مسلسل: ۱۸۹۵۸
خرداد ۱۴۰۲

مرکز پژوهش‌های مجلس شورای اسلامی

دفتر مطالعات انرژی، صنعت و معدن

شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا شماره (۲): قانون اساسی، قوانین و مقررات فدرال و ایالتی

تاریخ انتشار:
۱۴۰۲/۳/۲

شماره مسلسل: ۱۸۹۵۸
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 شماره (۲): قانون اساسی، قوانین و مقررات فدرال و ایالتی

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

مدیر مطالعه:
سهیلا خردمندنیا

تهیه و تدوین:
ابوالقاسم رجبی

ناظران علمی:
محمدحسن معادی رودسری، حبیب‌اله ظفریان، سعید شجاعی

اظهارنظرکنندگان:
حسن پوراسماعیل، امین پژمان، سیدعلی محسنیان، محمدمهدی مهربان هلان، ایمان اکبری، عطیه یوسفی، حسین بشری خاوه

صفحه آرا:
نفیسه حاجی‌صفری

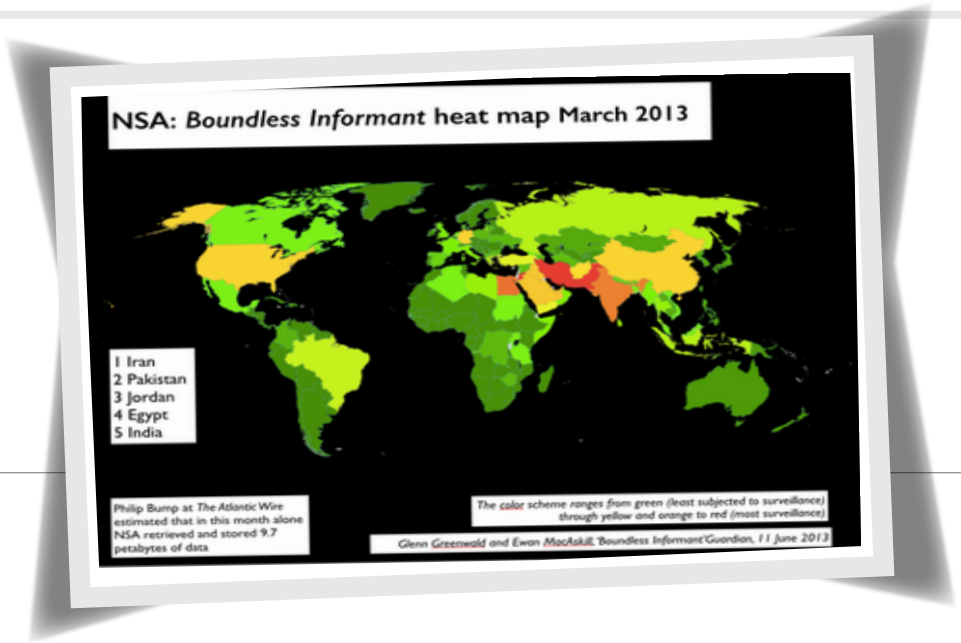
ویراستار ادبی:
سیده مرضیه موسوی راد

واژه‌های کلیدی:
۱. قانون حریم خصوصی ایالات متحده آمریکا
۲. الزامات اطلاع رسانی نشت اطلاعات
۳. حریم خصوصی اطفال
٤. حریم خصوصی وبگاه‌ها
۵. حریم خصوصی اطلاعات مکانی
٦. حریم خصوصی در قانون اساسی

دفتر مطالعات انرژی، صنعت و معدن

فهرست مطالب

فهرست جداول



شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا شماره (۲):

قانون اساسی، قوانین و مقررات فدرال و ایالتی

چکیده

هدف این گزارش شناسایی خلاءهای قانونی حفاظت ازحقوق داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا است. مطالعه حال حاضر نشان می‌دهد، قانون اساسی ایران در شناسایی حق حریم خصوصی از قانون اساسی آن کشور مترقی‌تر است. قوانین مصوب مجلس شورای اسلامی اصل حق حریم خصوصی را به‌نحو مناسبی به رسمیت شناخته‌اند، اما احقاق حقوق از نظر اجرایی با خلأهایی مواجه است. گرچه از نظر دایره شمول، قوانین کشور مانند قانون تجارت الکترونیکی بسیاری از جوانب یک قانون جامع حریم خصوصی را دارد، یعنی حق حریم خصوصی را به رسمیت می‌شناسد و نقض آن را جرم انگاری می‌کند، همینطور مصادیق اطلاعات حریم خصوصی در شیوه‌نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی مصوب سال ۸۹۳۱ مشخص شده است، اما قوانین کشور سازوکارهای اجرایی شایسته برای تحقق امر حفاظت از حریم خصوصی ندارد. مثلا، گرچه به شخص اختیار حذف داده پیام‌های شخصی‌اش داده می‌شود، اما سازوکار اعلام داده‌های در اختیار، شیوه درخواست و مهلت‌های قانونی پاک کردن داده شخصی تصریح نشده است. در نتیجه احکام حمایت از حقوق داده‌ها، از جنبه‌های مختلف قابلیت تحقق ندارد و تکلیف دلال‌های داده که بدون ارتباط کسب‌وکاری با شهروندان، اطلاعات آنها را گردآوری کرده و به فروش می‌رسانند، در قوانین کشور مشخص نشده است. تکلیف انواع خاص اطلاعات مانند اطلاعات کتابخانه‌ای، حفاظت‌های تخصصی از اطلاعات کودکان، نشت اطلاعات و سازوکارهای حمایت از حریم خصوصی استفاده‌کنندگان از خدمات اینترنت در قوانین کشور مسکوت هستند. لذا پیشنهاد می‌شود، سازوکارهای اجرایی برای تحقق حق حریم خصوصی در اصلاحیه قانون تجارت الکترونیکی یا تصویب قانون جدید مستقل انجام شود.

خلاصه مدیریتی

هدف از تدوین این گزارش شناسایی خلأهای قانونی حفاظت از حقوق داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا است. در قانون اساسی ایالات متحده آمریکا رعایت حریم خصوصی تصریح نشده، اما در اصل (۲۵) قانون اساسی جمهوری اسلامی بر حق حریم خصوصی تصریح شده است. در نتیجه **قانون اساسی ایران در شناسایی حق حریم خصوصی به‌مراتب از قانون اساسی ایالات متحده آمریکا مترقی‌تر است.** مقایسه قوانین جامع تصویب شده یا در آستانه تصویب ایالات کالیفرنیا، نیویورک، مریلند، ماساچوست، هاوایی و داکوتای شمالی با قانون تجارت الکترونیک ایران مصوب سال ۱۳۸۲ نیز نشان می‌دهد **در قوانین موضوعه مصوب مجلس شورای اسلامی نیز اصل حقوق مربوط به حریم خصوصی به‌صراحت به رسمیت شناخته شده** و حتی مجازات زندان برای تخلف در زمینه رعایت حقوق شخص موضوع داده وضع شده است، اما **در قوانین ایران این مشکلات وجود دارند:**

- **موضوع حریم خصوصی از جنبه شیوه احقاق حقوق و ضوابطی که با اجرای آنها فرد می‌تواند نسبت به احقاق حقوق خود اقدام کند روشن نشده است.**
- درحالی که تکالیفی برای نگهداری و حفظ برخی از اقلام داده‌ای از سوی برخی کسب‌وکارها و عرضه‌کنندگان خدمات فناوری اطلاعات وضع شده، در زمینه حفاظت از این داده‌ها و شیوه استفاده از این داده‌ها ضوابط مشخصی وضع نشده است. برای نمونه طبق تکلیف مواد (۳۲) و (۳۳) قانون جرائم رایانه‌ای **ارائه دهندگان خدمات مربوطه موظفند داده‌های ترافیکی را حداقل شش‌ماه و داده های ذخیره سازی را حداقل پانزده روز پس از خاتمه خدمت نگهداری کنند، اما بازه زمانی که داده‌ها باید قابلیت حذف یا امحا داشته باشند یا ملاحظات حریم خصوصی و حقوق داده‌های اشخاص موضوع این داده‌ها نیز تصریح نشده‌اند.** گرچه به‌نظر می‌رسد احکام حریم خصوصی قانون تجارت الکترونیکی در این حوزه قابل اعمال باشند.
- **برای ساماندهی به پدیده دلال‌های داده یعنی کسانی که بدون مراورده مستقیم کسب‌وکاری با اشخاص داده‌هایی در مورد آنها در اختیار دارند و این داده‌ها را به فروش می‌رسانند قوانین کافی وجود ندارد** و کسب‌وکارهای متعددی درحال گردآوری اطلاعات شهروندان در شبکه‌های اجتماعی مختلف هستند و الزام قانونی هم به افشای اطلاعات به اشخاص موضوع داده ازسوی این کسب‌وکارها وجود ندارد.
- **قوانین کسب‌وکارها را به ایجاد یک امکان مشخص برای درخواست پاک کردن اطلاعات شخصی افراد بکند، ملزم نکرده‌اند.**
- **فروش اطلاعات شخصی سامان دهی نشده است**
- **حمایت‌های حقوقی بیشتر از حریم خصوصی کودکان وجود ندارد.**
- حریم خصوصی مطالعه منابع الکترونیکی مقرراتگذاری نشده است.
- تکالیف کسب‌وکارها در زمینه اطلاع‌رسانی در مورد شیوه مدیریت داده‌های شخصی مدون نشده است.
- حریم خصوصی در رابطه کارگر و کارفرما تدوین نشده است.
- **کسب‌وکارها ملزم به اطلاع‌رسانی پیرامون نشت اطلاعات نیستند.**

در توسعه قوانین حمایت از حقوق داده‌ها و رفع خلأهای قانونی ملاحظاتی همچون، **مشخص کردن جامعه هدف، لزوم ساماندهی دلال‌های داده، ضرورت در نظر گرفتن حساسیت اطلاعات کتابخانه‌ای، منع استفاده از اطلاعات کودکان برای تبلیغات، ساماندهی نشت اطلاعات، تکلیف به ایجاد قابلیت نرم‌افزاری داخل نرم‌افزارهای برخط برای درخواست دسترسی و پاک شدن اطلاعات، ضرورت بازنگری و تقویت قانون تجارت الکترونیکی مصوب ۱۳۸۲** و انجام مطالعات مروری بیشتر در زمینه صیانت از حقوق داده‌ها پیشنهاد می‌شود.

