بسمه تعالی

مقدمه

نظام قضایی کشور به عنوان رکن رکین اجرای عدالت و احقاق حق در نظام جمهوری اسلامی ایران ، همواره در پی اعمال روشها و برنامه های شایسته و کار آمد در راستای اجرای شایسته تر وظایف و امور محوله به این قوه بوده است و در طول مدیریت رؤسای محترم پیشین قوه قضاییه ، ایده ها و برنامه های متعددی در جهت ارائه ی شایسته تر و مطلوبتر خدمات به مراجعین ، تصویب و به اجرا در آمده است.

علیرغم توسعهٔ تعاملات اقتصادی و حقوقی میان آحاد افراد جامعه در سالهای اخیر و همچنین بعضاً نا کار آمدی برخی مراجع اداری و سازمانی در انجام وظایف محوله ، آمار پرونده های وارده به قوه قضاییه به صورت سال به سال افزایش یافته و می یابد به حدی که در حال حاضر سالانه میلیونها پرونده به قوه قضاییه وارد می شود و ورود این حجم فوق العاده از پرونده ها ، عملاً امکان رسیدگی دقیق و سریع را مشکل و دشوار می نماید.در ارزیابی به عمل آمده در سالهای اخیر که با هدف آسیب شناسی مشکلات دستگاه قضایی به عمل آمده است ، دو مشکل (افزایش ورودی) و (اطاله دادرسی) به عنوان مهمترین مشکلات قوه شناسایی شده و با استقرار ریاست فعلی قوه قضاییه ، حضرت آیت ا... آملی لاریجانی (دام عزه) مقرر شد رویکردهای جدید در راستای رفع مشکلات و این دو مشکل به صورت خاص تدوین و اعمال گردد. یکی از راهکارهای پیش روی برنامه ریزان راهبردی قوه قضاییه ، استفاده از فناوری های نوین برای اعمال نظارت دقیق بر روند ورودی پرونده ها و مسیر رسیدگی و نهایتاً اجرای احکام بود. تصویب قانون دادرسی الکترونیکی را شاید بتوان یکی از اقدامات ارزشمند مجلس شورای اسلامی و نظام در سالهای اخیر دانست ، چرا که که با تصویب این قانون ، در خصوص بسیاری از تعاملات حقوقی فیمابین مردم در فضای مجازی که سالها بود بلاتکلیف مانده بود و همچنین نحوه رسیدگی به جرایم و تخلفات و خصوصا" اعتبار اسناد الکترونیک به خوبی تعیین تکلیف گردیده و به صراحت به این قبیل امور پرداخته شد . هر چند که میزان اثر بخشی و کارآمدی هر قانون طبیعتا" در پی اجرای آن در جامعه و بروز مزایا و معایب اجرای آن پدیدار خواهد شد اما به نظر می رسد که این قانون ، انشاا... آثار مثبتی در نظم بخشی به فضای تعاملات الکترونیک و مجازی خواهد داشت. از دیگر نکاتی که در قانون مذکور به آن پرداخته شد ، موضوع ایجاد دفاتر خدمات قضایی الکترونیک توسط قوه قضاییه و با استفاده از ظرفیت بخش خصوصی بوده است.

در سالهای اخیر سیستم سامانه مدیریت پرونده (سمپ) که امکان نظارت مستمر بر روند ورود و رسیدگی و اتخاذ تصمیم نسبت به پرونده ها بود ، طراحی و اجرا گردید و در تداوم این مسیر ، مقرر شد که در راستای اجرای سیاستهای کلی اصل ۴۴ (ابلاغی از سوی مقام معظم رهبری) مبنی بر واگذاری امور غیر حاکمیتی دولت (به معنای اعم آن) به بخش خصوصی و استفاده از ظرفیت این بخش نیز در دستور کار قرار گیرد. به همین منظور پروژه ی ایجاد ((دفاتر خدمات الکترونیک قضایی)) در سراسر کشور طراحی و تاسیس این دفاتر با هدف امکان طرح و پیگیری امور قضایی مراجعان در فضای مجازی اجرایی گردید. دفاتر خدمات الکترونیک قضایی که فی الواقع دفاتری مربوط به بخش خصوصی و تحت نظارت قوه قضاییه می باشند ، مسئولیت پذیرش دادخواستها و برخی شکایات آحاد مردم و ارسال آنها به محاکم به صورت الکترونیک را بر عهده دارند. در واقع با راه اندازی این دفاتر در سراسر کشور ، بخش قابل توجهی از امور غیر حاکمیتی قوهٔ قضاییه و سازمانهای وابسته به آنها به خارج از قوه منتقل گردیده و تحت نظارت مدیران این دفاتر که از حقوقدانان برجسته می باشند ، اداره می شوند.

با تصویب قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی ، بخصوص در تبصره ۲ ماده ۶۵۵ آن قانون ، به ایجاد دفاتر و همچنین ایجاد کانون دفاتر خدمات الکترونیک قضایی اشاره گردید و در همین راستا ، کانون مذکور نیز تأسیس و با تدوین آئین نامه آن که به تصویب ریاست محترم قوه قضاییه رسیده است و با ثبت رسمی و تشکیل شخصیت حقوقی کانون ، کلیه امور صنفی دفاتر به کانون محول گردید .

امید است انشاالله با اجرای شایسه ی این قانون ، امکان ارائه خدمات شایسته تر ملت شریف ایران فراهم گردد.

محمدرضا دشتی اردکانی

رئیس کانون دفاتر خدمات الکترونیک قضایی

چند موضوع در باب دادرسی الکترونیک

امضای الکترونیک

یکی از دستاوردهای فناوری الکترونیک، «امضای الکترونیکی» است. چیزی که حقوقدانان به آن به دیده تردید می‌نگریستند که چگونه می‌توان رضایت طرفین سندی را بدون اعلام شفاهی یا کتبی و صرفا به وسیله یک کد الکترونیک پذیرفت و آن را منشا اثر حقوقی دانست؟

از سوی دیگر سهولت زمینه الکترونیک گوی سبقت را از حقوقدانان ربود و با توجه به اصل آزادی ادله و نیز نیاز به سرعت در معاملات تجاری به خصوص در بخش اسناد و قراردادهای تجاری زمینه الکترونیک به سرعت رواج یافت و حقوقدانان و قانونگذاران به دنبال آن ناگزیر از پذیرش آن شدند و مقررات آن را به سرعت تدوین و تصویب کردند.

سند رسمی چیست؟

با گسترش استفاده از وسایل الکترونیک و اینترنت، یکی ازپدیده های عصر ارتباطات تنظیم سند رسمی الکترونیک است که در بعضی از کشورهای دنیا از جمله فرانسه مورد استفاده قرار گرفته و قوانینی نیز در این زمینه به تصویب رسیده است.

