

باسمه تعالی

لایحه حمایت از داده و حریم خصوصی در فضای مجازی

باب اول: تعاریف

ماده ۱: در این قانون اصطلاحات زیر در معانی ذیل به کار می‌روند:

- ۱- داده شخصی عبارت است از داده‌ای که به وسیله آن، به تنهایی یا به همراه داده‌های دیگر، بتوان شخص موضوع آن را شناسایی کرد.
- ۲- پردازش عبارت است از هر نوع جمع آوری، دریافت، ارسال، نگهداری، تبادل، به اشتراک گذاشتن یا هر نوع عملیات دیگر اعم از الکترونیک یا غیر الکترونیک که بر داده انجام شود و بتوان آن داده را به شخص موضوع آن مرتبط کرد.
- ۳- ایجاد داده: عبارت است از ثبت اطلاعات برای اولین بار.
- ۴- جمع آوری داده: عبارت است از گرد آوری داده‌هایی که قبلاً ایجاد شده‌اند.
- ۵- کنترل‌گر عبارت است از هر شخص حقیقی یا حقوقی که بر اساس قرار داد یا قانون یا در عمل هدف و چگونگی ثبت و پردازش داده را تعیین می‌کند.
- ۶- استفاده از داده عبارت است از به کار بردن آن در جهت کسب در آمد یا تحصیل هر نوع منفعت مادی و معنوی دیگر.
- ۷- فضای عمومی مجازی عبارت است از فضایی است که اشخاص داده‌ها را برای دسترسی عمومی در آن قرار می‌دهند.

باب دوم: مقررات عمومی

ماده ۲: به منظور محافظت از حریم داده‌های شخصی و حمایت از حیثیت و کرامت هر فرد، هر کس می‌تواند به داده‌های شخصی خود دسترسی داشته باشد و بر هر نوع پردازش این داده‌ها مطابق مقررات این قانون نظارت نماید.

ماده ۳:

۱- ایجاد، پردازش و استفاده از داده‌های شخصی باید مبتنی بر رضایت صریح یا ضمنی اشخاص موضوع آن باشد مگر به حکم قانون. اعلام رضایت حاصل از فریب یا تهدید یا اکراه معتبر نیست. کنترل‌گر باید پیش از ایجاد، پردازش یا استفاده از این داده‌ها، هدف معین و قانونی خود از این امور و همچنین حسب مورد عواقب عدم ارائه این داده‌ها را به نحو صریح اعلام کند.

۲- در صورت محجور بودن شخص موضوع داده اجازه ولی یا قیم قانونی او ضروری است.

۳- در موارد اختلاف، اثبات اعلام رضایت شخص موضوع داده بر عهده کنترل‌گر خواهد بود.

۴- در جهت حمایت و محافظت متناسب با موضوع برخی از انواع داده‌های شخصی به لحاظ اهمیت آنها یا نقش آن نوع داده‌ها در شرایط خاص سیاسی یا اجتماعی، کمیسیون مرکزی حمایت از داده‌ها می‌تواند اعلام رضایت شخص موضوع داده را از طریق الکترونیک معتبر نداند.

۵- پردازش داده‌های حاصل از راه فریب یا تهدید یا اکراه شخص موضوع آن ممنوع است.

۶- ارائه داده‌های شخصی توسط شخص موضوع داده در فضای عمومی مجازی به منزله رضایت به جمع‌آوری یا پردازش آنهاست.

۷- در هر صورت فردی که داده‌های شخصی او پردازش یا استفاده می‌شود نباید از این اقدام متضرر شود و در صورت ورود خسارت متعارف مادی یا معنوی، کنترل‌گر مکلف به جبران متناسب با آن ضرر است مگر اینکه شخص موضوع داده رضایت صریح یا ضمنی خود را به ورود خسارت احتمالی اعلام کرده باشد. اگر ورود خسارت مستند به فعل شخصی غیر از کنترل‌گر باشد در صورتی که کنترل‌گر اقدامات متناسب برای محافظت از داده‌ها را انجام داده باشد شخص ثالث مکلف به جبران خسارت است و در غیر این صورت، کنترل‌گر جبران خسارت می‌نماید و می‌تواند خسارتی را که پرداخت نموده است از او مطالبه کند.

