به نام خدا

پیش‌نویس لایحه

«صیانت و حفاظت از داده‌های شخصی»

(مرداد ماه ۱۳۹۷)

فهرست عناوین

مقدمه توجیهی

در اجرای:

الف) اصول مختلف فصل سوم قانون اساسی جمهوری اسلامی ایران راجع به «حقوق ملت»، به‌ویژه اصول نوزدهم، بیستم، بیست‌ودوم، بیست‌وسوم، بیست‌وپنجم، بیست‌وششم، سی‌وهشتم و سی‌ونهم؛ و

ب) سیاست‌های کلی نظام، ابلاغی مقام معظم رهبری مدظله‌العالی درباره:

۱. شبکه‌های اطلاع‌رسانی رایانه‌ای (به‌ویژه بندهای ۱ و ۷)؛

۲. نظام اداری (به‌ویژه بند ۲۳)؛

۳. پدافند غیرعامل (به‌ویژه بند ۱۱)؛

۴. امنیت فضای تولید و تبادل اطلاعات و ارتباطات (به‌ویژه بند ۱)؛ و

۵. برنامه ششم توسعه (به‌ویژه بندهای ۳۶ و ۵۳-۳)، و

پ) سایر قوانین مربوط، ازجمله و به‌ویژه:

۱. قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات؛

۲. قانون انتشار و دسترسی آزاد به اطلاعات؛

۳. قانون تجارت الکترونیکی؛

۴. قانون مجازات اسلامی ـ بخش تعزیرات؛

۵. قانون آیین دادرسی کیفری؛

۶. قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌نمایند؛

۷. قانون برنامه ششم توسعه؛

۸. قانون مطبوعات؛

۹. قانون اهداف و وظایف وزارت فرهنگ و ارشاد اسلامی؛

۱۰. قانون سلامت نظام اداری و مبارزه با فساد؛

۱۱. قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری؛

۱۲. قانون تجارت؛

۱۳. قانون حمایت از حقوق مصرف‌کنندگان؛ و

۱۴. قانون نظام صنفی.

و در عمل به فتوای مقام معظم رهبری مبنی بر حرام شرعی بودن نقض حریم خصوصی «قانون صیانت و حفاظت از داده‌های شخصی» به تصویب می‌رسد.

باب یکم: کلیات

بخش یکم: هدف قانون

ماده ۱. هدف اصلی این قانون صیانت از حیثیت و کرامت اشخاص موضوع داده‌ها از راه‌های ذیل است که قواعد و احکام آن‌ها در بخش‌های مربوط آمده است:

الف) تبیین حقوق اشخاص موضوع داده‌ها، به‌ویژه در تعامل با سایر حق‌های مشروع؛

ب) ضابطه‌مندی فرایند پردازش داده‌های شخصی؛

پ) مسئولیت‌پذیری پردازش؛

ت) هم‌افزایی امور تنظیمی و نظارتی پردازش؛ و

ث) جبران‌پذیری زیان‌ها و آسیب‌های پردازش.

بخش دوم: تعاریف

ماده ۲. تعاریف واژگان ذیل عبارت‌اند از:

الف) داده شخصی عبارت است از داده‌ای که به‌تنهایی یا به همراه داده‌های دیگر، مستقیم یا غیر مستقیم شخص موضوع داده را از طریق ارجاع به یک شناسه می‌شناساند.

ب) **داده شخصی حساس** عبارت است از داده شخصی که ریشه قومی یا قبیله ای، نظرات سیاسی، مذهبی و فلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار می‌سازد.

ب) پردازش هرگونه عملیات دستی یا خودکار بر داده‌های شخصی، شامل و نه محدود به ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه‌وتحلیل، طبقه‌بندی، ساختاربندی، تطبیق، ذخیره‌سازی، اشتراک‌گذاری، فرستادن، توزیع و عرضه، انتشار و در دسترس قرار دادن و پاک کردن آن‌ها.

پ) کنترل‌گر شخصی است که همه یا بخشی از هدف، سازوکار، شرایط، ویژگی‌ها و ابزارهای یک یا چند عملیات پردازش داده‌های شخصی در اختیار پردازشگر را تعیین می‌کند. مصوبات و تصمیمات مراجع صلاحیت‌دار در امور تنظیم‌گری، نظارت، ضابطین و دادرسی درباره پردازش داده‌های شخصی، جز در مواردی که جنبه فردی دارد، کنترل‌گری به شمار نمی‌آید.

ت) پردازشگر شخص مأذون کنترل‌گر در پردازش است. در صورت نبود کنترل‌گر یا عدم امکان اتصاف پردازش به آن، پردازشگر به‌عنوان کنترل‌گر نیز شناخته می‌شود.

ث) ناظر ویژه کسی است که پیرو حکم صادره از سوی کمیسیون، صلاحیت نظارت بر پردازش داده‌های شخصی را می‌یابد.

بخش سوم: دامنه شمول قانون

ماده ۳. اشخاص مشمول این قانون عبارت‌اند از:

الف) اتباع ایرانی حقیقی یا حقوقی عمومی یا خصوصی، اعم از آنکه داده‌های شخصی آن‌ها درون یا بیرون از ایران پردازش شود.

ب) اتباع خارجی حقیقی یا حقوقی عمومی یا خصوصی که داده‌های شخصی آن‌ها از سوی کنترل‌گر یا پردازشگر ایرانی پردازش می‌شود.

