مرکز پژوهش‌های مجلس شورای اسلامی
دفتر مطالعات انرژی، صنعت و معدن
مسلسل: ۱۹۹۳۶ ■ مرداد ۱۴۰۳

شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا (۳): قوانین مصوب و طرح‌های اعلام وصول شده در کنگره


بسم الله الرحمن الرحيم

تاریخ انتشار:
۱۴۰۳/۵/۱۳

شماره مسلسل: ۱۹۹۳۶
کد موضوعی: ۳۱۰

مرکز پژوهش‌های مجلس شورای اسلامی

عنوان گزارش:
شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا (۳): قوانین مصوب و طرح‌های اعلام وصول شده در کنگره

نوع گزارش: طرح/ لایحه ☐، نظارتی ☐، راهبردی ■

نام دفتر:
مطالعات انرژی، صنعت و معدن (گروه فناوری اطلاعات و ارتباطات)

مدیر مطالعه:
محمدامین احمدلو

تهیه و تدوین:
ابوالقاسم رجبی

ناظران علمی:
حبیب‌اله ظفریان، سعید شجاعی

اظهارنظرکنندگان:
امین پژمان (مطالعات حقوقی)، سهیلا خردمندنیا (گروه فناوری نوین)، حسن پوراسماعیل (گروه فناوری اطلاعات و ارتباطات)، سیدعلی محسنیان، مرتضی قاسم‌زاده عراقی (مطالعات فرهنگی)، یحیی مرتب (مطالعات مدیریت)

گرافیک و صفحه آرایی:
نفیسه حاجی‌صفری

ویراستار ادبی:
سیده مرضیه موسوی راد

تاریخ شروع:
۱۴۰۱/۳/۱

واژه‌های کلیدی:
۱. حفاظت از داده‌ها
۲. مطالعات تطبیقی
۳. قوانین ایالت متحده آمریکا
۴. صیانت از داده‌ها

دفتر مطالعات انرژی، صنعت و معدن

فهرست مطالب

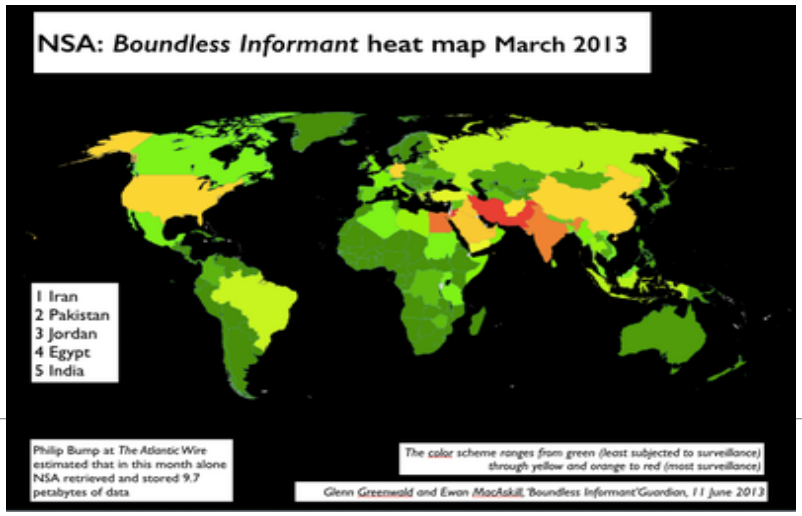
چکیده ۶
خلاصه مدیریتی ۷
۱. مقدمه ۸
۲. ساختار کنگره ایالات متحده آمریکا و شیوه گردآوری مصوبات فناوری اطلاعات آن ۱۰
۳. قوانین حفاظت از داده‌های در اختیار بخش عمومی آمریکا و مقایسه آن با ایران ۱۱
۴. قوانین حفاظت از داده‌های در اختیار بخش غیردولتی آمریکا و مقایسه آن با ایران ۱۷
۵. پیش‌نویس طرح‌ها و لوایح حفاظت از داده عرضه شده به کنگره در سال‌های اخیر ۱۹
۶. جمع‌بندی ۲۲
پیوست ۱. تاریخچه اصلاح قوانین نامه امنیت ملی ۲۴
پیوست ۲. متن یک قانون برنامه توسعه‌ای آمریکا در زمینه حفاظت از داده‌ها ۲۶
منابع و مآخذ ۲۸

فهرست شکل

شکل ۱. طبقه‌بندی قوانین ایالات متحده آمریکا ۹

فهرست جدول

جدول ۱. مقایسه قوانین نامه امنیت ملی ایالات متحده آمریکا با یکدیگر ۱۴



شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا (۳):

قوانین مصوب و طرح‌های اعلام وصول شده در کنگره

چکیده

اعتماد به خدمات فناوری اطلاعات و ارتباطات یا فاوای داخلی، محرک اصلی رشد دیجیتالی شدن خدمات و توسعه صنایع فاوا در کشور است. حفاظت از داده‌ها، پیرامون ضوابطی است که موجب افزایش اعتماد مردم به استفاده و نگهداری منصفانه و مسئولانه از داده‌هایشان می‌شود. نتایج بررسی قوانین حفاظت از داده‌های ایالات متحده آمریکا نشان می‌دهد که این قوانین به دو دسته کلی؛ قوانین مرتبط با بخش دولتی و بخش خصوصی قابل تقسیم هستند. مطالعه قوانین ایالات متحده آمریکا در زمینه حفاظت از داده در بخش دولتی نشان می‌دهد، انطباق دستگاه‌های دولتی با موازین حفاظت از داده‌ها تنها به تصویب قوانین موضوعه یا دائمی محدود نشده، بلکه به‌صورت مستمر در قوانین برنامه توسعه‌ای و قوانین بودجه سنواتی نیز اقداماتی برای تدوین چارچوب‌ها و انطباق دستگاه‌های اجرایی با موازین حریم خصوصی و حفاظت از داده‌ها در دستور کار قرار گرفته است. از سوی دیگر سخت‌گیری بیش از حد در گردآوری و کسب اطلاعات توسط بخش دولتی در برخی موارد موجب وابستگی غیرقابل بازگشت بخش دولتی به شرکت‌های خصوصی شده که عملاً تصمیم‌گیری در جهت منافع ملی را با مشکل مواجه کرده است.

از طرف دیگر، در تصویب قوانین عمومی حفاظت از داده‌ها در بخش خصوصی از اقشار آسیب‌پذیر مانند کودکان و افراد شاغل در مشاغل خاص مانند خبرنگاران نسبت به عموم جامعه حفاظت بیشتری شده است. همچنین در قوانین حفاظت از داده‌ها در بخش‌هایی از قبیل سلامت و امور مالی که با حساسیت بیشتری از این حیث مواجه هستند ضوابط عمیق‌تری لحاظ شده است.

خلاصه مدیریتی

بیان / شرح مسئله

به‌عنوان یک مفهوم حقوقی حفاظت از داده‌ها، دو حوزه حریم خصوصی داده (چگونگی کنترل، گردآوری، استفاده و توزیع اطلاعات شخصی) و امنیت داده (چگونگی حفاظت از داده‌های شخصی در مقابل دسترسی و استفاده غیرمجاز و پاسخ به دسترسی یا استفاده غیرمجاز) را با یکدیگر ترکیب می‌کند. ضوابط حفاظت از داده‌ها باید تعادلی بین سهولت توسعه سیستم‌های فناوری اطلاعاتی و اطمینان از رعایت مسئولیت کسب‌وکار و بخش دولتی نسبت به داده‌های شهروندان به‌وجود بیاورد. حساسیت بیشتر بعضی از داده‌ها مانند داده‌های سلامت یا امور مالی نیازمند سطوح بالاتری از ضوابط حفاظت از داده‌هاست. با وجود این، در حال حاضر بخش حمایت از داده‌های شخصی در قانون تجارت الکترونیکی ایران نمی‌تواند پاسخ‌گوی تمام نیازهای حفاظت از داده باشد. ازاین‌رو لایحه حفاظت از داده‌ها در انتظار اعلام وصول و بررسی در مجلس شورای اسلامی است. استفاده از تجارب بین‌المللی می‌تواند به کشـــور در قانونگذاری دقیق‌تر کمک کند. بنابراین تجربه ایالات متحده آمریکا به‌عنوان کشوری که قانونگذاری حفاظت داده‌ها را از حدود نیم قرن پیش آغاز و با تبعات مثبت و منفی آن مواجه شده است می‌تواند مفید باشد.

نقطه‌نظرات / یافته‌های کلیدی

طبق مطالعات ایالات متحده آمریکا به‌نظر می‌رسد برای قانونگذاری در زمینه حفاظت از داده‌ها این نکات قابل توجه هستند:

۱. حفاظت از داده‌ها شامل بخش دولتی و خصوصی می‌شود. طرح‌ها و لوایح، حقوق اشخاص موضوع داده‌ها در پایگاه‌های اطلاعاتی مختلف دولتی و خصوصی را شفاف‌سازی می‌کنند.

۲. ضوابط حفاظت از داده‌های حساس از قبیل اطلاعات مالی و سلامتی بسته به سطح حساسیت بالاتر از ضوابط عمومی حفاظت از داده‌ها تعیین شده‌است.

۳. اشخاص موضوع داده مختلف از حفاظت‌های قانونی متفاوتی برخوردار هستند. از یک‌سو کودکان و اقشار آسیب‌پذیر و مشاغلی مانند خبرنگاران فعال در زمینه افشاگری و مبارزه با فساد، مورد حفاظت بیشتر قانونی قرار گرفته‌اند. ازسوی‌دیگر شاغلین مناصب دارای دسترسی به اطلاعات حساس و محرمانه طبق ضوابط قانونی به‌عنوان شـــرط پذیرش جایگاه، داوطلبانه برای مبارزه با فساد، نفوذ و تخلف، نسبت به بخشی از حریم خصوصی خود صرف‌نظر می‌کنند.

۴. حفاظت از داده‌ها در شرایط بحران از قبیل همه‌گیری کرونا مورد بازنگری و تعدیل قرار می‌گیرد و ضوابط آن برای شرایط بحرانی می‌تواند انعطاف‌پذیری داشته باشد.

۵. حفاظت از داده‌ها یک فرایند است که با بلوغ سازمانی بخش دولتی محقق می‌شود. تصویب قوانین دائمی در بلندمدت به توسعه سطح حفاظت داده‌ها کمک می‌کند، اما در قوانین توسعه‌ای و سنواتی، ظرفیت‌سازی حفاظت از داده‌ها هدف‌گذاری می‌شود.

۶. در مراحل اولیه سامان‌دهی حفاظت از داده‌ها که بلوغ ســـازمانی پایین‌تر است، کمک گرفتن از مشاورین بیرونی به این امر سرعت داد، اما با شکل‌گیری دانش سازمانی، نهادها قادر شدند بدون کمک مشاورین و به‌صورت مستقل این وظایف را عهده‌دار شوند.

پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

بخش تقنین

پیشنهاد می‌شود در تدوین لایحه حفاظت از داده‌ها این نکات مدنظر قرار گیرد:

۱. اقتضائات خاص حفاظت از داده‌های دولتی (اولویت حقوق شهروندان و اتباع داخلی) و داده‌های در اختیار بخش خصوصی (تعادل بین هزینه رعایت ضوابط از سوی بخش خصوصی و حقوق شهروندان).

۲. رعایت انعطاف‌پذیری احکام در لایحه حفاظت از داده‌ها به‌خصوص در شرایط بحرانی از قبیل همه‌گیری کرونا.

۳. انعطاف‌پذیری حفاظت‌های حریم خصوصی بسته به سطح آسیب‌پذیری (کودکان و خبرنگاران) و میزانی که شخص موضوع داده در جایگاه قدرت قرار دارد.

۴. ایجاد نهادهای مستقل برای نظارت بر رعایت ضوابط حفاظت از داده از سوی نهادهای مجری قانون و بخش خصوصی.

۵. پرهیز از وابستگی غیرقابل بازگشت و بدون نظارت دولت به بخش خصوصی در ایجاد، نگهداری و عرضه نمایه‌های مربوط به داده‌های حساس مردم.

بخش نظارت

۱. در اجرای احکام امنیت فضای مجازی برنامه هفتم پیشرفت در فصل اقتصاد دیجیتال، احکام ظرفیت‌ساز برای حفاظت از داده‌ها (شناسایی و تحلیل حساسیت و طبقه‌بندی، نمایه‌سازی داده‌های در اختیار دستگاه‌ها از منظر حفاظت از داده و حریم خصوصی با کمک مشاورین) مدنظر قرار بگیرند.

۲. نظارت دوره‌ای بر پیشرفت تحقق احکام صورت پذیرد.

