دوفصلنامهٔ تخصصی حقوق فناوری‌های نوین، دورهٔ دوم، شمارهٔ ۴، پاییز و زمستان ۱۴۰۰، صفحهٔ ۱-۲۲

مطالعهٔ اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا

فاطمه قناد،[۱] الهام شریف[۲]

تاریخ دریافت: ۱۳۹۹/۵/۳۰ تاریخ پذیرش: ۱۴۰۰/۶/۱۵

نوع مقاله: پژوهشی

چکیده

حمایت از حریم ***خصوصی*** افراد، به‌منزلهٔ یک اصل جهانی، همواره مورد توجه نهادهای بین‌المللی قرار داشته و در بسیاری از اسناد بین‌المللی به رعایت حریم خصوصی افراد تصریح شده است. امروزه داده‌های شخصی افراد به لحاظ پیشرفت فناوری و قابلیت پردازش و انتقال سریع و در دسترس بودن آن‌ها در فضای مجازی بیش از هر زمان دیگر مورد توجه خاص قانونگذاران قرار گرفته است. در این میان، اتحادیهٔ اروپا پیشتاز بوده است و سند بین‌المللیِ «مقررات عمومی حفاظت از داده‌ها» یا به اختصار جی دی پی آر (GDPR) را به‌عنوان جایگزینی جامع برای «قانون حفاظت از دادهٔ اتحادیهٔ اروپا» در آوریل سال ۲۰۱۶ تنظیم کرد که در ۲۵ می ۲۰۱۸ از سوی پارلمان اروپا تصویب و لازم‌الاجرا شد. در این مقاله، با نگاهی به تاریخچهٔ حمایت از حریم خصوصی و بررسی مفهوم و دامنهٔ شمول داده‌های شخصی در سند بین‌المللی جی دی پی آر و نظام حقوقی ایران، ضرورت اصلاحاتی در زیرساخت‌ها و قانونگذاری جمهوری اسلامی ایران در زمینهٔ حمایت هرچه بیشتر از حریم خصوصی در فضای مجازی مطرح می‌شود.

واژگان کلیدی: داده‌های شخصی، حریم خصوصی، حمایت از داده‌ها، سند بین‌المللی مقررات عمومی حمایت داده‌های اروپایی، جی دی پی آر

---

۱. دانشیار گروه حقوق، دانشگاه علم و فرهنگ، تهران؛ ghanad@usc.ac.ir

۲. کارشناس ارشد رشته حقوق تجارت الکترونیکی، دانشگاه علم وفرهنگ، تهران؛ elhamsharif@hotmail.com

مقدمه

شبکه‌های اجتماعی از پدیده‌های فراگیر عصر حاضرند که در ابتدا فرایند تعامل افراد با یکدیگر را تسهیل می‌کنند؛ اما در این میان حجم زیادی از داده‌ها که نشان‌دهندهٔ هویت فردی، دیدگاه‌ها، نظرها و علایق افراد است در بستر شبکه‌های اجتماعی، از اینستاگرام و فیس‌بوک و توییتر گرفته تا پیام‌رسان‌هایی مانند تلگرام، واتس‌اپ و غیره، به اشتراک گذاشته می‌شود. امروزه به لحاظ پیشرفت فناوری، ماهیت شبکه‌های اجتماعی و اینترنت، همچنین قابلیت پردازش و انتقال سریع داده‌ها و نیز با توجه به حساسیت اطلاعاتی که روزانه میان میلیاردها نفر جابه‌جا می‌شود، ضرورت ایجاد مجموعه قوانین و چارچوب‌های جدید برای حمایت از داده‌های شخصی افراد بیش از هر زمان دیگری احساس می‌شود.

اخیراً یکی از تکان‌دهنده‌ترین اخباری که درخصوص پردازش غیرقانونی داده‌ها در جهان مطرح شد، پرده‌برداشتن از فعالیت شرکت کمبریج آنالیتیکا و فیس‌بوک بود که طی آن شرکت کمبریج آنالیتیکا داده‌های شخصی میلیون‌ها کاربر فیس‌بوک را به‌نحو غیرقانونی بدون رضایت علنی آن‌ها جمع‌آوری و تحلیل کرد و نتیجهٔ آن را در اختیار نهادهای انتخاباتی ریاست‌جمهوری سال ۲۰۱۷ آمریکا قرار داد (ur Rehman, 2019).

در این راستا و با توجه به تهدیدات موجود در ارتباط با نقض حریم خصوصی و داده‌های شخصی افراد، اغلب نظام‌های قانونی در صدد تدوین قوانین روزآمد برای حمایت از این مهم بوده و هستند. نخستین جلوه‌های حمایت از حریم خصوصی در اسناد بین‌المللی حقوق بشر به‌چشم می‌خورد. برخی از این اسناد به‌طور کلی بر اصل حمایت از حریم خصوصی تمرکز داشته و برخی مستقیماً به حمایت از حریم خصوصیِ اطلاعاتی و ارتباطی پرداخته‌اند. مهم‌ترین قانونگذاری فرامنطقه‌ای مرتبط با حوزهٔ حریم خصوصی و حمایت از اطلاعات را می‌توان در قوانین جی دی پی آر (GDPR)[1] و اسناد OECD مشاهده کرده که از پیشرفته‌ترین اسناد موضوعی مرتبط با حوزهٔ گردش آزاد اطلاعات و حریم خصوصی به‌شمار می‌روند (قناد، ۱۳۹۰). از اسناد بین‌المللی پایه‌گذار حمایت از حریم خصوصی می‌توان به اعلامیهٔ جهانی حقوق بشر و کنوانسیون اروپایی

1. Guide to General Date Protection Regulation, available at https://ico.org.uk/

حقوق بشر اشاره کرد. اعلامیهٔ جهانی حقوق بشر ۱۹۴۸، در مادهٔ ۱۲ خود، چنین مقرر می‌دارد: «احدی نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود مورد تعرض خودسرانه قرار گیرد. شرافت و اسم و رسمش نباید مورد حمله واقع شود. هرکس حق دارد که در مقابل این‌گونه تعرضات و حملات، مورد حمایت قانون قرار گیرد.» در سایر اسناد بین‌المللی نیز حمایت از حریم خصوصی مورد توجه قرار گرفته است، از جمله مادهٔ ۱۸ اعلامیهٔ اسلامی حقوق بشر، مادهٔ ۵ کنوانسیون بین‌المللی منع کلیهٔ اشکال تبعیض‌نژادی ۱۹۶۶، مادهٔ ۱۰ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی، و اخیراً مقررات عمومی حفاظت از داده‌های اروپایی مصوب ۲۰۱۸ که جامع‌ترین قانون حاضر در این خصوص به‌شمار می‌رود.

در حال حاضر، در نظام حقوقی ایران قانون مشخصی که به حفاظت از داده‌های شخصی اختصاص یافته باشد تصویب نشده است؛ بااین‌حال، قوانین و آیین‌نامه‌های متعددی وجود دارد که از حریم خصوصی افراد در همهٔ فضاها به‌خصوص فضای مجازی حمایت می‌کند؛ از آن جمله می‌توان از قانون احترام به آزادی‌های مشروع و حقوق شهروندی مصوب ۱۳۸۳، قانون آیین دادرسی کیفری، قانون جرایم رایانه‌ای،[1] قانون انتشار و دسترسی آزاد به اطلاعات و همچنین قانون تجارت الکترونیک مصوب ۱۳۸۲ نام برد که مواد ۵۸ تا ۶۱ آن‌ها صرفاً به موضوع داده‌های شخصی اختصاص یافته است.

