مرکز پژوهش‌های مجلس شورای اسلامی

دفتر مطالعات آموزش و فرهنگ

مسلسل: ۱۹۷۲۲ فروردین ۱۴۰۳

سلسله گزارش‌های دبیرخانه دائمی مقابله با فقر، فساد و تبعیض

شماره: ۲۳

فساد در زنجیره تأمین داده‌های فضای مجازی


بسم الله الرحمن الرحيم

تاریخ انتشار:
۱۴۰۳/۱/۲۹

شماره مسلسل: ۱۹۷۲۲
کد موضوعی: ۲۷۰

مرکز پژوهش‌های مجلس شورای اسلامی

عنوان گزارش:

فساد در زنجیره تأمین داده‌های فضای مجازی

زیر نظر دبیرخانه دائمی مقابله با فقر، فساد و تبعیض

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

نام دفتر:
مطالعات فرهنگ و آموزش (گروه رسانه، ارتباطات جمعی و فضای مجازی)

تهیه و تدوین‌کنندگان:
سیدعلی محسنیان، مرتضی قاسم‌زاده عراقی

همکار:
حسن صفرعلی

اظهارنظرکنندگان:
سینا شامخ، محمدتقی نظریان

ناظران علمی:
موسی بیات، سید یونس ادیانی

گرافیک و صفحه آرایی:
سیده فاطمه ابوطالبی

ویراستار ادبی:
زهره عطاردی

تاریخ شروع مطالعه:
۱۴۰۲/۸/۲۰

واژه‌های کلیدی:
۱. رانت داده
۲. سوءاستفاده از داده
۳. شفافیت داده
٤. حق دسترسی به داده
۵. حقوق شخص موضوع داده
٦. امنیت داده

دفتر مطالعات آموزش و فرهنگ

فهرست مطالب

فهرست اشکال و جدول

فساد در زنجیره تأمین داده‌های فضای مجازی

چکیده

فساد در زنجیره تأمین داده‌های کشور به‌عنوان یک پدیده نوظهور شناخته می‌شـــود. این پدیده شامل مواردی نظیر دسترسی، گردآوری، ذخیره‌سازی، پردازش، افشا، انتقال، اعطای دسترسی به بانک داده، امحای داده‌ها و به‌طور کلی سوءاستفاده یا استفاده خارج از ضوابط قانونی از داده‌ها برای به‌دست آوردن منافع شخصی یا گروهی می‌شود. فساد در داده می‌تواند در حوزه‌های مختلفی از جمله علمی، اقتصادی، سیاسی، فرهنگی، محیط زیست و سلامت رخ دهد و تأثیرات جدی بر سیاست، اقتصاد، افکار عمومی و حتی زیرساخت کشور داشته باشد. لذا با توجه به نقش و اهمیت رو به گسترش داده به‌عنوان منبع اصلی شکوفایی اقتصاد دیجیتال در کشور، شناسایی گلوگاه‌ها برای مقابله با فساد در داده ضرورت یافته است و به‌تبع آن در مقابله با پدیده فساد در داده، طراحی سازوکارهای قانونی، نظارتی و اجرایی مناسب بیش‌ازپیش پراهمیت شده است. در این گزارش تلاش شده تا ضمن بررســـی ابعاد مختلف پدیده فساد در داده‌های کشـــور، تجربیات جهانی احصا و زمینه‌های شکل‌گیری آن شناسایی و در انتها پیشنهادهای تقنینی، سیاستی و اجرایی برای جلوگیری از بروز فساد در زنجیره تأمین داده‌های کشور ارائه شود.

خلاصه مدیریتی

شرح / بیان مسئله

زنجیره تأمین داده یکی از بســـترهای فسادخیز در کشور محسوب می‌شـــود. فســـاد در زنجیره تأمین داده به‌معنای دستیابی، گردآوری، ذخیره‌سازی، پردازش، افشا، انتقال، اعطای دسترسی به بانک داده، امحای داده‌ها و به‌طور کلی سوءاستفاده یا استفاده خارج از ضوابط قانونی از داده‌ها برای به‌دست آوردن منافع شـــخصی یا گروهی می‌شود. فســـاد در داده می‌تواند در حوزه‌های مختلفی از جمله علمی، اقتصادی، سیاسی، فرهنگی، محیط زیست و سلامت رخ دهد و تأثیرات جدی بر سیاست، اقتصاد، افکار عمومی و حتی زیرساخت کشور داشته باشد. تصور مالکیت اشخاصی غیر از اشخاص موضوع داده و یا تولیدکنندگان داده از آنجا معنی پیدا می‌کند که داده‌ها در کنار یکدیگر، تولیدکننده مفاهیم کلی‌تری از اطلاعات در نسبت با کلیت جامعه هستند؛ این مفاهیم کلی، نشان‌دهنده ویژگی‌ها و خصوصیات جامعه هستند که از حیطه مالکیت شخصی افراد، موضوع و تولیدکنندگان آن خارج می‌شود. داده‌های شخصی و داده‌های غیرشخصی تقسیم‌بندی متعارفی است که برای تفکیک دو نوع داده از یکدیگر مطرح می‌شود [۲۰]. حاکمیت‌ها با طرح مقررات محافظت از داده‌های عمومی (برای مثال آن چیزی که در اروپا با عنوان قانون GDPR می‌شناسند)، سعی در حفظ و صیانت از تمامیت و استقلال جامعه در کنار حفظ حق مالکیت شخصی افراد را دارند. در بحث ریشه‌یابی فساد، اهمیت داده‌ها از دو منظر اجتماعی- سیاسی و اقتصادی بیش از سایر جوانب حائز اهمیت است. از منظر اقتصادی فساد در حوزه داده عمدتاً با انگیزه‌هایی نظیر کسب سود نامتعارف، رقابت غیرمنصفانه، انحراف مالیاتی و رانت‌های اطلاعاتی و از منظر سیاسی-اجتماعی عمدتاً با انگیزه‌هایی نظیر دست‌کاری و نفوذ در جریانات سیاسی، سوءاستفاده و دست‌کاری غیرمجاز در مدیریت اطلاعات عمومی و تأثیرات گسترده بر افکار عمومی و حوزه عمومی، انحراف در جریان صحیح اطلاع‌رسانی و دسترسی به اطلاعات صورت می‌پذیرد.

تجربیات بین‌المللی نشان می‌دهد که کشورهای پیشرو از طریق ایجاد سازوکارهای نظارتی، نهادهای تنظیم‌گر و رویه‌های تقنینی و قضایی، اقداماتی را برای جلوگیری از بروز فساد در زنجیره تأمین داده‌ها طرح‌ریزی کرده‌اند؛ اما این امر در کشور ما به‌رغم برخی از اقدامات مثبت تا حد زیادی مغفول مانده و جای توجه دارد. به‌طور مثال در کشورهای کره جنوبی، فرانسه، ایرلند، کانادا، انگلستان و ایتالیا بیش از ۱۲۴ الزام قانونی در حوزه حفاظت از داده‌های شخصی وجود دارد، این درحالی است که در قوانین ایران ۱۳ الزام دیده شده است.

نقطه‌نظرات / یافته‌های کلیدی

ابعاد مسئله فساد در زنجیره تأمین داده‌ها موضوعی پیچیده می‌باشد که نیازمند بررسی عمیق علل و عوامل مختلف است. در این گزارش عوامل آسیب‌پذیر (مصادیق) در زنجیره تأمین داده، امنیت فناوری و ضعف در سازوکارهای نظارتی که به افزایش فساد در شبکه‌های داده منجر می‌شود به‌شرح زیر احصا شد.

۱. دسترسی، جمع‌آوری و افشای غیرمجاز داده،
۲. پردازش و نگهداری داده‌ها برای همیشه،
۳. استفاده مجدد بی‌رویه از داده‌ها،
۴. عدم استقرار نهاد تنظیم‌گر بخشی و فقدان نظارت مؤثر بر داده‌ها،
۵. ایجاد محدودیت شخص موضوع داده در انتقال داده‌ها در زیست‌بوم محصور،
۶. ضعف ضوابط و سازوکارهای دسترسی،
۷. بی‌توجهی به امنیت داده‌ها و در برابر سرعت پردازش،
۸. عدم ارتقای امنیت داده‌ها،
۹. عدم اطلاع‌رسانی به شخص موضوع داده درخصوص پردازش الگوریتمی داده‌ها.

از این منظر و با توجه به آنچه گفته شد برای کاهش فساد در زنجیره تأمین داده‌ها، می‌توان اقدامات متعددی را در ابعاد مختلف موضوع پیش‌بینی کرد. از جمله اقدامات ممکن می‌توان به موارد زیر اشاره کرد:

۱. تشکیل نهادهای تخصصی تنظیم‌گر داده،
۲. به‌روزرسانی قوانین و مقررات،
۳. توسعه استانداردهای ایمنی و پدافندی داده،
۴. توسعه فرایندهای شفاف در زنجیره تأمین داده،
۵. ایجاد نظارت‌های مؤثر بر دارندگان دسترسی به انواع داده‌ها،
۶. افزایش آگاهی و آموزش مردم در مورد مخاطرات به اشتراک‌گذاری داده.

پیشنهاد راهکار تقنینی، نظارتی یا سیاستی

در ادامه با توجه به اقتضائات بومی و ساختارهای حکمرانی- سیاستی تأثیرگذار بر زنجیره تأمین داده‌های کشور پیشنهادهایی در سه بخش زیر برای جلوگیری از بروز فساد در زنجیره تأمین داده‌ها ارائه می‌شود:

الف) راهکارهای سیاستی- تقنینی

۱. تصویب قانون حمایت و حفاظت از داده و اطلاعات شخصی (تصویب طرح شماره ثبت ۶۱۲ دوره یازدهم مجلس شورای اسلامی که در تاریخ ۱۳۹۹/۰۷/۱۲ اعلام وصول شده است)،
۲. تصویب سند جامع امنیت فضای مجازی کشور با تأکید بر نگاشت دقیق نهادی از دستگاه‌ها و نظارت مستمر بر آن از طریق نهاد ناظر و تصویب ضمانت اجرای سند مذکور توسط مجلس شورای اسلامی،
۳. تصویب قانون الزام به انتشار داده و اطلاعات (تصویب طرح شماره ثبت ۲۸۳ دوره یازدهم مجلس شورای اسلامی که مورخ ۱۳۹۹/۰۸/۶ اعلام وصول شده است).

ب) راهکارهای فنی- اجرایی

۱. تدوین دستورالعمل اجرایی برای ستاد پدافند غیرعامل و فاوا، همان‌طور که در ماده (۱۰۳) قانون برنامه هفتم پیشرفت برای هماهنگی دستگاه‌ها و به‌منظور کنترل امنیت سایبری و نظارت مستمر بر آنها پیش‌بینی شده است،

۲. الزام به گزارش شفافیت درخصوص رضایت کاربران در اشتراک‌گذاری داده‌ها، تضمین امنیت داده‌ها، ناشناس‌سازی و مستعارسازی داده‌ها، رعایت حقوق شخص موضوع داده (اطلاع‌رسانی، دسترسی، اصلاح، حذف، انتقال، اعتراض، قرار نگرفتن در معرض پردازش خودکار)، ایجاد استانداردهای امنیتی، سیاست‌های انتقال داده‌های فرامرزی و سازوکارهای اخلاقی مدیریت داده توسط بازیگران زنجیره تأمین داده در سند سیاستی دادگان که پیش‌نویس آن در مرکز ملی فضای مجازی در حال تهیه است.

ج) تقویت چارچوب‌های تنظیم‌گری

۱. اصلاح وظایف و ساختار کمیسیون موضوع ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات از طریق:

- افزودن اعضای فرادولتی (بخش خصوصی و سایر ذی‌ربطان حاکمیتی و بخش عمومی غیردولتی) به کمیسیون،
- پیش‌بینی وظایف قانونی و ضمانت اجرای اداری، انتظامی و قضایی برای مستنکفین از قانون،
- تعیین شاخص‌های ارزیابی عملکرد دستگاه‌ها و مؤسسات خصوصی از طریق کمیسیون و ارائه گزارش ۶ ماهه رتبه‌بندی دستگاه‌ها، براساس این شاخص به هیئت‌وزیران و کمیسیون فرهنگی مجلس شورای اسلامی.

۲. استقرار نهاد تنظیم‌گر بخشی داده‌ها از طریق تصویب ماده‌واحده تقسیم کار ملی برای همکاری میان دو نهاد تنظیم‌گر (کارگروه تعامل‌پذیر دولت الکترونیکی موضوع ماده (۳) قانون مدیریت داده‌ها و اطلاعات ملی و کمیسیون موضوع ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات).