۱. مقدمه

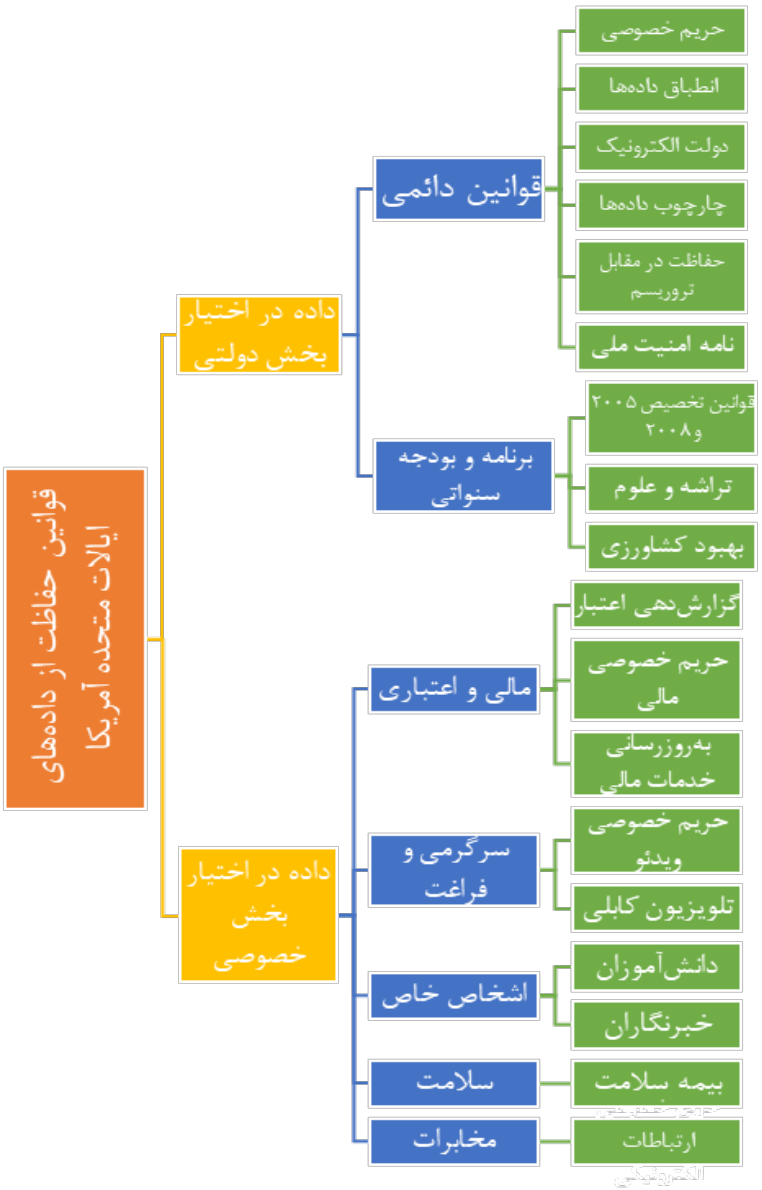
در عصر فناوری اطلاعات، دریافت، نگهداری و استفاده از داده و اطلاعات اشخاص به بخش مهمی از کسب‌وکارها و فعالیت‌های انتفاعی و غیرانتفاعی مختلف توسط اشخاص دولتی و غیردولتی مبدل می‌شـــود. حفاظت از داده‌ها، پیرامون ضوابطی اســـت که موجب افزایش اعتماد مردم به استفاده، نگهداری منصفانه و مسئولانه از داده‌هایشان می‌شود [۱]. درنتیجه، حفاظت از داده‌ها، گونه‌ای از معیارهای قابل پذیرش نزد عموم و نظامی از کنترل‌ها و مقابله‌هاست که بر ادعای منصفانه بودن اتکا دارد. حفاظت از داده‌ها، فرایند تضمین آزادی اختیار و حقوق افراد برای پردازش داده‌های مربوط به آنها را شامل می‌شود [۲]. به‌عنوان یک مفهوم حقوقی، حفاظت از داده‌ها دو حوزه حریم خصوصی داده (چگونگی کنترل گردآوری، استفاده و توزیع اطلاعات شخصی) و امنیت داده (چگونگی حفاظت از داده‌های شخصی در مقابل دسترسی و استفاده غیرمجاز و پاسخ به دسترسی یا استفاده غیرمجاز) را با یکدیگر ترکیب می‌کند [۳].

پایگاه‌های داده رایانه‌ای در دهه ۱۹۶۰ با ورود بازار شدن رایانه‌های ترانزیستوری شکل و در بخش مالی مورد استفاده قرار گرفتند. در ایالات متحده آمریکا، قانون گزارش‌دهی منصفانه اعتبار افراد[1] در سال ۱۹۷۰ یکی از اولین قوانین مرتبط با حریم خصوصی اطلاعات مالی در جهان است که تلاشی بر پایان یک دهه نابسامانی ناشی از اطلاعات غلط در مورد اشخاص در دهه ۱۹۶۰ بود.

پس از رسوایی واترگیت[2] و استفاده از زیرســـاخت‌های جاسوسی دولت برای شنود و کسب اطلاعات برای امور حزبی و جناحی [۴]، تصویب قانون حریم خصوصی در ســـال ۱۹۷۴، به‌منظور حفاظت از داده‌های بخش دولتی در ایالات متحده آمریکا در دستور کار قرار گرفت [۵]. استفاده از تجاربی که این کشور طی سال‌ها در مواجهه با چالش حفاظت از داده‌ها حتی با تصویب قانون معین حریم خصوصی و اصلاحات آن داشته است، می‌تواند در هر نوع مقررات‌گذاری حفاظت از داده‌ها در کشور ایران نیز مفید باشد. برای مثال در سال ۲۰۰۵ اطلاعات ۱۴۵ هزار نفر به سرقت رفت، در آن زمان خلأهای قانونی، دلیل موضوع اعلام، و برخی خواستار بازنگری قوانین مربوط به این موضوع شدند [۶]. در سال ۲۰۱۷ واقعه رخنه سایبری در اطلاعات شرکت اعتباری اکوئیفاکس[3] حادث شد که در آن اطلاعات ۱۴۲ میلیون شهروند این کشور از طرف هکرها به‌خاطر عدم توجه آن شرکت به رعایت مبانی اولیه امنیت سایبری به سرقت رفت و در ادامه کوتاهی شرکت مذکور و دولت در اطلاع‌رسانی واقعه به افرادی که تحت‌تأثیر قرار گرفته بودند نیز چالش زیادی ایجاد کرد. پس از این واقعه، نمایندگان حزب دمکرات چندین تلاش برای مقررات‌گذاری عام حفاظت از داده‌ها در بخش دولتی و خصوصی انجام دادند که تاکنون با توجه به عدم همراهی جناح جمهوری‌خواه که مقررات حفاظت از داده را به‌نوعی مقررات‌گذاری دست‌وپاگیر تلقی می‌کند به نتیجه نرسیده است [۷]. در حال حاضر قوانین این کشور در زمینه حفاظت از داده‌ها به دو دسته قوانین بخش خصوصی و عمومی تقسیم می‌شود. شکل زیر نمای کلی قوانین این کشور را نشان می‌دهد.

1. Fair Credit Reporting Act
2. Watergate Scandal
3. Equifax

شکل ۱. طبقه‌بندی قوانین ایالات متحده آمریکا



گزارش حاضر، سومین گزارش از مجموعه گزارش‌های پیرامون حفاظت از داده‌های آمریکاست. در گزارش اول، براساس چارچوب حفاظت از داده و مدل زنجیره ارزش داده‌ها، قوانین ایران در زمینه حفاظت از داده‌ها مدون شده است. در گزارش دوم، قانون اساسی، قوانین و مقررات فدرال و ایالتی این کشور با قوانین متناظر در ایران مقایسه شدند و گزارش حاضر نیز با هدف استخراج نکات مفید از تجربه قانونگذاری کشور آمریکا در حفاظت از داده در سطح قوانین کنگره، به بررسی مسائل زیر پرداخته است:

- معرفی ساختار کنگره و شیوه گردآوری مصوبات فناوری اطلاعاتی آن،
- معرفی قوانین حفاظت از حریم خصوصی داده‌های در اختیار بخش عمومی و خصوصی در این کشور،
- بازبینی قوانین حریم خصوصی در ایالات متحده آمریکا و مقایسه آنها با قوانین ایران،
- معرفی چند پیش‌نویس لایحه در زمینه قانون حریم خصوصی مطرح در این کشور.

بنابراین در ادامه، ابتدا ساختار کنگره و شیوه گردآوری مصوبات فناوری اطلاعات معرفی می‌شوند. سپس قوانین حفاظت از داده در بخش عمومی و خصوصی طبق طبقه‌بندی شکل ۱، بررسی می‌شوند.

۲. ساختار کنگره ایالات متحده آمریکا و شیوه گردآوری مصوبات فناوری اطلاعات آن

در ایالات متحده آمریکا، مجلس نمایندگان و سنا دو مجلسی هستند که در مجموع کنگره نامیده می‌شوند. اعضای مجلس نمایندگان بیشتر طرح‌های قانونی را پیشنهاد می‌دهند، اما اعضای مجلس سنا نیز می‌توانند طرح‌هایی را به مجلس سنا معرفی کنند. طرح‌های پیشنهادی ابتدا در کمیسیون مربوطه بررسی و در صورت تأیید در صحن مطرح می‌شود. پس از تصویب در صحن یکی از مجالس، در مجلس دیگر بررسی می‌شود. درصورتی‌که هر دو مجلس طرحی را تصویب کنند و رئیس‌جمهور هم طرح‌ها را رد نکند، این طرح‌ها تبدیل به قانون می‌شوند.

نحوه ارائه قوانین مصوب براساس دو نوع دسته‌بندی انجام می‌شود. در یک دسته‌بندی، قوانین در دو شاخه قوانین موقتی و بودجه‌ای با تاریخ انقضای مشخص و قوانین دائمی، طبقه‌بندی می‌شوند. قوانین دائمی و عمومی[1] توسط دفتر شورای بازنگری قوانین مجلس نمایندگان ایالات متحده آمریکا[2] در آدرس http://uscode.house.gov در یک طبقه‌بندی موضوعی ذیل ۵۳ عنوان[3] تقسیم‌بندی می‌شوند و هر عنوان شامل چند فصل[4] می‌شود و هر فصل شامل چندین بخش[5] است. در میان منابع رایگان،[6] این منبع به‌روزترین منبع طبقه‌بندی قوانین است. قوانین مربوط به مخابرات در عنوان ۴۷ این طبقه‌بندی قرار می‌گیرند و این عنوان بعضی قوانین مربوط به اینترنت را نیز دربر دارد. با وجود این، همه قوانین مرتبط با اینترنت در این بخش نیست و سایر بخش‌ها مانند تجارت و مبادله[7] در عنوان ۱۵ نیز بخش‌هایی مرتبط با اینترنت دارد.

در نوع دیگری از دسته‌بندی، طبقه‌بندی قوانین براساس مصوبات دوره مجالس کنگره صورت می‌پذیرد. با مراجعه به وب‌گاه کنگره به آدرس congress.gov می‌توان همه طرح‌هایی که از کنگره دوره ۹۳ تا کنگره دوره ۱۱۸ یعنی از سال ۱۹۷۳ تا ۲۰۲۴ در مجالس این کشور مطرح شده و در هر مرحله‌ای که هستند را در هر موضوعی جستجو کرد. در وب‌گاه کنگره، قوانین این کشور براساس حوزه‌های سیاستی[8] به ۳۲ حوزه تقسیم می‌شوند، قوانین مربوط به اینترنت در هر کدام از این حوزه‌ها قابل جستجو است، مثلاً مقررات مربوط به دو حوزه سیاستی آموزش[9] و خانواده[10] در زمینه اینترنت ممکن است قوانین مرتبط با حفاظت از کودکان در فضای مجازی را در خود داشته باشد. ازسوی‌دیگر قوانین این کشور از نظر تعریف سرفصل‌های قانونگذاری[11] به بیش از هزار عبارت موضوعی تقسیم شده است که هر عبارت را می‌توان برای جستجوی یک موضوع مشخص مورد بررسی قرار داد. اینترنت و رسانه‌های اینترنتی، خدمات‌رسان‌های اینترنتی از جمله عبارت‌های قانونی هستند که برای جستجوی قوانین مصوب دوره‌ای در زمینه اینترنت قابل استفاده هستند. در این گزارش، بخش قابل توجهی از قوانین مصوب کنگره ایالات متحده آمریکا براساس پایگاه کنگره بررسی شده‌اند تا هم قوانین دائمی و هم قوانین موردی و بودجه‌ای این کشور زیر پوشش قرار بگیرد.

نحوه ارائه و نمایش قوانین دوره‌ای مصوب ایالات متحده آمریکا معمولاً به این صورت است که در ابتدای قانون به‌طور خلاصه هدف از تصویب قانون بیان می‌شود. قسمتی با عنوان یافته‌ها[12] قبل از تعاریف در قانون گنجانده شده که شرایط اجرایی که موجب تصویب قانون شده و وضعیت عملکرد قبل از تصویب قانون را مشخص می‌کند. سپس کلمات و عباراتی که ممکن است در مورد آنها اختلاف‌نظر وجود داشته باشد در قسمت تعاریف[13] مدون می‌شوند. قوانین دوره‌ای ممکن است درواقع ترکیب چند قانون باشند که ارتباط دقیقی با یکدیگر نداشته باشند. مثلاً قانونی که سرمایه‌گذاری در بنادر ایالات متحده آمریکا را محدود می‌کند، موضوع قمار اینترنتی را نیز پوشش داده است. در این مواقع عناوین قانون[14] امکان تفکیک قوانین از یکدیگر را فراهم می‌کند.

---

1. General and Permanent Laws
2. Office of the Law Revision Counsel of the United States House of Representatives
3. Title
4. Chapter
5. Section

۶. طبقه‌بندی‌های حرفه‌ای‌تر مانند آنچه LexisNexis منتشر می‌کند، به‌روزتر هستند، سابقه قوانین را بهتر بیان می‌کنند و به احکام قضایی و آرای دادگاه‌ها و مقالات و تحقیقات مرتبط شده‌اند، اما با پرداخت وجه در دسترس هستند.

7. Commerce and Trade
8. Policy Area
9. Education
10. Families
11. Legislative Subject Terms
12. Findings
13. Definitions
14. Titles

مرکز پژوهش‌های کنگره آمریکا[۱] هفت موضوع شامل: ۱. حریم خصوصی اینترنتی، ۲. امنیت اینترنت و تجهیزات رایانه‌ای ۳. دسترسی به اینترنت پهن باند، ۴. تجارت الکترونیکی، ۵. پیام‌های ناخواسته، ۶. حکمرانی اینترنت و دامنه‌های اینترنتی، ۷. دولت الکترونیکی را مسائل مهم حول فناوری اینترنت در آن کشور برشمرده است [۸]. در ادامه قوانین حفاظت از داده‌ها با استناد به طبقه‌بندی مرکز پژوهش‌های کنگره آمریکا و پژوهش مستقیم اطلاعات وب‌گاه کنگره آمریکا استخراج و تا جای امکان با قوانین داخلی ایران مقایسه می‌شوند.

۳. قوانین حفاظت از داده‌های در اختیار بخش عمومی آمریکا و مقایسه آن با ایران

از دهه ۱۹۶۰، با رشد سامانه‌های دیجیتالی ذخیره و بازیابی اطلاعات، اصول مدیریت و جمع‌آوری اطلاعات توسط نهادهای دولتی و بین‌المللی نیز توسعه پیدا کرد. در سال ۱۹۷۳ اداره بهداشت، آموزش و رفاه ایالات متحده[۲] (HEW)، گزارشی را به کنگره ارسال کرد که در آن به کنگره پیشنهاد شده بود قوانینی را در زمینه سامانه‌هایی که داده‌های شخصی افراد را نگهداری می‌کنند وضع کند، این اصول به‌شرح زیر هستند [۹]:

- نباید هیچ‌گونه سامانه ذخیره داده‌های شخصی وجود داشته باشد که ماهیت وجودی آن محرمانه باشد.
- باید راهی برای فرد وجود داشته باشد تا بتواند با استفاده از اطلاعاتی که بدون رضایت وی و برای هدفی غیر از هدف اولیه که به همان منظور گردآوری شده، جلوگیری نماید.
- باید راهی برای هر فرد وجود داشته باشد تا بتواند اطلاعات قابل شناسایی در مورد خودش را اصلاح کرده، تغییر داده یا ضبط کند.
- هر سازمانی که داده‌های قابل شناسایی افراد را ایجاد، نگهداری، استفاده، یا منتشر می‌کند باید از قابلیت اطمینان داده‌ها برای تحقق هدف اولیه گردآوری داده اطمینان یافته و اقدامات احتیاطی را برای جلوگیری از سوءاستفاده از داده‌ها انجام دهد.