به موجب تعریفی که ماده ۱۲۸۷ قانون مدنی جمهوری اسلامی ایران ارائه داده است اسناد رسمی عبارتند از: اسنادی که در اداره ثبت اسناد و املاک و یا دفاتر اسناد رسمی یا در نزد سایر مامورین رسمی در حدود صلاحیت آنها و بر طبق مقررات قانونی تنظیم شده باشند.

سند رسمی دارای وجوه و امتیازاتی است که در سایر اسناد عادی وجود ندارد. اسناد عادی از حیث قابلیت اثبات از توان کمتری برخوردار هستند به طوری که به راحتی مورد انکار یا تردید قرار گرفته و نسبت به آنها ادعای جعل می شود و این در حالی است که تا زمانی که مجعولیت اسناد رسمی با حکم دادگاه به اثبات نرسد هیچ‌کس نمی‌تواند از حاکمیت قاطعانه آنها جلوگیری کند.

اما این تنها ویژگی اسناد رسمی نیست. اسناد رسمی، لازم‌الاجرا نیز هستند و این بدان معنی است که بدون مراجعه به دادگاه می‌توان اجرای مفاد آن را از مراجع ویژه خواست.

در نتیجه اجراییه صادره از این مراکز نه تنها ارزش کمتری از حکم دادگاه ندارد که مانند آنها باید اجرا شود.

فوائد استفاده از سند رسمی الکترونیک

برخی از امتیازات و منافع حاصل از استفاده از فناوری سند رسمی الکترنیک به اختصار عبارتند از:

۱- سرعت در نگارش و به مرحله رسمیت رساندن سند رسمی

۲- امکان استفاده از امکانات اینترنتی

۳- امنیت حقوق به نفع و در مقابل اشخاص ثالث

۴- حل مشکلات حاصل از مدت‌های لازم و مقرر در قانون برای اتمام مراحل به رسمیت شناختن مالک جدید در اموال غیر منقول و جلوگیری از سوءاستفاده‌های احتمالی.

به عنوان مثال در حال حاضر دفاتر اسناد رسمی موظفند ظرف مدت پنج روز از تاریخ امضای سند رسمی خلاصه معامله مربوطه را به اداره ثبت محل ارسال کنند تا مراتب توسط کارکنان ثبت در ردیف انتقال دفتر ثبت منظورشود.

واضح است که به محض امضای سند انتقال توسط طرفین سند و سردفتر، خریدار مالک مورد معامله خواهد بود. با این همه تا خلاصه معامله به اداره ثبت نرسد عملا مالکیت خریدار تحقق

کامل نیافته است و در این فاصله زمانی احتمال بروز مشکل وجود داشته و دست کم یک بار مراجعه به دادگاه برای ارائه سند به عنوان دلیل مالکیت اجتناب‌ناپذیر است. در حالی که در فناوری الکترونیک فقط چند لحظه بعد از امضای کامل سند از طریق الکترونیک و فقط با فشار دادن دکمه ورود در صفحه کلید رایانه چند لحظه پس از رسمیت سند، خلاصه معامله به ثبت محل رسیده و اداره ثبت مربوطه مطلع محسوب می‌شود.

دادرسی الکترونیکی

ماده۶۴۹ـ به منظور سیاستگذاری و تدوین راهبردهای ملی، برنامه‌ریزی میان‌مدت و بلندمدت و تدوین آیین‌نامه‌های لازم برای توسعه و ارتقای دادرسی الکترونیکی و نظارت بر حسن اجرای آنها، «شورای راهبری دادرسی الکترونیکی» که در این بخش به اختصار شورا نامیده می‌شود به ریاست رئیس قوه قضائیه و عضویت افراد زیر تشکیل می‌شود:

الف ـ رئیس مرکز آمار و فناوری اطلاعات قوه قضائیه (دبیر شورا)

ب ـ معاون حقوقی قوه قضائیه

پ ـ رئیس دیوان عالی کشور

ت ـ دادستان کل کشور

ث ـ رئیس دیوان عدالت اداری

ج ـ رئیس سازمان قضائی نیروهای مسلح

چ ـ رئیس سازمان زندان‌ها و اقدامات تأمینی و تربیتی کشور

ح ـ رئیس سازمان ثبت اسناد و املاک کشور

خ ـ رئیس سازمان بازرسی کل کشور

د ـ رئیس سازمان پزشکی قانونی کشور

ذ ـ معاون آموزش و تحقیقات قوه قضائیه

ر ـ معاون راهبردی قوه قضائیه

ز ـ مسؤول حفاظت و اطلاعات قوه قضائیه

ژ ـ وزیر دادگستری

س ـ وزیر ارتباطات و فناوری اطلاعات

ش ـ فرمانده نیروی انتظامی کشور

ص ـ یک‌نفر نماینده عضو کمیسیون قضائی و حقوقی به انتخاب مجلس شورای اسلامی به عنوان عضو ناظر

ض ـ سه نفر به انتخاب رئیس قوه قضائیه

تبصره۱ـ شورا با اکثریت اعضاء رسمیت می‌یابد و مصوبات آن با اکثریت آراء حاضران و پس از تصویب رئیس قوه قضائیه قابل اجراء است و نافی اختیارات رئیس قوه قضائیه نیست.

تبصره۲ـ دبیر شورا می‌تواند حسب مورد از مسؤولان مرتبط و کارشناسان برای حضور در جلسه دعوت به عمل آورد.

تبصره۳ـ دبیرخانه شورا در مرکز آمار و فناوری اطلاعات قوه قضائیه تشکیل می‌شود.

ماده۶۵۰ـ به منظور ساماندهی پرونده‌ها و اسناد قضائی و ارائه بهتر خدمات قضائی و دستیابی روزآمد به آمار و گردش کار قضائی در سراسر کشور و همچنین ارائه آمار و اطلاعات دقیق و تفصیلی در خصوص جرائم، متهمان، بزه‌دیدگان و مجرمان و سایر اطلاعات قضائی، «مرکز ملی داده‌های قوه قضائیه» در مرکز آمار و فناوری اطلاعات قوه قضائیه با استفاده از افراد موثق راه‌اندازی می‌شود.

تبصره۱ـ نحوه و میزان دسترسی مراجع ذی‌صلاح قضائی به اطلاعات این مرکز به موجب آیین‌نامه‌ای است که ظرف سه‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط شورا تهیه می‌شود و به تصویب رئیس قوه قضائیه می رسد.