باب دوم: حقوق اشخاص موضوع داده‌ها

بخش یکم: رضایت به پردازش

ماده ۴. پردازش داده‌های شخصی مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی، منوط به رضایت شخص موضوع آن‌هاست.

ماده ۵. اعلام رضایت اشخاص موضوع داده باید با رعایت شرایط ذیل باشد:

الف) پیش از پردازش باشد؛

ب) بیانگر آگاهی شخص موضوع داده باشد؛ و

پ) استنادپذیر باشد.

ماده ۶. پردازش داده‌های شخصی مربوط به وضعیت‌ها یا موقعیت‌های عمومی، بدون رضایت شخص یا اشخاص موضوع آن‌ها در صورتی بلامانع است که:

الف) خودش داده‌ها را در معرض پردازش قرار داده باشد؛ یا

ب) پردازش داده‌های خود را منع یا محدود نکرده باشد.

ماده ۷. رضایت حاصل از فریب یا تهدید یا اکراه شخص موضوع داده معتبر نیست و در صورت عدم اهلیت وی، رضایت ولی یا قیم او الزامی است. حالات اغما و مانند آن‌که بر نبود قصد و اراده وی دلالت دارند، موجب عدم اهلیت‌اند.

بخش دوم: درخواست پردازش یا توقف آن

ماده ۸. شخص موضوع داده حق دارد هر زمان، پردازش یا عدم پردازش همه یا بخشی از داده‌ها را از کنترل‌گر بخواهد، مشروط بر آنکه:

الف) داده‌ها یا نتایج حاصل از آن‌ها نادرست باشد؛

ب) داده‌ها یا پردازش آن‌ها خارج از محدوده رضایت وی باشد.

ماده ۹. درخواست انجام یا توقف پردازش داده‌های شخصی می‌تواند با هدف فراموشی مطرح شود، مشروط بر آنکه ذی‌نفع دیگری نباشد.

بخش سوم: انجام پردازش

ماده ۱۰. در شرایط ذیل، شخص موضوع داده حق دارد به داده‌های شخصی خود به‌منظور پردازش آن‌ها دسترسی یابد:

الف) شامل اطلاعات طبقه‌بندی‌شده عمومی یا داده‌های شخصی دیگران نشود؛

ب) استنادپذیری داده‌ها مخدوش نشود.

بخش چهارم: گمنامی در پردازش

ماده ۱۱. رضایت به پردازش، به معنای آشکاری هویت شخص موضوع داده‌ها نیست و حق دارد گمنامی‌اش در محدوده رضایت رعایت گردد.

تبصره- آشکاری هویت به معنای آگاهی اشخاص غیرمجاز از نام و نام خانوادگی شخص موضوع داده یا شناسه‌های تخصیص‌یافته و منتسب به آن است.

بخش پنجم: تعارض با حقوق دیگران

ماده ۱۲. در موارد ذیل، پردازش داده‌های شخصی در چارچوب قوانین مربوط، بدون رضایت اشخاص موضوع آن‌ها بلامانع است:

الف) برای صیانت از حیثیت، جان یا مال شخص موضوع داده ضروری باشد؛

ب) برای صیانت از حیثیت یا جان دیگری یا پیشگیری از زیان مالی شدید به او ضروری باشد؛

پ) برای پیشگیری یا پاسخ به تهدیدهای نظم، ایمنی و امنیت عمومی ضروری باشد؛

ت) برای کشف جرائم یا تخلفات یا شناسایی متهمان یا اجرای احکام قضایی و انتظامی ضروری باشد.

تبصره ــ استناد به هریک از معاذیر بالا تنها در صورتی موجه است که گزینه دیگری امکان‌پذیر نباشد.

ماده ۱۳. بهره‌برداری مالکانه از داده‌های شخصی، بدون رضایت شخص موضوع آن‌ها در صورتی بلامانع است که:

الف) گمنامی وی حفظ شود؛

ب) عرفاً زیان مادی یا معنوی برای وی نداشته باشد؛

پ) جلب رضایت وی عملاً امکان‌پذیر نباشد.

ماده ۱۴. در صورت تزاحم حق‌های دو یا چند شخص موضوع داده با یکدیگر، اولویت‌های ذیل رعایت گردد:

الف) آسیب‌های حیثیتی بر زیان‌های مالی؛

ب) اشخاص دارای ویژگی‌های فردی شامل سن و جنسیت یا دارای ویژگی‌های اجتماعی، مانند شغل، قومیت و مذهب که عرفاً آسیب‌پذیرند بر سایر اشخاص؛

پ) عدم رضایت بر رضایت ضمنی و هر دو آن‌ها بر رضایت صریح اشخاص موضوع داده؛

ت) وضعیت‌ها یا موقعیت‌های غیرعمومی بر وضعیت‌ها یا موقعیت‌های عمومی.

باب سوم: تعهدات کنترل‌گران و پردازشگران

بخش یکم: دامنه تعهدات کنترل‌گران و پردازشگران

ماده ۱۵. تعهدات مقرر در این باب به عهده کنترل‌گر است، مگر اینکه به‌موجب قانون یا توافق یا قرارداد، پردازشگر عهده‌دار آن‌ها شود.

ماده ۱۶. همه کارکردهای فرایند پردازش داده‌های شخصی باید بر پایه دستور یا درخواست مستند کنترل‌گر باشد. در غیر این صورت، پردازشگر به‌عنوان کنترل‌گر پردازش هم شناخته می‌شود.

ماده ۱۷. چنانچه هریک از کارکردهای پردازش، کنترل‌گر یا پردازشگر مختص به خود را داشته باشد، تنها نسبت به همان کارکرد تعهد خواهند داشت.