مقدمه

حریم خصوصی و حفاظت از داده دو موضوع مرتبط با یکدیگر در حکمرانی اینترنت هستند. در منابعی که به تمایز این دو مفهوم اعتقاد دارند، حفاظت از داده‌ها را سازوکار حقوقی می‌دانند که حریم خصوصی را تضمین می‌کند. حریم خصوصی نیز معمولاً حق شهروندان در کنترل اطلاعات شخصی آنها و تصمیم در مورد (افشا یا عدم افشا) آن هستند [۱]. به بیان دیگر حریم خصوصی داده تعریف می‌کند که چه کسی به داده دسترسی داشته باشد درحالی که حفاظت از داده ابزارها و سیاست‌هایی برای محدودکردن بالفعل دسترسی به داده‌ها وضع می‌کند. [۲] گرچه منابع معتبر دانشگاهی تمایز میان حریم خصوصی و حفاظت از داده‌ها را تمایزی با منشأ اروپایی می‌دانند. [۳] یعنی در مطالعات تطبیقی قوانین کشورها مرز میان حفاظت از داده و حریم خصوصی داده‌ها کم‌رنگ می‌شود [۴] و اصولاً حریم خصوصی و حفاظت از داده‌ها در احکام قانونی تفکیک‌پذیر نیستند. زیرا حکم حقوقی که در زمینه حفاظت از داده‌ها تدوین می‌شود، اصولاً ضوابط رعایت حریم خصوصی را تعیین می‌کند. این گزارش نیز در بررسی احکام قانونی تمایزی میان قوانین حریم خصوصی داده و حفاظت از داده‌ها قائل نیست و در نتیجه میان قوانین حفاظت از داده و حریم خصوصی داده‌ها تمایزی اعمال نشده است. واقعه رخنه سایبری در اطلاعات شرکت اعتباری اکوئیفاکس در سال ۲۰۱۷ که در آن اطلاعات ۲۴۱ میلیون شهروند ایالات متحده آمریکا از طرف هکرها به‌دلیل عدم توجه این شرکت به رعایت مبانی اولیه امنیت سایبری به سرقت رفت و در ادامه کوتاهی این شرکت در اطلاع‌رسانی واقعه به افرادی که تحت تأثیر قرار گرفته بودند، یکی از نقاط عطف در تاریخ مقرراتگذاری این کشور در حوزه حفاظت از داده‌ها به‌شمار می‌رود. پس از این واقعه نمایندگان حزب دموکرات چندین تلاش برای مقرراتگذاری عام صیانت از داده‌ها انجام دادند که تاکنون با توجه به عدم همراهی جناح جمهوری‌خواه که مقررات صیانت از داده را به‌نوعی مقرراتگذاری دست‌وپاگیر تلقی می‌کند به نتیجه نرسیده است [۵]. لذا ایالت‌های مختلف آمریکا به‌صورت مجزا مقرراتگذاری حریم خصوصی را به‌صورت جامع در دستور کار قرار دادند، اما احکام مربوط به صیانت از داده‌ها و حریم خصوصی در بخش عمومی و حقوق شهروندان را می‌توان در قانون اساسی ایالات متحده آمریکا، قانون اساسی ایالت‌ها و قوانین مصوب کنگره و قوانین ایالتی دنبال کرد. در این گزارش ضمن معرفی هرکدام از قوانین ایالتی این کشور درصورتی که مصوبه قانونی مشابه قوانین این کشور موجود باشد، معرفی می‌شود.

احکام حریم خصوصی و صیانت از داده در قانون اساسی ایالات متحده آمریکا در مقایسه با قانون اساسی جمهوری اسلامی ایران

قانون اساسی آمریکا شامل هفت اصل است که شیوه عملکرد دولت این کشور را تشریح می‌کند. این قانون شامل ۲۷ متمم است. نظام قضایی ایالات متحده آمریکا در بخش فدرال توانایی تفسیر قانون اساسی و اختیار لغو مصوبات کنگره مغایر با قانون اساسی را دارد. در قانون اساسی ایالات متحده آمریکا و متمم‌های آن احکامی که به‌صراحت حریم خصوصی را به‌عنوان یک حق به رسمیت بشناسد وجود ندارد، اما در نظام قضایی کامن لا ایالات متحده آمریکا در سایه احکام و استنتاجات قضات دیوان‌عالی این کشور حق حریم خصوصی استنتاج شده است. در صدور احکام مقالات حقوقی نیز مد نظر قضات قرار می‌گیرند. از جمله مهم‌ترین مقاله‌هایی که مورد استناد قضایی قرار گرفته‌اند عبارتند از [۶]:

■ **مقاله حق حریم خصوصی (حق تنها گذاشته شده بودن)** [۷]: که مقاله مروری حقوقی است که در سال ۱۸۹۰ در مجله حقوق هاروارد منتشر شد. این مقاله که توسط دو قاضی نوشته شده است یکی از تأثیرگذارترین مقاله‌ها در تاریخ حقوقی ایالات متحده آمریکا و اولین مقاله در دفاع از حق حریم خصوصی به‌شمار می‌رود. نویسندگان در این مقاله به اخذ و انتشار تصاویر آنی از سوی صنعت روزنامه انتقاد می‌کنند و به آنها اتهام وارد می‌کنند که به زندگی شخصی و حریم خصوصی افراد تجاوز می‌کنند و در مورد کفایت نظام حقوقی برای رسیدگی به این موضوع سوال وارد می‌کنند.

■ **مقاله شبه‌جرم‌های حریم خصوصی** [۸] در این مقاله نویسنده چهار قصور در زمینه نقض حریم شخصی که شخص می‌تواند از مرتکب بابت آنها شکایت و درخواست غرامت کند بیان کرده است. این کوتاهی‌ها عبارتند از:

- ورود بی‌اجازه به‌تنهایی یا عزلت، یا امور شخصی.[1]
- افشای عمومی حقایق خجالت‌آور شخصی.
- معروف‌سازی که شخص را به‌صورت غلطی در نظر عموم بیاورد.[2]
- تصاحب و تملک نام یا شباهت یک فرد.[3]

این دو مقاله در احکام قضایی دیوان‌عالی در زمینه حریم خصوصی مورد استناد قرار گرفتند. در زیر چند نمونه از احکام قضایی مهم در زمینه حریم خصوصی ذکر شده است:

■ **مورد قضایی گریزولد در برابر کنتیکت در سال ۱۹۶۵**: در این حکم دیوان‌عالی این کشور تشخیص داد که در حفاظت‌های فردی که در متمم‌های ۱، ۳، ۴ و ۹ بیان شده‌اند، حق ضمنی حریم خصوصی در قانون اساسی این کشور وجود دارد.

■ **مورد قضایی کاتز در برابر ایالات متحده آمریکا در سال ۱۹۶۷**: دیوان‌عالی این کشور حفاظت‌های متمم چهارم حامی حریم خصوصی در مقابل بازجویی و توقیف غیرقانونی خانه‌ها و املاک شهروندان را به هر جایی که شخص انتظار منطقی حریم خصوصی[4] داشته باشد تسری داده است.

■ **مورد قضایی آیزن‌اشتات در برابر بیرد در سال ۱۹۷۲**: حق حریم خصوصی توسط دیوان‌عالی این کشور از یک حق مربوط به خانواده‌ها به‌عنوان حق فردی به رسمیت شناخته شد و در حکم رو در برابر وید[5] با استناد به متمم چهاردهم قانون اساسی این حق را در مورد زنان نیز تسری داد.[6] [۹]

در قانون اساسی جمهوری اسلامی ایران قانونگذار در زمینه صیانت از داده صراحت دارد، یعنی حریم خصوصی حقی نیست که نیازمند تفسیر قانون باشد. بعضی از اصول مرتبط با حریم خصوصی در قانون اساسی جمهوری اسلامی ایران در ادامه ذکر شده است:

اصل بیست و دوم

حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند.

اصل بیست و سوم

تفتیش عقاید ممنوع است و هیچ‌کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مؤاخذه قرار داد.

اصل بیست و پنجم

بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون.

همان‌طور که مشاهده می‌شود در اصل بیست و پنجم قانون اساسی جمهوری اسلامی ایران به‌صراحت تأکید شده که استراق سمع و هرگونه تجسس ممنوع است. در نتیجه قانون اساسی ایران صراحت بیشتری در

1. Intrusion Upon Seclusion or Solitude, or into Private Affairs.
2. Publicity which Places a person in a false light in the public eye.
3. Appropriation of one's name or likeness.
4. reasonable expectation of privacy
5. Roe v. Wade,

۶. این احکام عموماً در مورد دعواهای پیشگیری از بارداری و سقط جنین هستند و حق بودن حریم خصوصی ضمن احکام نتایج دادگاه استنتاج شده و زمینه سقط جنین به دعواهای بین جمهوری‌خواهان و دموکرات‌ها در زمینه حریم خصوصی نیز بسط پیدا کرده است.

