مرکز پژوهش‌های مجلس شورای اسلامی
مسلسل: ۱۸۷۱۶
بهمن ۱۴۰۱
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 (۱): نگاشت قوانین


بسم الله الرحمن الرحیم
بنام خدای بزرگ بخشایش همیشه بخشاینده

تاریخ انتشار:
۱۴۰۱/۱۱/۹

شماره مسلسل: ۱۸۷۱۶
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 (۱): نگاشت قوانین

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

تهیه و تدوین:
ابوالقاسم رجبی

مدیر مطالعه:
حسن پوراسماعیل

همکاران:
امین پژمان، سیدعلی محسنیان

اظهارنظرکنندگان:
محمدمهدی مهربان‌هلان، حسین بشری خاوه، ایمان اکبری، عطیه یوسفی

ناظر علمی:
محمدحسن معادی رودسری

صفحه‌آرا:
نفیسه حاجی‌صفری

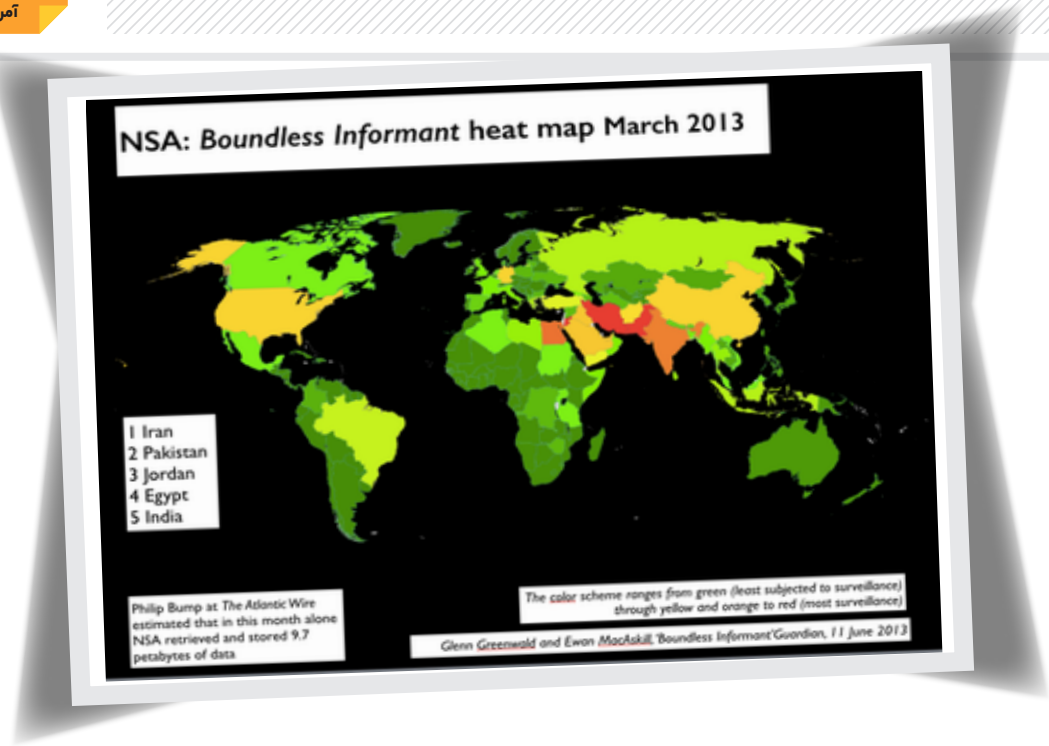
ویراستار ادبی:
طاهره سیدمحمد

دفتر مطالعات انرژی، صنعت و معدن

فهرست مطالب

فهرست جدول

فهرست نمودارها



شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا شماره (۱): نگاشت قوانین

چکیده

پیش‌نویس لایحه حفاظت از داده‌ها که با مشارکت مرکز پژوهش‌های مجلس تدوین و رونمایی شده است در حال طی مراحل تبدیل شدن به لایحه و تقدیم به مجلس شـــورای اسلامی اســـت و طرحی نیز در مجلس شورای اسلامی در زمینه حفاظت از داده‌ها اعلام وصول شده اســـت. به این ترتیب شـــیوه گذار از مقرراتگذاری بخشی حفاظت از داده به مقرراتگذاری جامع حفاظت از داده‌ها و نقش مقررات بخشـــی در حفاظت از داده‌ها در کشـــور ایران اهمیت می‌یابد. برای شناسایی خلأهای قانونی و قانونگذاری جدید نیاز اســـت که قوانین و مصوبات قبلی کشور در زمینه حفاظت از داده‌ها به‌صورت روشمند با مدل‌های نظری حریم خصوصی و حفاظت از داده‌ها مقایسه شوند. در این گزارش ابتدا با مأخذ قرار دادن چارچوب سولو از حریم خصوصی که منبعث از نظام حقوقی ایالات متحده آمریکاست و تکمیل آن با توجه به جوانب زنجیره ارزش داده‌ها، مصوبات مربوط به حفاظـــت از داده‌های ایران شناسایی و مورد بررســـی قرار گرفتند. با توجه به وجود احکام قانونی در زمینه‌های مختلف موضوع حفاظت از داده‌ها پیشنهاد می‌شود این احکام در بررســـی طرح‌ها و لوایح تعیین تکلیف شوند و ارتباط هر نوع طرح و لایحه پیشنهادی در موضوع حفاظت از داده‌ها با این مواد قانونی به‌صورت صریح مشخص شود.

خلاصه مدیریتی

شناسایی و رفع خلأهای قانونی حفاظت از داده‌ها و حریم خصوصی یکی از زیرساخت‌های حقوقی مهم جلب اعتماد داخلی به صنایع بومی فناوری اطلاعات و توسعه پایدار این صنعت و رقابت‌پذیری خدمات فناوری اطلاعات و ارتباطات ایرانی در بازارهای بین‌المللی و منطقه‌ای است. برای شناسایی خلأهای قانونی نیاز است قوانین و مصوبات قبلی کشور در زمینه حفاظت از داده‌ها به‌صورت روشمند با مدل‌های نظری حریم خصوصی و حفاظت از داده‌ها مقایسه شوند. در این گزارش ابتدا با مأخذ قرار دادن چارچوب سولو از حریم خصوصی که منبعث از نظام حقوقی ایالات متحده آمریکاست و تکمیل آن با توجه به جوانب زنجیره ارزش داده‌ها، مصوبات مربوط به حفاظت از داده‌های ایران شناسایی و مورد بررسی قرار می‌گیرند.

نگاشت قوانین ایران در چارچوب سولو ارتقا یافته نشان می‌دهد از جنبه **گردآوری اطلاعات در زیربخش جلوگیری از مراقبت و پایش غیرمنصفانه شهروندان**، برخی از اصول قانون اساسی و موادی از قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات مصوب ۱۳۸۲، قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند مصوب ۱۳۸۶ احکامی مرتبط با حفاظت حریم خصوصی به تصویب رسیده‌اند، همین‌طور از جنبه دیگر گردآوری اطلاعات یعنی **جلوگیری از بازجویی و استنطاق غیرمنصفانه از شهروندان** نیز در قانون تجارت الکترونیکی، قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ احکامی به تصویب رسیده‌اند.

گرچه قوانین و برنامه‌های متعددی برای تجمیع اطلاعات شهروندان در موضوعات یارانه‌ها در دستور کار قرار دارد، اما **از جنبه پردازش داده‌ها در زیربخش ترکیب یا تجمیع غیرمنصفانه داده‌ها احکامی در حمایت از شهروندان به تصویب نرسیده است.**

از جنبه **پردازش داده‌ها در زیربخش جلوگیری از ناامنی یا لزوم حفاظت و الزام به رعایت ضوابط پردازش ایمن اطلاعات** در قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ و قانون جرائم رایانه‌ای مصوب ۱۳۸۸ احکامی به تصویب رسیده است.

قانون تجارت الکترونیکی در جنبه پردازش داده‌ها در زیربخش‌های **تبعیض غیرمنصفانه از طریق: ۱. عدم اطلاع‌رسانی در مورد اطلاعات گردآوری شده پیرامون فرد و شیوه استفاده از آنها، ۲. بازاستفاده غیرمنصفانه از داده‌های فرد در موضوعی غیر از هدف اولیه و ۳. شناسایی فرد با استفاده از اتصال اطلاعات احکامی دارد. از جنبه تهاجم به حریم خصوصی از زیربخش نفوذ یا اختلال در آرامش و تنهایی فرد و مداخله در تصمیم‌گیری‌های فردی اشخاص نیز قوانین صریحی که موضوع را به‌خوبی پوشش دهند، در ایران وضع نشده است.**

در جنبه انتشار اطلاعات از زیربخش **نقض محرمانگی و افشای غیرمجاز اطلاعات به اشخاص فاقد صلاحیت**، قانون ارتقای

سلامت نظام اداری و مقابله با فساد مصوب ۱۳۹۰، قانون پایانه‌های فروشگاهی و سامانه مؤدیان مصوب ۱۳۹۸، قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱، قانون برنامه پنجساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۴۰۰ـ۱۳۹۶) احکامی مرتبط با حفاظت از داده‌ها دارند.

در جنبه **انتشار اطلاعات از زیربخش افشا یا آشکارسازی اطلاعات غیرمجاز به‌صورت عمومی** قانون تجارت الکترونیکی، قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳، قانون ارتقای سلامت نظام اداری و مقابله با فساد مصوب ۱۳۹۰، قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ و قانون پایانه‌های فروشگاهی و سامانه مؤدیان مصوب ۱۳۹۸ احکامی مرتبط با حریم خصوصی دارد. در جنبه **انتشار اطلاعات از زیربخش نمایان‌سازی و آشکارسازی احساسات و موضوعات شخصی مربوط به بدن** او در قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند مصوب ۱۳۸۶ احکامی در زمینه حفاظت از داده‌ها دارد. در جنبه **انتشار اطلاعات از زیربخش حق‌السکوت یا تهدید به افشای اطلاعات و طلب وجه بابت پاک کردن اطلاعات** در قانون تجارت الکترونیکی احکامی در زمینه حفاظت از اطلاعات وجود دارد. در جنبه **انتشار اطلاعات از زیربخش تحریف یا توزیع اطلاعات غلط** در مورد فرد در قانون تجارت الکترونیکی، قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ و قانون جرائم رایانه‌ای مصوب ۱۳۸۸ احکامی در زمینه حریم خصوصی داده‌ها دارند. در جنبه **انتشار اطلاعات از زیربخش دسترس‌پذیرسازی فزاینده** که با تشدید در دسترس بودن اطلاعات به‌واسطه الکترونیکی شدن و جستجوپذیری بهتر آنها رخ می‌دهد و همین‌طور غصب یا استفاده غیرمجاز از هویت افراد دیگر برای کسب منفعت تجاری در قوانین ایران احکامی در حمایت از شهروندان به تصویب نرسیده است.

