دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۲ (۱۲-۲۳)
https://monadi.isc.org.ir

ارائه‌شده در بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه تربیت مدرس و پژوهشگاه ارتباطات و فناوری اطلاعات، ۲۵ و ۲۶ مهرماه ۱۴۰۳

# تحلیل موضوعات راهبردی در قلمرو مقررات حفاظت از داده‌های عمومی★

ابوذر عرب سرخی[۱،*] و طلا تفضلی[۲]

[۱]گروه فناوری ارزیابی امنیت شبکه و سامانه‌ها، پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران
[۲]گروه امنیت اطلاعات و سامانه‌ها، پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

**اطلاعات مقاله**

کلمات کلیدی:
حفاظت از داده
موضوعات راهبردی
مقررات حفاظت از داده‌های عمومی
تحلیل محتوا

نوع مقاله: پژوهشی

**چکیده**

یکی از سرفصل‌های مهم و قابل اعتنا در عصر اطلاعات، حفاظت از داده و صیانت از اطلاعات است؛ چرا که عدم توجه به این مقوله در وهله اول اعتماد و به تبع آن کاربردپذیری و توسعه خدمات ارتباطی و فناوری اطلاعات را در معرض تهدید جدی قرار می‌دهد. از این رو، سیاست‌گذاران و تصمیم‌سازان سازمان‌ها، صنایع و دولت‌ها در پی تنظیم‌گری در این فضای تبادل اطلاعات پرآشوب هستند. این تنظیم‌گری مبتنی بر ملاحظات و متغیرهای تصمیم کلیدی حفاظت از داده انجام می‌شود که عدم توجه به آنها می‌تواند چالش‌برانگیز و بعضاً بحران‌زا باشد و در علوم مدیریت از آنها تحت عنوان موضوعات راهبردی یاد می‌شود. بر این اساس، تحقیق حاضر به شناسایی، تعریف و تحلیل موضوعات راهبردی می‌پردازد که دولت‌های مختلف از آن، جهت تقویت ساختارهای حکمرانی اطلاعات از جنس حفظ و مدیریت امنیت داده‌ها و اطلاعات بهره‌برداری می‌نمایند. این موضوعات راهبردی در قلمرو اسناد ملی، استانداردهای مرجع و مصوبات مرتبط با مقررات حفاظت از داده‌های عمومی (GDPR) آدرس‌دهی شده‌اند. بنابر این در تحقیق حاضر، ضمن بررسی اسناد و مراجع معتبر با مقررات حفاظت از داده‌های عمومی از طریق تحلیل محتوا، نسبت به تحلیل آنها جهت شناسایی موضوعات راهبردی اقدام خواهد شد.

© ۱۴۰۳ انجمن رمز ایران

## ۱ مقدمه

در دنیای امروز، فناوری‌های اطلاعاتی و ارتباطی نقشی دوگانه را ایفا می‌نمایند. از یک طرف این فناوری‌ها به‌عنوان یک توانمندساز نقشی مؤثر در خلق مدل‌های جدید کسب و کار، مدیریت و عرضه نسل جدید خدمات ارزش افزوده الکترونیکی، توسعه جامعه و شهر هوشمند، بکارگیری ابزارهای متصل و تسهیل سرویس‌پذیری در هر نقطه از جهان را ایفا می‌نمایند. از طرف دیگر فناوری‌های اطلاعاتی و ارتباطی می‌توانند نقشی ویرانگر را در دسترسی از راه دور، انکار فعالیت‌های مخرب، جعل هویت، افشاء اطلاعات شخصی و نیز مهندسی اجتماعی بازی کنند.

در هر شرایط و با توجه به سطح توسعه‌یافتگی جوامع و سازمان‌ها، فناوری‌های اطلاعاتی و ارتباطی نقش مولد و یک ساز و کار مدیریت داده‌های دیجیتالی را ایفا می‌کنند؛ داده‌هایی که می‌توانند شخصی، مالی، کاری، اجتماعی و یا قومیتی باشند. گستره وسیع شبکه‌های اجتماعی، فناوری‌های اطلاعاتی و خدمات ارتباطی موجب گردیده تا فضای کار و تعامل در عصر حاضر به یک شبکه حسگر اطلاعاتی بزرگ تبدیل شود؛ شبکه‌ای که حسگرهای آن‌ها تجهیزات موبایل، سامانه‌های رایانه‌ای، خدمات تحت وب و برنامه‌های کاربردی بوده که انواع و اقسام اطلاعات

★از کمیته علمی بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول.
آدرس‌های رایانامه: abouzar_arab@itrc.ac.ir (ابوذر عرب سرخی)، tafazoli@itrc.ac.ir (طلا تفضلی)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

فردی و سازمانی را به اقصی نقاط دنیا مخابره می‌کنند. در چنین شرایطی، اطلاعات و داده‌ها به مؤلفه سازنده و رکن اساسی جوامع و کسب و کارها تبدیل می‌شوند. با افزایش ارزش داده‌ها ما شاهد بروز و ظهور انواع تهدیدات و سوء استفاده‌ها حول آن‌ها هستیم؛ تهدیداتی که می‌توانند زمینه‌ساز بروز بحران‌های فردی یا حتی اجتماعی شوند [۱].

در این راستا، بسیاری از کشورها و اتحادیه‌های منطقه‌ای و بین‌المللی نسبت به تدوین مقررات حفاظت از داده‌های عمومی (GDPR) برای صیانت از حریم خصوصی افراد و شهروندان اقدام نموده‌اند. در حال حاضر، مجوز فعالیت عرضه‌کنندگان خدمات (مخابراتی، سلامت، حمل و نقل، آموزشی و ...) در بسیاری از کشورهای جهان تنها با رعایت این الزامات صادر و یا تمدید خواهد شد و در صورت بروز تخلف در زمینه نقض الزامات حفاظت از داده‌های عمومی، جرائم سنگینی پیرامون فرد یا نهاد متخلف اعمال می‌شود.

به عنوان مثالی از حفظ حریم خصوصی، به نتایج مطالعه‌ای اشاره می‌نماییم که توسط بهولا و همکارانش [۲] در خصوص تحلیل مقررات هشدار کوکی‌ها بر روی ۹۷۰۰۰ وب‌سایت اروپایی صورت گرفته است. گزارش این مطالعات درباره تخطی بالقوه از قانون GDPR می‌باشد. بر اساس نتایج بدست آمده از این مقاله، ٪۶۵/۴ از وب‌سایت‌ها به رضایت منفی کاربران احترام نمی‌گذارند و وب‌سایتهای با رتبه بالاتر انتخاب کاربر را بیشتر نادیده می‌گیرند اگر چه هشدار کوکی بیشتری دارند.

