

باسمه تعالی

لایحه تراکنش‌های الکترونیکی

بخش یکم: کلیات

گفتار یکم: هدف قانون

ماده ۱. اهداف این قانون عبارتند از:

- الف) اعتباربخشی قانونی به تراکنش‌های الکترونیکی، مانند تراکنش‌های تجاری و کسب‌وکار الکترونیکی، خدمات عمومی و اداری الکترونیکی و تراکنش‌های شخصی؛
- ب) استنادپذیری تراکنش‌های الکترونیکی در دعاوی قضایی و غیرقضایی؛
- پ) فراهم‌سازی پیش‌نیازهای قانونی جایگزینی دیوان‌سالاری سنتی با خدمات دولت الکترونیکی؛
- ت) یکپارچه‌سازی و هماهنگ‌سازی رویه‌ها و فرایندهای اعتباربخشی، اطمینان‌پذیری و استنادپذیری تراکنش‌های الکترونیکی، هم‌سو با رویه‌ها و فرایندهای بین‌المللی؛ و
- ث) حمایت از تراکنش‌های الکترونیکی در برابر اقدامات غیرمجاز و غیرقانونی.

گفتار دوم: تعاریف و اختصارها

ماده ۲. اختصارهای بکار رفته در این قانون عبارتند از:

الف) شورا: شورای عالی فضای مجازی

ب) وزارت: وزارت ارتباطات و فناوری اطلاعات

ماده ۳. تعابیر و واژگان زیر در معنای مشروح بکار می‌روند:

الف) تراکنش الکترونیکی: هرگونه فرایند خودکار یا نیمه خودکار بوسیله سامانه‌های الکترونیکی که موجب پردازش داده‌های قابل استناد رایانه‌ای می‌شود.

ب) تراکنش قابل استناد: هر تراکنشی که با انجام آن امکان استیفای یک حق یا ایفای یک تکلیف قانونی فراهم باشد.

پ) داده قابل استناد: به هر شکل داده رایانه‌ای، مانند متن، صوت، تصویر ویا ترکیبی از آنها و همچنین انواع برنامه‌های رایانه‌ای، علامت، کد و الگوریتم گفته می‌شود.

ت) داده‌ها و اطلاعات تراکنشی: هرگونه داده و اطلاعات که به شکل چاپی یا الکترونیکی نگهداری یا ذخیره شده و امکان اثبات یا رد اعتبارپذیری ویا استنادپذیری تراکنش مورد ادعا را داشته باشد.

ث) پردازش داده‌ها: هرگونه ایجاد، تغییر، ارسال، دریافت، جابه‌جایی، ذخیره‌سازی، حذف، اشتراک‌گذاری یا نمایش هدفمند داده‌های رایانه‌ای است.

ج) دارنده داده‌ها و اطلاعات تراکنشی: همه اشخاص حقوقی و حقیقی که به موجب این قانون تراکنش‌های الکترونیکی عمومی، خصوصی و شخصی را پردازش می‌کنند و در این قانون به اختصار «دارنده» نامیده می‌شوند.

گفتار سوم: دامنه شمول قانون

ماده ۴. در پرتو اهداف این قانون، تراکنش‌های قابل استناد الکترونیکی و داده‌ها و اطلاعات تراکنشی مشمول احکام و ضوابط آن می‌شوند.

ماده ۵. تراکنش‌های الکترونیکی موضوع این قانون در سه گروه زیر قرار می‌گیرند:

الف) تراکنش‌های الکترونیکی عمومی: تراکنش‌هایی که بوسیله سازمان‌ها و نهادهای زیرنظر مستقیم ولی فقیه و قوای سه‌گانه مقننه، مجریه و قضائیه، مجلس خبرگان رهبری، مجمع تشخیص مصلحت نظام، شورای نگهبان، شورای عالی امنیت ملی، شورای عالی انقلاب فرهنگی، شورای عالی و مرکز ملی فضای مجازی، شورای عالی استان‌ها، شوراهای اسلامی شهر و روستا، صدا و سیما و مؤسسات عمومی غیردولتی در حیطه وظایف و اختیاراتشان پردازش می‌شود.

ب) تراکنش‌های الکترونیکی خصوصی: تراکنش‌هایی که بوسیله مؤسسات خصوصی شامل بنگاه‌ها، شرکت‌ها یا نهادهای انتفاعی یا غیرانتفاعی که مشمول مؤسسات عمومی نمی‌شوند، در حیطه فعالیتشان پردازش می‌شود.

پ) تراکنش‌های الکترونیکی شخصی: تراکنش‌هایی که بوسیله اشخاص حقیقی پردازش می‌شود.

تبصره - در جایی که احکام این قانون، هم شامل مؤسسات عمومی و هم شامل مؤسسات خصوصی می‌شود، به اختصار «مؤسسات» بکار می‌رود.

ماده ۶. تراکنش‌های الکترونیکی موضوع این قانون به سه شکل زیر پردازش می‌شوند:

الف) تراکنش‌های الکترونیکی سامانه‌های رایانه‌ای و یا مخابراتی با یکدیگر؛

ب) تراکنش‌های الکترونیکی اشخاص و سامانه‌های رایانه‌ای و یا مخابراتی با یکدیگر؛ و

پ) تراکنش‌های الکترونیکی اشخاص با یکدیگر.

بخش دوم: اطمینان‌پذیری تراکنش‌ها

گفتار یکم: دسترس‌پذیری تراکنش‌ها و داده‌ها و اطلاعات تراکنشی

ماده ۷. هر شخص حق جستجو و دسترسی به داده‌ها و اطلاعات تراکنشی راجع به تراکنش‌های الکترونیکی قابل استناد خویش را دارد، مگر اینکه قانون صراحتاً منع کرده باشد.

ماده ۸. دسترس‌پذیری داده‌ها و اطلاعات تراکنشی به منزله افشای غیرمجاز آنها نیست و رعایت ضوابط مربوط الزامی است.

ماده ۹. درخواست دسترسی به داده‌ها و اطلاعات تراکنشی به صورت کتبی یا الکترونیکی از سوی ذی‌نفع یا نماینده قانونی وی به دارنده ارائه می‌شود.

ماده ۱۰. درخواست دسترسی به داده‌ها و اطلاعات تراکنشی شامل موضوع و نوع آنها، مشخصات درخواست‌کننده و اطلاعاتی که بتوان بوسیله آنها به او پاسخ داد، از قبیل نشانی پستی، شماره تماس یا رایانامه و شیوه پیشنهادی درخواست‌کننده می‌شود. دارنده حق دارد از پاسخ به درخواست‌های کلی و مبهم خودداری کند.