در این نوشتار سعی بر آن بوده است تا با نگاهی دقیق به پیشینهٔ حریم خصوصی، تعریف و دامنهٔ شمول دادهٔ شخصی در اسناد بین‌المللی، به‌ویژه سند جی دی پی آر[2] که در حال حاضر کامل‌ترین سند در خصوص حمایت از دادهٔ شخصی است، نواقص و کاستی‌های موجود در نظام حقوقی ایران و لزوم اصلاحات مورد بررسی قرار گیرد.

۱. تعریف دادهٔ شخصی

شاید یکی از چالش‌برانگیزترین دل‌مشغولی‌های امروز افراد در عصر دیجیتال حفظ امنیت حریم خصوصی و داده‌های شخصی‌شان باشد، زیرا فضای مجازی درعین‌حال که به افراد اجازه می‌دهد در مقابل سایرین به‌صورت بی‌نام‌ونشان فعالیت کنند، برای دولت‌ها و

۱. متن قانون قابل دسترسی در تارنمای مرکز پژوهش های مجلس شورای اسلامی به آدرس https://rc.majlis.ir/fa/law/show/135717

2. The General Data Protection Regulation, (EU) 2016/679

شرکت‌های عرضه‌کنندهٔ خدمات نیز امکان رصد فعالیت‌هایی را فراهم می‌کند که در صورت پردازش ممکن است دارای ارزش اقتصادی یا سیاسی باشند (Wachter et al., 2019, pp.120-128). یکی از اهداف تدوین قوانین حمایت از داده‌های شخصی نیز این است که در این خصوص امکان کنترل بیشتری به کاربران بدهد. داده‌های حاصل از رفتار امروز مشتری ممکن است رفتار فردای او را پیش‌بینی کند (Tamo-Larrieux, 2018, p.46). از طرفی، در اقتصاد دیجیتالی امروز، داده حکم سرمایه را دارد. شرکت‌های مختلف با تجزیه‌وتحلیل داده‌ها به الگوهای جدید و شایان‌توجهی دست می‌یابند. شاید یکی از بزرگ‌ترین چالش‌های اقتصاد دیجیتال دنیای مدرن این حقیقت است که افراد باارزش‌ترین داده‌های مربوط به خود را برای بهره‌مندی از خدمات اینترنتی به رایگان در اختیار شرکت‌ها و سازمان‌ها می‌گذارند و سپس همان شرکت‌ها و سازمان‌ها با استفاده از شیوه‌های فروش و بازاریابی داده‌های باارزش کاربران را به قیمت گزافی به خود آن‌ها می‌فروشند (Lehtiniemi & Kortesniemi, 2017). براساس برخی برآوردها، ارزش مالی داده‌های شخصی شهروندان اروپایی در سال ۲۰۲۰ حدود یک تریلیون یورو است (van Lieshout, 2015, pp.26-38). در گزارش گروه مشاوران بوستون در سال ۲۰۱۲، ارزش حاصل از داده‌های دیجیتالی میزان ناخالص درآمد داخلی کشورهای اتحادیهٔ اروپا را نزدیک به ۸ درصد افزایش می‌دهد.[۱] شایان ذکر است در قوانین اروپا و آمریکا کسی که به هر دلیل ـ از جمله به‌عنوان رسا۲ ـ عالمانه اطلاعاتی را در فضای الکترونیکی در اختیار دارد، ملزم به رعایت استانداردهای متعارف در نگه‌داری از آن‌ها است (السان، ۱۳۹۷، ص ۱۲۸–۱۲۷). بنابراین طبیعی است که دسترسی، جمع‌آوری، تحلیل و انتقال این اطلاعات نیز باید مانند هر اطلاعات ارزشمند دیگری قانونمند باشد.

در این راستا، پیش از هر چیز به تعریفی جامع و صحیح از حریم خصوصی و داده‌های شخصی و حدود و دامنهٔ آن‌ها نیاز داریم. یکی از جامع‌ترین تعاریف در اسناد حقوقی ایران از حریم خصوصی در سند «آیین‌نامهٔ اجرایی قانون انتشار و دسترسی آزاد

۱. موجود در وب‌سایت رسمی گروه مشاوران بوستون به آدرس www.bcg.com/The Value of Our Digital Identity

۲. عرضه‌دهندگان خدمات اطلاع‌رسانی و اینترنت

به اطلاعات» مصوب سال ۱۳۹۳ آمده است که حریم خصوصی را این‌گونه تعریف می‌کند: «قلمروی از زندگی شخصی فرد که انتظار دارد دیگران بدون رضایت یا اعلام قبلی

وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، واردشدن، نظاره‌کردن، شنود، دسترسی اطلاعات فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره‌شدهٔ خصوصی نظیر هتل و کشتی، همچنین آنچه حسب قانون فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود، از قبیل اسناد تجاری و اختراعات و اکتشافات.»

بنابراین داده‌های شخصی بخش چشمگیری از حریم خصوصی افراد را تشکیل می‌دهد که تعریف آن را در قوانین کشورمان باید به‌صورت جسته و گریخته در قوانین مختلف جست‌وجو کنیم. حریم خصوصی را می‌توان به دو گروه اطلاعات خصوصی و داده‌های شخصی تقسیم کرد. اطلاعات خصوصی به شیوه‌های جمع‌آوری، ضبط، دسترسی و آزادسازی اطلاعات اشاره دارد. اما داده‌های شخصی مربوط به حریم شخصی و فضای خصوصی فرد است (قناد و علیقلی، ۱۳۹۸).

در تعریفی دیگر می‌خوانیم، داده‌های شخصی هرگونه اطلاعات مستقیم یا غیرمستقیم دربارهٔ یک شخص حقیقی شناخته‌شده یا قابل‌شناسایی است که از طریق ارجاع به یک شمارهٔ شناسایی یا یک یا چند عنصر که ویژهٔ آن شخص است صورت می‌گیرد (زرکلام، ۱۳۹۱، ص۱۳۴). این تعریف اقتباسی مستقیم از مقررات عمومی حفاظت از داده‌های شخصی اروپا است. در لایحهٔ صیانت و حفاظت از داده‌های شخصی[1] سال ۱۳۹۷ که هنوز به تصویب مجلس شورای اسلامی نرسیده است، دادهٔ شخصی این‌گونه تعریف می‌شود: «دادهٔ شخصی عبارت است از داده‌هایی که به‌تنهایی یا به همراه داده‌های دیگر، مستقیم یا غیرمستقیم، شخص موضوع داده را از طریق یک شناسه می‌شناساند.» در همین لایحه تعریفی با عنوان «داده‌های شخصی حساس» وجود دارد با این مضمون که «دادهٔ شخصی حساس عبارت است از دادهٔ شخصی که ریشهٔ قومی یا قبیله‌ای، آرای سیاسی و مذهبی و فلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار

۱ متن لایحه قابل دسترسی در تارنمای مرکز پژوهش های مجلس شورای اسلامی به آدرس rc.majlis.ir/fa/news/show/1067376

می‌سازد.» که تقریباً مصداق همان داده‌های خاص[1] مقررات عمومی حفاظت از داده‌های اروپا است که در ادامه تعریف خواهد شد.