۱. مقدمه

هرگاه منابع به‌واسطه‌های مختلف ارزشمند تلقی می‌شوند، افراد تمایل دارند آن منابع را از آن خود کنند و نسبت به آن ادعای مالکیت نمایند. مالکیت ابتدای ماجرای نزاع، درگیری و فساد است. این موضوع را پیرامون منابع مختلف در طول تاریخ در سیاست، اقتصاد، فرهنگ و محیط زیست می‌توان جست‌وجو کرد. حمایت از حقوق مالکیت از الزامات اساسی هر جامعه است. با انقلاب صنعتی اشکال پیچیده‌تری از مالکیت ظهور کرده است. حقوق مالکیت به‌واسطه اختراعات، علائم تجاری و کپی‌رایت و در راستای حمایت از امور غیرملموس[1] مانند کلمات، ایده‌ها و ابتکارات گسترده شد، اما امروزه که داده‌ها بیشترین اهمیت را یافته‌اند؛ بررسی وضعیت حقوقی مالکیت داده‌ها، جایگاه ویژه‌ای در نظام حقوق کشورها یافته است.[2] داده‌ها نوع جدیدی از منابع ارزشمند در عصر دیجیتال به‌شمار می‌آیند، تا جایی که از آنها می‌توان با عنوان «نفت جدید» یاد کرد که نشان‌دهنده اهمیت آنها در دنیای جدید و ارزشمندی آنهاست. این ارزشمندی و نزاع بر سر مالکیت آنها به‌واسطه اهمیت و گستردگی و امکان تأثیرگذاری آنها بر تمام عرصه‌های سیاست، اقتصاد، اجتماع، سلامت و محیط زیست است.

اما پیش از مالکیت داده لازم است به این مسئله توجه کنیم که اساساً آیا حقی را مبتنی‌بر مالکیت داده‌ها می‌توان شناسایی کرد. به این منظور ابتدا باید مالکیت در داده‌ها به‌خوبی تعریف شود و حقوق مرتبط مانند حق دسترسی،[3] انتقال،[4] اصلاح[5] و حذف[6] داده‌ها که به‌طور طبیعی نشئت گرفته از شأن نظارتی است نسبت به بازیگران که ممکن است افراد، صاحبان پلتفرم و یا حاکمیت جامعه باشد، مشخص شود. «داده‌ها» اصیل نیستند، داده‌ها در وضعیت خام خود هیچ ابداعی نداشته و به نسبت کلی بوده و انتزاعی هستند. داده‌ها در نظام مالکیت ادبی و هنری، کپی‌رایت و همچنین در نظام ثبت اختراع که به‌جهت حمایت از تألیف و خلاقیت به‌وجود آمده است، قابل حمایت نیستند. ابهام در نظام حقوقی موجود در نسبت با موضوع داده‌ها، زمینه‌های فساد را در زنجیره تأمین داده ایجاد می‌کند. این ابهام فرصت را برای انحصار در استفاده، خرید، فروش و استفاده غیرمجاز و به‌طور کلی تخطی از حفظ و صیانت از داده‌ها که از مصادیق فساد به‌شمار می‌آیند را، به‌وجود آورده است.

1. Intangible
۲. پروین، فرهاد و عطار شیما (۱۴۰۰). «حقوق اتحادیه اروپا و چالش شناسایی حق مالکیت بر داده در عصر اقتصاد دیجیتال»، مجله حقوقی بین‌المللی/شماره ۶۵، ص ۳۰۴-۲۸۱.
3. Right to Access
4. Right to Data Portability
5. Right to Rectification
6. Right to Erasure

اما بحث از مالکیت داده، محدود به مسئله مالکیت نمی‌ماند و به‌واسطه کاربردهایی که داده‌ها دارند، وارد مسئله حکمرانی می‌شود. داده‌ها در مسئله حکمرانی به‌واسطه ردپای دیجیتالی (داده‌های تولید شده توسط کاربران در استفاده از فضای وب) که از خود برجای می‌گذارند، فرصت بزرگی را برای پردازش و بهره‌برداری در سیاست، اقتصاد، فرهنگ (افکار عمومی)، سلامت و محیط زیست و ... را فراهم می‌کنند. این فرصت بزرگ، هر بازیگری را برای انحصارطلبی و استفاده مجاز و یا حتی غیرمجاز از داده‌ها وسوسه می‌کند و مالکیت داده‌ها نسبت به افراد را با بهانه مختلف ازجمله: ۱. نسبت به افراد موضوع داده به بهانه حفظ حریم شخصی، ۲. نسبت به صاحبان پلتفرم و سکوها با بهانه استفاده از داده ها باهدف بهبود خدمات قابل ارائه به مشتریان و ۳. نسبت به دولت‌ها به بهانه حفظ امنیت و صیانت از نشت اطلاعات به دولت‌های متخاصم خارجی را به‌عنوان مسائل حل نشده باقی می‌گذارد.

هدایت و بالفعل کردن ظرفیت حوزه داده و اطلاعات می‌تواند «رشد» را تضمین کند. داده و اطلاعات می‌تواند تبدیل به ابزاری کارآمد برای نظارت شده و در نقطه مقابل می‌تواند تبدیل به سلاحی دردآور برای تهدید اقتصادی و اجتماعی شهروندان گردد. مقوله داده و اطلاعات می‌تواند ثروت‌ساز یا ثروت‌سوز باشد، می‌تواند قدرت‌ساز یا قدرت‌سوز باشد و می‌تواند فرصت‌آفرین یا فرصت‌سوز باشد. اینکه مقوله داده و اطلاعات فرصت باشد یا تهدید، وابسته به هنجارهای رسوب کرده در این عرصه است. اگر رها باشد، قطعاً تبدیل به تهدیدی بزرگ خواهد شد؛ اما اگر هنجارمند شده و به کنترل و هدایت درآید، تبدیل به سرمایه‌ای عظیم برای رشد و پیشرفت کشور خواهد شد. لذا ازاین‌رو است که حضور فعال حاکمیت برای قاعده‌مندی آن، ضرورتی اجتناب‌ناپذیر خواهد بود؛ به‌عبارت‌دیگر حکمرانی داده اجتناب‌ناپذیر خواهد بود. البته باید توجه داشت که تعلل بیشتر در ایجاد سازوکارهای حکمرانی داده می‌تواند ضرورت قاعده‌مند کردن فعالیت در این عرصه را سخت و دشوار کرده و عواقب و تهدیدات غیرقابل جبرانی را موجب شود.

حکمرانی داده درواقع حکمرانی بر سرچشمه کنش افراد و جامعه یعنی سطح بینشی و گرایشی است. با این بیان می‌توان ادعا کرد که بخش عمده قدرت (اگر نگوییم تمام آن) در اختیار کسی خواهد بود که حکمرانی بر داده در اختیار او باشد. شاید در این لحظه از زمان ادعای فوق، هنوز عینیت کامل نیافته است، اما بی‌شک طرح قدرت در آینده نمی‌تواند تهی از طرح حکمرانی داده باشد و حکمرانی بدون داشتن ابزاری برای کنترل، هدایت و عصاره‌گیری از داده، نمی‌تواند خود را بر زمین واقعیت نشست دهد.

حاکمیت نیازمندترین نهاد اجتماعی به داده و اطلاعات است و این نیاز با پیچیده‌تر شدن جوامع روزبه‌روز بیشتر می‌شود؛ تا جایی که بازیگران فعال در سیاست، اقتصاد فرهنگ، محیط زیست، سلامت و ... هم به این اطلاعات نیاز پیدا می‌کنند و به‌واسطه این داده‌ها تأثیراتی بر محیط هدف خود یعنی همان سیاست، اقتصاد و ... می‌گذارند. این نیاز سهم‌خواهی‌ها، انحصارطلبی‌ها و نظام مالکیتی را برای داده‌ها به‌وجود می‌آورد. این سهم‌خواهی‌ها اگر هنجارمند نباشند، مقدمات فساد را ایجاد می‌کند.

گفتنی است که ابهام و عدم شفاف شدن حقوق و تکالیف افراد در نسبت با داده و اطلاعات و نیز در نسبت با همدیگر و عدم شفاف شدن تکالیف دولت در این عرصه، بستری برای سوءاستفاده برخی و تعدی به حقوق بخش عمده‌ای از جامعه را فراهم آورده است. این ابهام، کلیت عرصه داده و اطلاعات را تبدیل به رانت بزرگی برای افراد خاص کرده است. به‌عبارت‌دیگر، پیش‌تر اگر از «رانت اطلاعاتی» صحبت می‌شد، امروز باید از «رانت داده» صحبت کرد. اگر در گذشته رانت اطلاعاتی ابزار و شاه‌کلید سبقت از دیگران برای فتح برخی عرصه‌های اقتصادی بود، امروزه کلیت عرصه داده و اطلاعات به‌واسطه ابهام‌های فراوان در آن، از حالت ابزار به غایت و از شاه‌کلید به خود گنج تغییر جایگاه داده است و این رانت در شرایط ابهام و خلأ قانونی کنونی، بزرگ‌ترین فساد در این عرصه است. به همین دلیل کشورهای مختلف سازوکارهای مختلف تقنینی، قضایی و تنظیم‌گری را برای جلوگیری از سوءاستفاده و بروز فساد در زنجیره تأمین داده ایجاد نموده‌اند.

تدوین مقررات حفاظت از اطلاعات عمومی (GDPR)[۱] در سال ۲۰۱۶ در اروپا، تشکیل کمیته داده‌های جغرافیایی فدرال (FGDC)[۲] در سال ۲۰۱۹ به‌منظور حفاظت از زیرساخت داده‌های ملی آمریکا، همچنین وضع مقرره در حوزه‌های مختلف نظیر حفاظت از حریم خصوصی برخط کودکان،[۳] حفظ حریم خصوصی ارتباطات الکترونیکی،[۴] حفاظت از حریم خصوصی ویدئویی،[۵] داده‌های مربوط به مؤسسات مالی[۶] ازجمله اقدامات بین‌المللی برای حفاظت از داده‌ها و جلوگیری از بروز فساد و سوءاستفاده از داده‌ها بوده است. در کشور ما نیز مجموعه‌ای از

۱. مقررات عمومی حفاظت از داده اتحادیه اروپا مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده در اتحادیه اروپا و منطقه اقتصادی اروپا وضع و در سال ۲۰۱۶ ازسوی پارلمان اروپا به تصویب رسید.

۲. کمیته داده‌های جغرافیایی فدرال (FGDC) یک کمیته دولتی ایالات متحده است که توسعه هماهنگ، استفاده، به اشتراک‌گذاری و انتشار داده‌های جغرافیایی در سطح ملی را ترویج می‌کند. ۳۲ عضو آن نمایندگانی از دفتر اجرایی رئیس‌جمهور و سطح کابینه و آژانس‌های مستقل فدرال هستند.

۳. قانون حفاظت از حریم خصوصی آنلاین کودکان (COPPA).

۴. قانون حفظ حریم خصوصی ارتباطات الکترونیکی (ECPA).

۵. قانون حفاظت از حریم خصوصی ویدئویی (VPPA).

۶. قانون نوسازی خدمات مالی (GLBA).

تدابیر مختلف درخصوص حفاظت از داده‌ها اتخاذ شده است. تصویب قوانین انتشار و دسترسی آزاد به اطلاعات (۱۳۸۷) و مدیریت داده‌ها و اطلاعات ملی (۱۴۰۱) [۱] ازجمله اقدامات تقنینی درخصوص مدیریت و حفاظت از داده‌هاست.