ماده ۱۱. دارنده موظف است با رعایت قوانین و مقررات مربوط نسبت به ارائه داده‌ها و اطلاعات تراکنشی اقدام کند و حق ندارد به دلایل واهی از ایفای این وظیفه خودداری کند.

ماده ۱۲. در صورتی که ارائه اطلاعات درخواست شده به موجب قانون صراحتاً ممنوع باشد، دارنده موظف است دلایل امتناع خود را به طور مستند و به شکل چاپی یا الکترونیکی به درخواست‌کننده ارائه دهد.

ماده ۱۳. هرگاه قرائن و اوضاع و احوال دلالت داشته باشد که ارائه داده‌ها و اطلاعات تراکنشی درخواست‌شده برای حفظ جان یا سلامتی یا آزادی یا حیثیت اشخاص ضروری است یا از خسارت مالی یا معنوی شدید به آنها یا از بروز یا گسترش خطرهای زیست‌محیطی جلوگیری می‌کند، دارنده موظف به ایفای فوری آن خواهد بود.

ماده ۱۴. دارنده باید در کمترین زمان نسبت به پاسخگویی اقدام کند و در هر صورت ارائه داده‌ها و اطلاعات تراکنشی درخواستی نباید بیش از ده روز از زمان دریافت درخواست به طول انجامد.

تبصره- هرگاه به دلایل موجه ارائه داده‌ها و اطلاعات درخواست شده در مهلت مقرر امکان‌پذیر نباشد، دارنده باید درخواست‌کننده را از دلایل مذکور به شکل مستند و مکتوب یا الکترونیکی آگاه کند و در هر حال مدت پاسخگویی نباید بیشتر از ۲۰ روز باشد.

ماده ۱۵. چنانچه اطلاعات درخواست شده نزد دارنده دیگری باشد، دریافت‌کننده درخواست باید درخواست‌کننده را راهنمایی کند.

ماده ۱۶. دریافت‌کنندگان درخواست حق ندارند از درخواست‌کننده هیچ‌گونه دلیل یا توضیحی درباره داده‌ها و یا اطلاعات موردنیاز خود بخواهند.

ماده ۱۷. دارنده باید به شیوه پیشنهادی درخواست‌کننده پاسخ دهد، مگر اینکه امکانات لازم جهت ارائه اطلاعات به شیوه مزبور را نداشته باشد.

ماده ۱۸. چنانچه دریافت‌کنندگان درخواست، مؤسسات باشند، باید رسید کتبی یا الکترونیکی شامل شماره ثبت، تاریخ دریافت و نام و سمت خود را به درخواست‌کننده تحویل دهند.

ماده ۱۹. درخواست‌کننده باید هزینه ارائه داده‌ها و اطلاعات درخواست‌شده را بپردازد. درخصوص داده‌ها و اطلاعات تراکنشی عمومی، مطابق تعرفه مصوب وزارت اقدام خواهد شد. درخصوص داده‌ها و اطلاعات تراکنشی خصوصی و شخصی، دارنده حق ندارد هزینه نامتعارفی را مطالبه کند.

ماده ۲۰. دارندگان داده‌ها و اطلاعات تراکنشی موظفند آنها را حداقل دو سال پس از ایجاد یا دو سال پس از آخرین پردازش انجام شده به نحوی نگهداری کنند که اطمینان‌پذیری آنها محفوظ بماند. مگر اینکه قانون مهلت بیشتری را مقرر کرده باشد.

ماده ۲۱. شیوه‌نامه‌ی دسترسی‌پذیری داده‌ها و اطلاعات تراکنشی عمومی، خصوصی و شخصی ظرف شش‌ماه به پیشنهاد وزارت به تصویب شورا می‌رسد.

گفتار دوم: صحت و تمامیت تراکنش‌ها و داده‌ها و اطلاعات تراکنشی

ماده ۲۲. اعتبار‌پذیری و استناد‌پذیری تراکنش‌های الکترونیکی منوط به احراز صحت و تمامیت آنهاست که با احراز صحت و تمامیت داده‌های ورودی تراکنش به عمل می‌آید.

ماده ۲۳. هرگاه داده‌های تراکنش پردازش شده باشد، صحت و تمامیت آن در صورتی قابل احراز است که داده‌ها و اطلاعات تراکنشی مربوط، مانند داده‌های رخدانگار (Log Files) در دسترس باشد و با بررسی آنها بتوان مجاز بودن اقدامات مذکور را احراز کرد.

ماده ۲۴. دارنده حق ندارد داده‌ها و اطلاعات تراکنشی قابل استناد را بدون آگاهی ذی‌نفع آنها پردازش کند. مگر اینکه به موجب قانون اجازه‌ی چنین کاری را داشته یا رضایت صریح یا ضمنی وی را دریافت کرده یا عرفاً ظن منطقی مبنی بر وجود چنین رضایتی را داشته باشد. در هر حال نگهداری داده‌ها و اطلاعات راجع به آنها برپایه‌ی ضوابط مقرر الزامی است.

ماده ۲۵. دارنده موظف است رویه‌ها، فرایندها، فناوری‌ها و سامانه‌های نرم‌افزاری و یا سخت‌افزاری مطمئنی را برای نگهداری داده‌ها و اطلاعات تراکنشی ذی‌نفعان به کار گیرد تا صحت و تمامیت آنها تضمین گردد.

ماده ۲۶. آیین‌نامه‌ی تضمین صحت و تمامیت داده‌ها و اطلاعات تراکنشی عمومی، خصوصی و شخصی، ظرف سه ماه به پیشنهاد وزارت به تصویب شورا خواهد رسید.

گفتار سوم: محرمانگی تراکنش‌ها و داده‌ها و اطلاعات تراکنشی

ماده ۲۷. نقض محرمانگی تراکنش‌های الکترونیکی مانع اعتبار و استناد‌پذیری آنها نیست، مگر اینکه از سوی استناد‌کننده‌ی داده‌ها و اطلاعات راجع به آنها یا به درخواست یا دستور وی صورت گرفته باشد.

ماده ۲۸. محرمانگی تراکنش‌ها و داده‌ها و اطلاعات تراکنشی عمومی برپایه طبقه‌بندی داده‌ها و اطلاعات راجع به آنها تعیین می‌شود.