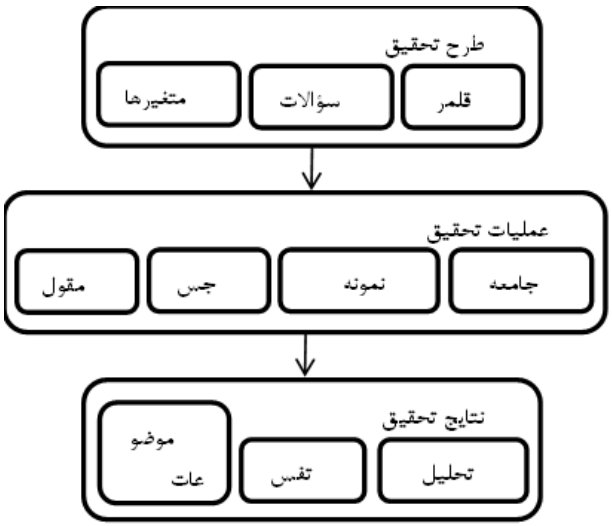
بر این اساس، در تحقیق حاضر مؤلفین به دنبال آن هستند تا ضمن بیان مختصر مفاهیم اصلی مرتبط با مقررات حفاظت از داده‌های عمومی، نسبت به بررسی و تحلیل تجارب سایر کشورها و متغیرهای اصلی تصمیم آنها در این حوزه –در قالب تحلیل موضوعات راهبردی– اقدام نمایند.

در بخش ۲، چارچوب تحقیق ارائه می‌شود. در بخش ۳، حفاظت از داده و چارچوب و مضامین آن مورد بررسی قرار می‌گیرد. در بخش ۴ وضعیت و شرایط و مقررات حفاظت از داده‌های عمومی ارائه می‌شود. بخش ۵ یافته‌های تحقیق است. در بخش ۶ برخی از چالش‌های پیاده‌سازی GDPR بررسی می‌شود و بخش ۷ جمع‌بندی و نتیجه‌گیری است.

## ۲ چارچوب تحقیق

### ۱.۲ ضرورت انجام تحقیق

بدون داشتن درک و آگاهی پیرامون راهبردها و موضوعات راهبردی سازنده قوانین و مقررات حفاظت از داده‌ها در کشورهای توسعه‌یافته و در حال توسعه (نظیر جمهوری اسلامی ایران) احتمال عدم آدرس‌دهی به موضوعات مهم و چالش‌برانگیز و تحمیل هزینه‌های فرصت به تصمیم‌سازان این حوزه در کشور افزایش می‌یابد. بنابر این نیاز است تا ملاحظات و موضوعات راهبردی حفاظت از داده مبتنی بر تحلیل اقدامات و برنامه‌های سایر کشورها و به روش‌های موجود شناسایی و آدرس‌دهی شوند.




**شکل ۱.** چارچوب پیشبرد تحقیق

### ۲.۲ سؤالات تحقیق

براساس مجموعه موارد مطرح شده، سؤال اصلی این پژوهش عبارتست از:

- موضوعات راهبردی جهت توسعه قوانین و مقررات حفاظت از داده‌ها کدامند؟

پاسخ به سؤال فوق مستلزم پاسخگویی به سؤالات فرعی زیر است:

- متغیرهای تصمیم راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشور کدام است؟
- اهمیت و فرکانس هریک از موضوعات و متغیرهای تصمیم راهبردی شناسایی‌شده به چه میزان است؟

### ۳.۲ کلیات و مراحل انجام تحقیق

مؤلفین در راستای ارائه شناسایی موضوعات راهبردی موضوع قوانین و مقررات حفاظت از داده‌ها نسبت به بررسی مقایسه‌ای اسناد ملی و بخشی و مقالات و استانداردهای مرجع این حوزه به روشی نظام‌مند اقدام نموده‌اند. این چارچوب در قالب شکل ۱ ارائه شده است [۳].

در گام اول و براساس جهت‌گیری تحقیق حاضر، مؤلفین به بیان سئوالات و متغیرهای تحقیق می‌پردازند. لازم به ذکر است که متغیرهای تحقیق حاضر همان موضوعات راهبردی و متغیرهای تصمیم در حوزه قوانین و مقررات حفاظت از داده‌ها در اسناد مرجع و کشورهای مختلف جهان است. در گام دوم تحقیق، تعیین جامعه آماری، نمونه‌گیری (بر اساس روش‌های نمونه‌گیری هدفمند)، جستجوی هدفمند (بر اساس کلمه‌ها، عبارت‌ها و مضامین معرف موضوعات راهبردی مدنظر) و نیز مقوله‌بندی (بر اساس دستورالعمل کُدگذاری دو مرحله‌ای باز) در دستورکار محقق قرار می‌گیرد. در گام سوم، مؤلفین نسبت به ارائه سیاهه‌ای از موضوعات راهبردی (براساس مقوله‌بندی برخواسته از داده) و نیز تحلیل و تفسیر

یافته‌ها (براساس تحلیل فراوانی موضوعات راهبردی و نیز بررسی‌های مقایسه‌ای) می‌پردازند.

در این پژوهش از روش تحلیل محتوی کیفی استفاده شده‌است که یکی از روش‌های انجام پژوهش کیفی است. تحلیل محتوی کیفی را می‌توان روش تحقیقی برای تفسیر ذهنی محتوایی داده‌های متنی –از طریق فرایندهای طبقه‌بندی نظام‌مند و بازنمایی دسته‌ها یا الگوهای شناخته‌شده– دانست [۳]. این امر مبنای شناسایی و تعریف موضوعات راهبردی در حوزه قوانین و مقررات حفاظت از داده‌ها است.

مؤلفین برای غنابخشی به یافته‌های تحقیق از مجموعه‌ای از روش‌ها و تکنیک‌های تحقیق در مرحله سوم (ارائه و گزارش‌دهی) استفاده نموده‌اند. در این گام و برای تحلیل یافته‌های تحقیق –مبتنی بر موضوعات راهبردی شناسایی‌شده– از تکنیک‌های بررسی درون موردی و بین موردی و نیز بررسی مقایسه‌ای موضوعات راهبردی استفاده شده‌است [۳].

جامعه آماری تحقیق حاضر متشکل از استانداردهای مرجع، مقالات معتبر و گزارش‌های ملی و بخشی منتشرشده در زمینه قوانین و مقررات حفاظت از داده‌ها است. مؤلفین برای تأمین جامعیت تحقیق حاضر نسبت به انتخاب هدفمند اسناد فوق اقدام نموده‌اند؛ به گونه‌ای که کلیه اسناد مشتمل بر ۳۸ نمونه موردی دسترس‌پذیر تا سال ۲۰۲۲ در قالب روش سرشماری، جمع‌آوری و مورد مطالعه و تحلیل عمیق (مبتنی بر روش‌ها تحلیل کیفی و تحلیل تِم) قرار گرفته‌اند.