ماده ۱۸. در صورت تعدد کنترل‌گران یا پردازشگران در هر کارکرد، فرض بر تعهد برابر آن‌هاست. مگر اینکه خلاف آن ثابت شود.

بخش دوم: اعتبارپذیری پردازش

بند یکم: مجاز بودن

ماده ۱۹. درجایی که اخذ رضایت از شخص موضوع داده الزامی است، متناسب با نوع و میزان پردازش، فراوانی اشخاص موضوع داده، شیوه اعلام رضایت از سوی آن‌ها و هزینه‌های مترتبه، رضایت‌نامه مربوط تدوین و به‌عنوان جزء لاینفک توافق پردازش لحاظ می‌گردد.

ماده ۲۰. نقش‌آفرینی در هریک از کارکردهای پردازش داده‌های شخصی به‌عنوان یک شغل یا حرفه مستقل، ولو به شکل موردی یا موقت، اعم از انتفاعی یا غیرانتفاعی، مستلزم دارا بودن پروانه یا گواهی از مرجع صلاحیت‌دار مربوط است.

تبصره ـ دارا بودن پروانه یا گواهی موضوع این ماده به‌منزله معافیت از سایر الزامات این قانون، به‌ویژه اخذ رضایت از اشخاص موضوع داده نیست و رعایت آن‌ها الزامی است.

ماده ۲۱. مشاغل کنترل‌گر یا پردازشگر داده‌های شخصی، در صورتی از الزام مقرر در ماده بالا معاف‌اند که صرفاً داده‌های شخصی مشتریان بالقوه یا بالفعل خود را تنها برای موضوع فعالیت خود پردازش نمایند.

ماده ۲۲. هرگونه واگذاری شغلی یا حرفه‌ای داده‌های شخصی، علاوه بر رعایت سایر مقررات، مستلزم ثبت در سامانه مرجع صلاحیت‌دار ذی‌ربط است.

بند دوم: نظارت‌پذیری

ماده ۲۳. نظارت از نگاه این قانون، شامل هرگونه اقدام مراجع صلاحیت‌دار نظارتی برای تأیید اعتبارپذیری، اعتمادپذیری، استنادپذیری یا الزامات پردازش فرامرزی داده‌های شخصی می‌شود، ازجمله مصاحبه، بررسی، بازرسی یا حسابرسی، رصد، ردیابی، پایش یا کنترل حضوری یا برخط موارد ذیل:

الف) مدیران، متصدیان و بهره‌برداران مستقیم یا مرتبط با پردازش داده‌های شخصی؛

ب) زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری و نرم‌افزاری، اعم از اختصاصی یا مشترک فراهم آمده برای پردازش داده‌های شخصی؛ و

پ) اسناد، اطلاعات و داده‌های کاغذی یا دیجیتالی راجع و مرتبط با پردازش داده‌های شخصی.

ماده ۲۴. فراهم آوردن همه امکانات، تجهیزات و نیروی انسانی موردنیاز برای حسن ایفای تعهدات نظارت‌پذیری پردازش، حسب مورد به عهده کنترل‌گر یا پردازشگر است.

ماده ۲۵. توافق کنترل‌گر یا پردازشگر با اشخاص موضوع داده یا دیگران درباره نظارت آن‌ها بر پردازش، تا جایی معتبر است که به تعهدات نظارتی این قانون خدشه وارد نیاورد.

بخش سوم: اعتمادپذیری پردازش

بند یکم: شفافیت

ماده ۲۶. کنترل‌گر یا پردازشگر موظف است اطلاعات ذیل را در اختیار یا در دسترس اشخاص موضوع داده قرار دهد:

الف) هدف پردازش، از قبیل، اقتصادی، اجتماعی، فرهنگی، سلامت و رفاه و حقوقی و قضایی و امنیتی؛

ب) نوع و نحوه پردازش، از قبیل تجمیع، تغییر، تجزیه‌وتحلیل، اشتراک‌گذاری، نگهداری و پاک کردن داده‌ها؛

پ) هویت، ماهیت و فعالیت کنترل‌گران یا پردازشگران اصلی و مرتبط؛

ت) موقعیت‌ها و وضعیت‌های پردازش، اعم از عمومی و غیرعمومی؛

ث) منابع پردازش، از قبیل پایگاه‌های اطلاعات مؤسسات عمومی یا خصوصی یا برگزاری آمایش‌ها و پیمایش‌های گوناگون؛

ج) ویژگی‌ها و شرایط فنی پردازش، به‌ویژه ازلحاظ برمی‌گزینی داده‌های شخصی اتباع ایرانی موضوع بخش پنجم این قانون؛

چ) گواهی‌ها یا پروانه‌های دریافت شده از مراجع صلاحیت‌دار؛

ح) سطح ایمنی و امنیت پردازش و دانش و هزینه مترتب بر آن؛

خ) حق‌های اشخاص موضوع داده نسبت به پردازش داده‌های شخصی‌شان و چگونگی استیفای آن‌ها؛

د) ناظر ویژه پردازش و سایر مراجع صلاحیت‌دار نظارتی و رسیدگی‌کننده به شکایات اشخاص موضوع داده.

تبصره ـ کنترل‌گر یا پردازشگر موظف است ظرف یک ماه از تاریخ دریافت داده‌های شخصی، مطابق این ماده اطلاع‌رسانی کند.