حقوق شخصی افراد دارد و شـــواهد تاریخی مانند استفاده از داده‌های سرشماری برای هدف کنترل اتباع دارای اصل و نسب ژاپنی در جنگ جهانی دوم و افشاگری‌های اخیر ادوارد اسنودن[1] در دهه اخیر نیز نشان می‌دهد که دولت ایران نسبت به ایالات متحده آمریکا در زمینه رعایت حقوق شهروندان در زمینه حفاظت از داده‌ها به‌مراتب پیشگام‌تر است. فرمان هشت‌ماده‌ای امام خمینی (ره) درباره حقوق مردم در تاریخ ۲۴ شهریورماه ســـال ۱۳۶۱ و تکلیف مقام معظم رهبری در حکم انتصاب اعضای شورای عالی فضای مجازی بر «حفظ حریم خصوصی آحاد جامعه و مقابله مؤثر با نفوذ و دست‌اندازی بیگانگان در این عرصه» نشان می‌دهد که حریم خصوصی در جمهوری اسلامی ایران بیشتر از آمریکا در قوانین و سیاست‌های کلان مورد تأکید می‌باشد و در عمل نیز نظام جمهوری اسلامی ایران راساً نسبت به نقض حریم خصوصی شهروندان خود اقدام نکرده است. گرچه حکم مقام معظم رهبری در زمینه لزوم مقابله با نفوذ و دست‌اندازی بیگانگان در زمینه حریم خصوصی نشان می‌دهد که کشور باید در این زمینه اقدام‌های بیشتری را انجام و جوانب فنی رعایت حریم خصوصی را توسعه دهد. در ایران انطباق مصوبات دستگاه‌های اجرایی با قانون اساسی توسط دیوان‌عالی کشـــور انجام می‌شود. بعضی احکام دیوان‌عالی کشور در زمینه حریم خصوصی در زیر آمده است:

رأی شماره ۴۹۰ هیئت عمومی دیوان عدالت اداری با موضوع ابطال تبصره ماده (۷) آیین‌نامه اجرایی تبصره «۴» ماده (۱۸۱) قانون مالیات‌های مســـتقیم مصوب وزرای دادگستری و امور اقتصادی و دارایی: در این رأی دیوان عدالت اداری در پاسخ به شکایتی که به اصل (۲۵) قانون اساسی استناد کرده بود، مصوبه وزرای دادگستری و امور اقتصادی و دارایی را به‌دلیل اینکه برای بازرسی از محل کار و سایر مکان‌هایی غیر از منزل مسکونی اخذ اجازه قضایی را لازم نمی‌دانستند، به‌دلیل عدم انطباق با این اصل قانون اساسی لغو کرد.

احکام حریم خصوصی در قوانین فدرال ایالات متحده آمریکا در مقایسه با مقررات اجرایی ایران

مقررات فدرال حریم خصوصی به دو دســـته مقررات مربوط به بخش دولتی و مقررات مربوط به بخش خصوصی قابل تقسیم هستند. مقررات بخش دولتی در قالب دستورات اجرایی ابلاغ می‌شوند و وزارت امنیت میهنی در این زمینه مسئولیت دارد. مقررات فدرال حریم خصوصی در قلمرو کنش کمیسیون تجارت فدرال است. در ادامه ابتدا مقررات حریم خصوصی در بخش دولتی بیان و سپس مقررات مربوط به فعالیت بخش خصوصی عرضه می‌شود.

مقررات فدرال حریم خصوصی در بخش دولتی

بخش مهمی از دستورات مربوط به حریم خصوصی در دستور اجرایی ریاست جمهوری این کشور منتشر شده‌اند. در زیر بعضی از دستورات اجرایی مهم ذکر شده‌اند:

دســـتور اجرایی ۱۳۶۳۶ بـــا عنوان بهبود امنیت ســـایبری زیرساخت‌های حیاتی و رهنمود سیاست ریاست جمهوری یا تاب‌آوری و امنیت زیرساخت‌های کلیدی مورخ ۱۲ فوریه سال ۲۰۱۳: نهادهای فدرال را ملزم می‌کند که مشـــارکت در یک چارچوب امنیت سایبری خنثی نسبت به فناوری را تشویق و توسعه دهند. حجم و وقت‌شناسی و کیفیت اشتراک‌گذاری اطلاعات تهدیدات سایبری با بخش خصوصی را نیز افزایش دهند. از این نظر احتمالاً بخشی از اقدامات این کشـــور برای کاهش سطح تهدیدات ســـایبری، اشتراک اطلاعات تهدیدات با بخش خصوصی است. مقامات عالی باید ارزیابی‌های خود را به دفتر آزادی‌های مدنی و حقوق مدنی و دفتر حریم خصوصی وزارت امنیت میهنی جهت درج در گزارش سالیانه تحلیل آزادی‌های مدنی و حریم خصوصی سالیانه ارائه کنند.

دستور اجرایی ۱۳۶۹۱ با عنوان بهبود اشتراک اطلاعات امنیت سایبری با بخش خصوصی مورخ ۱۳ فوریه سال ۲۰۱۵: این مصوبه بر لزوم نقش‌آفرینی بیشـــتر در اشـــتراک اطلاعات مرتبط با امنیت و سوانح سایبری برای دفاع جمعی این کشـــور تأکید بیشتری دارد. این دستور اجرایی، شکل‌گیری ســـازمان‌های اشتراک این قبیل اطلاعات را تشویق و ســـازوکارهای بهبود توانمندی‌های آنها را فراهم می‌آورد و آنها را قادر می‌سازد که براساس یک سازوکار داوطلبانه با دولت فدرال شراکت داشته باشند. بخش ۵ هر دو دستور اجرایی آژانس‌های فدرال را موظف می‌کند که با مقامات متناظر عالی بالادســـتی خود در حریم خصوصی و آزادی مدنی همکاری داشته باشـــند تا از حفاظت مناسب از حریم خصوصی و آزادی‌های مدنی در فعالیت‌های این دســـتورات اجرایی اطمینان حاصل کنند. مقامات عالی ملزم می‌شوند که اقدامات دستگاه‌های تحت نظر خود را از نظر رعایت حریم خصوصی و آزادی‌های مدنی ارزیابی و سالیانه گزارش دهند و نیز باید ارزیابی‌های خود را به دفتر آزادی‌های مدنی و حقوق مدنـــی و دفتر حریم خصوصی وزارت امنیت میهنی برای درج در گزارش ســـالیانه تحلیل آزادی‌های مدنی و حریم خصوصی ارائه کنند.

1. Edward Snowden

دستور اجرایی ۱۳۸۷۳ با عنوان ایمن‌سازی زنجیره ارزش خدمات و فناوری‌های ارتباطات و اطلاعات مورخ ماه می سال ۲۰۱۹[1] [۱۰]: به دستگاه‌های اجرایی اختیار می‌دهد که علیه فعالیت، خدمات یا فناوری ارتباطی و اطلاعاتی[2] که توسط اشخاصی توسعه‌یافته، تولید یا تأمین شده‌اند که توسط دشمن خارجی کنترل می‌شوند یا تحت قلمرو حقوقی کشور متخاصم خارجی قرار می‌گیرند، تحریم‌هایی وضع کنند. کشورهای متخاصم شامل ایران و چین نیز می‌شوند.

دستور اجرایی ۱۴۰۳۴ با عنوان حفاظت از داده‌های شخصی آمریکایی‌ها از دشمنان خارجی [۱۱]: پیرو اجرای دستور اجرایی ۱۳۸۷۳ محدودیت‌هایی برای رسانه اجتماعی چینی تیک‌تاک در دستور اجرایی ۱۳۹۴۲، پیام‌رسان وی‌چت در دستور اجرایی ۱۳۹۴۳، برنامه‌های کاربردی و دیگر نرم‌افزارهای توسعه‌یافته توسط شرکت‌های چینی در دستور اجرایی ۱۳۹۷۱ وضع گردید که البته این دستور اجرایی توسط دولت بایدن معلق شد، اما وزیر تجارت موظف شد با همکاری نهادهای امنیتی، دفاعی و بهداشتی ظرف مدت ۱۲۰ روز گزارشی حاوی پیشنهادهایی برای حفاظت در مقابل فروش بدون محدودیت، انتقال یا دسترسی به اطلاعات حساس اشخاص آمریکایی (شامل اطلاعاتی که منجر به شناسایی شخص می‌شوند، اطلاعات مربوط به سلامت و ژنتیک) به مشاور امنیت ملی ریاست‌جمهور ارائه دهد. این گزارش باید آسیب‌های ناشی از دسترسی انباره‌های بزرگ داده توسط اشخاصی که متعلق به کشورهای متخاصم هستند یا تابع قوانین یا تحت هدایت این کشورها را پوشش دهد. وزارت امنیت میهنی این کشور ظرف مدت ۶۰ روز باید گزارشی از آسیب‌پذیری‌ها ارائه دهد و اداره‌کننده اطلاعات ملی نیز باید گزارشی از تخمین تهدیدها بدهد.

مقررات فدرال بخش خصوصی

کمیسیون تجارت فدرال تاکنون گزارش‌هایی در زمینه کردارهای دلال‌های داده و کردارهای به‌روزرسانی امنیت تلفن همراه منتشر کرده است. [۱۲]. طبق ارزیابی مرکز مطالعات بین‌المللی بلفر[3]، [۱۳] کمیسیون تجارت فدرال نهاد اصلی حمایت از مصرف‌کننده است و هم‌اکنون بعضی از جنبه‌های حریم خصوصی را اعمال قانون می‌کند. کمیسیون تجارت فدرال براساس تکلیف قانونی خود در حمایت از مشتریان می‌تواند در زمینه صیانت از داده‌های مشتریان مصوباتی داشته باشد، اما اگر مصوبات این کمیسیون توسط کنگره لغو شود، اختیارات قانونگذاری در زمینه حریم خصوصی را از دست خواهد داد و تا تصویب قانونی که به‌صراحت این تکالیف را به این نهاد بسپارد، هیچ اختیاری در این زمینه نخواهد داشت. در عین حال دادگاه عالی نیز می‌تواند در صورت شکایت بخش خصوصی مصوبات این نهاد را لغو کند. این عوامل موجب شده که کمیسیون تجارت قدرال در زمینه حریم خصوصی در حدی که انتظار می‌رود فعالیت نداشته باشد.