## ۳ حفاظت از داده: مضامین و ابعاد

### ۱.۳ حریم خصوصی و حفاظت از داده‌های شخصی

«حریم خصوصی» به توانایی فرد یا گروهی اشاره دارد که می‌تواند خود یا اطلاعاتی را در مورد خود حفظ نماید و از این طریق اطلاعات خود را به هر صورتی که مایل باشد، بیان کند [۴]. زمانی که موضوعی برای شخص (یا اشخاصی) ماهیتی خصوصی دارد، معمولاً بدان معنی است که آن موضوع به‌طور ذاتی خاص یا حساس برای وی (آن‌ها) است [۴]. دامنه حریم خصوصی تا حدودی با امنیت هم‌پوشانی دارد؛ به طوری که می‌تواند مفاهیم استفاده مناسب و نیز حفاظت از اطلاعات را نیز در بر گیرد. عدم نقض غیرقانونی حریم خصوصی توسط دولت‌ها، شرکت‌ها و یا افراد بخشی از قوانین حفظ حریم خصوصی در بسیاری از کشورها است [۵] و در برخی موارد، در قانون اساسی کشورها نیز آمده است و چون این قوانین ذیل حقوق بشر تعریف می‌گردند، معمولاً قوانین سخت گیرانه‌ای نیز به شمار می‌آیند [۶].

### ۲.۳ اهداف حفاظت از داده‌های عمومی

برای حفاظت از داده‌ها سه هدف اصلی را می‌توان متصور بود [۷]:

(۱) ارائه و تدوین آیین‌نامه و قوانینی برای حمایت از اشخاص حقیقی در رابطه با پردازش داده‌های شخصی و نیز قوانینی در خصوص حرکت آزاد داده‌های شخصی.

(۲) حمایت از حقوق و آزادی‌های اساسی اشخاص حقیقی به‌ویژه در حوزهٔ حمایت از داده‌های شخصی آن‌ها.

(۳) کمک به نقل و انتقال آزاد اطلاعات شخصی بدون محدودیت و با رعایت مباحث مرتبط با حمایت از اشخاص حقیقی و نیز توجه به پردازش داده‌های شخصی.

باید به این موضوع توجه داشت که ساز و کارهای متنوعی برای این موضوع در کشورهای مختلف به کار گرفته شده است که بخشی از آن‌ها معرف خروجی‌های متنوع و کاربردی شده در سطح آزمایشگاه‌های معتبر و آکادمیک بوده است که می‌تواند در شناسایی راهکارها و فناوری‌های لازم برای حفاظت از داده‌های عمومی بسیار مؤثر باشند.

### ۳.۳ چارچوب مفاهیم مرتبط با حفاظت از داده‌ها

یکی از پیش‌نیازهای ضروری جهت ورود به مسئله حفاظت از داده‌ها، شناخت مفاهیم پایه و مرتبط است. بنابراین در این بخش از تحقیق به تبیین مفاهیم کلیدی در خصوص حفاظت داده‌ها پرداخته خواهد شد. شکل ۲ نمایی از چارچوب مفاهیم کلیدی در حوزه حفاظت داده را به تصویر کشیده است.

از بین مفاهیم مندرج در شکل یک تعدادی از آنها دارای اهمیت و جایگاه ویژه‌ای در حوزه حفاظت از داده هستند که در ادامه به بررسی آنها پرداخته خواهد شد.

**اطلاعات شخصی:** «داده‌های شخصی» به معنای هرگونه اطلاعات مربوط به یک شخصِ مشخص یا قابل شناسایی (موضوع داده) است [۸]. شخص حقیقی قابل شناسایی معرف فردی است که می‌تواند به طور مستقیم یا غیرمستقیم، به ویژه با مراجعه به شناسه‌ای –نظیر نام، شماره شناسایی، داده‌های مکانی، شناسه آنلاین یا یک یا چند عامل خاص جسمی یا فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی– مربوط به خود را احراز هویت نماید.

**پردازش:** پردازش به معنای مجموعه‌ای از عملیات است که بر روی داده‌های شخصی انجام می‌شود. جمع‌آوری، ضبط، سازماندهی، ساختاردهی، ذخیره‌سازی، سازگاری یا تغییر، بازیابی، نتیجه‌گیری، استفاده، افشاء از طریق انتقال، انتشار، تراز یا ترکیب، ایجاد محدودیت، پاک کردن و یا از بین بردن از عمده عملیات رایج پردازشی محسوب می‌شوند.

**کنترل‌کننده:** این مفهوم به معنای شخص حقیقی یا حقوقی، مرجع عمومی، سازمان یا یک نهاد دیگر است که به تنهایی یا به طور مشترک با دیگران، اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کند. در مواردی که اهداف و وسایل پردازش بر اساس قانون کشور تعیین شده باشد، لازم است کنترل‌کننده خود را با معیارهای مشخص شده تطبیق دهد [۹].

**شکل ۲.** چارچوب مفاهیم کلیدی در حوزه حفاظت از داده

**پردازش‌گر:** این مفهوم به معنای یک شخص حقیقی یا حقوقی، مقامات دولتی، سازمان یا یک نهاد دیگر است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند [۹].

**رضایت:** رضایت از موضوع داده‌ها به معنای هرگونه نشان دادن آزادانه و آگاهانه و بدون ابهام در مورد استفاده از داده‌ها است که توسط فرد با یک بیانیه یا با امضای یک تأییدیهٔ روشن، توافقی را برای پردازش داده‌های شخصی فرد ایجاد می‌کند.

**موضوع داده:** موضوع داده به هر فرد مشخصی اطلاق می‌شود که به طور مستقیم یا غیرمستقیم از طریق یک شناسه –نظیر نام، شماره شناسنامه، داده‌های محل یا از طریق فاکتورهای اختصاصی جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و یا هویت اجتماعی– شناسایی می‌شود [۱۰]. موضوع و افراد داده می‌توانند مشتریان، پیمانکاران، فروشندگان و حتی کارمندان یک سازمان باشند.

**بهره‌گیری مشروع از داده:** یکی از مفاهیم اساسی در پردازش داده‌ها، بهره‌برداری مشروع است که در بسیاری از موارد با ابهام مواجه می‌شود. برای این منظور در اینجا توضیح داده می‌شود که پردازش داده‌های فرد فقط در صورتی مجاز است که حداقل یکی از موارد زیر اعمال شود:

(۱) موضوع داده به پردازش اطلاعات شخصی خود برای یک یا چند هدف خاص رضایت داده باشد.
(۲) پردازش داده‌های فرد برای انجام امور قراردادی و یا پیمانکاری که سوابق داده‌ها در آن اهمیت دارد و یا برای انجام مراحل قبل از ورود به قرارداد لازم باشد.
(۳) پردازش داده‌ها برای سنجش رعایت تعهد قانونی ضروری باشد.
(۴) پردازش و بهره‌گیری از داده‌های فرد برای محافظت از منافع حیاتی وی و یا شخص حقیقی دیگری ضروری باشد.
(۵) پردازش و بهره‌گیری از داده‌ها برای انجام اموری که به نفع مردم باشد

و یا جزو وظایف رسمی کنترل‌کننده و بهره‌بردار باشد، ضروری است.

(۶) پردازش و بهره‌گیری از داده‌ها برای اهداف و منافع مشروعی که توسط کنترل‌کننده و بهره‌بردار و یا شخص ثالث دنبال می‌شود، ضروری باشد.