ماده ۲۷. اطلاع‌رسانی به اشخاص موضوع داده باید با شرایط و ویژگی‌های فردی و اجتماعی و امکانات در اختیار و سطح فراگیری آن‌ها سازگاری داشته باشد و علاوه بر پیام‌رسانی‌های همگانی و اختصاصی، در قالب مستنداتی از قبیل «شرایط و ملاحظات پردازش» به انجام رسد، تا آنجا که از آگاهی آن‌ها اطمینان حاصل شود.

بند دوم: تهدیدناپذیری

ماده ۲۸. هریک از کارکردها و مراحل پردازش، باید از تمهیدات ایمنی و امنیتی ویژه خود برخوردار باشد. این تمهیدات باید هر سه سطح ذیل را در برگیرند:

الف) ایمنی و حفاظت فیزیکی، شامل زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری مرتبط؛

ب) ایمنی و حفاظت اطلاعات، شامل انواع پردازنده‌های سخت‌افزاری و نرم‌افزاری؛ و

پ) ایمنی و حفاظت انسانی، شامل همه کنترل‌گران و پردازشگران اصلی و مرتبط.

ماده ۲۹. سازوکارها و ابزارهای سخت‌افزاری و نرم‌افزاری ایمنی و حفاظتی مقرر یا پیشنهادی باید با شرایط ذیل سازگار باشد:

الف) نوع و میزان آسیب‌زایی تهدیدهای بالقوه و بالفعل از نگاه اشخاص موضوع داده؛

ب) تأمین‌پذیری آن‌ها؛ و

پ) توانمندی فنی و اجرایی.

ماده ۳۰. اشخاص موضوع داده تنها در صورتی می‌توانند کنترل‌گر یا پردازشگر را به رعایت تمهیدات ایمنی و حفاظتی فراتر از ضوابط مراجع صلاحیت‌دار ملزم کنند که اجرای آن تمهیدات ایفای تعهدات آن‌ها را مختل نکرده و هزینه‌های آن را نیز عهده‌دار شوند.

بند سوم: پاسخگویی

ماده ۳۱. کنترل‌گران در برابر اشخاص موضوع داده از پاسخگویی کامل برخوردارند؛ اعم از آنکه تعهداتشان با آن‌ها پیرو عقد لازم، منعقدشده یا در تفاهم‌نامه یا اسنادی مانند خط‌مشی‌های حریم خصوصی مندرج باشد.

ماده ۳۲. فرض بر عدم اعراض حق اشخاص موضوع داده‌ها است و کنترل‌گر مکلف به ایفای همگی آن‌ها بوده، مگر اینکه بتوانند خلاف آن را ثابت کنند.

بخش چهارم: استنادپذیری پردازش

ماده ۳۳. کنترل‌گر یا پردازشگر موظف است همه یا هریک از داده‌ها و اطلاعات ذیل را تا حداقل تا شش‌ماه پس از پاک‌شدن داده‌های شخصی نگهداری کند:

الف) داده‌های رخدادنگار (Log Files) و داده‌های ترافیک حاصل از پردازش داده‌های شخصی؛

ب) اطلاعات هویتی اشخاص موضوع داده‌ها؛

پ) انواع پردازش‌های انجام‌شده بر روی داده موردنظر و هدف یا اهداف آن؛

ت) اطلاعات هویتی کنترل‌گران یا پردازشگران مرتبط با پردازش موردنظر.

تبصره- کمیسیون می‌تواند زمان نگهداری و حفاظت از اطلاعات و داده‌های موضوع این ماده را حسب مورد تا دو سال افزایش دهد.

ماده ۳۴. چنانچه صحت و تمامیت داده‌های شخصی اصلی مخدوش شده باشد، کنترل‌گر یا پردازشگر موظف است همه نسخه‌های اصلی و مخدوش شده داده‌ها را به مدت شش ماه از تاریخ آخرین پردازش موجب خدشه نگهداری نماید.

ماده ۳۵. داده‌ها و اطلاعات موضوع این بخش علیه کنترل‌گر و پردازشگر آن قابل استناد است.

ماده ۳۶. در صورت ابلاغ رویه‌ها و دستورالعمل‌های حفاظتی عمومی از سوی مراجع صلاحیت‌دار، اجرای آن در پردازش داده‌های شخصی الزامی و هزینه آن به عهده کنترل‌گر یا پردازشگر مربوط است.

تبصره ۱. اجرای رویه‌ها و دستورالعمل‌های خصوصی زنجیره حفاظتی، منوط به تأمین هزینه آن‌ها از سوی درخواست‌کننده و عدم مغایرت با رویه‌های عمومی است.

تبصره ۲. کنترل‌گر می‌تواند در صورت تعارض رویه‌ها و دستورالعمل‌ها از کمیسیون درخواست تعیین ارجحیت و اولویت کند.

بخش چهارم: پردازش‌های فرامرزی

ماده ۳۷. در موارد ذیل، پردازش داده‌های شخصی، فرامرزی انگاشته می‌شود:

الف) هریک از کنترل‌گران یا پردازشگران تابعیت خارجی داشته باشند؛

ب) سامانه‌های پردازنده داده‌ها در بیرون از قلمرو حاکمیتی جمهوری اسلامی ایران قرار داشته باشد؛

ماده ۳۸. در خصوص پردازش داده‌های شخصی اتباع ایرانی، رعایت شرایط ذیل الزامی است:

الف) تنها در مراکز داده واقع در قلمرو حاکمیتی جمهوری اسلامی ایران یا مراکز داده خارجی مورد تأیید مراجع صلاحیت‌دار ذخیره شوند؛

ب) همه پردازنده‌های سخت‌افزاری و نرم‌افزاری از گواهی مراجع صلاحیت‌دار ذی‌ربط برخوردار باشند؛

پ) بر روی شبکه ارتباطی مطمئن جابه‌جا شوند؛

ت) صلاحیت کنترل‌گران و پردازشگران خارجی مورد تأیید مراجع ذی‌ربط قرارگرفته باشد؛

ث) پردازش‌های فرامرزی بر پایه ضوابط مقرر به ثبت برسد.