در حال حاضر، یکی از جامع‌ترین و کارآمدترین تعاریفی که از داده‌های شخصی شده است تعریف اتحادیهٔ اروپا در سند جی دی پی آر است که داده‌های شخصی را داده‌هایی تعریف می‌کند که می‌توان با استفاده از آن‌ها مستقیم و یا غیرمستقیم یک شخص را شناسایی کرد. در بند الف مادهٔ ۴ این مقرره داده‌های شخصی این‌گونه تعریف شده است: «هر اطلاعاتی که مرتبط با یک شخص حقیقی شناخته‌شده یا قابل‌شناسایی باشد ("موضوع داده")؛ یک شخص حقیقی قابل‌شناسایی کسی است که مستقیم یا غیرمستقیم به‌ویژه با اشاره به یک شناسهٔ خاص مانند نام، شمارهٔ شناسایی، اطلاعات مکانی، شناسهٔ آنلاین، و یا با اشاره به یک یا چند ویژگی ازجمله فیزیکی، روان‌شناختی، ژنتیکی، ذهنی، اقتصادی یا اجتماعی قابل‌شناسایی باشد.» همچنین این سند به دستهٔ خاصی از اطلاعات شخصی تحت عنوان داده‌های خاص یا داده‌های حساس اشاره می‌کند که «داده‌هایی از قبیل ملیت، نوع مذهب، رنگ پوست، دیدگاه فرد به مسائل سیاسی و غیره را شامل می‌شود که همهٔ این‌ها نیز بخشی از اطلاعات شخصی محسوب می‌شوند.»

۲. حفاظت از داده‌های شخصی در اتحادیهٔ اروپا

اتحادیهٔ اروپا همواره برای تدوین مقرراتی در حمایت از حریم خصوصی افراد کوشیده است و اخیراً در سال ۲۰۱۸ مقرراتی را به نام مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا معروف به سند جی دی پی آر به تصویب رساند که در حقیقت جایگزینی برای قانون حفاظت از دادهٔ اتحادیهٔ اروپا[2] است. جی دی پی آر مجموعه مقرراتی است که در مورد حفاظت از داده و محرمانگی همهٔ اشخاص و خروج داده در اتحادیهٔ اروپا و منطقهٔ اقتصادی اروپا وضع شده است. این مقرره در ۱۱ فصل و ۹۹ ماده برای حفظ محرمانگی، اعطای کنترل داده‌ها به شهروندان و ساکنان این منطقه و یکسان‌سازی مقررات تنظیم شده است و شامل احکام و الزاماتی مرتبط با پردازش اطلاعات شخصی قابل‌تشخیص در اتحادیهٔ اروپا درخصوص همهٔ کسب‌وکارهایی که با این منطقهٔ اقتصادی مراودهٔ کاری

1. Special category
2. Data Protection Directive, EC/95/46

دارند، صرف‌نظر از مکان استقرارشان، می‌شود. بدین ترتیب، فرایندهای کسب‌وکارهایی که اطلاعات شخصی را اداره می‌کنند، باید مبتنی بر «حفاظت اطلاعات از طریق طراحی و به‌طور پیش‌فرض» باشد؛ یعنی اطلاعات شخصی باید به‌گونه‌ای ذخیره شود که حداکثر محرمانگی به‌طور پیش‌فرض درنظر گرفته شود، به‌نحوی که داده‌ها به‌هیچ‌وجه بدون رضایت صریح افراد، در دسترس عمومی قرار نگیرد.

اگرچه این قواعد بر مبنای مقرره‌های قبلی بنا شده است، موانع جدیدی را بر سر راه شرکت‌ها و حتی کاربران قرار می‌ده که بسیاری را در هر کسب‌وکار و بازاری نگران کرده است. نه این‌که وضع این مقررات جدید غیرضروری بوده باشد، اما چالش‌هایی به همراه می‌آورد که عملاً هر سازمانی را در سرتاسر جهان تحت تأثیر قرار می‌دهد (Caldear, 2016, pp.54-59). شاید یکی از چالش‌برانگیزترین مواردی که به این سند اضافه شده است حق قابلیت انتقال داده‌ها است (Mitchell, 2016) که در مادهٔ ۱۸ بیان می‌کند: «صاحب داده می‌تواند داده‌های خود را که به یک کنترل‌کننده داده است از او بگیرد و حق نشر آن را توسط او ساقط کند و آن را به هر شکل و قالب دلخواه در اختیار کنترل‌کنندهٔ دیگری قرار دهد.» سال‌های سال، سازمان‌هایی که به جمع‌آوری و بازاریابی و دیگر موارد استفاده از داده‌ها مشغول بودند گمان می‌کردند داده‌هایی که مجوز استفاده از آن‌ها را یک‌بار از صاحب آن گرفته‌اند برای همیشه متعلق به آن‌ها خواهد بود؛ اما اکنون صاحب داده می‌تواند بدون هیچ توضیح یا دلیلی اطلاعاتش را از یک پایگاه داده‌ها پاک کند یا نسخه‌ای از همهٔ آن‌ها را به کنترل‌کنندهٔ دیگری بدهد. از قضا این کنترل‌کننده ممکن است بزرگ‌ترین رقیب کنترل‌کنندهٔ قبلی باشد. اگرچه مقررات جی دی پی آر به حفاظت از اطلاعات شخصی کاربران کمک می‌کند، گاهی کاربران را در فضای سایبری سردرگم نگاه می‌دارد که یکی از مصادیق آن افزایش پیام‌های هشداردهنده است که کاربر برای دسترسی به سایت باید ابتدا آن‌ها را تأیید کند (Caldaer, 2016, pp.16-18). از دیگر تغییراتی که جی دی پی آر به ارمغان آورده است قوانین بهاشتراک‌گذاشتن داده‌ها پس از جمع‌آوری است. داده‌هایی که یک سایت ساده جمع‌آوری می‌کند گاهی به چند شرکت مختلف فروخته می‌شود که پیش از این کاربر اطلاعات چندانی درباره آن‌ها نداشت (Ibid). اما اکنون الزامات جدید سایت‌ها را به ارائهٔ اطلاعات شفاف دربارهٔ

دریافت‌کنندگان داده‌ها و اهداف آن‌ها ملزم می‌کند. در ادامه به بررسی تفصیلی این سند می‌پردازیم.

۱-۲. دامنهٔ شمول

مقررهٔ موردبحث (جی دی پی آر) از داده‌های شخصی افراد و کسانی که به‌طور فیزیکی در اتحادیهٔ اروپا ساکن هستند محافظت می‌کند، حتی اگر شهروند اتحادیهٔ اروپا نباشند. با توجه به حوزه‌ای که برای داده‌های شخصی تعریف شده است، دایرهٔ شمول و حوزهٔ قابلِ‌اعمال آن بسیار گسترده است و به‌طور مشخص شامل همهٔ وب‌سایت‌ها و برنامه‌هایی می‌شود که فعالیت کاربران خود را در فضای دیجیتالی به‌نوعی پایش می‌کنند (von Goethem, 2018, p.23). به عبارت کلی، در صورتی که هریک از کنترل‌کننده، پردازنده یا موضوع داده در اتحادیهٔ اروپا باشد، مقررات این قانون نافذ خواهد بود.[1] اگرچه جی دی پی آر سندی اروپایی است، در هر سازمانی که داده‌های شخصی مربوط به یک شهروند اتحادیهٔ اروپا یا هر شخصی که در این منطقه زندگی می‌کند را نگه‌داری یا پردازش می‌کند اِعمال می‌شود.