**زیرسکوهای نرم‌افزاری:** نرم‌افزارهای بکار رفته برای دسترسی به اینترنت یا ارائه خدمات مختلف به کاربران می‌باشند. این نرم‌افزارها ممکن است بومی یا غیربومی باشند.

## ۴ وضعیت و شرایط و مقررات حفاظت از داده‌های عمومی

### ۱.۴ نمایی از وضعیت ایران در حوزهٔ مقررات حفاظت از داده‌ها

در بسیاری از کشورها از جمله در ایران قوانین و مقررات خاصی برای حفاظت از اطلاعات و داده‌های فردی و عمومی تدوین، طراحی و ارائه شده است که لازمه اجرای آن ایجاد امکانات فناورانه در جهت پیشگیری، رصد و پایش و اقدام متناسب در حوزهٔ حفاظت از داده‌ها است. چنین شرایطی توجه تصمیم‌سازان و سیاست‌گزاران دولتی را بیش از پیش به موضوع حفاظت از داده‌ها معطوف داشته‌است و دولت‌ها نیز نقش مهمی در این روند ایفا خواهند کرد [۹]. در جدول ۱ به برخی از قوانین و مقررات حفاظت از داده در ایران اشاره شده است.

### ۲.۴ نمایی از وضعیت کشورهای مختلف در حوزهٔ مقررات حفاظت از داده‌ها

بررسی مجموعه راهبردها و موضوعات راهبردی کشورهای پیشرو و در حال توسعه و نیز استخراج اقدامات ضروری برای توسعه قوانین و مقررات در این حوزه ضروری به نظر می‌رسد تا از این طریق دید جامعی نسبت به آنچه که دولت‌ها درکشورهای مختلف انجام می‌دهند، به دست آید [۱۱]. البته مطالعه تجارب مفید و انتقال خط‌مشی‌ها و راهبردهای کاربردپذیر برای کشور صرفاً از طریق کپی‌برداری امکان‌پذیر نیست؛ چرا که اصول حاکم بر تصمیمات در سطح ملی و شرایط سیاسی، اقتصادی، اجتماعی و فناورانه از یک کشور به کشور دیگر متفاوت است. همین امر موجب گردیده تا کشورهای مختلف رویکردهای بعضاً متفاوتی را در مواجهه با این پدیده اتخاذ نمایند. در ادامه به بررسی سه نمونه منتخب از اقدامات کشورها در زمینه مقررات حفاظت از داده پرداخته خواهد شد.

#### ۱.۲.۴ ژاپن به‌عنوان نماینده آسیا

در سال ۲۰۰۳ بود که اولین قانون حفاظت از داده‌ها در ژاپن تحت عنوان قانون حفاظت از اطلاعات شخصی (APPI) تصویب شد. این قانون جزء نخستین مقررات حفاظت از داده‌ها در آسیا محسوب می‌شود. در سپتامبر ۲۰۱۵ و پس از افشای حجم بالایی از اطلاعات مشتریان ژاپنی، مشخص شد که الزامات APPI دیگر نیازهای امروز را برآورده نمی‌کنند. بر این اساس، برنامه اصلاح‌شده APPI در تاریخ ۳۰ مِی سال ۲۰۱۷ و یک سال پیش از مقررات حفاظت از داده‌های عمومی (GDPR) اتحادیه اروپا به اجرا در آمد [۱۲].

در تاریخ ۷ سپتامبر سال ۲۰۱۸، کمیسیون حفاظت از اطلاعات شخصی (PCC) ژاپن قوانینی را در مورد چگونگی پردازش داده‌های شخصی –برگرفته از مقررات اتحادیه اروپا– اعلام نمود. این قوانین هنگامی عملی می‌شوند که کمیسیون اروپا به‌طور رسمی تصویب کند که ژاپن از سطح کافی حفاظت از داده‌های شخصی –مطابق ماده (۴۵) از GDPR– برخوردار است [۱۲]. در این راستا، پنج تغییر اساسی در قانون حفاظت از اطلاعات شخصی (APPI) ژاپن انجام شد (رجوع به جدول ۲). این تغییرات با هدف تقویت مقررات حفظ حریم خصوصی داده‌ها در ژاپن –و همسویی با GDPR– در نظر گرفته شده است.

#### ۲.۲.۴ کانادا به‌عنوان نماینده آمریکای شمالی

کانادا مدت‌ها است که با تصویب «قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی» (PIPEDA) در اوایل سال ۲۰۰۰ در صدر کشورهای مدعی محافظت از داده‌ها قرار داشته است. این قانون اولیه براساس ۱۰ اصل مندرج در الگوی محافظت از اطلاعات شخصی تنظیم شده و مسئولیت‌پذیری، اخذ رضایت و محدودیت در جمع‌آوری داده‌ها را در بر می‌گیرد. امروزه، این اصول همچنین در آیین‌نامه حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) نیز دیده می‌شود [۱۳].

در PIPEDA به ۱۰ اصل اساسی حفاظت از داده‌ها اشاره شده است. در عین حال سازمان‌ها در هر زمان مسئولیت حفاظت از اطلاعات شخصی را بر عهده دارند و موظف هستند که اطمینان حاصل کنند که هر گونه جمع‌آوری، استفاده یا افشای اطلاعات شخصی فقط برای اهدافی انجام می‌شود که فرد –با توجه به شرایط موجود– آن را مناسب می‌داند. این اصول در جدول ۳ آمده است.

#### ۳.۲.۴ پارلمان اروپا به عنوان نماینده نهادی اروپا

مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) معرف مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده در اتحادیه اروپا و منطقه اقتصادی اروپا وضع شده است. هدف این مقررات اساساً اعطای کنترل داده‌ها به شهروندان و ساکنان این منطقه و ساده‌سازی محیط مقررات‌گذاری برای کسب‌وکارهای بین‌المللی از طریق یکسان‌سازی مقررات است [۹].

این مقررات جایگزین قانون حفاظت از داده اتحادیه اروپا (EC/46/95) شده است و شامل احکام و الزاماتی مرتبط با پردازش اطلاعات شخصی قابل تشخیص در اتحادیه اروپا می‌شود و در خصوص همه کسب و کارهایی مطرح می‌شود که با این منطقه اقتصادی مراوده کاری دارند (صرف‌نظر از مکان استقرارشان). بدین ترتیب، فرآیندهای کسب و کار که اطلاعات شخصی را اداره می‌کنند باید مبتنی بر «حفاظت اطلاعات از