با توجه به رشد روزافزون فناوری‌ها و نفوذ آنها به زندگی اجتماعی و فردی، همچنین اهمیت یافتن بیشتر داده‌ها به‌عنوان یکی از دارایی‌های ارزشمند دیجیتال، حائز اهمیت است که بررسی دقیق‌تری جهت شناسایی ابعاد مسئله داده‌ها و نقایص قانونی و اجرایی مرتبط با فساد در زنجیره تأمین داده صورت گیرد. در گزارش حاضر به بررسی ابعاد مختلف پدیده فساد در داده‌های کشور، تجربیات جهانی احصا و زمینه‌های شکل‌گیری آن شناسایی و مورد بررسی قرار می‌گیرد و در انتها پیشنهادهای تقنینی، سیاستی و اجرایی برای جلوگیری از بروز فساد در زنجیره تأمین داده‌های کشور ارائه شده است

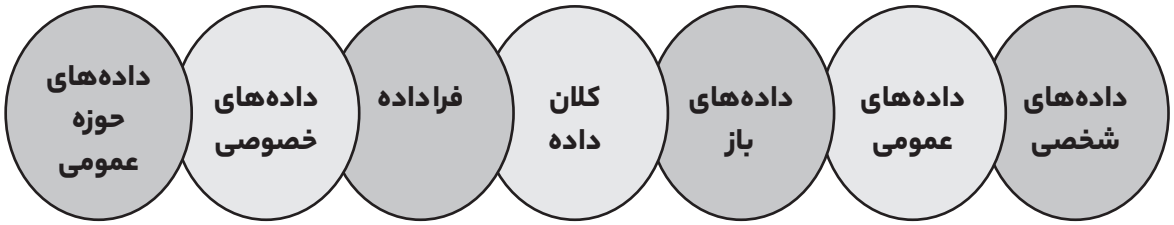
۲. انواع داده‌ها

به‌طور کلی داده‌ها را می‌توان از دو لحاظ دسته‌بندی کرد. نخست از لحاظ فنی و دوم از لحاظ حقوقی. در بررسی مسئله فساد در زنجیره تأمین داده با توجه به اصول و قواعد حقوقی حاکم بر داده‌ها، می‌توان داده‌ها را در دسته‌بندی‌های متفاوتی قرار داد. یکی از دسته‌بندی‌ها، بسیار کلی است که داده‌ها را به داده‌های شخصی و غیرشخصی تقسیم می‌کند [۲۰]. دسته‌بندی دیگری داده‌ها را در هفت دسته متمایز طبقه‌بندی می‌کند که عبارتند از: داده‌های شخصی،[۱] داده‌های عمومی،[۲] داده‌های باز،[۳] کلان‌داده،[۴] فرادادها،[۵] داده‌های خصوصی[۶] و داده‌های حوزه عمومی.[۷] این دسته‌بندی مبتنی‌بر چهار معیار مهم است که رژیم حقوقی حاکم بر هر دسته را تعیین می‌کند. معیار اول، هدف از وضع قوانین درباره هریک از انواع داده می‌باشد، برای مثال داده‌های عمومی عمدتاً برای ارتقای شفافیت در امور عمومی و شناسایی حق دسترسی شهروندان به اطلاعات موجود در مؤسسات عمومی و داده‌های شخصی برای حفاظت از حریم خصوصی افراد مورد توجه قانونگذاران قرار گرفته‌اند. معیار دوم، موضوع و محتوای قواعد حقوقی حاکم بر داده‌هاست. بر این اساس، مقررات و رویه‌های حاکم بر آزاد یا مجاز بودن دسترسی به داده‌ها، تملک داده‌ها، استفاده از داده‌ها، ذخیره‌سازی و پردازش داده‌ها، احکام متفاوتی را در مورد انواع داده‌ها مقرر کرده‌اند. معیار سوم، کنشگران اصلی و مرتبط با انواع داده‌هاست. برای مثال، در مورد داده‌های عمومی، کمیسیون‌های آزادی اطلاعات کنشگران اصلی هستند و درخصوص داده‌های شخصی، کنترل‌گر[۸] و پردازشگر،[۹] کنشگران اصلی هستند؛ و درنهایت معیار چهارم الگوی تنظیم‌گری حاکم بر هرکدام از انواع داده‌هاست [۷].

1. Personal Data
2. Public Data
3. Open Data
4. Big Data
5. Meta-Data
6. Private Data
7. Proprietary Data

۸. شخص حقیقی یا حقوقی که اهداف پردازش داده‌ها را مشخص می‌کند.
۹. شخص حقیقی یا حقوقی است که به درخواست کنترل‌گر، داده‌های شخصی را پردازش می‌کند.

شکل ۱. تقسیم‌بندی هفت‌گانه داده‌ها



۱-۲. داده‌های شخصی

داده‌های شخصی به‌معنای هر گونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی («موضوع داده‌ها») است. شخص حقیقی، هر فردی است که به‌صورت مستقیم یا غیرمستقیم، به‌ویژه توسط نام، شماره شناسایی، اطلاعات مکان، شناسه آنلاین یا یک یا چند عامل خاص فیزیکی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی، شناسایی می‌شود [۸].

قوانین مختلف داخلی و خارجی، موضوع داده‌های شخصی را مورد توجه قرار داده‌اند. در قوانین ایران دو قانون به تعریف داده‌های شخصی مبادرت شده است. قانون تجارت الکترونیکی مصوب ۱۳۸۲ در بخش تعاریف داده‌های شخصی (Private Data) را داده‌های مربوط به یک شخص حقیقی موضوع «داده» (Data Subject) مشخص و معین تعریف می نماید [۹]؛ همچنین قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ نیز داده‌های شخصی را شامل: 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 می‌داند [۱۰].

رویکردهای موجود در خصوص داده‌های شخصی

دو هدف نسبتاً متعارض در همه قوانین مربوط به حمایت از داده‌های شخصی وجود دارد:

- حمایت از اشخاص در برابر آثار احتمالی دستیابی دیگران به اطلاعات شخصی آنها،
- فراهم کردن امکان استفاده از داده‌های شخصی برای اهداف و مقاصد تجاری.

حسب اینکه در نظام حقوقی هر کشور کدام‌یک از این دو هدف بر دیگری برتری داده شود، چند رویکرد قابل شناسایی است:

- **رویکرد حق‌محور (اروپایی):** این رویکرد از حق افراد نسبت به تعیین سرنوشت اطلاعاتشان دفاع می کند. متأثر از این رویکرد، در سطح اروپا هم قواعدی عام در مورد حمایت از داده‌های شخصی وجود دارد و هم قواعد خاص برای حمایت از حوزه‌های خاص اطلاعات شخصی.
- **رویکرد تجارت‌محور (آمریکا):** رویکرد موسوم به حقوق و اقتصاد که از بازار داده‌های شخصی دفاع می کند. در آمریکا از داده‌های شخصی به‌عنوان کالاهای قابل عرضه در بازار دفاع می‌شود، برخلاف نظام اروپایی، از اطلاعات اشخاص تنها در حوزه‌های خاصی که احتمال سوءاستفاده علیه آنها وجود دارد، حمایت می کند.
- **رویکرد امنیت‌محور (چین):** این رویکرد ترکیبی از قواعد اروپایی و آمریکا در زمینه حمایت از داده‌های شخصی است. مبنای رویکرد کشورهایی مانند چین و روسیه در این راستا، انطباق داده‌های شخصی در زمینه اینترنت حاکمیتی است.

۲-۲. داده‌های عمومی

داده‌های عمومی،[1] کلیه اطلاعاتی هستند که در بخش عمومی موجود است؛ یعنی اطلاعاتی که به دولت تعلق دارد و در نقطه مقابل داده‌های خصوصی قرار دارد. داده‌های عمومی طبق اصل آزادی اطلاعات و به‌موجب قوانین آزادی اطلاعات برای اشخاص قابل دسترس است؛ مگر آنکه منع قانونی خاصی وجود داشته باشد. همچنین داده‌های موجود در بخش عمومی ممکن است در قالب‌های مکتوب یا الکترونیک باشد، عناوین گوناگون داشته باشند، توسط بخش عمومی تولید و یا توسط دیگران تولید شده باشند [۸].

در نظام حقوقی ایران، طبق قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ همه اشخاص حقیقی و حقوقی ایرانی بدون هیچ‌گونه تبعیضی حق دسترسی به اطلاعات عمومی را دارند [۱۰]. نکته مهم در خصوص حق دسترسی افراد به اطلاعات عمومی آن است که اطلاعات

1. Public Data

درخواستی باید بدون مطالبه هرگونه دلیل و توجیه از متقاضی، ارائه شود. سازوکار دسترسی فردی به داده‌های عمومی می‌تواند متمرکز (از طریق سامانه ملی) یا غیرمتمرکز (دسترسی سنتی) باشد. همچنین شیوه‌نامه «تشخیص و تفکیک اسرار دولتی از اطلاعات عمومی» مصوب کمیسیون انتشار و دسترسی آزاد به اطلاعات که طبق تبصره «۲» ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات در سال ۱۳۹۹ ضوابطی را در این خصوص تعیین کرده و عملاً این سطح از داده را در حوزه صلاحیت خود قرار داده است.

۲-۳. داده‌های باز

در نتیجه وضع قوانین آزادی اطلاعات در کشورهای مختلف جهان، دولت‌ها متعهد شدند از یک‌سو اطلاعات مورد درخواست شهروندان را در اختیار آنها قرار دهند و از سوی دیگر بخشی از اطلاعات خود را بدون وجود هرگونه تقاضا به‌صورت ابتکاری منتشر کنند. با گذشت زمان در اثر دیجیتالی شدن گسترده فعالیت‌های بخش عمومی و تولید حجم انبوهی از داده‌های دیجیتال، ضرورت اصلاح قوانین مربوط به انتشار ابتکاری داده‌های عمومی و استفاده از آنها احساس شد. بر همین اساس، کشورهای مختلف با وضع قوانین خاص به حمایت از داده‌های باز[1] پرداختند و شرایط و ضوابط استفاده از آنها را مشخص کردند. آسان بودن دسترسی و رایگان بودن استفاده از شرایط اصلی داده‌های باز هستند، ولی در برخی کشورهای جهان استفاده از این داده‌ها منوط به اخذ مجوزهای خاص است [۷]. به‌طور مثال اتحادیه اروپا در ماه مه ۲۰۱۹، کمیسیون اروپا «دستورالعمل داده باز» را تصویب کرد که مؤسسات اتحادیه اروپا و کشورهای عضو را موظف کرده است که داده‌های با کیفیت بالا و قابل خواندن ماشینی را به‌صورت رایگان برای استفاده مجدد ارائه کنند [۱۱]. این دستورالعمل در سراسر اروپا اجرا شده است و کشورهایی مانند آلمان راهبردهای ملی خاصی را برای حمایت از طرح‌های داده باز اتخاذ کرده‌اند.

۲-۴. کلان‌داده

مفهوم کلان‌داده،[2] معمولاً برای توصیف مجموعه‌ای از داده‌های بسیار زیاد استفاده می‌شود که از منابع گوناگون جمع‌آوری و ذخیره شده و با استفاده از فناوری‌های رایانه‌ای، برای استنتاج‌هایی در مورد الگوهای داده‌ها، روندها و همبستگی‌ها، قابل تحلیل و محاسبه هستند. کلان‌داده‌ها دارای دو رکن هستند: داده‌های زیاد و فناوری‌های تحلیل‌گر. چنانچه بر رکن اول تمرکز شود، مطالعه آن در ذیل انواع داده قرار می‌گیرد. در مورد کلان‌داده‌ها، عناصری همچون حجم، تنوع، سرعت و پویایی اثرگذار است. چشم‌انداز قانونی پیرامون کلان‌داده‌ها به‌دلیل قابلیت‌های نوآوری آنها به‌سرعت تغییر کرده و درعین‌حال با مشکلاتی مربوط به حریم خصوصی، امنیت، حقوق مالکیت معنوی و مسئولیت مواجه شده است.

۲-۵. فراداده‌ها

فراداده‌ها،[3] عبارتند از داده‌هایی که اطلاعاتی درباره دیگر داده‌ها ارائه می‌دهند. اســـتفاده از هر فناوری ممکن است فراداده‌های خاصی را تولید کند و تولید آن عمدتاً با استفاده از فناوری‌ها ملازمه دارد، ولی گاهی برای ارتقای کیفیت خدمات بهتر از طریق یک فناوری، به‌صورت داوطلبانه نسبت به جمع‌آوری فراداده اقدام می‌شود [۷]. یکی از تجربیات قانونی در این زمینه تصویب قانون اصلاحی ارتباطات راه دور (شنود و دسترسی) توسط دولت فدرال استرالیاست (۲۰۱۵) که در آن مسئولان ارتباطات استرالیا باید فراداده‌ها را حداقل برای دو سال نگه دارند. این قانون با انتقاد مواجه شد، زیرا نگرانی از تأثیر آن بر آزادی خبرنگاران و توانایی حفاظت از منابع محرمانه وجود داشت. موافقان این قانون معتقد بودند که این اقدامات برای پیشگیری از جنایت و مبارزه با تروریسم ضروری است [۱۲].

۲-۶. داده‌های حوزه عمومی

اصطلاح حوزه عمومی در معنای تعبیری که بیشتر رویکرد سیاسی دارد و در دفاع از دمکراسی مطرح شد؛[4] نخستین‌بار از سوی هابرماس ارائه و منظور آن قلمرویی از حیات اجتماعی بود که در آن چیزی شبیه به افکار عمومی می‌تواند شکل بگیرد. حوزه عمومی اطلاعاتی به حوزه‌ای گفته می‌شود که در آن اطلاعات (اعم از کتاب، موسیقی، فیلم و ...) آزاد است و هیچ‌کس حق منع یا محروم کردن دیگران از دسترسی به آنها را ندارد.

۲-۷. داده‌های خصوصی (مالکانه / غیرمالکانه)

داده‌های خصوصی،[5] داده‌هایی هستند که توســـط اشخاص خصوصی تولید می‌شـــوند یا قانوناً در تصرف یا کنترل اشخاص خصوصی قرار

1. Open Data
2. Big Data
3. Metadata
4. Public Sphere
5. Private Data

دارند. این دسته از داده‌ها یا در ذیل هیچ‌کدام از انواع داده‌های پیش‌گفته قرار نمی‌گیرند یا اینکه هم‌پوشانی محدودی با بعضی از آنها (مانند داده‌های شخصی) دارند. این داده‌ها برحسب اینکه از حمایت‌های حقوق مالکیت برخوردار باشند یا نه در دو دسته کلی مالکانه و غیرمالکانه تقسیم‌بندی می‌شوند [۷].

