دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۱ (۸۹–۱۰۱)
https://monadi.isc.org.ir

حفظ حریم خصوصی در عصر توسعه‌ی فناوری اطلاعات، درس‌هایی از قانون عمومی حفاظت از داده‌ی اروپا

بابک سیابی[۱] و پروین رستگاری*[۲،]

[۱]شرکت مهندسی ارتباطی پیام‌پرداز، اصفهان، ایران
[۲]گروه مهندسی برق و کامپیوتر، دانشکده فنی مهندسی گلپایگان، دانشگاه صنعتی اصفهان، گلپایگان، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۲ خرداد ۱۴۰۳
تاریخ پذیرش: ۲۱ شهریور ۱۴۰۳
انتشار آنلاین: ۷ آبان ۱۴۰۳

کلمات کلیدی:
حریم خصوصی
حفاظت از داده‌های شخصی
GDPR

نوع مقاله: فنی و ترویجی

چکیده

با توجه به افزایش روزافزون جمع‌آوری و پردازش داده‌ها در دنیای دیجیتال امروز، حفظ حریم خصوصی فردی و سازمانی، به یک ضرورت انکارناپذیر تبدیل شده است. در این راستا، همگام با تلاش‌های مراکز علمی و پژوهشی برای برخورد تخصصی با مسئله‌ی حریم خصوصی، قوانین متعددی نیز در کشورهای مختلف وضع شده‌اند. از این میان، به عقیده‌ی بسیاری از پژوهشگران، قانون حفاظت از داده‌ها در سطح اروپا (GDPR) بزرگ‌ترین تغییر در زمینه‌ی قوانین حفظ حریم خصوصی افراد در دهه‌های اخیر و الگویی مطلوب در جهت سامان دادن به داده‌های شخصی افراد است. بر این اساس، در این مقاله برای آشنایی با ابعاد مسئله‌ی حریم خصوصی، پس از مروری بر تاریخچه‌ی حفظ حریم خصوصی، بر روی قانون GDPR متمرکز شده و برخی از مهمترین نکات و ملاحظات در مورد ماهیت و ساختار این قانون و ضرورت و چالش‌های انطباق با آن ارائه می‌شود. همچنین، تدابیر متعدد در نظر گرفته شده در این قانون برای عملیاتی و اجرایی شدن سازوکار حفاظت از حریم خصوصی بیان می‌شود. در خاتمه، با نگاشت مطالب بیان شده به وضعیت کنونی حریم خصوصی در کشور، به برخی نکات کلیدی جهت پیاده‌سازی عملی قوانین حفظ حریم خصوصی در کشور اشاره می‌شود.

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

رشد روزافزون و سریع فناوری اطلاعات، علی‌رغم مزایای زیادی که برای بشر به ارمغان آورده، سبب بروز مشکلات و چالش‌های بسیاری در زمینه‌ی حقوق بشر، به ویژه از منظر حفظ حریم خصوصی [۱]، شده است. این چالش‌ها شامل گسترش روزافزون جمع‌آوری و پردازش داده‌ها، ظهور فناوری‌های نوین نظارتی، پیچیدگی چارچوب‌های مقرراتی و ناکارآمدی فناوری‌های تقویت حفظ حریم خصوصی است. از همین روی، دستکم در دهه‌ی اخیر، حریم خصوصی در سطح گسترده‌ای به یکی از موضوعات داغ محافل علمی به ویژه از منظر بحث‌های حقوقی و اجتماعی و پایاپای آن از منظر فناوری و امنیت اطلاعات تبدیل شده است. در عصر توسعه‌ی فناوری اطلاعات، اصطلاح حریم خصوصی در اکثر کاربردها برای اشاره به «حریم خصوصی داده‌ها [۲]» به کار برده می‌شود و به صورت حق اشخاص برای کنترل داده‌های شخصی که توسط سیستم‌های اطلاعاتی مختلف جمع‌آوری و استفاده می‌شوند، تعریف می‌گردد.

اگرچه تاریخچه‌ی بحث پیرامون مسائل مربوط به حریم خصوصی را می‌توان به قدمت بشریت دانست [۱]، با این وجود، قرن بیستم شاهد توسعه‌ی شایان توجهی در سیاست‌های مربوط به این حوزه بود. رویدادهای بزرگی مانند اعلامیه‌ی جهانی حقوق بشر در سال ۱۹۴۸ و

*نویسنده مسئول
آدرس‌های رایانامه: siabi@payampardaz.com (بابک سیابی)، p.rastegari@iut.ac.ir (پروین رستگاری)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

[1]Privacy

[2]Data Privacy

معرفی قوانین حفاظت از داده‌ها در دهه‌ی ۱۹۷۰ را می‌توان نقاط عطفی در تشخیص و حفظ حقوق حریم خصوصی دانست. اولین گزارش رسمی در مورد حقوق کاربران در سال ۱۹۷۳ توسط ویلیس هووارد ویر [1] در ایالت متحده‌ی امریکا منتشر شد [۲]. پس از آن، قوانین حریم خصوصی آلمان غربی تحت عنوان BDGG [2]، که در سال ۱۹۷۰ تصویب شده بود، از ژانویه‌ی ۱۹۷۸ لازم‌الاجرا شد [۳]. در سال ۱۹۸۰، سازمان توسعه و همکاری اقتصادی (OECD)، سیستم جامع محافظت از داده در اروپا را بر پایه‌ی هفت اصل اطلاعیه، هدف، رضایت، امنیت، افشا، دسترسی و پاسخگویی ارائه نمود [۴]. در سال ۱۹۸۹، با سقوط آلمان شرقی و افشای داده‌های پلیس از شهروندان، اهمیت وضع قوانین حفاظت از داده‌ها در بین کشورهای عضو اتحادیه‌ی اروپا بیش از پیش آشکار شد، که انگیزه‌ای برای پیشنهاد دستورالعمل حفاظت از داده‌ها ایجاد نمود. در ۲۴ اکتبر ۱۹۹۵، دستورالعمل حفاظت از داده‌ها (DPD) [3] تحت عنوان رسمی Directive 95/46/EC، در پارلمان اروپا تصویب شد [۵]. هرچند این مصوبه در سطح دستورالعمل بود و الزام اجرایی سرتاسری نداشت، اما از یک سو موضوعات پایه‌ای حریم خصوصی و انتقال اطلاعات شخصی در آن در نظر گرفته شده بود و از سوی دیگر با مشخص نمودن اهداف و اصول رعایت حریم خصوصی و محافظت از داده، پایه‌ی قوانین منطقه‌ای و ایالتی مرتبط با حریم خصوصی در کشورهای اروپایی بود. کشورهای عضو اتحادیه‌ی اروپا ملزم بودند تا انتهای سال ۱۹۹۸ قوانین منطقه‌ای خود در حوزه‌ی حریم خصوصی و حفاظت از داده‌ها را بر اساس اصول و اهداف دستورالعمل تدوین نمایند.

به عقیده‌ی بسیاری از پژوهشگران، GDPR بزرگ‌ترین تغییر در زمینه‌ی قوانین حفظ حریم خصوصی در بیست سال اخیر به شمار می‌آید [۷، ۹]. تا کنون پژوهش‌های بسیاری در زمینه‌ی تأثیر GDPR در توسعه‌ی فناوری [۱۰]، تجارت و بازرگانی [۱۱]، سیستم‌های آموزشی [۱۲]، فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی [۱۳، ۱۶] و ... انجام شده است. با توجه به مطالب بیان شده در مورد اهمیت GDPR، در مقاله‌ی حاضر تلاش شده است ماهیت و ساختار این قانون و نیز ضرورت و چالش‌های انطباق با آن بررسی شود و با برشمردن ابعاد و ویژگی‌های آن، نکات عملیاتی و اجرایی برای کمک به بهبود وضعیت حریم خصوصی در کشور بیان گردد.

ادامه‌ی مقاله به این شکل سازمان‌دهی شده است: در بخش ۲، مسائل اساسی مرتبط با حریم خصوصی از دیدگاه کلان و کشوری مطرح شده و به طور خاص، جایگاه GDPR از این منظر، مورد بررسی قرار گرفته است. در بخش ۳، به معرفی کلی GDPR و دلایل ضرورت انطباق با آن پرداخته می‌شود. در بخش ۴، در مورد کلیت ساختار و محتوای GDPR توضیح داده می‌شود. بخش ۵ به تشریح اقدامات لازم برای انطباق با GDPR تخصیص داده شده است. در بخش ۶، در مورد تقویت و گسترش قوانین مربوط به حریم خصوصی در سال‌های اخیر مطالبی ارائه می‌شود. در بخش ۷، ویژگی‌های عملیاتی و اجرایی GDPR مورد بررسی قرار می‌گیرد. در بخش ۸، با توجه به اهمیت حفظ حریم خصوصی در عصر حاضر، که منجر به تدوین قوانینی مانند GDPR شده است، به بررسی این مسئله در کشور پرداخته می‌شود. در نهایت، در بخش ۹ یک جمع‌بندی از مطالب بیان شده ارائه می‌گردد.