ماده ۲۹. محرمانگی تراکنش‌ها و داده‌ها و اطلاعات تراکنشی خصوصی برپایه داده‌ها و اطلاعات راجع به حریم مکان کار، مانند اسرار تجاری و ارتباطات غیرعمومی آنها تعیین می‌شود.

تبصره - منظور از اسرار تجاری هرگونه اطلاعات، فرمول‌ها، الگوها، نرم‌افزارها و برنامه‌ها، ابزار و روش‌ها، تکنیک‌ها و فرایندها، تألیفات منتشر نشده، روش‌های انجام تجارت و داد و ستد، فنون، نقشه‌ها و فراگردها، اطلاعات مالی، فهرست مشتریان، طرح‌های تجاری و مانند آنهاست که ارزش اقتصادی دارند و در دسترس عموم قرار ندارند و دارنده آنها اقدامات متعارفی را برای صیانت از آنها در برابر سوءاستفاده‌های مختلف انجام داده است.

ماده ۳۰. محرمانگی تراکنش‌های الکترونیکی شخصی برپایه داده‌ها و اطلاعات راجع به حریم تمامیت فردی، حریم اقامتگاه، حریم مکان کار، ارتباطات غیرعمومی و اطلاعات شخصی و به موجب قوانین و مقررات مربوط تعیین می‌شود.

تبصره - منظور از اطلاعات شخصی هرگونه اطلاعات وابسته به افراد، نظیر نام و نام خانوادگی، نشانی اقامتگاه و کار، شغل، اطلاعات مالی و بانکی، شماره تماس، وضعیت خانوادگی، عادت‌های فردی، وضعیت جسمی و روانی و همچنین اطلاعات راجع به گرایش‌های جنسی، اعتقادی، سیاسی یا صنفی و وضعیت نژادی و قومی است.

ماده ۳۱. قواعد و ضوابط حاکم بر طبقه‌بندی و تعریف سطوح دسترسی به داده‌ها و اطلاعات تراکنشی عمومی به موجب آیین‌نامه پیشنهادی وزارت خواهد بود که ظرف شش‌ماه جهت تصویب به شورا تقدیم می‌کند.

بخش سوم: اعتبارپذیری تراکنش‌ها

گفتار یکم: هویت کنشگران تراکنش

ماده ۳۲. منظور از کنشگران تراکنش، شخص و یا سامانه‌ای است که تراکنش را به سرانجام می‌رساند. در تراکنش خودکار پدیدآورنده سامانه نرم‌افزاری و یا مالک آن کنشگر بشمار می‌آید.

ماده ۳۳. تراکنش الکترونیکی منسوب به کنشگر آنست، مگر اینکه خلاف آن ثابت شود.

ماده ۳۴. کنشگر تراکنش می‌تواند برای صیانت از حریم هویتی خود، به شکل گمنام یا با هویت ساختگی تراکنش را به سرانجام برساند، مگر اینکه به موجب قانون بکارگیری هویت واقعی الزامی باشد. چنانچه تراکنش

به صورت گمنام یا با هویت ساختگی به سرانجام رسد، در صورتی معتبر است که مخاطب یا ذی‌نفع تراکنش هویت واقعی آن را احراز کند.

ماده ۳۵. هرگاه علاوه بر کنشگر، اشخاص یا سامانه‌های دیگری نیز در سرانجام یافتن تراکنش دخالت داشته باشند، هویت آنها نیز باید قابل احراز باشد.

گفتار دوم: ابزارها و رویه‌های اعتباربخشی تراکنش

ماده ۳۶. هویت کنشگر تراکنش برپایه شناسه‌های کاربردی برای شخص یا سامانه احراز می‌شود، مانند شماره سیم‌کارت، بارکد، شماره سریال، امضای الکترونیکی، امضای دیجیتالی، انواع شناسه‌های زیست‌سنجی، نام کاربری، شماره تلفن و نشانی رایانامه.

ماده ۳۷. شناسه هویتی باید شرایط زیر را داشته باشد:

الف) نسبت به کنشگر خود منحصر بفرد باشد؛

ب) هویت کنشگر خود را بطور مشخص و متمایز نشان دهد، مانند اینکه شخص حقوقی عمومی است یا خصوصی یا فرد عادی یا امکان احراز تعلق سامانه به هریک از آنها؛

پ) به شکل معتبر و قانونی ایجاد و واگذار شده باشد.

ماده ۳۸. صرف برخورداری یک تراکنش از شناسه الکترونیکی به معنای معتبر بودن آن نیست و صحت و تمامیت آن نیز باید احراز شود. مگر اینکه شناسه الکترونیکی بکاررفته از لحاظ فنی توانایی اثبات صحت و تمامیت تراکنش را نیز داشته باشد.

ماده ۳۹. شناسه‌های الکترونیکی به سه دسته زیر تقسیم می‌شوند:

الف) شناسه الکترونیکی مطمئن: شناسه‌ای که ساختن نمونه مشابه یا تغییر آن از لحاظ فنی تقریباً غیرممکن است؛

ب) شناسه الکترونیکی ایمن: شناسه‌ای که اطمینان‌پذیری آن با توجه به نوع کاربری موردنظر از سوی پدیدآورنده‌اش تأیید شده است.

پ) شناسه الکترونیکی عادی: شناسه‌ای که مشمول شناسه‌های بندهای «الف» و «ب» این ماده نمی‌شود.

ماده ۴۰. دریافت شناسه الکترونیکی منوط به ارائه اطلاعات زیر از سوی درخواست کننده است:

الف) نام و نام خانوادگی برای اشخاص حقیقی و نام و شماره ثبت برای مؤسسات خصوصی؛

ب) نشانی پستی اقامتگاه و یا مکان کار؛

پ) شماره تماس و نشانی رایانامه؛ و

ت) حیطة کاری که قرار است برای تراکنش‌های آن شناسه الکترونیکی درخواستی بکار رود و ویژگی‌های فنی و اجرایی متناسب با آن، به درخواست ارائه‌دهنده شناسه.

تبصره ۱. اطلاعات ارائه شده از سوی درخواست‌کننده شناسه الکترونیکی مشمول ضوابط نگهداری و محرمانگی داده‌ها و اطلاعات تراکنشی می‌شود و دسترسی به آنها پیرو ضوابط مربوط خواهد بود.

