تحلیل راهبردی اقدامات مقررات حفاظت از داده‌های عمومی (ارائه چارچوب مفهومی اقدامات کلان حفاظت از داده در کشور)

رحیم خانی زاد[۱]، ابوذر عرب سرخی[۲]

[۱] استادیار، دانشگاه علم و صنعت ایران، تهران
khanizad@iust.ac.ir
[۲] استادیار، پژوهشگاه فناوری اطلاعات و ارتباطات، تهران
abouzar_arab@itrc.ac.ir

چکیده

توسعه روزافزون فناوری‌های اطلاعاتی و رشد صعودی دارایی‌های اطلاعاتی منتشر شده در فضای سایبر علاوه بر ایجاد فرصت‌های بزرگ برای استفاده از آن در حوزه‌های مختلف، موجب بروز تهدیدات امنیتی متنوع و متفاوتی از سمت بازیگران مختلف هم در فضای فردی و هم در ابعاد اجتماعی، ملی و بین‌المللی شده است. کشور ایران نیز به دلیل موقعیت خاصی که در منطقه و جهان دارد، از لحاظ بین‌المللی نیز در معرض خطرات و تهدیدات اطلاعاتی خاص خود قرار گرفته است و در این شرایط نیازمند تقویت ساختارهای حکمرانی اطلاعاتی از جنس حفظ و مدیریت امنیت داده‌ها و اطلاعات کشور در این حوزه است. از این رو در مقاله حاضر مؤلف به دنبال آن است تا ضمن مطالعه و مقایسه رهیافت‌ها، راهبردها و خط مشی‌های ملی کشورهای مختلف نظیر ایالات متحده امریکا، کانادا، اتحادیه اروپا، آلمان، کره‌جنوبی و... در زمینه تدوین و بهره‌برداری از مقررات حفاظت از داده‌های عمومی، نسبت به شناسایی گزینه‌های راهبردی و ارائه چارچوب مفهومی اقدامات کلان در کشور حرکت نماید. این پژوهش امکان شناسایی رفتار مؤثر و کارا با پدیده‌های نوظهور را فراهم می‌آورد. در این راستا، شناسایی و مطالعه نظام‌مند اسناد راهبردی کشورها با بهره‌گیری از روش تحلیل محتوای کیفی متعارف انجام شد. در ادامه، به‌منظور ارزیابی و پایایی کُدگذاری محتوا، با محاسبه ضریب توافق کاپای کوهن معادل ۶۲.۰ به دست آمد. بر اساس نتایج تحقیق، مقوله‌هایی چون جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس، به‌عنوان مهم‌ترین درس‌های آموخته و محورهای چارچوب مفهومی اقدامات کلان پیشنهادی جهت تدوین راهبردهای ملی در زمینه‌ی توسعه مقررات حفاظت از داده‌های عمومی شناسایی شدند.

کلمات کلیدی: راهبردهای ملی توسعه مقررات حفاظت از داده‌های عمومی، تحلیل فراگیر راهبردها، تحلیل محتوا.

۱ مقدمه

شرکت‌ها، سازمان‌ها و کسب‌وکارهای مختلف هر کدام به دلایلی نظیر ارائه کالاها و خدمات، اعطای مجوز، شناسایی وضعیت و هویت افراد به‌نحوی با داده‌ها و اطلاعات افراد سر و کار دارند. از سوی دیگر افراد در سطوح مختلف با توجه به نوع فعالیت و مجوزهایی که از سوی مراجع مختلف صادر می‌شوند، سطحی از اعتماد در حفظ حریم خصوصی را برای این نهادهای حقوقی قائل هستند. این امر نه تنها از جنبه حفظ حریم و اطلاعات خصوصی، بلکه از جنبه اعتماد عمومی و اجتماعی نیز دارای اهمیت است که حاکمیت بتواند نه تنها اعتماد افراد، بلکه اعتماد به ساختارهای سازمان‌محور تحت حمایت و حاکمیت خود را از استفاده بجا و بدون سوء استفاده از داده‌ها و اطلاعاتشان در هر سطحی مطمئن سازد. از سوی دیگر، ماهیت هر جایی، هر زمانی و گستردگی کاربردهای فناوری‌های مبتنی بر داده و اطلاعات از یک سو و پراکندگی و گستردگی شرکت‌ها، سازمان‌ها و نهادهایی که با اطلاعات عمومی در ارتباط هستند از سوی دیگر، موجب شده است که نظارت بر چنین امری (حفاظت از داده‌ها) به مقوله‌ای چالش‌برانگیز و در عین حال اجتناب‌ناپذیر تبدیل شود. این امر لزوم طراحی ساز و کارهای متنوع برای حفاظت از داده‌های عمومی را دوچندان کرده و با توجه به شیوع و پیشرفت آن در طول زمان، اهمیت و فوریت آن را نیز افزایش داده است.