در ادامه قوانین متعددی در ایالات متحده آمریکا در حوزه حفاظت از داده‌های دولتی به تصویب رسیده که به دو دسته قوانین دائمی و قوانین بودجه‌ای قابل تقسیم است.

۳-۱. قوانین دائمی حفاظت از داده در بخش عمومی

ازجمله قوانین دائمی مهم حریم خصوصی ایالات متحده آمریکا می‌توان به قانون حریم خصوصی ۱۹۷۴، قانون انطباق رایانه‌ای و حفاظت از حریم خصوصی سال ۱۹۸۸، قانون دولت الکترونیکی سال ۲۰۰۲ و قانون چارچوب داده‌ای وزارت امنیت میهنی سال ۲۰۱۸ اشاره کرد. این قوانین به‌صورت مختصر در ادامه ذکر شده‌اند.

۳-۱-۱. قانون حریم خصوصی ۱۹۷۴[۳]

این قانون بر گردآوری، استفاده و توزیع اطلاعات افراد توسط آژانس‌های دولت فدرال محدودیت‌هایی وضع می‌کند. طبق این قانون، آژانس‌های فدرال مگر با رضایت شخصی فرد موضوع داده یا رضایت قبلی وی حق افشای هیچ‌گونه اطلاعاتی در مورد او را ندارند. قانون، اکثر افراد را مجاز می‌سازد که به اطلاعات پیرامون خودشان دسترسی پیدا کنند و الزام می‌کند که اطلاعات گردآوری شده باید صحیح، کامل، مرتبط و به‌روز باشد. شخص موضوع داده می‌تواند صحت داده‌ها را به چالش بکشد.

این مصوبه کنگره، اولین قانونی بود که این موضوعات را در بخش دولتی راهبری می‌کرد. در این قانون، کمیسیون حفاظت از حریم خصوصی (به‌عنوان یک سازمان) تشکیل می‌شود، کمیسیون موظف شد که:

۱. نقض این قانون را بررسی و به مراجع مشخص شده گزارش دهد.

۲. گزارش ارسالی نهادهایی که ایجاد سیستم‌های اطلاعاتی یا بانک‌های داده یا بسط قابل ملاحظه این نوع بانک‌های داده را اطلاع می‌دهند،[۴] بسنجد و اثر آن اقدامات بر حریم خصوصی و دیگر حقوق افراد را ارزیابی کند.

---

۱. Congress Research Service: بازوی مشورتی بی‌طرف و غیرجناحی کنگره آمریکا که تحقیقات را به سفارش و درخواست نمایندگان و مشاوران آنها به انجام می‌رساند.

2. Health, Education and Welfare

3.5. U.S.C. 552a. The Privacy Act of 1974

۴. برای طولانی نشدن روند توسعه سیستم‌های اطلاعاتی نیازی به اجازه این نهاد نیست، اما اطلاع رسانی الزامی است.

۳. یافته‌ها و رهنمودها در زمینه کنش‌های اداری و قانونی مرتبط با پیشنهادهای ردیف ۲ در بالا را برای انطباق با اهداف و الزامات این قانون عرضه کند.
۴. در صورت گزارش کمیسیون به کنگره در مورد عدم انطباق پیشـــنهاده[1] یا پروپوزال ایجاد یا اصلاح یک بانک داده یا سامانه اطلاعاتی با استانداردها (که پیرو این قانون تصویب می‌شود)، نهاد فدرالی پیشنهاددهنده باید تا ۶۰ روز پس از دریافت هشدار کمیسیون در زمینه عدم انطباق آن بانک اطلاعاتی یا سامانه اطلاعاتی با استانداردها، تأسیس یا اصلاح آن بانک اطلاعاتی را متوقف کند.
۵. اختیار بازرسی، برگزاری جلسه استماع، اخذ گواهی و شهادت شهود، الزام شهود به حضور در جلسات از طریق احضاریه، تولید مدارک و سوابق و گردآوری قسم‌ها.
۶. اختیار لغو، اصلاح یا پذیرش قوانین و مقررات مربوط به شیوه عمل اداره، سازمان‌ها و کارمندان زیر حوزه این کمیسیون.
۷. الزام کمیســـیون به انجام مطالعه‌ای روی بانک‌های اطلاعاتی، برنامه‌های پردازش داده خودکار و سیستم‌های اطلاعاتی دولتی، محلی و سازمان‌های خصوصی برای بررسی استانداردها و رویه‌های حفاظت از اطلاعات شخصی جهت تعیین میزان برآورد اهداف قانون.
۸. الزام کمیسیون به بررسی و تحلیل موارد زیر:

- انتقال میان ایالتی اطلاعات پیرامون افراد از طریق فرم‌های دستی یا رایانه‌ای و دیگر ابزارهای الکترونیکی یا مخابراتی.
- بانک‌های داده و برنامه‌های اطلاعاتی و سامانه‌های پردازش کننده بخش زیادی از اطلاعات مربوط به حریم خصوصی، حقوق مالکیت و دیگر حقوق افراد.
- استفاده از شماره‌های تأمین اجتماعی، شماره پلاک خودرو، شناساگرهای جهانی و دیگر نمادها برای شناسایی افراد در بانک‌های داده برای کسب دسترسی، یکپارچه‌سازی یا متمرکزسازی سیستم‌های اطلاعاتی و فایل‌ها.

۲-۱-۳. قانون انطباق رایانه‌ای و حفاظت از حریم خصوصی سال ۱۹۸۸[2]

۱. هنگامی که اطلاعات در اختیار نهادهای مختلف از یک شـــخص واحد با یکدیگر انطباق داده شوند، اطلاعاتی جدید از فرد قابل اکتشاف است که از اطلاعات مجزا قابل یافتن نیست، به این عمل انطباق رایانه‌ای یا انطباق پیشینه (رکوردهای)[3] رایانه‌ای گفته می‌شود. آشکار شدن آسیب‌های این موضوع باعث شد که اصلاحیه قانون حریم خصوصی ۱۹۷۴ و رویه‌های ایمنی‌افزا برای انطباق پیشینه رایانه‌ای تحت پوشش قانون، در دستور کار قرار گیرد. این قانون، نهادهای فدرال را موظف می‌کند که قبل از افشای اطلاعات برای استفاده در برنامه‌های انطباق وارد موافقت‌نامه‌های کتبی با نهادهای فدرال دیگر یا هستارهای غیرفدرال شوند.
۲. توجیه ضرورت انطباق، آگاهی دادن به افراد موضوع انطباق (ازجمله کارمندان فدرال) در مورد انطباق پیشینه داده مربوط به آنها، رویه‌های نگهداری و از بین بردن داده پس از انطباق و ممنوعیت افشای رکوردهای اطلاعاتی، بخش‌هایی از مفاد موافقت‌نامه‌های کتبی هستند.
۳. ارسال یک نسخه از موافقت‌نامه به کمیته‌های کنگره را الزامی می‌کند و در صورت درخواست باید مفاد موافقت‌نامه‌ها در دسترس قرار بگیرند.
۴. تا زمانی که اطلاعات حاصل از انطباق رایانه‌ای توسط کمیسیون اعتبارسنجی نشده باشند، نهادها را از خاتمه دادن، تعلیق، کاهش یا منع نهایی کمک مالی یا پرداخت به افراد، یا هرگونه کنش منفی علیه آن فرد منع می‌کند و برای افراد حق به چالش کشیدن چنین اطلاعاتی را قائل می‌شود.
۵. نهادها را ملزم می‌کند که هشدار راه‌اندازی یا بازنگری برنامه انطباق رایانه‌ای را در روزنامه رسمی دولت فدرال آمریکا منتشر کنند.
۶. نهادها را ملزم می‌کند که هر نوع پیشنهاده یا پروپوزال برای برقراری یا اصلاح چنین برنامه‌هایی را به کنگره یا اداره مدیریت و بودجه پیشاپیش اطلاع بدهد.
۷. هر نهاد موظف می‌شود که برای نظارت و هماهنگی بر اجرای این قانون هیئت تمامیت داده[4] تشکیل بدهد.
۸. قبل از اینکه نهاد از طریق تحلیل هزینه فایده نشان بدهد که برنامه انطباق مقرون‌به‌صرفه است هیئت تمامیت را از تأیید هرگونه برنامه انطباق منع می‌کند.
۹. تعیین رویه‌های فرجام‌خواهی موافقت‌نامه‌های رد شده را فراهم می‌سازد.
۱۰. تکلیف به انتشار دو سالیانه (امروزه سالیانه) قوانین اعمالی و هشدارهای نهادها در مورد رکوردهای اطلاعاتی حفظ‌شده پیرامون افراد توسط روزنامه رسمی فدرال.

---

1. Proposal
2. S.496 - Computer Matching and Privacy Protection Act of 1988
۳. اگر اطلاعات رایانه‌ای در یک جدول ذخیره شده باشند که ستون عنوان، ویژگی‌های ذخیره شده باشد و سطر اطلاعات مربوط به موجودیت خاصی باشد که اطلاعات مختلفی در مورد آن در جدول ذخیره شده است. رکورد به سطرها گفته می‌شود.
4. Data integrity

۳-۱-۳. قانون دولت الکترونیکی سال ۲۰۰۲

تکالیف حفاظت از داده‌ها در بخش‌های مختلف این قانون از جمله ۲۰۵، ۲۰۸، ۳۰۲ و ۵۱۲ وجود دارد. در بند «۳» از بخش ۲۰۵ دیوان عالی را مکلف می‌کند که مقرراتی جهت موضوعات حفاظت از امنیت و حریم خصوصی در فرایندهای الکترونیکی قضایی تدوین و ابلاغ کند.

بخش ۲۰۸ با عنوان ملاحظات حریم خصوصی، دستگاه‌های ذی‌ربط را ملزم به تخمین اثر حریم خصوصی (PIA[1]) پیش از توسعه و استفاده از فناوری‌های اطلاعاتی مربوط به گردآوری، نگهداری یا توزیع اطلاعات که منجر به شناسایی افراد بر حد نصاب‌های تعیین‌شده براساس اندازه سیستم اطلاعاتی، حساسیت اطلاعات و مخاطره آسیب ناشی از دسترسی غیرمجاز به آن داده‌ها می‌کند. همچنین گزاره‌هایی در زمینه اصلاح و معافیت از رعایت الزامات این بخش به‌دلیل مسائل امنیتی یا حفاظت از اطلاعات شخصی، حساس و طبقه‌بندی شده وضع می‌کند.

این قبیل تخمین‌ها به این موضوعات می‌پردازند که چه اطلاعاتی قرار است گردآوری شوند، چرا این اطلاعات باید گردآوری شوند، با چه کسانی به اشتراک گذاشته خواهند شد، چگونه به اشخاص هشدار یا امکان رضایت به آنها داده خواهد شد؟ هدف استفاده از اطلاعات، چگونگی ایمن‌سازی اطلاعات و این موضوع که سامانه سوابق طبق قانون حریم خصوصی ۱۹۷۴ ساخته خواهد شد از جمله اهداف این بخش از قانون است.

ریاست هر سازمان مشمول قانون را ملزم می‌کند که:

۱. سیاست‌ها و رهنمودهای اجرای این تخمین‌ها را تدوین کنند.

۲. بر پیاده‌سازی فرایند تخمین اثر حریم خصوصی در سراسر دولت نظارت کند.

۳. نهادها را ملزم می‌کند که در مورد سیستم‌های اطلاعاتی یا مجموعه‌های فعلی داده‌های منجر به شناسایی خودشان تخمین اثر حریم خصوصی انجام بدهند.

۴. همچنین اداره‌کنندگان نهادها ملزم می‌شوند که در وب‌گاه‌های نهاد که توسط عموم استفاده می‌شوند هشدار حریم خصوصی را ایجاد و نمایش بدهند.

در بخش ۳۰۲، قدرت الزام استانداردهای حداقلی امنیت سایبری به نهاد تخصصی اعطا می‌شود.

در بخش ۵۱۲، در مورد داده‌هایی که برای آمارگیری گردآوری شده‌اند، اشتراک‌گذاری بدون گمنام‌سازی را ممنوع و استفاده از آنها برای اهدافی غیر از هدف اولیه را مشمول مجازات می‌کند.

۴-۱-۳. قانون چارچوب داده‌های وزارت امنیت میهنی سال ۲۰۱۸[2]

این مصوبه، وزارت امنیت میهنی را مکلف می‌کند که این اقدامات را انجام دهد:

۱. برای یکپارچه‌سازی سامانه‌ها و مجموعه داده‌های وزارتخانه، چارچوب داده‌ای توسعه بدهد که دسترسی کارمندان مجاز را به‌صورتی منطبق با اختیارات قانونی آنها و رعایت سوگیری‌های حریم خصوصی، حقوق شهروندی و آزادی‌های مدنی برقرار سازد.

۲. اطمینان حاصل شـــود که همه اطلاعات ادارات وزارت امنیت میهنی یا زیرمجموعه‌های آن در افق چشم‌انداز اشتراک‌گذاری اطلاعات قرار می‌گیرند و هرگونه اطلاعات یا هوشمندی مرتبط با اولویت‌های مورد نیاز مأموریت و قابلیت‌های مورد نیاز امنیت میهنی که وزیر تشخیص بدهد در چارچوب داده قرار گیرد.

۳. اطمینان حاصل شود که چارچوب اطلاعات، در دسترس کارمندانی از وزارت امنیت میهنی باشد که مجوز امنیتی مناسب دارند و برای انجام وظیفه‌ای گمارده شده‌اند که در انجامش به دسترســـی به این اطلاعات نیاز دارند و در مورد استانداردهای منطبق بر حفاظت از این اطلاعات آموزش‌های لازم را گذرانده‌اند.

۵-۱-۳. قانون حفاظت در مقابل تروریسم و اصلاح ساختار بخش اطلاعات سال ۲۰۰۴[3]

در بخشی از این قانون، هیئت پنج عضوی نظارت بر آزادی‌های مدنی و حریم خصوصی[4] تأسیس شده تا بر عملکرد دستگاه‌های اطلاعاتی در اجرای قوانین ضد تروریسم نظارت کنند. دو عضو این هیئت با رأی مجلس سنا منصوب می‌شوند. هیئت حریم خصوصی و آزادی‌های مدنی در دفتر اجرایی ریاست‌جمهوری تأسیس شد.