ماده ۴: کمیسیون مرکزی حمایت از داده‌ها نظارت بر اجرای مقررات حمایت از داده‌های شخصی افراد را بر عهده دارد. تصمیمات این کمیسیون قابل شکایت در دیوان عدالت اداری است.

ماده ۵: پردازش داده‌های شخصی اشخاص حقوقی نباید موجب نقض حقوق و آزادی‌های مشروع، افشای داده‌های شخصی یا سلب امنیت اشخاص حقیقی شود.

ماده ۶: حق مالکیت فکری بر داده‌های شخصی نافی حقوق اشخاص موضوع داده‌ها نیست. در صورت تزامم حقوق، حق اشخاص بر داده‌های شخصی آنها اولویت خواهد داشت.

باب دوم: پردازش مجاز داده‌های شخصی

بند اول: مقررات عمومی

ماده ۷: پردازش داده‌های شخصی در صورتی مجاز است که :

- ۱- مطابق ماده ۲ این قانون ایجاد یا پردازش شده باشند. و
 - ۲- مطابق با اهداف اعلام شده توسط کنترل‌گر، ایجاد یا جمع‌آوری شده یا مطابق با آن اهداف از پردازش ناشی شده باشد مگر اینکه قانونگذار پردازش یا استفاده از آن‌ها را برای هدف خاص دیگری تجویز کند.
- تبصره: به جز داده‌های شخصی حساس، پردازش داده‌های شخصی جهت انجام بررسی‌های آماری یا پژوهش‌های علمی یا تاریخی، مجاز است.

ماده ۸: مسئولیت صحت و تمامیت و به روز بودن داده‌های شخصی بر عهده ثبت‌کننده این داده‌ها است مگر اینکه قانون این مسئولیت را بر عهده شخص دیگری قرارداده باشد.

ماده ۹: کنترل‌گر مکلف است اقدامات لازم جهت حذف یا اصلاح داده‌هایی که با توجه به هدف از بدست آوردن یا پردازش آنها نادرست یا ناکافی هستند را انجام دهد.

ماده ۱۰: داده‌های شخصی باید به گونه‌ای پردازش و استفاده شوند که شخص موضوع داده قابل شناسایی نباشد مگر اینکه شناسایی شخص موضوع داده برای اجرای قانون یا دستیابی به اهداف اعلام شده در ماده ۳ ضروری باشد.

ماده ۱۱: کنترل‌گر نباید داده‌هایی بیش از آنچه برای اجرای قانون یا دستیابی به اهداف اعلام شده موضوع ماده ۳ لازم است ثبت کند.

ماده ۱۲: پردازش داده‌های شخصی بدون تحصیل رضایت موضوع آن داده در صورتی جایز است که:

- برای انجام تکالیفی که قانونگذار بر عهده کنترل‌گر قرار داده است ضروری باشد؛ یا
- برای حفظ حیثیت یا جان شخص موضوع داده ضروری باشد. یا
- برای حفظ منافع مسلم شخص موضوع داده ضروری و با آن منافع متناسب باشد و اخذ رضایت او ممکن نباشد.
- برای حفظ امنیت عمومی، حفظ امنیت ملی، منافع ملی، تعقیب جرم یا حفظ سلامت و ایمنی عمومی ضروری باشد.

ماده ۱۳: استفاده تجاری از داده شخصی به شرط آنکه هویت اشخاص موضوع داده شناسایی نشود مجاز است.

ماده ۱۴: دادگاه صرفاً می‌تواند به داده‌های شخصی که با رعایت مقررات این قانون یا قوانین مرتبط دیگر بدست آمده باشند استناد کند. با این حال بررسی صحت و سقم محتوای داده بر عهده دادگاه است.