۲ مسائل اساسی مرتبط با حریم خصوصی

بدیهی است که پیش از هر چیز، حریم خصوصی مسئله‌ای است که افراد با آن درگیر هستند و از توجه به آن منتفع یا از عدم توجه به آن متضرر می‌شوند. اما موضوع مهمی که چندان بدیهی به نظر نمی‌رسد، تأثیر مسئله‌ی حریم خصوصی بر مسائل و چالش‌های کلان جامعه است. برای روشن شدن این موضوع و برای تأکید بر اهمیت و حیاتی بودن توجه به حفظ حریم خصوصی و عواقب غفلت از آن، در این بخش، به برخی از مهمترین جنبه‌های تأثیرات کلان مسئله‌ی حریم خصوصی پرداخته می‌شود. در ادامه، برای تأیید اهمیت شایان توجه این موضوع، به طور خاص به بررسی جایگاه قانون عمومی حفاظت از داده‌ی اروپا پرداخته می‌شود.

۱.۲ مسائل اساسی مرتبط با حریم خصوصی افراد از دیدگاه کلان و کشوری

برخی از مهمترین جنبه‌های کلان مسئله‌ی حریم خصوصی که می‌توانند تأثیرات مهمی بر جامعه داشته باشند، شامل موارد زیر است:

- توجه به موضوع حفاظت از حریم خصوصی افراد علاوه بر این که به طور ذاتی به جهت قرار داشتن در فهرست حقوق اولیه‌ی شهروندان جامعه حائز اهمیت است، از بابت آسیب‌های روانی، خانوادگی، شغلی و ... که ممکن است از این جانب به اشخاص وارد شود، نیز اهمیت فراوانی دارد. این موضوع به طور خاص در ارتباط با کودکان حائز اهمیت به‌سزایی است. پیاده‌سازی سازوکار کارآمد برای حفاظت از حریم خصوصی افراد می‌تواند از ابعاد مختلف و به طور چشمگیر به سلامت جامعه کمک کند.
- سامان‌دهی مناسب موضوع حریم خصوصی می‌تواند به طور ریشه‌ای از بروز بخشی از پرونده‌های قضایی و هزینه‌ها و مشکلات ناشی از آن‌ها برای کشورها جلوگیری نماید.
- در سال‌های اخیر، نفوذ به سیستم‌های اطلاعاتی و سرقت داده‌های کاربران شیوع بسیاری داشته است. هر دو بخش دولتی و خصوصی مورد حملات متعددی قرار گرفته‌اند. در برخی از نفوذها شاهد وضع فاجعه‌باری بوده‌ایم که طی آن‌ها عناوین متعدد داده‌های شخصی میلیون‌ها کاربر به صورت یک‌جا به سرقت رفته است. سازوکار دقیق محافظت از حریم خصوصی می‌تواند هم با الزام رعایت نکات امنیتی متعدد، احتمال نفوذ به سامانه‌ها را کاهش دهد و هم با الزام عدم جمع‌آوری داده‌های شخصی زاید و اضافی به کاهش عناوین داده‌های شخصی افشا شده در نفوذهای موفق منجر شود.
- علاوه بر نفوذهای بیرونی به سامانه‌ها، دسترسی‌های کنترل نشده و غیرمجاز داخلی به داده‌های شخصی کاربران می‌تواند منجر به بروز

[1] Willis Howard Ware [2] Bundesdatenschutzgesetz [3] Data Protection Directive

مصادیق فساد و سوءاستفاده در سازمان‌ها شود. وجود سیاست‌های کنترل دسترسی شفاف به همراه پیاده‌سازی سازوکارهای اعمال آن که از الزامات حفاظت از حریم خصوصی است، می‌تواند به نحو مؤثری از دسترسی‌های غیرمجاز و در نتیجه از فسادهای خرد و کلان مرتبط با آن‌ها جلوگیری نماید.

۲.۲ جایگاه قانون عمومی حفاظت از داده‌ی اروپا

همان‌طور که قبلاً اشاره شد، بسیاری از پژوهشگران، GDPR را به عنوان بزرگ‌ترین تغییر در زمینه‌ی قوانین حفظ حریم خصوصی در بیست سال اخیر به شمار می‌آورند. وضع قانون GDPR با نگاهی جامع و همه‌جانبه به موضوع حریم خصوصی صورت گرفته است. آمارهای ارائه شده در مورد تأثیرات GDPR در اتحادیه‌ی اروپا و نیز در سطح بین‌المللی مؤید اهمیت این قانون است و نشان می‌دهد که این قانون به میزان زیادی توانسته است اهداف مورد نظر در زمینه‌ی حریم خصوصی را برآورده نماید. بر اساس یک نظرسنجی، ٪۶۷ از اروپایی‌ها از GDPR آگاهی دارند و ٪۵۷ از آن‌ها از مرجع ملی حفاظت از داده‌های خود مطلع هستند. این آگاهی نشان می‌دهد که GDPR تأثیر قابل توجهی بر درک عمومی از حقوق حریم خصوصی داده‌ها داشته است [۱۷]. بسیاری از سازمان‌ها، پس از تصویب GDPR، اقدامات حفاظت از داده‌های خود را بهبود بخشیده‌اند. مطالعه‌ای از Cisco نشان می‌دهد که ٪۵۹ از سازمان‌ها گزارش داده‌اند که تمامی یا بیشتر الزامات GDPR را رعایت می‌کنند. همچنین براساس این مطالعه، سازمان‌هایی که در زمینه‌ی حریم خصوصی داده‌ها سرمایه‌گذاری کرده‌اند، از مزایایی مانند کاهش نقض داده‌ها، تأخیرهای کوتاه‌تر در فروش و پویایی بیشتر برخوردار شده‌اند [۱۸]. لازم به ذکر است که GDPR قوانین حفاظت از داده‌ها را در سطح جهانی نیز تحت تأثیر قرار داده است. کشورهایی مانند برزیل، ژاپن و کره جنوبی قوانین حریم خصوصی خود را برای همخوانی با اصول GDPR وضع یا به‌روزرسانی کرده‌اند، که نشان‌دهنده‌ی نقش مؤثر آن در تعیین استاندارد جهانی برای حفاظت از داده‌هاست.

لازم به ذکر است که یکی از مهم‌ترین دلایل جایگاه ویژه‌ی GDPR، ویژگی‌های عملیاتی و اجرایی آن است که به تفصیل در بخش ۷ مورد بررسی قرار می‌گیرد. بالطبع، جایگاه ویژه‌ی GDPR، نگاه جامع و همه‌جانبه‌ی آن به موضوع حریم خصوصی و ویژگی‌های عملیاتی و اجرایی آن، این قانون را به الگوی مناسبی برای وضع قوانین مربوط به حریم خصوصی در جهان تبدیل کرده است. لذا، در ادامه، به بررسی این قانون پرداخته و سعی می‌شود برای مسئله‌ی حفظ حریم خصوصی در کشور، به نحو مناسبی از این قانون الگوبرداری شود.

۳ معرفی GDPR و ضرورت انطباق

همان‌طور که در بخش مقدمه اشاره شد، GDPR مجموعه‌ای از قوانین صریح و سخت‌گیرانه در حوزه‌ی حفاظت از داده‌های شهروندان اروپایی است که توسط نهادهای قانون‌گذاری اتحادیه‌ی اروپا وضع شده و در دسترس عموم قرار گرفته است. همه‌ی نهادهای دولتی و خصوصی (اعم از سازمان‌ها و کسب‌وکارها)، در داخل یا خارج اروپا، که به نحوی با اتحادیه‌ی اروپا مراوده‌ی کاری یا اقتصادی دارند و داده‌های شهروندان این منطقه را جمع‌آوری و پردازش می‌کنند، ملزم به رعایت GDPR هستند. درحقیقت، GDPR مجموعه‌ی قوانین اتحادیه‌ی اروپا برای حفاظت از حقوق اشخاص حقیقی در ارتباط با داده‌های شخصی آن‌ها است. بر اساس این مجموعه‌ی قوانین، باید هرگونه جمع‌آوری، پردازش، انتقال و یا پاک‌سازی داده‌های شخصی مربوط به شهروندان اروپایی قانونی باشد و رعایت حقوق مالک داده در این خصوص اجباری است.

به منظور این که قوانین گرد آمده در GDPR الزام‌آور باشند، جریمه‌های سنگینی برای عدم رعایت آن‌ها در نظر گرفته شده که ممکن است کسب‌وکارهای کوچک یا متوسط را حتی به ورطه‌ی ورشکستگی بکشانند. این جریمه‌ها، شامل موارد زیر است:

- جریمه‌ی مالی تا ۲ درصد درآمد جهانی برای تخلفات فنی و تا ۴ درصد گردش مالی سالانه
- جهانی یا ۲۰ میلیون یورو (هرکدام که بیشتر است) برای نقض اصول قانون،
- انتشار اجباری اطلاعیه‌ی نقض امنیت (حداکثر تا ۷۲ ساعت)،
- پیگیری دادخواست‌های حقوقی افرادی که متضرر شده اند،
- و در موارد حاد، ممنوعیت کامل پردازش داده‌های شخصی.

بر اساس آمار ارائه شده در [۱۹]، در بازه‌ی زمانی جولای ۲۰۱۸ تا انتهای سال ۲۰۲۳، ۱۹۷۳ مورد جریمه‌ی ناشی از نقض GDPR معادل ۴۴۳۱۴۸۲۴۸۴ یورو ثبت شده است. ده مورد اول از شرکت‌هایی که مشمول بیشترین جریمه‌ها شده‌اند، در جدول ۱ آورده شده است. همچنین بر اساس جدول ۲، بیشترین مبلغ جریمه به دلیل عدم انطباق با اصول عمومی پردازش داده بوده است.