تبصره۲ـ اسناد، مدارک و اطلاعات این مرکز با رعایت قوانین و مقررات به موجب آیین‌نامه‌ای که ظرف سه‌ماه از تاریخ تصویب این قانون توسط شورا تهیه و به تصویب رئیس قوه قضائیه می‌رسد، در اختیار مراکز علمی، پژوهشکده‌ها و پژوهشگران قرار می‌گیرد. استفاده از اسناد، مدارک و اطلاعات مزبور نباید موجب هتک حرمت و حیثیت اشخاص شود. انتشار اطلاعات مربوط به هویت افراد مرتبط با دادرسی از قبیل نام، نام خانوادگی،

شماره‌پستی و شماره‌ملی آنان جز در مواردی که قانون تجویز کند، ممنوع است.

ماده۶۵۱ـ کلیه دستگاههای تابعه قوه قضائیه، نظیر دیوان عدالت اداری، سازمان بازرسی کل کشور، سازمان زندان‌ها و اقدامات تأمینی و تربیتی کشور، سازمان ثبت اسناد و املاک کشور، سازمان پزشکی قانونی، سازمان قضائی نیروهای مسلح و مراجع ذی‌ربط در عفو و بخشودگی و سجل کیفری، و روزنامه رسمی جمهوری اسلامی، موظفند کلیه اطلاعات خود را در مرکز ملی داده‌های قوه قضائیه قرار دهند و آنها را روزآمد نگه دارند.

تبصره۱ـ آیین‌نامه اجرائی نحوه دسترسی به اطلاعات محرمانه و سری در مرکز ملی داده‌های قوه قضائیه توسط آن قوه تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

تبصره۲ـ مراجع انتظامی و سایر ضابطان و دستگاهها، هیأتها و کمیسیون های ذی ربط موظفند اطلاعات مرتبط با امورقضائی خود را در مرکز ملی داده‌های قوه قضائیه قرار دهند و آنها را روزآمد نگه دارند.

ماده۶۵۲ـ قوه قضائیه موظف است به منظور ساماندهی ارتباطات الکترونیکی بین محاکم، ضابطان و دستگاههای تابعه خود و نیز سایر اشخاص حقیقی و حقوقی که در جریان دادرسی به اطلاعات آنها نیاز است، «شبکه ملی عدالت» را با به‌کارگیری تمهیدات امنیتی مطمئن از قبیل امضای الکترونیکی راه‌اندازی کند.

تبصره‌ـ مراجع قضائی می‌توانند استعلامات قضائی و کسب اطلاعات لازم را از طریق شبکه ملی عدالت به‌عمل آورند. در این صورت دستگاههای دولتی، نهادهای عمومی غیردولتی و شخصیت‌های حقوقی بخش خصوصی موظفند پاسخ لازم را از طریق شبکه مزبور اعلام کنند. مستنکف از مفاد این تبصره مشمول ماده (۵۷۶) قانون مجازات اسلامی ـ کتاب پنجم تعزیرات مصوب ۱۳۷۵/۳/۲ـ است.

ماده۶۵۳ـ قوه‌قضائیه موظف است اطلاعات زیر را ازطریق «درگاه ملی قوه‌قضائیه» ارائه کند وآنها را روزآمد نگه دارد.

الف ـ اهداف، وظایف، سیاست‌ها، خط‌مشی‌ها و ساختار کلان مدیریتی و اجرائی قوه‌قضائیه به همراه معرفی مسؤولان و شرح وظایف و نحوه ارتباط با آنان

ب ـ نشانی، شماره تماس و پیوند به تارنمای (وب‌سایت) تمامی معاونت‌ها و دادگستری‌های استانها، دستگاههای تابعه قوه قضائیه،وزارت دادگستری، کانون‌های وکلای دادگستری و کارشناسان رسمی دادگستری

پ ـ کلیه قوانین لازم الاجراء، آراء وحدت رویه هیأت عمومی دیوان عالی کشور و آراء هیأت عمومی دیوان عدالت اداری، بخشنامه‌های رئیس قوه قضائیه و نظریات مشورتی اداره حقوقی قوه قضائیه

ت ـ آراء صادره از سوی محاکم درصورتی که به تشخیص قاضی اجرای احکام خلاف عفت عمومی یا امنیت ملی نباشد به صورت برخط (آنلاین) برای تحلیل و نقد صاحب‌نظران و متخصصان با حفظ حریم خصوصی اشخاص

ث ـ خدمات معاضدت قضائی به مقامات ذی‌صلاح سایر کشورها بر پایه اسناد و معاهده‌های همکاری حقوقی بین‌المللی و اطلاعات راجع به خدمات حقوقی و قضائی به‌اتباع سایر کشورها

ج ـ آموزش آسان و قابل‌درک عمومی چگونگی اقامه دعوی برای شهروندان

چ ـ اطلاعات پژوهشی و علمی حقوقی ـ قضائی

ماده۶۵۴ـ قوه قضائیه موظف است برای دادگستری استانهای سراسر کشور، و دستگاههای تابعه قوه قضائیه، تارنمای(وب‌سایت) اختصاصی راه‌اندازی کند و مراجع مزبور موظفند اطلاعات ذیل را در آن ارائه کنند و آنها را روزآمد نگه‌دارند:

الف ـ نمودار تشکیلاتی دادگاهها، به تفکیک تخصص و سلسله مراتب قضائی، به‌همراه معرفی مسؤولان و شرح وظایف و نحوه ارتباط با آنان

ب ـ نشانی و شماره تماس دادگاهها، سایر دستگاههای تابعه قوه قضائیه و مراجع انتظامی در سطح استان

پ ـ پیوند به تارنماهای سایر مراجع قضائی و دستگاههای ذی‌ربط

ت ـ کلیه اطلاعات مورد نیاز برای محاسبه هزینه دادرسی، مانند بهای منطقه‌ای املاک

ث ـ آموزش آسان و قابل‌درک عمومی چگونگی اقامه دعوی برای شهروندان

ج ـ سمینارها یا نشستهای الکترونیکی استانی قضائی زنده یا ضبط شده

چ ـ اطلاعات پژوهشی و علمی حقوقی ـ قضائی

ماده۶۵۵ـ در هر مورد که به موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رأی، امضاء، اثر انگشت، ابلاغ اوراق

قضائی، نشانی و مانند آن لازم باشد صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است.

تبصره۱ـ در کلیه مراحل تحقیق و رسیدگی حقوقی و کیفری و ارائه خدمات الکترونیک قضائی، نمی‌توان صرفاً به لحاظ شکل یا نحوه تبادل اطلاعات الکترونیکی از اعتبار بخشیدن به محتوا و آثار قانونی آن خودداری نمود. قوه قضائیه موظف است سامانه‌های امنیتی لازم را جهت تبادل امن اطلاعات و ارتباطات بین اصحاب دعوی، کارشناسان، دفاتر خدمات الکترونیک قضائی، ضابطان و مراجع قضائی و سازمان‌های وابسته به قوه قضائیه ایجاد نماید.