باب چهارم: تنظیم و نظارت بر پردازش داده‌های شخصی

ماده ۳۹. تنظیم و نظارت بر پردازش داده‌های شخصی به عهده ارکان ذیل است:

الف) کمیسیون صیانت و حفاظت از داده‌های شخصی؛

ب) هیأت نظارت؛

پ) کارگروه‌های تخصصی؛ و

پ) دبیرخانه اجرایی کمیسیون.

بخش یکم: کمیسیون صیانت و حفاظت از داده‌های شخصی

بند یکم: اعضای کمیسیون

ماده ۴۰. کمیسیون از اعضای ذیل تشکیل می‌شود:

۱. وزیر ارتباطات و فناوری اطلاعات به‌عنوان رئیس کمیسیون؛

۲. وزیر اطلاعات؛

۳. وزیر کشور؛

۴. وزیر دادگستری؛

۵. وزیر فرهنگ و ارشاد اسلامی؛

۶. وزیر اقتصاد و امور دارایی؛

۷. دبیر شورای عالی و رئیس مرکز ملی فضای مجازی؛

۸. معاون پیشگیری از وقوع جرم قوه قضائیه؛

۹. رئیس کمیسیون اصل نودم مجلس شورای اسلامی؛

۱۰. دادستان کل کشور؛ و

۱۱. دبیر شورای اجرایی فناوری اطلاعات به‌عنوان دبیر کمیسیون.

تبصره ۱. به تشخیص رئیس کمیسیون، جلسات در سطح اعضا یا معاونین ذی‌ربط آن‌ها با دعوت‌نامه رسمی تشکیل می‌شود.

تبصره ۲. احکام عضویت نمایندگان اعضاء از سوی رئیس کمیسیون صادر می‌شود.

بند دوم: وظایف و اختیارات کمیسیون

ماده ۴۱. کمیسیون وظایف و اختیارات ذیل را به عهده دارد:

الف) همسوسازی امور تنظیم و نظارت کارگروه‌های تخصصی با یکدیگر و همچنین با هیأت نظارت؛

ب) تعدیل، تجمیع، تلفیق یا تفکیک وظایف و یا اعضای کارگروه‌های تخصصی بر پایه اختیارات قانونی آن‌ها؛

پ) تصویب آیین‌نامه داخلی و دبیرخانه کمیسیون؛

ت) حل‌وفصل اختلافات بین کارگروه‌های تخصصی و هیأت نظارت و همچنین با سایر نهادهای حاکمیتی؛

ث) پیشنهاد مصوبات راهبردی و تقنینی موردنیاز به مراجع ذی‌ربط؛

ج) هماهنگی مصوبات و تصمیمات کمیسیون، کارگروه‌های تخصصی و هیأت نظارت با مقررات اداری کشور؛

چ) صدور احکام رؤسای کارگروه‌های تخصصی و ناظران ویژه؛

ح) استماع گزارش هیأت نظارت و ناظران ویژه درباره مأموریت‌های محوله از سوی کمیسیون و تصمیم‌گیری درباره آن‌ها؛ و

خ) گزارش به مراجع بالادستی درباره وضعیت صیانت از داده‌های شخصی و تنظیم و نظارت بر پردازش آن‌ها.

ماده ۴۲. مصوبات و تصمیمات کمیسیون برای کارگروه‌های تخصصی و هیأت نظارت لازم‌الاتباع است.

بند سوم: جلسات و مصوبات کمیسیون

ماده ۴۳. جلسات کمیسیون با حضور دوسوم اعضاء و مصوبات آن با رأی اکثریت حاضران رسمیت می‌یابد.

ماده ۴۴. حضور اعضاء و کارشناسان کارگروه‌های تخصصی و همچنین سایر مقامات، خبرگان و کارشناسان با حق اظهارنظر در جلسات کمیسیون به تشخیص رئیس کمیسیون بلامانع است.

بند چهارم: دبیرخانه کمیسیون

ماده ۴۵. دبیرخانه کمیسیون در محل وزارت ارتباطات و فناوری اطلاعات تشکیل می‌شود.

ماده ۴۶. وظایف دبیر کمیسیون عبارت‌اند از:

الف) انجام امور دبیرخانه‌ای کمیسیون؛

ب) هماهنگی و نظارت بر دبیرخانه‌های اجرایی کارگروه‌های تخصصی و هیأت نظارت؛

پ) اطلاع‌رسانی و ابلاغ مصوبات و تصمیمات کمیسیون؛

ت) برگزاری و تنظیم دستور جلسات، دعوت از اعضاء و سایرین و هماهنگی امور آن؛

ث) پیشنهاد آیین‌نامه اجرایی دبیرخانه جهت تصویب در کمیسیون.

بخش دوم: کارگروه‌های تخصصی صیانت و حفاظت از داده‌های شخصی

بند یکم: تشکیل کارگروه‌ها

ماده ۴۷. کارگروه‌های تخصصی، متشکل از نمایندگان نهادهای متولی امور حاکمیتی مرتبط با صیانت و حفاظت از داده‌های شخصی هستند که به وظایف مقرر در این قانون می‌پردازند.