**جدول ۱.** سیاهه‌ای از مهمترین قوانین و مقررات پیرامون حفاظت از داده در ایران

| ردیف | عنوان | موضوع کلیدی مطرح‌شده |
|---|---|---|
| ۱ | اصل بیست و پنجم قانون اساسی (۱۳۵۸) | دسترسی غیرمجاز به داده‌های شخصی مردم و نیز افشای آن را مدنظر قرار داده است. |
| ۲ | مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب شورای‌عالی انقلاب فرهنگی (۱۳۸۰) | وظایف ISPها که دربرگیرنده حریم‌خصوصی کاربران و تعیین جرایم افشاء است. |
| ۳ | قانون تجارت الکترونیکی (۱۳۸۲) | حمایت از داده پیام‌های شخصی را مدنظر قرار داده است. |
| ۴ | قانون جرائم رایانه‌ای (۱۳۸۸) | دسترسی غیرمجاز به اطلاعات را مدنظر قرار داده است. |
| ۵ | منشور حقوق شهروندی (۱۳۹۵) | بند ۱: تفکیک حریم عمومی از حریم‌خصوصی و نهادینه کردن خدمت در هر دو حریم را مدنظر قرار داده است که متاسفانه جزئیاتی پیرامون آن اشاره نشده است. |
| ۶ | قانون انتشار و دسترسی آزاد به اطلاعات | بند «ب» ماده ۱ قانون: اطلاعات شخصی معرف اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است. |
| ۷ | ماده ۱۳۰ قانون برنامه چهارم توسعه (۱۳۸۳) | لایحه «حفظ و ارتقاء حقوق شهروندی و حمایت از حریم‌خصوصی افراد، در راستای اجرای اصل بیستم (۲۰) قانون اساسی جمهوری اسلامی ایران» توسط قوه قضائیه تدوین می‌شود. |
| ۸ | قانون برنامه پنجم توسعه (۱۳۹۴-۱۳۹۰) | • تبصره ماده ۲۰۶: عدم افشاء اطلاعات، • بند الف ماده ۳۵: صیانت از اطلاعات پزشکی |
| ۹ | بند «ب» اساسنامه سازمان بیمه سلامت ایران | تشکیل و صیانت از پرونده الکترونیکی سلامت افراد مدنظر است. |
| ۱۰ | بند ۴ ماده ۱۲ دستورالعمل تشکیل بانک اطلاعات هویت ژنتیک ایران | دستورالعمل حفاظت از اطلاعات ژنتیکی در آزمایشگاه‌ها را مدنظر قرار داده‌است. |
| ۱۱ | مصوبه شورای‌عالی اداری در خصوص منشور حقوق شهروندی (۱۳۹۵) | تمهیدات فنی و قانونی لازم را برای حفظ حریم‌خصوصی افراد و تأمین امنیت داده‌های شخصی آنان توسط قوه قضائیه مدنظر قرار گیرد. |
| ۱۲ | لوایح وزارت اطلاعات و فناوری اطلاعات | • پیش نویس لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی (دی ماه ۱۳۹۶)، • پیش‌نویس صیانت و حفاظت از داده‌های شخصی» (تیرماه سال ۱۳۹۷) |

طریق طراحی و به طور پیش فرض» باشند؛ یعنی اطلاعات شخصی باید با استفاده از مستعارسازی یا بی‌نام‌سازی ذخیره شود و حداکثر محرمانگی به طور پیش‌فرض در نظر گرفته شود؛ به گونه‌ای که داده‌ها بدون رضایت صریح به طور عمومی در دسترس نباشد و بدون اطلاعات اضافی جداگانه برای تعیین هویت اشخاص قابل استفاده نباشد. بر این اساس هیچ‌گونه اطلاعات شخصی نمی‌تواند پردازش شود، مگر آنکه تحت مبنای قانونی که به وسیله مقررات مشخص‌شده، انجام شود یا آنکه کنترل‌کننده یا پردازنده داده‌ها اجازه صریح مختارانه صاحب داده‌ها را دریافت کرده باشد. صاحب داده‌ها می‌تواند در هر زمانی این اجازه را لغو کند [۹].

این قانون در ۱۴ آوریل ۲۰۱۶ وضع شد و بعد از سپری شدن دو سال به عنوان دوره گذار، از ۲۵ می ۲۰۱۸ به اجرا در آمد. اعمال این قانون نیازمند تصویب قانون جداگانه در کشورهای عضو اتحادیه نمی‌باشد و به طور خودکار در همه آن‌ها لازم‌الاجرا است.

### ۳.۴ نگاهی مقایسه‌گونه به قوانین و مقررات حفاظت از داده در ایران و نمونه‌های برتر خارجی

براساس موارد و اسناد بررسی‌شده در بندهای (۴-۱) و (۴-۲) این تحقیق و نیز بررسی‌های به عمل آمده پیرامون ۳۸ سند منتخب پیرامون قوانین و مقررات حفاظت از داده، مقررات حفاظت از داده‌های عمومی (GDPR) و قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی (PIPEDA) به عنوان دو مرجع اصلی و معتبر با مقررات حفاظت از داده موجود در جمهوری اسلامی ایران مورد قیاس قرار گرفته‌اند که نتایج حاصله در قالب جدول ۴ ارائه گردیده است.

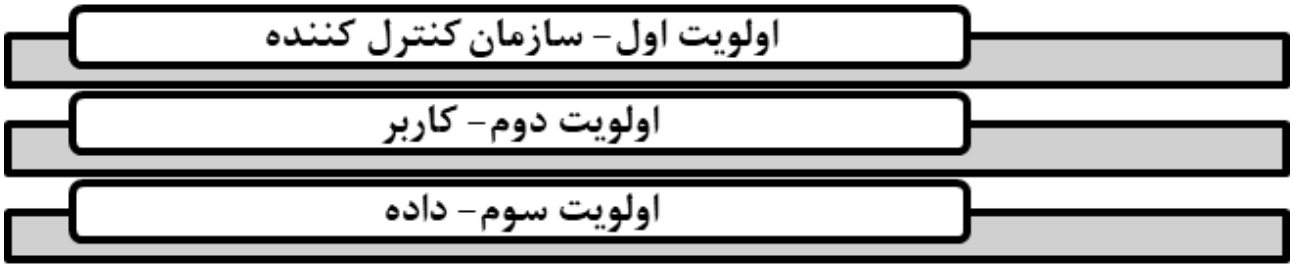
## ۵ یافته‌های تحقیق

پس از تعیین متن اسناد و مراجع تخصصی معتبر، محقق نسبت به مطالعه تطبیقی پیرامون موضوعات اصلی مرتبط با حفاظت از داده در سه محور داده، کاربران (موضوع داده) و سازمان‌ها (پردازش‌کنندگان) و کنترل‌کنندگان در سطح ۳۸ کشور منتخب اقدام نمود که نتیجه در قالب جدول ۵ ارائه شده است.

شایان ذکر است که مؤلفه‌های سازنده سه موضوع (داده، کاربران (موضوع داده) و سازمان‌ها (پردازش‌کنندگان) و کنترل‌کنندگان) حفاظت از داده بر اساس مطالعه عمیق منابع و مقوله‌بندی داده‌ها شناسایی که نتایج در قالب جدول ۶ ارائه شده است. همچنین با توجه به نتایج به دست آمده، اولویت و تمرکز موضوعات راهبردی –بر اساس مجموع فراوانی گزاره‌های راهبردی (مقوله‌ها) در اسناد– به ترتیب در قالب شکل ۳ به تصویر کشیده شده است.