تبصره۲ـ قوه قضائیه می‌تواند جهت طرح و پیگیری امور قضائی مراجعان موضوع این قانون در فضای مجازی نسبت به ایجاد دفاتر خدمات الکترونیک قضائی و جهت هماهنگی فعالیت دفاتر، نسبت به ایجاد کانون دفاتر خدمات الکترونیک قضائی، با استفاده از ظرفیت بخش خصوصی اقدام نماید. دفاتر خدمات الکترونیک قضائی می‌توانند از بین دفاتر اسناد رسمی و غیر آن انتخاب یا تأسیس شوند. آیین‌نامه اجرائی این ماده ظرف سه ماه از تاریخ لازم‌الاجراء شدن این قانون توسط شورا تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

تبصره۳ـ مراجعان به قوه قضائیه موظفند پست الکترونیکی و شماره تلفن همراه خود را در اختیار قوه قضائیه قرار دهند، و در صورت عدم دسترسی به پست الکترونیک، مرکز آمار موظف است برای شهروندان و متقاضیان امکانات لازم برای دسترسی به پست الکترونیکی ملی قضائی جهت امور قضائی ایجاد کند.

ماده۶۵۶ـ به منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری اطلاعات مبادله‌شده میان شهروندان و محاکم قضائی، قوه قضائیه موظف است تمهیدات امنیتی مطمئن برای امضای الکترونیکی، احراز هویت و احراز اصالت را فراهم آورد.

تبصره‌ـ قوه قضائیه موظف است مرکز صدور گواهی ریشه برای امضای الکترونیکی را جهت ایجاد ارتباطات و مبادله اطلاعات امن راه اندازی نماید.

ماده۶۵۷ـ مرکز آمار و فناوری اطلاعات قوه قضائیه موظف است به منظور اجراء و توسعه خدمات پرداخت الکترونیکی هزینه‌های دادرسی و سایر پرداخت‌های مربوط به‌دادرسی و اجرای حکم توسط شهروندان، اقدام و راهنمایی لازم را به عمل آورد.

تبصره‌ـ در راستای ترغیب شهروندان به بهره‌برداری از دادرسی الکترونیکی، در مرحله بدوی هزینه دادرسی آنان پنج درصد(۵٪) و حداکثر تا سقف ده میلیون ریال کمتر خواهد بود.

ماده۶۵۸ـ قوه قضائیه موظف است تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان، در چهارچوب اقدامات این بخش فراهم آورد.

ماده۶۵۹ـ به کارگیری سامانه‌های ویدئو کنفرانس و سایر سامانه‌های ارتباطات الکترونیکی به منظور تحقیق از اصحاب دعوی، اخذ شهادت از شهود یا نظرات کارشناسی در صورتی مجاز است که احراز هویت، اعتبار اظهارات فرد مورد نظر و ثبت مطمئن سوابق صورت پذیرد.

ماده۶۶۰ـ چنانچه اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به طور غیرمجاز آنها را افشاء کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از دو تا ده سال محکوم خواهند شد.

ماده۶۶۱ـ چنانچه اشخاصی که مسؤول حفظ امنیت مراکز، سامانه‌های رایانه‌ای و مخابراتی و اطلاعات موضوع این بخش هستند یا داده‌ها یا سامانه(سیستم)های مذکور در اختیار آنان قرار گرفته است بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم مهارت یا عدم رعایت تدابیر متعارف امنیتی موجبات ارتکاب جرائم رایانه‌ای به‌وسیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از شش ماه تا دو سال یا انفصال ازخدمت تا پنج سال یا جزای‌نقدی از ده تا صدمیلیون ریال محکوم خواهند شد.

ماده۶۶۲ـ قوه قضائیه موظف است برای آموزش دادرسی الکترونیکی به قضات، کارکنان قضائی، دستگاههای تابعه قضائی و مراجع انتظامی اقدام کند.

ماده۶۶۳ـ آیین‌نامه‌های اجرائی این بخش، ظرف سه ماه از تاریخ تصویب این قانون توسط شورا تهیه و به تصویب رئیس قوه قضائیه می رسد.

ماده۶۶۴ـ علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران صلاحیت رسیدگی به موارد زیر را دارند:

الف ـ داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حاملهای داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری‌اسلامی‌ایران ذخیره شود.

ب ـ جرم از طریق تارنماهای دارای دامنه مرتبه‌بالای کد کشوری ایران (**ir .**) ارتکاب یابد.

پ ـ جرم توسط تبعه ایران یا غیرآن در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یابد.

ت ـ جرائم رایانه ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود.

ماده۶۶۵ـ چنانچه جرم رایانه ای درصلاحیت دادگاههای ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را

انجام دهد. درصورتی‌که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و درصورت اقتضاء صدور کیفرخواست می کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند.

ماده۶۶۶ـ قوه قضائیه موظف است به تناسب ضرورت، شعبه یا شعبی از دادسراها، دادگاههای کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.

تبصره‌ـ مقامات قضائی دادسراها و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب می‌شوند.

ماده۶۶۷ـ ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش‌ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره۱ـ داده ترافیک، هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می‌کنند 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.

تبصره۲ـ اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (**IP**)، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.

ماده۶۶۸ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.

ماده۶۶۹ـ هرگاه حفظ داده های رایانه ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام‌قضائی 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 قضائی می توانند دستور حفاظت را صادر کنند و مراتب را حداکثر تا بیست و چهار ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی 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 قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نود و یک روز تا شش‌ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هردو مجازات محکوم می‌شوند.

تبصره۱ـ حفظ داده ها به منزله ارائه یا افشاء آنها نیست و مستلزم رعایت مقررات مربوط است.

تبصره۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه‌ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.

ماده۶۷۰ـ مقام قضائی می تواند دستور ارائه داده های حفاظت شده مذکور در مواد (۶۶۷)، (۶۶۸) و (۶۶۹) این قانون را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. خودداری از اجرای این دستور و همچنین عدم نگهداری وعدم مواظبت از این داده‌ها موجب مجازات مقرر در ماده (۶۶۹) این قانون می‌شود.

ماده۶۷۱ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد.

ماده۶۷۲ـ 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 می‌شود. درصورت عدم حضور یا امتناع از حضور آنان چنانچه تفتیش یا توقیف ضرورت داشته باشدیا فوریت امر اقتضاء کند، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می‌کند.

ماده۶۷۳ـ دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای 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 باشد که به اجرای صحیح آن کمک می کند.