تبصره ۲. هرگاه شناسه الکترونیکی به اشخاص حقیقی فعال یا مرتبط با مؤسسات اختصاص می‌یابد، ثبت اطلاعات راجع به آنها مطابق این ماده الزامی است.

تبصره ۳. در صورت تغییر اطلاعات، گیرنده شناسه موظف است فوراً ارائه‌دهنده شناسه را آگاه کند.

ماده ۴۱. گواهی تأیید اعتبار شناسه الکترونیکی از سوی ارائه‌دهنده آن برای ذی‌نفعان تراکنش صادر می‌شود. ذی‌نفع تراکنش هر شخصی است که امکان بکارگیری آن را به عنوان یک تراکنش قابل استناد دارد.

تبصره - صدور گواهی تأیید اعتبار برای ذی‌نفع منوط به ارائه اطلاعات موضوع ماده (۴۰) به جز بند «ت» آن خواهد بود.

ماده ۴۲. گواهی تأیید اعتبار شناسه الکترونیکی شامل اطلاعات زیر می‌شود:

الف) هویت واقعی و ساختگی (در صورت ایجاد) دارنده شناسه؛

ب) حوزه‌هایی که بکارگیری شناسه الکترونیکی موردنظر در آنها اعتبار دارد؛

پ) نام و مشخصات ارائه‌دهنده شناسه؛

ت) نام و مشخصات درخواست‌کننده گواهی اعتبار؛

ث) مدت زمان اعتبار شناسه الکترونیکی؛

ج) مرجعی که قرار است گواهی برای آن صادر گردد، مگر اینکه ذی‌نفع برای خود درخواست کرده باشد.

ماده ۴۳. گواهی تأیید اعتبار شناسه الکترونیکی با رعایت ضوابط اطمینان‌پذیری و اعتبارپذیری می‌تواند به صورت چاپی یا الکترونیکی صادر شود.

ماده ۴۴. در تراکنش‌های زیر بکارگیری شناسه الکترونیکی مطمئن الزامی است:

الف) معاملاتی که در خصوص اموال غیرمنقول به انجام می‌رسد؛

ب) امور مربوط به احوال شخصیه شهروندان ایرانی و اتباع خارجی؛

پ) امور مربوط به مهاجرت و سفرهای برون‌مرزی، مانند گذرنامه و روادید؛

ت) امور مربوط به اسناد و اوراق قضایی؛

ث) امور مربوط به سلامت، بهداشت، درمان و تأمین اجتماعی شهروندان؛

ج) امور مربوط به ثبت و تأسیس مؤسسات خصوصی؛

چ) امور مربوط به اسناد الکترونیکی واجد ارزش پول و اوراق بهادار بانکی؛

ح) معاملات منقولی که ارزش آنها بیش از یک میلیارد ریال است.

تبصره - میزان ارزش معاملات منقول مندرج در بند «ج» براساس نرخ تورم رسمی و حسب اعلام بانک مرکزی هر سه سال یک بار به پیشنهاد وزارت و تصویب هیأت وزیران قابل تعدیل است.

ماده ۴۵. اشخاص حق دارند از کنشگر یا مخاطب تراکنش بخواهند شناسه الکترونیکی ایمن را بکار برد، مگر اینکه امکان بکارگیری آن فراهم نباشد که در این صورت حق ندارند به صرف بکارگیری شناسه عادی از سوی کنشگر یا مخاطب تراکنش اعتبار آن را رد کنند. اثبات اعتبار تراکنش دارای شناسه عادی به عهده بکارگیرنده آن خواهد بود.

ماده ۴۶. نسبت به تراکنش‌های دارای شناسه الکترونیکی مطمئن ادعای انکار و تردید مسموع نیست و تنها امکان طرح دعوای جعل امکان‌پذیر است.

ماده ۴۷. در موارد زیر از شناسه الکترونیکی لغو اعتبار می‌گردد:

الف) به موجب دستور مقام صلاحیت‌دار قضایی؛

ب) فوت یا انحلال شخص حقیقی یا حقوقی یا از کارافتادن سامانه دارنده شناسه الکترونیکی؛

پ) پایان مدت اعتبار شناسه الکترونیکی؛

ت) درخواست دارنده شناسه الکترونیکی.

تبصره - در جایی که اعتبار شناسه الکترونیکی به دلیل کارایی فنی پایان می‌یابد، ارائه‌دهنده موظف است دارنده شناسه را آگاه و در صورت رضایت وی شناسه معتبر دیگری را جایگزین آن کند.

ماده ۴۸. هرگاه ارائه‌دهنده شناسه الکترونیکی به موجب حکم صادره از سوی مراجع صلاحیت‌دار یا دلایل دیگر امکان ادامه فعالیت و ارائه خدمات به کاربران خود را نداشته باشد، موظف است با هماهنگی وزارت نسبت به جایگزینی ارائه‌دهنده خدمات دیگر اقدام کند.

گفتار سوم: مراجع تعیین و تأیید اعتبار تراکنش

ماده ۴۹. وزارت مرجع تعیین اعتبار تراکنش‌های الکترونیکی است. اشخاص حقوقی که از وزارت پروانه خدمات شناسه‌های الکترونیکی را دریافت کرده‌اند، مراجع تأیید اعتبار تراکنش‌های الکترونیکی شناخته می‌شوند.

ماده ۵۰. وظایف وزارت برای اجرای این قانون عبارتند از:

الف) بررسی صلاحیت و اعطای پروانه فعالیت به ارائه‌دهندگان شناسه‌های الکترونیکی؛

ب) تدوین و پیشنهاد آیین‌نامه‌های مقرر در این قانون جهت تصویب نزد مراجع صلاحیت‌دار؛

پ) انجام نظارت‌های کارآمد و اثربخش بر نحوه فعالیت ارائه‌دهندگان شناسه‌های الکترونیکی، بویژه رعایت تعهدات کمی و کیفی آنها در ارائه خدمات و اعمال ضمانت اجراهای راجع به تخلفات ارتکاب‌یافته از سوی آنها

برپایه آیین‌نامه مصوب شورا و معرفی مؤسسات عمومی متخلف به مراجع صلاحیتدار رسیدگی‌کننده به تخلفات اداری؛

ت) استانداردگزینی فنی - اجرایی برای امور مربوط به شناسه‌های الکترونیکی به تفکیک سطوح مطمئن، ایمن و عادی؛