با توجه به مطالب بیان شده، هر کسب و کاری که قصد دارد فعالیت تجاری در اروپا داشته باشد، لازم است بررسی نماید که آیا مشمول قوانین GDPR است یا خیر و در صورتی‌که مشمول این قوانین است، لازم است به طور جدی در راستای انطباق با آن‌ها قدم بردارد.

۴ ساختار و محتوای GDPR

در این بخش، نگاهی کلی بر ساختار و محتوای GDPR خواهیم داشت. برای این منظور، ابتدا به توضیح برخی تعاریف اساسی در این قانون پرداخته می‌شود. سپس توضیحاتی در خصوص ماهیت قانون و ساختار آن ارائه خواهد شد.

جدول ۱. ده مورد اول بیشترین جریمه‌ی ناشی از نقض GDPR [۱۹]

	Controller	Country	Fine-€	Type of Violation	Date
1	**Meta** Platforms Ireland Limited	IRELAND	**1.2 B**	Insufficient legal basis for data processing	**2023**-05-12
2	**Amazon** Europe Core S.a.r.l.	LUXENBOURG	**746 M**	Non-compliance with general data processing principles	**2021**-07-16
3	**Meta** Platforms Ireland Limited	IRELAND	**405 M**	Non-compliance with general data processing principles	**2022**-09-05
4	**Meta** Platforms Ireland Limited	IRELAND	**390 M**	Non-compliance with general data processing principles	**2023**-01-04
5	**TikTok** Limited	IRELAND	**345 M**	Non-compliance with general data processing principles	**2023**-09-01
6	**Meta** Platforms Ireland Limited	IRELAND	**265 M**	Insufficient technical and organizational measures	**2022**-11-25
7	**WhatsApp** Ireland Ltd.	IRELAND	**225 M**	Insufficient fulfilment of information obligations	**2021**-09-02
8	**Google** LLC	FRANCE	**90 M**	Insufficient legal basis for data processing	**2021**-12-31
9	**Facebook** Ireland Ltd.	FRANCE	**60 M**	Insufficient legal basis for data processing	**2021**-12-31
10	**Google** Ireland Ltd.	FRANCE	**60 M**	Insufficient legal basis for data processing	**2021**-12-31

جدول ۲. ده مصداق نقض GDPR با بیشترین تکرار و بالاترین جمع جریمه [۱۹]

Type of Violation	Sum of Fines	
Non-compliance with general data processing principles	**2,036,371,279**	(at **521** fines)
Insufficient legal basis for data processing	**1,648,890,212**	(at **601** fines)
Insufficient technical and organizational measures to ensure information security	**383,375,975**	(at **347** fines)
Insufficient fulfilment of information obligations	**237,303,920**	(at **183** fines)
Insufficient fulfilment of data subjects rights	**98,169,170**	(at **187** fines)
Unknown	**9,250,000**	(at **9** fines)
Insufficient cooperation with supervisory authority	**6,147,929**	(at **91** fines)
Insufficient fulfilment of data breach notification obligations	**1,781,082**	(at **32** fines)
Insufficient data processing agreement	**1,057,110**	(at **11** fines)
Insufficient involvement of data protection officer	**919,300**	(at **15** fines)

۱.۴ تعاریف اساسی

برخی تعاریف و اصطلاحاتی که به‌کرّات در مباحث مربوط به GDPR دیده می‌شوند عبارت‌اند از:

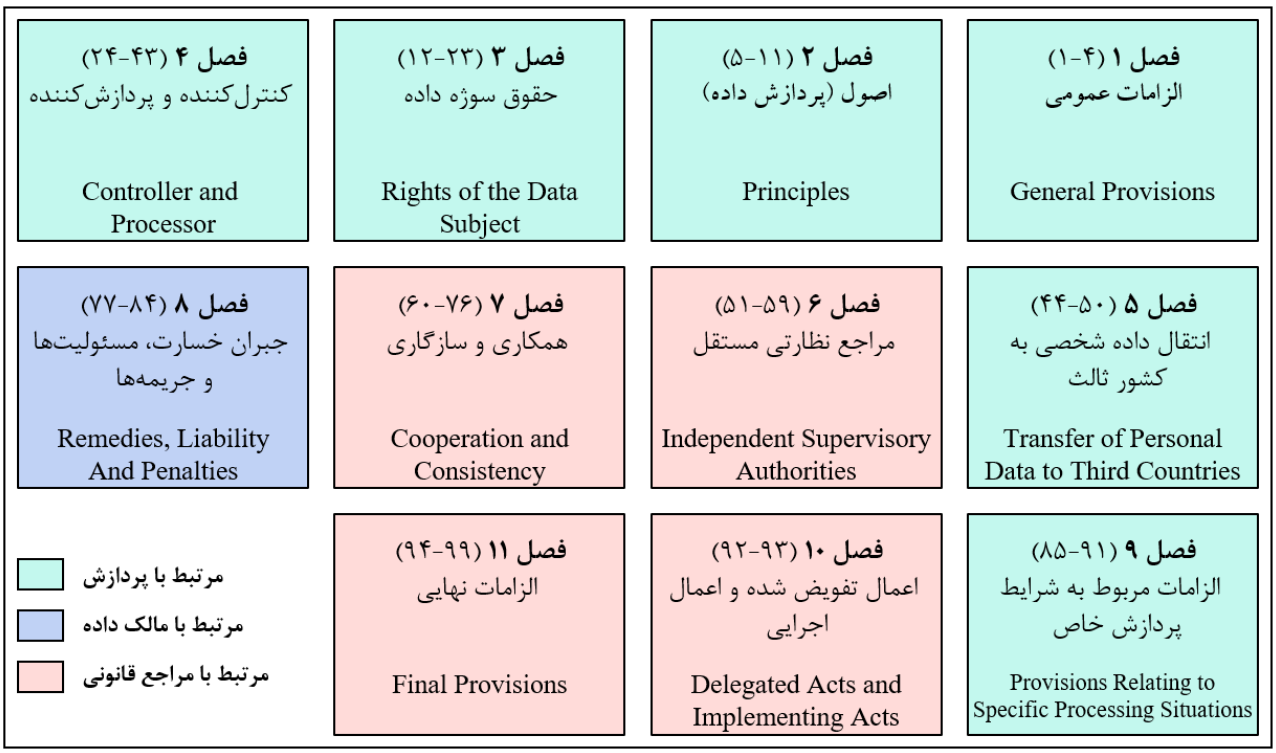
- **مالک داده:** به هر شخص حقیقی که داده‌های مربوط به او جمع‌آوری و پردازش می‌شود، مالک داده گفته می‌شود.
- **داده‌های شخصی**[۱]: این اصطلاح به هر اطلاعات مربوط به یک شخص حقیقی مانند نام، شماره‌ی شناسایی، شناسه‌ی برخط، اطلاعات فیزیولوژیکی و ژنتیکی، اقتصادی، فرهنگی و ... اطلاق می‌شود.
- **پردازش**[۲]: به اعمال هر عملیاتی روی داده‌های شخصی شامل جمع‌آوری، ضبط، سازمان‌دهی، ویرایش، پاک کردن و ... پردازش گفته می‌شود.
- **کنترل‌کننده**[۳]: به هر شخص حقیقی یا حقوقی، مقام عمومی، سازمان یا هر نهاد دیگری که به‌تنهایی یا به طور مشترک با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند، کنترل‌کننده گفته می‌شود.
- **پردازش‌کننده**[۴]: به هر شخص حقیقی یا حقوقی، مقام عمومی، سازمان یا هر نهاد دیگری که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند، پردازش‌کننده گفته می‌شود.
- **رضایت**[۵]: رضایت مالک داده به‌معنای هرگونه نشانه‌ی آزادانه، مشخص، آگاهانه و بدون ابهام از خواسته‌های مالک داده است که به‌موجب آن، مالک داده با یک بیانیه یا یک اقدام مثبت واضح، موافقت خود را با پردازش داده‌های شخصی مربوط به خود ابراز می‌کند.
- **مرجع نظارتی**[۶]: یک مقام عمومی مستقل است که توسط یک کشور عضو تأسیس شده است و وظیفه‌ی رسیدگی به تخلفات را دارد.

۲.۴ ماهیت قانون GDPR

ماهیت قانون GDPR بر کنترل داده‌های شخصی، شفافیت، عدالت و قانونی بودن پردازش‌ها جهت حفاظت از حقوق مالک داده استوار است. اصول پردازش داده‌های شخصی بر اساس ماده‌ی ۵ قانون عبارت‌اند از:

[1]Personal Data [2]Processing [3]Controller

[4]Processor [5]Consent [6]Supervisory Authority



شکل ۱. ساختار قانون GDPR

(۱) قانونی بودن، عدالت و شفافیت [۱]،
(۲) محدود کردن اهداف [۲]،
(۳) کمینه نمودن داده [۳]،
(۴) دقت [۴]،
(۵) محدودیت ذخیره‌سازی [۵]،
(۶) یکپارچگی و محرمانگی [۶].