ترک فعل‌های مهم در زنجیره ارزش داده‌ها شامل: ۱. سلب اختیار از ترابردپذیری داده‌های شخصی بین عرضه‌کنندگان خدمات فناوری یکسان، ۲. پنهان‌کاری در مورد اقدامات علیه امنیت داده‌های شخصی و گزارش به‌موقع به فرد متأثر از این اقدامات و ۳. قلمرو قضایی داده‌ها یا شفافیت در موازین مربوط به ذخیره اطلاعات خاص در قلمرو قضایی کشور ایران نیز در قوانین مغفول هستند.

همان‌طور که مشاهده می‌شود **قانون تجارت الکترونیکی به‌تنهایی بخش‌های زیادی از موضوع حریم خصوصی و حفاظت از داده‌های مصرف‌کنندگان را پوشش می‌دهد** و درنتیجه در هر نوع قانونگذاری در زمینه حریم خصوصی و حفاظت از داده‌ها اصلاح این قانون نیز باید مورد توجه قرار گیرد و یکی از گزینه‌های رفع خلأ قانونی در زمینه حفاظت از داده‌ها، پیشنهاد اصلاحیه قانون تجارت الکترویکی است. همین‌طور احکامی که در ارتباط با جوانب مختلف موضوع حفاظت از داده‌های شخصی و حریم خصوصی ذکر شدند در هر نوع تنظیم قوانین باید به‌طور شفاف تعیین تکلیف شوند. درنتیجه پیشنهاد می‌شود به‌جای ذکر عبارت کلیه قوانین مغایر با این قانون لغو می‌شوند، در انتهای طرح‌ها و لوایح قانونی اصلاحیه‌های احکام متأثر از قانون حفاظت از داده‌ها در خود طرح یا لایحه به‌صورت شفاف ذکر شوند.

مقدمه

داده، نفت قرن بیست‌ویکم و نیروی پیش‌برنده همه ابزارهای فناوری اطلاعاتی مانند وبگاه‌ها و برنامه‌های کاربردی است.[۱] داده به یکی از مهم‌ترین دارایی‌های کسب‌وکارها مبدل شده و توسعه پایدار و تکمیل زنجیره ارزش داده بومی از طریق تحقق حداقل‌های حفاظت از داده به میدان رقابت میان کشورها مبدل شده است.[۲] در حالی که اقتصاد داده[۱] بسیاری از حوزه‌های مختلف را متحول کرده، اما تبعاتی ناخواسته نیز برای کاربران به ارمغان آورده است. بسیاری از بازیگران اقتصاد داده، از داده‌های کاربران خود مانند یک کالای تجاری استفاده می‌کنند و آن را بدون اجازه یا اطلاع کاربران با طرف‌های ثالث به اشتراک می‌گذارند. از نظر اقتصادی استفاده از داده یکی از منابع درآمدی به‌شمار می‌رود.[۳] در حالی که مصرف‌کنندگان هیچ ابزار متناسبی برای ممانعت از پردازش داده‌هایشان برای اهداف ناخواسته و سرزده در اختیار ندارند. دولت‌ها نیز برای اجرای موفق سیاست‌های خود نیازمند اشراف اطلاعاتی ضابطه‌مند هستند.[۴]

در گذشته پژوهشگران، مقررات حفاظت از داده‌های کشورها را به دو دسته بخشی و جامع تقسیم‌بندی می‌کردند.[۵] کشورهای چین، برزیل و ایالات متحده آمریکا کشورهای مهمی بودند که مقرراتی جامع در راستای حفاظت از داده‌ها و حریم خصوصی نداشتند. اما امروزه برزیل[۶] مقررات جامع حفاظت از داده‌ها دارد، چین مقررات حفاظت داده‌ای سخت‌گیرانه‌تر و عمیق‌تر از اتحادیه اروپا تدوین کرده[۷] و ایالات متحده آمریکا نیز با توجه به تصویب قانون حریم خصوصی مصرف‌کننده کالیفرنیا و اقدامات مشابه در ایالت‌های دیگر و امکان شکل‌گیری تصمیم فراحزبی و درخواست شرکت‌های بزرگ برای تصویب مقررات جامع حفاظت از داده‌ها در سطح کنگره، احتمالاً به‌زودی قانون جامع حفاظت از داده‌ها خواهد داشت. با این چشم‌انداز گذار از نظام بخشی به نظام جامع حفاظت از داده‌های شخصی در این کشور اهمیت یافته است. در کشور ایران نیز بعضی مقررات پراکنده در زمینه حفاظت از داده‌ها به تصویب رسیده است. مثلاً قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون ارتقای سلامت نظام اداری و مقابله با فساد مصوب ۱۳۹۰ و قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۷ ازجمله این قوانین هستند. لایحه حفاظت از داده‌ها که با مشارکت مرکز پژوهش‌های مجلس تدوین و رونمایی شده است در حال طی مراحل تبدیل شدن به لایحه و تقدیم به مجلس شورای اسلامی است و طرحی نیز در مجلس شورای اسلامی در زمینه حفاظت از داده‌ها اعلام وصول شده است. به این ترتیب شیوه انتقال از مقرراتگذاری بخشی حفاظت از داده به مقرراتگذاری جامع حفاظت از داده‌ها و نقش مقررات بخشی در حفاظت از داده‌ها در کشور ایران اهمیت می‌یابد. اما انتقال از مقرراتگذاری بخشی به مقرراتگذاری جامع حفاظت از داده‌ها نیازمند تشخیص خلأهای قانونی حفاظت از داده‌ها و حریم خصوصی است.

هدف و روش تحقیق

هدف از این پژوهش شناسایی خلأهای قانونی و قوانین مرتبط با موضوع حریم خصوصی و حمایت از داده‌هاست. برای شناسایی خلأهای قانونی نیاز به مدل‌های نظری حریم خصوصی و حمایت از داده است. بنابراین در قسمت بعد مفهوم‌شناسی حریم خصوصی و طبقه‌بندی انواع موضوعات حریم خصوصی از زاویه دید زنجیره ارزش داده بررسی می‌شود. یعنی ابتدا زنجیره ارزش داده‌ها برای شناسایی ذی‌نفعان حول داده معرفی می‌شود، سپس بحث حریم خصوصی و حفاظت از داده‌ها از زاویه مدل‌های دانشگاهی معرفی می‌شود. در ادامه مدل حفاظت از داده‌ها براساس آموزه‌های زنجیره ارزش داده‌ها اصلاح می‌شود و سپس اصول قانون اساسی و موادی از قوانین مصوب مجلس شورای اسلامی که به‌نحوی با حریم خصوصی مرتبط هستند در مدل مربوط به حریم خصوصی نگاشت می‌شوند. به این ترتیب خلأهای قانونی و مواد قانونی مرتبط با حریم خصوصی که باید در بررسی هر پیش‌نویس طرح یا لایحه صیانت از داده‌ها مورد توجه قرار گیرد شناسایی می‌شود.

1. Data Economy

مفهوم‌شناسی حریم خصوصی و طبقه‌بندی انواع موضوعات

حریم خصوصی از زاویه دید زنجیره ارزش داده

زنجیره ارزش مفهومی است که زنجیره کامل فعالیت‌های یک کسب‌وکار در خلق یک محصول و خدمت را توصیف می‌کند. زنجیره ارزش به‌عنوان یک ابزار تحلیلی می‌تواند بر جریان داده اعمال شود تا خلق ارزش از طریق فناوری داده درک شود. این نگرش مفهومی می‌تواند برای شناسایی بازیگران زیست‌بوم داده‌ها مورد استفاده قرار گیرد. زنجیره ارزش داده‌ها فرایند خلق داده و استفاده از آن را از مرحله شناخت به نیاز به آن تا استفاده نهایی از آن و باز استفاده از آن را توصیف می‌کند.[۳] به بیان دیگر در یک زنجیره ارزش داده جریان اطلاعات به‌عنوان مجموعه‌ای متوالی از گام‌ها توصیف می‌شود که برای خلق ارزش و بینش‌های مفید از داده کاربرد دارد. شکل ۱ نمونه‌ای از یک زنجیره ارزش داده‌ها در موضوع داده‌های بزرگ را نشان می‌دهد.

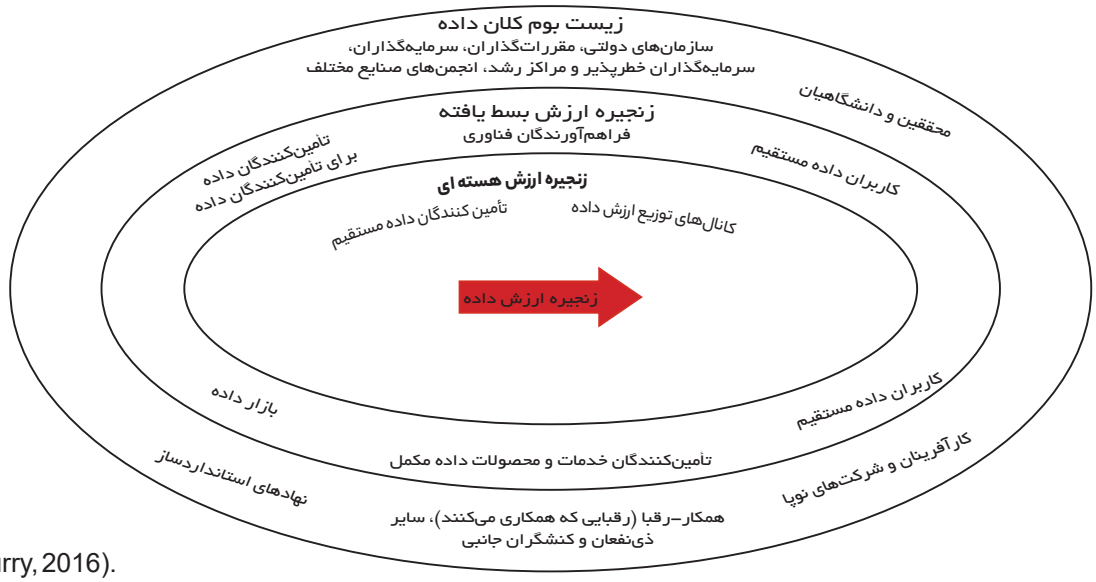
شکل ۱. مراحل زنجیره ارزش داده‌ها

جمع‌آوری داده	تحلیل داده	گزینش داده	ذخیره داده	کاربرد داده
فرایند گردآوری، تصفیه و پالایش داده‌ها قبل از قرار گرفتن آن‌ها در انباره داده‌ها یا هر راهکار ذخیره‌سازی جهت تحلیل داده‌ها	قابل استفاده کردن داده‌های خام اولیه برای تصمیم‌گیری که شامل پیمایش، تبدیل و مدل‌سازی داده با هدف برجسته‌سازی داده مرتبط و استخراج اطلاعات پنهان و سودمند و دارای قابلیت بالا برای تحقق اهداف کسب‌وکار می‌شود.	مدیریت فعال داده‌ها در طول دوره عمر آن برای اطمینان از حفظ الزامات کیفیت آن جهت استفاده مؤثر، شامل خلق محتوا، انتخاب، طبقه‌بندی، تبدیل، اعتبارسنجی و حفاظت می‌شود.	ماندگاری و مدیریت داده‌ها به صورت مقیاس‌پذیر که کاربردهایی که به دسترسی سریع به داده‌ها نیاز دارند را ممکن می‌کند.	شامل فعالیت‌های کسب‌وکاری مبتنی‌بر داده‌ها که به دسترسی به داده‌ها، تحلیل آن‌ها و ابزارهایی برای یکپارچه‌سازی تحلیل داده‌ها در ارتباط با فعالیت کسب‌وکاری نیاز است.