ث) تعامل با نهادها و مراجع معتبر فراملی درباره امور مرتبط با این قانون؛

ج) هدایت و حمایت از پژوهش‌های علمی و کاربردی مرتبط با این قانون؛

چ) تعامل با دستگاه‌های اجرایی دست‌اندرکار و ذی‌ربط به منظور اجرای شایسته مقررات این قانون؛

ح) رسیدگی به گزارش‌ها و شکایات ذی‌نفعان شناسه‌های الکترونیکی درباره موارد نقض مقررات این قانون؛

خ) همکاری با مراجع صلاحیتدار دادگستری در خصوص رسیدگی به پرونده‌های مرتبط با این قانون؛

د) فراهم‌آوردن زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری و نرم‌افزاری موردنیاز برای اجرای مقررات این قانون با اولویت بهره‌برداری از توان فنی، اقتصادی و اجرایی بخش غیردولتی؛

ذ) تدوین و ابلاغ منشور اخلاقی و کدهای رفتاری برای ارائه‌دهندگان خدمات، کاربران و ناظران تراکنش‌های الکترونیکی؛

ر) اجرای طرح ملی بیمه تراکنش‌های الکترونیکی.

ماده ۵۱. آن دسته از دستگاه‌های اجرایی که تاکنون در زمینه تعیین و تأیید اعتبار شناسه‌های الکترونیکی فعالیت داشته‌اند، مانند امضای الکترونیکی، امضای دیجیتالی و زیست‌سنج‌ها، موظفند برپایه سیاست‌های مصوب شورا و هماهنگی با سازمان، نسبت به یکپارچه‌سازی و سازگاری زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری و نرم‌افزاری یکدیگر اقدام نمایند.

ماده ۵۲. مجوزهای ارائه شناسه‌های الکترونیکی مطمئن، ایمن و عادی بطور جداگانه و پس از احراز شرایط زیر برای مؤسسات خصوصی صادر می‌شود:

الف) صلاحیت امنیتی پس از استعلام از سوی مراجع صلاحیتدار؛

ب) صلاحیت فنی، از قبیل برخورداری از زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری و نرم‌افزاری موردنیاز برپایه سطح و گستره فعالیت؛

پ) توانایی اداری - اجرایی به منظور پشتیبانی کاربران برپایه سطح و گستره فعالیت؛ و

ت) تابعیت ایرانی.

ماده ۵۳. ارائه شناسه‌های الکترونیکی از سوی مؤسسات عمومی منوط به داشتن شرایط برشمرده برای مؤسسات خصوصی موضوع ماده فوق و اخذ پروانه از وزارت است.

ماده ۵۴. آیین‌نامه صدور پروانه خدمات شناسه‌های الکترونیکی ظرف سه ماه از تاریخ تصویب این قانون به پیشنهاد وزارت به تصویب شورا می‌رسد.

بخش چهارم: استنادپذیری تراکنش‌ها

گفتار یکم: مقررات عمومی

ماده ۵۵. تراکنش‌هایی استنادپذیر بشمار می‌آیند که انکارناپذیری و اطمینان‌پذیری آنها محرز باشد.

ماده ۵۶. برای احراز انکارناپذیری تراکنش باید موارد زیر به اثبات برسد:

الف) اثبات هویت کنشگر، اعم از واقعی و یا ساختگی؛ و

ب) انتساب تراکنش به کنشگر.

ماده ۵۷. برای اثبات انتساب می‌توان به داده‌ها و اطلاعاتی استناد کرد که رابطه کنشگر با تراکنش را از لحاظ فنی به شکل متمایز اثبات می‌کند. وزارت موظف است ظرف سه ماه آیین‌نامه داده‌ها و اطلاعات فنی قابل استناد برای اثبات انتساب تراکنش‌ها در محیط‌های قابل پردازش رایانه‌ای را به تصویب شورا برساند و همواره روزآمد نگاه دارد.

ماده ۵۸. برای احراز اطمینان‌پذیری تراکنش باید ثابت شود که هرگونه پردازش آن با رعایت ضوابط قانونی، مقرراتی و قراردادی یا مبتنی بر توافق بوده و غیرمجاز سرانجام نیافته است.

ماده ۵۹. ارائه یا ادای ادله قانونی، شامل اقرار، شهادت، سوگند یا اسناد رسمی بوسیله تراکنش‌های الکترونیکی در صورتی استنادپذیر است که از شناسه الکترونیکی مطمئن برخوردار و اطمینان‌پذیری آنها نیز محرز باشد.

ماده ۶۰. استنادپذیری تراکنش‌های الکترونیکی مطمئن با اتیان سوگند یا ادای اقرار یا شهادت قابل رد نیست.

ماده ۶۱. در صورت جمع بودن شرایط زیر، استنادپذیری تراکنش الکترونیکی مفروض انگاشته می‌شود:

الف) کنشگر تراکنش هیچ سمتی در دعوا نداشته و یا ذی‌نفع آن نباشد؛

ب) کنشگر تراکنش را برپایه سازوکارها، رویه‌ها و یا فرایندهای استاندارد و متعارف پردازش کرده باشد؛

پ) تراکنش بخشی از فرایند مرسوم و پیوسته کنشگر باشد، مانند تراکنش‌هایی که در ارائه خدمات عمومی الکترونیکی به سرانجام می‌رسند؛ و

ت) ظن منطقی درباره اطمینان‌پذیری تراکنش وجود داشته باشد و در صورت کاستی یا نارسایی اجرایی و یا فنی به حیطة تراکنش موردنظر مربوط نباشد.

ماده ۶۲. استناد به تراکنش الکترونیکی به عنوان دلیل مستقیم تنها در صورتی بلامانع است که از شناسه الکترونیکی مطمئن برخوردار باشد. منظور از دلیل مستقیم دلیلی است که بدون واسطه موضوع دعوا را اثبات یا رد کند.

ماده ۶۳. نسخه‌های چاپی ارائه‌شده از تراکنش الکترونیکی اصل بشمار می‌آیند. مشروط بر آنکه نسخه الکترونیکی آنها در دسترس باشد.

ماده ۶۴. هرگاه بخشی از تراکنش به صورت چاپی و بخشی دیگر به صورت الکترونیکی پردازش شده باشد، در صورتی استنادپذیر خواهد بود که یکپارچگی فرایند برپایه ضوابط اطمینان‌پذیری و اعتبارپذیری احراز گردد.