سؤالی که ممکن است در اینجا مطرح شود این است که منظور از قانونی بودن پردازش چیست؟ در پاسخ باید گفت که در GDPR شش رکن اصلی برای قانونی بودن پردازش داده‌های شخصی در نظر گرفته شده است، که عبارت‌اند از:

(۱) اجرای قراردادهای منعقد شده بین مالک داده و کنترل‌کننده،
(۲) انطباق با الزام قانونی که کنترل‌کننده دارد،
(۳) دست‌یابی به منافع مشروع کنترل‌کننده،
(۴) حفاظت از منافع حیاتی مالکین داده،
(۵) منافع عمومی،
(۶) رضایت مالک داده.

به بیان دیگر، بر اساس GDPR، پردازش داده‌های شخصی مالکین داده تنها در صورتی قانونی است، که حداقل یک مورد از ارکان شش‌گانه‌ی فوق وجود داشته باشد.

[1]Lawfulness, Fairness and Transparency [2]Purpose Limitation [3]Data Minimisation [4]Accuracy [5]Storage Limitation [6]Integrity and Confidentiality

هدف نهایی از وضع این مجموعه‌ی قوانین، حفظ حقوق مالک داده در خصوص داده‌های شخصی خود می‌باشد. این حقوق هشت‌گانه که به حفظ حریم خصوصی مالک داده منجر می‌شوند عبارت‌اند از:

(۱) پردازش عادلانه [۷]،
(۲) حق دسترسی [۸]،
(۳) حق ویرایش [۹]،
(۴) حق پاک کردن [۱۰]،
(۵) حق محدودسازی پردازش [۱۱]،
(۶) حق انتقال داده [۱۲]،
(۷) حق اعتراض [۱۳]،
(۸) حقوق مربوط به تصمیم‌گیری خودکار [۱۴]

۳.۴ ساختار قانون GDPR

قانون GDPR، در دو بخش اصلی توضیحات [۱۵] (شامل ۱۷۳ مورد) و مواد قانونی [۱۶] (شامل ۱۱ فصل و ۹۹ ماده) گردآوری شده است. شکل ۱، ساختار کلی GDPR را در یک نگاه نشان می‌دهد.

[7]Fair Processing [8]Right to Access [9]Right to Rectification [10]Right to Erasure [11]Right to Restriction of Processing [12]Right to Data Portability [13]Right to Object [14]Right in Relation to Automated Decision-Making [15]Articles [16]Compliance

۵ انطباق

قانون GDPR حاوی الزامات و دستورالعمل‌هایی برای سازمان‌ها و شرکت‌هاست تا با پیروی از آن‌ها بتوانند از داده‌های شخصی و حریم خصوصی کاربران محافظت نمایند. پیروی از دستورالعمل GDPR اصطلاحاً انطباق با این قانون خوانده می‌شود. در این بخش بیان می‌شود که برای انطباق با GDPR، سازمان‌ها و شرکت‌ها می‌بایست چه اهدافی را مد نظر قرار داده و چه اقداماتی را انجام دهند.

۱.۵ اهداف

همان‌طور که تشریح شد، هدف کلی قانون GDPR محافظت از داده‌های شخصی در هر سازمان یا شرکتی است که داده‌های اشخاص حقیقی را جمع‌آوری می‌نماید. برای رسیدن به این هدف، در این قانون الزامات متعددی گردآوری شده است که برآورده نمودن هر کدام مستلزم اقدام یا اقداماتی از سوی سازمانی است که قصد انطباق با GDPR را دارد. دسته‌ای از این اقدامات شامل ایجاد روال‌های سازمانی جدید یا تغییر روال‌های پیشین هستند، در حالی که دسته‌ی دیگر از اقدامات شامل ایجاد یا اصلاح حفاظت‌های فنی و امنیتی هستند. بر این اساس، می‌توان اظهار کرد که هدف کلی در انطباق با GDPR، طراحی، پیاده‌سازی و اجرای اقدامات مقتضی برای برآورده نمودن الزامات و خواسته‌های مندرج در قانون است.

در عین حال، بر اساس قانون GDPR، لازم است سازمان‌ها بتوانند به شکل روشن و مستند انطباق خود با این قانون را نشان دهند. بازرسان و ممیزها در سرکشی‌های خود اطلاعات و اسنادی (اسناد طراحی، سیاست‌ها، ثبت وقایع و ...) را از سازمان درخواست می‌کنند که بتواند درستی ادعای انطباق را نشان دهد. همچنین در صورت بروز شکایت علیه سازمان، اطلاعات مشابهی لازم است به دادگاه ارائه شود تا سازمان با اثبات عدم تخلف از قانون بتواند از جریمه‌های سنگین در امان باشد. بنابراین، هدف دوم در انطباق با قانون GDPR، طراحی و پیاده‌سازی اقداماتی است که انطباق با قانون را اثبات نمایند.

در نهایت، با توجه به این که GDPR نگاهی بلند مدت و مستمر نسبت به محافظت از داده‌های شخصی و حریم خصوصی دارد، حفظ انطباق از طریق به‌روزرسانی سیاست‌ها، روال‌ها و حافظت‌های فنی، هدف سوم در انطباق با این قانون است.

۲.۵ خواسته‌های GDPR

همان‌طور که اشاره شد، در متن GDPR الزامات و دستورات متعددی ذکر شده است که قانون از سازمان‌ها و شرکت‌ها انتظار دارد آن‌ها را رعایت نمایند. این موارد را می‌توان در دو دسته‌ی کلی در نظر گرفت که در این بخش تشریح می‌شوند.

دسته‌ی اول: طراحی و مستندسازی انتظار می‌رود سازمان‌ها به صورت سیستماتیک و بر اساس چارچوب‌های حفاظت از حریم خصوصی، برنامه‌ها، طرح‌ها و سیاست‌های مقتضی و متناسب با سازمان را تدوین نموده و به صورت مکتوب مستند نمایند. رعایت شفافیت، صراحت و سادگی در مستندات (چه در برابر کاربران و مالکان داده و چه در برابر نهادهای نظارتی) از الزامات قانون GDPR است. بر این اساس، لازم است هر سازمان بتواند برای سؤالات متعددی پاسخ‌های مناسب بیابد و این پاسخ‌ها را به صورت مکتوب نگهداری و از طریق کانال‌های مناسب به مخاطبین مربوطه اعلام نماید. نمونه‌ای (نسبتاً جامع) از این سؤالات با یک بخش‌بندی چهارگانه در ادامه آمده است:

- بخش اول: تعیین داده‌ها و پردازش‌ها
  - چه اطلاعاتی جمع‌آوری می‌شود؟
  - چه پردازشی روی داده انجام می‌شود؟
  - چرا این پردازش لازم و قانونی است؟
  - فهرست پردازش‌کنندگان داده چیست؟
  - داده به کجا ارسال می‌شود؟
- بخش دوم: بیان حقوق مالک داده
  - بیان شفاف حقوق مالک داده به او
  - بیان نحوه‌ی تضمین حقوق مالک داده
  - مالک داده با چه فرد یا بخشی تماس بگیرد؟
  - کانال ثبت درخواست مالک داده چیست؟
  - ظرف چه مدت درخواست پاسخ داده می‌شود؟
- بخش سوم: تدوین و مستندسازی سیاست‌ها
  - سیاست‌های امنیت اطلاعات
  - سیاست‌های دسترسی به داده
  - سیاست‌های محافظت از داده‌ی شخصی
  - سیاست‌های دورکاری[1] (سیاست‌های BYOD)
  - سیاست‌های نگهداری داده
  - سیاست‌های کوکی‌ها
- بخش چهارم: راه‌کارهای محافظت
  - کلیات حفاظت فیزیکی به کار رفته چیست؟
  - چه مکانیزم‌های امنیتی در نظر گرفته شده‌اند؟
  - بیان کلیات مدیریت ریسک
  - چارچوب امنیتی و حفاظتی مورد استفاده چیست؟
  - استانداردهای محرمانگی اخذ شده چه هستند؟

دسته‌ی دوم: پیاده‌سازی پس از تدوین برنامه‌ها و سیاست‌ها، لازم است سازمان به پیاده‌سازی الزامات و دستورات مختلف پیش‌بینی شده در قانون مبادرت ورزد. در اینجا فهرستی (نسبتاً جامع) از آن‌چه که انتظار می‌رود سازمان‌ها برای انطباق با قانون GDPR پیاده‌سازی کنند در هفت بخش آمده است. دقت شود که بسته به مأموریت و اهداف سازمان، نوع داده‌ها، اندازه‌ی سازمان و ویژگی‌هایی از این دست، برخی از موارد بیان

[1] Bring Your Own Device

شده ممکن است نیاز به پیاده‌سازی نداشته باشند.