Source: (Curry, 2016).

طبق دیدگاه کمیسیون اروپا زنجیره ارزش داده به‌مثابه «مرکز اقتصاد دانش آینده، فراهم‌آورنده فرصت‌های توسعه دیجیتالی برای بخش‌های سنتی‌تر (از قبیل حمل‌ونقل، خدمات مالی، بهداشت، تولید و خُرده‌فروشی) عمل می‌کند». یعنی یک زیست‌بوم کامل از بازیگران در موضوع زنجیره ارزش داده درگیر می‌شوند که حوزه‌های مختلفی را از بخش بهداشت و درمان تا فروشگاه‌ها و خدمات حمل‌ونقل را دربر می‌گیرند. شکل ۲ نمونه‌ای از زیست‌بوم زنجیره ارزش داده‌ها را نشان می‌دهد.

شکل ۲. زیست‌بوم زنجیره ارزش داده‌ها



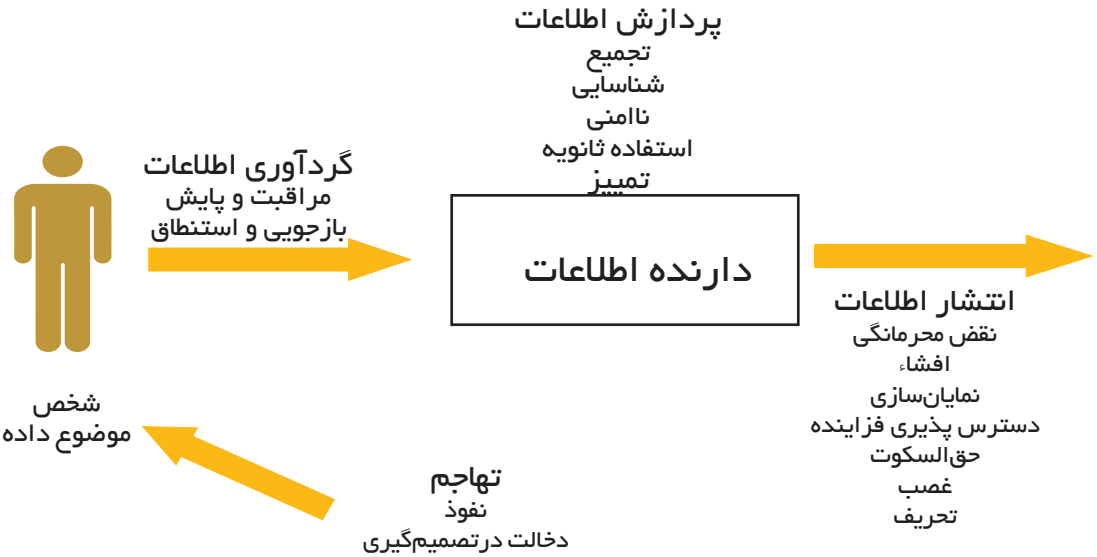
Source: (Curry, 2016).

همان‌طور که در شکل ۲ مشاهده می‌شـود، زنجیره ارزش داده‌ها در مورد هر نوع کسب‌وکاری قابل ترسیم است. اما فراهم‌آورندگان فناوری حوزه‌های مختلف را متحول کرده و به شـکل‌گیری انواع جدیدی از زنجیـره ارزش داده‌ها در حوزه‌های مختلف کمـک می‌کنند. اجزای مختلف بازیگران زنجیره ارزش داده در زیر فهرست شده‌اند:[۳]

- **تأمین‌کنندگان داده:** شـخص یا سـازمان (بنگاه‌های اقتصادی بزرگ و کوچک و متوسط) که از منابع عمومی و خصوصی، داده را خلق، گردآوری، تجمیع و تبدیل می‌کنند.
- **تأمین‌کنندگان فناوری:** معمولاً سـازمان‌هایی (بزرگ و کوچک و متوسط) که ابزارها، سـکوها، خدمات و دانش شیوه مدیریت داده را فراهم می‌آورند.
- **کاربران نهایی:** فرد یا سازمان‌های مختلف که از بخش‌های مختلف صنایع (بخش خصوصی و عمومی) که از خدمات و فناوری داده برای مزیت‌های خودشان بهره می‌گیرند.
- **بازار داده:** شخص یا سازمانی که داده را از منتشرکنندگان مختلف میزبانی می‌کند و به کاربران نهایی/مصرف‌کنندگان عرضه می‌کند.
- **کارآفرینان و شـرکت‌های نوپا:** توسـعه‌دهندگان خدمات، محصولات و فناوری‌های مبتنی‌بر داده خلاقانه.
- **محققان و دانشگاهیان:** کسانی که الگوریتم‌های جدید، فناوری‌ها و روش‌شناسی‌های مختلف، مدل‌های کسب‌وکار و جنبه‌های اجتماعی مورد نیاز پیشرفت داده را بررسی می‌کنند.
- **مقرراتگذاران:** مقرراتگذاران حریم خصوصی و جنبه‌های حقوقی.
- **نهادهای استانداردساز:** نهادهایی که استانداردهای فناورانه (رسمی و دفاکتو) ارتقای پذیرش جهانی فناوری داده را تدوین می‌کنند.
- **سرمایه‌گذاران، صندوق‌های خطرپذیر و مراکز رشد:** شخص یا نهادهایی که منابع و خدمات را جهت توسـعه قابلیت‌های تجاری زیست‌بوم فراهم می‌آورند.

داده یک بخش اساسی از این فعالیت‌هاست و درنتیجه حریم خصوصی نیز در این زمینـه اهمیت دارد، گرچه در مـورد اینکه حریم خصوصی و ابعاد آن چیسـت اتفاق‌نظر وجود ندارد. اما بـرای تفاهم پیرامون این موضوع تلاش‌هایی صورت گرفته است. در مقاله الگوی صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه،[۵] نویسندگان با مطالعه تمامی کشورهای دارای قانون در حوزه حریم خصوصی اطلاعاتی، شامل ۵۸ کشور مدلی در ۷ بُعد شامل: ۱. الزامات گردآوری داده‌های شخصی شـهروندان، ۲. الزامات استفاده از داده‌های شخصی شهروندان، ۳. الزامات نگهداری داده‌های شخصی شهروندان، ۴. الزامات افشـای داده‌های شخصی شهروندان، ۵. حقوق شهروند در زمینه حریم خصوصی اطلاعاتی، ۶. مسئولیت‌های کنترلگر داده‌های شـخصی و ۷. الزامات دسترسی شهروند به داده‌های شخصی پیشنهاد شده‌است. از بین ۱۲۴ الزام شناسایی شده برای حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک به‌عنوان شاخص‌های این ابعاد، ۱۰۵ الزام از سوی نویسندگان به‌عنوان اصول استاندارد جهانی برای کشورهای در حال توسعه جهت ضابطه‌مند ساختن توسعه دولت الکترونیک در زمینه حفظ حریم خصوصی اطلاعاتی شهروندان پیشنهاد شده اسـت. با توجه به گستردگی و مشـابهت زیاد میان شاخص‌های شناسایی شده در مقاله مورد اشـاره به یک طبقه‌بندی جداگانه از این شاخص‌ها نیاز خواهد بود که مطالعه‌ای جدا می‌طلبد. طبقه‌بندی سولو از حریم خصوصی[۸] نمونه‌ای از یک مدل اسـت که حریم خصوصی را براسـاس فعالیت‌های مرتبط با حریم خصوصی نشان می‌دهد. شکل ۳ مدل سولو از انواع مختلف جوانب حریم خصوصی را نشان می‌دهد:

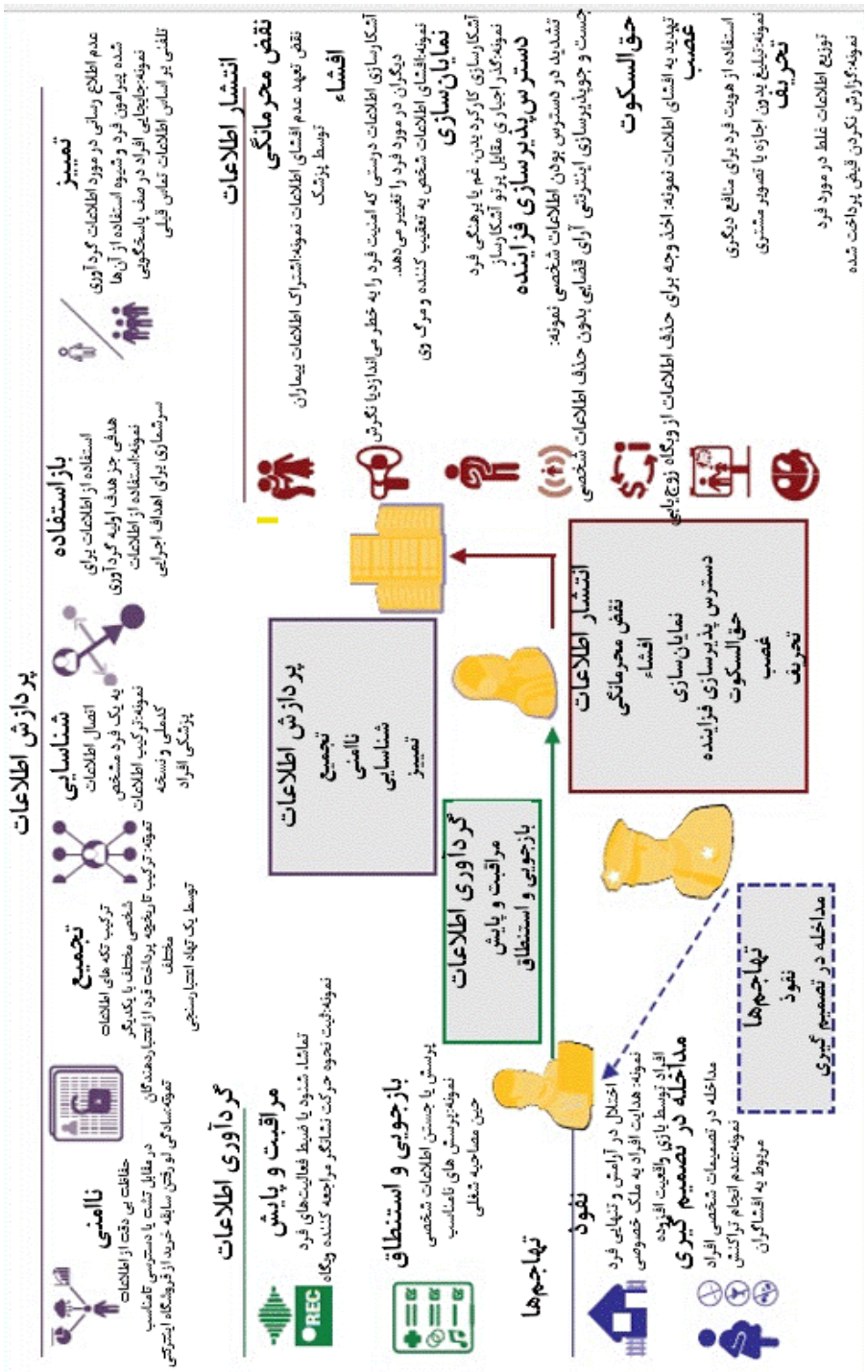
شکل ۳. طبقه‌بندی فعالیت‌های مرتبط با حریم خصوصی