۲-۲. هفت اصل زیربنایی جی دی پی آر

۲-۲-۱. اصول پردازش داده‌های شخصی

طبق این مقرره، داده‌های شخصی باید به‌صورت قانونی، با رعایت انصاف، و به‌نحوی شفاف دربارهٔ موضوع داده پردازش شوند. در مادهٔ ۵ این مقرره به سه اصل «قانونمندی»، «عدالت» و «شفافیت» اشاره شده است که همواره باید در پردازش داده‌های شخصی مورد توجه قرار گیرد. مواد ۲۴، ۲۵ و ۳۲ مقررهٔ مذکور اقدامات فنی ویژه‌ای را در راستای مخاطرات پردازش داده الزامی می‌دارد. این بدین معناست که کنترل‌کننده یا پردازشگر باید مطابق با فعالیت‌های خود اقدامات فنی متناسبی لحاظ کند (Bitar & Jakobsson, 2017). جی دی پی آر در بند ۲ مادهٔ ۵ و مادهٔ ۳۰ تصریح می‌کند مستند این اقدامات همواره باید برای اثبات، مطابقت و ارائه به مقامات ناظر آماده باشد. در متن مقرره این اقدامات فنی به‌صراحت مشخص نشده‌اند و هیچ توضیحی جز آن‌که داده‌های شخصی باید با رضایت شخصِ موضوعِ داده و با رعایت حسن‌نیت جمع‌آوری، ذخیره یا پردازش

1. General Data Protection Regulation (GDPR), available at https://gdpr-info.eu/

شوند نیامده است. در این خصوص، مرکز امنیت اینترنت سی آی ای برای کمک به سازمان‌ها در تحصیل امنیت سایبری و مطابقت با الزامات امنیتی دستورالعملی به نام «کنترل‌های حیاتی برای دفاع مؤثر سایبری»[۱] تنظیم کرده است که نسخهٔ نهایی آن شامل بیست کنترل حیاتی است که از میان آن‌ها ده کنترل حفاظت از داده‌ها در میان کنترل‌های امنیتی بحرانی پایه قرار دارند.[۲]

۲-۲-۲. مشروعیت پردازش

طبق مادهٔ ۶ فصل دوم، این مقرره اصل پردازش داده‌های شخصی را فقط تحت شرایط خاصی قانونمند می‌داند که از آن جمله رضایت شخص، مطابقت داده‌ها با قوانین و مقررات حاکم، تابعیت از مقررات عمومی، هدف مشخص و حفظ محرمانگی لازمهٔ آن است.

۲-۲-۳. اصل رضایت

اصل رضایت یکی از مهم‌ترین اصول این قانون و اساس شروع به پردازش است. مادهٔ ۷ از فصل دوم تصریح می‌دارد، برای هرگونه پردازش داده‌های شخصی، فرد باید علاوه‌بر رضایت کامل، از نحوه و زمان و هدف پردازش نیز آگاه و به آن‌ها نیز رضایت داشته باشد. همچنین شخص می‌تواند، پس از اعلام رضایت، آن را پس بگیرد. مطابق با قوانین جی دی پی آر رضایت باید علنی، منحصربه‌فرد، مشخص و بدون هرگونه ابهام باشد. قانونگذار با این الزامات قصد داشته است موانع بیشتری سر راه شرکت‌ها برای گرفتن رضایت کاربران برای پردازش اطلاعاتشان بگذارد (**Gocheva**, 2017).

۲-۲-۴. شرایط ناظر بر رضایت اشخاص صغیر در مورد داده‌های شخصی

بند ۱ مادهٔ ۸ این قانون بیان می‌کند، اطلاعات مربوط به افراد زیر شانزده سال باید با رضایت ولی قانونی آن‌ها باشد و کنترل‌کننده باید به طرق قانونی از رضایت حتمی ولی فرد اطمینان یابد.

---

۱ CIS Critical Security Controls for Effective Cyber Defense کنترل‌های امنیتی بحرانی ابتدا سال ۲۰۰۸ توسط مؤسسه SANS تدوین و سپس در سال ۲۰۱۵ به CIS (Center for Internet Security) منتقل شدند. این دستورالعمل‌ها در راستای کسب امنیت سیستم‌های اطلاعاتی و داده‌ها در سطح جهانی تنظیم شده و همواره توسط متخصصان فناوری بررسی و به روز رسانی می‌شوند.

۲. The CIS 20 Critical Security Controls Explained, available at https://www.cisecurity.org

۲-۲-۵. پردازش داده‌های شخصی خاص

در بند ۱ مادهٔ ۹ این قانون می‌خوانیم، پردازش داده‌های خاص که اطلاعات نژادی، قومی، دیدگاه سیاسی، اعتقادات مذهبی و فلسفی، عضویت اتحادیه‌ها و اصناف، داده‌های ژنتیکی، داده‌های بیومتریک شناسایی افراد، داده‌های پزشکی و گرایش‌های جنسی را آشکار می‌کنند ممنوع است. البته این ماده استثنائاتی را نیز مطرح می‌کند؛ برای مثال، وقتی‌که دولت ضرورت پردازش چنین داده‌هایی را در جهت حفظ نظم عمومی یا جلوگیری از وقوع جرم لازم بداند.

۲-۲-۶. پردازش داده‌های شخصی مربوط به جرایم و محکومیت‌های کیفری

مادهٔ ۱۰ فصل دوم این سند بیان می‌دارد، پردازش داده‌های شخصی مربوط به جرایم و مجازات کیفری فقط تحت کنترل مقامات قضایی و رسمی و برای اهداف امنیتی مجاز است.

۲-۲-۷. پردازش داده‌هایی که نیاز به شناسایی ندارد

طبق بند ۱ مادهٔ ۱۱ فصل دوم این سند، اگر هدفی که کنترل‌کننده برای آن داده‌های شخصی را پردازش می‌کند نیازی به شناسایی موضوع داده نداشته باشد، وی موظف به حفظ، تحصیل یا پردازش اطلاعات بیشتری در جهت شناسایی موضوع داده (فقط درخصوص آن هدف خاص) نیست.

۲-۳. حقوق موضوع داده

فصل سوم این سند به حقوق موضوع داده یا شخص اختصاص یافته است و در چهار بخش به‌تفصیل این حقوق صراحتاً بیان می‌شود. اولین اصل این مبحث «اصل شفافیت و کیفیت» است که طبق آن کنترل‌کننده موظف است همواره موضوع داده را از هرگونه اطلاعات مزبور به او مطلع سازد. همچنین کنترل‌کننده موظف است هرگونه اطلاعات مربوط به زمان و مکان پردازش داده‌ها را به اطلاع موضوع داده برساند. موضوع داده همچنین باید از اهداف پردازش، اطلاعات مربوط به داده‌های شخصی خود، دریافت کنندگان داده‌ها، نحوهٔ دسترسی و کنترل داده‌هایش نیز مطلع باشد. موضوع داده حق دارد در صورت هک یا افشای اطلاعاتش در اسرع وقت مطلع شود. در صورتی که داده‌های کاربران به هر دلیلی در معرض افشاشدن قرار گیرد، سازمان مربوطه باید حداکثر طی ۷۲

ساعت این مسئله را به اطلاع آن‌ها برساند. یکی دیگر از بندهای جی دی پی آر درخصوص حمایت از موضوع داده، حق پاک‌سازی اطلاعات است که به کاربر اجازه می‌دهد به‌صورت شفاهی یا کتبی و بدون اعلام هیچ دلیل به‌خصوصی خواستار حذف داده‌هایش از پایگاه دادهٔ یک سایت شود. یافته‌ها نشان می‌دهند این سند تأثیر بسزایی در شفافیت، کنترل، اعتماد و امنیت عمومی داده‌ها داشته است؛ اما کاربران هنوز به‌درستی از حقوق خود آگاه نیستند و در نهایت، اگرچه افراد این مقرره را تضمینی برای حفاظت از داده‌های شخصی خود می‌بینند، آنچه میزان موفقیت این مقررات جدید را تعیین می‌کند میزان وفاداری و مسئولیت‌پذیری شرکت‌ها و سازمان‌ها است (Kovacs, 2019).