1. Privacy Impact Assessment
2. H.R.2454 - Department of Homeland Security Data Framework Act of 2018
3. The Intelligence Reform and Terrorism Protection Act (P.L. 108-458) of 2004
4. Privacy and Civil Liberties Oversight Board

۶-۱-۳. قوانین اعطای حق ارسال نامه امنیت ملی به نهاد کنترل کننده داده‌ها

در قوانین ایالات متحده آمریکا، نامه‌های امنیت ملی،[1] گونه‌ای از احضاریه‌های اداری[2] هستند که توسط دولت ایالات متحده آمریکا برای گردآوری اطلاعات برای امور امنیت ملی به کار می‌روند. صدور این نامه‌ها، نیازی به تأیید قاضی ندارند و هنگامی که نیروهای امنیتی حین بررسی‌های خود نیازمند اطلاعات باشند برای تحقیقات خود می‌توانند این نامه‌ها را به کسانی که اطلاعات دیگران را نگهداری می‌کنند ارسال کنند.

به‌طور خلاصه قوانین نامه امنیت ملی ایالات متحده آمریکا طبق ارزیابی مرکز پژوهش‌های کنگره این کشور به پنج دسته تقسیم می‌شود که همان‌طور و در جدول ۱ اشاره شده، از جنبه‌های مختلف قابل مقایسه است.

جدول ۱. مقایسه قوانین نامه امنیت ملی ایالات متحده آمریکا با یکدیگر

	دسترسی ضدجاسوسی به قبض تلفن و سوابق تلفنی[3]	رویه‌های ویژه ضدجاسوسی و مبارزه با تروریسم[4]	افشا به اداره تحقیقات فدرال جهت امور ضدجاسوسی[5]	افشا به نهادهای دولتی جهت امور ضدتروریسم[6]	درخواست‌های بررسی‌کننده مجاز[7]
مخاطب	عرضه‌کنندگان خدمات ارتباطی	نهادهای مالی	نهادهای سنجش اعتبار مصرف‌کننده	نهادهای سنجش اعتبار مصرف‌کننده	نهادهای مالی، نهادهای سنجش اعتبار مصرف‌کننده
مقامات تأییدکننده	مقامات عالی پلیس فدرال و رؤسای استانی آن[8]	مقامات عالی پلیس فدرال و رؤسای استانی آن	مقامات عالی پلیس فدرال و رؤسای استانی آن	نهاد نظارتی (هر نهادی که فعالیت‌های ضد اطلاعاتی مرتبط با تحلیل تروریسم جهانی انجام می‌دهد)	مقامات عالی که از معاون وزیر یا دستیار ویژه وزیر سطح آنها پایین‌تر نباشد (فقط برای کارمندان دارای دسترسی به اطلاعات محرمانه)
اطلاعات تحت پوشش	نام، آدرس، طول خدمت و اطلاعات صورت حساب مشتری شناسایی‌شده	سوابق مالی مشتری شناسایی‌شده	نام، آدرس، آدرس‌های قبلی، محل کار و محل‌کارهای قبلی مصرف‌کننده شناسایی‌شده	همه اطلاعات مرتبط با مصرف‌کننده شناسایی‌شده	همه اطلاعات مالی مرتبط با کارمند شناسایی‌شده
استاندارد / هدف	مرتبط با تحقیقات برای حفاظت در مقابل تروریسم بین‌الملل یا فعالیت‌های اطلاعاتی محرمانه	درخواست شده برای اهداف ضدجاسوسی برای محافظت در برابر تروریسم بین‌الملل یا فعالیت‌های جاسوسی محرمانه	درخواست شده برای تحقیقات برای حفاظت از تروریسم بین‌الملل یا فعالیت‌های جاسوسی محرمانه	ضروری برای تحقیقات، فعالیت‌ها یا تحلیل‌های نهاد در ارتباط با تروریسم بین‌الملل	ضروری برای تحقیقات اعمال قانون، بررسی ضدجاسوسی یا تضمین امنیت
به اشتراک‌گذاری	فقط طبق رهنمود دادستان کل	فقط طبق رهنمود دادستان کل	از پلیس فدرال به دستگاه‌های نظامی برای تحقیقات جاسوسی به بازرسین نظامی برای اطلاعات مربوط به فرد نظامی	فاقد گزاره قانونی	فقط به نهاد کارمندی که تحت بررسی است، وزارت دادگستری جهت اعمال قانون یا اهداف جاسوسی هنگامی که طور شفاف در راستای عملیات باشد.
مصونیت قانونی / حق‌الزحمه	فاقد گزاره قانونی	فاقد گزاره قانونی	حق‌الزحمه، مصونیت قانونی بابت همکاری با حسن ظن با نامه امنیت ملی	مصونیت قانونی بابت همکاری با حسن ظن با نامه امنیت ملی	جبران هزینه / مصونیت قانونی بابت همکاری با حسن‌ظن با نامه امنیت ملی

1. National Security Letter
2. Administrative Subpoena
3. 18. U.S. Code § 2709 - Counterintelligence Access to Telephone toll and Transactional Records
4. 12 U.S. Code § 3414 - Special procedures
5. 15. U.S. Code § 1681u - Disclosures to FBI for Counterintelligence Purposes
6. 15. U.S. Code § 1681v - Disclosures to Governmental Agencies for Counterterrorism Purposes
7. 50 U.S. Code § 3162 - Requests by Authorized Investigative Agencies
8. Special Agents in Charge: پلیس فدرال آمریکا در ۵۶ منطقه تقسیم شده است که تقریباً معادل ایالت‌ها و درنتیجه مشابه استان‌های ایران است. عالی‌ترین مقام پلیس فدرال آمریکا در هر منطقه می‌تواند نامه امنیت ملی را صادر کند. در ایران این معادل رئیس پلیس فرماندهی استان‌هاست.

همان‌طور که در جدول ۱ مشاهده می‌شود، در این نامه‌ها، اطلاعات مختلفی درخواست می‌شود، در بعضی زمینه‌ها قانونگذار آمریکایی برای اخذ اطلاعات از طریق نهادهای امنیتی بدون حکم قاضی، محدودیت‌هایی وضع کرده است، مثلاً در زمینه مخابرات، اطلاعات محتوایی[1] قابل درخواست نیست، بلکه اطلاعات سوابق تراکنش‌ها درخواست می‌شود. مثلاً شماره‌هایی که فرد با آنها تماس گرفته از اپراتور مخابراتی درخواست می‌شود، اما این درخواست نمی‌تواند شامل محتوای تماس باشد. در زمینه اطلاعات در برخی قوانین همچون قانون حریم خصوصی ارتباطات الکترونیکی، قانون گزارش‌دهی اعتبار عادلانه، قانون حق حریم خصوصی مالی کنگره به پلیس فدرال اجازه داده که چنین نامه‌هایی به شرکت‌های دارنده اطلاعات مشترکان ارسال کند. شرکت‌هایی که این نامه‌ها را دریافت می‌کنند حق دارند در دادگاه نسبت به نقض حریم خصوصی مشترکان شان شکایت کنند، اما حق افشای این درخواست‌ها را ندارند. این قوانین به‌مرور زمان تکامل پیدا کرده‌اند. سوابق اصلاحات این قانون در پیوست شماره ۱ قابل مطالعه است.

این اختیارات قانونی برای نهادهای مجری قانون در مورد اتباع خارجی برای مقابله با جاسوسی خارجی و تروریسم بین‌الملل نشان می‌دهد که سیاست‌های حریم خصوصی بین اتباع خارجی و داخلی می‌تواند متفاوت باشد و از اتباع داخلی حمایت بیشتری بشود. در حالی که برای حمایت از داده کودکان سیاست‌های قوی‌تر حفاظت از داده قابل تدوین است، در مورد افرادی که دارای سطح بالاتری از دسترسی به اطلاعات محرمانه هستند، یا افراد در مرحله استخدام با مجوز قانونگذار، برای تصاحب این مشاغل باید نسبت به سایر اقشار جامعه از حریم خصوصی خود بیشتر صرف‌نظر کنند.

به باور برخی محققین [۴] در واکنش به سخت‌گیری‌های قانون حفاظت از حریم خصوصی سال ۱۹۷۴ برای بخش دولتی و قوانینی که پس از آن تصویب شدند، آژانس‌های اطلاعاتی ایالات متحده آمریکا به استفاده روزافزون از خدمات شرکت‌های خصوصی روی آوردند. این شرکت‌ها با استفاده از خلأهای قانونی به گردآوری گسترده اطلاعات شخصی شـــهروندان پرداختند. در حالی که اکثر شهروندان نیز از وجود چنین شرکت‌هایی خبر نداشتند. در نتیجه هنگامی که نشت اطلاعات شرکت چویس پوینت در سال ۲۰۰۴ آشکار شد، مشخص شد که شرکت‌های دلال داده تا چه حد وارد حریم خصوصی افراد شده‌اند. عدم معرفی نماینده به جلسه استماع از سوی این شرکت‌ها موجب شد که یک نماینده مجلس سنا، انتقادهای شدیدی را متوجه این شرکت‌ها کند و از آنها با عنوان صنعت در سایه نام ببرد. در سال ۲۰۱۳ نیز در گزارش کمیته حمل‌ونقل، علوم و تجارت مجلس سنا نیز بر عدم شفافیت فعالیت این شرکت‌ها تأکید شد [۱۰]، اما تاکنون کنگره این کشور موفق به اتخاذ اقدام بازدارنده علیه دلال‌های داده نشده است.

۷-۱-۳. قوانین دائمی مصوب مجلس شورای اسلامی ایران مرتبط با حفاظت از داده‌ها در بخش عمومی

در جمهوری اسلامی ایران بند «ف» ماده (۳) قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات حفاظت و حراست و عدم ضبط و افشای مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی را جزو وظایف وزارت ارتباطات تعیین کرده است. همین قانون اختیار تأیید نمونه (Type Approval) تجهیزات فناوری اطلاعاتی را به وزارت ارتباطات داده است. البته شمول عبارت تجهیزات به نرم‌افزارهای پایه‌ای و به‌روزرسانی‌های آنها ابهام دارد، اما در ابعاد جهانی فرایند تأیید نمونه در مورد نرم‌افزارها نیز صادق است و نهادی که تجهیزات را تأیید نمونه کرده، در مورد نرم‌افزارهای آنها نیز باید این کار را انجام بدهد.

بندهای «ک» و «ل» ماده (۳) قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات اختیارات تدوین و پیشنهاد استانداردهای ملی و اعمال استانداردهای فناوری اطلاعاتی را به این وزارتخانه داده است که به‌صورت طبیعی می‌تواند شامل استانداردهای امنیتی و حفاظت از داده‌ها نیز باشد، البته برای نادیده گرفتن استانداردهای ابلاغی ضمانت اجرایی در این قانون دیده نشده است.

طبق ماده (۵) قانون مدیریت داده‌ها و اطلاعات ملی مصوب سال ۱۴۰۱، دستگاه‌ها و نهادهای مشمول این قانون در امر تولید، نگهداری، پردازش، حفظ امنیت و صیانت از داده‌های شخصی و تبادل و اشتراک‌گذاری و تکمیل و به‌روزرسانی داده‌ها و اطلاعات ملی، سیاست‌ها و نظامات مصوب شورای‌عالی فضای مجازی و مصوبات کارگروه تعامل‌پذیر دولت الکترونیکی را اعمال و اجرا نمایند، اما چارچوب قانون و مصوبات صیانت از داده که باید براساس آن دستگاه‌ها به رعایت ضوابط حفاظت از داده ملزم شوند مشخص نیست.

طبق ماده (۶) قانون مدیریت داده‌ها و اطلاعات ملی، اعمال تدابیر حفاظتی و امنیتی جهت صیانت از داده‌ها و اطلاعات و حفظ محرمانگی داده‌ها و اطلاعات اشخاص برعهده دستگاه‌ها و نهادهای مشمول این قانون و ارائه‌دهندگان خدمات ذیل تنظیم‌گران بخشی است که مسئول تولید، نگهداری یا پردازش‌کننده داده‌ها و اطلاعات هستند و دستورالعمل و استانداردهای امنیت تبادل داده‌ها و اطلاعات و تأمین امنیت و ارزیابی آن مطابق نظامات و مصوبات شورای‌عالی فضای مجازی خواهد بود.

---

۱. برای این‌گونه اطلاعات حکم قضایی لازم است.

در ماده (۸) قانون مدیریت داده‌ها و اطلاعات ملی، به‌منظور صیانت و حفظ یکپارچگی در داده‌ها و اطلاعات ملی و صرفه‌جویی در تبادل داده‌ها و اطلاعات، دولت می‌تواند متناسب با کارکرد و نحوه و تواتر به‌روزرسانی آنها در مراکز داده دولت، براساس مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی، این داده‌ها را نگهداری نماید. دستگاه‌ها و نهادهای مشـــمول این قانون موظف به به‌روزرسانی برخط این پایگاه‌های اطلاعاتی هستند. تعیین سطح دسترسی به این پایگاه‌های اطلاعات به‌موجب مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی می‌باشد.

در بند «ب» ماده (۱) قانون انتشار و دسترسی آزاد به اطلاعات اطلاعات شخصی بدین شرح تعریف می‌شود: «اطلاعات فردی به مواردی نظیر نام و نام‌خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور اطلاق می‌شود». در ماده (۶) این قانون دادن اطلاعات شخصی فقط به شخص و نماینده قانونی او مجاز شده است. به‌صورت ضمنی این قانون، دستگاه‌ها را نسبت به گرفتن این اطلاعات مجاز می‌داند. درصورتی که اگر این اطلاعات در یک مرجع تخصصی ذخیره‌سازی شده و در مواقع لزوم فراخوانی شوند، ضمن کاهش افزونگی و اطلاعات متناقض در پایگاه‌های اطلاعاتی دستگاه‌های اجرایی در صورت ایجاد رخنه در یک دستگاه، اطلاعات کمتری از شهروندان افشا خواهد شد. اساساً ذخیره داده‌های تکراری غیرتخصصی توسط بخش‌های دولتی می‌تواند مورد بازنگری قرار بگیرد، همچنین در قوانین ایران تکالیفی مبنی‌بر تحلیل آثار داده‌های جمع‌آوری شده بر حریم خصوصی افراد وجود ندارد.

۲-۳. قوانین موقت و بودجه‌ای حفاظت از داده در بخش عمومی

در قوانین بودجه ایالات متحده احکام متعددی برای اجرایی‌سازی قوانین دائمی به تصویب رسیده است که در ادامه به‌صورت خلاصه ذکر می‌شوند:

۱-۲-۳. قانون تخصیص ادغام سال ۲۰۰۵[1]

بخش ۵۲۲ قانون تخصیص ادغام سال ۲۰۰۵ همه نهادهای فدرال را موظف می‌کند که یک مسئول عالی حریم خصوصی داشته باشند که وظیفه اصلی او اعمال سیاست حریم خصوصی باشد. هر نهاد را ملزم می‌کند که جهت حکمرانی بر گردآوری، استفاده، اشتراک‌گذاری، انتقال، ذخیره‌سازی و امنیت اطلاعات منجر به شناسایی کارمندان و عموم رویه‌های حفاظت از داده و حریم خصوصی جامع تدوین کنند. هر نهاد را ملزم می‌کند که حداقل هر دو سال یک‌بار ممیزی طرف ثالث برای این سیاست‌ها و رویه‌ها انجام بدهند. متن بخش ۵۲۲ این قانون برای آشنایی با شیوه تنظیم قوانین این کشور در زمینه حریم خصوصی در پیوست ۲ قابل مشاهده است.