**جدول ۲.** الزامات کمیسیون حفاظت از اطلاعات شخصی (PPC) در ژاپن

| موارد لازم‌الرعایه | قانون فعلی در ژاپن | قوانین تکمیلی PPC | مفاهیم عملی |
|---|---|---|---|
| دامنه اطلاعات شخصی که نیاز به بررسی دقیق دارند | اطلاعات مربوط به زندگی جنسی افراد، گرایش جنسی و عضویت در اتحادیه‌های کارگری به عنوان «اطلاعات شخصی حائز اهمیت» برای همسویی با «داده‌های شخصی حساس» که در تعریف GDPR آمده، تعریف شده است. | اطلاعات مربوط به زندگی جنسی موضوع داده‌های اتحادیه اروپا، گرایش جنسی و عضویت در اتحادیه های کارگری باید به عنوان «اطلاعات شخصی که نیاز به دقت لازم دارند» تلقی شوند تا از الزامات «داده‌های شخصی حساس» که تحت عنوان GDPR تعریف می‌شوند، پیروی نمایند. | جلب رضایت موضوع داده برای دستیابی به چنین اطلاعاتی لازم است. ارائه چنین داده‌هایی به شخص ثالث –با استفاده از ترتیبات امتناع– مطابق با قوانین ژاپن ممنوع است؛ یعنی برای این‌کار رضایت صریح لازم است. |
| اجازه دسترسی | در صورت حذف ظرف ۶ ماه دیگر موضوع داده حق دسترسی به اطلاعات شخصی خود را ندارند. در واقع آنها تنها حق دسترسی به داده‌های شخصی را دارند که ظرف مدت ۶ ماه حذف نمی‌شوند. | شرکت‌ها موظفند اطلاعات شخصی که به آنها داده شده است را بنا به درخواست موضوع داده اتحادیه اروپا –بدون در نظر گرفتن مدت زمان نگهداری این داده‌ها– افشاء نمایند. | شرکت‌هایی که داده‌های شخصی را از ساکنان اتحادیه اروپا جمع‌آوری می‌کنند و این داده‌ها را برای دوره‌های زمانی حفظ می‌کنند باید به درخواست‌های افشاء موضوع داده عمل نمایند. |
| جانشینی هدف استفاده | هیچ قانون مشخصی وجود ندارد. | اطلاعات شخصی موضوع داده‌های اتحادیه اروپا که از شخص ثالث دریافت می‌شود، فقط مطابق با هدفی که در ابتدا مبنای جمع‌آوری بوده است باید مورد استفاده قرار گیرد. | شرکت‌ها نیاز دارند تا اهدافی را که در ابتدای جمع‌آوری داده‌های شخصی ساکنان اتحادیه اروپا به دست آمده بود، تأیید و ردیابی کنند. بنابراین باید استفاده از این داده‌های شخصی را محدود نمایند. ردیابی مناسب و بجا که استفاده‌های مجاز از مجموعه داده‌های مختلف را میسر می‌سازد بسیار چالش برانگیز است و باید به دقت پایش شوند. |
| انتقال مجدد داده‌های شخصی افراد اتحادیه اروپا از ژاپن به کشورهای خارجی | زمانی مجاز است که: ۱) رضایت موضوع داده جلب شود. ۲) اقدامات کافی برای تامین امنیت داده‌ها بین انتقال‌دهنده و تحویل گیرنده انجام شده باشد. ۳) تحویل‌گیرنده در یک کشور خارجی است که توسط PPC تعیین شده است. | موارد (۱) و (۲) همچنان ادامه دارد. با توجه به مورد (۳)، حفاظت براساس ضوابط ژاپن باید بین انتقال‌دهنده و تحویل‌گیرنده از طریق قرارداد تأمین شود. | قانون فعلی ژاپن درباره مورد (۲) مشخص نیست. البته قوانین تکمیلی روشن می‌کند که قرارداد با تحویل‌گیرنده طرف ثالث الزامی است، مگر اینکه رضایت موضوع داده اتحادیه اروپا اخذ شود؛ یا اینکه تحویل‌گیرنده در یک لیست سفید قرار دارد که توسط PPC تعیین شده است. |
| اطلاعات پردازش‌شده ناشناس (که از حمایت خاصی برخوردار نیست و معاف است) | برخی از داده‌ها ممکن است به عنوان «اطلاعات پردازش‌شده ناشناس» استفاده شوند، حتی اگر اطلاعات لازم برای شناسایی موضوع داده‌ها به صورت جداگانه نگه داشته شوند. | برای استفاده از داده‌ها به عنوان «اطلاعات پردازش‌شده ناشناس» باید بخشی از اطلاعات با روش گمنام‌سازی حذف شوند. | براساس معافیت قانونی ژاپن، شرکت‌ها باید اطمینان حاصل نمایند که اطلاعات مربوط به روند گمنام‌سازی حذف شده‌اند. |




**شکل ۳.** اولویت و تمرکز موضوعات راهبردی در اسناد مرجع و معتبر مطالعه‌شده

**جدول ۳.** اصول دهگانهٔ PIPEDA

| اصل | توضیحات |
|---|---|
| مسئولیت‌پذیری | یک سازمان مسئول اطلاعات شخصی تحت کنترل خود است و باید برای حصول اطمینان از پیروی از PIPEDA، یک افسر حفظ حریم خصوصی را استخدام کند. |
| شناسایی اهداف | سازمان‌ها باید اهدافی را شناسایی کنند که برای جمع‌آوری داده‌های شخصی آن‌ها اقدام می‌کنند. |
| رضایت | رضایت افراد برای جمع‌آوری، استفاده یا افشای اطلاعات شخصی مورد نیاز است. برخی از معافیت‌ها در مورد این اصل اعمال می‌شود. به عنوان مثال در مواردی که دلایل قانونی، پزشکی یا امنیتی مطرح است ممکن است اخذ رضایت غیرممکن یا غیرعملی باشد. |
| محدودیت سازمان | اطلاعات باید با استفاده از روش‌های منصفانه و قانونی جمع‌آوری شوند و فقط به داده‌های مورد نیاز برای هدف مشخص‌شده توسط سازمان محدود شود. |
| محدودیت استفاده، افشاء و نگهداری اطلاعات | اطلاعات شخصی فقط برای اهدافی که برای آن جمع‌آوری شده است می‌تواند مورد استفاده یا افشاء قرار گیرد و باید صرفاً برای مدت زمان مورد نیاز برای انجام این اهداف نگه داشته شود، مگر اینکه فرد رضایت داده یا به صورتی قانونی مجاز باشد. |
| دقت | اطلاعات شخصی باید تا حد امکان دقیق، کامل و به‌روز باشد تا به درستی اهداف استفاده را برآورده سازد. |
| محافظت | اطلاعات شخصی باید از طریق ضمانت امنیتی مناسب در برابر از دست دادن یا سرقت و همچنین دسترسی غیرمجاز، افشاء، کپی، استفاده و یا اصلاح محافظت شوند. |
| صراحت | سازمان‌ها باید در مورد سیاست‌ها و شیوه‌های مربوط به مدیریت داده‌های شخصی آزاد باشند و اطمینان حاصل کنند که چنین اطلاعاتی به‌راحتی در قالب کاملاً قابل فهم در دسترس افراد قرار می‌گیرد. |
| دسترسی فردی | در صورت درخواست فرد باید از وجود، استفاده و افشای اطلاعات شخصی خود مطلع شده و به آن دسترسی پیدا کند. اشخاص حق دارند صحت و کامل بودن اطلاعات را به چالش کشیده و در صورت لزوم اصلاح کنند. |
| چالش انطباق PIPEDA | فرد می‌تواند انطباق یک سازمان با اصول PIPEDA را به چالش کشیده و چالش خود را به مسئول امور حفظ حریم خصوصی شرکت –که مسئولیت انطباق با PIPEDA را بر عهده دارد– ارایه کند. |