۲-۴. مسئولیت کنترل‌کننده‌ها و پردازشگرها

در مقررهٔ جدید جی دی پی آر، وظایف مجزایی برای کنترل‌کننده و پردازشگر درنظر گرفته شده است.

طبق تعریف اتحادیهٔ اروپا، کنترل‌کننده «کسی است که به‌تنهایی یا مشترکاً با دیگران اهداف و روش‌های پردازش داده‌های شخصی را تعیین می‌کند». چرایی و چگونگی پردازش داده‌ها با تصمیم کنترل‌کننده تعیین می‌شود. همچنین، این قانون یک نکتهٔ دیگر به تعریف کنترل‌کننده اضافه می‌کند و آن نکته این است که کنترل‌کننده تصمیم می‌گیرد کدام‌یک از انواع داده‌های شخصی باید ذخیره شوند. کنترل‌کننده کسی است که به‌صورت قانونی منطق پردازش و روش‌های آن را تعیین می‌کند. اما زمانی که عملیات پردازش غیرقانونی انجام می‌شود و باید کنترل‌کنندهٔ مسئول پیدا شود، ممکن است در نهایت یک شخص حقیقی یا حقوقی یا یک مقام عمومی که تصمیم پردازش داده‌ها را اتخاذ کرده است مسئول شناخته شود. در چنین مواردی، صرف‌نظر از این‌که آن شخص قانوناً اختیار انجام این کار را داشته است یا خیر، باید کنترل‌کننده درنظر گرفته شود. بنابراین درخواست حذف داده‌ها و توقف پردازش باید همیشه به کنترل‌کنندهٔ «واقعی» ارائه شود، فارغ از این‌که صلاحیت قانونی داشته است یا خیر.

طبق تعریف جی دی پی آر، پردازنده یک شخص حقیقی، حقوقی یا سازمانی است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند. وظایف و فعالیت‌های محول‌شده به پردازنده ممکن است کاملاً محدود به یک عمل یا زمینهٔ بسیار خاص باشد

یا ممکن است به‌صورت کلی و فراگیر باشد. در حقوق شورای اروپا، معنای پردازنده با معنی آن در حقوق اتحادیهٔ اروپا یکسان است. پردازنده‌ها، علاوه‌بر پردازش داده‌های دیگران، شخصاً کنترل‌کننده‌های پردازش داده‌های مرتبط با اهداف شخصی خود مثلاً ادارهٔ امور کارمندان، فروش و یا حساب‌های خودشان نیز خواهند بود. در نهایت آنچه از سند جی دی پی آر درخصوص مسئولیت کنترل‌کننده‌ها و پردازشگرها برداشت می‌شود این است که پردازشگر باید نرم‌افزار یا سازوکار حذف یا محوکردن داده‌های شخصی را در اختیار کنترل‌کننده بگذارد. البته این موضوع ممکن است در آینده مشکلاتی به‌وجود آورد که کاربر یا کنترل‌کننده بخواهد بداند چرا اطلاعات ذخیره‌شدهٔ سال‌های پیش دیگر وجود ندارد (Reini, 2019).

۲-۵. مراجع نظارتی مستقل

هریک از کشورهای عضو این مقرره موظف‌اند یک یا چند مرجع قانونی مستقل برای کنترل و نظارت بر اجرای مواد این مقرره معرفی کنند. این مراجع باید همواره از اجرای تمام مفاد مقررات عمومی حفاظت از داده‌ها اطمینان داشته باشند و مطابق با فصل هفتم سند مذکور با دیگر مراجع و نیز کمیسیون همکاری کنند.

کنترل‌کننده‌ها و پردازشگرها باید سوابق پردازش‌های خود را برای مطابقت با قوانین جی دی پی آر به تصویب مراجع نظارتی خاص برسانند (Voigt & von dem Bussche, 2017, pp.34-37).

اگر در هر جای جهان شرکتی دارید که کاربرانتان اروپایی‌اند، بهتر است هرچه زودتر مرجع نظارتی خود را بیابید. فضای مجازی آنقدرها هم که بسیاری فکر می‌کنند بدون مرز نیست و شرکت‌ها باید با توجه به این مقررهٔ جدید بسیار مراقب فعالیت‌های خود باشند (Denley et al, 2019, pp.9-10).

۲-۶. جرایم و مسئولیت‌ها

به‌دنبال تصویب و اجرای مقررات عمومی حفاظت از دادهٔ اروپایی در ۲۵ می۲۰۱۸، اکنون سازمان‌ها باید فعالیت‌های خود را با مقررات سختگیرانهٔ این مقرره که در جهت مدیریت و حفاظت از داده‌های شخصی افراد الزامات بسیار گسترده‌تری برای شرکت‌ها قرار داده است منطبق سازند. واقعیت این است که بسیاری از سازمان‌ها و شرکت‌ها هنوز

به‌درستی با این مقررات آشنا نیستند و طبق پیش‌فرض‌های قبلی خود به فعالیت‌هایشان ادامه می‌دهند. طبق این مقرره، اگر شرکت‌ها و سازمان‌های مشمولْ قوانین جی دی پی آر را به‌درستی رعایت نکنند و مشخص شود به هر نحوی از انحا قوانین را به‌درستی اجرا نکرده یا تخلفی داشته‌اند و یا از هریک از اصول این مقرره سرپیچی کرده باشند، طبق مادهٔ ۸۳ این مقرره بسته‌به نوع تخلف باید بین ۲ تا ۵ درصد از درآمد سالیانه‌شان و تا سقف ۲۰ میلیون یورو جریمه بپردازند.

۳. حفاظت از داده‌های شخصی در نظام حقوقی ایران

تاکنون در نظام حقوقی ایران مقررات منسجم و جامعی درخصوص حمایت از حریم خصوصی و داده‌های شخصی تبیین نشده است و لایحه‌ای نیز که سال‌های اخیر تحت عنوان لایحهٔ حمایت از حریم خصوصی و داده‌های شخصی تدوین شده است، هنوز به تصویب مجلس شورای اسلامی نرسیده است. ازاین‌رو، قوانین ناظر بر حمایت از حریم خصوصی افراد را باید در قوانین مختلف ازجمله قانون اساسی، قانون مجازات اسلامی،[۱] قانون انتشار و دسترسی آزاد به اطلاعات[۲] و قانون تجارت الکترونیک[۳] مصوب ۱۳۸۲ جست‌وجو کرد.