۲-۲-۳. قانون تخصیص ادغام سال ۲۰۰۸

این قانون ضمن بازنگری در رویه‌های حفاظت از داده و حریم خصوصی در قانون مصوب سال ۲۰۰۵، الزام ممیزی نهادها توسط طرف‌های ثالث بی‌طرف را لغو می‌نماید و استفاده از ظرفیت‌های بیرونی را به تشـــخیص نهاد وا می‌گذارد و با تعریف جایگاه بازرس کل در سازمان‌ها، ممیزی، سیاست‌ها و رویه‌های حفاظت از داده‌ها و حریم خصوصی را مدون می‌کند.

۳-۲-۳. قانون تراشه و علوم سال ۲۰۲۲[2]

زیر بخش «ت» این قانون، با عنوان ایمن‌سازی تحقیق آمریکایی در مقابل سرقت سایبری،[3] برنامه‌ای جهت امنیت شبکه‌های تحقیقاتی این کشور پیشنهاد می‌دهد، اما در ارکان برنامه تکلیف می‌شود که باید طرح کلی برای انطباق برنامه امنیتی با پروتکل‌های فدرال حفاظت از داده‌ها نیز تهیه شود.

۴-۲-۳. قانون بهبود کشاورزی سال ۲۰۱۸[4]

کنگره، تشکیل سیســـتم اطلاعاتی برای اطلاعات یارانه توزیع مکمل‌ها ایجاد کرد و بخشی از تکالیف در ایجاد این سامانه رعایت پروتکل‌های حفاظت از داده بود. در بخشی از احکام عبارت‌هایی مانند حفاظت از داده زیر حکم درج می‌شود و در آن عنوان می‌شود که اطلاعات موضوع این بند فقط برای اهداف این بخش قابل استفاده است. یا جای دیگر کنگره تصریح می‌کند که اطلاعاتی که به مراکز تحقیقاتی داده می‌شود نباید منجر به شناسایی اطلاعات شخصی افراد شامل شماره تأمین اجتماعی و آدرس محل سکونت آنها شود.

---

1. HR 4818 Consolidated Appropriations Act, 2005
2. H.R.4346 - Chips and Science Act of 2022
۳. Securing American Research From Cyber Theft (d): از بخش ۱۰۳۷۴ به‌عنوان رایانش پیشـــرفته از قانون تأمین مالی امنیت دیوان عالی سال ۲۰۲۲ که قانون رایانش ظرفیت بالای سال ۱۹۹۱ بازنگری می‌کند.
4. Agriculture Improvement Act of 2018.

۴. قوانین حفاظت از داده‌های در اختیار بخش غیردولتی آمریکا و مقایسه آن با ایران

در آمریکا قانونگذاری در زمینه حفاظت از داده‌ها در بخش خصوصی عمدتاً برای داده‌های مربوط به حوزه‌های خاص مانند اطلاعات مالی و سلامتی انجام شده است. منطق قانونگذار آمریکایی از رویکرد بخشی در قانونگذاری ایالات متحده آمریکا این بوده است که فعالان بخش خصوصی می‌توانند در رقابت عادلانه با دیگر بازیگران، حفاظت لازم از کاربران را فراهم بیاورند. با وجود این، قوانینی نظیر قانون کمیسیون فدرال تجارت و قانون حفاظت مالی از مصرف‌کنندگان به‌صورت عام نیز بر رفتار کسب‌وکارها نظارت دارند.

کمیسیون فدرال تجارت به‌عنوان نهاد تنظیم‌گر می‌تواند کسب‌وکارها را نسبت به عدم تحقق وعده‌هایی همچون رعایت تدابیر امنیتی مربوط به نگهداری داده یا حفظ حریم خصوصی کاربران مورد بازخواست و تعقیب قضایی قرار دهد. به‌استناد قانون، تشکیل این کمیسیون حفاظت از داده به‌صورت کلان بخشی از الزامات و تعهدات کسب‌وکارها تلقی می‌شود. به‌بیان دیگر اگر کسب‌وکاری ادعا کند که از داده‌های اشخاص به‌خوبی حفاظت می‌کند و این کار را به‌درستی انجام ندهد، مرتکب کردارها یا کنش‌های فریبکارانه یا غیرمنصفانه در تجارت شده است. این موضوع در بخش پنج قانون کمیسیون تجارت جرم‌انگاری شده است. رفتار غیرمنصفانه در قانون، کرداری است که محتمل است یا می‌تواند منجر به آسیب جدی به مصرف‌کننده شـــود و مصرف‌کننده نمی‌تواند خودش اقدامی برای تعدیل آسیب انجام بدهد و این کردار به‌واسطه مزایایی که نصیب کاربر می‌شود قابل توجیه نیست، البته این قانون بر کسب‌وکارهایی که قانون خاص دارند قابل اعمال نیست.

قانون حفاظت مالی از مصرف‌کنندگان نیز مانند قانون کمیسیون تجارت فدرال، خط قرمزهایی که بر شرکت‌های بورسی و بازار اوراق بهادار، قابل اعمال است را تعریف می‌کند که از این خط قرمزها امکان وضع مقررات حفاظت از حریم خصوصی نیز قابل استنتاج است. این قانون اشخاص مشمول خودش را از ارتکاب کنش‌ها یا کردارهای تحمیلی، گمراه‌کننده یا غیرمنصفانه در پیشنهاد یا تأمین خدمت یا محصول مالی مصرفی باز می‌دارد. دفتر حمایت مالی مصرف‌کننده، مجری یا نهاد تنظیم‌گر این قانون است. این دفتر نسبت به کمیسیون تجارت فدرال از اختیارات بیشتری برای تنظیم‌گری نهادهای تحت پوشش خود برخوردار است. زیرا می‌تواند آنها را ملزم کند که استانداردهای رویه‌ای خاصی را رعایت کنند.

نکته حائز اهمیت این است که با توجه به اینکه ایالات متحده آمریکا به‌صورت سنتی صادرکننده اصلی خدمات فناوری اطلاعات بین‌المللی از طریق شرکت‌های اینترنتی بوده است، وضع مقررات سخت‌گیرانه در زمینه حریم خصوصی می‌توانسته با ایجاد سرمشقی برای کشورهای دیگر سلطه و هژمونی این کشور در این حوزه را با چالش مواجه کند [۱۱]. به این دلیل بسیاری از این محافظت‌ها، صرفاً در شرایط ضروری و در مواردی محافظت‌هایی بیش از آنچه در یک چارچوب عام حفاظت از داده‌ها لازم است، صورت می‌پذیرد.

حوزه‌هایی که حفاظت از داده در آنها از منظر قانونگذار ایالات متحده آمریکا نیازمند مقررات‌گذاری تشریحی بوده است عبارتند از: **امور مالی و اعتباری، سرگرمی و فراغت، اشخاص خاص نظیر کودکان و خبرنگاران، سلامت و داده‌های مخابراتی.**

۴-۱. حفاظت از داده‌ها در امور مالی و اعتباری

۴-۱-۱. قانون گزارش‌دهی اعتبار عادلانه ۱۹۷۰[1]

قانون گزارش‌دهی اعتبار عادلانـــه ۱۹۷۰ قدیمی‌ترین قانون حریم خصوصی ایالات متحده آمریکا به‌شـــمار می‌رود. ایـــن قانون با قانون تراکنش‌های اعتباری صحیح و عادلانه ۲۰۰۳ اصلاح شد. این قانون به تبیین حقوق افراد و مسئولیت آژانس‌های گزارش‌دهنده اعتبار[2] در آماده‌سازی و توزیع اطلاعات فردی در گزارش اعتباری می‌پردازد. طبق این قوانین آژانس‌های گزارش‌دهنده اعتبار نباید اطلاعات اعتباری را نزد افراد فاقد اهداف مجاز افشا کنند. شرایط افشا، اطلاعات را مشـــخص می‌کند و تا زمانی که نامه معتبر از سوی نهادهای امنیتی ارسال نشود نهاد مالی حق ارسال داده را ندارد. مفاد نامه معتبر درخواست اطلاعات از سوی قانونگذار در این قانون تشریح می‌شود و ریاست عالی نهاد امنیتی باید در نامه تصریح کند که برای عملیات اطلاعات خارجی و به‌دلیل مشکوک بودن فرد به جاسوسی یا ارتباط با این موضوعات این اطلاعات را درخواست می‌کند. این قوانین به شهروندان حق دسترسی رایگان سالیانه به اطلاعات مرتبط به خودشان و درخواست بازبینی و تصحیح اقلام اطلاعاتی را می‌دهد. همچنین اگر این اطلاعات مبنای رد درخواست شغل یا هر درخواستی باشند کسی که از اطلاعات استفاده می‌کند باید به کسی که درخواستش را رد می‌کند اطلاع بدهد که مبنای رد درخواست اطلاعات گزارش‌های پیرامون فرد است. به این ترتیب شخص می‌تواند درخواست تصحیح اطلاعات خود را بدهد.

1.15 U.S.C. 1681 – 81t. The Fair Credit Reporting Act of 1970 (FCRA)

۲. Credit Reporting Agencies: نهادهایی که وضعیت اعتباری افراد را براساس اطلاعات گردآوری شده از سوابق مالی آنها تعیین می‌کنند.

۲-۱-۴. قانون حق حریم خصوصی مالی ۱۹۷۸[1]

قانون حق حریم خصوصی مالی ۱۹۷۸ دسترسی دولت فدرال به اطلاعات رکوردهای بانکی را محدود می‌کند و رویه‌هایی برای دسترسی دولت فدرال به رکوردهای داده حساب‌های بانکی تعیین می‌کند.

۳-۱-۴. قانون گرام- لیچ- بلیلی یا به‌روزرسانی خدمات مالی ۱۹۹۹[2]

این قانون مؤسسات مالی را ملزم می‌کند استانداردهای مناسبی از جنبه حفاظت‌های اداری، فنی، فیزیکی، تدوین و رعایت کنند به‌نحوی که:

۱. از امنیت و محرمانگی اطلاعات و سوابق مشتریان اطمینان حاصل شود.

۲. کلیه سوابق در مقابل هر نوع تهدید یا خطر پیش‌بینی شده امنیتی حفاظت شوند.

۳. از دسترسی غیرمجاز یا استفاده از این اطلاعات یا سوابق برای اعمال آسیب یا نارضایتی هر مشتری حفاظت شود.

مؤسسات مشمول باید سیاست‌های حریم خصوصی خود و شیوه به اشتراک‌گذاری اطلاعات را به مشترکان خود اعلام کنند. مشتری می‌تواند اشتراک‌گذاری داده‌هایش را ممنوع کند و این نهادها اجازه نخواهند داشت اطلاعات شماره‌های حساب را با بازاریاب‌های از راه دور و بازاریاب‌های حضوری به اشتراک بگذارند.

۲-۴. قوانین حریم خصوصی در حوزه سرگرمی و فراغت

۱-۲-۴. قانون حفاظت از حریم خصوصی ویدئویی ۱۹۸۸ و قانون اصلاحیه حریم خصوصی اینترنتی ویدئویی ۲۰۱۲[3]

در این قانون، سوابق فردی که مشترک یا بیننده تصاویر متحرک یک عرضه‌کننده است، به‌وسیله اجازه اینترنتی او، قابل رونمایی به دیگران برای مقاصد دیگر است، البته زمان انقضای این اجازه حداکثر دو سال است، مگر اینکه فرد زودتر اجازه را لغو کند.

۲-۲-۴. قانون سیاستگذاری تلویزیون کابلی ۱۹۸۴[4]

این قانون افشای نام، آدرس و اطلاعات مربوط به نحوه استفاده کاربر را محدود می‌کند. طبق این قانون، مشترک خدمات تلویزیون کابلی باید به همه اطلاعات منجر به شناسایی که در مورد او گردآوری و حفظ شده، دسترسی داشته باشد. این قبیل اطلاعات باید در زمان‌های منطقی و از طریق جایگاه‌های مشخص از سوی اپراتور تلویزیون کابلی در اختیار مشترک قرار بگیرد. همچنین گردآوری هر نوع اطلاعاتی در مورد مشترک نیز باید از قبل به اطلاع او برسد و موافقت وی جلب شود. همچنین اپراتورها باید پس از خاتمه کاربرد داده‌های منجر به شناسایی فرد، نسبت به پاک کردن و از بین بردن این داده‌ها اقدام کنند.

۳-۴. قوانین حریم خصوصی اشخاص خاص

۱-۳-۴. قانون صیانت از حریم خصوصی اطلاعات و مستندات خبرنگاران سال ۱۹۸۰

در این قانون با استثنا قائل شدن برای امور خیلی حساس نظیر مستندات مربوط به امنیت ملی، اسرار هسته‌ای و حفظ زندگی افراد در سایر امور از خبرنگاران در مقابل دستور دستگاه‌های مجری قانون در زمینه ارائه هرگونه اطلاعات و محصولات کاری، مدارک و مستندات قبل از انتشار عمومی محافظت می‌کند و بر رعایت حریم خصوصی خبرنگاران حین بازرسی‌ها تأکید می‌کند.

۲-۳-۴. قوانین حریم خصوصی در حوزه کودکان و نوجوانان

قانون حریم خصوصی و آموزشی خانواده، ۱۹۷۴ دسترسی و افشای اطلاعات آموزشی به والدین، دانش‌آموزان و اشخاص ثالث را تنظیم می‌کند. ابزار قانونگذار آمریکایی برای تحقق امر حفاظت از اطلاعات بودجه است. تخصیص بودجه، مدارسی که شرایط مدنظر قانونگذار را رعایت نکنند، مثلاً دسترسی اطلاعات تحصیلی را به والدین ندهند از سوی قانونگذار غیرقانونی می‌شود.