Source[۸]:

همان‌طور که در شکل ۳ مشاهده می‌شود، انتشار اطلاعات،[1] پردازش اطلاعات، گردآوری اطلاعات و تهاجم‌ها چهار دسته از کردارهای مهمی هستند که حریم خصوصی در مورد آنها به مسئله تبدیل می‌شود. این کردارها خود مجموعه‌ای از زیرکردارها هســـتند که جنبه‌های حریم خصوصی را به‌صورت تشـــریحی‌تر بیان می‌کنند. در شکل ۴ این ابعاد حریم خصوصی به‌صورت تشریحی‌تر بیان شده‌اند.

شکل ۴.طبقه‌بندی تشریحی فعالیت‌های مربوط به حریم خصوصی



Source[9] :

1. Information dissemination

همان‌طور که در شکل ۴ مشاهده می‌شود حریم خصوصی در انواع مختلف کردارها می‌تواند محل توجه باشد. هرکدام از این جوانب نقض حریم خصوصی، می‌تواند در بخشی از قوانین و مقررات مربوط به حفاظت از داده و حریم خصوصی مورد بررسی قرار گیرد. با توجه به اینکه چارچوب سولو براساس قوانین ایالات متحده آمریکا تدوین شده است؛ لذا به‌خوبی می‌تواند تحلیل قوانین این کشور را در حوزه حریم خصوصی ممکن کند و با معیار قرار دادن این چارچوب می‌توان مقایسه دقیق‌تری میان قوانین و مقررات کشور ایران و آمریکا در زمینه حریم خصوصی داشت. گرچه بعضی از مواردی که در این مدل بیان شده‌اند در سایر مدل‌های مربوط به کشورهای دیگر به صورت‌های دیگر نیز صورت‌بندی شده‌اند، مثلاً بازاستفاده از داده‌ها در این مدل که به‌صورت یکی از کردارهای نقض حریم خصوصی به‌شمار می‌رود، در مدل‌های منبعث از قانون عمومی صیانت از داده‌های اتحادیه اروپا به‌عنوان حق محدودسازی هدف[1] صورت‌بندی شده‌اند.[10] اما از زاویه دید زنجیره ارزش داده این مدل نقص‌هایی دارد؛ مثلاً در موضوعاتی از جنس ترک فعل مانند سلب اختیار از ترابردپذیری داده‌های[2] شخصی بین ارائه‌دهندگان خدمات یکسان[11] یا پنهان‌کاری در مورد اقدامات علیه امنیت داده‌های شخصی، مثلاً نقض حق کاربر در مطلع شدن پیرامون نشت داده‌های شخصی وی در این مدل به‌وضوح بیان نشده است. همچنین مبحث قلمرو قضایی داده‌ها[3] و الزام به ذخیره و پردازش داده‌های شهروندان و اتباع آن کشور در داخل کشور نیز در مدل مغفول است در حالی که این موارد از موضوعات مهم حریم خصوصی و حفاظت از داده‌ها هستند.[4]

هر مدلی که در مراجع علمی تدوین می‌شود قابل تقویت است و چارچوب سولو نیز از این دو جنبه قابل بهبود است. با معیار قرار دادن این چارچوب در فصل بعدی نتیجه بررسی بعضی از قوانین مرتبط با حریم خصوصی بیان می‌شود. البته باید توجه داشت که اگر مدل‌های بومی در این حوزه تدوین شود احتمالاً خلأهای قانونی بیشتری قابل احصا خواهد بود و خلأهای قانونی که در ادامه شناسایی می‌شوند، همه خلأهای قانونی این حوزه نیستند.

احکام حفاظت از داده در قوانین ایران

حفاظت از داده در کشورمان در اسناد بالادستی و قوانین مختلفی مورد توجه قرار گرفته است. اصول (۲۲)، (۲۳) و (۲۵) قانون اساسی صراحتاً در مورد حفاظت از حریم خصوصی است. مهم‌ترین قوانینی که بخش‌هایی از موضوعات حفاظت از داده‌ها را دربر می‌گیرند عبارتند از: ۱. قانون تجارت الکترونیکی (مصوب ۱۳۸۲)، ۲. قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات (مصوب ۱۳۸۲)، ۳. قانون جرائم رایانه‌ای (مصوب ۱۳۸۸)، ۴. قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند (مصوب ۱۳۸۶)، ۵. قانون ارتقای سلامت نظام اداری و مقابله با فساد (مصوب ۱۳۹۰)، ۶. قانون انتشار و دسترسی آزاد به اطلاعات (مصوب ۱۳۸۷)، ۷. قانون پایانه‌های فروشگاهی و سامانه مؤدیان مصوب ۱۳۹۸، ۸. قانون برنامه پنج‌ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۴۰۰-۱۳۹۶)، ۹. قانون مدیریت داده‌ها و اطلاعات ملی (مصوب ۱۴۰۱). متن این قوانین در پیوست ۱ ذکر شده است. این قوانین در چارچوب سولو به شرح زیر قابل انطباق هستند:

جدول ۱. قوانین ایران در چارچوب سولو ارتقا یافته

ابعاد کلان	ابعاد خُرد	قوانین مرتبط
گردآوری اطلاعات	مراقبت و پایش	اصول (۲۲)، (۲۳) و (۲۵) قانون اساسی، بند «ف» ماده (۳) قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات مصوب ۱۳۸۲، ماده (۶۶۷)، (۶۶۸)، (۶۶۹)، (۶۷۰) و (۶۸۳) قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳، ماده (۲) و (۵) قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و ماده (۵) قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب ۱۳۸۶
	بازجویی و استنطاق	ماده (۵۸) قانون تجارت الکترونیکی، ماده (۱۵۳)، تبصره «۳» ماده (۶۷۳)، (۶۷۴)، (۶۷۵)، (۶۷۶)، (۶۷۷)، (۶۷۸)، (۶۷۹)، (۶۸۱)، (۶۸۲) قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی، مصوب ۱۳۹۳

1. Purpose Limitation
2. Data Portability
3. Data Jurisdiction

۴. با توجه به سلطه جهانی شرکت‌های فناوری ایالات متحده آمریکا پیگیری این سیاست‌ها با توجه به تأثیر روی بهبود رقابت با خدمات این شرکت‌ها، می‌تواند به کاهش سلطه شرکت‌های فناوری این کشور منجر شود.

ابعاد کلان	ابعاد خُرد	قوانین مرتبط
پردازش اطلاعات	تجمیع	
	ناامنی	ماده (۶۵۰)، (۶۵۱)، (۶۵۶)، (۶۵۸)، (۶۶۰)، (۶۶۱) و (۶۸۴) قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی، مصوب ۱۳۹۳ و ماده (۵) قانون جرائم رایانه‌ای، مصوب ۱۳۸۸
	شناسایی	ماده (۵۸) و (۷۱) تا (۷۳) قانون تجارت الکترونیکی
	بازاستفاده	بند «ب» ماده (۵۹) و (۷۱) تا (۷۳) قانون تجارت الکترونیکی
	تمییز	بند «د» ماده (۵۹) و (۷۱) تا (۷۳) قانون تجارت الکترونیکی
تهاجم‌ها	نفوذ	
	مداخله در تصمیم‌گیری	
انتشار اطلاعات	نقض محرمانگی	ماده (۱۷) قانون ارتقای سلامت نظام اداری و مقابله با فساد مصوب ۱۳۹۰، ماده (۱۵) قانون پایانه‌های فروشگاهی و سامانه مؤدیان مصوب ۱۳۹۸، ماده (۱۲) قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱، بند «الف» ماده (۷۴) قانون برنامه پنج‌ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۴۰۰-۱۳۹۶)
	افشا	ماده (۵۸) و (۶۸) قانون تجارت الکترونیکی، تبصره «۲» ماده (۶۵۰) و بند «ت» ماده (۶۵۳) قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی، مصوب ۱۳۹۳ ماده (۱۷) قانون ارتقای سلامت نظام اداری و مقابله با فساد مصوب ۱۳۹۰، ماده (۱۵) قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷، ماده (۱۵) قانون پایانه‌های فروشگاهی و سامانه مؤدیان، مصوب ۱۳۹۸
	نمایان‌سازی	ماده (۵) قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب ۱۳۸۶
	دسترس‌پذیرسازی فزاینده	
	حق‌السکوت	بند «هـ» ماده (۵۹) و ماده (۶۸) قانون تجارت الکترونیکی
	غصب	
	تحریف	بند «ج» ماده (۵۹) و مواد (۶۷) و (۶۸) قانون تجارت الکترونیکی، ماده (۲۱) قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷، ماده (۱۶) قانون جرائم رایانه‌ای، مصوب ۱۳۸۸
ترک فعل‌های مهم	سلب اختیار از ترابردپذیری داده‌های شخصی	
	پنهان‌کاری در مورد اقدامات علیه امنیت داده‌های شخصی	
	قلمرو قضایی داده‌ها	

همان‌طور که در جدول ۱ مشاهده می‌شود، در ایران قوانینی که حریم خصوصی را از جنبه تجمیع داده‌ها بررسی کند وجود ندارند. گرچه قوانین و برنامه‌های متعددی برای تجمیع اطلاعات شهروندان در موضوعات یارانه‌ها در دستور کار قرار دارد و بازاستفاده از داده‌های شهروندان برای اهدافی جز اهداف اولیه در دستور کار است که البته با توجه به اینکه متقاضیان یارانه نسبت به این امر رضایت دارند، این موضوع قابل توجیه است، اما ذخیره و نگهداری اطلاعات افرادی که متقاضی دریافت یارانه نیستند، محل اشکال است. در موضوع تهاجم‌ها (اعم از نفوذ و مداخله در تصمیم‌گیری‌ها) نیز قوانین صریحی که موضوع را به‌خوبی پوشش دهند وضع نشده است. همین‌طور دسترس‌پذیر ساختن فزاینده در قوانین فعلی به‌خوبی مورد توجه قرار نگرفته است. ترک فعل‌های مهمی همچون سلب اختیار از ترابردپذیری داده‌های شخصی و پنهان‌کاری در مورد اقدامات علیه امنیت داده و رعایت قلمرو قضایی داده‌ها در قوانین قبلی مشاهده نشد. قانون تجارت الکترونیکی به‌تنهایی بخش‌های زیادی از موضوع حریم خصوصی را پوشش می‌دهد، اما وجود مواد قانونی به‌معنای این نیست که این قوانین کامل هستند و نیاز به بازنگری ندارند. زیرا چارچوب نظری بسیاری از سایر جنبه‌های قانون مانند تعیین متولی اجرای قانون و تدوین آیین‌نامه اجرایی و ضمانت اجرای قوانین را پوشش نمی‌دهد و این موارد باید با مقایسه متون قانونی با یکدیگر حاصل شود. مشروح قوانین در پیوست ۱ گزارش ذکر شده‌اند.