ماده۶۷۴ـ تفتیش داده‌ها یا سامانه‌های رایانه ای و مخابراتی شامل اقدامات ذیل می‌شود:

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

ب ـ دسترسی به حاملهای داده از قبیل دیسکت ها یا لوحهای فشرده یا کارتهای حافظه

پ ـ دستیابی به داده های حذف یا رمزنگاری شده

ماده۶۷۵ـ در توقیف داده ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روشهایی از قبیل چاپ داده ها، تصویربرداری از تمام یا بخشی از داده ها، غیرقابل دسترس کردن داده ها با روشهایی از قبیل تغییرگذرواژه یا رمزنگاری و ضبط حاملهای داده عمل می‌شود.

ماده۶۷۶ـ در شرایط زیر سامانه های رایانه ای یا مخابراتی توقیف می‌شوند:

الف ـ داده های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد.

ب ـ تفتیش و تجزیه و تحلیل داده ها بدون سامانه سخت افزاری امکان پذیر نباشد.

پ ـ متصرف قانونی سامانه رضایت داده باشد.

ت ـ تصویربرداری از داده ها به لحاظ فنی امکان پذیر نباشد.

ث ـ تفتیش در محل باعث آسیب داده‌ها شود.

ماده۶۷۷ـ توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روشهایی از قبیل تغییر گذرواژه به منظور عدم دسترسی به سامانه، مهر و موم (پلمب) سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده۶۷۸ـ چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به‌سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند.

ماده۶۷۹ـ توقیف داده ها یا سامانه های رایانه ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود، ممنوع است مگر اینکه توقیف برای اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد.

ماده۶۸۰ـ در جایی که اصل داده ها توقیف می شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده های توقیف‌شده منافی با ضرورت کشف حقیقت نباشد و به روند تحقیقات لطمه ای وارد نسازد و داده ها مجرمانه نباشد.

ماده۶۸۱ـ در مواردی که اصل داده ها یا سامانه 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 درجرم ارتکابی، در مهلت متناسب و متعارف برای آنها تعیین تکلیف کند.

ماده۶۸۲ـ متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است.

ماده۶۸۳ـ کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است.

تبصره‌ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است.

ماده۶۸۴ـ آیین‌نامه اجرائی نحوه نگهداری و مراقبت از ادله الکترونیکی جمع‌آوری‌شده ظرف شش‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط وزیر دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

ماده۶۸۵ـ چنانچه داده های رایانه ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده ها خدشه وارد نشود، قابل استناد است.

ماده۶۸۶ـ کلیه مقررات مندرج در این بخش، علاوه بر جرائم رایانه ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می گیرند نیز می شود.

ماده۶۸۷ـ در مواردی که در این بخش برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آیین‌دادرسی پیش‌بینی نشده است، تابع مقررات‌عمومی آیین دادرسی کیفری است.

بخش یازدهم ـ آیین‌دادرسی جرائم اشخاص حقوقی

ماده۶۸۸ـ هرگاه دلیل کافی برای توجه اتهام به اشخاص حقوقی وجود داشته باشد، علاوه بر احضار شخص حقیقی که اتهام متوجه او می‌باشد، با رعایت مقررات مربوط به احضار، به شخص حقوقی اخطار می شود تا مطابق مقررات نماینده قانونی یا وکیل خود را معرفی نماید. عدم معرفی وکیل یا نماینده مانع رسیدگی نیست.

تبصره ـ فردی که رفتار وی موجب توجه اتهام به شخص حقوقی شده است، نمی تواند نمایندگی آن را عهده‌دار شود.

ماده۶۸۹ـ پس از حضور نماینده شخص حقوقی، اتهام وفق مقررات برای وی تبیین می شود. حضور نماینده شخص حقوقی تنها جهت انجام تحقیق و یا دفاع از اتهام انتسابی به شخص حقوقی است و هیچ یک از الزامات و محدودیت‌های مقرر در قانون برای متهم، در مورد وی اعمال نمی شود.

ماده۶۹۰ـ در صورت وجود دلیل کافی دایر بر توجه اتهام به شخص حقوقی و درصورت اقتضاء منحصراً صدور قرارهای تأمینی زیر امکانپذیر است. این قرارها ظرف ده روز پس از ابلاغ، قابل اعتراض در دادگاه صالح است.

الف ـ قرار ممنوعیت انجام بعضی از فعالیت های شغلی که زمینه ارتکاب مجدد جرم را فراهم می کند.

ب ـ قرار منع تغییر ارادی در وضعیت شخص حقوقی از قبیل انحلال، ادغام و تبدیل که باعث دگرگونی یا از دست دادن شخصیت حقوقی آن شود.

تخلف از این ممنوعیت موجب یک یا دو نوع از مجازات‌های تعزیری درجه هفت یا هشت برای مرتکب است.

ماده۶۹۱ـ در صورت توجه اتهام به شخص حقوقی صدور قرار تأمین خواسته طبق مقررات این قانون بلامانع است.

ماده۶۹۲ـ در صورت انحلال غیر ارادی شخص حقوقی حسب مورد قرار موقوفی تعقیب یا موقوفی اجراء صادر می شود. مقررات مربوط به قرار موقوفی تابع مقررات آیین دادرسی کیفری است. در مورد دیه و خسارت ناشی از جرم وفق مقررات مربوط اقدام می شود.

ماده۶۹۳ـ اجرای احکام مربوط به اشخاص حقوقی تابع مقررات آیین دادرسی کیفری است.

ماده۶۹۴ـ در صورتی که شخص حقوقی دارای شعب یا واحدهای زیرمجموعه متعدد باشد، مسؤولیت کیفری تنها متوجه شعبه یا واحدی است که جرم منتسب به آن است. در صورتی که شعبه یا واحد زیرمجموعه بر اساس تصمیم مرکزیت اصلی شخص حقوقی اقدام کند، مسؤولیت کیفری متوجه مرکزیت اصلی شخص حقوقی نیز می باشد.

ماده۶۹۵ـ اظهارات نماینده قانونی شخص حقوقی علیه شخص حقوقی اقرار محسوب نمی شود و اتیان سوگند نیز متوجه او نیست.

ماده۶۹۶ـ در مواردی که مقررات ویژه‌ای برای دادرسی جرائم اشخاص حقوقی مقرر نشده است مطابق مقررات عمومی آیین‌دادرسی کیفری که در مورد این اشخاص قابل اجراء است اقدام می‌شود.