ماده ۴۸. در نخستین جلسه کمیسیون، آیین‌نامه تشکیل کارگروه‌ها مشتمل بر بخش‌ها و حیطه کار آن‌ها، ریاست، دبیر و محل دبیرخانه، اعضاء، تکالیف و مأموریت‌ها، چگونگی اداره و رسمیت یافتن جلسات و مصوبات، تعامل کارگروه‌ها، گزارش به کمیسیون و سایر مراجع صلاحیت‌دار به تصویب می‌رسد.

بند دوم: وظایف و اختیارات کارگروه‌ها

ماده ۴۹. آیین‌نامه نحوه تشکیل و تعیین وظایف و اختیارات کارگروه‌های تخصصی ظرف سه‌ماه توسط کمیسیون تدوین و به تصویب هیئت‌وزیران خواهد رسید.

ماده ۵۰. ضوابط مقرر از سوی کارگروه‌های تخصصی در هریک از امور تنظیمی و نظارتی، پس از تأیید و تصویب کمیسیون لازم‌الاجراست.

بخش سوم: هیأت نظارت بر داده‌های شخصی

بند یکم: اعضای هیأت نظارت

ماده ۵۱. اعضای هیأت نظارت عبارت‌اند از:

۱. وزیر دادگستری به‌عنوان رئیس هیأت؛
۲. رئیس کمیسیون اصل نودم مجلس شورای اسلامی؛
۳. رئیس مرکز ملی فضای مجازی؛
۴. دبیر کمیسیون.

ماده ۵۲. هیأت نظارت در محل وزارت دادگستری تشکیل می‌شود. آیین‌نامه تشکیل و طرز کار هیأت و دبیرخانه آن به تصویب کمیسیون می‌رسد.

بند دوم: وظایف هیأت نظارت

ماده ۵۳. وظایف هیأت نظارت عبارت‌اند از:

الف) نظارت بر حسن اجرای امور نظارتی کارگروه‌های تخصصی؛

ب) دریافت و رسیدگی به شکایات ذی‌نفعان صیانت و حفاظت از داده‌های شخصی؛

پ) شناسایی و معرفی ناظران ویژه به کمیسیون و نظارت بر امور و فعالیت‌های آن‌ها بر پایه شیوه‌نامه مصوب کمیسیون؛

ت) نظارت بر تدوین شیوه‌نامه‌های اختصاصی استناد پذیری ادله ناظر به داده‌های شخصی از سوی کارگروه‌های تخصصی، تصویب در کمیسیون و ابلاغ پس از تأیید رئیس کمیسیون؛

ث) ایفای سایر امور محوله از سوی کمیسیون.

بند سوم: ناظر ویژه

ماده ۵۴. در موارد ذیل، ناظر ویژه تعیین می‌شود:

الف) پردازش داده‌های شخصی حیاتی و حساس؛

ب) پردازش کلان داده‌های شخصی؛

پ) زیان‌ها و آسیب‌های جدی یا پرشمار بالقوه و بالفعل پردازش‌ها به داده‌های شخصی؛

ت) سایر موارد به تشخیص هیأت نظارت و تأیید کمیسیون.

ماده ۵۵. شرایط احراز صلاحیت ناظر ویژه عبارت‌اند از:

الف) نداشتن سوءپیشینه کیفری و انتظامی؛

ب) داشتن حسن شهرت؛

پ) دارا بودن تجربه و تخصص لازم؛

ت) نداشتن تعارض منافع با موضوع نظارت.

ماده ۵۶. مدت فعالیت ناظر ویژه به دو شکل تعیین می‌شود:

الف) موردی متناسب با موضوع نظارت واگذارشده به وی؛

ب) دوره‌ای برای مدت سه سال و قابل تمدید برای دوره‌های مشابه.

ماده ۵۷. شرایط فعالیت ناظر ویژه عبارت‌اند از:

الف) تکالیف و مأموریت‌های وی به پیشنهاد هیأت نظارت به تصویب کمیسیون رسیده و به وی ابلاغ می‌شود.

ب) حیطه کار ناظر ویژه به‌طور معین و مشخص تعریف می‌شود و امور نظارتی مبهم و مجمل اعتبار ندارد.

پ) کنترل‌گران و پردازشگران موظف‌اند به هزینه خود نیازمندی‌های نظارتی متعارف ناظر ویژه را فراهم آورند.

ت) هیأت نظارت موظف است حمایت‌های قانونی و تسهیلات لازم را برای حسن ایفای تعهدات ناظر ویژه فراهم آورد.

ث) نظارت ویژه قائم به شخص است و حق واگذاری همه یا بخشی از آن به دیگری را ندارد.

ج) توقف یا تعلیق فعالیت، برکناری یا قبول استعفای وی تنها از سوی کمیسیون امکان‌پذیر است.

چ) در دوره تصدی نظارت ویژه، حق پذیرش نظارت‌های بیرون از چارچوب مقرر از سوی کمیسیون، اعم از انتفاعی یا غیرانتفاعی را ندارد.

بخش چهارم: بودجه تنظیم و نظارت بر داده‌های شخصی

ماده ۵۸. بودجه موردنیاز این قانون به نحو متمرکز در ذیل ردیف بودجه دبیرخانه کمیسیون و مستقل در قوانین بودجه سنواتی پیش‌بینی می‌شود.