جمع‌بندی

مقایسه چارچوب نظری حریم خصوصی و حفاظت از داده‌های شخصی، خلأهای قانونی را در زمینه حفاظت از داده‌ها نشـــان می‌دهد. یکی از حقوق شخص موضوع داده این اســـت که اطلاعاتی که از او نزد مراجع مختلف قرار دارد بدون اجـــازه وی تجمیع و بـــه حریم خصوصی وی تجاوز نشـــود. قوانینی که به‌صورت مستقیم موضوع تهاجم‌ها به حریم خصوصی را پوشش دهند در بررســـی‌ها یافت نشده است و در مبحث انتشار اطلاعات موضوعاتی همچون دسترس‌پذیرسازی فزاینده که با دیجیتالی شدن و الکترونیکی شدن اسناد قدیمی رو به افزایش نیز است در تدابیر قانونی پوشش داده نشده است. غصب اطلاعات و انتفاع مادی از افشای اطلاعات شخصی دیگران نیز در قوانین مغفول مانده است. ترک فعل‌های مهم در زمینه ترابردپذیری و اطلاع‌رسانی در زمینه اقدامات علیه امنیت سایبری و رعایت قلمرو قضایی داده‌ها نیز در قوانین موضوعه نیازمند توجه اســـت. رفع خلأهای قانونی نیازمند بررســـی محتوایی تجارب متکثر جهانی و ایجاد راه‌حل‌های بومی اســـت. در گزارش‌های بعدی با مقایسه قانون اساسی، قوانین فدرال، قوانین ایالتی و درنهایت قوانین و پیش‌نویس لوایح قانونی مربوط به حفاظت از داده‌ها در کنگره ایالات متحده آمریکا در یک چارچوب واحد به‌صورت محتوایی مقررات حفاظت از داده‌های ایران و ایالات متحده آمریکا مقایسه می‌شوند.

منابع و مآخذ

1. Lauren , Zabierek , Bolton Tatyana , Pugh Brandon, Lesmes Sofia , and Simpson Cory . 2022. The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation. https://www.belfercenter.org/publication/role-federal-trade-commission-federal-data-security-and-privacy-legislation.
2. Bannan, Karen. 2019. China's Data Protection Laws Go Further Than GDPR. https://www.infogoto.com/chinas-data-protection-laws-go-further-than-gdpr/.
3. Curry, E. (2016). The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches. In J. M. Cavanillas, E. Curry, & W. Wahlster (Eds.), New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe (pp. 2937-). Springer International Publishing. https://doi.org/10.1007/9783_3-21569-319-3-
4. Congress. 2020. S.3300 - Data Protection Act of 2020. 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.
5. Cooley, LLP. 2018. Worldwide: Brazil's New Data Protection Law: The LGPD. http://www.mondaq.com/brazil/x/737694/data+protection/Brazils+New+Data+Protection+Law+The+LGPD.
6. Cornel .2022 .Privacy .https//:www.law.cornell.edu/wex/privacy.
7. Enterprivacy Consulting Group .2018 .A TAXONOMY OF PRIVACY .enterprivacy.
8. FTC .2022 . FTC Policy Work .https//:www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/ftc-policy-work.
9. Green, Andy. 2021. Complete Guide to Privacy Laws in the US. Varonis. https://www.varonis.com/blog/us-privacy-laws.
10. i-scoop. 2022. Data portability under the GDPR: the right to data portability explained. https://www.i-scoop.eu/right-to-data-portability/.
11. Klosowski, Thorin. 2021. The State of Consumer Data Privacy Laws in the US (And Why It Matters). https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
12. Knabke, Tobias, and Sebastian Olbrich. 2015. "Exploring the future shape of business intelligence: mapping dynamic capabilities of information systems to business intelligence agility." Twenty-first Americas Conference on Information Systems. Puerto Rico,.
13. LAZARUS, DAVID. 2018 . Column: Months after Equifax data breach, we're still no closer to privacy protections. https://www.latimes.com/business/lazarus/la-fi-lazarus-cybersecurity-data-breaches-20180102-story.html.
14. NCLS. 2022. State Laws Related to Digital Privacy. 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. Newlands, Gemma , Christoph Lutz, and Christian Fieseler. 2019. "Trading on the Unknown: Scenarios for the Future Value of Data." Law & Ethics of Human Rights.
16. PWC. 2020. Privacy megatrend: Race to own the data-value chain. https://www.pwc.com/us/en/services/

consulting/cybersecurity-risk-regulatory/library/seven-privacy-megatrends/data-value-chain.html.
17. Sacks, Samm. 2018. New China Data Privacy Standard Looks More Far-Reaching than GDPR. https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.
18. Smith, Marcia , John Moteff , and Lennard Kruger. 2004. Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth. CRS.
19. Solove, D. J. 2006. "A taxonomy of privacy." University of Pennsylvania law review.

پیوست

پیوست ۱. بعضی احکام حفاظت از داده‌ها در اسناد بالادستی و قوانین جمهوری اسلامی ایران

۱ حفاظت از داده در قانون اساسی

اصل بیست‌ودوم

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

اصل بیست‌وسوم

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

اصل بیست‌وپنجم

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.

اصل چهل‌وششم

هرکس مالک حاصل کســـب‌وکار مشروع خویش اســـت و هیچ‌کس نمی‌تواند به‌عنوان مالکیت نسبت به کسب‌وکار خود، امکان کسب‌وکار را از دیگری سلب کند.

۲ حفاظت از داده در قانون تجارت الکترونیک، مصوب ۱۳۸۲

فصل سوم قانون تجارت الکترونیکی، مصوب ۱۳۸۲ با عنوان حمایت از داده‌ها (Data Protection) بعضی احکام عمومی در زمینه حفاظت از داده‌ها دارد و در ماده (۶۰) و (۷۹) وزارت بهداشت تکالیفی در زمینه حفاظت از داده‌های مربوط به سلامت دارد. ماده (۲) این قانون نیز تعاریفی دارد که در موضوع حفاظت از داده‌ها قابل استفاده است، مواد مرتبط با حمایت از داده‌ها در قانون تجارت الکترونیکی در زیر فهرست شده‌اند:

ماده (۲)

الف) «داده پیام» (Data Message): هر نمادی از واقعه، اطلاعات یا مفهوم است که با وســـایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال دریافت، ذخیره یا پردازش می‌شود.

ب) «اصل‌ساز» (Originator): منشأ اصلی «داده پیام» است که «داده پیام» به‌وسیله او یا از طرف او تولید یا ارسال می‌شود، اما شامل شخصی که در خصوص «داده پیام» به‌عنوان واسطه عمل می‌کند، نخواهد شد.

ج) «مخاطب» (Addressee): شخصی است که اصل‌ساز قصد دارد وی «داده پیام» را دریافت کند، اما شامل شخصی که در ارتباط با «داده پیام» به‌عنوان واسطه عمل می‌کند، نخواهد شد.

د) «ارجاع در داده پیام» (Incorporation By Reference): یعنی به منابعی خارج از «داده پیام» عطف شود که در صورت مطابقت با ماده (۱۸) این قانون جزئی از «داده پیام» محسوب می‌شود.

هـ) «تمامیت داده پیام» (Integrity): عبارت است از موجودیت کامل و بدون تغییر «داده پیام». اَعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به‌طور معمول انجام می‌شود خدشه‌ای به تمامیت «داده پیام» وارد نمی‌کند.

و) «سیستم رایانه‌ای» (Computer System): هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری ـ نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده پیام» عمل می‌کند.

ز) «سیستم اطلاعاتی» (Information System): سیستمی برای تولید (اصل‌سازی) ارسال دریافت، ذخیره یا پردازش «داده پیام» است.

ح) «سیستم اطلاعاتی مطمئن» (Secure Information System): سیستم اطلاعاتی است که:

۱. به‌نحوی معقول در برابر سوءاستفاده و نفوذ محفوظ باشد.
۲. سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد.
۳. به‌نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازمان‌دهی شده باشد.
۴. موافق با رویه ایمن باشد.

ط) «رویه ایمن» (Secure Method): رویه‌ای است برای تطبیق صحت ثبت «داده پیام» منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره‌سازی «داده پیام» از یک زمان خاص. یک رویه ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود.