**جدول ۴.** مقایسه قوانین و مقررات حفاظت از داده ایران و سایر نمونه‌های برتر جهانی

| اصل یا موضوع | GDPR | PIPEDA | ایران |
|---|---|---|---|
| مسئولیت‌پذیری | × | × | × |
| شناسایی اهداف | × | × | |
| رضایت | × | × | |
| محدودیت سازمان | × | × | |
| دقت | × | × | |
| به حداقل رساندن داده‌ها | × | × | |
| محافظت | | × | |
| دسترسی فردی | | | × |
| صیانت از حیثیت و کرامت اشخاص | | | × |
| هم‌افزایی امور تنظیمی | | | × |
| جبران‌پذیری زیان‌ها و آسیب‌های پردازش | | | |
| قانونی بودن، انصاف و شفافیت | × | | |
| صداقت و محرمانگی (امنیت) | × | | |

## ۶ برخی از چالش‌های پیاده‌سازی GDPR

در این بخش به برخی از چالش‌های پیاده‌سازی GDPR اشاره می‌نماییم [۱۴]. برخی از آنها به شرح ذیل هستند:

- در GDPR راهنماهای خاصی در رابطه با فناوری‌هایی که برای رعایت کردن نیازمندی‌هایش لازم است، ارائه نشده است [۱۵].
- PGDPR راهنماهای خاصی را برای پیاده‌سازی این قوانین ارائه ننموده است [۱۶].
- اجرای قانون GDPR ممکن است گران و زمان‌بر باشد زیرا که نیازمند منابع انسانی و مالی است [۱۷].
- قانون‌گذاری GDPR حجم کارهای مدیریتی را افزایش می‌دهد [۱۸].
- عدم وجود دانش و تجربه در زمینه حریم خصوصی در سطح سازمان‌ها ممکن است نیازمند بودجه اضافه باشد تا متخصصین حریم خصوصی استخدام شوند و هزینه کسب و کار افزایش می‌یابد [۱۹].

## ۷ جمع بندی و نتیجه‌گیری

بر اساس مطالعاتی که در این پژوهش صورت گرفت، به نظر می‌رسد که لزوم تدوین یك چارچوب جامع برای حفظ داده‌های موجود در فضای مجازی کشور، با توجه به افزایش روزافزون ضریب نفوذ اینترنت در جامعه، بیش از پیش احساس می‌شود و لازم است کشور هر چه سریعتر به یك توافق فراگیر و قانون جامع در این زمینه دست پیدا کند.

برای دستیابی به جامعیت حفاظت از داده ها، موضوعات راهبردی و متغیرهای تصمیم مختلفی درکشورهای مختلف مورد توجه واقع شده است. با توجه به بررسی کشورهای مختلف، مهمترین موضوعات مورد توجه در کشورهای مختلف در قالب یک چارچوب مرجع دسته‌بندی شده است که در قالب شکل ۳ ارائه گردیده است. همانطور که مشاهده می‌شود نتایج برآمده از تحلیل اسناد، به سه موضوع راهبردی بنیادی برای سیاست‌گذاری

**جدول ۵.** مهمترین موضوعات کلیدی حفاظت از داده مورد توجه در کشورهای مختلف جهان

| ردیف | کشور | داده‌ها | کاربران | سازمان‌ها و کنترل‌کنندگان | مجموع موضوعات مورد توجه |
|---|---|---|---|---|---|
| ۱ | کره جنوبی | ۱۰ | ۹ | ۱۰ | ۲۹ |
| ۲ | سنگاپور | ۱۰ | ۸ | ۱۰ | ۲۸ |
| ۳ | تایوان | ۱۲ | ۱۰ | ۹ | ۳۱ |
| ۴ | اسپانیا | ۳ | ۹ | ۱۰ | ۲۲ |
| ۵ | نیجریه | ۱۲ | ۹ | ۹ | ۳۰ |
| ۶ | ژاپن | ۱۱ | ۱۰ | ۹ | ۳۰ |
| ۷ | فیلیپین | ۱۲ | ۷ | ۱۰ | ۲۹ |
| ۸ | هند | ۱۲ | ۹ | ۹ | ۳۰ |
| ۹ | اندونزی | ۱۰ | ۷ | ۹ | ۲۶ |
| ۱۰ | نیوزیلند | ۹ | ۶ | ۱۰ | ۲۵ |
| ۱۱ | ایالات متحده امریکا | ۱۲ | ۱۰ | ۹ | ۳۱ |
| ۱۲ | سوئد | ۹ | ۷ | ۱۰ | ۲۶ |
| ۱۳ | کنیا | ۱۲ | ۸ | ۱۰ | ۳۰ |
| ۱۴ | افریقای جنوبی | ۱۲ | ۷ | ۹ | ۲۸ |
| ۱۵ | آرژانتین | ۱۲ | ۶ | ۹ | ۲۷ |
| ۱۶ | اوکراین | ۱۲ | ۸ | ۸ | ۲۸ |
| ۱۷ | استرالیا | ۱۱ | ۱۰ | ۸ | ۲۸ |
| ۱۸ | مکزیک | ۰ | ۵ | ۹ | ۱۴ |
| ۱۹ | آلمان | ۱۲ | ۸ | ۹ | ۲۹ |
| ۲۰ | تایلند | ۰ | ۷ | ۸ | ۱۵ |
| ۲۱ | کلمبیا | ۱۱ | ۷ | ۷ | ۲۵ |
| ۲۲ | قزاقستان | ۳ | ۶ | ۶ | ۱۵ |
| ۲۳ | چین | ۱۱ | ۶ | ۷ | ۲۴ |
| ۲۴ | مالزی | ۱۲ | ۶ | ۷ | ۲۵ |
| ۲۵ | روسیه | ۱۲ | ۸ | ۵ | ۲۵ |
| ۲۶ | انگلستان | ۱ | ۷ | ۶ | ۱۴ |
| ۲۷ | هنگ کنگ | ۱۲ | ۵ | ۶ | ۲۳ |
| ۲۸ | زیمباوه | ۱۲ | ۴ | ۶ | ۲۲ |
| ۲۹ | فرانسه | ۱۱ | ۸ | ۱۰ | ۲۹ |
| ۳۰ | ویتنام | ۱۲ | ۳ | ۳ | ۱۸ |
| ۳۱ | مغولستان | ۱۲ | ۲ | ۳ | ۱۷ |
| ۳۲ | کانادا | ۱۲ | ۱۰ | ۱۰ | ۳۲ |
| ۳۳ | نروژ | ۱۰ | ۸ | ۱۰ | ۲۸ |
| ۳۴ | کامبوچ | ۱۲ | ۱ | ۰ | ۱۳ |
| ۳۵ | مصر | ۰ | ۱ | ۱ | ۲ |
| ۳۶ | میانمار | ۱۰ | ۰ | ۰ | ۱۰ |
| ۳۷ | سریلانکا | ۵ | ۰ | ۰ | ۵ |