ماده ۶۵. تراکنش الکترونیکی علیه کنشگر آن استنادپذیر است، مگر اینکه بتواند انتساب آن را انکار و اطمینان‌پذیری آن را رد کند.

ماده ۶۶. ارائه‌دهندگان خدمات تراکنش‌های الکترونیکی موظف به ارائه داده‌ها و اطلاعات تراکنشی مطابق ضوابط دسترس‌پذیری آنها و همچنین سایر اسناد و مستندات مورد نیاز مرجع رسیدگی به دعاوی مرتبط با تراکنش‌های الکترونیکی هستند. این اشخاص عبارتند از:

الف) ارائه‌دهندگان خدمات دسترسی: هر شخص حقیقی یا حقوقی که امکان ارتباط با شبکه‌های رایانه‌ای را با ارائه خدماتی از قبیل تلفن همراه، تلفن ثابت و ارتباطات داده‌ها، خدمات عمومی انتقال داده‌ها از طریق خطوط کابلی (PAP)، خدمات انتقال داده‌ها از طریق ارتباطات ماهواره‌ای (SAP)، خدمات ارتباطات بی‌سیم مبتنی بر فناوری WiMAX، خدمات تلفن اینترنتی (VoIP) و خدمات مخابراتی ارتباطات همراه بین‌المللی ماهواره‌ای (GMPCS) فراهم می‌آورد. ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت‌ها) و مؤسسات که برای کارکنان و اعضای خود شبکه رایانه‌ای درون‌سازمانی ملی یا فراملی راه‌اندازی می‌کنند، در حکم ارائه‌دهنده خدمات دسترسی هستند.

ب) ارائه‌دهندگان خدمات میزبانی: اشخاصی که سامانه‌های رایانه‌ای و مخابراتی متعلق به خود یا متقاضی اینگونه خدمات را که در قلمرو حاکمیتی ایران قرار دارند، به منظور ذخیره یا پردازش محتوای رایانه‌ای، جهت انتشار، توزیع یا ارائه در شبکه‌های رایانه‌ای ملی یا فراملی یا هر جهت دیگر مدیریت می‌کنند. آن دسته از دستگاه‌های اجرایی و اشخاص حقوقی خصوصی که پایگاه‌های داده درون‌سازمانی راه‌اندازی می‌کنند، در حکم ارائه‌دهنده خدمات میزبانی‌اند. انباشت موقت داده‌ها در جریان ارائه خدمات دسترسی، خدمات میزبانی به شمار نمی‌آید.

پ) تأمین‌کنندگان محتوای تراکنش الکترونیکی: پدیدآورندگان و عرضه‌کنندگان مجاز انواع داده‌های قابل استناد و نرم‌افزارهای رایانه‌ای؛

ت) خدمات فناوری اطلاعات و ارتباطات: مانند خدمات مدیریت و امنیت فناوری اطلاعات؛

ث) ارائه‌دهندگان شناسه‌های الکترونیکی.

گفتار دوم: مقررات اختصاصی

ماده ۶۷. هرگاه به موجب شکایت کیفری، ضابطان دادگستری مسؤول گردآوری و ارائه تراکنش‌های الکترونیکی به محاکم صلاحیتدار دادگستری شوند، موظف به رعایت ضوابط این قانون هستند.

ماده ۶۸. مسؤولیت‌های راجع به نگهداری، حفاظت فوری و ارائه داده‌ها و اطلاعات تراکنشی و همچنین اقداماتی که به‌هنگام تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی و شنود محتوای ارتباطات رایانه‌ای نسبت به تراکنش‌های الکترونیکی به انجام می‌رسد، با رعایت احکام بخش دوم قانون جرایم رایانه‌ای مصوب ۱۳۸۸ خواهد بود.

ماده ۶۹. کلیه اقداماتی که از سوی ضابطان دادگستری در فرایند تفتیش، توقیف، بازیابی، مستندسازی، جابه‌جایی، نگهداری و ارائه داده‌ها و تراکنش‌های الکترونیکی به انجام می‌رسد، با رعایت احکام مربوط به اطمینان‌پذیری و اعتبارپذیری این قانون و به منظور تأمین زنجیره حفاظتی، برپایه آیین‌نامه استنادپذیری تراکنش‌های الکترونیکی در دادرسی کیفری به عمل می‌آید که ظرف سه ماه از سوی وزارت با همکاری نیروی انتظامی جمهوری اسلامی ایران تهیه و جهت تصویب تقدیم شورا می‌شود.

ماده ۷۰. به منظور رعایت احکام اطمینان‌پذیری و اعتبارپذیری نسبت به تراکنش‌های الکترونیکی موضوع اقدامات ضابطان دادگستری، آیین‌نامه موضوع ماده فوق شامل ضوابط زیر می‌شود:

الف) احراز هویت همه مقامات تصمیم‌گیر و مأمورانی که در فرایند استنادپذیری به هر نحو و به هر میزان دخالت یا مشارکت داشته‌اند؛

ب) نحوه دستیابی به داده‌ها و اطلاعات، بویژه داده‌ها و اطلاعاتی که مشمول ضوابط گوناگون محرمانگی می‌شوند؛

پ) رویه‌ها، فرایندها و شگردها، مانند فنون تحقیقاتی ویژه که به موجب آنها اقدامات موضوع این آیین‌نامه تعریف و اجرا می‌شوند، به تفکیک موقعیت شبکه‌ای و سامانه‌های مستقل؛

ت) ابزارها، امکانات و سامانه‌های سخت‌افزاری و نرم‌افزاری که در اجرای این آیین‌نامه به کار گرفته می‌شوند؛ و

ث) قوانین و مقرراتی که به موجب آنها اقدامات ضابطان دادگستری مجاز شمرده می‌شود.

بخش پنجم: مسؤولیت‌ها و ضمانت اجراها

گفتار یکم: مسؤولیت مدنی و جبران‌ها

بند یکم: صلاحیت محاکم مدنی

ماده ۷۱. در دعاوی مدنی راجع به تراکنش‌های الکترونیکی، دادگاه محل سرانجام‌یافتن تراکنش صالح به رسیدگی می‌باشد.

ماده ۷۲. هرگاه در یک دعوا چند تراکنش الکترونیکی مورد استناد قرار گرفته باشد، دادگاه محل سرانجام یافتن تراکنشی که دلیل مستقیم دعوا شناخته می‌شود یا دادگاه محل بیشترین تراکنش‌های سرانجام یافته صالح به رسیدگی می‌باشد.