حریم خصوصی در مصوبات شوراها و هیئت وزیران قوه مجریه جمهوری اسلامی ایران

در چارچوب قوانین موضوعه مصوب مجلس شورای اسلامی، حریم خصوصی در مصوبات هیئت وزیران و شوراهای ذکر شده در قوانین قابلیت مقرراتگذاری دارد. از جمله در بند «ج» ماده (۷۹) قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ ذخیره، پردازش و یا توزیع «داده پیام»های مربوط به سوابق پزشکی و بهداشتی باید ازسوی وزارت بهداشت با همکاری سازمان مدیریت و برنامه‌ریزی کشور پیشنهاد و در هیئت وزیران مصوب شود که البته هنوز پس از ۱۹ سال انجام نشده است. ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات مصوب سال ۱۳۸۷ کمیسیون انتشار و دسترسی آزاد به اطلاعات را تشکیل داد. تبصره «۲» ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات مصوب سال ۱۳۸۷ مقرر کرد که مصوبات این کمیسیون پس از تأیید رئیس‌جمهور لازم‌الاجراست. براساس اختیارات این ماده این کمیسیون، شیوه‌نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی را در سال ۱۳۹۸ منتشر کرد. این شیوه‌نامه در (۲۳) ماده مصادیق اطلاعات شخصی را تدوین کرده است. در آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب سال ۱۳۹۳ نیز بخشی از تکالیف مربوط به حفاظت از داده‌ها در فرایندهای قضایی تشریح شده است.

1. Securing the Information and Communications Technology and Services Supply Chain.
2.Information and Communications Technology or Services.
3. Belfer Center for Science and International Affairs, Harvard Kennedy School.

احکام حریم خصوصی در قوانین ایالتی ایالات متحده آمریکا در مقایسه با قوانین مصوب مجلس ایران

قوانین ایالتی ایالات متحده آمریکا نیز در دادگاه‌های عالی و قوانین ایالتی جنبه‌های مختلف موضوع صیانت از داده را توسعه داده‌اند. هر ۵۰ ایالت آمریکا قوانینی در جنبه‌های مختلف حریم خصوصی به تصویب رسانده‌اند که البته پس از سال ۲۰۱۷ قانونگذاری ایالتی در زمینه حریم خصوصی رونق بیشتری گرفته است. کنفرانس ملی قانونگذاران ایالاتی ایالات متحده آمریکا، قوانین حریم خصوصی دیجیتال[1] ایالات را به قوانین حریم داده مصرف‌کننده جامع، سیاست‌های حریم‌خصوصی وب‌گاه‌ها، حریم‌خصوصی بارگیری و مطالعه کتاب، بازاریابی برخط محصولات مشخص برای اطفال و نظارت بر ایمیل‌های کارمندان طبقه‌بندی کرده است. [۱۴]

همچنین این نهاد، قوانین مربوط به اطلاع‌رسانی نشست اطلاعات شخصی را به‌طور جداگانه تحلیل و ازسویی دیگر سایر انواع قوانین ایالتی که به موضوع حریم خصوصی می‌پردازند را نیز در دسته حریم خصوصی فعالیت‌های برخط طبقه‌بندی کرده است.

قوانین حریم خصوصی مصرف‌کننده جامع ایالتی و مقایسه با قانون تجارت الکترونیکی ایران

پنج ایالت کالیفرنیا، کلرادو، کنتیکت، یوتا و ویرجینیا قوانین جامع حریم خصوصی مصرف‌کننده تصویب کرده‌اند. چندین گزاره مشترک این قوانین شامل حق دسترسی و پاک کردن اطلاعات شخصی و حق خروج‌گزینی (Opt-out) یا تصمیم به خروج از قرارداد فروش اطلاعات شخصی می‌شود. سایر تدابیر وب‌گاه‌های تجاری و ارائه‌دهندگان خدمات برخط را ملزم می‌کند که نوع اطلاعات شخصی که گردآوری می‌شود، اطلاعاتی که با دیگران به اشتراک گذاشته می‌شود و شیوه‌های تقاضای تغییر در اطلاعات مشخص ازسوی مصرف‌کنندگان را طی یک متن سیاست حریم خصوصی در محل مناسب ارسال کنند.

کالیفرنیا

قانون حریم خصوصی مصرف‌کننده کالیفرنیا سال ۲۰۱۸[2]

این قانون به مصرف‌کنندگان حق می‌دهد که از کسب‌وکار، انواع و تکه‌های مشخص اطلاعات شخصی که ذخیره کرده را مطالبه کند و همچنین کسب و کار باید منبع این اطلاعات و مقاصد کسب‌وکاری گردآوری اطلاعات را افشا کنند. این قانون تعیین می‌کند که مشتریان حق دارند از کسب‌وکارها بخواهند که اطلاعات شخصی که در مورد مصرف‌کننده گردآوری کرده‌اند را پاک کند و حکم می‌دهد که مصرف‌کنندگان حق دارند که حتی پس از انعقاد معامله در مورد فروش اطلاعات خصوصی خودشان، فروش اطلاعات را ملغی کنند و کسب‌وکار نمی‌تواند تبعیضی علیه این مصرف‌کننده اعمال کند. این قانون برای تمامی ساکنین کالیفرنیا اعمال می‌شود.

قانون حقوق حریم خصوصی مصرف‌کننده کالیفرنیا سال ۲۰۲۰[3] این قانون: ۱. قوانین حریم خصوصی داده مصرف‌کننده را گسترش می‌دهد و به مصرف‌کنندگان اجازه می‌دهد که کسب‌وکار را از اشتراک اطلاعات شخصی منع کنند، ۲. اطلاعات شخصی غلط را تصحیح کند. ۳. استفاده کسب‌وکار از اطلاعات شخصی حساس (شامل مکان جغرافیایی دقیق، نژاد، قومیت، مذهب، داده‌های ژنتیک، ارتباطات شخصی، گرایش‌های جنسی و اطلاعات سلامتی خاص) را ممنوع کند. آژانس حفاظت از حریم خصوصی کالیفرنیا را برای تقویت بیشتر و پیاده‌سازی و اعمال قوانین حریم خصوصی و وضع جریمه تأسیس می‌کند. شرایط کسب‌وکارهایی که مشمول این قوانین هستند را تغییر می‌دهد، کسب‌وکارها را از نگهداری اطلاعات شخصی بیش از مقدار ضرورت منطقی منع می‌کند، مجازات‌های مربوط به نقض قانون را در مورد مصرف‌کنندگان زیر ۱۶ سال سن سه برابر می‌کند و اعمال مجازات‌های مدنی برای سرقت اطلاعات ورود به حساب کاربری مصرف‌کنندگان را به شیوه مشخص مجاز می‌کند.

کلرادو

قانون حریم خصوصی کلرادو: این قانون در قوانین حمایت از مصرف‌کننده این ایالت وضع می‌شود. حقوق مصرف‌کننده در زمینه حریم خصوصی، تکالیف شرکت‌ها در حفاظت از داده شخصی و مجاز کردن دادستان کل و دادستان‌های مناطق برای اقدامات اعمال قانون ازجمله موضوعاتی است که در این قانون به آنها پرداخته می‌شود. این قانون، چندین اصطلاح در زمینه کسب‌وکارهای مشمول قانون، مصرف‌کنندگان و داده را داراست. برای مثال اصطلاح «کنترل‌کننده» شخص یا گروهی از اشخاص هستند که تعیین می‌کند، داده چگونه استفاده و پردازش شود؟ یا «مصرف‌کننده» افراد ساکن در کلورادو، در بافت خانوار یا به‌صورت فردی هستند که شامل کارمندان یا افراد متقاضی کار درگیر رابطه کاری نمی‌شوند. این قانون از سال ۲۰۲۳ اجرایی خواهد شد.

1 .Digital Privacy.
2 .California Consumer Privacy Act of 2018 (CCPA).
3 .California Consumer Privacy Rights Act (CPRA).

کنتیکت

قانون حریم خصوصی و نظارت برخط ســـال ۲۰۲۲ [1] این قانون چارچوبـــی برای کنتـــرل و پردازش داده‌های شـــخصی مشـــخص می‌کند، وظایف و اســـتانداردهای صیانت از حریـــم خصوصی را در مورد کنترل‌کنندگان و پردازش‌کنندگان داده مشخص می‌کند و به مصرف‌کنندگان حق دسترسی، تصحیح، پاک‌کردن، کسب یک نسخه از داده‌های شخصی و خروج از قرار داد پردازش داده‌های شخصی را اعطا می‌کند. سال جرای این قانون ۲۰۲۳ تعیین شد.

یوتا

قانون حریـــم خصوصی مصرف‌کننده یوتا ســـال ۲۰۲۲ [2] این قانون برای مصرف‌کننـــدگان این حق را به‌وجود مـــی‌آورد که بدانند کسب‌وکار چه اطلاعاتی جمع می‌کند؟ کســـب‌وکار از داده‌ها چگونه استفاده می‌کند؟ و آیا اطلاعات شخصی را می‌فروشد یا خیر؟ این قانون همچنین این حق را برای مصرف‌کننده به‌وجود می‌آورد که به داده‌های گردآوری شده دسترسی داشته و اطلاعات شخصی که کسب‌وکار نگه می‌دارد را پاک کند و از قرارداد گردآوری و استفاده از داده‌های شخصی خارج شـــود. همچنین این قانون بعضی کســـب‌وکارهای مشخص را مکلف می‌کند که از داده‌های شخصی کاربران حفاظت کنند، اطلاعات شفافی پیرامون شیوه استفاده از داده‌های شخصی دهند و درخواست مصرف‌کننده برای دسترســـی، پاک کردن یا توقـــف فروش اطلاعات شخصی را بپذیرند. قانون به دادستان کل این اختیار را می‌دهد که اقدام اجرایی اتخاذ و جریمه وضع کند. تاریخ اجرایی شـــدن این قانون ۳۱ دسامبر سال ۲۰۲۳ تعیین شد.