- بخش اول: سازمان‌دهی داده‌ها و پردازش‌ها
  - انتصاب Data Protection Officer (DPO)
  - تهیه‌ی سیاهه‌ی داده‌ها
  - اجرای Data Mapping
  - اجرای DPIA و مدیریت ریسک
  - پیاده‌سازی اصول پردازشی (Privacy by design and by default)
- بخش دوم: مدیریت حقوق سوژه داده
  - ایجاد کانال‌های ارتباطی
  - تهیه‌ی مستندات لازم مانند Privacy Policy، فرم‌های حقوق مالک داده، فرم رضایت، فرم انصراف از رضایت و ... و قرار دادن آن‌ها در اختیار مالک داده
  - ایجاد روال‌های دریافت درخواست‌ها
  - فعال شدن روند انطباق درخواست با سیاست‌ها
  - فعال شدن عملیات مناسب برای رسیدگی به درخواست
  - گزارش رد شدن درخواست
  - تضمین بازه‌ی زمانی پاسخگویی
- بخش سوم: مدیریت انطباق طرف‌های سوم
  - قراردادهای DPA با پردازش‌کننده‌ها
  - مکانیزم رصد انطباق پردازش‌کننده‌ها
- بخش چهارم: مدیریت انتقال داده‌های شخصی
  - تدوین سیاست‌های انتقال
  - توافق با پردازش‌کننده‌ها
- بخش پنجم: مکانیزم‌های حفاظت از اطلاعات شخصی
  - احراز اصالت کاربران
  - کنترل دسترسی
  - امن‌سازی سیستم‌ها - امن‌سازی سرورها
  - رمزگذاری داده‌ها - گمنام‌سازی داده‌ها
  - امن‌سازی ارتباطات
- بخش ششم: آگاه‌سازی پرسنل
  - برگزاری دوره‌های آموزشی
  - ایجاد فرهنگ سازمانی
- بخش هفتم: رسیدگی به بحران‌ها
  - شناسایی بحران
  - اطلاع‌رسانی به مرجع نظارتی
  - اطلاع رسانی به مالکین داده
  - تضمین محدودیت زمانی اطلاع‌رسانی
  - ثبت و نگهداری اطلاعات بحران در تاریخچه

۳.۵ استانداردهای انطباق با GDPR

بخشی از قانون GDPR به تعریف سازوکار استانداردهای انطباق اختصاص یافته است. در واقع، قانون‌گذار پیش‌بینی کرده است که برای نشان دادن انطباق با قانون می‌توان از سازوکارهایی استفاده کرد که پیاده‌سازی موفق خواسته‌های GDPR در سازمان را بررسی و تصدیق نمایند. الزامات، شرایط و جوانب مختلف چنین استانداردی چه از نظر سازمانی و چه از نظر روال‌ها در متن قانون آمده است.

در حال حاضر، استاندارد EuroPrivacy تنها مکانیزمی است که دارای تأیید رسمی از برد محافظت از داده‌ی اروپا (EDPB [1]) بوده و می‌تواند گواهی انطباق با قانون را برای پردازش‌ها صادر نماید [۲۰]. در رابطه با این استاندارد ذکر این نکته دارای اهمیت است که گواهی EuroPrivacy انطباق سازمان با قانون را نشان نمی‌دهد بلکه تعدادی از پردازش‌های درخواست شده از طرف سازمان را بررسی نموده و انطباق آن‌ها با GDPR را در صورت گذراندن موفق نیازمندی‌ها تأیید می‌نماید.

همچنین، GDPR سازمان‌ها را تشویق می‌کند که با چارچوب‌های حفاظت از حریم خصوصی موجود سازگاری یافته و برای نشان دادن توجه به GDPR گواهی انطباق با آن‌ها را کسب نمایند. نمونه‌هایی از این چارچوب‌ها، استاندارد ISO 27001 و به‌خصوص تعمیم‌یافته‌ی حفاظت از حریم خصوصی آن یعنی ISO 27701، استاندارد ISO 29100 و همچنین استاندارد BS-10012 هستند.

ضروری است به این نکته‌ی کلی در رابطه با استانداردها و چارچوب‌ها توجه شود که در هر حال، مسئول اصلی انطباق با GDPR سازمان (به عبارت دقیق‌تر کنترل‌کننده) است و تهیه‌ی گواهی‌های انطباق، در صورت نقض قانون، موجب سلب مسئولیت از کنترل‌کننده نمی‌شود.

۶ تقویت و گسترش قوانین حریم خصوصی در سال‌های اخیر

در سال‌های اخیر، مقررات مربوط به حریم خصوصی به دلیل نگرانی‌های فزاینده درباره‌ی حفاظت از داده‌ها و افزایش میزان اطلاعات شخصی که توسط سازمان‌ها پردازش و ذخیره می‌شود، به شدت تقویت شده‌اند. در سال ۲۰۲۴، کمیسیون اروپا، به منظور هماهنگ‌سازی همکاری‌ها بین مقامات حفاظت از داده‌های کشورهای عضو اتحادیه‌ی اروپا، قوانین جدیدی را برای تقویت اجرای GDPR در موارد بین‌مرزی پیشنهاد کرده است. همچنین، با پیشرفت روزافزون هوش مصنوعی (AI [2])، اتحادیه‌ی اروپا به طور فعال در حال کار بر روی مقرراتی برای حاکمیت بر توسعه و استفاده از هوش مصنوعی (AI) است تا اطمینان حاصل شود که به صورت مسئولانه، اخلاقی و ایمن استفاده می‌شود. مقررات هوش مصنوعی (AI) و مقررات عمومی حفاظت از داده‌ها (GDPR) به طور نزدیکی مرتبط هستند، زیرا هر دو چارچوب به‌دنبال حفاظت از حقوق افراد و اطمینان

[1] European Data Protection Board (EDPB) [2] Artificial Intelligence

از استفاده‌ی اخلاقی و مسئولانه از فناوری، به ویژه در زمینه‌ی پردازش داده‌ها و حریم خصوصی، می‌باشند. در دو زیربخش بعدی تقویت GDPR در روابط بین‌مرزی و قانون هوش مصنوعی اتحادیه‌ی اروپا به‌ترتیب مورد بررسی قرار می‌گیرند.

۱.۶ تقویت GDPR در روابط بین‌مرزی

اگرچه GDPR، از زمان تصویب، سنگ بنای حفاظت از داده‌ها در اتحادیه‌ی اروپا بوده است، با این وجود، اجرای آن به ویژه در موارد بین‌مرزی، به دلیل تفاسیر و رویه‌های متفاوت در کشورهای مختلف عضو، با چالش‌هایی مواجه شده است. برای رسیدگی به این مسائل، کمیسیون اروپا در جولای ۲۰۲۳، پیشنهادیه‌ای برای تقویت GDPR در موارد بین‌مرزی مطرح کرد که در سال ۲۰۲۴، به صورت مدون ارائه گردید. این قوانین به منظور هماهنگ‌سازی همکاری‌ها بین مقامات حفاظت از داده‌های کشورهای عضو اتحادیه‌ی اروپا طراحی شده‌اند [۲۱].

اهداف اصلی این پیشنهادیه عبارت‌اند از:

- هماهنگ کردن حقوق رویه‌ای[1] : این امر مستلزم استانداردسازی حقوق افراد درگیر در شکایات بین‌مرزی است، که تضمین‌کننده‌ی ثبات در بین کشورهای عضو می‌باشد.
- کارآمدسازی و تقویت همکاری بین مقامات نظارتی: این هدف، در جهت بهبود کارایی و همکاری بین مقامات حفاظت از داده‌ها در کشورهای مختلف هنگام رسیدگی به پرونده های بین‌مرزی است.
- مشخص کردن جزئیات مکانیسم حل اختلاف GDPR: این تقویت، به‌دنبال ایجاد رویه‌های روشن برای حل و فصل اختلافات بین مقامات حفاظت از داده‌های کشورهای مختلف است.

در حال حاضر، پارلمان اروپا موضع خود را در اولین خوانش اتخاذ نموده، بر اهمیت تقویت حقوق شاکیان، نقش مقامات نظارتی و هیئت حفاظت از داده‌های اروپا تأکید کرده، و کماکان در حال بررسی این پیشنهاد است. درصورت اجرایی شدن پیشنهادیه موارد زیر قابل حصول است:

- افزایش اطمینان حقوقی برای مشاغلی که در خارج از مرزها فعالیت می‌کنند،
- حفاظت قوی‌تر برای افرادی که داده‌های آن‌ها در چندین کشور اتحادیه‌ی اروپا پردازش می شود،
- اجرای کارآمدتر و سازگارتر GDPR.

لازم به ذکر است که مهم‌ترین ملاحظات کلیدی و چالش‌های مطرح در این زمینه عبارت‌انداز:

- ایجاد تعادل بین منافع: یافتن توازن مناسب بین حمایت از حقوق افراد، تضمین اطمینان قانونی برای کسب و کارها و اجتناب از تشریفات اداری بیش از حد، کاری پیچیده است.
- پیاده‌سازی: اجرای مؤثر قوانین جدید، به منابع و آموزش کافی برای مقامات حفاظت از داده‌ها نیاز دارد.
- همکاری بین‌المللی: هماهنگی با کشورهای غیر اتحادیه‌ی اروپا در مورد مسائل حفاظت از داده‌ها همچنان یک چالش است.

۲.۶ قانون هوش مصنوعی اتحادیه‌ی اروپا

اتحادیه‌ی اروپا ظهور و گسترش فناوری هوش مصنوعی را با حساسیت قابل ملاحظه‌ای پی گرفته است و پیشتاز بحث‌ها و فعالیت‌ها پیرامون گسترش هوش مصنوعی با محوریت اخلاق و مسئولیت بوده است. نگاهی به فعالیت‌های انجام شده و مرور گزارش‌های منتشر شده توسط این اتحادیه [۲۲، ۲۵]، به روشنی نشان می‌دهند که از دید این اتحادیه، فناوری هوش مصنوعی نیازمند نظارت و کنترل است و عدم کنترل آن می‌تواند آسیب‌های جدی به حقوق بنیادی افراد وارد نماید. قانون هوش مصنوعی اتحادیه‌ی اروپا، با همین دیدگاه و با هدف ایجاد اطمینان نسبت به توسعه و استفاده از کاربردهای مبتنی بر هوش مصنوعی به صورت اخلاقی و مسئولانه در سال ۲۰۲۱ و توسط کمسیون اروپا پیشنهاد شد. این قانون پس از طی روال‌های قانون‌گذاری و اصلاحیه‌های متعدد توسط پارلمان اروپا و شواری اتحادیه‌ی اروپا، سرانجام در سال ۲۰۲۴ مورد پذیرش رسمی قرار گرفت و از اول آگوست ۲۰۲۴ الزام‌آور و اجرایی خواهد بود.