---

1. 12 U.S.C 3401. The Right to Financial Privacy Act of 1978
2. Gramm–Leach–Bliley Act (GLBA)or Financial Services Modernization Act of 1999
3. Video Privacy Protection Act Amendments Act of 2012
4. 47 U.S.C. 551. The Cable Communications Policy Act of 1984, 47 U.S.C. 551

۴-۴. قوانین حریم خصوصی در حوزه سلامت

۴-۴-۱. قانون پاسخ‌گو بودن و قابل انتقال بودن بیمه سلامت ۱۹۹۶[1] و قانون فناوری اطلاعات سلامت برای اقتصاد و سلامت بیمارستانی ۲۰۰۹[2]

این قوانین، تدوین استانداردهای ملی برای حفاظت از اطلاعات منجر به شناسایی سلامت افراد را الزامی می‌کنند. این استانداردها که به‌صورت سنواتی به‌روزرسانی می‌شوند، انواع داده‌ها و تراکنش‌های حوزه سلامت را تعریف و ضوابط حفاظت از آنها را مشخص می‌کنند و درنهایت افشای اطلاعات حفاظت‌شده حوزه سلامتی افراد (PHI)[3] را محدود می‌نمایند. البته این قانون به اطلاعات سلامت در اختیار بخش رسمی نظام درمانی این کشور می‌پردازد و اطلاعات سلامتی گردآوری شده توسط ابزارهای هوشمند مانند ساعت‌های هوشمند و برنامه‌های کاربردی مشمول آن نیست.

۴-۴-۲. قانون حفاظت از داده بخش سلامت ایران در مقایسه با ایالات متحده آمریکا

در ایران، قانون تجارت الکترونیکی تدوین آیین‌نامه حریم خصوصی اطلاعات پزشکی را به وزارت بهداشت تکلیف کرده که تاکنون محقق نشده است.

۴-۵. قوانین حریم خصوصی در حوزه مخابرات

قانون حریم خصوصی ارتباطات الکترونیکی ۱۹۸۶،[4] محدودیت‌های لازم را بر نظارت الکترونیکی،[5] در اختیار داشتن تجهیزات نظارت الکترونیکی و استفاده از اطلاعات به‌دست آمده از طریق نظارت الکترونیکی اعمال می‌کند. این قانون، ارتباطات سیمی و الکترونیکی ذخیره‌شده (مانند پست الکترونیکی و پست صوتی)، دسترسی به رکوردهای تراکنش، ثبت‌کننده ارتباطات ارسالی و دریافتی[6] را مقررات‌گذاری می‌کند. این قانون دسترسی غیرمجاز به ارتباطات الکترونیکی ذخیره‌شده و افشای اطلاعات برای فراهم‌کننده ارتباطات را ممنوع می‌کند. همچنین عرضه‌کننده خدمات ارتباطی را در ارائه اطلاعات تراکنش به دولت محدود می‌کند.

۵. پیش‌نویس طرح‌ها و لوایح حفاظت از داده عرضه شده به کنگره در سال‌های اخیر

بررسی‌ها نشان می‌دهد که نمایندگان کنگره، طرح‌های متعددی را جهت بهبود حریم خصوصی در این کشور به کنگره تقدیم کرده‌اند. در اینجا به‌ترتیب زمانی چند مورد از این طرح‌ها به‌صورت مختصر معرفی می‌شوند:

۵-۱. قانون حفاظت از داده‌های مصرف‌کننده در کووید ۱۹ سال ۲۰۲۰

این لایحه قانونی با هدف حفاظت از اطلاعات سلامتی، مجاورت،[7] ابزارها و داده‌های مکان جغرافیایی طی بحران بهداشت عمومی ویروس کرونا پیشنهاد شده است. این قانون با توجه به شرایط بحرانی، به کسب‌وکارهای دارای دسترسی به بعضی از اطلاعات مؤثر در مبارزه با ویروس کرونا، اجازه پردازش بعضی از انواع مشخص داده را می‌دهد و حقوق مشـــتریان این کسب‌وکارها و تکالیف نهادهایی که داده‌ها را در اختیار دارند از طرف قانونگذار مدون می‌شود.

این طرح قانونی با توجه به این حقیقت تدوین شده که در شـــرایط اضطراری نیاز به انواعی از گردآوری اطلاعات است، اما پس از رفع وضعیت اضطرار لازم است که گردآوری اطلاعات خاتمه پیدا کند و امکان شناسایی صاحب داده از داده‌های عرضه شده از بین برود.

1. 42 U.S.C. 1320d note. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191)
2. Health Information Technology for Economic and Clinical Health Act of 2009
3. Protected Health Information
4. 18 U.S.C. 2510-2522, 2701-2711, 3121-3126. The Electronic Communications Privacy Act of 1986 (ECPA)
5. Surveillance
6. Pen Register and Trap and Trace Device
7. Proximity

۲-۵. قانون حفاظت از داده‌های سال ۲۰۲۰[1]

در صورت تصویب این طرح ایالات متحده آمریکا، یک قانون جامع حفاظت از داده‌ها در سطح فدرال خواهد داشت. در مواد طرح اشاره شده که این قانون تنها در مواردی که قوانین ایالتی و فدرال حفاظت‌های ضعیف‌تری اعمال می‌کنند جاری است. طی این طرح نهاد مستقلی با عنوان مرجع حفاظت از داده‌ها تشکیل خواهد شد و بعضی از وظایف کمیسیون تجارت فدرال در زمینه حفاظت از داده‌ها به این نهاد جدید منتقل خواهد شد [۱۲].

در این طرح قانونی «هستار زیر پوشش»[2] به‌معنای هر فردی[3] که داده‌های شخصی را گردآوری، پردازش یا به روشی دیگر کسب کرده است؛ با استثنای فردی[4] که داده‌های شخصی را برای امور شخصی یا فعالیت خانوار ذخیره می‌کند. اصلی‌ترین مفاد تعریف شده در این قانون به‌شرح ذیل است:

۱-۲-۵. کردار داده‌ای پرمخاطره

الف) هرگونه بررسی نظام‌مند یا گسترده اطلاعات شخصی شامل نمایه‌سازی،

ب) کاربرد داده‌های حساس،

ج) نظارت سامان‌مند داده‌های در دسترس عموم در مقیاس وسیع،

د) استفاده از فناوری‌های جدید در پردازش داده،

ه) تولید داده‌های مؤثر بر دسترسی شخص به محصولات و خدمات که تا حدی به‌صورت خودکار انجام می‌شود،

و) هرگونه نمایه‌سازی برای افراد در مقیاس وسیع،

ز) هرگونه پردازش داده‌های زیستی برای شناسایی یک فرد خاص،

ح) هرگونه پردازش اطلاعات ژنتیکی یا سایر اطلاعات مربوط به سلامتی،

ط) ترکیب، مقایسه یا انطباق داده از چند منبع،

ی) پردازش داده پیرامون اشخاص که مستقیماً از وی اخذ نشده است،

ک) استفاده از داده‌های کودکان،

ل) پردازش اطلاعات مکانی افراد.

۲-۲-۵. داده شخصی

داده شخصی اصطلاحی است که به‌معنای هرگونه اطلاعاتی است که به‌صورت مستقیم یا غیرمستقیم شخص یا وسیله‌ای را شناسایی و آن را توصیف می‌کند، یا قادر است به آن مرتبط شود یا منطقاً می‌تواند مرتبط شود. شامل:

الف) یک شناساگر از قبیل نام واقعی، نام مستعار، امضا، وضعیت تأهل، ویژگی‌ها یا توصیف فیزیکی، آدرس پستی، شماره تماس، شناساگر واحد شخص، شماره شناسایی نظامی، شناساگر برخط، آدرس پروتکل اینترنت، آدرس ایمیل، نام حساب، نام خانوادگی پیش از ازدواج، شماره تأمین اجتماعی، شماره گواهینامه رانندگی، شماره پاسپورت، یا دیگر شناساگرهای مشابه؛

ب) اطلاعاتی همچون، وضعیت اشتغال، سوابق شغلی، یا سایر اطلاعات حرفه‌ای مرتبط با شغل؛

ج) شماره حساب بانکی، شماره کارت اعتباری، شماره کارت اعتباری نقدی، شماره بیمه‌نامه یا هرگونه اطلاعات مالی دیگر؛

د) اطلاعات پزشکی، اطلاعات سلامت روان یا اطلاعات بیمه سلامت؛

ه) اطلاعات تجاری، شامل سوابق دارایی‌های شخصی، محصولات یا خدمات خریداری‌شده، کسب شده یا مدنظر قرار گرفته یا دیگر سوابق یا گرایش‌های مصرف یا خرید؛

و) ویژگی‌های رده‌های حفاظت‌شده در قوانین فدرال شامل نژاد، رنگ، ملیت، مذهب، جنسیت، سن یا ناتوانی؛

ز) اطلاعات زیست‌سنجی؛

ح) اطلاعات فعالیت‌های اینترنتی یا دیگر فعالیت‌های شبکه‌ای شامل، سابقه مرورگری، سابقه جستجو، محتوا و اطلاعات پیرامون تعامل یک شخص با وب‌گاه اینترنتی، برنامه موبایلی یا تبلیغات؛

---

1. S.3300 - Data Protection Act of 2020
2. Covered Entity
3. Person
4. Individual

ط) داده‌های مکان جغرافیایی آنی یا سوابق آن؛
ی) اطلاعات بویایی، حرارتی، دیداری یا شنیداری و مشابه آن؛
ک) سوابق آموزشی؛
ل) اطلاعات سیاسی؛
م) تصاویر دیجیتالی محافظت شده از طریق گذرواژه و ویدئوهایی که در دسترس عموم نیستند؛
ن) اطلاعات پیرامون اتهامات یا سابقه جلب؛
س) اطلاعاتی (مانند آدرس پروتکل اینترنت یا دیگر شناساگرها) که جداسازی یک شـــخص یا وسیله برای تعامل را ممکن می‌سازد حتی بدون شناسایی فرد یا وسیله؛
غ) استنتاج‌هایی که هرگونه از اطلاعاتی که در این زیر بخش شناسایی‌شده برای اســـتخراج یک نمایه بازتاب‌دهنده ترجیحات، ویژگی‌ها، روندهای روان‌شناسانه، تمایلات، رفتارها، گرایشات، هوشمندی، توانمندی‌ها و شایستگی‌های فرد.

۳-۲-۵. پردازش[1]

اصطلاح پردازش یعنی اجرای یک عملیات یا مجموعه‌ای از عملیات بر روی داده‌های شخصی، به‌صورت دستی یا خودکار که شامل و نه محدود می‌شود به گردآوری،[2] ضبط،[3] سازمان‌دهی،[4] ساختاردهی،[5] ذخیره،[6] تطبیق[7] یا اصلاح،[8] بازیابی،[9] مشاوره،[10] افشا،[11] از طریق جابه‌جایی،[12] مرتب‌سازی،[13] طبقه‌بندی،[14] توزیع،[15] در دسترس قرار دادن، همراستاسازی یا ترکیب،[16] محدودسازی،[17] پاک کردن[18] یا انهدام.[19]

۴-۲-۵. اطلاعات و گزارش‌ها

یکی از بخش‌های مجزای این طرح قانونی «اطلاعات و گزارش‌ها»[20] نام دارد. در این بخش، نهاد متولی حفاظت از داده‌ها موظف شده که به‌طور سالیانه گزارش‌هایی را از عملکرد خودش به کمیسیون‌های مجلس این کشور عرضه کرده و همین طور آنها را در وب‌گاه رسمی خود منتشر کند. محتوای هر گزارشی که قانون الزامی کرده است باید[21] شامل:

۱. بحثی پیرامون مشکلات مهمی که افراد پیرامون حریم خصوصی یا امنیت اطلاعات شخصی با آن مواجه هستند؛
۲. توجیهی از درخواست بودجه سالیانه نهاد برای سال آتی، مگر اینکه توجیه بودجه آن سال قبلاً در گزارش‌های تهیه شده براساس رهنمودهای این ماده منتشر شده باشد.
۳. فهرستی از قوانین مهم و دستوراتی که توسط نهاد اتخاذ شده‌اند و ابتکاراتی که نهاد در طول دوره ۶ ماهه اجرا کرده و سایر ابتکاراتی که قرار است در ۶ ماه آینده اتخاذ شوند.

---

1. Process
2. Collecting
3. Recording
4. Organizing
5. Structuring
6. Storing
7. Adapting
8. Altering
9. Retrieving
10. Consulting
11. Disclosing
12. Transmission
13. Sorting
14. Classifying
15. Disseminating
16. Combining
17. Restricting
18. Erasing
19. Destroying
20. Information and Reports
21. Shall

۴. تحلیلی از شکایات نسبت به نقض حریم خصوصی یا امنیت اطلاعات شخصی که نهاد دریافت و طی ۶ ماه گذشته گردآوری کرده است.
۵. تخمینی از اقدامات مهمی که طی ۶ ماه گذشته دادستان‌های کل در ارتباط با موضوعات مرتبط با این قانون اتخاذ کرده‌اند یا قوانینی که در این قانون توصیف شده‌اند.

از نحوه تنظیم این طرح قانونی مشاهده می‌شود که تکالیف هستارهای تحت پوشش مستقیماً ازسوی قانونگذار به آنها تکلیف نشده، بلکه قانونگذار در قالب مسئولیت نهاد متولی حفاظت از داده‌ها آنها را صورت‌بندی کرده است. بدین ترتیب هم در حجم مصوبه صرفه‌جویی شده و هم مصوبه و مسئولیت نهاد متولی حفاظت از داده شفافیت بیشتری پیدا کرده است. مثلاً قانونگذار به‌جای اینکه تکلیف کند شرکت‌ها حق ندارند برنامه‌های کسب‌وکار مبتنی‌بر خرید حریم خصوصی را اجباری کنند، یکی از تکالیف نهاد حفاظت از داده را این موضوعات تعیین کرده است: از عادلانه بودن مفاد قراردادها در بازار اطمینان حاصل کند، شامل ممنوع کردن درج «گزاره‌های پرداخت به‌ازای حریم خصوصی» و «پذیرش یا رها کردن» در مفاد خدمات، همچنین به‌جای اینکه طراحی امن را اجباری کند، دیگر وظیفه نهاد حفاظت از داده این کشور را این تعیین می‌کند که باید «فنون ارتقای امنیت از قبیل حریم خصوصی از طریق طراحی و فنون حداقل‌سازی داده را ترویج کند». تعیین ضمانت اجرا در این طرح قانونی در حوزه اختیارات مجلس قانونگذاری این کشور باقی مانده است. در فصل مربوط به زمان‌بندی اجرا، سقف مجازاتی که این نهاد می‌تواند برای متخلفین اعمال کند مشخص شده است. همچنین قانونگذار تدابیری جهت عدم تداخل وظایف میان نهاد جدید و نهادهای قدیمی در نظر گرفته است، مثلاً همکاری میان این نهاد تازه تأسیس و دادستانی این کشور در طرح قانونی ضابطه‌مند شده است، یا از کمیسیون تجارت فدرال در زمینه حفاظت از داده‌ها صراحتاً خلع مسئولیت شده است.

۵-۳. قانون ذخیره داده آمریکا در خاک آمریکا[1]

این طرح قانونی توسط نمایندگان جمهوری‌خواه به مجلس پیشنهاد شده اســت. این طرح، ممنوعیت ذخیره داده شهروندان آمریکا توسط شرکت‌هایی مانند تیک تاک در کشورهای خارجی متخاصم نسبت به این کشور شامل چین و ایران را دنبال می‌کند. همچنین این قانون دسترسی مقامات دولتی کشورهای متخاصم به داده‌های تحت پوشش را ممنوع می‌کند.