ویرجینیا

قانون حفاظت از داده مصرف‌کننده ۲۰۲۱ [3] این قانون چارچوبی برای کنترل و پردازش داده شـــخصی در مشـــترک‌المنافع ویرجینیا تدوین می‌کند. قانون به همه اشـــخاصی که در این مشـــترک‌المنافع کسب‌وکار دارند و ۱. حداقل اطلاعات ۱۰۰ هزار مصرف‌کننده را کنترل یا پردازش کنند. ۲. بیش از ۵۰ درصد درآمد ناخالص آنها از فروش یا کنترل اطلاعات شـــخصی حداقل ۲۵ هزار مصرف‌کننده کسب شود. قانون رئوس و خلاصه مســـئولیت‌ها و استانداردهای حفاظت از حریم خصوصی کنترل‌کنندگان و پردازنده‌های داده را تدوین می‌کند. این قانون به هستارهای [4] دولت محلی و ایالتی اعمال نمی‌شود و بعضی از انواع داده و اطلاعات که در قوانین فدرال حکمرانی می‌شوند را استثنا کرده است. قانون به مصرف‌کننده حق می‌دهد که به اطلاعات دسترسی داشته باشد، آن را تصحیح و پاک کند، از داده خود نسخه‌برداری کرده و از قرارداد پردازش داده شخصی برای اهداف تبلیغات هدفمند خارج شود. قانون به دادســـتان کل، اختیار انحصاری می‌دهد که تخلفات از قانون را اعمال قانون کند و صندوق حریم خصوصی مصرف‌کننده نیز برای پشتیبانی از این تلاش به‌وجود می‌آید. قانون کمیسیون مشترک علوم و فناوری را برای تأســـیس کارگروهی با مشارکت دستگاه‌های دولتی و فعالان مشمول قانون برای بازبینی تدابیر قانون هدایت کرده و ظرف مدت ۶ماه گزارشی از اجرای قانون به نهاد قانونگذاری این ایالت ارائه دهد. البته تاریخ اعمال کامل همه مواد قانون اول ژانویه سال ۲۰۲۳ تعیین شد.

از میان ایالت‌های آمریکا طبق ارزیابی کارشناسان، ایالت کالیفرنیا قوی‌ترین حمایت‌های حریـــم خصوصی را عرضـــه می‌کند [۱۵]. سایر ایالت‌ها نیز در زمینه حریم خصوصی داده‌های مصرف‌کننده، قوانینی در دست اقدام دارند که ازســـوی محققین طبق جدول زیر با یکدیگر و قانون ایالت کالیفرنیا مقایســـه شـــده‌اند، قانون تجارت الکترونیکی ایران نیز در این جدول با قوانین ایالاتی آمریکا مقایسه شده است.

1.Personal Data Privacy and Online Monitoring.
2.Utah Consumer Privacy Act.
3.Consumer Data Protection Act.
4. Entities

جدول ۱. مقایسه قوانین جامع ایالات مختلف آمریکا و قانون تجارت الکترونیک ایران

نام ایالت	حق پاک کردن	حق دسترسی	حق تصحیح	حق اقدام بخش خصوصی[1]	تعریف موسع اطلاعات شناسایی کننده فرد[2]	کسب و کارهای تحت پوشش
کالیفرنیا	بله	بله	خیر	۷۵۰ دلار برای هر شخص (نشت)	بله (نسبی)	درآمدهای بالای ۲۵ میلیون دلار
نیویورک	بله	بله	خیر	۷۵۰ دلار برای هر شخص	بله	همه
مریلند	بله	بله	خیر	خیر. فقط توسط نهاد	بله (نسبی)	درآمدهای بالای ۲۵ میلیون دلار
ماساچوست	بله	بله	خیر	۷۵۰ دلار برای هر شخص	بله (نسبی)	درآمدهای بالای ۱۰ میلیون دلار
هاوایی	بله	بله	خیر	خیر	بله	همه
داکوتای شمالی	بله	بله	خیر	محدود	خیر	درآمدهای بالای ۲۵ میلیون دلار
قانون تجارت الکترونیکی ایران	بله	بله	بله	بله. (۱ تا ۳ سال زندان)	بله	همه

مأخذ: [۱۶] و مطالعات مرکز پژوهش‌های مجلس شورای اسلامی.

همان‌طور که مشاهده می‌شود، بخش حفاظت از داده قانون تجارت الکترونیکی ایران از نظر تعیین حقوق شخص موضوع داده نسبت به قوانین ایالتی آمریکا جامع محسوب می‌شود. به‌صورتی که در ماده (۵۹) این قانون تأکید شده «در صورت رضایت شخص موضوع «داده پیام» و نیز به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره، پردازش و توزیع «داده پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

الف) اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشند.

ب) «داده پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

ج) «داده پیام» باید صحیح و روزآمد باشد.

د) شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام»های ناقص و یا نادرست را محو یا اصلاح کند.

هـ) شخص موضوع «داده پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای «داده پیام»های شخصی مربوط به خود را بنماید». یعنی در بند «هـ» ماده (۵۹) به شخص موضوع داده پیام اختیار پاک کردن و در بند «د» ماده (۵۹) نیز اختیار دسترسی و اصلاح تأکید شده است، اما ضمانت اجرای این قانون کیفری است و در ماده (۷۱) قانون تجارت الکترونیکی ۱ تا ۳ سال زندان برای عدم رعایت ماده (۵۹) وضع شده است. برای مثال اگر شخصی بابت عدم امکان ویرایش اطلاعات در یک بستر مبادلات الکترونیکی به مرجع قضایی شکایت کند. در صورت اثبات بزه مرتکب به ۱ تا ۳ سال زندان محکوم خواهد شد. یعنی قانون ایران حق حریم خصوصی را به رسمیت شناخته است، اما متولی اجرای ماده (۵۹) قانون تجارت الکترونیکی و کلاً بخش مربوط به حمایت از داده‌ها (Data protection) در قانون تجارت الکترونیکی مشخص نیست. درحالی که در ماده (۶۱) قانون تجارت الکترونیکی آمده: «سایر موارد راجع به دسترسی موضوع «داده پیام»، ازقبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان «داده پیام»های شخصی به‌موجب مواد مندرج در باب چهارم این قانون وآئین‌نامه مربوطه خواهد بود». در باب چهارم مسئولیت تدوین آیین‌نامه‌های فرایندهای اعتراض، فراگردهای ایمنی و دیده‌بانی و کنترل داده پیام‌های شخصی مشخص نیست. گرچه تدوین ضوابط نگاهداری داده‌های پزشکی به وزارت بهداشت سپرده شده که از سال ۱۳۸۲ تاکنون انجام نشده است.

1. Private Right of Private Action?
2. Broad Definition of PII?

سایر قوانین ایالتی حریم خصوصی مصرف‌کننده کلیدی

کالیفرنیا

قانون ثبت دلال داده سال ۲۰۱۹[1]. این قانون دلالان داده را ملزم می‌کند که خود را نزد دادستان کل ثبت کنند و اطلاعات خاصی را به او بدهند. در این قانون دلال داده به‌عنوان کسب‌وکاری تعریف می‌شود که با برخی استثنائات، آگاهانه اطلاعات شخصی مصرف‌کننده‌ای که با آن کسب‌وکار رابطه مستقیم ندارد را خریده و به طرف‌های ثالث می‌فروشد. قانون دادستان کل را مکلف می‌کند که اطلاعاتی که توسط دلال‌های داده تهیه شده است را در وب‌گاه داخلی خودش در دسترس قرار دهد. دلال‌های داده که خود را ثبت نکنند مشمول شکایت و مسئولیت مجازات‌های مدنی، هزینه دادرسی و هزینه‌های جاری[2] می‌شوند و هرگونه وصولی به شیوه تعیین شده باید به صندوق حریم خصوصی مصرف‌کننده واریز شود. متن سند قانونی شامل بخش یافته‌های قانونگذار، بیانیه و مقصود از قانونگذاری نیز است.

ورمونت

حفاظت از داده‌های شخصی: دلال‌های داده[3]- دلال‌های داده را ملزم می‌کند که سالیانه نزد وزارت امور داخلی ایالت ورمانت خود را ثبت کنند. دلال‌های داده همچنین باید به مصرف‌کنندگان اطلاعاتی مشخص، شامل نام، پست الکترونیک، آدرس‌های اینترنتی دلال داده را بدهند. چه دلال داده به مصرف‌کننده اجازه بدهد که از گردآوری یا فروش داده‌ها خارج شود یا اجازه ندهد روش درخواست خروج از قرارداد گردآوری داده، فعالیت‌هایی که خروج از قرارداد یا فروش مشمول آنها می‌شوند و اینکه آیا دلال داده به شخص ثالث اجازه می‌دهد به‌جای مصرف‌کننده او را از قرار داده خارج کند جزو اطلاعاتی است که باید به مصرف‌کننده بدهند.

همراه با سایر افشاگری‌ها، بیانیه‌ای که در آن گردآوری داده، پایگاه‌های داده، فعالیت‌های فروشی که یک مصرف‌کننده می‌تواند از قرارداد آنها خارج شود، وجود یا عدم وجود اعتبارسنجی خریداران اطلاعات، باید ازسوی عرضه‌کننده خدمات افشا شود. دلال‌های داده باید برنامه مکتوب امنیت اطلاعات حاوی تدابیر حفاظت فیزیکی، فنی و مدیریتی برای حفاظت از اطلاعات قابل شناسایی شخصی پیاده‌سازی و نگاهداری کنند.

در ایران قوانینی که واقعاً مربوط به دلال‌های داده باشد وجود ندارد و کسب‌وکارهای متعددی درحال گردآوری اطلاعات شهروندان در شبکه‌های اجتماعی مختلف هستند و الزام قانونی هم به افشای اطلاعات ازسوی کسب‌وکارها وجود ندارد.