۳. واکاوی ابعاد مسئله فساد در زنجیره تأمین داده‌ها

شواهد فراوانی نشان می‌دهد که در دهه‌های گذشته، فعالیت‌های اقتصادی، سیاسی و اجتماعی به‌شکل گسترده‌ای به اینترنت منتقل شده‌اند. به‌عنوان‌مثال، گزارش بانک جهانی نشان از افزایش سه برابری اقتصاد جهانی، تحت‌تأثیر رشد اقتصاد دیجیتال را دارد که طی آن رشد تولید ناخالص ملی جهانی از سال ۲۰۰۰ تا ۲۰۲۲ از ۳۳,۸۵ تریلیون دلار به ۱۰۰,۵۶ تریلیون دلار رسیده است. همچنین گزارش‌ها نشان می‌دهد که اقتصاد مبتنی‌بر فناوری‌های دیجیتال بیش از ۵۰ درصد از تولید ناخالص داخلی را تشکیل می‌دهند و بازارهای مرتبط با دیجیتالی‌سازی، به رشد اقتصاد قابل‌توجهی در عصر اقتصاد دیجیتال منجر شده است [۲].

رشد مدل‌های کسب‌وکار مبتنی‌بر فناوری مالی[1] (فین‌تک)، نظیر صنایع پرداخت، وام‌دهی، تجارت الکترونیک، بانکداری، رمزارزها، مبادلات ارز، مدیریت مالی، نرم‌افزار و هوش مصنوعی، همچنین زیست اجتماعی انسان‌ها در فضای مجازی و حضور اجتماعی افراد در بستر رسانه‌های اجتماعی، امکان ایجاد داده‌های ارزشمند مرتبط با فعالیت‌های اقتصادی-اجتماعی را برای شرکت‌ها، دولت‌ها و افراد فراهم ساخته است. ازاین‌رو، فناوری‌های پیشرفته کنونی به مؤسسات امکان ذخیره‌سازی و پردازش انبوهی از اطلاعات استثنایی از منابع مختلف ازجمله تلفن‌های همراه، کارت‌های نقدی، سامانه موقعیت‌یاب، تراکنش‌ها، گزارش‌های آنلاین و سوابق الکترونیکی را فراهم می‌کند [۳]. در عرصه‌ای اجتماعی و سیاسی نیز کلان‌داده‌ها[2] یک منبع ارزشمند به‌شمار می‌روند. این داده‌ها حاوی اطلاعات حجیم، متنوع و با سرعت بالا هستند که معمولاً از منابع گوناگون نظیر رسانه‌ها، شبکه‌های اجتماعی، سامانه‌های دولتی، شرکت‌ها و سازمان‌ها جمع‌آوری می‌شوند. این داده‌ها می‌توانند تأثیرات گسترده‌ای در زمینه تحلیل روندها و پیش‌بینی رویدادها و درنهایت اثر گذرا بر آن را داشته باشند.

بنابراین ارزش داده‌ها که از آن به‌مثابه «نفت جدید» قرن بیست‌ویکم تعبیر می‌شود [۴]، این فضا را به‌طور بالقوه در معرض سوءاستفاده از ارزش داده‌ها برای منافع خصوصی و یا گروهی خاص قرار داده است. این نوع از فساد در سطح اقتصادی عمدتاً با انگیزه‌های نظیر کسب سود نامتعارف، رقابت غیرمنصفانه، انحراف مالیاتی و رانت‌های اطلاعاتی و فروش داده‌ها و در سطح سیاسی-اجتماعی عمدتاً با انگیزه‌های نظیر دست‌کاری و نفوذ در جریانات سیاسی، سوءاستفاده و دست‌کاری غیرمجاز در مدیریت اطلاعات عمومی و تأثیرات گسترده بر حوزه عمومی، انحراف در جریان صحیح اطلاع‌رسانی و دسترسی به اطلاعات صورت می‌پذیرد.

درواقع، اهمیت و ارزش داده‌ها در حوزه‌های سیاسی، اقتصادی، اجتماعی، فناوری، زیست‌محیطی و حقوقی[3] به‌گونه‌ای است که استفاده غیرقانونی از آنها نگرانی‌های جدی را ایجاد کرده است. به‌طور مثال ارزش مالی یک تریلیون یورویی داده‌های شخصی شهروندان اروپایی در سال ۲۰۲۰، زمینه‌ساز ایجاد پرونده‌های مالی متعددی علیه سکوهای دیجیتال در اتحادیه اروپا به‌دلیل نقض داده‌ها بوده است [۵]. همچنین شواهد متعدد دیگری نشان از سوءاستفاده از داده‌ها برای اهداف اجتماعی و سیاسی می‌باشد؛ پرونده فعالیت شرکت کمبریج آنالیتیکا[4] و فیس‌بوک[5] در پردازش غیرقانونی داده‌های شخصی کاربران در سال ۲۰۱۶ در ایالات متحده آمریکا به‌منظور تأثیرگذاری بر نتایج انتخابات ریاست جمهوری این کشور [۶]، ازجمله پرونده‌های مرتبط با اهداف سیاسی-اجتماعی بروز فساد در این سطح است.

فساد در زنجیره تأمین داده به‌معنای دستیابی، گردآوری، ذخیره‌سازی، پردازش، افشا، انتقال، اعطای دسترسی به بانک داده، امحای داده‌ها و به‌طور کلی سوءاستفاده یا استفاده خارج از ضوابط قانونی از داده‌ها برای به‌دست آوردن منافع شخصی یا گروهی است. این نوع از فساد می‌تواند با اهداف مختلف اقتصادی، سیاسی و امنیتی در زمینه‌های مختلفی اتفاق بیفتد؛ بنابراین فساد در داده‌ها، یا فساد اجتماعی-سیاسی و یا فساد اقتصادی هستند که می‌توانند در مراحل مختلف زنجیره تأمین داده‌ها (شکل ۲) به وقوع بپیوندند.

1. Financial Technology
2. Big Data
3. PESTEL Analysis (Political, Economic, Social, Technological, Environmental and Legal Factors)
۴. کمبریج آنالیتیکا (Cambridge Analytica) یک شرکت سهامی خاص در آمریکاست که با ترکیب داده‌کاوی و تحلیل داده‌ها در فرایندهای انتخاباتی و سیاسی، خدماتی مربوط به ارتباطات راهبردی ارائه می‌دهد. این شرکت در سال ۲۰۱۸ به‌دلیل جنجال‌های رسانه‌ای درخصوص سوءاستفاده از داده‌ها و از دست دادن مشتریان خود اعلام ورشکستگی کرد.
5. Facebook

شکل ۲. محورهای اصلی در زنجیره تأمین داده‌ها

۴. مصادیق و عوامل زمینه‌ساز فساد در زنجیره تأمین داده

ابعاد مسئله فساد در زنجیره تأمین داده‌ها موضوعی پیچیده می‌باشد که نیازمند بررسی عمیق علل و عوامل مختلف است. روش مدنظر نگارندگان در این گزارش برای احصای مصادیق فساد، بهره‌گیری از روش چندجانبه با رهیافت کیفی است. این روش شامل روش کتابخانه‌ای و روش تحلیلی و تفسیری می‌باشد که به‌طور مشخص برای گردآوری اطلاعات از طریق اسناد و تفسیر شواهد بهره گرفته شده است. براساس مطالعات اسنادی و بررسی شواهد، مسائلی مانند امنیت فناوری اطلاعات، خلأهای نظارت مؤثر از سوی دستگاه‌های نظارتی به افزایش فساد در شبکه‌های داده منجر می‌شود. مصادیق بروز فساد در داده‌ها و همچنین زمینه‌هایی که باعث شکل‌گیری آنها شده را با توجه به شواهد تقنینی و شواهد نقض و سوءاستفاده از داده‌ها در قالب مصادیق ۹گانه زیر قابل ارائه شده است.

شکل ۳. مصادیق و عوامل زمینه‌ساز فساد در زنجیره تأمین داده

۱-۴. دسترسی، جمع‌آوری و افشای غیرمجاز داده‌ها

یکی از عوامل بروز فساد و سوءاستفاده از داده‌ها، به اشتراک‌گذاری داده‌های شخصی یا حساس بدون رضایت افراد موضوع داده و یا مغایر با شروط خدمات یا توافق‌نامه‌های حریم خصوصی و حفاظت از داده‌هاست. برمبنای مقررات بین‌المللی، اطلاعات شخصی باید به‌صورت قانونی (معمولاً با آگاهی) و برای یک هدف خاص جمع‌آوری شـــوند؛ همچنین این داده‌ها نباید بدون رضایت شخص موضوع داده یا برای اهداف غیرمرتبط استفاده شوند (مگر به حکم قوانین). به همین دلیل کاربران و افراد موضوع داده باید حقوق خاصی بر داده‌های مرتبط با خود داشته باشند. قوانین و مقررات مختلفی، الزامات معینی را در این زمینه ارائه داده‌اند. مقررات عمومی حفاظت از داده‌ها (GDPR) ملاحظاتی را همچون اصول قانونی، منصفانه و شفاف بودن، محدود بودن به اهداف، حداقلی بودن، صحت، محدود بودن به زمان، تمامیت- محرمانگی و پاسخ‌گویی به‌عنوان ناظر بر پردازش و جمع‌آوری داده‌های شخصی و حساس و همچنین چارچوب‌های همچون رضایت فرد موضوع داده، رعایت انصاف و شفافیت، حق انتقال، حق به فراموشی (حق حذف) را در حفاظت از حریم خصوصی شهروندان و حفاظت از داده‌ها مورد توجه قرار می‌دهد [۱۳].

اسناد سیاستی درخصوص داده در ایران نیز این موضوع مورد توجه قرار داده‌اند. برای مثال در بخش اول از سند سیاست‌ها و الزامات حفاظت از داده‌ها (دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی)[۱] چهار اصل «رضایت»، «تعیین اهداف»، «شیوه‌های دریافت» و «قانونی» بودن به‌عنوان اصول حاکم بر داده‌ای شخصی مورد توجه قرار گرفته است.

سطح دیگری از مصادیق فساد در داده‌ها، افشای غیرقانونی داده‌های است که قرار بوده خصوصی نگه داشته شوند. افشای داده‌ها ممکن است در سطوح داده‌های شخصی، داده‌های عمومی متعلق به دولت‌ها و یا داده‌های مربوط به کســب‌وکارها رخ دهد. افشای غیرمجاز داده‌های حساس می‌تواند عواقب جدی برای افراد، سازمان و حتی دولت‌ها داشته باشد، عواقب افشای غیرمجاز داده، می‌تواند دربرگیرنده زیان‌های

۱. مصوب یک‌صدوبیست‌وهفتمین جلسه مورخ ۱۴۰۲/۱۱/۱۰ کمیسیون عالی تنظیم مقررات فضای مجازی کشور.

مالی برای سازمان، آسیب به شهرت افراد و حتی تهدید امنیت ملی کشورها باشد. عمدتاً افشای غیرمجاز داده‌ها در هر شرایطی رخ می‌دهد که داده‌های حساس به‌اندازه کافی در برابر تهدیدات احتمالی مانند دسترسی غیرمجاز، سوءاستفاده، هک و سرقت محافظت نشده باشد.

از این منظر، نگاه نظام‌های حقوقی مختلف از جمله در ایران عمدتاً سازوکارهای مختلف حقوقی و قضایی را بر افشای داده‌ها و اطلاعات در سطوح داده‌های شخصی (برای مثال ماده (۱۶) قانون جرائم رایانه‌ای)،[۱] داده و اسرار تجاری و اقتصادی بنگاه‌ها (برای مثال ماده (۶۴) قانون تجارت الکترونیکی)[۲] و انتشار و افشای اسناد و داده‌های دولتی (برای مثال قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی)[۳] وضع کرده‌اند.

یکی از شواهد برجسته افشای داده‌های دولتی، پرونده ادوارد اسنودن درخصوص افشای اسرار دولتی در سال ۲۰۱۳ آمریکا بود. در ایالات متحده، اقدامات اسنودن به‌عنوان نقض قانون جاسوسی ۱۹۱۷ شناخته شد و درنهایت مورد تعقیب قضایی قرار گرفت. فارغ از اینکه آیا اقدامات ادوارد اسنودن تخلفی از قوانین داده‌ها بود یا نه، این پرونده نشان داد که افشای داده‌ها می‌تواند تأثیرات گسترده‌ای داشته باشند و به گسترش بحران امنیتی و حریم خصوصی منجر شوند.