بند دوم: ایجاد، پردازش و استفاده از داده‌های شخصی حساس

ماده ۱۵:

۱- ایجاد، پردازش یا استفاده از داده‌های شخصی حساس یا اجبار اشخاص به ارائه این نوع داده‌ها ممنوع است.

- ۲- داده‌های مرتبط با عقاید سیاسی، حزبی، فلسفی، دینی یا مذهبی، قومیت، وضعیت جسمانی، رفتارهای جنسی، اتهامات و محکومیت‌های کیفری داده شخصی حساس محسوب می‌شود.
- ۳- در موارد ذیل ایجاد، پردازش یا استفاده از داده‌های شخصی حساس ممنوع نیست:
- ۳-۱- شخص موضوع داده رضایت صریح خود را به این امور بیان کرده باشد.
- ۳-۲- برای حفظ زندگی شخص موضوع داده ضروری باشد و به دلیل عدم اهلیت رضایت او فاقد اثر قانونی باشد یا تحصیل رضایت از او به دلیل دیگری عملاً ممکن نباشد.
- ۳-۳- شخص موضوع داده آن داده را به طور عمومی منتشر نموده باشد.
- ۳-۴- برای کشف جرم یا اجرای مجازات ضروری باشد.
- ۳-۵- برای حفظ نظم عمومی یا امنیت ملی ضروری باشد.
- ۳-۶- قانون ایجاد یا پردازش یا استفاده از این نوع داده را بدون رضایت شخص موضوع داده مجاز نموده باشد.
- ماده ۱۶:** داده‌هایی که برای سرشماری عمومی نفوس و مسکن توسط مرکز آمار ایران جمع‌آوری می‌شوند از ممنوعیت بند ۱ ماده ۱۶ مستثنی هستند. با این حال این داده‌ها باید به گونه‌ای ذخیره و نگهداری شوند که نتوان داده‌های شخصی را به موضوع آنها مرتبط کرد.
- ماده ۱۷:** ایجاد یا پردازش داده‌های شخصی حساس برای حفظ سلامت عمومی جامعه یا جلوگیری از سرایت و انتشار فراگیر بیماری منحصراً توسط وزارت بهداشت، درمان و آموزش پزشکی مجاز است.
- ماده ۱۸:** ایجاد یا پردازش داده‌های شخصی حساس برای انجام پژوهش‌های پزشکی، پیرا پزشکی و روانشناسی توسط دانشگاه‌ها و مراکز تحقیقاتی و موسسات پژوهشی و پژوهشکده‌ها و پژوهشگاه‌های کشور مجاز است. ارائه این داده‌ها به نهاد‌های علمی بین‌المللی تنها با تصویب هیئت وزیران مجاز است.
- ماده ۱۹:** در صورتی که شخص موضوع داده از دیگری به دلیل ایجاد، پردازش یا استفاده از داده‌های شخصی حساس مرتبط با خود به دادگاه شکایت نماید و او نتواند اثبات کند که اقدام او منطبق بر استثنائات بند ۳ ماده

۱۶ یا مواد مرتبط دیگر بوده است، بر اساس اینکه اقدام او منجر به افشای محدود یا انتشار عمومی آن داده ها شده باشد، به مجازات مقرر در این قانون محکوم خواهد شد.

باب سوم: تکالیف کنترل‌گر

ماده ۲۰:

- ۱- در صورت درخواست شخص موضوع داد، کنترل‌گر مکلف است موارد زیر را در اختیار او قرار دهد:
 - الف- نسخه ای از داده های شخصی ثبت شده از او یا داده های پردازش شده مرتبط با آن داده ها که در اختیار کنترل‌گر است؛ و
 - ب- شخص یا اشخاص حقیقی یا حقوقی که داده های شخصی او به آنها منتقل شده است یا در دسترس آنها قرار گرفته است؛ و
 - ج- اطلاعات مرتبط با داده‌های جمع آوری شده از او مانند منبع اطلاعات؛
 - د- هدف از جمع آوری داده؛
- ۲- کنترل‌گر از اجرای تکلیف بند ۱ معاف است اگر:
 - الف- کنترل‌گر در جهت اجرای تکالیف مرتبط با کشف جرم، داده را ایجاد یا جمع آوری کرده باشد و اجرای تکلیف بند ۱ مانعی در روند رسیدگی ایجاد کند.
 - ب- ارائه موارد مذکور در بند ۱ :
 - خطر جانی با حیثیتی برای دیگری داشته باشد.
 - امنیت یا منافع ملی یا آسایش عمومی را به خطر اندازد.
 - منجر به افشای هویت مأمورین امنیتی، نظامی یا انتظامی گردد.
 - ج- موارد مذکور در بند ۱ موضوع اسناد طبقه بندی شده باشد.
 - د- سایر قوانین ارائه موارد مذکور در بند ۱ را ممنوع کرده باشد.