ی) «امضای الکترونیکی» (Electronic Signature): عبارت از هر نوع علامت منضم شده یا به‌نحو منطقی متصل شده به «داده پیام» است

که برای شناسایی امضاکننده «داده پیام» مورد استفاده قرار می‌گیرد.
ک) «امضـای الکترونیکی مطمئـن» (Secure/Enhanced/Advanced Electronic Signature): هر امضای الکترونیکی است که مطابق با ماده (۱۰) این قانون باشد.
ل) «امضاکننده» (Signatory): هر شـخص یـا قائم مقام وی که امضای الکترونیکی تولید می‌کند.
م) «شخص» (Person): اعم اسـت از شخص حقیقی و حقوقی و یا سیستم‌های رایانه‌ای تحت کنترل آنان.
ن) «معقول» (سنجش عقلانی)، (Reasonableness Test): با توجه به اوضاع و احوال مبادلـه «داده پیام» از جمله: طبیعت مبادله، مهارت و موقعیت طرفین، حجم مبادلات طرفین در موارد مشـابه، در دسترس بودن گزینه‌های پیشنهادی و رد آن گزینه‌ها از جانب هریک از طرفین، هزینه گزینه‌های پیشنهادی، عرف و روش‌های معمول و مورد استفاده در این نوع مبادلات، ارزیابی می‌شود.
س) «مصرف کننـده» (Consumer): هـر شـخصی اسـت که به‌منظوری جز تجارت یا شغل حرفه‌ای اقدام می‌کند.
ع) «تأمین کننده» (Supplier): عبارت از شـخصی است که بنابه اهلیت تجاری، صنفی یا حرفه‌ای فعالیت می‌کند.
ف) «وسایل ارتباط از راه دور» (Means Of Distance Communication): عبارت از هر نوع وسـیله‌ای است که بدون حضور فیزیکی هم‌زمان تأمین کننـده و مصرف‌کننده جهـت فروش کالا و خدمات استفاده می‌شود.
ص) «عقد از راه دور» (Distance Contract): ایجاب و قبول راجع به کالاها و خدمات بین تأمین‌کننده و مصرف‌کننده با استفاده از وسایل ارتباط از راه دور است.
ق) «واسـط بادوام» (Durable Medium): یعنی وسـایلی که به‌موجب آن مصرف‌کننده بتواند شـخصاً «داده پیام»های مربوطه را بر روی آن ذخیره کند، از جمله شـامل فلاپی‌دیسک، دیسک فشرده، دیسک سخت و یا پست الکترونیکی مصرف‌کننده.
ر) «داده پیام‌هـای شـخصی» (Private Data): یعنـی «داده پیام»های مربوط به یک شـخص حقیقی (موضـوع «داده» Data Subject) مشخص و معین.
طبق ماده (۵۸) این قانون ذخیره، پردازش و یا توزیع «داده پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشـخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است. در ماده (۵۹) به‌شرط رضایت شخص موضوع «داده پیام» و به‌شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع «داده پیام»های شـخصی 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 متناسـب با اهدافی که در هنگام جمع‌آوری برای شـخص موضوع «داده پیام» شـرح 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 شـخصی مربوط به خود دسترسی داشـته 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.
در ماده (۶۰) ذخیره، پردازش و یا توزیـع «داده پیام»های مربوط به سوابق پزشکی و بهداشتی به آیین‌نامه‌ای موکول شده است طبق ماده (۷۹) این قانون خواهد آمد.

ماده (۶۱)
سایر موارد راجع به دسترسی موضوع «داده پیام»، از قبیل استثنائات، افشای آن برای اشـخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان «داده پیام»های شخصی به‌موجب مواد مندرج در باب چهارم این قانون و آیین‌نامه مربوطه خواهد بود.

باب چهارم ـ جرائم و مجازات‌ها

مبحث اول ـ کلاهبرداری کامپیوتری

ماده (۶۷)
هر کس در بسـتر مبادلات الکترونیکی، با سوءاسـتفاده و یا استفاده غیرمجاز از «داده پیام»ها، برنامه‌ها و سیسـتم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالـی نظیر ورود، محو، توقف «داده پیام»، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود.
تبصره ـ شروع به این جرم نیز جرم محسـوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد.

فصل دوم ـ نقض حمایت از «داده پیام»های شخصی حمایت از داده

ماده (۷۱)
هر کس در بسـتر مبادلات الکترونیکی شـرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.

ماده (۷۲)
هرگاه جرائم راجع به «داده پیام»های شـخصی توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در ماده (۷۱) این قانون محکوم خواهد شد.

ماده (۷۳)
اگر به‌واسـطه بی‌مبالاتی و بی‌احتیاطی دفاتـر خدمات صدور گواهی الکترونیکی جرائم راجع به «داده پیام»های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون (۵۰،۰۰۰،۰۰۰) ریال محکوم می‌شود.

قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، مصوب ۱۳۸۲

ماده (۳)

وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات:

ف) حفاظت و حراست و عدم ضبط و افشای انواع مراسلات و امانات پستی و همچنین مکالمات تلفنی و مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی طبق قانون.

۲. کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده)، مصوب ۱۳۷۵

کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) مصوب ۱۳۷۵

فصل اول ـ در جرائم ضدامنیت داخلی و خارجی کشور

ماده (۸)

هرکس با هدف بر هم زدن امنیت کشور به هر وسیله اطلاعات طبقه‌بندی شده را با پوشش مسئولین نظام یا مأمورین دولت یا به‌نحو دیگر جمع‌آوری کند چنانچه بخواهد آن را در اختیار دیگران قرار دهد و موفق به انجام آن شود به حبس از ۲ تا ۱۰ سال و در غیر این صورت به حبس از ۱ تا ۵ سال محکوم می‌شود.

ماده (۹)

چنانچه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی شده می‌باشند و به آنها آموزش لازم داده شده است در اثر بی‌مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند به ۱ تا ۶ ماه حبس محکوم می‌شوند.

ماده (۴۰)

افشای اطلاعات مربوط به هویت و محل اقامت بزه‌دیده، شهود و مطلعان و سایر اشخاص مرتبط با پرونده توسط ضابطان دادگستری، جز در مواردی که قانون معین می‌کند، ممنوع است.

ماده (۱۰۱)

بازپرس مکلف است در مواردی که دسترسی به اطلاعات فردی بزه‌دیده، از قبیل نام و نام‌خانوادگی، نشانی و شماره تلفن، احتمال خطر و تهدید جدی علیه تمامیت جسمانی و حیثیت بزه‌دیده را به‌همراه داشته باشد، تدابیر مقتضی را برای جلوگیری از دسترسی به این اطلاعات اتخاذ کند. این امر در مرحله رسیدگی در دادگاه نیز به تشخیص رئیس دادگاه و با رعایت مصالح بزه‌دیده اعمال می‌شود.

ماده (۱۵۳)

مقامات و مأموران وزارتخانه‌ها، سازمان‌ها، مؤسسات دولتی، شرکت‌های دولتی، مؤسسات یا نهادهای عمومی غیردولتی و نهادها و شرکت‌های وابسته به آنها، سازمان‌های نظامی و انتظامی، بانک‌ها و مؤسسات مالی و اعتباری، دفاتر اسناد رسمی و دستگاه‌هایی که شمول قانون بر آنها مستلزم ذکر نام است مکلفند اسباب، ادله و اطلاعات راجع به جرم و آن قسمت از اوراق و اسناد و دفاتری را که مراجعه به آنها برای تحقیق امر کیفری لازم است، به درخواست مرجع قضایی در دسترس آنان قرار دهند، مگر در مورد اسناد سری و به‌کلی سری که این درخواست باید با موافقت رئیس قوه قضائیه باشد. متخلف از این ماده، درصورتی که عمل وی برای خلاصی متهم از محاکمه و محکومیت نباشد، حسب مورد به انفصال موقت از خدمات دولتی یا عمومی از سه ماه تا یک سال محکوم می‌شود.

تبصره ـ درخصوص اسناد سری و به‌کلی سری مربوط به نیروهای مسلح رئیس قوه قضائیه می‌تواند اختیار خود را به رئیس سازمان قضایی نیروهای مسلح تفویض کند.

قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی، مصوب ۱۳۹۳

بخش هشتم ـ آیین دادرسی جرائم نیروهای مسلح

فصل ششم ـ ترتیب رسیدگی، صدور و ابلاغ رأی

ماده (۶۳۳)

انتشار اطلاعات مربوط به آرای دادگاه‌های نظامی ممنوع است. اما رئیس سازمان قضایی در موارد ضروری و در صورت اقتضای مصلحت، می‌تواند اطلاعات مربوط به آرای قطعی دادگاه‌های نظامی را جهت انتشار در اختیار پایگاه اطلاع‌رسانی قوه قضائیه و سازمان قضایی قرار دهد.

تبصره ـ در مواردی که به تشخیص دادستان نظامی یا رئیس سازمان قضایی، جهت پیشگیری از جرم آموزش ضروری باشد، به میزان لازم اطلاعات مربوط به احکام و فرایند رسیدگی به جرم در اختیار یگان‌ها قرار می‌گیرد.

بخش نهم ـ دادرسی الکترونیکی

ماده (۶۵۰)

به‌منظور سامان‌دهی پرونده‌ها و اسناد قضایی و ارائه بهتر خدمات قضایی و دستیابی روزآمد به آمار و گردش کار قضایی در سراسر کشور و همچنین ارائه آمار و اطلاعات دقیق و تفصیلی درخصوص جرائم، متهمان، بزه‌دیدگان و مجرمان و سایر اطلاعات قضایی، «مرکز ملی داده‌های قوه قضائیه» در مرکز آمار و فناوری اطلاعات قوه قضائیه با استفاده از افراد موثق راه‌اندازی می‌شود.

تبصره «۱» ـ نحوه و میزان دسترسی مراجع ذی‌صلاح قضایی به اطلاعات این مرکز به‌موجب آیین‌نامه‌ای است که ظرف سه ماه از تاریخ لازم‌الاجرا شدن این قانون توسط شورا تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

تبصره «۲» ـ اسناد، مدارک و اطلاعات این مرکز با رعایت قوانین و مقررات به‌موجب آیین‌نامه‌ای که ظرف سه ماه از تاریخ تصویب این قانون توسط شورا تهیه و به تصویب رئیس قوه قضائیه می‌رسد، در اختیار مراکز علمی، پژوهشکده‌ها و پژوهشگران قرار می‌گیرد. استفاده از اسناد، مدارک و اطلاعات مزبور نباید موجب هتک حرمت و حیثیت اشخاص شود. انتشار اطلاعات مربوط به هویت افراد مرتبط با دادرسی از قبیل نام، نام‌خانوادگی، شماره پستی و شماره ملی آنان جز در مواردی که قانون تجویز کند، ممنوع است.

ماده (۶۵۱)

کلیه دستگاه‌های تابعه قوه قضائیه، نظیر دیوان عدالت اداری، سازمان

بازرسی کل کشور، سازمان زندان‌ها و اقدامات تأمینی و تربیتی کشور، سازمان ثبت اسناد و املاک کشور، سازمان پزشکی قانونی، سازمان قضایی نیروهای مسلح و مراجع ذی‌ربط در عفو و بخشودگی و سجل کیفری و روزنامه رسمی جمهوری اسلامی، موظفند کلیه اطلاعات خود را در مرکز ملی داده‌های قوه قضائیه قرار دهند و آنها را روزآمد نگه دارند.

تبصره «۱»ـ آیین‌نامه اجرایی نحوه دسترسی به اطلاعات محرمانه و سری در مرکز ملی داده‌های قوه قضائیه توسط آن قوه تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

تبصره «۲»ـ مراجع انتظامی و سایر ضابطان و دستگاه‌ها، هیئت‌ها و کمیسیون‌های ذی‌ربط موظفند اطلاعات مرتبط با امور قضایی خود را در مرکز ملی داده‌های قوه قضائیه قرار دهند و آنها را روزآمد نگه دارند.