بخش دوازدهم ـ سایرمقررات

ماده۶۹۷ـ دولت موظف است به تکالیف مقرر در اجرای احکام مواد (۶۵۰)، (۶۵۲) و (۶۵۴) تا (۶۵۶) این قانون با توجه به بندهای (ح) و (ف) ماده (۲۱۱) قانون برنامه پنجساله پنجم توسعه جمهوری اسلامی ایران در مدت باقی‌مانده اجرای آن عمل نماید. بار مالی اضافی ناشی از اجرای این‌قانون از محل افزایش درآمدهای قانون آیین‌دادرسی کیفری تأمین می‌گردد.

ماده۶۹۸ـ از تاریخ لازم‌الاجراء شدن این قانون، ماده واحده قانون راجع به تجویز دادرسی غیابی در امور جنایی مصوب ۱۳۳۹/۳/۲، قانون دادرسی نیروهای مسلح جمهوری اسلامی ایران مصوب ۱۳۶۴/۲/۲۲ به‌جز مواد (۴)، (۸) و (۹) آن قانون، قانون تشکیل دادگاههای کیفری (یک و دو) و شعب دیوان عالی کشور مصوب ۱۳۶۸/۴/۲۰، قانون تجدیدنظر آرای دادگاهها مصوب ۱۳۷۲/۵/۱۶، مواد (۷۵۶) الی (۷۷۹) الحاقی مورخ ۱۳۸۸/۳/۵به قانون مجازات اسلامی (تعزیرات و مجازاتهای بازدارنده) و ماده (۵۶۹) قانون آیین‌دادرسی کیفری مصوب ۱۳۹۲/۱۲/۴ و اصلاحات و الحاقات بعدی آنها ملغی است.

ماده۶۹۹ـ این قانون با رعایت ترتیب شماره مواد به عنوان بخشهای هشتم، نهم، دهم، یازدهم و دوازدهم قانون آیین‌دادرسی کیفری مصوب ۱۳۹۲/۱۲/۴ الحاق و مقررات هر دو قانون از تاریخ ۱۳۹۴/۴/۱ لازم‌الاجراء است.

قانون فوق مشتمل بر ۱۲۹ ماده و۵۶ تبصره در جلسه مورخ هشتم مهرماه یکهزار و سیصد و نود و سه کمیسیون قضائی و حقوقی مجلس شورای اسلامی طبق اصل هشتاد و پنجم (۸۵) قانون اساسی تصویب گردید و پس از موافقت مجلس با اجرای آزمایشی آن به‌مدت سه سال در تاریخ ۱۳۹۳/۷/۳۰ به تأیید شورای نگهبان رسید

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 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 (۵،۰۰۰،۰۰۰)ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) 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 سامانه 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 میلیون (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) 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 سامانه های رایانه ای یا مخابراتی یا حاملهای 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 میلیون (۲۰،۰۰۰،۰۰۰) ریال تا شصت میلیون (۶۰،۰۰۰،۰۰۰) 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 ای مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

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

تبصره ۲ـ آئین 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 ۴ – هرکس به قصد دسترسی به داده های سری موضوع ماده (۳) 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 (۱۰،۰۰۰،۰۰۰)ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد .

ماده ۵ – چنانچه مأموران دولتی که مسؤول حفظ داده های سری مقرر در ماده (۳) 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، حاملهای داده یا سامانه های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰)ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) 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 سامانه 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 میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد:الف) تغییر یا ایجاد داده های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها ،

ب) تغییر داده ها یا علایم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانه داده ها یا علائم 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 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 (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) 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، 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 (۱۰،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۱۰ – هرکس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده ها، تغییر گذرواژه 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 (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۱۱ – هرکس به قصد به خطر انداختن امنیت ، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه 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 های متعلق به دیگری را برباید، چنانچه عین داده ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۱۳ – 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 (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرایم علیه عفت و اخلاق عمومی

ماده ۱۴ – هرکس به وسیله سامانه های رایانه ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) 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 و صور قبیحه باشد.

تبصره ۲ ــ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون (۱،۰۰۰،۰۰۰) ریال تا پنج میلیون (۵،۰۰۰،۰۰۰) ریال جزای نقدی محکوم خواهد شد.

تبصره ۳ ــ 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 ــ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی یا متنی 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 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 یا ترغیب یا 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 (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد .

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون (۲،۰۰۰،۰۰۰) ریال تا پنج میلیون (۵،۰۰۰،۰۰۰) 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 میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم می شود .

تبصره ــ 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 ــ هتک حیثیت و نشر اکاذیب

ماده ۱۶ – 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 (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

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

ماده ۱۷ – هرکس 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 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 میلیون (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) 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 سامانه 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 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 (۵،۰۰۰،۰۰۰) ریال تا چهل میلیون (۴۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ــ 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 و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهد 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 ـ 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.

ماده ۲۱ – ارائه دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرایم رایانه ای و محتوایی که برای ارتکاب جرایم رایانه ای به کار می‌رود را پالایش (فیتلر) 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 غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال و در مرتبه دوم به جزای نقدی از یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال تا یک میلیارد (۱،۰۰۰،۰۰۰،۰۰۰) ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ۱- چنانچه محتوای مجرمانه به تارنماهای (وب سایتهای) 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، تارنما (وب سایت) مزبور تا صدور حکم نهایی پالایش (فیلتر) نخواهد شد.

تبصره ۲- پالایش (فیلتر) 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 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، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه (کمیته) را تشکیل خواهند داد. ریاست کارگروه (کمیته) به عهده دادستان کل کشور خواهد بود.

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

تبصره ۲- کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آنها تصمیم‌گیری کند.

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

ماده ۲۳ – ارائه‌دهندگان 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 سیستم 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 بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخست به جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال و در مرتبه دوم به یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال تا یک میلیارد (۱،۰۰۰،۰۰۰،۰۰۰) ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ـ ارائه‌دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه(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 (۱۰۰،۰۰۰،۰۰۰) ریال تا یک میلیارد (۱،۰۰۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده ۲۵ – هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) 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 قرار دادن گذرواژه 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 غیر مجاز ، شنود غیر مجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی .

تبصره ـ 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 ـ 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 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 با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به طور کلی اعضا 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 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.

هـ) جرم در سطح گسترده ای ارتکاب یافته باشد.

ماده ۲۷ – در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم 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 زیر نیز صالح به رسیدگی خواهند بود:

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

ب) جرم از طریق تارنماهای (وب سایتهای) 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 سایتهای) 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 تارنماهای (وب سایتهای) دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

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

ماده ۲۹ – 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 رأی مقتضی را صادر خواهد کرد.