نوادا

قانون الزامات حریم خصوصی اطلاعات جمع شده از اینترنت در مورد مصرف‌کنندگان[4] **وب‌گاه‌ها** را ملزم می‌کند که به کاربران اجازه دهند که از قرارداد مربوط به فروش داده‌های شخصی خودشان به اشخاص ثالث خارج شوند. اپراتورها (افرادی که مالک یا اداره‌کننده یک وب‌گاه یا خدمات برخط برای اهداف تجاری هستند یا انواع مشخصی از داده را از افراد مقیم نوادا گردآوری می‌کنند) را ملزم می‌کند که یک آدرس مشخص جهت درخواست راه‌اندازی کنند که مصرف‌کنندگان از طریق آن بتوانند درخواستی تأیید شده بدهند و اپراتور را به این سمت هدایت کند که هرگونه فروش اطلاعات تحت پوشش قانون مربوط به وی را ممنوع کند. اصطلاح «فروش» در این قانون به‌معنای مبادله اطلاعات تحت پوشش قانون به‌دلیل ملاحظات پولی توسط اپراتور به شخص دیگر به‌صورتی که شخص بتواند اطلاعات تحت پوشش قانون را به اشخاص دیگری نیز بفروشد. قانون همچنین اپراتورهایی که چنین درخواست‌هایی دریافت کرده‌اند را از فروش هرگونه اطلاعات تحت پوشش قانون پیرامون مصرف‌کننده منع می‌کند. دادستان کل می‌تواند برای چنین تحلفاتی احکام قضایی صادر کند یا جرائم مدنی وضع کند.

قانون اصلاحیه‌های حریم خصوصی اینترنتی سال ۲۰۲۱ نوادا[5]

فصل ۲۹۲ این قانون به حریم خصوصی اینترنتی مربوط می‌شود. این قانون بعضی از معافیت‌ها به بعضی اشخاص خاص داده و اطلاعاتی که در این ایالت در مورد یک مصرف‌کننده ذخیره شده را از الزامات اپراتورها، دلالان داده و اطلاعات تحت پوشش رفع می‌کند. درصورتی که مصرف‌کننده منع کرده باشد، دلال داده از فروش اطلاعات منع می‌شود. این قانون بعضی تدابیر مربوط به فروش بعضی اطلاعات خاص پیرامون مصرف‌کننده که از این ایالت گردآوری شده‌اند را مورد بازنگری قرار داد. در ایران قوانینی که کسب‌وکارها را به ایجاد یک امکان مشخص برای درخواست پاک کردن اطلاعات شخصی افراد بکند، وجود نداشته و قانون مشخصی که به فروش اطلاعات شخصی سامان بدهد نیز وجود ندارد.

حریم خصوصی اطلاعاتی که توسط عرضه‌کنندگان خدمات اینترنت نگاهداری می‌شود.

نوادا و مینیاپولیس ارائه‌دهندگان خدمات اینترنتی را ملزم می‌کنند که بعضی از اطلاعات در مورد مشتریان‌شان را خصوصی نگاه دارند، مگر اینکه مشتری خودش اجازه افشای آن اطلاعات را بدهد. مینسوتا نیز ارائه‌دهندگان خدمات اینترنتی را ملزم می‌کند که پیش از افشای اطلاعات در مورد عادات مرور برخط و وب‌گاه‌های اینترنتی مشاهده شده

1 .Data Broker Registration.
2 .fees, and costs.
3 . 9V.S.A § 2446-2447: Protection of Personal Information: Data Brokers.
4 .Notice Regarding Privacy of Information Collected on Internet from Consumers.
5 .SB260.

توسط کاربران از مشترکین کسب اجازه کنند. ایالت مین[1] استفاده، افشا، فروش یا اجازه به دسترسی اطلاعات شخصی مشتری را بدون رضایت صریح مشترک منع می‌کند. این ایالت همچنین عرضه‌کننده خدمات را از ممانعت از ارائه خدمت، وضع جریمه یا عرضه تخفیف به مشتری بابت اطلاعات را ممنوع کرده است.[2]

مواد (۳۲) و (۳۳) قانون جرائم رایانه‌ای مصوب سال ۱۳۸۸ به مباحث عرضه‌کنندگان خدمات اینترنت می‌پردازد.

«فصل دوم ـ جمع‌آوری ادله الکترونیکی

مبحث اول ـ نگهداری داده‌ها

ماده (۳۲) ـ ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش‌ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره «۱»ـ داده ترافیک هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی ازقبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره «۲»ـ اطلاعات کاربر هرگونه اطلاعات راجع به کاربر خدمات دسترسی ازقبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی (IP)، شماره تلفن و سایر مشخصات فردی اوست.

ماده (۳۳) ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند».

همان‌طور که در مواد (۳۲) و (۳۳) قانون جرائم رایانه‌ای آمده است، در این قانون نگه‌داشتن حداقل ۶ ماه داده‌های ترافیکی مشترکین به عرضه‌کنندگان خدمات دسترسی تکلیف شده است، و عرضه کنندگان خدمات میزبانی هم باید تا ۱۵ روز اطلاعات مشخص شده را نگاهداری کنند، اما بازه زمانی که باید داده‌ها نابود شوند یا ملاحظات حریم خصوصی تصریح نشده‌اند. گرچه به‌نظر می‌رسد احکام حریم خصوصی قانون تجارت الکترونیکی در این حوزه قابل اعمال باشند.

حریم خصوصی اینترنتی اطفال

کالیفرنیا

قانون حقوق حریم خصوصی برای اطفال کالیفرنیایی در دنیای دیجیتالی[3] سال ۲۰۱۵ که به قانون پاک‌کن نیز معروف است، به اطفال اجازه می‌دهد که اطلاعات یا محتوایی که به یک وب‌گاه اینترنتی، خدمات اینترنتی، برنامه اینترنتی یا برنامه تلفن همراه ارسال کرده‌اند را پاک کنند یا درخواست دسترسی و پاک کردن آنها را بدهند. این قانون همچنین اپراتور وب‌گاه یا خدمات برخط که ویژه اطفال ایجاد شده است را از تبلیغات یا بازاریابی محصولات مشخصی که خرید آنها توسط اطفال به‌واسطه قانون منع شده است را ممنوع می‌کند. قانون همچنین تبلیغات و بازاریابی محصولاتی مشخص براساس اطلاعات شخصی خاص اطفال را ممنوع می‌کند، همین‌طور استفاده آگاهانه، افشا، جمع‌آوری یا اجازه به شخص ثالث برای چنین کاری را نیز منع می‌کند.

دلاور[4]

ممنوعیت تبلیغات و بازاریابی به کودکان[5] یا زیر فصل ۱۲۰۴سی در قانون حریم خصوصی اینترنتی ایالت دلاور،[6] اداره‌کنندگان وب‌گاه‌ها، خدمات رایانش ابری یا برخط، برنامه‌های کاربردی برخط، یا برنامه‌های کاربردی تلفن همراه که جامعه هدف‌شان کودکان هستند، از تبلیغ یا بازاریابی خدمات یا محصولات اینترنتی نامناسب برای کودکان شامل الکل، تنباکو، اسلحه یا هرزه‌نگاری منع می‌شوند.

هنگامی که تبلیغات یا بازاریابی روی یک خدمت اینترنتی معطوف به کودکان توسط یک خدمت تبلیغاتی عرضه می‌شود، اپراتور خدمات اینترنت موظف است که به خدمت‌رساننده هشدار بدهد که از چه زمانی ممنوعیت تبلیغات و بازاریابی محصولات و خدمات به‌صورت مستقیم بر خدمات تبلیغاتی مستقیماً اعمال خواهد شد. قانون همچنین اپراتور یا عرضه‌کننده خدمات اینترنتی که با استفاده از اطلاعات شخصی می‌داند که کودک از خدمات اینترنتی استفاده می‌کند را از استفاده از اطلاعات قابل شناسایی کودک برای تبلیغات و بازاریابی خدمات و محصولات به او منع می‌کند، همچنین افشای اطلاعات قابل شناسایی کودک نیز با دانش نسبت استفاده از آن برای اهداف بازاریابی و تبلیغات آن نوع محصولات و خدمات به کودک ممنوع است.

در ایران قوانین مشابهی که حمایت‌های بیشتری از حریم خصوصی کودکان به‌وجود بیاورد، وجود ندارد.

1 .Maine.
2 .Maine - 35-A MRSA § 9301 (effective 7-1-20).
3 .Calif. Bus. & Prof. Code §§ 22580-22582: California's Privacy Rights for California Minors in the Digital World Act
4 .Delaware.
5 § 1204C. Prohibitions on online marketing or advertising to a child.
6 .Del. Code § 1204C.

حریم خصوصی خواندن اینترنتی

آریزونا

بخش ۴۱-۱۵۱,۲۲ در قانون اطلاعات کتابخانه‌ای در قانون کتابخانه‌های آریزونا، آرشیوهای عمومی تأسیس شده در دفتر وزارت امور داخلی آریزونا[1] تعیین می‌کند که کتابخانه یا سیستم کتابخانه‌ای که توسط بودجه عمومی پشتیبانی می‌شود نباید به هیچ‌گونه سوابق اطلاعاتی یا هرگونه اطلاعات شامل کتاب‌های الکترونیکی مطالعه شده یک کاربر خدمات کتابخانه‌ای اجازه افشا بدهند.

کالیفرنیا

بخش‌های ۶۲۵۴، ۶۲۶۷ و ۶۲۷۶ از قانون دولتی کالیفرنیا[2]

رکودهای کتابخانه‌ای اشخاص از قبیل رکوردهای مکتوب یا تراکنش‌های الکترونیکی که اطلاعات قرض گرفتن یا استفاده از منابع کتابخانه‌ای شامل و نه محدود به سوابق جستجوی پایگاه داده، سوابق قرض گرفتن کتاب، موسیقی و هرگونه اطلاعات مربوط به درخواست یا جستجوی منابع اطلاعاتی را حفاظت می‌کند.