قانون اساسی هر کشوری جایگاه و اهمیت ویژه‌ای در میان قوانین آن کشور دارد، زیرا چارچوب حقوقی آن را تشکیل می‌دهد و در قانون اساسی جمهوری اسلامی ایران نیز، اگرچه صراحتاً به عبارت «حریم خصوصی» اشاره نشده است، در تحلیل چند اصل مهم آن به‌وضوح می‌توان مصادیق حمایت از حریم خصوصی را مشاهده کرد (گلی‌زاده، ۱۳۹۶). برای مثال، در اصل ۲۲ قانون اساسی می‌خوانیم: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز می‌کند.»؛ یا در اصل ۲۵ می‌خوانیم: «بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق‌سمع و

۱. متن قانون قابل دسترسی در تارنمای مرکز پژوهش های مجلس شورای اسلامی به آدرس https://rc.majlis.ir/fa/law/show/90621

۲. متن قانون قابل دسترسی در تارنمای مرکز پژوهش های مجلس شورای اسلامی به آدرس https://rc.majlis.ir/fa/law/show/780303

۳. متن قانون قابل دسترسی در تارنمای مرکز پژوهش های مجلس شورای اسلامی به آدرس https://rc.majlis.ir/fa/law/show/93997

هرگونه تجسس ممنوع است، مگر به حکم قانون» که صراحتاً عمده مصادیق داده‌های شخصی افراد را مصون می‌دارد. در ادامه به بررسی قوانین مربوط به حفاظت از داده‌های شخصی در قانون مجازات اسلامی، قانون انتشار و دسترسی آزاد به اطلاعات و قانون تجارت الکترونیک می‌پردازیم.

۳-۱. حفاظت از داده‌های شخصی در قانون مجازات اسلامی

در فصل سی‌ام قانون مجازات اسلامی تحت عنوان قانون جرایم رایانه‌ای، به امر حریم خصوصی و حفاظت از داده‌های شخصی پرداخته شده است. این قانون در راستای تعیین مصادیق استفادهٔ مجرمانه از سامانه‌های رایانه‌ای و مخابراتی در سال ۱۳۸۸ به تصویب مجلس شورای اسلامی رسید. فصل نخست این قانون به جرایم علیه محرمانگی داده‌ها و سامانه‌های اختصاصی و مخابراتی اختصاص یافته است. مادهٔ ۱ از مبحث یکم این قانون (مادهٔ ۷۲۹ قانون مجازات اسلامی) تحت عنوان «دسترسی غیرمجاز» بیان می‌کند: «هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت شده است، دسترسی یابد به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.» حال باید دید حدود و ابعاد دسترسی غیرمجاز چیست. در تعریف و بیان دسترسی غیرمجاز موضوع این ماده، از سوی حقوق‌دانان مطالب متفاوتی بیان شده است. برخی حقوق‌دانان آن را به معنای رخنهٔ غیرقانونی به سامانه‌های رایانه‌ای حفاظت‌شده می‌دانند، عده‌ای دسترسی غیرمجاز را به معنای کسب بدون مجوز داده‌ها و برنامه‌ها و اطلاعات، و گروهی نیز آن را به معنای دستیابی بدون مجوز به محتوای ذخیره‌شده یا درحال پردازش در یک یا چند سامانهٔ رایانه‌ای، مخابراتی یا شبکه‌ای می‌انگارند .اما باید گفت تعاریف مزبور و سایر تعاریفی که صرفاً دسترسی را ناظر به رخنه یا دسترسی به سامانهٔ حفاظت‌شده بیان می‌کنند، تعریفی جامع که شامل مادهٔ ۷۲۹ قانون مجازات باشد محسوب شوند؛ زیرا این ماده، علاوه‌بر دسترسی غیرمجاز به سامانه، دسترسی غیرمجاز به دادهٔ حفاظت‌شده را نیز بیان کرده و ممکن است سامانه تحت حفاظت نباشد؛ بلکه صرفاً داده تحت حفاظت قرار گیرد. تعریفی هم که دسترسی را به معنای کسب بدون مجوز داده‌ها بیان کرده، از این جهات مخدوش است که نخست «کسب» اخص از «دسترسی» است و

ممکن است دسترسی بدون کسب داده باشد و دوم، دسترسی غیرمجاز نسبت‌به «سامانه» نیز قابلیت تحقق دارد که تعریف کسب داده شامل آن نمی‌شود. تعریف دسترسی غیرمجاز، به دسترسی به محتوای ذخیره‌شده یا درحال پردازش تعریفی اخص از مادهٔ ۷۲۹ است، زیرا در این ماده واژهٔ «داده» بیان شده و داده اعم از داده‌محتوا،[۱] داده‌ترافیک[۲] و داده‌پیام[۳] است (مژده، ۱۳۹۸).

در نهایت، با توجه به اطلاق مادهٔ یک قانون جرایم رایانه‌ای صرف دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت شده باشد مشمول مقررات مادهٔ مذکور خواهد بود و طریق دسترسی، اعم از مستقیم یا با واسطه، تأثیری در اصل موضوع ماده ندارد.

۳-۲. حفاظت از داده‌های شخصی در قانون دسترسی و انتشار آزاد اطلاعات

قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ در راستای شفافیت در امور نهادهای حکومتی و امکان نظارت شهروندان و رسانه‌ها تدوین شد. اگرچه هدف این قانون امکان حق دسترسی شهروندان و رسانه‌ها به اطلاعات بود، موادی را نیز به تعریف داده‌های شخصی و حفاظت از آن‌ها اختصاص داده است.

بند ب مادهٔ ۱ این قانون، اطلاعات شخصی را این‌گونه تعریف می‌کند: «اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شمارهٔ حساب بانکی و رمز عبور است.» مادهٔ ۳ تصریح می‌دارد: «هر شخصی حق دارد از انتشار یا پخش اطلاعاتی که به‌وسیلهٔ او تهیه شده ولی در جریان آماده‌سازی برای انتشار تغییر یافته است جلوگیری کند، مشروط به آن‌که اطلاعات مزبور به سفارش دیگری تهیه نشده باشد که در این صورت تابع قرارداد بین آن‌ها خواهد بود.» در مادهٔ ۶ می‌خوانیم، «درخواست دسترسی به اطلاعات شخصی تنها از اشخاص حقیقی که اطلاعات به آن‌ها مربوط می‌گردد یا

۱. داده‌محتوا همان داده‌پیام است، اما داده‌های عام‌تر از داده‌پیام را شامل می‌شود. داده‌هایی که متضمن تصویر، صوت یا نوشتهٔ ذخیره‌شده در رایانه‌اند.

۲. داده ترافیک، داده‌های مربوط به ورود کاربر در شبکه شامل زمان شروع، پایان، مدت و موقعیت‌های دسترسی را دربر دارد.

۳. داده‌پیام در تجارت الکترونیک هر نمادی از واقعه، مفهوم یا اطلاعات است که با وسایل الکترونیکی، نوری یا فناوری‌های جدید اطلاعات را تولید، ارسال، دریافت، ذخیره یا پردازش می‌کند.

نمایندهٔ قانونی آنان پذیرفته می‌شود.» درخصوص حمایت از حریم خصوصی در مادهٔ ۱۴ آمده است: «چنانچه اطلاعات درخواست‌شده مربوط به حریم خصوصی اشخاص باشد و یا در زمرهٔ اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود.» مادهٔ ۱۶ این قانون نیز از داده‌های مرتبط با سلامت یا تجارت حمایت می‌کند: «در صورتی که برای مؤسسات مشمول این قانون با مستندات قانونی محرز باشد که در اختیار قراردادن اطلاعات درخواست‌شده، جان یا سلامت افراد را به مخاطره می‌اندازد یا متضمن ورود خسارت مالی یا تجاری برای آن‌ها باشد، باید از در اختیار قراردادن اطلاعات امتناع کنند.»