۳- در مواردی که کنترل‌گر از اجرای تکلیف بند ۱ خودداری می‌کند، مراتب را به صورت کتبی همراه با دلیل خودداری از انجام این تکلیف به متقاضی اعلام می‌نماید. در صورت اعتراض شخص موضوع داده، کمیسیون استانی حمایت از داده‌ها و آزادی اطلاعات تصمیم‌گیری خواهد نمود.

ماده ۲۱: کنترل‌گر باید داده‌های شخصی را پس از ثبت، پردازش یا استفاده حداقل به مدت یک‌سال نگهداری نماید مگر اینکه کمیسیون مرکزی حمایت از داده‌ها و آزادی اطلاعات زمان دیگری را مقرر نماید.

ماده ۲۲:

- ۱- شخص موضوع داده می‌تواند از کنترل‌گر موارد ذیل را مطالبه نماید:
- حذف داده‌ای که مغایر با قانون از او ثبت یا پردازش شده است؛
 - عدم پردازش داده‌ای که پردازش آن مغایر قانون است؛
 - اصلاح یا تکمیل داده‌ای که از او ثبت یا به هر شکلی پردازش شده است؛
- ۲- در صورت استنکاف کنترل‌گر، تصمیم کمیسیون استانی حمایت از داده‌ها و آزادی اطلاعات ملاک خواهد بود.

ماده ۲۳: در صورتی که در ارائه داده‌های شخصی، قراردادی بین کنترل‌گر و شخص موضوع داده وجود داشته باشد، در اجرای این قرارداد مواد ۱۵، ۱۶، ۱۷ این قانون لحاظ خواهد شد.

ماده ۲۴: استفاده از داده‌های شخصی در جهت تبلیغ کالا یا خدمات تنها در صورتی مجاز است که:

- شخص موضوع داده در هنگام ارائه داده به کنترل‌گر رضایت صریح خود را به این نوع استفاده اعلام نموده باشد؛ یا
- برای تضمین منافع کنترل‌گری که نهاد خصوصی است ضروری باشد به شرط آنکه در تضاد با منافع یا حقوق یا آزادی‌های موضوع داده نباشد و شخص موضوع داده نیز از انجام این پردازش نهي نکرده باشد. در هر صورت اصل بر این است که این پردازش در تضاد با منافع یا حقوق یا آزادی‌های موضوع داده است مگر خلاف آن احراز شود.

باب چهارم: نهاد نظارت کننده بر اجرای صحیح مقررات این قانون

ماده ۲۵: به منظور رسیدگی به شکایات راجع به تخلف از مقررات این قانون، کمیسیون‌های استانی حمایت از داده‌ها در محل استانداری با ترکیب زیر تشکیل می‌شود:

الف) یک قاضی به انتخاب رئیس قوه قضائیه به عنوان رئیس کمیسیون؛

ب) یک خبره به انتخاب رئیس جمهور؛

پ) یک وکیل به انتخاب هیأت مدیره کانون وکلای منطقه‌ای؛

ت) یک خبره به انتخاب شورای عالی استان‌ها؛ و

ث) مدیر اداره کل مدیریت و برنامه‌ریزی استان یا معاون ذی‌ربط وی.

تبصره ۱- دبیرخانه کمیسیون استانی در محل استانداری تشکیل می‌شود.