۱.۱ 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 [۱]. 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 [۱]. دامنه حریم خصوصی تا حدودی با امنیت هم‌پوشانی دارد؛ به‌طوری 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 [۲] و در برخی موارد، در قانون اساسی کشورها نیز آمده است و چون این قوانین ذیل حقوق بشر تعریف می‌گردند، معمولاً قوانین سخت‌گیرانه‌ای نیز به‌شمار می‌آیند [۳].

۲.۱ اهداف حفاظت از داده‌های عمومی

برای حفاظت از داده‌ها سه هدف اصلی را می‌توان متصور بود [۴]:

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[1].

۲. حمایت از حقوق و آزادی‌های اساسی اشخاص حقیقی به‌ویژه در حوزه حمایت از داده‌های شخصی آن‌ها.

[1] Free Movement of Personal Data

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 به‌کار گرفته شده است که بخشی از آن‌ها معرف خروجی‌های متنوع و کاربردی شده در سطح آزمایشگاه‌های معتبر و آکادمیک بوده که می‌تواند در شناسایی راهکارها و فناوری‌های لازم برای حفاظت از داده‌های عمومی بسیار مؤثر باشد.

۳.۱ دامنه کاربرد قوانین و مقررات حفاظت از داده‌ها

در اسناد مختلف در خصوص دامنه کاربرد مقررات حفاظت از داده‌ها، عناوین متعددی اشاره شده است که فصل مشترک آن‌ها را می‌توان در موارد زیر خلاصه کرد [۵]:

الف) هر نوع پردازش داده‌های شخصی، با استفاده از روش‌های خودکار و یا غیرخودکار که تمام یا بخشی از یک سامانه بوده و تمام یا بخشی (به‌طور کامل یا جزئی) از داده‌های شخصی را مورد پردازش قرار دهد.

ب) برای پردازش داده‌های شخصی توسط نهادها، ارگان‌ها و سازمان‌های خاص لازم است تا آیین‌نامه‌های جداگانه‌ای طراحی و اعمال شده و با مقررات کلی حفاظت از داده‌ها سازگار شود.

ج) لازم است برای ارائه‌دهندگان خدمات واسطه‌ای[۲] نیز آیین‌نامه‌های جداگانه‌ای طراحی و ارائه شده و با مقررات کلی حفاظت از داده‌ها سازگار شود.

البته قوانین و مقررات در این حوزه در برخی از موارد استثناء نیز قائل شده‌اند که از مهم‌ترین آن‌ها به‌شرح زیر هستند [۶]:

- چنانچه فعالیتی خارج از چارچوب‌های جغرافیایی شمول مقررات باشد.
- توسط سازمان‌ها و نهادهایی انجام گیرد که از سوی قانون مجوز آن را دارا می‌باشند.
- توسط اشخاص با ویژگی‌های خاص و برای مصارف صرفاً شخصی و محدود انجام شود.
- توسط مقامات ذی‌صلاح و به‌منظور پیشگیری، تحقیق، کشف یا پیگرد قانونی از جرائم کیفری یا اجرای مجازات‌های کیفری – از جمله حراست و جلوگیری از تهدیدات برای امنیت ملی و عمومی – انجام شود.

[2] Intermediary Service Providers

۲ تعاریف و مفاهیم مرتبط با حفاظت از داده‌ها

بررسی منابع و مراجع مختلف، محقق را به مجموعه‌ای از مفاهیم کلیدی در فضای مقررات عمومی حفاظت از داده‌ها می‌رساند که در ادامه مورد بررسی قرار خواهند گرفت.

اطلاعات شخصی: «داده‌های شخصی»[۳] به‌معنای هرگونه اطلاعات مربوط به یک شخصِ[۴] مشخص یا قابل شناسایی[۵] (موضوع داده) است [۷]. شخص حقیقی قابل شناسایی معرف فردی است که می‌تواند به‌طور 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. این تعریف گسترده و کاملاً فراگیر است که شامل موارد زیر است:

الف) هرگونه اطلاعات مربوط به یک شخصِ مشخص (یعنی اطلاعات شخصی‌شده).

ب) اطلاعات مربوط به شخصی که بر اساس انواع شناسه‌ها قابل شناسایی باشد.