تبصرهٔ مادهٔ ۲۱ این قانون نقض مفاد آن را صراحتاً دارای مسئولیت مدنی می‌پندارد: «در صورت انتشار اطلاعات واقعی برخلاف مفاد این قانون، اشخاص حقیقی و حقوقی حق دارند که مطابق قواعد عمومی مسئولیت‌های مدنی، جبران خسارت‌های واردشده را مطالبه نمایند.» بنابراین از نص قانون چنین برداشت می‌شود که در صورت نقض مفاد این قانون و نقض حریم خصوصی، قانونگذار پیش‌بینی‌هایی درخصوص جبران خسارت کرده است، هرچند این پیش‌بینی‌ها ابهاماتی نیز دارند (حسینی نیک، ۱۳۹۶).

۳-۳. حفاظت از داده‌های شخصی در قانون تجارت الکترونیک

قانون تجارت الکترونیک مصوب سال ۱۳۸۲ قواعد و مقرراتی درخصوص حمایت از حریم خصوصی اطلاعات شخصی در فضای مجازی و محیط اینترنتی تعریف کرده است و قانونگذار فصل سوم از باب سوم این قانون، مواد ۵۸ تا ۶۱ را به «حمایت از داده‌پیام‌های شخصی» اختصاص داده است.

در مادهٔ ۵۸ این قانون می‌خوانیم: «ذخیره، پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و«داده‌پیام»های راجع‌به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هرعنوان غیرقانونی است.»

مادهٔ ۵۹ این قانون به شرایط ذخیره، پردازش و توزیع داده‌پیام‌های شخصی می‌پردازد و با تأکید بر اصل رضایت شخص موضوع داده‌پیام و نیز به شرط آن‌که محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره و پردازش و توزیع داده‌پیام‌های

شخصی در بستر مبادلات الکترونیکی را با لحاظ شرایطی ازجمله هدف مشخص، ضرورت و تناسب با اهداف تعیین‌شده، صحیح و روزآمدبودن داده‌پیام، امکان دسترسی و اصلاح داده‌پیام توسط شخص و همچنین امکان محو کامل داده‌پیام‌های شخصی مجاز می‌داند.

مادهٔ ۶۰ قانون مزبور به اطلاعات شخصی پزشکی و بهداشتی می‌پردازد و بیان می‌کند که ذخیره یا پردازش یا توزیع داده‌پیام‌های مربوط به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ای است که در مادهٔ ۷۹ این قانون خواهد آمد.

مادهٔ ۶۱ همین قانون سایر موارد راجع‌به دسترسی موضوع داده‌پیام، از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان داده‌پیام‌های شخصی را بررسی می‌کند و رسیدگی به آن را به مواد مندرج در باب چهارم این قانون وآیین‌نامهٔ مربوطه می‌سپارد.

همان‌طور که در دستورالعمل‌های اروپایی و قوانین دیگر کشورها می‌بینیم، استثنائاتی از قبیل امنیت ملی پیش‌بینی شده است که بر اساس آن‌ها پردازش داده‌های شخصی بدون اجازهٔ صریح شخص موضوع داده نیز امکان‌پذیر است (کارگری، ۱۳۹۸).

جرم‌انگاری نقض مواد مذکور نیز در باب چهارم همین قانون، طی مواد ۷۱ تا ۷۳، حبس و جزای نقدی تعیین شده است. مادهٔ ۷۱ قانون بیان می‌کند هرکس در بستر مبادلات الکترونیکی شرایط مقرر در مواد ۵۸ و ۹۵ این قانون را نقض کند مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود. در مادهٔ ۷۲ این قانون نیز آمده است: هرگاه جرایم راجع‌به داده‌پیام‌های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در مادهٔ ۷۱ این قانون محکوم خواهد شد. مادهٔ ۷۳ دفاتر خدمات صدور گواهی را مخاطب قرار داده و می‌گوید: «اگر به‌واسطهٔ بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع‌به داده‌پیام‌های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون ریال محکوم می‌شود.»

۴. ضرورت اصلاح قوانین حفاظت از داده‌های شخصی در نظام حقوقی ایران

مقایسهٔ بین قوانین حفاظت از داده‌های شخصی در ایران و بالاخص قانون تجارت الکترونیکی مصوب ۱۳۸۲ که در حال حاضر کامل‌ترین قانونی است که در این خصوص در دسترس داریم با مقررات اتحادیهٔ اروپا نشان می‌دهد که حقوق ایران دارای نقایصی در تعریف داده‌های شخصی، فقدان مقررات صریح و همچنین نبود دستورالعمل‌های مشخص است.

اگرچه قوانین و مقررات متعددی در کشور ما به موضوع حریم خصوصی و داده‌های شخصی افراد پرداخته‌اند و با جست‌وجو در قوانین متعدد می‌توان تا حدودی از حمایت قانون از حریم خصوصی افراد اطمینان یافت، اما خلئی که بیش از هرچیز به‌چشم می خورد، تبیین حدوحدود حریم خصوصی و مصادیق دسترسی غیرمجاز به داده‌های شخصی است که می‌بایست مورد توجه قانون‌گذار و مراجع ذی‌صلاح قرار گیرد.

در مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی، اصولی دربارهٔ ماهیت داده ازجمله اصل تحصیل قانونی (مادهٔ ۵۸)، اصل تحصیل مضیق و مرتبط (بندهای الف و ب مادهٔ ۵۹)، اصل درستی یا صحت داده‌های گردآوری‌شده (بند ج مادهٔ ۵۹)، اصلی دسترسی (بند د مادهٔ ۵۹) و اصل امحا (بند هـ مادهٔ ۵۹) درنظر گرفته شده است؛ اما برخی اصول دیگر که در مقررهٔ جی دی پی آر آمده است مانند اصل انتخاب، اصل امنیت، اصل شفاف‌سازی، اصل ممنوعیت افشا، اصل پردازش مرتبط و اصل عدم انتقال مورد توجه قانوگذار قرار نگرفته است (زرکلام، ۱۳۸۶).

اصل دسترسی به داده‌های گردآوری و پردازش‌شده نیز همانند اصل رضایت دارای مستثنیاتی است که قانونگذار در قانون ایران در مورد آن‌ها سکوت اختیار کرده است (اصلانی، ۱۳۸۴، ص۳۴۳).

در فصل ۴ جی دی پی آر، به‌تفصیل و صراحت به وظایف و مسئولیت‌های افراد و سازمان‌هایی که به جمع‌آوری داده‌ها می‌پردازند پرداخته شده است، اما متأسفانه قانون ایران فاقد دستورالعمل مشخصی دربارهٔ نحوهٔ برخورد با این افراد و سازمان‌ها است و نظارت دقیقی بر نحوهٔ فعالیت، وظایف، مسئولیت‌ها و اختیارات آن‌ها وجود ندارد و مادهٔ ۶۱ قانون تجارت الکترونیک نیز پیگیری در این زمینه را به آیین‌نامه ارجاع می‌دهد.

اشکالی دیگری که بر قانون ایران وارد است از حیث مصادیق داده‌های موردحمایت است که در متن قانون به‌صراحت به آن‌ها اشاره نشده است.