ماده ۷۳. در صورت بروز اختلاف در صلاحیت، مطابق مقررات آیین دادرسی مدنی عمل خواهد شد.

بند دوم: زیان‌های مادی و معنوی ناشی از تراکنش‌ها

ماده ۷۴. زیان مادی ناشی از جرایم و تخلفات این قانون مطابق مقررات آیین دادرسی کیفری قابل مطالبه است.

ماده ۷۵. در صورت اثبات ورود خسارت معنوی، دادگاه به درخواست زیان دیده علاوه بر الزام مرتکب به اعاده حیثیت، وی را با لحاظ تأثیر هتک حیثیت و جایگاه اجتماعی زیان دیده و میزان زیانهای مادی وارد شده، به پرداخت ده میلیون تا یک میلیارد ریال خسارت در حق وی محکوم می‌کند.

ماده ۷۶. در موارد زیر، چنانچه فعل زیان بار در جهت منافع و به نام اشخاص حقوقی ارتکاب یابد، شخص حقوقی نیز تضامنا مسؤول جبران خسارت خواهد بود:

الف) چنانچه مدیر شخص حقوقی مرتکب فعل زیان بار شود؛

ب) چنانچه مدیر شخص حقوقی دستور یا درخواست ارتکاب فعل زیان بار را داده باشد؛

پ) هرگاه یکی از کارکنان شخص حقوقی با آگاهی مدیر یا در اثر تقصیر وی مرتکب فعل زیان بار شود.

گفتار دوم: تخلفات و ضمانت اجرای مقرراتی

ماده ۷۷. تخلفات موضوع این قانون عبارتند از:

الف) عدم رعایت ضوابط مربوط به دسترس پذیری و ارائه داده‌ها و اطلاعات تراکنشی درخواستی برخلاف ضوابط مقرر؛

ب) عدم رعایت ضوابط راجع به تأمین صحت و تمامیت و محرمانگی داده‌ها و اطلاعات تراکنشی؛

پ) عدم رعایت ضوابط راجع به ایجاد و واگذاری شناسه‌های الکترونیکی؛

ت) عدم رعایت ضوابط راجع به ثبت و روزآمدسازی اطلاعات کاربران تراکنش‌های الکترونیکی؛

ث) عدم رعایت ضوابط مربوط به لغو اعتبار شناسه الکترونیکی؛

ج) عدم رعایت ضوابط مربوط به کیفیت و پشتیبانی خدمات تراکنش الکترونیکی؛ و

چ) عدم رعایت ضوابط مربوط به حفظ صلاحیت‌های امنیتی، فنی، اداری - اجرایی و تابعیت ایرانی.

ماده ۷۸. چنانچه هریک از کارکنان مؤسسات عمومی مقررات این قانون را نقض کند، علاوه بر جریمه مقرر از سوی شورا، برای بار نخست به یکی از تنبیهات اداری مقرر در بندهای «ج» یا «د» ماده ۹ قانون رسیدگی به تخلفات اداری مصوب ۱۳۷۲ و برای بار دوم به یکی از تنبیهات اداری مقرر در بندهای «ه» تا «ز» ماده مزبور و برای بار سوم به یکی از تنبیهات مقرر در بندهای «ح» تا «ک» آن ماده محکوم خواهد شد.

ماده ۷۹. هرگاه مؤسسات خصوصی برپایه شرایط برشمرده برای مسؤولیت کیفری اشخاص حقوقی، مرتکب تخلفات این قانون شوند، به ترتیب زیر به ضمانت اجراهای مقرراتی محکوم خواهند شد:

الف) چنانچه ارائه‌دهنده خدمات تراکنش الکترونیکی باشند، برپایه ضوابط مقرر از سوی شورا به ضمانت اجراهای پروانه‌ای شامل لغو، تعلیق و کاهش مدت اعتبار پروانه، جریمه نقدی، ممنوع‌الخروج شدن مدیران مؤسسه، محرومیت از تمدید اعتبار پروانه و یا اخذ سایر پروانه‌های خدمات تراکنش‌های الکترونیکی محکوم خواهد شد.

ب) چنانچه ارائه‌دهنده خدمات تراکنش الکترونیکی نباشند، در صورتی که از سوی یک دستگاه اجرایی پروانه فعالیت اخذ کرده باشند، مشمول ضمانت اجراهای مقرر در بند فوق می‌شوند و در غیر این صورت، به دستور دادگاه صلاحیتدار به انحلال مؤسسه، تعلیق فعالیت، جریمه نقدی و محرومیت از فعالیت در حیطه موردنظر محکوم خواهند شد.

تبصره - درخصوص مؤسسات مشمول بند «ب» این ماده، وزارت می‌تواند به نمایندگی از شاکیان حقیقی و حقوقی، نزد مراجع صلاحیتدار اقامه دعوا کند.

ماده ۸۰. هرگاه اشخاص حقیقی تخلفات موضوع این قانون را نسبت به تراکنش‌های در اختیار خود مرتکب شوند، برپایه ضوابط مقرر از سوی شورا، به محرومیت از ارائه و یا کاربری خدمات تراکنش الکترونیکی و یا خدمات عمومی الکترونیکی محکوم می‌شوند.

ماده ۸۱. وزارت موظف است ظرف سه ماه فهرست تفصیلی تخلفات این قانون را به تفکیک حوزه‌های برشمرده در ماده (۷۷) و ضمانت اجرای مقرراتی آنها را به موجب پیش‌نویس آیین‌نامه تخلفات و ضمانت اجرای مقرراتی تراکنش‌های الکترونیکی جهت تصویب تقدیم شورا کند.

ماده ۸۲. به هنگام تعریف، تخصیص و تعیین ضمانت اجرای مقرراتی برای هریک از کارکنان مؤسسات عمومی، مؤسسات خصوصی و اشخاص حقیقی متخلف، رعایت معیارهای با‌دارندگی، اثربخشی و تناسب ضمانت اجراها با تخلفات الزامی است و در این خصوص شاخص‌هایی چون شدت و گستردگی زیان‌های مادی و یا معنوی، هویت زیان‌دیده یا زیان‌دیدگان، انگیزه متخلف، شیوه ارتکاب تخلف، مانند سازمان‌یافتگی مرتکبان و دستاوردهای بالقوه و یا بالفعل ناروای ناشی از ارتکاب تخلف مدنظر قرار خواهد گرفت.