منطبق با رویکرد اتحادیه‌ی اروپا در مواجهه با فناوری هوش مصنوعی، این قانون سیستم‌های هوش مصنوعی را بر اساس میزان خطرآفرین بودن آن‌ها نسبت به حقوق و ایمنی افراد به چهار رده‌ی زیر تقسیم‌بندی می‌کند:

- سیستم‌های AI با ریسک غیرقابل قبول،
- سیستم‌های AI با ریسک بالا،
- سیستم‌های AI با ریسک محدود و
- سیستم‌های AI با ریسک حداقلی.

یکی از عوامل تعیین کننده در دسته‌بندی سیستم‌های هوش مصنوعی از حیث خطرآفرین بودن، چگونگی برخورد آن‌ها با داده‌های شخصی و حریم خصوصی بوده است. از این حیث، قانون GDPR به عنوان مرجع قرار داده شده و موضوعات اصلی مرتبط با داده‌های شخصی و حریم خصوصی با ارجاعات متعدد به این قانون مورد بحث قرار گرفته است. موضوعات بسیار مهم مرتبط با داده‌های شخصی و حریم خصوصی که در قانون هوش مصنوعی اتحادیه‌ی اروپا بررسی شده‌اند عبارت‌اند از:

- شفافیت: لازم است سیستم هوش مصنوعی اطلاعات مورد نیاز برای نشان دادن چگونگی تأثیر سیستم هوش مصنوعی بر افراد استفاده کننده را تهیه و در اختیار عموم استفاده‌کنندگان قرار دهد. مصداق‌های این اطلاعات که تأثیر سیستم هوش مصنوعی بر داده‌های شخصی است در قانون GDPR ذکر شده‌اند (از جمله، فهرست داده‌های شخصی جمع‌آوری شده، فهرست پردازش‌های متصور، اهداف هر پردازش، محدودیت‌ها و زمان‌بندی‌ها).

[1] Procedural Rights

- محافظت از داده‌ها: سیستم هوش مصنوعی الزام دارد از داده‌هایی که جزء داده‌های شخصی تقسیم‌بندی می‌شوند محافظت نماید. برای این کار، اصول محدودسازی پردازش‌ها و کمینه نمودن داده‌ها و همچنین پیاده‌سازی اصول طراحی پردازش‌ها (Privacy by design and by default) و گمنام‌سازی و رمزگذاری داده‌ها مورد تأکید قرار گرفته است.
- عدالت و عدم تبعیض: سیستم هوش مصنوعی الزام دارد که عاری از خروجی‌های جانبدارانه به نفع شخص یا گروهی از اشخاص باشد. برای رسیدن به این هدف، حقوق مرتبط با تصمیم‌گیری خودکار و حق دسترسی که در GDPR برای مالک داده در نظر گرفته شده است و الزامات مرتبط با این حقوق مورد تأکید قرار گرفته‌اند.
- مسئولیت‌پذیری: قانون هوش مصنوعی الزام می‌کند که اشخاص حقیقی یا حقوقی مرتبط و مسئول در امر توسعه، استقرار و استفاده از هر سیستم هوش مصنوعی شناخته شده و معین باشند. این اشخاص معادل کنترل‌کننده در قانون GDPR هستند و در قبال داده‌های شخصی و حریم خصوصی پاسخگو می‌باشند.

در اینجا لازم به ذکر است که موضوع قانون هوش مصنوعی، به طور خاص پیش‌بینی و کنترل مخاطرات احتمالی فناوری هوش مصنوعی است و قانون GDPR به عنوان ابزار قانونی و جامع برای سامان‌دهی به داده‌های شخصی و حریم خصوصی، در خلال این قانون مورد استفاده قرار گرفته است. با این وجود، با توجه به گستره‌ی وسیع داده‌های شخصی و ارتباط تنگاتنگ فناوری هوش مصنوعی با داده‌ها، در جای جای قانون هوش مصنوعی، ارجاع به GDPR و کمک گرفتن از پیش‌بینی‌ها و الزامات این قانون جامع قابل مشاهده است.

۷ ویژگی‌های عملیاتی و اجرایی GDPR

در تدوین قانون GDPR، نکات و جوانب متعددی برای ایجاد اطمینان نسبت به اجرایی شدن آن گنجانده شده است. در حقیقت، تدوین کنندگان GDPR نیازمندی‌های حقوقی، فنی و عملیاتی یک سازوکار جامع برای حفظ حریم خصوصی را تا حد بسیار زیادی پیش‌بینی نموده و روش‌های مناسبی جهت تامین آن‌ها ارائه کرده‌اند. همان‌طور که پیش‌تر در بخش ۲.۲ اشاده شد، یکی از مهم‌ترین دلایل جایگاه تأثیرگذار GDPR، ویژگی‌های عملیاتی و اجرایی آن است که می‌تواند الگوی مناسبی برای وضع قوانین مربوط به حریم خصوصی در کشور باشد. از این رو، پیش از پرداختن به مسئله‌ی حریم خصوصی در کشور در بخش ۸، در این بخش به مرور برخی جنبه‌های عملیاتی و اجرایی GDPR می‌پردازیم، که عبارت‌اند از:

- **لزوم وجود سازوکار قانونی:** تجربه‌ی تلاش‌هایی که پیش‌تر به مقوله‌ی حریم خصوصی پرداخته‌اند نشان داده است که رعایت حریم خصوصی افراد پدیده‌ای نیست که به صورت خودجوش یا خودسازمان‌ده در جامعه ایجاد شود. در حقیقت، بدون وجود دستورالعمل‌های منسجم و همه‌جانبه با پشتوانه‌ی اجرایی، دست‌یابی به حریم خصوصی میسر نیست. دلایل متنوعی برای این امر قابل ذکر است. یکی از مهمترین دلایل، عدم وجود انگیزه‌ی ملموس برای رعایت حریم خصوصی در نزد جمع‌آوری‌کنندگان داده‌های شخصی است. حتی در مواردی، جمع‌آوری‌کننده‌ی داده‌های شخصی از عدم رعایت حریم خصوصی نفع خواهد برد. دلیل مهم دیگر، قدرت نابرابر مالکین داده در مقابل جمع‌آوری‌کنندگان داده است. در اکثر سناریوها، خدماتی از سوی جمع‌آوری‌کننده‌ی داده‌های شخصی ارائه می‌شود که مالک داده به آن خدمت نیازمند است. در نتیجه، مالک داده در عمل نمی‌تواند در مقام معترض به شیوه‌ی جمع‌آوری داده ظاهر شود. این نابرابری قدرت در مورد مواجهه‌ی افراد با سازمان‌های ارائه‌دهنده‌ی خدمات دولتی و حکومتی به مراتب شدیدتر است. یکی از نکات مهم در رابطه با GDPR آن است که چنین نیازمندی‌ای در آن به درستی درک شده و سازوکار مناسب برای حفاظت از داده‌های شخصی و حریم خصوصی افراد را در قالب سازوکار قانونی با ضمانت‌های اجرایی مناسب پیاده‌سازی کرده است.
- **تعیین دقیق ساختار تشکیلات اجرایی:** در متن قانون GDPR تمامی نهادهای لازم برای اجرای قانون تعیین شده، قدرت عمل، وظایف و مسئولیت‌های هر نهاد به وضوح تبیین شده و سلسله مراتب و چگونگی ارتباط نهادها با یکدیگر به‌روشنی تعیین شده است. همچنین زمان‌بندی قابل قبول برای تشکیل و استقرار تدریجی نهادها پیش‌بینی شده است. بدین ترتیب، ابهام و سردرگمی در چگونگی اجرای قانون و بلاتکلیفی افراد و سازمان‌های متولی عملاً منتفی شده است.
- **انسجام و جلوگیری از تفرق:** یکی از مهمترین نکات درباره‌ی GDPR آن است که با وضع این قانون، رویکرد اتحادیه‌ی اروپا به مسئله‌ی حریم خصوصی از وضع دستورالعمل و توصیه به کشورهای عضو خارج شده و به رویکردی فعال و منسجم و هماهنگ برای سراسر اروپا تبدیل شده است که تفرق و ناسازگاری در اجرای آن وجود ندارد. این رویکرد با ماهیت حریم خصوصی و داده‌های شخصی که عملاً قابل مرزبندی و محدود به جغرافیا و زمان نیستند تناسب بیشتری دارد.
- **تعیین ابزار الزام‌آوری متناسب:** در تدوین GDPR، به درستی پیش‌بینی شده است که بدون وضع جرائم سنگین، جمع‌آوری کنندگان داده‌های شخصی تمایلی به اجرای قانون نشان نخواهند داد. وضع جریمه‌های سنگین باعث شده است انطباق با GDPR به یکی از اولویت‌های نهادها و کسب و کارهایی که با داده‌های شخصی شهروندان اروپایی سروکار دارند تبدیل شود.
- **پیش‌بینی معیارها و تعریف استانداردها:** از آن‌جا که رعایت الزامات GDPR ممکن است برای کسب و کارها و سازمان‌ها با پیچیدگی همراه باشد، روال‌های لازم برای کمک به انطباق با این قانون در متن قانون گنجانده شده است. از آن جمله، چگونگی تهیه‌ی راهنما برای صنف‌ها ـ که در آن مجموعه‌ی الزامات و معیارهای انطباق با GDPR برای صنف مورد نظر گردآوری می‌شود ـ در قانون آمده است. علاوه بر این، ویژگی‌های سیستم اعطای استاندارد انطباق با GDPR نیز به طور دقیق در متن قانون بیان شده است.
- **الزامات واقع‌بینانه:** یکی از نکات بسیار آموزنده که در GDPR به