ماده ۳۰ – قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه های عمومی و انقلاب، 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 انتخاب خواهند 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 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 ۱ــ داده ترافیک هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبداء تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبداء، 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 پروتکل اینترنتی (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 های رایانه ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می‌تواند 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 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 های حفاظت شده را افشا 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 نود و یک روز تا شش ماه یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا ده میلیون (۱۰،۰۰۰،۰۰۰) 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 های حفاظت شده مذکور در مواد (۳۲)، (۳۳) و (۳۴) فوق را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (۳۴) این قانون محکوم خواهد شد.

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

ماده ۳۶ – تفتیش و توقیف داده ها یا سامانه 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 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 ۳۸ – 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 ۳۹ – تفتیش داده ها یا سامانه های رایانه ای و مخابراتی شامل اقدامات ذیل می‌شود:

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 های فشرده یا کارت‌های حافظه.

ج) دستیابی به داده های 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 هر یک ازموارد زیر سامانه های رایانه ای یا مخابراتی توقیف خواهند شد:

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

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

ج) متصرف قانونی سامانه رضایت داده باشد،

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

هـ) تفتیش در محل باعث آسیب داده ها شود،

ماده ۴۲ – توقیف سامانه 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 سامانه، پلمپ سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده ۴۳ – چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده های مرتبط با جرم ارتکابی در سایر سامانه 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 سامانه های مذکور گسترش داده و داده های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده ۴۴ – چنانچه توقیف داده ها یا سامانه های رایانه ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی می شود ممنوع است.

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

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 سامانه 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 ــ شنود محتوای ارتباطات رایانه ای

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

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

فصل سوم ــ 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 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 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 ــ سایر مقررات

ماده ۵۲ – 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 ــ 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 ۵۳ – 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 ۵۴ – 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 قضائیه خواهد رسید .

ماده ۵۵ – شماره مواد (۱) تا (۵۴) این قانون به عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرائم رایانه ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد .

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

قانون فوق مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی روز سه شنبه مورخ پنجم خردادماه یکهزار و سیصد و هشتادو هشت مجلس شورای اسلامی تصویب و در تاریخ ۱۳۸۸،۳،۲۰ به تأیید شورای نگهبان رسید .

آیین نامه جمع آوری و استنادپذیری

ادله الکترونیکی

فصل اول: تعاریف

ماده ۱ـ واژه ها و اصطلاحات بکار برده شده در این آیین نامه در معانی زیر بکار می رود

الف ـ ارائه دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه های رایانه ای یا مخابراتی و ارتباطی داخلی یا بین المللی یا هر شبکه مستقل دیگر فراهم می آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه های رایانه ای یا مخابراتی .

ب ـ ارائه دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه های رایانه ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می کنند تا رأساً یا توسط کاربر متقاضی، داده های رایانه ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه های داخلی یا بین المللی یا هر منظور دیگر ذخیره یا پردازش کنند .

ج ـ ارائه داده های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از داده های حفظ یا نگهداری شده توسط ارائه دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده ها را تحت تصرف یا کنترل دارند .

د ـ جمع آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه های رایانه ای یا مخابراتی یا حامل های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می شوند .

هـ ـ زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی با بکارگیری ابزارها و روش های استاندارد در مراحل شناسایی، کشف، جمع آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا درآورده و ثبت می کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد .

و ـ شنود: عبارت است از هر گونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه ها و تجهیزات سخت افزاری و نرم افزاری مربوط .

زـ مجری حفاظت: شخصی است که به نحوی داده های رایانه ای ذخیره شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می شود .

ح ـ متصرف قانونی: در مورد اشخاص حقیقی، شخص مالک یا شخصی است که به نحوی داده یا سامانه را به صورت مشروع در اختیار دارد یا نماینده یا ولی یا سرپرست قانونی وی. در مورد اشخاص حقوقی دولتی یا عمومی غیردولتی، بالاترین مقام آنها یا نماینده قانونی آنها طبق مقررات مربوط و در مورد سایر اشخاص حقوقی، مدیر یا نماینده قانونی آنهاست .

ط ـ قانون: منظور از قانون در این آیین نامه، قانون جرایم رایانه ای مصوب ۱۳۸۸/۳/۵ می باشد .

تبصره ـ سایر اصطلاحات به شرح تعریف ارائه شده در قوانین دیگر می باشد .

فصل دوم: جمع آوری ادله الکترونیکی

الف: نگهداری داده ها

ماده ۲ـ ارائه دهندگان خدمات دسترسی و میزبانی موظفند از سامانه هایی استفاده نمایند که قابلیت نگهداری داده های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد .

ماده ۳ـ ارائه دهندگان خدمات دسترسی موظفند سامانه های خود را به نحوی تنظیم کنند که کلیه ارتباطات رایانه ای را که از طریق آنها انجام می شود ثبت کنند و کلیه داده های ترافیک مربوط به خود و کاربران مربوط را تا شش ماه پس از ایجاد نگهداری کنند .

تبصره ـ عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی نت ها) موظفند مشخصات هویتی، آدرس، ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی **(IP)** تخصیصی را در دفتر روزانه ثبت نمایند .

ماده ۴ـ ارائه دهندگان خدمت دسترسی موظفند اطلاعات کاربران را حداقل ۶ ماه پس از خاتمه اشتراک یا لغو قرارداد کاربر نگهداری کنند. هویت و نشانی کاربر باید در قرارداد منعقده درج شود .

ماده ۵ـ ارائه دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه دهندگان خدمات میزبانی خارجی 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. برگه اشتراک باید به نحوی تنظیم شود که هویت و نشانی آنان مشخص باشد .

تبصره ۱ـ ارائه دهندگان خدمات میزبانی موظفند سامانه های رایانه ای خود را به نحوی تنظیم کنند که هر گونه تغییر اعم از اصلاح یا حذف محتوا و داده ترافیک حاصل از آن را ذخیره نماید .

تبصره ۲ـ اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می کنند، ارائه دهنده خدمات میزبانی محسوب نمی شوند .

ماده ۶ـ ارائه دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظفند امنیت داده های ترافیکی و محتوای نگهداری و حفاظت شده را مطابق با ضوابط و دستورالعمل هایی که به تصویب رئیس قوه قضاییه می رسد، تأمین نمایند .

ماده ۷ـ داده های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند .

ماده ۸ـ در مواردی که برابر قانون نگهداری و حفاظت داده ها الزامی است، نگهداری و حفاظت باید به گونه ای انجام شود که مدیریت جستجو و گزارش دهی آنها امکان پذیر باشد .

ماده ۹ـ وزارت ارتباطات و فناوری اطلاعات هماهنگی های لازم برای تنظیم زمان سامانه های جمع آوری داده های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می آورد .

