازم باشد مقام قضایی می‌تواند دستور حفاظت از داده‌های ذخیره شده را به اشخاصی که داده‌های ذکر شده به گونه‌ای تحت تصرف یا کنترل آنها قرار دارد، صادر نماید و در موارد فوری ضابطان دادگستری می‌توانند دستور حفاظت را صادر نموده، مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضایی برسانند. چنانچه هریک از کارکنان دولت یا سایر اشخاص از اجرای دستور ذکرشده خودداری نمایند کارکنان دولت به مجازات امتناع از اجرای دستور مقام قضایی وسایر اشخاص به جزای نقدی از سه میلیون ریال تا ده میلیون محکوم خواهند شد.

تبصره ــ *مدت زمان حفاظت حداکثر سه ماه می باشد و با نظر مقام قضایی قابل تمدید است.*

مبحث سوم: افشای داده‌ها

ماده ۲۳ ــ مقام‌های قضایی می‌توانند دستور افشای داده‌های حفاظت شده ذکر شده در مواد ۲۱ و ۲۲ را به اشخاصی که داده‌های ذکر شده را در تصرف و یا کنترل دارند صادر نموده تا در اختیار ضابطان قرار گیرد. مستنکف از اجرای دستور به مجازات مقرر در ماده ۲۲ محکوم خواهند شد.

مبحث چهارم: تفتیش و توقیف داده هاو سیستم‌ها

ماده ۲۴- تفتیش و توقیف داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی در مواردی بعمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم در آنها وجود داشته باشد.

ماده ۲۵- دستور مقام قضایی به‌منظور تفتیش و توقیف درصورت امکان باید شامل اجرای دستور در داخل یا خارج از محل و اطلاعاتی نظیر مکان و محدوده تفتیش و توقیف، نوع داده‌های مورد نظر، مشخصات احتمالی فایل‌ها و سخت افزارها و نرم‌افزارها، تعداد آنها ، مدت زمان مورد نیاز ، نحوه دستیابی به فایل‌های رمزگذاری شده باشد. تفتیش مشتمل بر موارد زیر خواهد بود:

الف) تفتیش تمام یا بخشی از سیستم رایانه‌ای یا مخابراتی؛

ب) تفتیش داده‌های رایانه‌ای ذخیره شده؛

ج) تفتیش حامل‌های داده از قبیل: دیسکت و لوح فشرده؛

د) دستیابی به فایل‌های حذف شده یا رمزنگاری شده.

ماده ۲۶- داده‌ها، حامل‌های داده و سیستم‌های رایانه‌ای یا مخابراتی که دلیل یا وسیله ارتکاب جرم بوده و یا از جرم تحصیل شده‌اند، قابل توقیف می‌باشند.

ماده ۲۷- در جمع‌آوری داده‌ها با رعایت تناسب، نوع، اهمیت و نقش داده‌ها در ارتکاب جرم، به روش‌هایی از قبیل موارد زیر عمل می شود:

الف) غیر قابل دسترس نمودن داده‌ها با روشهایی چون تغییر گذر واژه و رمزنگاری؛

ب) تهیه پرینت از فایلها؛

ج) تهیه کپی یا تصویر از تمام یا بخشی از داده‌ها؛

د) ضبط حاملهای داده.

ماده ۲۸- توقیف سیستم‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل موارد زیر صورت می‌گیرد:

الف) تغییر گذر واژه به منظور عدم دسترسی به سیستم؛

ب) خاموش نمودن سیستم؛

ج) پلمپ سیستم در محل استقرار؛

د) ضبط سیستم.

ماده ۲۹- در موارد زیر سیستم‌های رایانه‌ای یا مخابراتی توقیف خواهند شد:

الف) داده‌های ذخیره شده به سهولت قابل دسترس نبوده و یا حجم زیادی داشته باشند؛

ب) بهره‌برداری و تجزیه و تحلیل داده‌ها بدون وجود سیستم سخت افزاری امکان‌پذیر نباشد؛

ج) مالک یا مسئول یا متصرف قانونی سیستم به توقیف رضایت داده باشد؛

د) تهیه کپی از داده‌ها به لحاظ فنی امکان‌پذیر نباشد؛

ه) تفتیش در محل سبب ایراد صدمه به داده‌ها گردد؛

و) سایر موارد با تصمیم مقام قضایی.