چشم می‌خورد، پرهیز از توصیه‌های کلی و ایده‌آل و توجه دقیق به سناریوها و نیازهای واقعی است. در حقیقت، قوانین حریم خصوصی GDPR از تحمیل روال‌های پیچیده و هزینه‌های نامعقول به سازمان‌ها یا کسب و کارها پرهیز می‌کند. برای مثال، برخی الزامات به حالتی که داده‌های شخصی به صورت کاغذی نگهداری می‌شوند قابل اعمال نیستند. به عنوان نمونه‌ای دیگر، در برخی سناریوها ممکن است پاک کردن داده‌های شخصی کاربر از تمام محل‌هایی که داده در آن‌ها ذخیره شده است غیر عملی باشد. لذا بر اساس متن صریح قانون، رعایت الزامات مربوط به پاک کردن داده‌ها تا حدی که تکنولوژی روز اجازه می‌دهد قابل قبول است.

- **توجه به جزئیات سناریوها:** از آنجا که طیف بسیار گسترده و متنوعی از سناریوها از مناسبات روزمره گرفته تا فناوری‌های نوین همگی با مسئله‌ی حفظ حریم خصوصی درگیر هستند، چالشی که GDPR به خوبی توانسته آن را مرتفع نماید، تقسیم‌بندی مناسب سناریوها و وضع الزامات جامع و فراگیر بوده است. در تمامی بخش‌های این قانون اجتناب از کلی‌نگری و توجه به جزئیات سناریوها و بررسی و تعیین تکلیف حالت‌های خاص قابل مشاهده است به طوری که ابهام در برداشت از قانون و تفسیرهای متفاوت از آن عملاً ممکن نیست. می‌توان گفت که این جنبه از GDPR اساسی‌ترین عاملی است که آن را به قانونی قابل اجرا و مفید در سناریوهای عملی تبدیل نموده است.

۸ مسئله‌ی حفظ حریم خصوصی در کشور

در این بخش، به مسئله‌ی حریم خصوصی در کشور پرداخته و سعی می‌شود با الگوبرداری از GDPR به ویژه ویژگی‌های عملیاتی و اجرایی آن، که به واقع آن را به قانونی تأثیرگذار در جهان مبدل کرده است، اقدامات اساسی لازم برای سامان‌دهی به وضعیت موجود در کشور مورد بررسی قرار گیرد.

۱.۸ وضعیت فعلی مسئله‌ی حریم خصوصی در کشور

می‌توان گفت علی‌رغم اهمیت غیرقابل انکار بحث محافظت از حریم خصوصی افراد، تاکنون نهادهای مسئول در کشور به جز اعلان‌ها و دستورالعمل‌های موردی، به صورت منسجم توجهی به این موضوع حیاتی نداشته‌اند. از جمله مصوباتی که به صورت موردی و جزئی به این مسئله پرداخته‌اند عبارت‌اند از:

- قانون تجارت الکترونیکی: این قانون، که در دی ماه سال ۱۳۸۲ به تصویب رسید، به مسائل مرتبط با حفظ حریم خصوصی در مبادلات الکترونیکی می‌پردازد و شامل موادی است که از حقوق مصرف‌کنندگان در خرید و فروش‌های آنلاین حمایت می‌کند [۲۶].
- قانون جرایم رایانه‌ای: این قانون در خرداد ماه سال ۱۳۸۸ به تصویب رسید و شامل موادی است که به حفاظت از داده‌ها و حریم خصوصی افراد در فضای مجازی می‌پردازد [۲۷].
- قانون حمایت از حقوق مصرف‌کنندگان: این قانون، که در مهر ماه سال ۱۳۸۸ مصوب شد، شامل موادی است که به حفظ حریم خصوصی مصرف‌کنندگان در معاملات تجاری می‌پردازد و از حقوق آن‌ها در برابر سوءاستفاده‌های احتمالی دفاع می‌کند [۲۸].
- قانون آیین دادرسی کیفری: این قانون در سال ۱۳۹۲ تصویب شد و در خرداد ماه ۱۳۹۴ اصلاحیه‌ای برای آن مصوب گردید. در موادی از این قانون، به نحوه‌ی برخورد با جرایم مرتبط با حریم خصوصی و جمع‌آوری اطلاعات شخصی افراد توسط دستگاه‌های قضایی پرداخته شده است [۲۹].

یکی از معدود مصوبات جامع‌تر در زمینه‌ی حفظ حریم خصوصی، «دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه‌ی جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی» است که در یکصد و بیست و هفتمین جلسه‌ی کمسیون عالی تنظیم مقررات فضای مجازی کشور در تاریخ ۱۴۰۲/۴/۱۱ مصوب و منتشر شده است [۳۰]. برخی از مهمترین موارد اشاره شده در این دستورالعمل به شرح زیر است:

- بیان شفاف سیاست‌های جمع‌آوری، پردازش و نگهداری داده‌های کاربران
- تعیین اهداف جمع‌آوری و پردازش داده‌ها
- اخذ رضایت کاربران
- اعلام صریح و شفاف تغییر سیاست‌ها و اخذ مجدد رضایت کاربران
- کمینه نمودن داده‌ها
- ایجاد امکان حذف داده‌ی کاربر (درصورت درخواست کاربر)

کلیه‌ی ارائه‌دهندگان خدمات از طریق سامانه‌ها و سکوهای فضای مجازی موظف شده‌اند در فرصتی دو ماهه دستورالعمل اشاره شده را پیاده‌سازی نمایند.

صدور دستورالعمل‌های مقطعی مانند آن‌چه مرور شد، هرچند نشان‌دهنده‌ی درک نسبی اهمیت موضوع از سوی نهادهای مسئول است، اما در عمل قادر نخواهد بود اثر قابل توجهی در سامان دادن به وضع موجود بر جای گذارد. نقض مکرر داده‌های کاربران ایرانی در سال‌های اخیر، مؤید این امر است. پرداختن به دلایل و ریشه‌های عدم توجه منسجم و جدی به بحث حریم خصوصی و سامان‌دهی آن، خارج از حوصله‌ی بحث حاضر است.

۲.۸ اقدامات اساسی برای سامان‌دهی به وضع موجود بر اساس ویژگی‌های عملیاتی و اجرایی GDPR

همان‌طور که اشاره شد، وضع کنونی حریم خصوصی در کشور نابسامان است و لازم است برای جلوگیری از آسیب‌های آن و برای حصول سازوکار مناسب، توجه ویژه‌ای از سوی نهادهای مسئول به این بحث مبذول گردد. بر اساس آن‌چه که در رابطه با حریم خصوصی و به‌خصوص قانون GDPR بیان شد، اقدامات اساسی حداقلی زیر برای دست‌یابی به سازوکار مناسب

برای حفاظت از حریم خصوصی افراد در سطح کشور لازم و حیاتی به نظر می‌رسند:

تعریف الزامات حریم خصوصی و تصویب قوانین مناسب پیش از این اشاره شد که رعایت حریم خصوصی افراد پدیده‌ای نیست که به صورت خودجوش یا خودسازمان‌ده در جامعه ایجاد شود و بدون وجود دستورالعمل‌های منسجم و همه‌جانبه با پشتوانه‌ی اجرایی، دست‌یابی به حریم خصوصی میسر نیست. بنابراین، تدوین قوانین جامع که شامل تعریف دقیق حریم خصوصی و همچنین نهادها، فرآیندها و دستورالعمل‌های رعایت حریم خصوصی در جامعه باشند حیاتی است.

یکی از نکات قابل ملاحظه در رابطه با قوانین حریم خصوصی آن است که دستورالعمل‌هایی که در این حوزه وضع می‌شوند لازم است ضمن در نظر گرفتن جنبه‌های مختلف مبحث حریم خصوصی افراد، رکن اجراپذیر بودن را نیز دارا باشند. بنابراین، لازم است قوانین حریم خصوصی تا حد ممکن روال‌های کاری سازمان‌ها یا کسب و کارها را محدود ننمایند یا روال‌های پیچیده‌ای به آن‌ها تحمیل نکنند.

الزام‌آوری اجرای قوانین رعایت حریم خصوصی در جامعه علاوه بر تدوین قوانین، مستلزم عزم جدی در راستای اجرای قوانین و الزام بخش‌های دولتی و خصوصی به پیاده‌سازی گسترده‌ی مصوبات مرتبط با حریم خصوصی است. این امر به نوبه‌ی خود، مستلزم انتخاب ابزارهای مناسب الزام‌آوری مانند وضع جریمه‌های نقدی برای تضمین اجرای قوانین است. علاوه بر این، لازم است در هنگام وضع قوانین حریم خصوصی، نهادهایی برای نظارت بر اجرای قوانین و همچنین تمهیداتی برای تسهیل پیاده‌سازی دستورالعمل‌ها در نظر گرفته شوند. پس از تصویب قوانین، ضروری است نهادهای تعریف شده در اسرع وقت تشکیل شده و شروع به کار نمایند.