موارد افشای اطلاعات و داده در طول سال‌های اخیر منجر به صدور احکام قضایی از جمله جریمه سکوها در اتحادیه اروپا شده است. در سال ۲۰۲۱ کمیسیون حفاظت از داده‌های ایرلند، شرکت متا را به‌دلیل نقض قوانین اتحادیه اروپا در جمع‌آوری غیرقانونی داده‌های ۱,۳ میلیارد از کاربران جریمه کرد؛ از زمانی که اتحادیه اروپا «مقررات عمومی حفاظت از داده‌ها» را وضع کرده است، این یکی از مهم‌ترین و سنگین‌ترین مجازات‌های است که، نسبت به یک سکو اعمال می‌شود. تنظیم‌گران اروپایی معتقدند که شرکت متا درخصوص محافظت از داده‌های کاربران در سکوهایی همچون فیس‌بوک از انتقال فرامرزی داده‌ها (از اروپا به آمریکا) در برابر آژانس‌های جاسوسی به‌اندازه کافی شفاف نبوده است. نمونه دیگر از موارد نقض داده‌های کاربران در ارتباط با موضوع کوکی‌هاست.[۴] درواقع موضوع کوکی‌ها و ردیابی علایق شخصی کاربران و استفاده مجدد این داده‌ها در بازارهای ثانویه یکی از دلایل صدور احکام قضایی و جریمه‌های مالی علیه شرکت‌های فناوری است. در جولای ۲۰۲۱ اعلام شد که شرکت آمازون به‌دلیل سیاست‌های غیرواضح و عدم رضایت کاربران درباره کوکی‌ها، ۸۸۷ میلیون دلار جریمه شد. این اولین‌بار نبود که آمازون به‌دلیل نحوه جمع‌آوری و اشتراک‌گذاری داده‌های شخصی از طریق کوکی‌ها مجازات می‌شود. در اواخر سال ۲۰۲۰، فرانسه آمازون را به‌دلیل موضوعات مرتبط به رضایت‌نامه کوکی‌ها، ۳۵ میلیون یورو جریمه کرده بود. هرچقدر که وادار کردن کاربران به «موافقت کردن» با کوکی‌ها- یا انصراف از کوکی‌ها- برای جمع‌آوری هرچه بیشتر داده‌های شخصی وسوسه‌انگیز باشد؛ اما تنظیم‌گران قوانین جدی برای اجرای قوانین کوکی‌ها در اتحادیه اروپا وضع کرده‌اند [۱۴].

۲-۴. پردازش و نگهداری داده‌ها برای همیشه

در دهه اخیر، با پذیرش یادگیری ماشینی و تحلیل داده‌های بزرگ در طراحی سیستم‌های اطلاعاتی، وابستگی به داده‌ها به‌شدت افزایش یافته است؛ بنابراین، شرکت‌های فناوری در تلاشند نه‌تنها داده‌های کاربران را جمع‌آوری کنند، بلکه آنها را برای همیشه در خدمت داشته باشند. بااین‌حال، قوانین مختلفی در سراسر جهان الزامات حقوقی را درباره بازه‌های زمانی (زمان برای زندگی)[۵] برای مدت زمان نگهداری و پردازش داده‌ها تعیین کرده‌اند. به‌عنوان‌مثال، قانون حمایت از داده‌های عمومی (GDPR) الزام می‌کند که هیچ داده‌ای نباید برای همیشه زنده بماند. ماده (۱۷) این قانون به کاربران این حق را می‌دهد که داده‌های شخصی خود را در یک زمان معقول از تمامی سیستم‌ها حذف کنند. همچنین مواد (۵) و (۱۳) این مقررات، مسئولیت‌های اضافی برای کنترل‌گر داده‌ها تعیین می‌کند: ۱. اطلاع به کاربران درباره مدت ذخیره داده‌های شخصی، ۲. اگر دیگر نیازی به داده‌های شخصی برای هدفی که برای آن جمع‌آوری شده‌اند وجود نداشته باشد، باید از بین برود. بااین‌وجود، این محدودیت درخصوص بایگانی داده‌ها در راستای هدف مرتبط با منافع عمومی یا برای اهداف تحقیقاتی، تاریخی یا علمی اعمال نمی‌شود [۸]. حذف داده‌ها در دنیای واقعی حفاظت از داده‌ها چالش‌برانگیز است. به‌عنوان‌مثال، سکوی ابری گوگل اعلام کرده است تا ۱۸۰ روز طول

۱. هرکس 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.

۲. به‌منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرّر در این قانون خواهد رسید.

۳. قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳ مجلس شورای ملی.

۴. کوکی‌ها (Cookies) فایل‌های متنی با داده‌های کوچکی مانند نام کاربری و رمز عبور هستند که برای شناسایی کامپیوتر شما هنگام استفاده از شبکه به‌کار می‌روند. این داده‌ها به‌صورت فایل در کامپیوتر کاربران ذخیره می‌شوند و زمانی که یک کاربر از وب‌سایتی استفاده می‌کند، این اطلاعات به سرور وب‌سایت ارسال می‌شود. داده‌های ذخیره شده در کوکی با یک شناسه منحصربه‌فرد برای شما و کامپیوتر تان برچسب‌گذاری شده‌اند. هنگامی که کوکی بین کامپیوتر شما و سرور شبکه مبادله می‌شود، سرور شناسه را می‌خواند و می‌داند که چه اطلاعاتی را به‌طور خاص باید به شما ارائه دهد.

5. Time-To-Live (TTL)

می‌کشد تا داده‌های مشـــتری را به‌طور کامل حذف کند. علاوه‌بر این، داده‌ها در زیرسیستم‌های ذخیره‌ســـازی مانند حافظه، دیسک‌ها و دیتاسنترهای توزیع شده جغرافیایی تکثیر می‌شوند که باعث به تأخیر افتادن و تضمین کردن حذف داده‌ها می‌شود [۱۵].

۳-۴. استفاده مجدد و بی‌رویه از داده‌ها

در زمان طراحی سیستم‌های نرم‌افزاری، عموماً داده‌ها به‌عنوان یک منبع کمکی در نظر گرفته می‌شوند که به سیستم‌های اطلاعاتی سطح بالا در دستیابی به اهدافشان کمک می‌کنند. این رویکرد، به سازمان‌هایی مانند گوگل و آمازون امکان می‌دهد که داده‌های کاربران را جمع‌آوری کرده و برای شخصی‌سازی تجربیات خود از این داده‌ها در موارد گوناگون اســـتفاده کنند. بااین‌حال، مقررات GDPR این عمل را ممنوع می‌کند. به‌عنوان‌مثال ماده (۵) این دستورالعمل، محدودیت اهداف را تعیین می‌کند. ماده (۶) مربوط به قانونی بودن پردازش داده‌های شخصی تنها برای موارد خاصی که موضوع داده با پردازش آنها موافقت کرده باشد؛ همچنین، ماده (۲۱) به کاربران این حق را می‌دهد که در هر زمان نسبت به استفاده از داده‌های شخصی خود برای هر هدفی اعتراض کنند [۱۵].

شواهد متعددی نشـــان می‌دهد، داده‌هایی که فقط برای اهداف خاص از کاربران جمع‌آوری شده توسط برخی از شرکت‌های فناوری مورد سوءاستفاده قرار گرفته است. برای مثال، در ژانویه ۲۰۱۹، کمیســـیون حفاظت از داده فرانسه گوگل را به پرداخت جریمه ۵۰ میلیون یورو محکوم کرد، زیرا ازسوی کمیسیون این اعتقاد وجود داشت که تبلیغات شخصی‌سازی شرکت، مبانی قانونی مشخصی نداشته بود، به‌طور خاص، این حکم ذکر کرد که رضایت کاربر به‌دست‌آمده توسط گوگل به‌اندازه کافی «مشخص» نیست و داده‌های شخصی به‌دست‌آمده از این طریق نباید در ۲۰ سرویس استفاده می‌شود.

۴-۴. عدم استقرار نهاد تنظیم‌گر بخشی و فقدان نظارت مؤثر بر داده‌ها

یکی از عوامل سوءاستفاده و بروز فساد در داده‌ها، ضعف نظارت و عدم وجود نهاد تنظیم‌گر با اختیارات کافی بر زنجیره تأمین داده‌هاست. نیاز به حفاظت از داده‌ها، جلوگیری از سوءاستفاده و انطباق مقررات با هرکدام از انواع داده، ضرورت وجود یک مقام نظارتی را در قالب نهادهای مستقل و یا وابسته برجسته کرده است. مرجع نظارتی ممکن است یک مقام واحد، یک مقام دولتی، بازرس یا یک نهاد با چند عضو مستقل باشد؛ در برخی از موارد قانونگذاران سازوکار خاص نهادی را برای تشکیل یک نهاد ناظر بر داده‌ها در نظر می‌گیرند. برای مثال این نهادها از منظر استقلال ساختاری، کارکردی و اداری آن، ترکیب مراجع مختلف قضایی، تقنینی و اجرایی، روش انتصاب اعضا، قدرت و چارچوب زمانی، تخصیص منابع کافی قابل تفکیک هستند و هرکدام از نظام‌های حقوقی ویژگی‌هایی را برای نهادهای ناظر در نظر می‌گیرند (به‌عنوان‌مثال، بند «۱۱۷» GDPR). مقام ناظر ممکن است اختیارات خاصی را در زمینه‌های مختلف انطباق فعالیت‌ها با چارچوب‌های قانونی، رسیدگی به شکایات عمومی، تعیین الزامات خاص در پردازش و نگهداری از داده‌ها، صدور حکم درخصوص نقض داده‌ها و ارتقای آگاهی عمومی از حقوق افراد موضوع داده را داشته باشد؛ بنابراین فقدان مقررات و نهاد ناظر بر حسن اجرای مقررات یکی از زمینه‌های بروز فساد در حوزه داده‌هاست. این مهم در بسیاری از کشورها از طریق ایجاد سازوکار نهادی مورد توجه قرار گرفته است. اداره نظارت بر حفاظت داده‌های استونی یک نهاد حقوقی مهم است. این اداره که در سال ۱۹۹۹ تأسیس شده است، زیر نظر وزارت دادگستری فعالیت می‌کند و مسئولیت نظارت بر اجرای قوانین حفاظت داده و اطلاعات عمومی را دارد. هدف اصلی این اداره، حفاظت از حقوق شـــخصی به حریم خصوصی و اطمینان از شفافیت فعالیت‌های دولت است. مدیر این اداره توسط دولت منصوب می‌شود و نامزدی او با مشارکت مجلس تصویب می‌شود [۱۶].

قانون حفاظت اطلاعات شخصی آفریقای جنوبی (۲۰۱۳) یک نهاد مستقل تنظیم‌گر اطلاعات را ایجاد کرد. این نهاد توسط رئیس‌جمهور با پیشنهاد شورای ملی تعیین می‌شود. این سازمان دارای وظایف گسترده‌ای در زمینه‌های مختلفی ازجمله آموزش عمومی، نظارت بر اجرای قوانین، رسیدگی به شکایات فردی، انجام تحقیقات، صدور آیین‌نامه‌ها و دستورالعمل‌ها و تسهیل همکاری‌های فرامرزی است. همچنین این سازمان مسئول ارزیابی دوره‌ای و نظارت بر نهادهای دولتی و خصوصی درگیر در پردازش داده‌های شخصی و نظارت بر استفاده از شناسه‌های منحصربه‌فرد است.

در کشور ما نیز مطابق در ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۸۷) به‌منظور حمایت از آزادی اطلاعات و دسترسی همگانی به اطلاعات موجود در مؤسسات عمومی و مؤسسات خصوصی که خدمات عمومی ارائه می‌دهند، تدوین برنامه‌های اجرایی لازم در عرصه اطلاع‌رسانی، نظارت کلی بر حسن اجرا، رفع اختلاف در چگونگی ارائه اطلاعات موضوع این قانون از طریق ایجاد وحدت‌رویه، فرهنگ‌سازی،

ارشاد و ارائه نظرات مشورتی، کمیسیون انتشار و دسترسی آزاد به اطلاعات به دستور رئیس‌جمهور تشکیل شده است. همچنین کمیسیون دوام (کمیسیون داده‌ها و اطلاعات ملی موضوع ماده (۳) قانون مدیریت داده‌ها و اطلاعات ملی) به‌منظور اجرای سیاست‌ها و راهبردهای کلان شورای عالی فضای مجازی در داده و اطلاعات ملی و نظارت و مدیریت بر نحوه نگهداری، پردازش، دسترسی، یکپارچه‌سازی، امنیت و به‌ویژه تبادل و به اشتراک‌گذاری داده و اطلاعات ملی تشکیل شده است.