ماده ۳۰- توقیف حامل‌های داده غیر متصل به سیستم رایانه‌ای یا مخابراتی، مانند ضبط آلات و ادوات جرم خواهد بود.

ماده ۳۱- چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سیستم‌های رایانه‌ای یا مخابراتی که تحت کنترل و یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سیستم‌های دیگر گسترش داده و داده‌های مورد نظر را تفتیش و یا توقیف خواهند نمود.

ماده ۳۲- در موارد توقیف داده‌ها، چنانچه به روند تحقیقات لطمه‌ای وارد نیاید با تقاضا و هزینه مالک یا دارنده حق دسترسی به داده‌ها و دستور مقام قضایی، کپی داده‌های توقیف شده به ایشان تحویل می‌شود، مگر آنکه داده‌ها غیر قانونی باشد.

ماده ۳۳- در مواردی که با تشخیص مقام قضایی توقیف سیستم یا داده‌ها سبب ایراد لطمه‌های جانی یا مالی شدید به افراد یا اخلال در برنامه‌های خدمات عمومی گشته و یا مخل امنیت کشور باشد از روش‌های مناسبتری به جای توقیف استفاده خواهد شد.

ماده ۳۴- متضرر می‌تواند در مورد عملیات و اقدام‌های مأموران در توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ۱۰ روز به مرجع قضایی دستور دهنده تسلیم نماید، به درخواست یاد شده خارج از نوبت رسیدگی شده و تصمیم اتخاذ شده قابل اعتراض است.

مبحث پنجم: شنود داده ها

ماده ۳۵- شنود داده محتوا ممنوع است، جز در مواردی که به امنیت کشور مربوط است و یا برای احقاق حقوق اشخاص به نظر قاضی ضروری تشخیص داده شود. مدت زمان شنود باید توسط مقام قضایی تعیین شود.

مبحث ششم : سایر موارد

ماده ۳۶- داده‌های رایانه‌ای و مخابراتی در صورتی که مطابق این قانون جمع‌آوری و نگهداری شده باشند می‌توانند در اثبات جرم مورد استناد قرار گیرند.

ماده ۳۷- به منظور جلوگیری از بروز هرگونه تغییر، تحریف یا آسیب و حفظ وضعیت اصلی داده‌های رایانه‌ای یا مخابراتی جمع‌آوری شده، لازم است تا زمانی که مرجع قضایی مربوط ضروری می‌داند، از آن نگهداری و مراقبت به عمل آید.

تبصره- *آئین نامه شیوه جمع آوری، نگهداری و مراقبت از داده‌های رایانه‌ای و مخابراتی توسط وزارت دادگستری با همکاری نیروی انتظامی و وزارت ارتباطات و فناوری اطلاعات ظرف سه ماه از تاریخ تصویب این قانون تهیه گشته، به تصویب رییس قوه قضائیه خواهد رسید.*

بخش چهارم: همکاری‌های بین المللی

ماده ۳۸- همکاری‌های بین‌المللی، هرگونه مبادله اطلاعات و انجام امور اداری و پلیسی و قضایی که دولت ایران و سایر دولت‌ها را قادر به کشف، پیگیری، تعقیب،رسیدگی و اجرای حکم نماید، در بر خواهد گرفت.

تبصره- *چگونگی پیگیری و انجام امور ذکر شده در این ماده و تشکیلات سازمانی مورد نیاز برای اجرای آن به موجب آئین نامه‌ای خواهد بود که ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با کسب نظر از مراجع مربوط تهیه گشته، به تصویب رییس قوه قضاییه خواهد رسید.*

ماده ۳۹- در مواردی که سیستم رایانه ای یا مخابراتی به عنوان وسیله یا ابزار ارتکاب جرم مورد استفاده قرار گیرد و در این قانون مجازاتی تعیین نشده باشد مرتکب مطابق مقررات قانون مربوط مجازات خواهد شد .

ماده ۴۰- قوانین و مقررات مغایر با این قانون ملغی است.