بخش ۱۷۹۸,۹۰ قانون مدنی کالیفرنیا[3] **یا قانون حریم خصوصی مطالعه کالیفرنیا** از اطلاعات پیرامون کتاب‌هایی که کالیفرنیایی‌ها از طریق فروشندگان کتاب برخط و خدمات الکترونیکی دارای اطلاعات تشریحی در مورد خوانندگان، مرور کرده‌اند، خریده‌اند یا خوانده‌اند، حفاظت می‌کند. با تعیین یکسری استثنائات از قبیل خطر آنی مرگ یا صدمه جدی، کسب‌وکارها برای افشای اطلاعات شخصی مشتریان نیازمند دستور دادگاه، حکم تفتیش[4] یا رضایت صریح مشترک خواهند شد.

دلاور

زیر بخش ۱۲۰۶ پ از قانون حفاظت و حریم خصوصی برخط دلاور[5] **با عنوان حریم خصوصی اطلاعات در مورد کاربران خدمات کتاب**[6] مفادی مشابه قانون کالیفرنیا در این زمینه دارد و ارائه‌دهنده خدمات کتاب را مکلف می‌کند که مگر در صورت معاف شدن، سالیانه گزارشی برخط در زمینه افشای اطلاعات منتشر کند.

واحد حفاظت از مصرف‌کننده در وزارت دادگستری این ایالت موظف به بازرسی و پیگیرد تخلف از قانون می‌شود.

میسوری

ماده ۸۱۵ و ۸۱۷ از فصل ۱۸۲[7] **بخش یازده قانون کتابخانه‌ها و آموزش میسوری**[8] کتاب الکترونیکی[9] و مواد یا منابع دیجیتالی[10] را تعریف می‌کند و آنها را به گزینه‌هایی که باید در تعریف مواد کتابخانه‌ای[11] می‌افزاید که یک مشترک کتابخانه ممکن است استفاده کند، قرض بگیرد، درخواست کند. تعیین می‌کند که هر شخص ثالث طرف قرار داد با یک کتابخانه که سوابق کتابخانه‌ای را دریافت می‌کند، انتقال می‌دهد یا نگهداری می‌کند، نمی‌تواند بدون رضایت شخصی که در سوابق شناسایی می‌شود یا دستور قاضی این اطلاعات را افشا یا منتشر کند.

در ایران قوانینی که بحث حریم خصوصی مطالعه الکترونیکی را مقرراتگذاری کند وجود ندارد.

سیاست‌های حریم خصوصی و کردارهای وب‌گاه‌ها و خدمات برخط

کالیفرنیا

ماده (۲۲۵۷۵) فصل ۲۲ مقررات کسب‌وکارهای خاص با عنوان الزامات حریم خصوصی اینترنتی سال ۲۰۰۳[12] اداره‌کنندگان وب‌گاه‌های تجاری یا خدمات برخط را ملزم می‌کند که سیاست‌های حریم خصوصی خود را در زمینه نحوه پاسخ به سیگنال عدم تعقیب مرورگر[13] یا سازوکارهای مشابه و توانایی اعمال انتخاب در مورد تعقیب برخط در یک وب‌گاه یا خدمات در طول زمان را افشا کنند. همچنین این قانون اپراتور را ملزم می‌کند که در مورد امکان انجام این قبیل رهگیری‌ها روی خدمات یا وب‌گاه اپراتور توسط اشخاص ثالث اطلاع‌رسانی کنند.

1. Arizona State Library, Archives and Public Records Established in the Office of the Secretary of State.
2 .Cal. Govt. Code §§ 6254, 6267 and 6276.28.
3 .Cal. Civil Code § 1798.90.
4 .search warrant.
5 .Delaware Online Privacy and Protection Act.
6 .Privacy of information regarding book service users.
7 .Mo. Rev. Stat. §§ 182.815, 182.817.
8 .Title Xi Education and Libraries.
9 .E-book.
10 .Digital Resource or Material.
11 ."Library Material".
12 .Calif. Bus. & Prof. Code § 22575 .
13 .'Do Not Track'.

فصل ۱۷۹۸ از عنوان ۱,۸۱,۵. قانون حریم خصوصی مصرف‌کننده کالیفرنیا[1] بعضی شرکت‌های خاص را ملزم می‌کند که اطلاعات مشخص شده‌ای همچون داشتن یا نداشتن سیاست حریم خصوصی را در یک بیانه یا بیانه‌های سیاست حریم خصوصی اعلام و آنها را هر ۱۲ ماه به‌روزرسانی کنند و بعضی شرکت‌های خاص را ملزم می‌کند که توصیفی از حقوق مصرف‌کنندگان ذیل بخش ۱۷۹۸,۱۲۰ که طبق آن یک پیوند مجزا به صفحه اینترنتی ذیل سیاست‌های حریم خصوصی با عنوان «اطلاعات شخصی من را نفروشید» قرار داده شود.

ماده ۹۹۱۲۲ قانون شیوه‌نامه آموزشی کالیفرنیا[2] نهادهای آموزشی دانشگاهی انتفاعی و غیرانتفاعی خصوصی را ملزم می‌کند که سیاست حریم خصوصی رسانه اجتماعی را بر روی وب‌گاه اینترنتی مؤسسه ارسال کنند.

کنتیکت

بخش ۴۲-۴۷۱ قانون حفاظت از شماره تأمین اجتماعی و اطلاعات شخصی[4] هر شخصی که شماره تأمین اجتماعی را در جریان کسب‌وکار گردآوری می‌کند را موظف می‌کند که یک بیانیه سیاست صیانت از حریم خصوصی تدوین کند. بیانیه سیاست باید از طریق ارسال آن بر روی یک صفحه وب به‌صورت عمومی نمایش داده شود و ۱. از محرمانگی شماره‌های تأمین اجتماعی حفاظت کند. ۲. افشای غیرقانونی شماره تأمین اجتماعی را ممنوع کند و ۳. دسترسی به شماره‌های تأمین اجتماعی را محدود کند.

دلاور

ماده (۲۰۵) از فصل دوازدهم یا حمایت از حریم خصوصی شخصی و برخط[5] **ذیل زیرعنوان دوم یا دیگر قوانین مرتبط با تجارت و بازرگانی**[6] **از عنوان دوم قانون تجارت و بازرگانی**[7] اپراتور وب‌گاه اینترنتی تجاری، خدمات رایانش ابری یا برخط، برنامه کاربردی برخط، یا برنامه تلفن هوشمند که اطلاعات قابل شناسایی شخصی را از طریق اینترنت در مورد کاربران منفرد مقیم ایالت دلاور جمع می‌کنند را ملزم می‌کند که سیاست حریم خصوصی خودشان را در محلی که به‌وضوح قابل مشاهده باشد قرار بدهند. اپراتورها تنها درصورتی ناقض این زیر بخش هستند که ظرف مدت ۳۰ روز از دریافت هشدار در مورد عدم انطباق با قانون سیاست حریم خصوصی خود را به‌وضوح قابل مشاهده نکنند. این قانون همچنین شرایط انطباق با قانون را مشخص می‌کند.

نوادا

ماده (۳۴۰) از فصل الف ۶۰۳[8] **قانون امنیت و حریم خصوصی اطلاعات شخصی**[9] اپراتور وب‌گاه اینترنتی یا خدمات برخطی که اطلاعات قابلیت شناسایی شخصی را گردآوری می‌کند را ملزم می‌کند که انواع اطلاعاتی که از طریق وب‌گاه یا خدمات خود گردآوری کرده است را اعلام کند.

اورِگن[10]

کردارهای تجاری، کسب‌وکار غیرقانونی[11] **در ماده (۶۰۷) از فصل ۶۴۶**[12] **با عنوان مقررات ضد انحصار و کردارهای تجاری**[13] انتشار بیانیه‌های غلط یا نادرست در مورد سیاست‌های حریم خصوصی را غیرقانونی اعلام می‌کند.

در ایران قوانینی که به‌وضوح تکالیف کسب‌وکارها در زمینه اطلاع‌رسانی در مورد شیوه مدیریت داده‌های شخصی را مشخص کند، وجود ندارد.

اطلاعات غلط و گمراه‌کننده در زمینه سیاست‌های حریم خصوصی

تمامی ۵۰ ایالت متحده آمریکا قوانینی در زمینه کردارها و کنش‌های گمراه‌کننده و غیرمنصفانه دارند که در مورد اطلاعاتی که به‌صورت برخط ارسال می‌شود نیز قابل اعمال است. قوانین نبراسکا[14]، اورِگن[15]

1 .TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100.
2 .Cal. Ed. Code § 99122.
3 .Conn. Gen. Stat. § 42-471.
4 .Protection of Social Security Numbers and Personal Information.
5 .CHAPTER 12C. Online and Personal Privacy Protection.
6 .Other Laws Relating to Commerce and Trade.
7 .Del. Code Tit. 6 § 205C.
8 .NRS § 603A.340.
9 .Security and Privacy of Personal Information.
10 .Oregon.
11 646.607 Unlawful Business, Trade Practices.
12 .ORS § 646.607.
13 .Trade Practices and Antitrust Regulation.
14 .§ 87-302 15).
15 .ORS § 646.607.

و پنسیلوانیا[1] انتشار بیانیه‌های حریم خصوصی گمراه‌کننده یا غلط را جرم‌انگاری کرده‌اند.

هشـــدار در زمینه نظارت بر ارتباطات پســـت الکترونیکی، دسترسی اینترنتی و اطلاعات مکانی

ایالت‌های کنِتیکت[2]، دلاور[3] و نیویـــورک، کارفرمایان را ملزم می‌کنند که قبل از نظارت بر ارتباطات پست الکترونیکی یا دسترسی اینترنتی کارمندان به آنها هشـــدار بدهند. کلرادو[4] و تنســـی،[5] ایالت‌ها و دیگر نهادهای عمومی را ملزم می‌کنند که یک سیاست در زمینه نظارت بر ایمیل‌های کارمندان بخش عمومی اتخاذ کنند. هاوایی،[6] کارفرمایان را از اجبار کارمندان به بارگیری برنامه کاربردی بر روی وسایل ارتباطی شـــخصی کارمندان جهت رهگیری مکان کارمند یا افشای اطلاعاتی شخصی کارمند منع می‌کند.