ماده ۱۰ـ مرکز آمار و فناوری اطلاعات با همکاری وزارت ارتباطات و فناوری اطلاعات سالانه رویه های فنی نحوه نگهداری، حفاظت، توقیف و ارائه داده ها و اطلاعات کاربران و همچنین راهنماهای عملی حفظ امنیت و استنادپذیری داده ها را تصویب و به ارائه دهندگان خدمات دسترسی و میزبانی و بهره برداران ابلاغ می نماید .

ب: حفاظت از ادله رایانه ای

ماده ۱۱ـ مقام قضایی در جریان تحقیق و فرآیند رسیدگی می تواند دستور حفاظت هر نوع داده رایانه ای ذخیره شده را از جمله داده های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده هایی که نوع و نام آنها موقتاً تغییر یافته و یا داده هایی که برای بررسی آنها نیاز به سخت افزار مخصوصی می باشد، صادر نماید .

تبصره ۱ـ ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون می توانند رأساً دستور حفاظت داده های ذخیره شده را صادر کنند .

تبصره ۲ـ قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می باشد .

ماده ۱۲ـ دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده ها، موضوع و مدت زمان با رعایت تبصره ۲ ماده ۳۴ قانون، باشد .

ماده ۱۳ـ در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می شود .

ماده ۱۴ـ مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجرا و صورت جلسه ای را مشتمل بر زمان اجرای دستور، نحوه حفاظت، حجم و نوع داده های حفاظت شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادرکننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد .

ماده ۱۵ـ دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می شود؛ مگر آن که ابلاغ به آنها مخلّ رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می باشد .

تبصره ـ روش مطمئن روشی است که با توجه به نوع داده ها و طول مدت زمان حفاظت، امکان بهره برداری از داده های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد .

ماده ۱۶ـ حفاظت از داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شود .

ج: ارائه ادله رایانه ای

ماده ۱۷ـ دستور ارائه توسط مقام قضایی صادر می شود و باید به طور صریح و شفاف و مشتمل بر شخص ارائه دهنده، موضوع و نوع داده ها، شیوه و زمان تحویل داده ها و مرجع تحویل گیرنده باشد .

ماده ۱۸ـ ارائه داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه به یکی از شیوه های ذیل باشد :

الف ـ تحویل یک نسخه چاپ شده از داده .

ب ـ تحویل یک نسخه رایانه ای از داده .

ج ـ ایجاد دسترسی به داده .

د ـ انتقال تجهیزات رایانه ای و مخابراتی .

ماده ۱۹ـ هنگام ارائه داده ها صورت جلسه ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می رسد :

الف ـ شماره و تاریخ دستور قضایی ارائه داده ها

ب ـ مشخصات ارائه دهنده

ج ـ مشخصات تحویل گیرنده

د ـ زمان و مکان ارائه

هـ ـ نوع و حجم داده ها

وـ اطلاعات مربوط به نحوه حفظ یا نگهداری داده ها

ز ـ روش های امنیتی بکاررفته در زمان ارائه

ح ـ مشخصات سخت افزاری و نرم افزاری تجهیزات

ط ـ شیوه ارائه و مشخصات داده .

تبصره ۱ـ در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها به عمل می آید .

تبصره ۲ـ یک نسخه از صورت جلسه به مرجع قضایی ارسال می شود و نسخه ای در اختیار ارائه دهنده و نسخه دیگر در اختیار تحویل گیرنده قرار می گیرد .

ماده ۲۰ـ از زمان ارائه داده ها به ضابطان قضایی یا دیگر اشخاص ذیربط، مسئولیت حفظ داده های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود .

ماده ۲۱ـ ارائه داده هایی که افشا یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توأم با تشریفات می باشد، تابع مقررات مربوط است .

ماده ۲۲ـ دستور ارائه داده، مجوز افشای آن نمی باشد و پس از دستور ارائه هر گونه دسترسی به مفاد داده مستلزم صدور دستور قضایی است .

ماده ۲۳ـ اشخاصی که مسئول اجرای هر یک از دستورات قضایی اعم از نگهداری، حفاظت، ارائه، تفتیش و توقیف سامانه و داده یا شنود آن می باشند یا دستور به آنها ابلاغ می شود یا به نوعی مرتبط با دستورات یاد شده هستند، حق افشای مفاد دستور و یا داده ها و اطلاعات مربوط را ندارند .

د: تفتیش و توقیف ادله رایانه ای

ماده ۲۴ـ ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاب می نماید در درخواست خود اعلام نمایند. همچنین، موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند :

الف ـ دلایل ضرورت تفتیش و توقیف

ب ـ حتی الامکان نوع و میزان داده ها و سخت افزارها

ج ـ محل تفتیش یا توقیف

د ـ دلایل لازم برای تصویربرداری و بررسی در خارج از محل

هـ ـ زمان تقریبی لازم برای تفتیش و توقیف .

ماده ۲۵ـ در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی الامکان در محل استقرار سامانه انجام پذیرد .

ماده ۲۶ـ مدت توقیف و فرصت اجرای تفتیش باید در دستور قضایی تصریح و کمترین فرصت ممکن منظور شود. در صورت نیاز به زمان بیشتر، به درخواست مجری تفتیش یا توقیف و ذکر علت آن، این مدت قابل تمدید می باشد .

ماده ۲۷ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود .

ماده ۲۸ـ در مواردی که تفتیش یا توقیف طبق دستور قضایی بدون حضور متصرف قانونی یا شخصی که داده یا سامانه را تحت اختیار دارد، انجام پذیرد، مراتب پس از انجام فوراً به ذینفع ابلاغ خواهد شد .

ماده ۲۹ـ چنانچه پس از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده ها یا سامانه های رایانه ای یا مخابراتی بیم لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی برود مراتب از مرجع قضایی صادرکننده دستور توقیف کسب تکلیف شده و در صورت تشخیص قاضی حسب مفاد ماده ۴۴ قانون عمل می گردد .

ماده ۳۰ـ قوه قضاییه تمهیدات لازم از جمله بسترسازی و ایجاد زیرساخت های ارتباط رایانه ای و الکترونیکی و همچنین راه اندازی سامانه ها و درگاه های مبتنی بر فناوری اطلاعات را جهت تسهیل در عملیاتی کردن فرایندها و روش های موضوع این آیین نامه فراهم می آورد .

ماده ۳۱ـ اشخاصی که داده ها یا سامانه های رایانه ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان پذیر نباشد، نحوه دسترسی به داده ها یا سامانه ها از قبیل ورود به محل، رفع موانع استفاده از سخت افزار و نرم افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد .

ماده ۳۲ـ رضایت متصرف قانونی سامانه موضوع بند ج ماده ۴۱ قانون، باید کتبی و با امضای وی باشد .