۴-۵. تعریف حق مالکیت برای اشخاص در زیست بوم‌های محصور (باغ دیواری) در انتقال داده‌ها[۱]

در اوایل فرایند گسترده کالایی‌سازی داده‌های شخصی، استانداردهای مناسب برای جمع‌آوری، به اشتراک گذاشتن و فروش مجدد این داده‌ها هنوز تعیین نشده است. این موضوع باعث ایجاد ابهامات زیادی برای کاربران و درنهایت چالش‌های مختلف برای کنترل داده‌ها بین نهادهای کنترل‌گر داده شده است. سیستم عامل تلفن همراه آی‌اواس[۲] ساخت شرکت اپل، شبکه اجتماعی فیس‌بوک و پلتفرم کیندل[۳] آمازون مهم‌ترین نمونه‌های زیست‌بوم محصور (باغ دیواری) هستند. همه این زیست‌بوم‌ها از کاربرانشان می‌خواهند که در محدوده پلتفرم‌هایشان کار کنند، بدون آنکه کاربران، توانایی اعمال استقلال کامل در انتقال دارایی‌ها و داده‌های خود داشته باشند و در صورت زیر پا گذاشتن شرایط خدمات از سرویس این سکوها می‌توانند با حذف دسترسی، کاربران خود را مجازات کنند. این زیست‌بوم‌های محصور نگرانی‌هایی را در باب حفظ حریم خصوصی و کنترل داده‌ها ایجاد کرده‌اند. چراکه در این محیط‌های بسته، شرکت‌ها به داده‌های گسترده‌ای از کاربران حتی فراتر از آنچه برای برنامه مورد نیاز است، دسترسی دارند. این سکوها این داده‌ها را از طریق روش‌های مختلف مانند تعاملات کاربر، علایق، رفتارها و دستگاه‌های متصل جمع‌آوری می‌نمایند و از این طریق ابرداده‌هایی را مانند مکان، آدرس‌های مبتنی‌بر آی پی و موارد دیگر ایجاد می‌کنند. حتی گفته شده است که سکوی اجتماعی فیس‌بوک تا ۵۲۰۰۰ ویژگی کاربران خود را ردیابی می‌کند. درواقع شیوه‌های جمع‌آوری داده‌ها و ردیابی کاربر در زیست‌بوم‌های محصور، سؤالات جدی را در مورد میزان رعایت حریم خصوصی کاربران این سکوها ایجاد کرده است. عدم شفافیت در استفاده و اشتراک‌گذاری داده‌ها این نگرانی‌ها را بیشتر می‌کند، چراکه کاربران از نحوه استفاده از داده‌های خود بی‌اطلاع هستند [۱۷]. از این منظر، کاربران فناوری‌های نوین، نگران ناتوانی در ردیابی داده‌ها پس از فروش یا اشتراک‌گذاری در بازارهای ثانویه هستند. درواقع برخی از شرکت‌های فناوری با ایجاد باغ‌های دیواری و کاهش شفافیت، داده‌های کاربران را در بازارهای ثانویه به فروش می‌رسانند.

بااین‌حال، قانون حفاظت اطلاعات عمومی اروپا (GDPR) این روش‌ها را محدود می‌کند. طبق ماده (۲۰) این قانون، افراد حق دارند داده‌های شخصی مربوط به خود را که به یک کنترل‌کننده ارائه کرده‌اند، دریافت کنند. علاوه‌بر این، آنها می‌توانند از کنترل‌کننده بخواهند که مستقیماً تمام داده‌های شخصی را به کنترل‌کننده دیگری منتقل کند. ماده (۱۴) این قانون نیز رفتار شرکت‌ها را در بازارهای ثانویه تنظیم می‌کند که دسترسی به داده‌ها را نیازمند اطلاع‌رسانی به کاربران است؛ این ماده بیان می‌کند که سکوها باید در مدت یک ماه به کاربران اطلاع دهند: ۱. چگونگی جمع‌آوری داده‌ها، ۲. چه‌مدت ذخیره می‌شوند، ۳. برای چه هدفی استفاده می‌شوند و ۴. قصد اشتراک‌گذاری آن با دیگران [۱۵].

زمانی که الزامات مقررات عمومی داده‌ها در اروپا بر شرکت‌های حوزه فناوری فعال شـــد، تعدادی از شرکت‌ها، ابزارهای دانلود داده را برای کاربران اتحادیه اروپا راه‌اندازی کردند. به‌عنوان‌مثال، ســـرویس پشـــتیبان‌گیری گوگل[۴] به کاربران این امکان را می‌دهد که نه‌تنها به تمام داده‌های شخصی خود در سیستم خود دسترسی داشته باشند، بلکه داده‌ها را مستقیماً به سرویس‌های خارجی انتقال دهند.

۴-۶. ضعف ضوابط و سازوکارهای دسترسی

عدم پیاده‌سازی یا پیاده‌سازی ضعیف مجوزهای کاربر و سطوح دسترســـی که منجر به دسترسی کاربران به داده‌های حساس بدون مجوز می‌شود؛ یکی از عوامل بروز فســـاد در حوزه داده اســـت. ازاین‌رو، امروزه مجموعه‌ای از ســـازوکارهای فنی و اجرایی به‌منظور جلوگیری از سوءاستفاده از داده‌ها ذیل موضوع مجوزهای دسترسی به داده‌ها پیاده‌سازی می‌شوند. سازوکار کنترل دسترسی به داده‌ها، سازمان‌ها را قادر می‌سازد تا دسترسی به داده‌های خود را مدیریت و کنترل کنند. این شامل تنظیم خط‌مشی‌ها، مجوزها و اقدامات امنیتی است تا اطمینان حاصل شود که فقط کاربران مجاز می‌توانند به داده‌ها دسترسی داشته باشـــند، آنها را تغییر دهند یا حذف کنند. اجرای کنترل دسترسی

۱. باغ‌های دیواری (Walled garden) به اکوسیستم‌های بسته اطلاق می‌شوند که در آن شرکت‌ها سخت‌افزار، نرم‌افزار و خدمات را به‌شدت کنترل می‌کنند تا تجربه‌ای یکپارچه را به کاربران ارائه دهند. همچنین این قابلیت مزایایی مانند افزایش رضایت تجربه کاربری، افزایش امنیت و تجربیات شخصی‌سازی شـــده را ارائه دهند. باغ‌های دیواری همچنین موانعی از جمله انتخاب محدود مصرف‌کننده، نگرانی‌های مربوط به حفظ حریم خصوصی داده‌ها و قفل شدن فروشنده را نیز به‌همراه دارند.

2. IOS

۳. یک پلتفرم خودنشر است که به نویسندگان این اجازه را می‌دهد که کتاب‌های خود را در Amazon.com منتشر کرده و به فروش برسانند.

4. Google Takeout

مناسب به داده‌ها، به سازمان‌ها این امکان را می‌دهد که از اطلاعات حساس محافظت کرده، از نقض داده‌ها جلوگیری کنند و از رعایت مقررات اطمینان حاصل کنند. کنترل دسترسی به داده‌ها با تعریف و اجرای قوانین دسترسی و محدودیت‌های مربوط به منابع داده‌ها انجام می‌شود. این مجموعه اقدامات شامل عناصر کلیدی احراز هویت،[1] مجوز قانونی،[2] سیاســـت‌های دسترسی،[3] لیست کنترل دسترسی[4] و شفافیت در دسترسی و حسابرسی و ثبت[5] گزارش است.

۴-۷. بی توجهی به امنیت داده‌ها در برابر سرعت پردازش

شرکت‌های فناوری مدرن با چالش ایجاد و مدیریت سیستم‌های نرم‌افزاری پیچیده‌تر در محیطی مواجه هستند که نیاز به نوآوری سریع دارد. این امر به‌ویژه در شرکت‌های عصر اینترنت منجر به اولویت دادن سرعت بر صحت شده است. یک باور پذیرفته شده در این زمینه این موضوع می‌باشد که تا زمانی که شما در حال شکستن چیزی جدید نیستید، به‌اندازه کافی سریع حرکت نمی‌کنید. بااین‌حال، مقررات عمومی حفاظت از داده‌ها به صراحت این رویکرد را در هنگام برخورد با داده‌های شخصی محدود می‌کند.

ماده (۳۵) این قانون، کنترل‌گر داده را ملزم به ارزیابی تأثیر حفاظت از داده‌ها به‌ویژه با استفاده از فناوری‌های جدید می‌کند؛ همچنین ماده (۳۶) ضرورت بررسی‌ها در دو سطح در نظر می‌گیرد، سطح اول برای کنترل‌کننده داخلی است، جایی که ارزیابی تأثیر باید ماهیت و دامنه خطرات را تجزیه‌وتحلیل کند و سپس تدابیر لازم برای کاهش آنها را پیشنهاد کند. در مرحله بعد، اگر خطرات، ماهیت نظام‌مند دارند یا مربوط به پلتفرم‌های مشترک، اعم از داخلی و خارجی هستند، مسئول حفاظت از داده‌ها باید قبل از هر پردازشی با مقام نظارتی مشورت کند [۱۵].

به‌رغم تدابیر گوناگون برای کاستن از خطرات اولویت داشتن ســـرعت بر دقت، همچنان بسیاری از شرکت‌های فناوری مانند فیس‌بوک با مشکلات ناشی از آن مواجه بوده‌اند. در ســـال ۲۰۱۸، دو نقض بزرگ فاش شد: اول اینکه واسط برنامه‌نویسی نرم‌افزار کاربردی (API) آنها به کمبریج آنالیتیکا اجازه می‌داد تا به‌طور غیرقانونی، داده‌های شخصی ۸۷ میلیون کاربر را جمع‌آوری کند و سپس از ویژگی در نظر گرفتن (View As) جدید آنها برای به‌دست آوردن کنترل بیش از ۵۰ میلیون حساب کاربری مورد سوءاستفاده قرار گرفت. بااین‌حال، این روش یعنی اولویت دادن به‌سرعت بر امنیت تنها محدود به یک شرکت نیست. به‌عنوان‌مثال، در نوامبر ۲۰۱۷، برنامه ورزشی استراوا (Strava) یک ابزار انگیزشی ورزش‌کار به نام نقشه جهانی حرارت [۲۶] منتشر کرد که فعالیت‌های ورزشی کاربران در سراسر جهان را به تصویر می‌کشید. بااین‌حال، در عرض چند ماه این نقشـــه‌ها برای شناســـایی پایگاه‌های نظامی نامعلوم و عملیات امنیتی مخفی مورد استفاده قرار گرفت و مأموریت‌ها و جان سربازان را به خطر انداخت.

۴-۸. عدم ارتقای امنیت داده‌ها

ازجمله مهم‌ترین مباحث در حکمرانی داده، موضوع امنیت داده و الزام ســـازمان‌ها به اجرای الزامات حفاظتی از تمام سامانه‌های فناوری اطلاعات است. هک اطلاعات کاربران و مواردی مشابه هک سامانه هوشمند سوخت نشان می‌دهد که مدیریت مخاطرات فضای مجازی در داخل کشور دارای ضعف جدی است. اطلاعات و داده‌ها باید به‌طور ایمن ذخیره و پردازش شوند و در برابر پردازش غیرمجاز یا غیرقانونی، گم شدن، سرقت، تخریب یا آسیب محافظت شـــود. در برخی صنایع، حفظ امنیت داده‌ها برای رعایت مقررات حفاظت از اطلاعات بسیار حائز اهمیت است. به‌عنوان‌مثال، سازمان‌هایی که اطلاعات کارت پرداختی را پردازش می‌کنند، موظفند از روش‌ها و مکانیسم‌های امن برای ذخیره و استفاده از این اطلاعات استفاده کنند. همچنین، سازمان‌های بهداشتی در ایالات متحده موظف به حفظ اطلاعات مربوط سوابق پزشکی الکترونیکی (PHI) مطابق با استانداردهای قانون قابلیت انتقال و مسئولیت بیمه سلامت (HIPAA)[6] هستند [۱۸].

نتایج تحقیقات پیرامون هزینه نقض داده‌ها از سوی مؤسسه پونمون[7] نشـــان می‌دهد که میانگین خسارت ناشی از یک نقض داده در ایالات

1. Authentication
2. Authorization
3. Access Policies
4. Access Control Lists (ACLs)
5. Auditing and Logging
۶. HIPAA یا Health Insurance Portability and Accountability Act به‌معنی قانون قابلیت انتقال و مسئولیت بیمه سلامت است. این قانون در سال ۱۹۹۶ تصویب شده است. HIPAA سلسله‌ای از استانداردهای نظارتی است که طرح افشای قانونی اطلاعات بهداشتی محافظت شده (PHI) و استفاده از آن را ارائه می‌دهد. پروتکل HIPAA توسط سازمان سلامت و سرویس‌های انسانی (HHS) تنظیم و توسط دفتر حقوق شهروندی (OCR) اجرا شده است.
7. Ponemon Institute

متحده، ۸ میلیون دلار بوده است. در میانگین هر حادثه داده، ۲۵,۵۷۵ حساب کاربری تحت‌تأثیر قرار گرفته است.
شکایت‌های حقوقی، حل اختلافات و جریمه‌های مربوط به نقض داده‌ها نیز در حال افزایش است و بسیاری از دولت‌ها مقررات سخت‌گیرانه‌تری را در مورد حفاظت از داده‌ها اعمال می‌کنند. قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA)،[۱] قانون برنامه کاربردی تلفن (APPs act)،[۲] مقررات امنیت اطلاعات استرالیا (CPS 234)[۳] از جمله مقررات و چارچوب‌های قانونی هستند که الزاماتی را بر سازمان‌های ارائه دهنده خدمات برای ارتقا امنیت اطلاعات و حفاظت از اطلاعات مشتریان اعمال می‌کنند. در این قوانین برخی از اقدامات معمول برای تضمین امنیت داده‌ها تدوین شده که برخی عبارتند از: رمزگذاری داده‌ها،[۴] ناشناس‌سازی و مستعارسازی نام داده‌ها، محرمانه بودن داده‌ها و یکپارچگی داده‌ها و سیستم‌هایی استفاده یا تولیدکننده از داده‌ها.