در ایران بند «۹» مـــاده (۱) مصوبه حقوق شـــهروندی در نظام اداری مصـــوب ۱۳۹۵/۱۱/۹ شـــورای‌عالی اداری «اجتنـــاب از رویکردهای سلیقه‌ای، جناحی، تبعیض‌آمیز و روش‌های ناقض حریم خصوصی در فرایند جذب و گزینش» مورد تأکید قـــرار گرفته، اما مصداقی از موارد نقض حریم خصوصی ذکر نشده است.

سیاست‌های حریم خصوصی وب‌گاه‌های دولتی

حداقل ۱۶ ایالت، وب‌گاه‌های دولتی یا درگاه‌های دولتی را ملزم می‌کنند که رویه‌ها و بیانیه سیاست حریم خصوصی تدوین کنند و آن را به‌صورت قابلیت خوانده شدن توسط ماشین[7] در وب‌گاه‌های خود قرار دهند.

قوانین اطلاع‌رسانی در مورد نشت اطلاعات شخصی

تمامی ۵۰ ایالت متحده آمریکا، ناحیه کلمبیا، گوام، پورتوریکو و جزایر ویرجین، قوانینی دارند که کسب‌وکارها و در اغلب ایالت‌ها هستارهای دولتی را ملزم می‌کنند که نشت امنیتی که شامل اطلاعات موجب قابل شناسایی شدن شخص می‌شود را به افراد هشدار دهند.

قوانین نشـــت امنیتی عموماً تدابیری درخصوص اینکه چه کسی باید قانون را اعمال کند (مثلاً کســـب‌وکارها، دلال‌هـــای داده و اطلاعات، هستارهای دولتی و مانند آن)، تعریف اطلاعات شخصی (مثلاً ترکیب نام و شماره تامین اجتماعی، گواهی رانندگی، کارت هویت ایالتی، شماره حساب و از این قبیل)، نشت شـــامل چه چیزهایی می‌شود (دسترسی غیرمجاز به داده)، الزامات هشدار (مثلاً زمانبندی و شیوه اعلام هشدار، اشخاصی که باید هشـــدار را دریافت کنند) و معافیت‌ها (مثلاً در مورد اطلاعات رمز شده) دارند.

در ایران قوانینی که کسب‌وکارها را ملزم به اطلاع‌رسانی پیرامون نشت اطلاعات کند، وجود ندارد.

جمع‌بندی

گرچه از نظر دایره شـــمول احکام، قانون تجـــارت الکترونیکی بســـیاری از ظواهر یک قانون جامع را دارد، اما فاقد سازوکارهای اجرایی شـــفاف برای تحقق امر حفاظت از حریم خصوصی است. مثلاً گرچه به شـــخص موضوع داده اختیار حذف داده پیام‌های شخصی او داده می‌شود، اما ســـازوکار اعلام داده‌های در اختیار، شیوه درخواست و مهلت‌های قانونی مشخص نیستند. نتایج این مطالعه نشان می‌دهد به طور کلی در توســـعه قوانین حمایت از حقوق داده‌ها و رفع خلأهـــای قانونی ملاحظات ذیل باید مدنظر قرار گیرد:

۱. مشخص کردن جامعه هدف: قوانین حریم خصوصی از نظر جامعه هدفی که حقوقش مورد تأکید قـــرار می‌گیرد، می‌توانند مصرف‌کنندگان خدمات و کالا به‌صورت عام، کارمندان، مراجعین به کتابخانه‌ها، اســـتفاده‌کنندگان از خدمات خاص و کودکان و سایر اقشـــار نیازمند حمایت را دربر بگیرند. سطوح حفاظتی که نســـبت به هرکدام از این جوامع هدف رعایت می‌شود، می‌تواند متفاوت باشد. برای مثال قانونگذار می‌تواند سختگیری بیشتری در زمینه حذف ســـوابق مربوط به کودکان یا گردآوری اطلاعات آنها نسبت به اشخاص عادی اعمال کند. قوانین حریم خصوصی از نظر جامعه هدفی که اعمالش ضابطه‌مند می‌شود، می‌تواند شامل بخش دولتی، فعالین بخش خصوصی به‌صورت عمومی یا اشخاص حقیقی و حقوقی شاغل در حوزه‌های خاص شوند. در نتیجه در مستندات پشتیبان هر نوع طرح حقوقی باید استدلال مشخص

1.18 Pa. C.S.A. § 4107(a)(10).
2 .Gen. Stat. § 31-48d.
3 .Del. Code § 19-7-705.
4 .Colo. Rev. Stat. § 24-72-204.5.
5 .Tenn. Code § 10-7-512.
6 .2021 H.B. 1253.
7 .Machine-Readable.

بشود که جامعه هدف چگونه انتخاب شـــده و یا چرا یک جامعه هدف مورد تاکید قرار نمی گیرد.

۲.لزوم ساماندهی دلال‌های داده: دلال‌های داده بدون ارتباط کسب‌وکاری با شـــهروندان اطلاعات آنها را گردآوری کرده و به فروش می‌رسانند، از این رو لازم است که تکلیف آن‌ها در قوانین کشور مشخص بشود.

۳.ضرورت در نظر گرفتن حساسیت اطلاعات کتابخانه‌ای: اطلاعات مربوط به ترجیح مطالعاتی افـــراد، مبین گرایش‌های فکری و اندیشه افراد می‌تواند باشد و از این رو حفاظت‌های قانونی شدیدتر در مورد آن‌ها قابل در نظر گرفتن است.

۴. منع استفاده از اطلاعات کودکان برای تبلیغات: برای تحقق هدف حمایت از حریـــم خصوصی کودکان یکی از عواملی که انگیزه گردآوری اطلاعات کـــودکان را کاهش می‌دهد ایجاد ممنوعیت تبلیغ بر اساس اطلاعات عادات کاربری آن‌ها است.

۵. ســـاماندهی نشـــت اطلاعات: نشـــت اطلاعات یکی از موضوعات مهم در زمینه حقوق داده‌ها است و اطلاع‌رسانی سریع و جرم‌انگاری لاپوشـــانی و پنهان کاری در این زمینه می‌تواند با حمایت از اطلاع رســـانی بهنگام به افراد موضوع داده کمک کند ضرر و آســـیب وارده احتمالی حاصل از نشت اطلاعات را کاهش بدهند.

۶. تکلیف به ایجاد قابلیت نرم‌افزاری داخل نرم‌افزارهای برخط برای درخواست دسترسی و پاک شدن اطلاعات: ذکر کلی حق دسترســـی کاربران در قوانین برای احقاق حقوق کاربران قابلیت اجرایی کافی ندارد و کاربرپسند بودن و سهولت درخواست دسترســـی و اصلاح نیز قابلیت تاکید از سوی قانون گذار را دارد.

۷. ضرورت بازنگری و تقویت قانون تجارت الکترونیکی مصوب ۱۳۸۲: با توجه بـــه مفاد این قانون بخشـــی از هر نوع قانونگذاری در زمینه صیانـــت از داده‌ها تعیین و تکلیف وضعیت قانون تجارت الکترونیکی خواهد بود.

۸. ضرورت انجام مطالعات بیشتر: پیشنهاد می‌شود که در پژوهش‌های آینده موضوع مالکیـــت داده و حفاظت از داده‌ها با دقت بیشتری بررسی و از یافته‌های پژوهش برای بررسی طرح ها و لوایح مرتبط استفاده شود. همچنین بررسی کشورهایی مانند ژاپن یا بعضی از کشورهای درحال توسعه مسلمان مانند مالزی، سنگاپور، هند، اندونزی، ترکیه و ... در آینده می‌تواند مفید واقع شوند.

منابع و ماخذ

[1] C. Perarnaud, "Privacy and data protection," 2022. [Online]. Available: https://dig.watch/topics/privacy-and-data-protection#:~:text=Privacy%20and%20data%20protection%20are,to%20disclose%20information%20or%20not)..

[2] cloudian, "Data Protection and Privacy: 12 Ways to Protect User Data," 2022. [Online]. Available: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/#:~:text=Data%20privacy%20defines%20who%20has,to%20protect%20private%20user%20data

[3] H. 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.

[4] C. Kuner, ransborder data flows and data privacy law, Oxford University Press, 2013.

[5] D. 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.

[6] safecomputing, "History of Privacy Timeline," 2021. [Online]. Available: https://safecomputing.umich.edu/privacy/history-of-privacy-timeline.

[7] S. D. Warren and L. D. Brandeis, "The Right to Privacy," Harvard Law Review, 1890.

[8] W. L. Prosser, “Privacy,” California Law Review, 1960.

[9] Cornel, “Privacy,” 2022. [يطخنورد]. Available: https://www.law.cornell.edu/wex/privacy.

[10] federalregister, "Securing the Information and Communications Technology and Services Supply Chain," 2019. [Online]. Available: https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[11] federalregister, "Protecting Americans' Sensitive Data From Foreign Adversaries," 2021. [Online].

Available: https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.
[12] FTC , "FTC Policy Work," 2022. [Online]. Available: https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/ftc-policy-work.
[13] Z. Lauren , B. Tatyana , . P. Brandon, L. Sofia and S. Cory , "The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation," 2022. [Online]. Available: https://www.belfercenter.org/publication/role-federal-trade-commission-federal-data-security-and-privacy-legislation.
[14] NCLS, "State Laws Related to Digital Privacy," 2022. [Online]. Available: https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others..
[15] T. Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," 2021. [Online]. Available: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
[16] A. Green, "Complete Guide to Privacy Laws in the US," Varonis, 2021.

مرکز پژوهش های مجلس شورای اسلامی

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

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

وب سایت: rc@majles.ir