فرهنگ‌سازی و اطلاع‌رسانی عمومی بدون آگاهی افراد از حقوق خود در زمینه‌ی حریم خصوصی، اقدامات دیگر در این زمینه کارکرد مورد انتظار را نخواهند داشت. از آنجا که حریم خصوصی بخشی از حقوق افراد است، اطلاع‌رسانی عمومی و گسترش آگاهی نسبت به این حق در سطح جامعه، در بلند مدت منجر به بروز روحیه‌ی مطالبه‌گری رعایت حریم خصوصی در افراد خواهد شد. بدیهی است این روحیه به نوبه‌ی خود اهرمی قوی برای متمایل کردن جامعه به رعایت گسترده‌ی حفظ حریم خصوصی خواهد بود. به این ترتیب، با فرهنگ‌سازی و اطلاع‌رسانی مناسب، بخش قابل توجهی از هزینه‌های ناشی از عدم رعایت حریم خصوصی، از جمله هزینه‌ی شکایت‌ها و طی شدن روال‌های قانونی کاهش خواهد یافت.

توجه به تربیت متخصصین حریم خصوصی رعایت حریم خصوصی در هر سازمان نیازمند طراحی و پیاده‌سازی سیاست‌ها و فرآیندهای متعدد و همچنین استفاده از فناوری‌ها و ابزارهای خاص، به خصوص در زمینه‌ی علم داده و امنیت اطلاعات و ارتباطات است. بنابراین، در صورت تصویب و اجرای قوانین حریم خصوصی، متخصصانی نیاز خواهند بود که بتوانند این قوانین را به شکل مؤثری در سازمان‌ها جاری کنند. با پیش‌بینی این موضوع و تدوین برنامه‌هایی مانند گنجاندن مباحث نظری و عملی مرتبط با حریم خصوصی در دروس دانشگاهی و استفاده از ظرفیت‌های آموزشی و ترویجی انجمن‌های علمی مرتبط، می‌توان برای رفع نیاز به متخصصین حوزه‌ی حفظ حریم خصوصی گام‌های مؤثری برداشت.

۹ نتیجه‌گیری

در این مقاله، تلاش شد اهمیت مسئله‌ی حفاظت از حریم خصوصی اشخاص، به عنوان یکی از مهم‌ترین چالش‌های عصر حاضر، و همچنین وضعیت توجه به این مسئله در سطح جهان و در سطح کشور روشن شود. تاریخچه‌ی مختصری که در این باب بیان شد نشان می‌دهد که در عصر توسعه‌ی ارتباطات و فناوری اطلاعات، توجه به حفاظت از حریم خصوصی پررنگ‌تر شده و اهمیت این موضوع بیش از پیش درک شده است و به مرور با روشن شدن اهمیت و حساسیت این موضوع، قوانینی برای حفاظت از حریم خصوصی اشخاص در جوامع مختلف تدوین شده‌اند. اشاره شد که از این میان، قانون عمومی حفاظت از داده در اروپا (GDPR)، به دلیل نگاه جامع و دقیق به موضوع و نیز ویژگی‌های عملیاتی و اجرایی مناسب، بیشترین توجه را در بیست سال اخیر، به خود اختصاص داده است. همچنین بیان شد که جایگاه ویژه و تأثیرگذاری GDPR، این قانون را به الگوی مناسبی برای وضع قوانین مربوط به حریم خصوصی در جهان تبدیل کره است. مباحثی که در ارتباط با ماهیت، ساختار، محتوا و خواسته‌های قانون GDPR در این مقاله مرور شد، هرچند خلاصه و گذرا، می‌تواند ابعاد مهم موضوع حریم خصوصی و المان‌های مهم جهت برخورد سیستماتیک با این مسئله را نشان دهد. در نهایت، پس از مرور ویژگی‌های عملیاتی و اجرایی GDPR، وضعیت موجود کشور در خصوص مسئله‌ی حفظ حریم خصوصی افراد به اجمال بررسی و سعی شد با در نظر گرفتن کاستی‌های موجود نسبت به قوانین بین‌المللی مانند GDPR، گام‌های حداقلی برای سامان‌دهی شرایط پیشنهاد شود.

سپاسگزاری

پژوهش حاضر با حمایت مادی و معنوی شرکت مهندسی ارتباطی پیام‌پرداز اجرا شده است که بدین وسیله از حسن توجه و حمایت‌های صورت گرفته تشکر و قدردانی می‌شود.

مراجع

[1] Holvast, J. History of privacy. In The history of information security, pp. 737-769, Elsevier Science BV, 2007.

[2] Ware, W. H. Records, computers and the rights of citizens, 1973.

[3] https://www.gesetze-im-internet.de/bdsg_2018/

[4] Organisation for Economic Co-operation and Development. Council. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD, 1980.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[6] https://gdpr-info.eu/

[7] Bharti, S. S., & Aryal, S. K. The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the companies. Journal of Contemporary European Studies, 31(4), 1391-1402, 2023.

[8] Häuselmann, A., & Custers, B. Substantive fairness in the GDPR: Fairness Elements for Article 5.1 a GDPR. Computer Law & Security Review, 52, 105942, 2024.

[9] Ke, T. T., & Sudhir, K. Privacy rights and data security: Gdpr and personal data markets. Management Science, 69(8), 4389-4412, 2023.

[10] Li, H., Yu, L., & He, W. The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22(1), 1-6, 2019.

[11] Tankard, C. What the GDPR means for businesses. Network Security, 2016(6), 5-8, 2016.

[12] Marchetti, E., Valente, A., Witfelt, C., Amo-Filvà, D., Garcia-Holgado, A., Garcia-Holgado, L., ... & Moreira, F. Teachers' perspective on the implementation of GDPR in schools: a design-oriented case study. In Lecture Notes in computer sciences: LNCS. Springer, 2024.

[13] Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. GDPR compliant blockchains–a systematic literature review. IEEE Access, 9, 50593-50606, 2016.

[14] Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Research and Applications, 100129, 2023.

[15] Kesa, A., & Kerikmäe, T. Artificial intelligence and the GDPR: Inevitable nemeses. TalTech Journal of European Studies, 10(3), 68-90, 2020.

[16] Meszaros, J., & Ho, C. H. (2021). AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR. Computer Law & Security Review, 41, 105532, 2021.

[17] https://europa.eu/eurobarometer/surveys/detail/2222

[18] https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

[19] https://www.enforcementtracker.com/?insights

[20] https://www.europrivacy.com/

[21] Newly proposed rules to strengthen GDPR enforcement in cross-border cases (europa.eu)

[22] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[23] European Commission. High-Level Expert Group on AI C., Ethics guidelines for trustworthy AI. 2019.

[24] European Commission. White Paper on Artificial intelligence – A European approach to excellence and trust. 2020.

[25] European Parliament. Artificial Intelligence Act. Legislative resolution, P9_TA '(2024)0138. 13 Mar. 2024.

[26] https://rc.majlis.ir/fa/law/show/93997

[27] https://rc.majlis.ir/fa/law/show/135717

[28] https://rc.majlis.ir/fa/law/show/136112

[29] https://rc.majlis.ir/fa/law/show/934354

[30] https://rc.majlis.ir/fa/law/show/1797869

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 1 (pp. 89–101)
https://monadi.isc.org.ir

Preserving privacy in the age of information technology development, lessons from the european general data protection regulation

Babak Siabi [1] and Parvin Rastegari [2,*],

[1] *PayamPardaz Communication Engineering Company, Isfahan, Iran*
[2] *Electrical and Computer Engineering Group, Golpayegan College of Engineering, Isfahan University of Technology, Golpayegan, 87717-67498, Iran*

ARTICLE INFO.

Article history:
Received: June 1, 2024
Accepted: September 11, 2024
Published Online: October 28, 2024

Keywords:
Privacy
Protection of Personal Data
GDPR

Type: Technical paper

ABSTRACT

Due to the increasing amount of data collection and processing in today's digital world, preserving individual and organizational privacy has become an undeniable necessity. In this regard, alongside the efforts of scientific and research centers to address privacy issues, several laws have been established in different countries. Among these, the General Data Protection Regulation (GDPR) at the European level is widely regarded by researchers as the most significant change in the field of privacy laws in recent decades and serves as a strong model for managing personal data. Based on this, in this article, to explore the multifaceted nature of privacy, we first review the history of privacy protection, then focus on the GDPR law. Some of the most important points and considerations regarding the nature and structure of this law, as well as the necessity and challenges of compliance with it, are presented. Additionally, the extensive measures outlined in this law for the implementation and enforcement of privacy protection mechanisms are discussed. Finally, by mapping the discussed content to the current state of privacy in Iran, some key points for the practical implementation of privacy laws in Iran are highlighted.

© 2024 ISC

* Corresponding author
Email addresses: siabi@ payampardaz.com (Babak Siabi), p.rastegari@iut.ac.ir (Parvin Rastegari)
© 2024 ISC. All rights reserved.