۵-۴. طرح‌ها و لوایح حفاظت از داده در دولت و مجلس شورای اسلامی ایران

در ایران طرح حمایت و حفاظت از داده و اطلاعات شخصی در ماه‌مهر سال ۱۳۹۹ اعلام وصول شد، در ادامه با توجه به اعلام دولت مبنی‌بر ارائه لایحه حفاظت از داده‌ها این طرح مسکوت ماند. به‌نظر می‌رسد لایحه حفاظت از داده‌ها مراحل پایانی نهایی شدن و ارسال به مجلس را طی می‌کند.

۶. جمع‌بندی

در نظام حقوقی ایالات متحده آمریکا، قانونگذار میان داده‌های متفاوت مثلاً داده‌های مالی و مربوط به سلامت و اشخاص مختلف موضوع داده مثلاً کودکان و خبرنگاران در حقوق مربوط به داده‌ها، تمایزهایی قائل شده که با قوانین عمومی حفاظت از داده‌ها، متفاوت است. به‌بیان دیگر در این نظام حقوقی حفاظت از داده‌های مالی و حفاظت از داده‌های مربوط به سلامتی، چارچوب‌های متفاوتی از محافظت را تجربه می‌کنند. کودکان و افراد خردسال و صاحبان برخی مشاغل مانند خبرنگاران از جمله اشخاص موضوع داده‌ای هستند که حقوق و تکالیف کسب و کارها و دولت نسبت به آنها از نظر قانونگذار بالاتر از سایر اقشار جامعه تدوین شده، اما افراد متقاضی خدمت در مشاغل دارای دسترسی به اطلاعات محرمانه با حکم قانونگذار جهت بهبود نظارت و جلوگیری از بروز فساد مالی و یا کاغذبازی و پر کردن فرم‌های گزارش مختلف باید داوطلبانه از بخشی از حریم خصوصی خود به نسبت سایر اقشار جامعه صرف‌نظر کنند. بررسی پیش‌نویس‌های قوانین حمایت از حقوق داده در ایالات متحده آمریکا نشان می‌دهد در شرایط بحران مانند کووید ۱۹ سطوح حفاظتی حریم خصوصی باید انعطاف لازم را داشته باشد.

مقررات حفاظت از داده‌ها به دو دسته قوانین حفاظت از داده‌های بخش دولتی و بخش خصوصی قابل تقسیم هستند. در زمینه حفاظت از داده‌های دولتی ایالات متحده آمریکا دو دهه قبل از دیگر کشورهای مهم مانند کره جنوبی مقررات‌گذاری حفاظت از داده‌های شهروندان در پایگاه‌های اطلاعاتی دولتی را آغاز کرده است.

1. H.R.6410 - U.S. Data on U.S. Soil Act

انطباق دستگاه‌های دولتی با موازین حفاظت از داده‌ها تنها به تصویب قوانین محدود نمی‌شود، تجربه ایالات متحده آمریکا نشان می‌دهد این موضوع یک پروژه از جنس برنامه‌های توسعه‌ای است. این کشور در زمینه حفاظت از داده‌هایی که بخش خصوصی عهده‌دار نگهداری آن است، با توجیه لزوم تداوم سلطه شرکت‌های آمریکایی بر جریان اطلاعات جهانی نسبت به دیگر کشـــورهای مهم جهان عقب‌ماندگی دارد، اما این عقب‌ماندگی با لابی گری و کارشکنی این بازیگران تاکنون رفع نشده است.

به‌بیان‌دیگر مقررات بسیار سخت‌گیرانه در حمایت از مشتریان یا برآوردن نیاز اطلاعاتی دولت می‌تواند رشد اقتصاد داده در کشور را دچار مشکل کند. سخت‌گیری بیش از حد در مسیر گردآوری اطلاعات توسط بازیگران دولتی نیز می‌تواند بخش امنیتی کشورها را وابسته به نهادهای خصوصی غیرپاسخ‌گو و غیرشفاف کند و عملاً با واگذاری قدرت اطلاعات به بخش خصوصی نهادهای امنیتی و نظام قانونگذاری کشور آمریکا به‌رغم درک مشکل نتوانسته است اقدامی در جهت منافع عمومی جامعه اتخاذ کند. بنابراین اقدام قانونگذار برای توانمند ساختن شهروندان در کنترل معنادار حریم خصوصی خود در عین توسعه یک زیست‌بوم داده مستعد و روبه‌رشد که در آن کارآفرینان و شرکت‌های فناوری بتوانند با رقبای خارجی رقابت داشته باشند و اشراف اطلاعاتی مسئولانه دولت‌ها محقق شود، با توجه به شکست ایالات متحده آمریکا در حمایت از شهروندان خودش اهمیت می‌یابد. قانونگذاران کشورهای مختلف با تصویب قوانین و مقررات حفاظت از داده‌ها در تلاش هستند که براساس سیاست‌های کلی کشور خود میان این اهداف مزاحم و متضاد تعادل برقرار کنند.

باید از اجبار شهروندان به چشم‌پوشی از حریم خصوصی خود به‌ازای استفاده از محصولات یا خدمات شرکت‌ها جلوگیری کرد. یعنی یک شرکت نباید چشم‌پوشی اجباری شهروندان از حق حریم خصوصی خود را شرط استفاده از محصولات خود قرار دهد. حق دسترسی، تصحیح و پاک کردن داده‌های شخصی که در اختیار یک شرکت خصوصی است باید از جمله حقوق قانونی شهروندان باشد. شرکت‌ها باید از گردآوردن مقادیر زیادی از داده‌هایی که ربطی به آنچه برای عرضه خدمت به مشتری به آن نیاز ندارند منع شوند. شرکت‌ها باید فقط داده‌هایی را بگیرند که برای عرضه خدمات‌شان ضروری است.

شرکت‌ها باید موظف باشند که داده‌های خصوصی مشتریان خودشان را به‌شکل ایمن و حفاظت‌شده نگهداری کنند. هدف‌گذاری قوانین باید به‌گونه‌ای باشد که نشت اطلاعات روز به‌روز کاهش یابد. همچنین قوانین باید از کودکان و نوجوانان بیشتر محافظت کنند. قانونگذار باید به دولت، قدرت اجرایی متناسب با تکالیف آن را بدهد تا دولت اختیار لازم برای اجرای قوانین متناسب با پیشرفت فناوری را داشته باشد. حریم خصوصی اینترنتی ملاحظات متنوعی را دربر می‌گیرد. از یک طرف اینترنت کسب اطلاعات پیرامون کاربران را برای بخش دولتی و خصوصی تسهیل می‌کند، از طرف دیگر این اطلاعات ممکن است علیه کاربران استفاده شود. ارسال و اشتراک این داده‌ها با طرف‌های ثالث که ممکن است بدون اطلاع فرد موضوع داده صورت گیرد، از جمله موارد مهم در این زمینه هستند.

براساس مطالعه صورت گرفته پیشنهاد می‌شود:

۱. داده در اختیار بخش دولتی نیز در چارچوب حفاظت از داده مدنظر قرار بگیرد.

۲. در قوانین مربوط به انطباق داده‌های مربوط به پیشینه موضوعات مختلف مثلاً اطلاعات مالی برای موضوع یارانه‌ها حتماً رضایت شخص موضوع داده مدنظر قرار گیرد، به‌صورتی که در صورت عدم رضایت شخص داده‌های او پردازش نشود، در صورت رضایت شخص موضوع داده، استعلام‌ها ابتدا به‌خود او اعلام و در صورت تأیید وی برای دریافت خدمات به نهاد نیازمند اطلاعات ارسال شود، البته تا زمانی که داده‌ها دریافت نشده‌اند خدمات عرضه نمی‌شوند.

۳. بخش مهمی از تدابیر دولت الکترونیکی باید همراه با رعایت تدابیر حفاظت از داده باشد و هر برنامه توسعه دولت الکترونیکی باید مکلف به رعایت ضوابط حفاظت از داده‌ها و تعیین وضعیت و سطح مخاطره داده‌های در اختیار بشود.

۴. طبق ماده (۳) قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، طراحی و تدوین نظام ملی فناوری اطلاعات کشور، تدوین و پیشنهاد استانداردهای ملی مربوط به ارتباطات و فناوری اطلاعات در کشور به مراجع ذی‌ربط، اعمال استانداردها، ضوابط و نظام‌های کنترل کیفی و تأیید نمونه تجهیزات شبکه‌های فناوری اطلاعات در کشور، حفاظت و حراست مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی، را در حوزه اختیارات وزارت ارتباطات قرار داده است، اما دستگاه‌ها الزامی به رعایت ضوابط، نظام‌ها و استانداردهای پیشنهادی وزارت ارتباطات و فناوری اطلاعات ندارند، بنابراین لازم است که دستگاه‌های اجرایی مختلف مکلف به رعایت این تدابیر شوند و برای عدم رعایت تدابیر ابلاغی وزارت ارتباطات، ضمانت اجرایی کافی تصویب شود.

۵. هیئت مستقل نظارت بر رعایت تدابیر حفاظت از داده‌ها می‌تواند نظارت بر اجرای تدابیر را عهده‌دار شود، اما در ایران این وظیفه می‌تواند برعهده سازمان بازرسی کل کشور نیز قرار گیرد.
۶. استفاده از سامانه‌های قابل نظارت پسینی برای ارسال درخواست اطلاعات ازسوی نهادهای مجری قانون می‌تواند ضمن سرعت دادن به روند درخواست اطلاعات مورد نیاز مجریان قانون و نهادهای انتظامی نظارت بر رعایت حریم خصوصی ازسوی این نیروها را نیز تسهیل کند.
۷. قوانین بودجه باید ابتدا با کمک بخش خصوصی و سپس با تکیه بر توان دولت برای ظرفیت‌سازی حفاظت از داده‌ها در بخش دولتی اقدام کنند.
۸. هر طرح توسعه سامانه‌های اطلاعاتی باید همراه با پیوست حفاظت از داده باشد و در این زمینه وزارت ارتباطات و فناوری اطلاعات می‌تواند به دستگاه‌ها کمک کند.
۹. برای اطلاعات مالی اعتباری و سلامت می‌توان حفاظت از داده‌های بالاتری را نسبت به سایر داده‌های در اختیار بخش خصوصی تعیین کرد.
۱۰. ضوابط حفاظت از داده‌های سلامت نباید محدود به نظام بهداشت و درمان باشد و می‌تواند شامل اطلاعات اینترنت اشیا نیز بشود.
۱۱. ضوابط مربوط به حریم خصوصی حوزه سلامت و سرگرمی در حوزه ویدئو به‌صورت تقاضا (برای مثال فیلیمو، نماوا یا تلوبیون) نیازمند تدوین و تنظیم است.
۱۲. ضوابط حریم خصوصی اشخاص خاص مانند کودکان و خبرنگاران می‌تواند بالاتر از سایر اقشار جامعه تعیین شود.
۱۳. برای در اختیار داشتن تجهیزات غیرمجاز و غیرقانونی شنود مخابراتی باید مجازات‌های بازدارنده وضع و بر اجرای این مجازات‌ها نظارت کافی صورت گیرد.

پیشنهاد مطالعات آتی

پیشنهاد می‌شود در گزارش‌های آینده، موارد زیر مورد بررسی قرار گیرد:
۱. مقایسه مجموعه قوانین کنگره، قوانین مصوب مجالس ایالتی و قانون اساسی ایالات متحده آمریکا در چارچوب‌های حریم خصوصی تدوین شده توسط آقای سولو و ارتقا یافته با قوانین ایران و طرح‌ها و لوایح مجلس شورای اسلامی ارائه پیشنهادهایی برای بهبود قوانین.
۲. سیر تاریخچه قوانین حفظ حریم خصوصی داده‌ها در ایالات متحده و نحوه تکامل آن براساس نقاط عطف در دهه‌های ۱۹۶۰، ۱۹۷۰ و ۲۰۱۰.
۳. بررسی قوانین مصوب و طرح‌های اعلام وصول شده در کنگره از زاویه ضمانت‌های اجرایی.
۴. نظام نظارت بر اجرای قوانین حریم خصوصی.
۵. مقایسه مصوبات شورای‌عالی فضای مجازی و کمیسیون عالی تنظیم مقررات آن نظیر: ۱. دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی، ۲. دستورالعمل سامان‌دهی خدمات میزبانی در فضای مجازی با قوانین ایالات متحده آمریکا.

پیوست ۱. تاریخچه اصلاح قوانین نامه امنیت ملی

در عنوان پنجم قانون کنترل نرخ بهره و تنظیم‌گری نهادهای مالی سال ۱۹۷۸[1] یا قانون حق حریم خصوصی مالی ۱۹۷۸، به نهادهای مالی اجازه داده شده بود که اطلاعات مالی را به اداره تحقیقات فدرال بدهند، اما الزامی به ارائه اطلاعات نبود. درنتیجه در ایالت‌هایی که قوانین حریم خصوصی مستقل مالی تصویب شده بود، این اطلاعات به این اداره داده نمی‌شد. بنابراین قانون نامه امنیت ملی طی اصلاحیه سال ۱۹۸۶ به تصویب کنگره رسید تا به پلیس فدرال اجازه صدور نامه امنیت ملی داده شود.

1. Financial Institutions Regulatory and Interest Rate Control Act of 1978

قانون حریم خصوصی ارتباطات الکترونیکی سال ۱۹۸۶:[1] در این قانون که اصلاحیه قوانین قبلی بود، صدور نامه امنیت ملی برای دسترسی اطلاعات تلفنی و اطلاعات مشتریان سایر خدمات ارتباطاتی را فراهم کرد. هر دوی این قوانین استفاده از این اختیار را به موضوعات جاسوسی خارجی و ارتباط با مقابله با جاسوسی خارجی محدود کرده بودند.

بخش ۸۰۲ قانون مجوز جاسوسی سال مالی ۱۹۹۵:[2] این قانون، اختیار نامه امنیت ملی را به کارمندان دولتی مظنون به جاسوسی و افرادی که خواستار اشتغال در مشاغل حساس بودند گسترش داد. از یک طرف این قانون به‌سرعت مبارزه با جاسوسی منجر شد و از طرف دیگر با این کار، کارمندان شاغل در جایگاه‌های حساس که به اطلاعات محرمانه دسترسی دارند، نیازمند ارائه گزارش‌های وقت‌گیر نخواهند بود و نظارت دولت بر طرح‌های ضد جاسوسی بهبود پیدا می‌کند.