گفتار سوم: مسؤولیت کیفری و ضمانت اجراها

بند یکم: صلاحیت محاکم کیفری

ماده ۸۳. هرگاه همه یا بخشی از تراکنش الکترونیکی مجرمانه بر روی سامانه رایانه‌ای واقع در قلمرو حاکمیتی ایران پردازش شده باشد، در حکم جرم رایانه‌ای واقع شده در ایران است.

تبصره - منظور از تراکنش الکترونیکی مجرمانه تراکنشی است که به وسیله آن یک جرم رایانه‌ای ارتکاب می‌یابد یا آماج یک جرم رایانه‌ای قرار می‌گیرد.

ماده ۸۴. چنانچه محتوای تراکنش مجرمانه بوسیله تارنمای دارای دامنه مرتبه بالای کد کشوری ایران (.ir) توزیع یا منتشر شود یا به هر نحو در دسترس قرار گیرد، در حکم جرم واقع شده در ایران است.

تبصره - دامنه‌های مرتبه بالای کد کشوری ایران، اعم از سطح یک مانند iran.ir یا سطح دو iran.ac.ir یا معادل فارسی آنها، یعنی «ایران» مشمول این ماده می‌شوند.

ماده ۸۵. در صورتی می‌توان مرتکب تراکنش الکترونیکی مجرمانه را تحت پیگرد قرار داد که در ایران حضور داشته باشد یا به ایران مسترد گردد.

ماده ۸۶. در موارد زیر، مقام صلاحیتدار قضایی با رعایت مقررات قانونی شروع به تحقیق می‌کند:

الف) محتوای تراکنش مجرمانه در سامانه رایانه‌ای واقع در حوزه قضایی محل مأموریت وی ذخیره شده باشد؛

ب) محتوای تراکنش مجرمانه در سامانه رایانه‌ای واقع در حوزه قضایی دیگری ذخیره شده، ولی جرم رایانه‌ای در حوزه قضایی محل مأموریت او کشف یا متهم در آن حوزه دستگیر شده باشد؛ و

پ) محتوای تراکنش مجرمانه در سامانه رایانه‌ای واقع در حوزه قضایی دیگری ذخیره شده، اما متهم یا مظنون به ارتکاب جرم در حوزه قضایی محل مأموریت او مقیم باشد.

ماده ۸۷. چنانچه جرم موضوع این قانون در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای تخصصی جرایم رایانه‌ای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده ۸۸. در صورت بروز اختلاف در صلاحیت، موارد ذیل مبنای تعیین مرجع قضایی اصلح قرار می‌گیرد:

الف) حضور متهم در حوزه قضایی؛

ب) ذخیره بودن محتوای تراکنشی مجرمانه موردنظر در سامانه(های) واقع در حوزه قضایی؛

پ) وجود دلایل و امارات معتبر و استنادپذیر در حوزه قضایی؛

ت) حضور بزه‌دیده به عنوان شاکی در حوزه قضایی؛ و

ث) توانایی مرجع قضایی به لحاظ برخورداری از ضابطان قضایی آموزش‌دیده و آزمایشگاه جنایی رایانه‌ای.

بند دوم: جرایم و مجازات‌ها

ماده ۸۹. هرکس بدون دریافت پروانه قانونی به ارائه خدمات تراکنشی الکترونیکی بپردازد، به جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا حبس از یک سال تا سه سال یا هر دو مجازات محکوم خواهد شد.

ماده ۹۰. در موارد زیر، مرتکب به جزای نقدی از بیست تا دویست میلیون ریال محکوم خواهد شد، مگر اینکه در قوانین دیگر کیفر شدیدتری مقرر شده باشد:

الف) از ارائه ویا دسترس‌پذیری داده‌ها و اطلاعات تراکنشی در اختیار خود خودداری کند؛

ب) به قصد عدم ارائه یا دسترس‌پذیری داده‌ها و اطلاعات تراکنشی، از نگهداری‌شان خودداری کند؛ و

پ) مانع ارائه یا دسترس پذیری داده‌ها و اطلاعات تراکنشی به درخواست‌کننده آنها شود.

تبصره - چنانچه داده‌ها و اطلاعات به موضوعات مندرج در ماده (۱۳) این قانون مربوط شود و در پی ارتکاب رفتارهای مقرر در این ماده پیامدهای برشمرده رخ دهد، مرتکب علاوه بر حداکثر جزای نقدی به حبس از سه تا ده سال محکوم خواهد شد.

ماده ۹۱. رسیدگی به جرایم علیه محرمانگی و صحت و تمامیت داده‌ها و اطلاعات تراکنشی و همچنین سوءاستفاده‌های مالی از تراکنش‌های الکترونیکی به موجب قوانین مربوط، بویژه قانون جرایم رایانه‌ای، مصوب ۱۳۸۸ خواهد بود.

ماده ۹۲. صدور غیرمجاز گواهی تأیید اعتبار شناسه الکترونیکی و استناد غیرمجاز به آن، حسب مورد موجب محکومیت به کیفر جعل و استفاده از سند یا داده مجعول رایانه‌ای خواهد بود.

ماده ۹۳. رسیدگی به کیفر اشخاص حقوقی مرتکب جرایم این قانون، مطابق شرایط مقرر در مواد (۱۹) و (۲۰) قانون جرایم رایانه‌ای، مصوب ۱۳۸۸ خواهد بود.

ماده ۹۴. دادگاه می‌تواند مرتکب را برای بار اول یا در صورت تکرار جرایم موضوع این قانون، از ارائه یا کاربری خدمات الکترونیکی عمومی محروم کند. آیین‌نامه خدمات عمومی مشمول این ماده و ضوابط راجع به چگونگی اجرای احکام قضایی آن به پیشنهاد وزارت و با همکاری وزارت دادگستری به تصویب شورا می‌رسد.

بخش ششم: مقررات پایانی

ماده ۹۵. وزارت موظف است هر شش‌ماه یا به دستور شورا گزارشی از پیشرفت مقررات این قانون را ارائه کند.

ماده ۹۶. از تاریخ تصویب این قانون قوانین مغایر زیر لغو می‌شوند:

الف) مواد (۵) تا (۳۲) قانون تجارت الکترونیکی، مصوب ۱۳۸۲؛ و

ب) مواد (۴۹)، (۵۰) و (۵۴) قانون جرایم رایانه‌ای، مصوب ۱۳۸۸.