تبصره ۲: جلسات کمیسیون با حضور رئیس و دو نفر از اعضاء رسمیت می‌یابد و تصمیمات آن با رأی اکثریت و موافقت قاضی معتبر خواهد بود.

ماده ۲۶: تصمیمات کمیسیون‌های استانی ظرف ۲۰ روز از تاریخ ابلاغ، نزد کمیسیون مرکزی حمایت از داده‌ها قابل اعتراض خواهد بود.

ماده ۲۷: به منظور نظارت بر حسن اجرای این قانون، تجدیدنظر از آرای کمیسیون‌های استانی، ایجاد وحدت رویه و ارائه نظرهای مشورتی، کمیسیون مرکزی حمایت از داده‌ها با ترکیب زیر تشکیل می‌شود:

الف) یک خبره به انتخاب رئیس جمهور؛

ب) یکی از قضات دیوان عالی کشور به انتخاب هیأت عمومی دیوان؛

پ) یکی از قضات دیوان عدالت اداری به انتخاب هیأت عمومی دیوان؛

ث) دو نماینده مجلس شورای اسلامی به انتخاب مجلس؛

ج) یکی از حقوقدانان برجسته عضو هیأت علمی به انتخاب وزیر دادگستری؛

چ) نماینده وزیر ارتباطات و فناوری اطلاعات؛

ح) نماینده وزیر فرهنگ و ارشاد اسلامی؛

خ) نماینده دبیر شورای عالی فضای مجازی؛

د) یکی از وکلای دادگستری به انتخاب هیأت مدیره اتحادیه سراسری کانون وکلای کشور.

ذ) یکی از مدیران مسئول مطبوعات به انتخاب آنها

تبصره ۱: جلسات کمیسیون با حضور ۹ نفر از اعضاء رسمیت می یابد و تصمیمات آن با اکثریت مطلق حاضران، معتبر خواهد بود. رأی کمیسیون قطعی است.

تبصره ۲: دبیرخانه کمیسیون در محل مرکز ملی فضای مجازی تشکیل می شود.

ماده ۲۸: اعضای کمیسیون برای مدت چهار سال انتخاب می شوند. دوره تصدی کسانی که به دلایلی جانشین اعضای شورا می شوند، به میزان بقیه دوره تصدی عضو قبلی خواهد بود.

تبصره: نحوه تشکیل و اداره جلسات و وظایف دبیرخانه های کمیسیون های حمایت از داده ها به موجب شیوه نامه ای خواهد بود که توسط کمیسیون مرکزی تصویب خواهد شد.

باب پنجم: ضمانت اجرا

ماده ۲۹: هر کس به طور غیرمجاز داده های شخصی دیگران را ایجاد، جمع آوری، پردازش یا استفاده کند، به جزای نقدی درجه ۶ محکوم خواهد شد. در صورتی که مرتکب، این اقدامات را به قصد انتفاع مالی خود یا دیگری انجام داده باشد، یا از این طریق موجب وارد شدن ضرر مالی یا حیثیتی به دیگری شده باشد، به مجازات حبس و جزای نقدی درجه ۶ محکوم خواهد شد.

تبصره ۱: هرگاه داده های شخص، حساس باشند یا داده های شخصی به طور غیرمجاز در اختیار دیگران قرار داده شده یا منتشر شده باشند، حسب مورد، مرتکب به حداکثر مجازات مقرر محکوم خواهد شد.

تبصره ۲: در مواردی که ایراد ضرر مالی یا حیثیتی ناشی از تقصیر مرتکب باشد، چنانچه داده های شخصی، حساس نباشند مرتکب به حداقل مجازات مقرر و چنانچه داده های شخصی، حساس باشند، به حداکثر مجازات محکوم خواهد شد.

تبصره ۳: در جرایم فوق چنانچه شخص حقوقی مطابق ماده ۱۴۳ قانون مجازات اسلامی مسئول شناخته شود، به جزای نقدی درجه ۲ تا ۶ و یک یا چند ممنوعیت از ممنوعیت‌های درجه ۶ محکوم خواهد شد.