ماده (۶۵۲)

قوه قضائیه موظف است به‌منظور سامان‌دهی ارتباطات الکترونیکی بین محاکم، ضابطان و دستگاه‌های تابعه خود و نیز سایر اشخاص حقیقی و حقوقی که در جریان دادرسی به اطلاعات آنها نیاز است، «شبکه ملی عدالت» را با به‌کارگیری تمهیدات امنیتی مطمئن از قبیل امضای الکترونیکی راه‌اندازی کند. تبصره (اصلاحی ۱۰/۱۱/۱۳۹۵) مراجع قضایی می‌توانند استعلامات قضایی و کسب اطلاعات لازم را از طریق شبکه ملی عدالت به‌عمل آورند. در این صورت دستگاه‌های دولتی، نهادهای عمومی غیردولتی و شخصیت‌های حقوقی موظفند پاسخ لازم را از طریق شبکه مزبور اعلام کنند. مستنکف از مفاد این تبصره مشمول ماده (۵۷۶) قانون مجازات اسلامی ـ کتاب پنجم تعزیرات مصوب ۲/۳/۱۳۷۵ ـ است.

ماده (۶۵۳)

قوه قضائیه موظف است اطلاعات زیر را از طریق «درگاه ملی قوه قضائیه» ارائه کند و آنها را روزآمد نگه دارد.

الف) اهداف، وظایف، سیاست‌ها، خط‌مشی‌ها و ساختار کلان مدیریتی و اجرایی قوه قضائیه به‌همراه معرفی مسئولان و شرح وظایف و نحوه ارتباط با آنان،

ب) نشانی، شماره تماس و پیوند به تارنمای (وب‌سایت) تمامی معاونت‌ها و دادگستری‌های استان‌ها، دستگاه‌های تابعه قوه قضائیه، وزارت دادگستری، کانون‌های وکلای دادگستری و کارشناسان رسمی دادگستری،

پ) کلیه قوانین لازم‌الاجرا، آرای وحدت رویه هیئت عمومی دیوان عالی کشور و آرای هیئت عمومی دیوان عدالت اداری، بخشنامه‌های رئیس قوه قضائیه و نظریات مشورتی اداره حقوقی قوه قضائیه،

ت) آرای صادره از سوی محاکم در صورتی که به تشخیص قاضی اجرای احکام خلاف عفت عمومی یا امنیت ملی نباشد به‌صورت برخط (آنلاین) برای تحلیل و نقد صاحب‌نظران و متخصصان با حفظ حریم خصوصی اشخاص،

ث) خدمات معاضدت قضایی به مقامات ذی‌صلاح سایر کشورها بر پایه اسناد و معاهده‌های همکاری حقوقی بین‌المللی و اطلاعات راجع به خدمات حقوقی و قضایی به اتباع سایر کشورها،

ج) آموزش آسان و قابل درک عمومی چگونگی اقامه دعوی برای شهروندان،

چ) اطلاعات پژوهشی و علمی حقوقی ـ قضایی.

ماده (۶۵۵)

در هر مورد که به‌موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رأی، امضا، اثر انگشت، ابلاغ اوراق قضایی، نشانی و مانند آن لازم باشد صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است.

تبصره «۱»ـ در کلیه مراحل تحقیق و رسیدگی حقوقی و کیفری و ارائه خدمات الکترونیک قضایی، نمی‌توان صرفاً به‌لحاظ شکل یا نحوه تبادل اطلاعات الکترونیکی از اعتبار بخشیدن به محتوا و آثار قانونی آن خودداری نمود. قوه قضائیه موظف است سامانه‌های امنیتی لازم را جهت تبادل امن اطلاعات و ارتباطات بین اصحاب دعوی، کارشناسان، دفاتر خدمات الکترونیک قضایی، ضابطان و مراجع قضایی و سازمان‌های وابسته به قوه قضائیه ایجاد نماید.

تبصره «۲»ـ قوه قضائیه می‌تواند جهت طرح و پیگیری امور قضایی مراجعان موضوع این قانون در فضای مجازی نسبت به ایجاد دفاتر خدمات الکترونیک قضایی و جهت هماهنگی فعالیت دفاتر، نسبت به ایجاد کانون دفاتر خدمات الکترونیک قضایی، با استفاده از ظرفیت بخش خصوصی اقدام نماید. دفاتر خدمات الکترونیک قضایی می‌توانند از بین دفاتر اسناد رسمی و غیر آن انتخاب یا تأسیس شوند. آیین‌نامه اجرایی این ماده ظرف سه ماه از تاریخ لازم‌الاجرا شدن این قانون توسط شورا تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

تبصره «۳»ـ مراجعان به قوه قضائیه موظفند پست الکترونیکی و شماره تلفن همراه خود را در اختیار قوه قضائیه قرار دهند و در صورت عدم دسترسی به پست الکترونیک، مرکز آمار موظف است برای شهروندان و متقاضیان امکانات لازم برای دسترسی به پست الکترونیکی ملی قضایی جهت امور قضایی ایجاد کند.

ماده (۶۵۶)

به‌منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری اطلاعات مبادله شده میان شهروندان و محاکم قضایی، قوه قضائیه موظف است تمهیدات امنیتی مطمئن برای امضای الکترونیکی، احراز هویت و احراز اصالت را فراهم آورد.

تبصره ـ قوه قضائیه موظف است مرکز صدور گواهی ریشه برای امضای الکترونیکی را جهت ایجاد ارتباطات و مبادله اطلاعات امن راه‌اندازی نماید.

ماده (۶۵۸)

قوه قضائیه موظف است تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افـراد و تأمین امنیت داده‌های شـخصی آنان، در چارچوب اقدامات این بخش فراهم آورد.

ماده (۶۵۹)

به‌کارگیری سامانه‌های ویدئوکنفرانس و سـایر سامانه‌های ارتباطات الکترونیکی به‌منظور تحقیق از اصحاب دعوی، اخذ شهادت از شهود یا نظرات کارشناسی در صورتی مجاز است که احراز هویت، اعتبار اظهارات فرد مورد نظر و ثبت مطمئن سوابق صورت پذیرد.

ماده (۶۶۰)

چنانچه اشـخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به‌طور غیرمجاز آنها را افشا کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از ۲ تا ۵ سـال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از ۲ تا ۱۰ سال محکوم خواهند شد.

ماده (۶۶۱)

چنانچه اشخاصی که مسئول حفظ امنیت مراکز، سامانه‌های رایانه‌ای و مخابراتی و اطلاعات موضوع این بخش هسـتند یا داده‌ها یا سـامانه (سیستم)های مذکور در اختیار آنان قرار گرفته است بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم مهارت یا عدم رعایت تدابیر متعارف امنیتی موجبات ارتکاب جرائم رایانه‌ای به‌وسـیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از ۶ ماه تا ۲ سال یا انفصال از خدمت تا ۵ سال یا جزای نقدی از ده تا صد میلیون ریال محکوم خواهند شد.

بخش دهم ـ آیین دادرسی جرائم رایانه‌ای

ماده (۶۶۷)

ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا ۶ ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا ۶ ماه 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 از قبیل مبدأ، مسـیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره «۲»ـ اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (IP)، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.

ماده (۶۶۸)

ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا ۶ ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.

ماده (۶۶۹)

هرگاه حفظ داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می‌تواند دسـتور حفاظت از آنها را برای اشخاصی که به‌نحوی تحت تصرف یا کنترل دارند صادر کند. در شـرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضایی می‌توانند دستور حفاظت را صادر کنند و مراتب را حداکثر تا بیست‌وچهار ساعت به اطلاع مقام قضایی برسانند. چنانچه هریک از کارکنان دولت یا ضابطان قضایی یا سایر اشـخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشا کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضایی و کارکنان دولت به مجازات امتناع از دستور مقام قضایی و سایر اشخاص به حبس از نودویک روز تا ۶ ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات محکوم می‌شوند.

تبصره «۱»ـ حفظ داده‌ها به‌منزله ارائه یا افشای آنها نیست و مستلزم رعایت مقررات مربوط است.

تبصره «۲»ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضایی قابل تمدید است.

ماده (۶۷۰)

مقام قضایی می‌تواند دستور ارائه داده‌های حفاظت شده مذکور در مواد (۶۶۷)، (۶۶۸) و (۶۶۹) این قانون را به اشـخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. خودداری از اجرای این دسـتور و همچنین عدم نگهداری و عدم مواظبت از این داده‌ها موجب مجازات مقرر در ماده (۶۶۹) این قانون می‌شود.

ماده (۶۷۳)

دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های مورد نظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوه دسـتیابی به داده‌های رمزنگاری یا حذف شـده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می‌کند.

ماده (۶۷۴)

تفتیش داده‌ها یا سـامانه‌های رایانه‌ای و مخابراتی شـامل اقدامات ذیل می‌شود: الف) دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای یا مخابراتی،

ب) دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوح‌های فشرده یا کارت‌های حافظه، پ) دستیابی به داده‌های حذف یا رمزنگاری شده.

ماده (۶۷۵)
در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود.

ماده (۶۷۶)
در شرایط زیر سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شوند: الف) داده‌های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد. ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت‌افزاری امکان‌پذیر نباشد. پ) متصرف قانونی سامانه رضایت داده باشد. ت) تصویربرداری از داده‌ها به‌لحاظ فنی امکان‌پذیر نباشد. ث) تفتیش در محل باعث آسیب داده‌ها شود.

ماده (۶۷۷)
توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل تغییر گذرواژه به‌منظور عدم دسترسی به سامانه، مهروموم (پلمب) سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده (۶۷۸)
چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند.

ماده (۶۷۹)
توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود، ممنوع است، مگر اینکه توقیف برای اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد.

ماده (۶۸۱)
در مواردی که اصل داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت‌افزارها و نرم‌افزارهای مورد نظر و نقش آنها در جرم ارتکابی، در مهلت متناسب و متعارف برای آنها تعیین تکلیف کند.

ماده (۶۸۲)
متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ۱۰ روز به مرجع قضایی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است.

ماده (۶۸۳)
کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است.
تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است.

ماده (۶۸۴)
آیین‌نامه اجرایی نحوه نگهداری و مراقبت از ادله الکترونیکی جمع‌آوری شده ظرف ۶ ماه از تاریخ لازم‌الاجرا شدن این قانون توسط وزیر دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

۱. قانون جرائم رایانه‌ای، مصوب ۱۳۸۸

بخش یکم ـ جرائم و مجازات‌ها

فصل یکم ـ جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث دوم ـ شنود غیرمجاز

ماده (۲)
هرکس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ده میلیون (۱۰,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ جاسوسی رایانه‌ای

ماده (۵)
چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو

مجازات و انفصال از خدمت از ۶ ماه تا دو سال محکوم خواهند شد.