۹-۴. عدم اطلاع‌رسانی به کاربران در خصوص پردازش الگوریتمی داده‌ها

روش تصمیم‌گیری الگوریتمی در حوزه‌های مختلفی همچون مدیریت محتوای رسانه‌ای، مدیریت عملیات صنعتی، تجارت ابزارهای مالی، شخصی‌سازی تبلیغات و حتی مبارزه با اخبار جعلی با موفقیت انجام شده است. مهارت، دقت و مقیاس‌پذیری ذاتی آنها (بدون هیچ انسانی در حلقه) آنها را به یک ضرورت در طراحی سیستم مدرن تبدیل کرده است. امروزه پلتفرم‌های اطلاعات دیجیتال و سرگرمی به‌طور فزاینده‌ای، توصیه‌های خودکار (سیستم‌های توصیه‌گر) را بر اساس اطلاعات جمعیتی، انتخاب‌های قبلی، فیلتر مشارکتی یا فیلتر مبتنی‌بر محتوا به کاربران ارائه می‌دهند. بااین‌حال، بسیاری از مقررات در مورد داده‌ها با نگاه تردید و بدبینانه به این مسئله نگاه می‌کنند. ماده (۲۲) مقررات عمومی حفاظت از داده‌ها (GDPR)، درخصوص تصمیم‌گیری فردی خودکار اشاره دارد که شخص موضوع داده حق دارد که مشمول تصمیمی که صرفاً براساس پردازش خودکارباشد، قرار نگیرد. همچنین برمبنای ماده (۱۵) موضوع داده‌ها باید از کنترل‌گر اطلاعات معناداری در مورد منطق مربوطه و همچنین اهمیت و پیامدهای پیش‌بینی شده چنین پردازشی دریافت کند [۸].
با گسترش هوش مصنوعی بحث در مورد حریم خصوصی و تفسیرپذیری در تصمیم‌گیری خودکار و پردازش الگوریتمی آغاز شده است. در سال ۲۰۱۶ کنفرانس بین‌المللی مشترک هوش مصنوعی (IJCAI) و کنفرانس بین‌المللی یادگیری ماشین (ICML)، مباحث مختلفی همچون موضوعات مربوط به حقوق هوش مصنوعی را مورد مداقه قرار داده‌اند. در ژانویه ۲۰۱۹، مرکز اروپایی حقوق دیجیتال (NoYB) به‌دلیل نقض الزامات ماده (۱۵) در سیستم‌های توصیه خود، شکایت‌هایی را علیه هشت سرویس استریم شامل آمازون، اپل موزیک، نت فلیکس، سان کلود، اسپوتیفای، یوتیوب، فیلم میت و دازن انجام داد [۱۵].

۱. قانون حریم خصوصی مصرف‌کننده کالیفرنیا لایحه‌ای است که حقوق حریم شخصی و حمایت از مصرف‌کننده افراد مقیم ایالت کالیفرنیا در کشور ایالات متحده آمریکا را بهبود می‌دهد. این لایحه توسط مجلس ایالتی کالیفرنی در سال ۲۰۱۸ به تصویب رسیده است.
۲. این قانون با هدف ایجاد شفافیت بیشتر و کنترل کاربر بر پردازش داده‌های جمع‌آوری شده توسط برنامه‌های کاربردی تلفن همراه و افزایش امنیت داده‌ها در سال ۲۰۱۸ در آمریکا به تصویب رسید.
۳. CPS ۲۳۴ مقررات اجباری درخصوص امنیت اطلاعات است که در سال ۲۰۱۹ از سوی تنظیم‌گر استرالیا (APRA) ابلاغ شده است.
۴. رمزنگاری داده‌ها (Encryption) روشی برای به هم پیوستن داده‌هاست؛ به‌طوری که تنها افراد مجاز قادر به درک آن اطلاعات می‌باشند.

۵. الزامات حقوقی برای جلوگیری از بروز فساد در زنجیره تأمین داده‌ها

در مبارزه با فساد در حوزه داده، قوانین ایفای نقش بسیار حیاتی دارند. این قوانین معمولاً شامل مقررات مربوط به حریم خصوصی، امنیت اطلاعات، جرم اینترنتی، مالکیت معنوی و سایر موارد مرتبط با داده‌ها می‌شود. با تعیین قوانین دقیق و مؤثر، می‌توان از طریق تنظیم رفتار و فعالیت‌های درون شبکه‌ای و برخط، فساد در فناوری اطلاعات را کاهش داد. همچنین، برقراری قوانین مربوط به شفافیت و شفاف‌سازی امور مالی و دولتی در حوزه داده نیز اهمیت دارد. این موضوع باعث شده تا طیف وسیعی از الزامات حقوقی برای جلوگیری از بروز خلأهای مختلف در زمینه فساد و سوءاستفاده از داده‌ها در بین کشورهای گوناگون مورد توجه سیاستگذاران و قانونگذاران قرار گرفته است. مطالعه‌ای توسط تقوی‌فرد و همکاران (۱۳۹۵) پیرامون مقایسه تطبیقی قوانین حمایت از داده‌ها و حریم خصوصی در ایران و کشورهای منتخب (کره جنوبی، فرانسه، ایرلند، کانادا، انگلستان و ایتالیا) نشان‌دهنده این است که از میان ۱۲۴ الزامی که در کشورهای منتخب (کره جنوبی، فرانسه، ایرلند، کانادا، انگلستان و ایتالیا) برای حفاظت از حریم خصوصی اطلاعاتی شناسایی شده است؛ تنها ۱۳ مورد در قوانین ایران وجود دارد. این در حالی است که ۸۱ مورد از این الزامات در میان کشورهای منتخب مشترک است [۱۹].

الزامات احصا شده در هفت حوزه مورد مقایسه (نگهداری داده، استفاده از داده‌ها، دسترسی به داده‌ها، نگهداری داده‌ها، افشای داده‌ها، حقوق شخص موضوع داده‌ها و مسئولیت کنترل‌گر) در قالب جدول زیر ارائه شده است.

جدول ۱. عناوین الزامات حقوقی داده

ردیف	حوزه مرتبط	الزام
۱	گردآوری داده	مشخص بودن اهداف، الزام به ارائه اطلاعات کافی به سوژه، قانونی بودن، مبتنی‌برسوژه‌ها، موجب جلب‌رضایت سوژه، با تعیین حدکفایت داده‌ها، مجاز بودن گردآوری بدون رضایت با حکم قانون، مرتبط برای مقاصد تحقیقاتی، عدم گردآوری بدون جلب‌رضایت، گردآوری برای وظایف قانونی متولی، اجتناب‌ناپذیر بنابر قرارداد متولی، با هدف حفاظت از اموال و دارایی سوژه، گردآوری از منبعی غیر از سوژه، برای احکام قضایی، برای منافع عمومی، حفاظت از منافع مشروع متولی، حفاظت از امنیت ملی، پیگرد قضایی مجرمان، عدم روش‌های فریبنده، تحقیق پیرامون نقض قانون
۲	استفاده از داده	عدم استفاده از داده‌ها در صورت غیرمجاز شمرده شدن گردآوری آنها، مجاز بودن برای سازمان ثالث، مجاز بودن برای حفاظت از جان سوژه، اموال سوژه، سازگار بودن برای استفاده، بنابر قرارداد با سوژه، تعلیق استفاده، برای تحقیقات (علمی، آماری، تاریخی)، در صورت وجود الزامات قانونی، استفاده به‌صورت منصفانه، استفاده به‌صورت قانونی، برای حفاظت از امنیت ملی، برای دعاوی حقوقی، پایمال نشدن منافع سوژه، برای وظایف قانونی، پیگرد قانونی مجرمان، برای تحقیقات جنایی
۳	نگهداری داده	غیرمجاز بودن نگهداری براساس غیرمجاز شمرده شدن، لزوم اطمینان از صحت داده‌ها قبل از نگهداری، نگهداری تا زمان رسیدن به اهداف اولیه، به‌روزرسانی در هنگام ضرورت، لزوم نابودسازی داده‌ها در صورت منقضی شدن زمان نگهداری، نابودسازی در صورت تقاضای سوژه، نگهداری برای مقاصد تحقیقاتی (علمی، آماری، تاریخی)، نگهداری داده در صورت وجود الزام قانونی، اطمینان از کامل بودن داده‌ها پیش از نگهداری، لزوم حذف داده‌های غیردقیق
٤	افشای داده	غیرمجاز بودن افشا در صورت نبودن جز اهداف، غیرمجاز بودن بدون جلب‌رضایت سوژه، مجاز بودن افشا در صورت لزوم قضایی، مجاز بودن افشا برای وظایف قانونی، لزوم ارائه پیش از افشا، افشا بنا به قرارداد میان متولی و سوژه، درخواست سوژه برای تعلیق، غیرمجاز بودن به‌دلیل منقضی شدن زمان نگهداری آن، افشا برای حفاظت از اموال سوژه، مجاز بودن برای تحقیقات مربوط به جرائم، مجاز بودن برای الزام قانونی افشا، افشا برای نهادهای پزشکی حرفه‌ای، مجاز بودن افشا برای حفاظت از امنیت ملی، آگاهی از عدم صحت و ناقص بودن، موجه بودن برای حذف داده‌های شخصی، انتقال به کشورهای خارجی با سطح پایین امنیت، انتقال به کشورهای خارجی برای حفاظت از جان و مال سوژه، رمزنگاری داده، عمومی‌سازی داده، افشا به سازمان دیده‌بان حریم خصوصی
۵	دسترسی به داده	امکان دسترسی توسط کنترل‌گر، ارائه تمامی داده مربوط به شهروند، استفاده از روش‌های ایمن، ایجاد قابلیت ویرایش، رد درخواست سوژه مربوط به اطلاعات امنیت ملی، ارائه داده‌های شخصی قابل درک و بدون نیاز به نرم‌افزار، مجاز بودن رد درخواست سوژه به‌جهت وجود منع قانونی
٦	شخص موضوع داده	حق آگاهی از وجود داده نزد سازمان، رضایت یا عدم رضایت از پردازش داده‌های شخصی، پردازش داده‌های شخصی حساس، آگاهی از اطلاعات شخصی توسط نهاد ثالث، آگاهی از هویت متولی داده شخصی، اهداف گردآوری داده شخصی، دسترسی به داده شخصی، اصلاح داده شخصی غیردقیق، حق حذف داده‌های شخصی، حق درخواست تعلیق استفاده از داده‌های شخصی، پردازش تمام‌خودکار داده‌های شخصی، حذف داده‌های شخصی در صورت توجیه، آگاهی از منبع گردآوری، پیامدهای اعلام عدم رضایت، حق پیگرد قانونی هر خسارت، حق منع استفاده از داده‌های شخصی، حق حریم خصوصی سوژه، آگاهی از هویت متولی، حق تقاضای پذیرش غیرخودکار، حق آگاهی از زمان نگهداری
۷	مسئولیت کنترل‌گر	امنیت سازمانی برای حفاظت از داده‌های شخصی، امنیت فنی برای حفاظت از داده‌های شخصی، پاسخ‌گویی به تمام درخواست‌های سوژه، شفافیت در صورت رد درخواست سوژه، عقد قرارداد مکتوب با پردازشگر، تدارک امنیت فیزیکی (سخت‌افزار)، امنیت داده براساس سطح حساسیت، جبران خسارت براساس نقض حریم خصوصی اطلاعاتی، نصب مأمور حفظ حریم خصوصی اطلاعاتی، تدوین و انتشار برخط سیاست حریم اطلاعاتی، آگاه‌سازی کارکنان، در دسترس قراردادن سند امنیت کارکنان، انتخاب شایسته‌ترین پردازشگر، تعریف حوزه دسترسی کارکنان، استقرار سیستم احراز هویت

۶. نتیجه‌گیری و پیشنهادهای سیاستی

فساد و سوءاســـتفاده از داده‌ها یک تهدید نوپدید و جدی برای اقتصاد ملی، دارایی‌های دیجیتال، امنیت ملی و امنیت سیاسی- اجتماعی کشور به‌شمار می‌رود. فساد در زنجیره تأمین داده‌ها به شرایطی اطلاق می‌شود که طی آن دستیابی، گردآوری، ذخیره‌سازی، پردازش، افشا، انتقال، اعطای دسترسی به بانک داده و امحای داده‌ها با سوءاستفاده یا استفاده خارج از ضوابط قانونی و برای به‌دست آوردن منافع شخصی یا گروهی، صورت پذیرد. شواهد فساد در حوزه داده‌ها، عمدتاً در حوزه‌های اقتصادی و سیاسی- اجتماعی قابل مشاهده است و این اقدامات می‌تواند تبعات بسیار جدی را برای افراد، سازمان‌ها و حتی حاکمیت ملی در پی داشته باشـــد. بنابراین در جهان امروز حکمرانی داده یک ضرورت اجتناب‌ناپذیر است، طرح حکمرانی نمی‌تواند تهی از ابزارهای تقنینی، سیاستی، نظارتی و اجرایی برای زنجیره تأمین داده‌ها باشد. ازاین‌رو، چارچوب حکمرانی داده‌های کشور باید دربرگیرنده سیاست‌ها، مقررات، استانداردها و رویه‌های مناسب برای پیشگیری از بروز فساد در زنجیره تأمین داده‌ها باشد.