**جدول ۶.** مقوله‌بندی و تبیین موضوعات راهبردی در حوزه مقررات

| داده | | | | | | | | | | | کاربر | | | | | | | | | | سازمان کنترل کننده | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| جمع‌آوری و اصلاح | استفاده و افشای داده | نگهداری و از بین بردن داده‌ها | حفظ امنیت داده‌ها | اعلان نقض در اطلاعات | انتقال اطلاعات | باز بودن داده‌ها | حفظ کیفیت اطلاعات | محدودیت پردازش و استفاده | محدودیت در جمع‌آوری داده | مشخص بودن هدف از جمع‌آوری داده‌ها | محدودیت در پردازش اضافه‌تر | حق تعریف اطلاعات و داده‌های شخصی | حق حفظ حریم خصوصی آنلاین | حق تعریف داده‌های حساس | حق اعلام جمع‌آوری | حق درخواست دسترسی | حق فراموش شدن | حق درخواست تعلیق پردازش | حق حمل و نقل داده‌ها | حق اعلان نقض اطلاعات | حق انتقال اطلاعات | مأمور محافظت از داده | مسئولیت‌پذیری | محدودیت پردازش و استفاده | عدم جمع آوری بیش از توافق اولیه | عدم پردازش بیش از توافق اولیه | مشخص نمودن هدف از پردازش | باز بودن داده‌ها | حفظ کیفیت اطلاعات | الزام مسئول حفظ داده‌ها | مشارکت دادن و ایجاد دسترسی برای موضوع داده | انجام اقدامات امنیتی و استفاده از شخص ثالث | اعلام تغییر در داده های جمع آوری شده | حفظ محدودیت‌های انتقال داده‌های مرزی | عدم استفاده در بازاریابی مستقیم | حفظ حریم خصوصی آنلاین | پردازش اطلاعات شخصی حساس |

منتج شد که ملاحظات سیاست‌گذاران و نیز اقتضائات و نیازهای توسعه قوانین و مقررات حفاظت از داده‌های عمومی در کشورهای مختلف را پوشش می‌دهد.

## مراجع

[1] Labadie, Clément and Legner, Christine. Building data management capabilities to address data protection regulations: Learnings from eu-gdpr. *Journal of Information Technology*, 38(1):16–44, 2023.

[2] Bouhoula, Ahmed, Kubicek, Karel, Zac, Amit, Cotrini, Carlos, and Basin, David. Automated {Large-Scale} analysis of cookie notice compliance. in *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 1723–1739, 2024.

[3] Shejy, Geocey. Data privacy and security in social networks. *Principles of Social Networking: The New Horizon and Emerging Challenges*, pp. 387–411, 2022.

[4] Tamburri, Damian A. Design principles for the general data protection regulation (gdpr): A formal concept analysis and its evaluation. *Information Systems*, 91:101469, 2020.

[5] Slepchuk, Alec N and Milne, George R. Informing the design of better privacy policies. *Current Opinion in Psychology*, 31:89–93, 2020.

[6] Zainab, Syeda Sana e and Kechadi, Tahar. Sensitive and private data analysis: A systematic review. in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pp. 1–11, 2019.

[7] Purtova, Nadezhda. The law of everything. broad concept of personal data and future of eu data protection law. *Law, Innovation and Technology*, 10(1):40–81, 2018.

[8] Clarke, Roger. Privacy impact assessment: Its origins and development. *Computer law & security review*, 25(2):123–135, 2009.

[9] Commission, European. Special Eurobarometer 423 Cyber Security. tech. rep., European Commission, 2015.

[10] Markos, Ereni, Milne, George R, and Peltier, James W. Information sensitivity and willingness to provide continua: a comparative privacy study of the united states and brazil. *Journal of Public Policy & Marketing*, 36(1):79–96, 2017.

[11] Gauthier, Chassang. The impact of the eu general data protection regulation on scientific research. *ecancermedicalscience*, 11, 2017.

[12] Data protection in japan to align with gdpr. https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr. September 24, 2018.

[13] H.-. F. H. &. S. E. Shanon. Three approaches to content analysis.

[14] Zaguir, Nemer A, Magalhães, Guilherme H, and Spinola, Mauro M. Challenges and enablers for gdpr compliance: systematic literature review and future research directions. *IEEE Access*, 2024.

[15] Tikkinen-Piri, Christina, Rohunen, Anna, and Markkula, Jouni. Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153, 2018.

[16] Agarwal, Sushant. Towards dealing with gdpr uncertainty. *IFIP Summer School*, pp. 1–7, 2016.

[17] Tikkinen-Piri, Christina, Rohunen, Anna, and Markkula, Jouni. Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153, 2018.

[18] Magnusson, Lars and Iqbal, Sarfraz. Implications of eu-gdpr in low-grade social, activist and ngo settings. *International Journal of Business and Technology*, 6(3):1–7, 2018.

[19] Lindgren, Peter. Gdpr regulation impact on different business models and businesses. *Journal of Multi Business Model Innovation and Technology*, 4(3):241–254, 2016.

*MonadiAfta*-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 2 (pp. 12–23)
https://monadi.isc.org.ir

Presented at the ISCISC 2024 in Tarbiat Modares University & Research Institute for Information and Communication Technology, Tehran, Iran

# Analysis of strategic issues in the field of general data protection regulations★

Abouzar ArabSorkhi * and Tala Tafazoli

*ICT Research Institute, Tehran, Iran*

**ARTICLE INFO.**

*Keywords:*
Data protection
Strategic issues
General data protection regulations
Content analysis

**Type:** Research paper

**ABSTRACT**

One of the most important issues in information technology era is data protection; If this issue is not considered, confidence and usability and extension of information and communication technology will be threatened. In this way, politiceans and decision makers in organizations, industry and governments want to regulate the information and communication era. This regularization is performed based on decision making considerations and variables, while forgetting them may rise challenges and cause crisis. In management sciences they are called strategic issues. Current research identifies, defines, and analyzes strategic issues that different goverments, use them to reinfornce information governance structures like maintenance and governance of data and information security. These strategic issues are in the range of national documents, reference standards and documentation related to general data protection regulations (GDPR). In this research, we investigate documents and references related to data protection regulations using content analysis, to identify strategic issues.

© 2024 ISC

★ The ISCISC 2024 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: abouzar_arab@itrc.ac.ir (Abouzar ArabSorkhi), tafazoli@itrc.ac.ir (Tala Tafazoli)
© 2024 ISC. All rights reserved.