فصل پنجم ـ هتک حیثیت و نشر اکاذیب

ماده (۱۶)

هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به‌نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده (۱۷)

هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

۲. قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب ۱۳۸۶

ماده (۵)

مرتکبان جرائم زیر به ۲ تا ۵ سال حبس و ۱۰ سال محرومیت از حقوق اجتماعی و هفتادوچهار ضربه شلاق محکوم می‌شوند:

ب) تهیه فیلم یا عکس از محل‌هایی که اختصاصی بانوان بوده و آنها فاقد پوشش مناسب می‌باشند مانند حمام‌ها و استخرها و یا تکثیر و توزیع آن.

ج) تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران و تکثیر و توزیع آن.

۳. قانون ارتقای سلامت نظام اداری و مقابله با فساد، مصوب ۱۳۹۰

ماده (۱۷)

دولت مکلف است طبق مقررات این قانون نسبت به حمایت قانونی و تأمین امنیت و جبران خسارت اشخاصی که تحت عنوان مخبر یا گزارش‌دهنده، اطلاعات خود را برای پیشگیری، کشف یا اثبات جرم و همچنین شناسایی مرتکب، در اختیار مراجع ذی‌صلاح قرار می‌دهند و به این دلیل در معرض تهدید و اقدامات انتقام‌جویانه قرار می‌گیرند، اقدام نماید. اقدامات حمایتی عبارتند از:

الف) عدم افشای اطلاعات مربوط به هویت و مشخصات خانوادگی و محل سکونت یا فعالیت اشخاص مذکور، مگر در مواردی که قاضی رسیدگی کننده به‌لحاظ ضرورت شرعی یا محاکمه عادلانه و تأمین حق دفاع متهم افشای هویت آنان را لازم بداند. چگونگی عدم افشای هویت اشخاص یاد شده و همچنین دسترسی اشخاص ذی‌نفع، در آیین‌نامه اجرایی این قانون مشخص می‌شود.

ماده (۳۴)

هر گونه افشای اطلاعات پایگاه‌های اطلاعاتی دستگاه‌های مذکور برخلاف قوانین و مقررات، ممنوع است و متخلف به مجازات مندرج در قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۲۹/۱۱/۱۳۵۳ محکوم می‌گردد.

ماده (۳۵)

هر گونه دسترسی غیرمجاز به پایگاه‌های اطلاعاتی موضوع این قانون ممنوع است و متخلف حسب مورد به مجازات حبس از ۶ ماه تا یک سال محکوم می‌شود. شروع به جرم مزبور نیز مشمول مجازات حبس از نودویک روز تا ۶ ماه است.

۴. قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۷

ماده (۱)

در این قانون اصطلاحات زیر در معانی مشروح مربوط به‌کار می‌رود:

الف) اطلاعات: هر نوع داده که در اسناد مندرج باشد یا به‌صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد.

ب) اطلاعات شخصی: اطلاعات فردی نظیر نام و نام‌خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.

ج) اطلاعات عمومی: اطلاعات غیرشخصی نظیر ضوابط و آیین‌نامه‌ها، آمار و ارقام ملی و رسمی، اسناد و مکاتبات اداری که از مصادیق مستثنیات فصل چهارم این قانون نباشد.

ماده (۱۵)

مؤسسات مشمول این قانون درصورتی که پذیرش درخواست متقاضی متضمن افشای غیرقانونی اطلاعات شخصی درباره یک شخص حقیقی ثالث باشد باید از در اختیار قرار دادن اطلاعات درخواست شده خودداری کنند، مگر آنکه:

الف) شخص ثالث به‌نحو صریح و مکتوب به افشای اطلاعات راجع به خود رضایت داده باشد.

ب) شخص متقاضی، ولی یا قیّم یا وکیل شخص ثالث، در حدود اختیارات خود باشد.

ج) متقاضی یکی از مؤسسات عمومی باشد و اطلاعات درخواست شده در چارچوب قانون مستقیماً به وظایف آن به‌عنوان یک مؤسسه عمومی مرتبط باشد.

ماده (۲۱)

هر شخصی اعم از حقیقی یا حقوقی که در نتیجه انتشار اطلاعات غیرواقعی درباره او به منافع مادی و معنوی وی صدمه وارد شده است حق دارد تا اطلاعات مذکور را تکذیب کند یا توضیحاتی درباره آنها ارائه دهد و مطابق با قواعد عمومی مسئولیت مدنی جبران خسارت‌های وارد شده را مطالبه نماید.

تبصره ــ در صورت انتشار اطلاعات واقعی برخلاف مفاد این قانون، اشخاص حقیقی و حقوقی حق دارند که مطابق قواعد عمومی مسئولیت‌های مدنی، جبران خسارت‌های وارد شده را مطالبه نمایند.

۵ قانون پایانه‌های فروشگاهی و سامانه مؤدیان، مصوب ۱۳۹۸

ماده (۱۵)

اطلاعات سامانه مؤدیان، محرمانه است و سازمان مجاز به افشای آن جز به حکم قانون و یا مرجع قضایی نمی‌باشد. کارگروه راهبری سامانه مؤدیان مکلف است امکان استفاده از این اطلاعات را مشروط به رعایت ملاحظات امنیتی و حریم خصوصی اشخاص برای دستگاه‌های اجرایی موضوع ماده (۵) قانون مدیریت خدمات کشوری و سایر متقاضیان با شرایط زیر فراهم کند:

الف) در مورد دستگاه‌های اجرایی، دسترسی به این اطلاعات در مواردی خواهد بود که مطابق قوانین و مقررات، اطلاعات موجود در سامانه، در راستای انجام وظایف آنها باشد.

ب) در مورد سایر متقاضیان، دسترسی به این اطلاعات در مواردی خواهد بود که متقاضی به‌منظور انجام امور تحقیقاتی و پژوهشی نیازمند استفاده از اطلاعات مزبور باشد. در این صورت متقاضی مکلف است درخواست مکتوب خود را که در بردارنده اطلاعات مورد نیاز است به‌همراه معرفی‌نامه از سوی دستگاه یا نهادهای پژوهشی مرتبط نظیر مراکز علمی و دانشگاهی به سازمان ارائه کند. کارگروه راهبری سامانه مؤدیان موظف است با بررسی درخواست مزبور، اطلاعات مورد درخواست را به‌صورت داده‌های ناشناس و به میزان لازم جهت انجام تحقیقات و پژوهش مورد نظر در اختیار متقاضی قرار دهد.

تبصره «۱» ــ سازمان مکلف است در ایجاد و استقرار سامانه، نسبت به صیانت و حفاظت از اطلاعات اشخاص و رعایت مقررات امنیت فضای تبادل اطلاعات (افتا) اقدام کند.

تبصره «۲» ــ متخلفان از مفاد این ماده ضمن جبران خسارت وارده مشمول مجازات موضوع ماده (۲۷۹) قانون مالیات‌های مستقیم الحاقی مصوب ۳۱/۴/۱۳۹۴ می‌شوند. الزام به جبران خسارت شامل مواردی که وارد شدن آسیب منتسب به متخلف نیست، نمی‌گردد.

۶. قانون برنامه پنجساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۴۰۰ــ۱۳۹۶)

ماده (۷۴ــالف)

وزارت بهداشت، درمان و آموزش پزشکی با هدف ارائه خدمات الکترونیکی سلامت مکلف است ظرف دو سال اول اجرای قانون برنامه نسبت به استقرار سامانه پرونده الکترونیکی سلامت ایرانیان و سامانه‌های اطلاعاتی مراکز سلامت با هماهنگی پایگاه ملی آمار ایران و سازمان ثبت احوال کشور با حفظ حریم خصوصی و منوط به اذن آنها و محرمانه بودن داده‌ها و با اولویت شروع برنامه پزشک خانواده و نظام ارجاع اقدام نماید.

وزارت بهداشت، درمان و آموزش پزشکی مکلف است با همکاری سازمان‌ها و مراکز خدمات سلامت و بیمه سلامت حداکثر ظرف مدت ۶ ماه پس از استقرار کامل سامانه فوق، خدمات بیمه سلامت را به‌صورت یکپارچه و مبتنی بر فناوری اطلاعات در تعامل با سامانه «پرونده الکترونیکی سلامت ایرانیان» سامان‌دهی نماید.

۷. قانون مدیریت داده‌ها و اطلاعات ملی، مصوب ۱۴۰۱

ماده (۱۲)

الف) در تبصره «۴» ماده (۱۶۹ مکرر) قانون مالیات‌های مستقیم اصلاحی مصوب ۳۱/۴/۱۳۹۴، عبارت «کارگروه تعامل‌پذیری دولت الکترونیکی» جایگزین عبارت «هیئت وزیران و حفظ طبقه‌بندی مربوط،» می‌شود.

ب) در ماده (۲۳۲) قانون مالیات‌های مستقیم اصلاحی مصوب ۲۷/۱۱/۱۳۸۰، عبارت «جز در موارد مربوط به حوزه قضا فقط با تصویب کارگروه تعامل‌پذیری دولت الکترونیکی به سایر دستگاه‌ها ارائه دهند و در غیر این صورت» جایگزین عبارت «محرمانه تلقی و از افشای آن جز در امر تشخیص درآمد و مالیات نزد مراجع ذی‌ربط در حد نیاز خودداری نمایند و در صورت افشا» می‌شود.

پ) در ماده (۳۴) قانون ثبت احوال مصوب ۱۶/۴/۱۳۵۵، عبارت «دستگاه‌های اجرایی با مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی» جایگزین «دولتی ذی‌صلاح» می‌شود.

ت) تبصره ماده (۷۳) قانون مبارزه با قاچاق کالا و ارز مصوب ۳/۱۰/۱۳۹۲ به شرح زیر اصلاح می‌شود:

تبصره ــ تعیین نحوه و سطوح دسترسی به داده‌ها جز در مواردی که مشمول دسترسی‌های قوه قضائیه است، برعهده کارگروه تعامل‌پذیری دولت الکترونیکی می‌باشد.

ث) ماده (۱۵) قانون پایانه‌های فروشگاهی و سامانه مؤدیان مصوب ۲۱/۷/۱۳۹۸ به شرح زیر اصلاح و تبصره‌های آن حذف می‌شود:

ماده (۱۵)

دستورالعمل نحوه دسترسی به اطلاعات سامانه مؤدیان توسط کارگروه تعامل‌پذیری دولت الکترونیکی تعیین می‌شود.

ج) در ماده (۱۹) قانون بازار اوراق بهادار جمهوری اسلامی ایران مصوب ۱/۹/۱۳۸۴ عبارت «کارگروه تعامل‌پذیری دولت الکترونیکی» جایگزین عبارت «دادستان کل کشور» می‌شود.

مرکز پژوهش های مجلس شورای اسلامی

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

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

وب‌سایت: rc@majles.ir