نتیجه‌گیری و پیشنهاد

همزمان با پیشرفت فناوری و انبوه اطلاعاتی که هرروزه در شبکه‌های اجتماعی و از طریق اینترنت جابه‌جا می‌شود، منطقی است که همهٔ نظام‌های حقوقی در صدد نظام‌مندکردن قوانین حاکم بر حفاظت و صیانت از داده‌های شخصی افراد باشند. در این میان، اتحادیهٔ اروپا پیشتاز بوده است و در سال ۲۰۱۸ مقررات عمومی حفاظت از داده‌های اروپایی معروف به جی دی پی آر را تصویب کرد که ضامن حفاظت از داده‌های شخصی شهروندان اروپایی داخل اتحادیهٔ اروپا و حتی خارج از آن بوده و همهٔ شرکت‌های اتحادیهٔ اروپا و حتی خارج از آن را که به‌نحوی با داده‌های شخصی شهروندان اروپایی سروکار دارند به رعایت مقررات سند مذکور ملزم می‌کند. ایران نیز در چند سال اخیر سعی کرده است همگام با بسیاری از کشورها قوانینی در جهت حفاظت از داده‌های شخصی تنظیم کند که کامل‌ترین آن‌ها در قانون تجارت الکترونیک مصوب ۱۳۸۲ مشاهده می‌شود. البته همان‌طور که پیش‌تر نیز به آن اشاره شد، فقدان مقررات صریح و دستورالعمل‌های مشخص از نواقص و کاستی‌هایی است که انتظار می رود با تصویب لایحهٔ حریم خصوصی بتوان بر بخشی از آن‌ها فائق آمد. از سویی، ازآنجاکه پیش‌نویس این لایحه نیز در سال ۱۳۸۴ تهیه شده است، به‌نظر می رسد حتی پس از تصویب آن نیز با مشکلاتی در تفسیر و اجرا روبه‌رو باشیم.

نهایتاً، با عنایت به مباحث مطرح‌شده، درخصوص تنظیم قوانینی برای حفاظت و صیانت از داده‌های شخصی افراد در نظام حقوقی کشورمان پیشنهاد می‌شود:

۱. تعریف مشخصی از حدود حریم خصوصی و مرز آن با حریم غیرخصوصی و داده‌های شخصی و مصادیق نقض آن‌ها در قانون جدید ارائه شود.

۲. وظایف و مسئولیت‌های افراد و سازمان‌هایی که به جمع‌آوری داده‌ها می‌پردازند به‌طور صریح در قانون جدید مشخص شود.

۳. ضمانت اجراهای متناسب با نقض صیانت از داده‌های شخصی افراد از سوی هریک از عوامل خاطی در قانون جدید درنظر گرفته شود.

۴. تعریف استانداردهای امنیتی و تبیین نهادهای نظارتی در دستور کار دولت قرار گیرد.

منابع

اصلانی، حمیدرضا (۱۳۸۴). *حقوق فناوری اطلاعات- حریم خصوصی در جامعه اطلاعاتی*. تهران: نشر میزان، چاپ اول.

السان، مصطفی (۱۳۹۷). *حقوق تجارت الکترونیک*. تهران: انتشارات سازمان سمت، چاپ پنجم.

حسینی نیک، سیدعباس (۱۳۹۶). *نقدی بر قانون انتشار و دسترسی آزاد به اطلاعات*. خبرگزاری مهر. آخرین تاریخ به‌روزرسانی ۱۳۹۹/۱۰/۱۷. www.mehrnews.com/news/4187143

زرکلام، ستار (۱۳۹۱). *حقوق تجارت الکترونیک همراه با تحلیل قانون تجارت الکترونیکی ایران*. مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، چاپ سوم.

زرکلام، ستار (۱۳۸۶). «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیهٔ اروپا)». *پژوهشنامهٔ حقوق اسلامی*، دورهٔ ۸، شمارهٔ ۲۵، ص ۱۷۳-۱۹۶.

قناد، فاطمه و علیقلی، امیره (۱۳۹۸). «حمایت از حریم خصوصی در فضای وب در پرتو قانون اروپایی حمایت از داده‌های شخصی و نظام حقوقی ایران». *پنجمین کنفرانس ملی وب‌پژوهی، دانشگاه علم و فرهنگ*.

قناد، فاطمه (۱۳۹۰). «حمایت از داده‌پیام‌های شخصی در بستر تجارت الکترونیکی». مجلهٔ *تحقیقات حقوقی*، ضمیمهٔ شمارهٔ ۵۶، ص ۸۰۹ تا ۸۴۰.

کارگری، ابراهیم (۱۳۹۸). «بررسی تطبیقی آثار نقض حق حریم خصوصی در فضای سایبری در حقوق ایران و حقوق خارجی». *دومین کنفرانس ملی پدافند سایبری*.

گلی‌زاده، امین (۱۳۹۶). «قلمرو حریم خصوصی در قانون اساسی جمهوری اسلامی ایران». *دومین کنفرانس ملی حقوق، الهیات و علوم سیاسی، شیراز*.

مژده، احمد (۱۳۹۸). «جرایم علیه محرمانگی داده‌ها و سامانه‌ها رایانه‌ای و مخابراتی». وب‌سایت مؤسسهٔ حقوقی فرصت، https://forsatlawfirm.com

Bitar, H., & Jakobsson, B. (2017). *Securing Personal Data in Compliance with GDPR*. Master Thesis, Leula University.

Caldaer, A. (2016). *EU GDPR A Pocket Guide*. ITGP, 2nd Edition.

Denley A., Foulsham, M., & Hitchen, B. (2019). *GDPR: How To Achieve and Maintain Compliance*.

Gocheva, V. (2017). *Challenges for the business when complying with the GDPR*. Master`s Thesis, Tilburg University.

Kovacs, Z. (2019). *The impact of the GDPR on data privacy experience: How do EU consumers see their privacy in the era of the GDPR*?, Master Thesis, Alato University.

Lehtiniemi, T., & Kortesniemi, Y. (2017). *Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach.* Sage journals

Mitchell, A. (2016). GDPR: Evolutionary or revolutionary?. *Journal of Direct, Data and Digital Marketing Practice*, 17(4), 217-221..

Reini, P. (2019). *GDPR Implementation*. Master`s thesis, JAMK University of Applied Science.

Tamo-Larrieux, A. (2018). *Designing for Privacy and Its legal Framework: Data Protection by Design and Default for the Internet Things*. Springer.

ur Rehman, I. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*, 1-11.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection: A Practical Guide*. Springer, 1st Edition.

van Goethem, Alexander (2018). *The Effects Of Brexit On GDPR Implementation, An investigation into data protection legislation within the United Kingdom.* Master's Thesis, Leiden University.

van Lieshout, M. (2015). "The Value of Personal Data". In: Jan Camenisch, Simone Fischer-Hubner, Marit Hansen (eds). *Privacy and Identity Management for the Future Internet in the Age of Globalization*; London: Springer.

Wachter, S., & Mittelstadt, B. (2019). *A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI*. Columbia University Academic Commons.

Comprehensive Study of Personal Data Protection in Iran's Legal System and European General Data Protection Regulations

Fatemeh Ghanad,[۱] Elham Sharif[۲]

Abstract

Protecting the privacy of individuals has always been considered a global principle by international institutions and has been stipulated in many international documents. Nowadays, lawmakers have considered personal data more than ever due to the fast pace of the technology and consequently the availability of personal data in cyberspace, their ease of transfer, and the convenience of their processing.

The EU has been a frontrunner and, as a comprehensive alternative to the EU Data Protection Act, set out the International Document of General Data Protection Regulations (GDPR) in April 2016, which was approved and implemented by the European Parliament on May 25, 2018. This article aims to demonstrate the scope of personal data and its protection in the General Data Protection Regulations as an international document and Iran's legal system. It further recommends some improvements in cyberspace infrastructures and regulations and the necessity of better designating regulatory bodies to protect individual privacy better.

Keywords: Personal Data, Individual Privacy, Data protection, GDPR

1. Associate Professor, University of Science and Culture, Tehran, Iran; elhamsharif@hotmail.com
2. Master of Electronic Commerce Law, University of Science and Culture, Tehran, Iran; ghanad@USC.ac.ir