باب پنجم: مسؤولیت‌ها و ضمانت اجراها

بخش یکم: دامنه مسؤولیت کنترل‌گران و پردازشگران

ماده ۵۹. کنترل‌گر و پردازشگر در برابر تعهدات خود مسؤولیت مستقل دارند.

ماده ۶۰. پردازشگر در صورتی معاف از مسؤولیت است که:

الف) اقدام وی با دستور یا درخواست کنترل‌گر مغایرت نداشته باشد؛

ب) در صورت غیرقانونی دانستن دستور یا درخواست موردنظر، آگاهی لازم را به کنترل‌گر داده باشد.

بخش دوم: مسؤولیت‌های مدنی

ماده ۶۱. کنترل‌گر موظف است حسب درخواست زیان‌دیده تمامی ضرر و زیان وارده به شخص موضوع داده را جبران کند. در صورت عدم جبران ضرر و زیان، موضوع حسب شکایت زیان‌دیده از طریق مراجع قضائی پیگیری خواهد شد.

بند یکم: جبران‌های مادی

ماده ۶۲. درجایی که شخص حقیقی وابسته به شخص حقوقی به دیگری زیان می‌رساند، مسؤولیت جبران با شخص حقوقی خواهد بود. مگر اینکه بتواند ثابت کند شخص حقیقی فراتر از اختیارات خود عمل نموده و شخص حقوقی نیز در نظارت بر حسن ایفای تعهدات وی مرتکب قصور نشده است.

ماده ۶۳. چنانچه شخص موضوع داده حقوق خود را به‌طور ناروا استیفا و به دیگری زیانی وارد کند، مسئول جبران آن خواهد بود.

ماده ۶۴. مرجع صلاحیت‌دار قضایی یا انتظامی می‌تواند متناسب با نوع و گستره آسیب حیثیتی وارده، میزان جبران‌پذیری و زیان‌های مادی ناشی از آن، مرتکب را به پرداخت جریمه تنبیهی یا محدودیت‌های اجتماعی در حق آسیب‌دیده محکوم نماید. شیوه‌نامه تعیین و تقویم زیان‌های مادی ناشی از پردازش غیرمجاز داده‌های شخصی و نحوه اعاده حیثیت ناشی از ورود آسیب‌های معنوی و جریمه به پیشنهاد کارگروه‌های تخصصی به تصویب کمیسیون می‌رسد.

بخش سوم: مسؤولیت‌های کیفری

بند یکم: جرائم و مجازات

ماده ۶۵. مجازات مقرر در این قانون در صورتی اعمال می‌شود که در قوانین دیگر مجازات شدیدتری برای جرم موردنظر پیش‌بینی‌نشده باشد.

ماده ۶۶. هرگونه استناد به داده‌ها و نتایج حاصل از نقض مقررات این قانون ممنوع و مرتکب به مجازات درجه ۵ محکوم می‌شود.

ماده ۶۷. هریک از کارکردهای پردازش که برای آن‌ها جرم و مجازات مستقلی در دیگر قوانین تعریف شده است، به همان ترتیب و بر پایه ضوابط مربوط به تعدد جرائم لحاظ خواهند شد.

ماده ۶۸. مرتکبان ذیل به مجازات مقرر محکوم می‌شوند:

الف) نقض حق رضایت شخص موضوع داده، چنانچه داده‌های وضعیت‌ها و موقعیت‌های غیرعمومی پردازش شود، به مجازات درجه ۵ و چنانچه داده‌های وضعیت‌ها و موقعیت‌های عمومی پردازش شود، به مجازات درجه ۶؛

ب) ممانعت از استیفای همه یا بخشی از حق درخواست شخص موضوع داده درباره پردازش یا توقف آن یا انجام پردازش داده‌های شخصی به‌وسیله خود وی یا نقض حق گمنامی، به یک یا هر دو مجازات درجه ۶؛

پ) نقض تعهدات اعتبار پذیری، اعتمادپذیری یا استناد پذیری پردازش داده‌های شخصی، به یک یا هر دو مجازات درجه ۵؛

ت) استیفای ناروای حقوق مندرج در این قانون از سوی شخص موضوع داده، با توجه به‌شدت جرم و زیان‌ها و آسیب‌های وارده به یک یا هر دو مجازات درجه ۶؛

ث) کنترل غیرمجاز پردازش از سوی مقام صلاحیت‌دار دستگاه اجرایی، علاوه بر مجازات مقرر برای جرم موردنظر به انفصال‌ازخدمت از شش ماه تا سه سال؛

ج) امتناع از اجرا یا اجرای نادرست یا اقدام به‌نحوی‌که اجرای همه یا بخشی از ضوابط این قانون یا دستور کمیسیون یا هیأت نظارت یا ناظر ویژه منتفی گردد، مانند عدم نگهداری همه یا بخشی از داده‌ها، حسب مورد یک یا هر دو مجازات درجه ۵.

تبصره ۱. دادگاه می‌تواند مرتکب را به گذراندن دوره‌های ویژه صیانت و حفاظت از داده‌های شخصی و دریافت گواهی‌های مربوط، پیرو شیوه‌نامه مصوب کمیسیون ملزم نماید.

تبصره ۲. چنانچه اشخاص حقوقی موضوع ماده (۷۴۷) قانون مجازات اسلامی مرتکب جرائم مقرر در مواد (۶۹)، (۷۰) و (۷۱) شوند، مطابق ماده (۷۴۸) آن قانون مجازات خواهند شد.