در این گزارش پس از بررسی مسئله فساد در زنجیره تأمین داده‌ها و ابعاد آن، دلایل بروز، بررسی شواهد فساد در زنجیره تأمین داده و درنهایت بررسی تجربیات تقنینی داخلی و خارجی با توجه به اقتضائات بومی و ساختارهای حکمرانی- سیاستی تأثیرگذار در کشور پیشنهادهایی در سه بخش: ۱. راهکارهای سیاستی- تقنینی، ۲. تقویت چارچوب‌های تنظیم‌گری و ۳. راهکارهای فنی و اجرایی برای جلوگیری از بروز فساد در این حوزه ارائه می‌شود.

۶-۱. تصویب قانون حمایت و حفاظت از داده و اطلاعات شخصی

در راستای اجرای اصول مختلف فصل سوم قانون اساسی جمهوری اســـلامی ایران راجع‌به «حقوق ملت» و به‌منظور رفع خلأهای قانونی مربوط به داده‌ها و اطلاعات به‌ویژه آن دسته اطلاعات که در فضای مجازی توسط ارائه‌دهندگان خدمات از مردم و کسب‌وکارها اخذ، گردآوری و پردازش می‌شود، حمایت و حفاظت از اشخاص موضوع داده، طرحی در تاریخ ۱۳۹۹/۷/۱۲ به شماره ثبت ۶۱۲ در مجلس یازدهم شورای اسلامی اعلام وصول شده است که با توجه به اهمیت حفاظت از داده‌های شـــخصی، این طرح نیازمند بررسی و تصویب ازسوی نمایندگان محترم مجلس شورای اسلامی است.

۶-۲. تصویب سند جامع امنیت فضای مجازی کشور

بسیاری از کشورها اسناد و راهبردهای مختلفی را برای امنیت فضای مجازی خود تدوین کرده‌اند (به‌طور مثال تصویب سند استراتژی ملی امنیت سایبری آمریکا در سال ۲۰۱۸ و تصویب سند استراتژی امنیت سایبری چین در سال ۲۰۱۴)، هدف این اسناد عموماً ارتقای امنیت فضای مجازی، حفاظت از اطلاعات حساس، پیشگیری از حملات سایبری، تضمین حفظ حریم خصوصی و محرمانگی اطلاعات است. ازاین‌رو و با توجه به ملاحظات و شواهد مختلف درخصوص حملات سایبری، هک خدمات، افشای اطلاعات و نشت داده‌ها در سال‌های اخیر، کشور نیازمند سندی جامع در زمینه «امنیت سایبری» می‌باشد. لذا پیشنهاد می‌شود تدوین و تصویب سند جامع امنیت فضای مجازی کشور با تأکید برنگاشت دقیق نهادی از دستگاه‌ها و نظارت مستمر بر آن از طریق نهاد ناظر و تصویب ضمانت اجرای سند مذکور توسط مجلس شورای اسلامی مورد مداقه و توجه نهاد سیاستگذار این حوزه (شورای عالی فضای مجازی) و همچنین مجلس شورای اسلامی قرار گیرد.

۶-۳. تصویب قانون الزام به انتشار داده و اطلاعات

یکی از اقدامات مهم در موضوع حکمرانی داده در راستای عدالت در دسترســـی به اطلاعات، مقابله با فساد، افزایش شفافیت و جلوگیری از ایجاد رانت‌های اطلاعاتی، الزام به انتشار داده‌ها و اطلاعات با حفظ حریم خصوصی ارتباطاتی و اطلاعاتی اشخاص حقیقی و حقوقی و اسرار حاکمیتی است. این مهم در مجلس یازدهم در سال ۱۳۹۹ طی طرحی به شماره ثبت ۲۸۳ اعلام وصول شد، اما تاکنون به تصویب کمیسیون و به‌تبع صحن علنی مجلس نرسیده است. لذا پیشنهاد می‌شود پیگیری تصویب این طرح در دستور کار هیئت‌رئیسه مجلس قرار گیرد.

۶-۴. تدوین دستورالعمل اجرایی توسط ستاد پدافند غیرعامل و فاوا

وفق ماده (۱۰۳) قانون برنامه هفتم پیشرفت برای هماهنگی دستگاه‌ها برای کنترل امنیت سایبری و نظارت مستمر بر آنها، کارگروه (کمیته) دائمی پدافند غیرعامل مسئول تدوین و تصویب استانداردها و ضوابط ارائه خدمات امن‌سازی و ارزیابی و رتبه‌بندی سالیانه امنیت رایانکی (سایبری) دستگاه‌های اجرایی است. لذا پیشنهاد می‌شود دستورالعمل اجرایی درخصوص حفاظت از داده‌ها توسط ستاد پدافند غیرعامل و فاوا تدوین و توسط شورای عالی فضای مجازی ابلاغ شود.

۶-۵. اتخاذ رویکرد ترکیبی در تدوین سند سیاستی حمایت حقوق افراد موضوع داده

مواجهه با چالش‌های مربوط به زنجیره تأمین داده‌ها، به‌خصوص زمانی که به داده‌های حساس یا شخصی مربوط می‌شود، نیازمند ترکیبی از رویکردهای قانونی، فنی و اجرایی است؛ بنابراین پیشنهاد می‌شـــود پیش‌بینی محورهای زیر توسط بازیگران زنجیره تأمین داده در سند سیاستی حمایت از حقوق افراد موضوع داده مورد توجه قرار گیرد:

شفافیت و رضایت کاربران در اشتراک‌گذاری داده‌ها برمبنای توافق‌نامه‌ها مورد تأیید نهاد تنظیم‌گر،

- تضمین امنیت داده‌ها،
- ناشناس‌سازی و مستعارسازی داده‌ها،
- حق اطلاع‌رسانی به شخص موضوع داده‌ها،
- حق دسترسی به داده‌ها،
- حق اصلاح داده‌ها،
- حق پاک کردن داده‌ها،
- حق اعتراض به داده‌ها،
- حق انتقال داده‌ها،
- حق قرار نگرفتن در معرض پردازش خودکار (الگوریتمی)،
- توانمندسازی و آموزش،
- ایجاد استانداردهای امنیتی،
- سیاست‌های انتقال داده‌های فرامرزی،
- سازوکارهای اخلاقی مدیریت داده‌ها.

۶-۶. اصلاح وظایف و ساختار کمیسیون موضوع ماده (۱۸) قانون انتشار و دسترسی آزاد به اطلاعات

این قانون یکی از سازوکارهای تنظیم‌گرانه برای نظارت کلی بر حسن‌اجرا و رفع اختلاف در قانون انتشار و دسترسی آزاد به اطلاعات تشکیل کمسیون ماده (۱۸) است؛ بااین‌وجود به‌دلیل برخی از موارد نظیر عدم عضویت بخش‌های غیردولتی و عدم ضمانت اجرایی مصوبات، به‌منظور افزایش اثربخشی، این کمیسیون نیازمند تقویت جایگاه است. لذا پیشنهاد می‌شود از طریق موارد زیر وظایف و ساختار کمیسیون اصلاح شود:

الف) افزودن اعضای فرادولتی (بخش خصوصی و سایر ذی‌ربطان حاکمیتی و بخش عمومی غیردولتی) به کمیسیون،

ب) پیش‌بینی وظایف قانونی و ضمانت اجرای اداری، انتظامی و قضایی برای مستنکفین از قانون،

ج) تعیین شاخص‌های ارزیابی عملکرد دستگاه‌ها و مؤسسات خصوصی و ارائه گزارش شش‌ماهه رتبه‌بندی دستگاه‌ها براساس این شاخص به هیئت‌وزیران و کمیسیون فرهنگی مجلس شورای اسلامی.

۶-۷. استقرار تنظیم‌گر بخشی داده‌ها از طریق تقسیم‌کار و همکاری میان دو نهاد تنظیم‌گر

به‌منظور هم‌افزایی و اثربخشـــی بالاتر اقدامات تنظیم‌گرانه درخصوص مدیریت داده‌ها و جلوگیری از بروز فساد در زنجیره تأمین داده‌ها، پیشنهاد می‌شود ماده‌واحده تقسیم‌کار ملی برای همکاری میان دو نهاد تنظیم‌گر (کمیسیون داده‌ها و اطلاعات ملی موضوع ماده (۳) قانون مدیریت داده‌ها و اطلاعات ملی و کمیسیون داده‌ها موضوع ماده (۱۸) قانون انتشار و دسترســـی آزاد به اطلاعات) به تصویب شورای عالی فضای مجازی برسد.

منابع و مآخذ

۱. مجلس شورای اسلامی؛ «قانون مدیریت داده‌ها و اطلاعات ملی». ۱۴۰۱، مرکز پژوهش‌های مجلس شورای اسلامی: تهران.

2. Zhang, R., et al., New engines of economic growth: How digital currencies lead the way to growth in the era of digital economy. Economic Analysis and Policy, 2023. 80.

3. Panjaitan, F.H. and Y. Indawati, Misuse of Personal Data on Illegal Fintech.

4. Greenwood, D., et al., The new deal on data: A framework for institutional controls. Privacy, Big Data, and the public good: Frameworks for engagement, 2014. 1.

5. Sheet, E.C.-F. uestions and Answers - Data protection reform package. 2017.

6. Confessore, N., Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, in The New York Times. 2018.

۷. انصاری، باقر. «حقوق داده‌ها و هوش‌مصنوعی مفاهیم و چالش‌ها، ۱. ۱۴۰۰، تهران: سهامی انتشار.

8. EU, General Data Protection Regulation 2016/679 (GDPR). 2016.

۹. مجلس شورای اسلامی؛ «قانون تجارت الکترونیکی». ۱۳۸۲، مرکز پژوهش‌های مجلس شورای اسلامی ایران: تهران.

۱۰. مجلس شورای اسلامی؛ «قانون انتشار و دسترسی آزاد به اطلاعات». ۱۳۸۷، مرکز پژوهش‌های مجلس شورای اسلامی: تهران.

11. EU, Open Data and the re-use of public sector information (recast). 2019.

12. Brevini, B., Metadata laws, journalism and resistance in Australia. Media and Communication, 2017.

13. Group's, T.W.B. Data protection and privacy laws. 2021; Available from: https://id۴d.worldbank.org/guide/data-protection-and-privacy-laws.

14. Komnenic, M., 61 Biggest GDPR Fines & Penalties So Far, in TERMLY 2024.

15. Shastri, S., M. Wasserman, and V. Chidambaram. The seven sins of {Personal-Data} processing systems under {GDPR}. in 11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 19). 2019.

16. Aguilar Rivera, A.M. and K. Vassil, Estonia. 2015.

17. Pullis, G., What Are Walled Gardens? Understanding Their Significance and Impact. 2023.

18. Imperva, Data Security, in Imperva. 2020.

۱۹. تقوی‌فرد، سیدمحمدتقی؛ تقوا، محمدرضا؛ فقیهی، مهدی؛ جمشیدی، محمدجواد. «مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب. مجلس و راهبرد، ۲۰۱۷. ۸۹(۲۴).

20. Florent Thouvenin and Aurelia Tamò-Larrieux, Big Data and Global Trade Law. 2021: Published online by Cambridge University Press

گزیده سیاستی

فساد در زنجیره تأمین داده‌های کشور به‌طورکلی به سوءاستفاده یا استفاده خارج از ضوابط قانونی از داده‌ها برای به‌دست آوردن منافع شخصی یا گروهی در حوزه‌های اقتصادی و سیاسی– اجتماعی اطلاق می‌شود که مواجهه با آن در گرو تقویت الزامات سیاستی، تقنینی، نظارتی و اجرایی در جمع‌آوری، پردازش، استفاده، دسترسی، حقوق افراد موضوع داده و ذخیره‌سازی آن است.

مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاسـداران، روبروی پـارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

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

وب‌سایت: rc.majles.ir