بخش ۶۰۱ قانون مجوز جاسوسی سال مالی ۱۹۹۶:[3] پلیس فدرال در این قانون به سوابقی که طبق قانون گزارش منصفانه اعتبار گردآوری شده بودند دسترسی پیدا کرده است. شرایطی که این اداره طبق آن به سوابق دسترسی پیدا می‌کند مانند دسترسی نهادهای مالی به این سوابق است. طبق این قانون باید ریاست سازمان پلیس فدرال یا یک مقام منصوب او آن را صادر کند و رؤسای بخش‌های دیگر سازمان پلیس فدرال نمی‌توانند نامه امنیت ملی را صادر کنند. مقام ذی‌صلاح نیز فقط درصورتی که درخواست نامه امنیت ملی برای مبارزه با تروریسم و فعالیت‌های جاسوسی مخفیانه باشد می‌تواند آن را تأیید کند.

قانون میهن‌پرستی ایالات متحده آمریکا ۲۰۰۱:[4] این قانون سه مورد از قوانین نامه امنیت ملی قبلی (قانون حریم خصوصی ارتباطات الکترونیکی بخش (U.S.C. 2709 18)، قانون حق حریم خصوصی مالی بخش ((U.S.C. 3414(a)(5 12)) و قانون گزارش منصفانه اعتبار بخش (U.S.C. 1681u 15)) را اصلاح کرد و مورد پنجمی نیز ایجاد کرد. به‌بیان‌دیگر در این قانون این موارد تغییر کرد:

- اختیار انتشار نامه‌های امنیت ملی را از مرکز پلیس فدرال به رؤسای دفاتر منطقه‌ای این اداره بسط داد.
- الزام اینکه سوابق اطلاعاتی لزوماً متعلق به یک قدرت خارجی یا کارگزار قدرت خارجی باشد را پایان داد.
- به‌جای آن تأکید کرد که نامه امنیت ملی باید با تحقیقات برای حفاظت در مقابل تروریسم بین‌المللی یا جاسوسی خارجی باشد.
- هشدار قانونی اضافه کرد که هیچ‌کدام از این تحقیقات در مورد شهروندان آمریکا نمی‌توانند به استثنا قائل شدن در مورد فعالیت‌های حفاظت‌شده در متمم اول قانون اساسی (قسمت حقوق مدنی قانون اساسی این کشور مانند آزادی‌های فردی و محدوده مداخله و تصمیم دولت در این زمینه).

تغییر اساسی این قانون این بود که اختیار صدور نامه امنیت ملی را از پلیس فدرال این کشور به سایر دستگاه‌های درگیر در موضوع امنیت ملی بسط داد و آنها نیز می‌توانستند با رعایت این قانون، مستقل از پلیس فدرال نامه امنیت ملی صادر کنند.

در دو قانونی که کنگره ۱۰۹ ام، برای اصلاحیه قانون میهن‌پرستی صادر کرد اصلاحاتی وضع شد که عبارتند از:

- سازوکار اعمال قوانین و بازنگری قضایی برای درخواست‌ها و رعایت الزامات عدم افشا پیاده‌سازی شد.
- مجازات مشخصی برای عدم انطباق یا توجه به الزامات عدم افشا وضع شد.
- تصریح شد که الزامات عدم افشا درخواست نامه‌های امنیت ملی مانع از مشورت دریافت‌کننده نامه با وکیل نیست.
- فرایندی برای تسهیل الزامات عدم افشا وضع شد.
- نظارت کنگره افزایش پیدا کرد.
- ممیزی بازرس کل از نحوه استفاده از این اختیارات درخواست شد.

1. Electronic Communications Privacy Act of 1986
2. Intelligence Authorization Act for Fiscal Year 1995
3. Intelligence Authorization Act for Fiscal Year 1996
4. USA PATRIOT ACT Act of 2001: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

پیوست ۲. متن یک قانون برنامه توسعه‌ای آمریکا در زمینه حفاظت از داده‌ها

بخش ۵۲۲[1]

الف) هر نهاد فدرال باید یک مقام عالی حریم خصوصی داشته باشـــد که وظیفه اصلی او اعمال سیاست حفاظت از داده و حریم خصوصی باشد، شامل:

۱. تضمین حفظ و عدم کاهش حفاظت‌های حریم خصوصی هنگام استفاده از فناوری‌ها برای استفاده، گردآوری و افشای اطلاعات منجر به شناسایی.

۲. تضمین امکان نظارت مستمر بر انطباق با کردارها و سیاست‌های حریم خصوصی تدوین شده در مورد گردآوری، استفاده توزیع اطلاعات در عملیاتی‌سازی برنامه.

۳. تضمین انطباق کامل اطلاعات شخصی موجود در سوابق سامانه‌های قانونی حریم خصوصی با کردارهای اطلاعاتی منصفانه تعریف شده در قانون حریم خصوصی ۱۹۷۴.

۴. بررسی پیشنهاده‌های مقررات‌گذاری و قانونی شامل استفاده، افشای اطلاعات شخصی توسط دولت فدرال.

۵. تخمین اثر حریم خصوصی بر روی آیین‌نامه‌های[2] پیشنهاد شده توسط وزارتخانه‌ها شامل نوع اطلاعات منجر به شناسایی و تعداد افراد متأثر از آیین‌نامه.

۶. آماده‌سازی گزارش سالیانه برای ارائه به کنگره در مورد فعالیت‌های اثرگذار بر حریم خصوصی نهادها، شامل شکایت‌ها بابت نقض حریم خصوصی و اجرایی کردن بخش الف ۵۵۲.

۷. تضمین حفاظت از اطلاعات منجر به شناسایی در مقابل تخریب، اصلاح، اغتشاش، افشا، استفاده و دسترسی غیرمجاز ازسوی وزارتخانه.

۸. آموزش‌وپرورش کارمندان در زمینه سیاست‌های حفاظت از داده و حریم خصوصی برای اعتلای آگاهی و انطباق با سیاست‌های حفاظت از داده و حریم خصوصی.

۹. تضمین انطباق با سیاست‌های حفاظت از داده و حریم خصوصی وزارتخانه‌ها.

ب) تدوین سیاست‌ها و رویه‌های حفاظت از داده و حریم خصوصی:

عموماً - طی ۱۲ ماه از تصویب این قانون، هر نهادی باید رویه‌های حفاظت از داده و حریم خصوصی در مورد گردآوری، استفاده، اشتراک، افشا، انتقال، ذخیره‌سازی و امنیت اطلاعات منجر به شناسایی مربوط به عموم و کارمندان را تدوین و پیاده‌سازی کند. این رویه‌ها باید با رهنمودهای مقرراتی و قانونی، شامل مقررات دفتر مدیریت بودجه، قانون حریم خصوصی سال ۱۹۷۴ و بخش ۲۰۸ قانون دولت الکترونیکی سال ۲۰۰۲ سازگار باشند.

پ) ثبت - همه نهادها باید گزارشی مکتوب از استفاده خودشان از اطلاعات منجر به شناسایی همراه با رویه‌ها و سیاست‌های حفاظت از داده تهیه کنند و آن را نزد بازرس کل نهاد قرار دهند تا به‌عنوان معیار عملکرد نهاد مورد استفاده قرار بگیرد. هر گزارش باید توسط مقام عالی حریم خصوصی امضا شود تا تأیید کند که نهاد خواستار انطباق با رویه‌های ذکر شده در گزارش است. با امضای گزارش مقام حریم خصوصی تأیید می‌کند که اطلاعات منجر به شناسایی افراد تنها به‌صورتی که در گزارش تشریح شده استفاده می‌شود.

ت) ممیزی شخص ثالث بی‌طرف-

۱. عموماً- حداقل هر دو سال یک‌بار هر نهادی باید یک ممیزی شخص ثالث مستقل از استفاده از اطلاعات منجر به شناسایی در رویه‌های حفاظت از داده‌ها و حریم خصوصی نهاد به‌صورتی انجام بدهند که:

الف) صحت توصیف اطلاعات منجر به شناسایی را تعیین کند.

ب) مؤثر بودن رویه‌های حفاظت از داده‌ها را تعیین کنند.

پ) انطباق سیاست‌های حفاظت از داده‌ها و حریم خصوصی ابلاغ شده با قوانین و مقررات مرتبط با آنها را تضمین کنند.

---

1. Sec. 522. <<NOTE: 5 USC 552a note.>>

۲. Rule در قوانین آمریکا مصوبه وزارتخانه‌ها و با امضای رئیس‌جمهور و نهادهای اجرایی است که در قانون ایران، آیین‌نامه نامیده می‌شود.

ت) تضمین اینکه همه فناوری‌هایی که برای گردآوری، استفاده، ذخیره و افشای اطلاعات منجر به شناسایی افراد، نظارت مستمر انطباق با کردارها و سیاست‌های اعلام شده حاکم بر گردآوری، استفاده و توزیع اطلاعات در اجرای برنامه را ممکن می کنند.

۲. اهداف- هدف از ممیزی طبق این زیر بخش:

الف) تضمین صحت توصیف نهاد از نحوه استفاده از داده‌های منجر به شناسایی فرد و انطباق فناوری و رویه‌های جاری پردازش اطلاعات منجر به شناسایی آن.

ب) سنجش کردارهای حفاظت از داده‌های شخصی و حریم خصوصی براساس رویه‌های حفاظت از داده و حریم خصوصی.

پ) تضمین انطباق و سازگاری با سیاست‌های حفاظت از داده‌ها و حریم خصوصی اعلامی در حالت برخط و غیر برخط.

ت) آگاه‌سازی در مورد وضعیت جاری و پیشنهاد در مورد رویه‌های حفاظت از داده‌ها و حریم خصوصی است.

۳. الزامات ممیزی- بازرس کل هر نهاد باید با یک شخص ثالث مستقل (که رهبری شناخته شده در زمینه مشاوره حریم خصوصی، فناوری حریم خصوصی، گردآوری داده و مدیریت استفاده از داده و مسائل حریم خصوصی جهانی است) قراردادی منعقد کند که:

الف) استفاده سازمان از اطلاعات منجر به شناسایی را بسنجد؛

ب) رویه‌های حفاظت از داده و حریم خصوصی نهاد را بسنجد؛

پ) راهبردها و گام‌های مشخصی برای بهبود مدیریت حفاظت از داده و حریم خصوصی پیشنهاد بدهد.

۴. محتوا - هر ممیزی که طبق این زیر بخش انجام شود باید شامل:

الف) ممیزی فناوری‌ها، کردارها و رویه‌های هر نهاد در ارتباط با گردآوری، استفاده، اشتراک‌گذاری، افشا، انتقال و ذخیره‌سازی اطلاعات منجر به شناسایی.

ب) ممیزی از رویه‌های حفاظت از داده‌ها و حریم خصوصی اعلامی در ارتباط با گردآوری، استفاده، به اشتراک‌گذاری، افشا، انتقال و امنیت اطلاعات شخصی منجر به شناسایی.

پ) تحلیل تشریحی اینترنت، شبکه و وب‌گاه‌های نهاد برای آسیب‌پذیری‌های حریم خصوصی شامل:

۱. عدم انطباق با سیاست‌ها و رویه‌های حریم خصوصی اعلامی.

۲. مخاطرات انتشار ناخواسته اطلاعات در حالت قابل شناسایی از وب‌گاه نهاد.

ت) ممیزی انطباق عملکرد نهاد با این قانون.

ث) گزارش

۱. عموماً- به‌محض اتمام ممیزی، بازرس کل نهاد باید گزارشی تشـــریحی از ممیزی بدهد که شامل پیشنهاد بهبود یا پیشرفت مدیریت داده‌های منجر به شناسایی و رویه‌های حفاظت از داده و حریم خصوصی نهاد نیز بشود.

۲. دسترس‌پذیری اینترنتی- همه نهادها باید همه گزارش‌های شخص ثالث مستقل و گزارش‌های بازرس کل در ارتباط با آن گزارش‌ها را در دسترس عمومی قرار دهند.

ج) تعاریف - در این بخش تعریف اطلاعات منجر به شناسایی معادل تعریف قانون عمومی شماره ۱۰۷-۳۴۷، قانون دولت الکترونیکی سال ۲۰۰۲ تعیین می‌شود و به‌معنای هر نوع اطلاعاتی است که به‌صورت منطقی به‌صورت مستقیم یا غیرمستقیم از آن هویت شخص مرتبط با آن داده‌ها قابل استنتاج است.

منابع و مآخذ

[1] 0ico, “Some basic concepts,” 2023. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/some-basic-concepts/#:~:text=Data%20protection%20is%20about%20ensuring, purposes%2C%20you%20need%20to%20comply..

[2] 0H. Hijmans, “Privacy and Data Protection as Values of the EU That Matter, Also in the Information Society, ” در The European Union as Guardian of Internet Privacy, Springer, 2016, p. 40.

[3] 0S. P. Mulligan and C. D. Linebaugh, “Data Protection and Privacy Law: An Introduction, “ CRS, 2022.

[4] 0j. Mccain, “Applying The Privacy Act of 1974 to Data Brokers Contracting with the Government, “ Public Contract Law Journal, 2009.

[5] 0Edps, “The History of the General Data Protection Regulation,” 2022. [درون خطی]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[6] 0T. Zeller, “Breach Points Up Flaws in Privacy Laws,” 2005. [درون خطی]. Available: https://www.nytimes.com/2005/02/24/business/breach-points-up-flaws-in-privacy-laws.html.

[7] 0D. LAZARUS, “Column: Months after Equifax data breach, we’re still no closer to privacy protections,” 2018 . [Online]. Available: https://www.latimes.com/business/lazarus/la-fi-lazarus-cybersecurity-data-breaches-20180102-story.html.

[8] 0. M. Smith, J. Moteff and L. Kruger, “Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth, “ CRS, 2004.

[۹] مهدی فقیهی و محمدجواد جمشیدی. حفاظت از داده‌های کاربران: رویکردهای جهانی و گونه‌شناسی تنظیم مقررات، مرکز پژوهش‌های مجلس شورای اسلامی، تهران، ۱۳۹۷.

[10] 0senate, “A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes,” 2013.

[۱۱] ابوالقاسم رجبی. رایانش ابری، مرکز پژوهش‌های مجلس شورای اسلامی، تهران، ۱۳۹۰.

[12] 0Congress, “S.3300 - Data Protection Act of 2020,” 2020. [Online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/3300/text?q=%7B%22search%22%3A%5B%22data+protection%22%5D%7D&r=1&s=1.

گزیده سیاستی

حفاظت از داده‌ها باید بین هزینه توسعه سیستم‌های فناوری اطلاعاتی و رعایت مسئولیت کسب‌وکار و بخش دولتی نسبت به داده‌های شهروندان تعادل به‌وجود آورد.

مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاســـداران، روبروی پـــارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۵۸۵۵-۱۵۸۷۵ پست الکترونیک: mrc@majles.ir

وب‌سایت: rc@majles.ir