بند دوم: تشدید مجازات

ماده ۶۹. در صورت وجود یک یا چند شرط ذیل، مجازات مرتکب یک یا دو درجه بالاتر تعیین می‌شود:

الف) به‌واسطه شغل یا حرفه خود مرتکب جرم شده باشد؛

ب) نسبت به گستره و دامنه فعالیت خود، شمار قابل‌توجهی از اشخاص را هدف قرار داده باشد؛

پ) زیان مادی یا آسیب معنوی قابل‌توجه یا جبران‌ناپذیری را وارد آورده باشد؛

ت) داده‌های شخصی حیاتی یا حساس، ابزار یا نتیجه جرم باشند؛ و

ث) به شکل گروهی یا سازمان‌یافته مرتکب شده باشد.

ماده ۷۰. چنانچه عواید مالی حاصل از ارتکاب جرائم این قانون بیشتر از جزای نقدی مقرر برای آن‌ها باشد، همان مبنا قرار می‌گیرد. در صورت اعمال حبس به‌جای جزای نقدی، تفاضل عواید مالی مذکور در این ماده نیز باید به‌عنوان جزای نقدی اعمال گردد.

بخش چهارم: مسؤولیت‌های انتظامی

بند یکم: تخلفات انتظامی

ماده ۷۱. تخلفات انتظامی پیشنهادی از سوی کارگروه‌های تخصصی جهت تصویب در کمیسیون، موارد ذیل را در برمی‌گیرد:

الف) همه جرائم مقرر در این قانون؛

ب) نقض تعهدات کنترل‌گران و پردازشگران، اعم از اعتبار پذیری، اعتمادپذیری، استنادپذیری و پردازش‌های فرامرزی؛

پ) نقض تعهدات اشخاص موضوع داده در برابر سایر ذی‌نفعان؛

ت) نقض تعهدات قراردادی یا سایر اسناد تعهدآور.

بند دوم: ضمانت اجراهای انتظامی

ماده ۷۲. ضمانت اجراهای انتظامی قابل تصویب در کمیسیون و به پیشنهاد کارگروه‌های تخصصی برای تخلفات بر پایه معیارهای بازدارندگی، تناسب و اثربخشی می‌تواند یک یا چند گزینه زیر باشد:

الف) جریمه نقدی؛

ب) منع فعالیت یا بهره‌برداری یا انفصال از خدمت در یک یا چند رده حرفه‌ای یا تخصصی برای مدت معین؛

پ) منع فعالیت یا بهره‌برداری یا انفصال از خدمت در همه یا برخی نهادها یا اشخاص موضوع این قانون برای مدت معین؛

ج) کاهش مدت اعتبار پروانه یا گواهی یا قرارداد فعالیت یا بهره‌برداری یا سنوات خدمت یا تعلیق آن برای مدت معین؛

چ) منع تمدید اعتبار پروانه یا گواهی یا قرارداد فعالیت یا بهره‌برداری یا دریافت پروانه یا گواهی فعالیت یا بهره‌برداری یا احراز سمت دیگر برای مدت معین؛

ح) لغو اعتبار پروانه یا گواهی یا قرارداد فعالیت یا بهره‌برداری یا انفصال از خدمت برای مدت معین.

تبصره ۱. کارگروه‌های تخصصی موظف‌اند ضمانت اجراهای انتظامی خود را بر پایه ضوابط قانون مجازات اسلامی طبقه‌بندی نمایند.

تبصره ۲. احراز شرایط تخلف و مسائل مربوط به معاونت، مشارکت، تعدد و تکرار، مسؤولیت اشخاص حقوقی متخلف و مانند آن و همچنین عوامل رافع، مانع، مخففه و مشدده مسؤولیت، بر پایه قانون مجازات اسلامی خواهد بود.

بخش پنجم: ضمانت اجراهای قراردادی

ماده ۷۳. هرگونه توافق مغایر با احکام و ضوابط الزامی این قانون فاقد اعتبار است و موجب بطلان آن می‌شود.

ماده ۷۴. طرفین توافق‌های موضوع این قانون موظف‌اند ارتکاب تخلفات و جرائم آن را نقض توافق بدانند و ضمانت اجراهای قراردادی متناسب، اثربخش و بازدارنده پیش‌بینی نمایند.

بخش ششم: پیشگیری از تخلفات و جرائم

ماده ۷۵. مسؤولیت تدوین برنامه‌های پیشگیرانه از تخلفات و جرائم این قانون به عهده کارگروه‌های تخصصی است که به تأیید کمیسیون می‌رسد.

بخش هفتم: آمار و اطلاعات

ماده ۷۶. هریک از کارگروه‌های تخصصی موظف به فراهم‌سازی و روزآمد نگاه‌داشتن آمار و اطلاعات راجع به مسؤولیت‌های مدنی، کیفری، انتظامی و قراردادی بخش خود بر پایه شیوه‌نامه مصوب کمیسیون هستند.

باب ششم: نسخ قوانین و تدوین مقررات لازم

ماده ۷۷. از تاریخ تصویب این قانون کلیه قوانین و مقررات مغایر با آن نسخ می‌گردد و مادام که در قوانین بعدی نسخ و یا اصلاح مواد و مقررات این قانون صریحاً و با ذکر نام این قانون و ماده موردنظر قید نشود، معتبر خواهد بود.

ماده۷۸ . آیین‌نامه اجرایی این قانون ظرف ۳ ماه پس از تشکیل کمیسیون توسط اعضاء تهیه و به تصویب هیأت وزیران خواهد رسید.