ارائه این تعریف برای افراد «مشخص» نسبتاً ساده است. به‌عنوان مثال، چنانچه شخصی گواهینامه رانندگی، مجوز کار، استعلام سوابق کیفری و... را داشته باشد، یک هویت مشخص مانند مدرسه، کارفرما یا صاحبخانه فرد (به عنوان کنترل‌کننده) به راحتی می‌تواند آن را شناسایی کند. بدین ترتیب هر نوع داده‌ای از شما، مثل تاریخ تولد، آدرس، شماره تلفن، حقوق و دستمزد و هزینه اجاره خانه شما، داده‌های شخصی محافظت‌شده تحت GDPR را تشکیل می‌دهند.

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، پاک‌کردن و یا از بین بردن از عمده عملیات رایج پردازشی محسوب می‌شوند.

محدودسازی پردازش: این مفهوم به معنی علامت‌گذاری بر روی داده‌های شخصی ذخیره‌شده با هدف محدودکردن پردازش آن‌ها در آینده است.

کنترل‌کننده: این مفهوم به معنای شخص حقیقی یا حقوقی، مرجع عمومی، سازمان یا یک نهاد دیگر است که به تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کند. در مواردی که اهداف و وسایل پردازش براساس قانون کشور تعیین شده باشد، لازم است کنترل‌کننده خود را با معیارهای مشخص‌شده تطبیق دهد [۱۰].

[3] Personal Data
[4] Natural Person
[5] Identifiable

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 [۱۰].

شخص ثالث: این مفهوم به معنای شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا ارگان‌های دیگر (به غیر از موضوع داده، کنترل‌کننده و پردازش‌گر) و اشخاصی است که تحت اختیار مستقیم کنترل‌کننده و یا پردازش‌گر، مجاز به پردازش داده‌های شخصی هستند [۱۱].

رضایت: رضایت[۶] از موضوع داده‌ها به معنای هرگونه نشان‌دادن آزادانه و آگاهانه و بدون ابهام در مورد استفاده از داده‌ها است که توسط فرد با یک بیانیه یا با امضای یک تأییدیه روشن، توافقی را برای پردازش داده‌های شخصی فرد ایجاد می‌کند.

داده‌های ژنتیکی: این مفهوم به معنی داده‌های شخصی مربوط به ویژگی‌های ژنتیکی ارثی یا اکتسابی یک فرد حقیقی است که اطلاعات خاصی را در مورد فیزیولوژی یا سلامتی – به‌ویژه از تجزیه و تحلیل نمونه بیولوژیکی – آن شخص ارائه می‌دهد [۱۱].

داده‌های بیومتریک: این مفهوم به معنای داده‌های شخصی ناشی از پردازش فنی خاص مربوط به خصوصیات جسمی، فیزیولوژیکی یا رفتاری یک شخص حقیقی است که به شناسایی منحصر به فرد آن شخص – مانند تصاویر صورت یا داده‌های انگشت‌نگاری[۷]– منجر می‌شود.

اطلاعات مربوط به سلامتی: این مفهوم به معنای داده‌های شخصی مربوط به سلامت جسمی یا روانی یک شخص – از جمله خدمات مراقبت‌های بهداشتی ارائه‌شده به شخص – است که اطلاعاتی را پیرامون وضعیت سلامتی وی نشان می‌دهد.

مرکز اصلی تأسیس: مرکز اصلی تأسیس[۸] در مورد کنترل‌کننده‌ها و پردازش‌گرها بدین معنی است:

الف) در مورد یک کنترل‌کننده با استقرار در بیش از یک کشور و دارای محل استقرار در کشور، محل مدیریت مرکزی آن در کشور مرجع ملاک تصمیم و مسئول در مورد اهداف و ابزارهای پردازش داده‌های شخصی خواهد بود، مگر اینکه آن‌را به یکی از شعب خود واگذار کرده باشد که در این‌صورت نیز مسئول تصمیمات، شعبه اصلی خواهد بود [۱۲].

ب) در مورد یک پردازنده با استقرار در بیش از یک کشور و دارای محل استقرار در کشور، محل مدیریت مرکزی آن در کشور مرجع ملاک تصمیم و مسئول در مورد اهداف و ابزارهای پردازش داده‌های شخصی خواهد بود، مگر اینکه آن را به یکی از شعب خود واگذار کرده باشد که در این صورت نیز مسئول تصمیمات، شعبه اصلی خواهد بود.

[6] Consent
[7] Dactyloscopy
[8] Main Establishment

بنگاه اقتصادی: این مفهوم به معنای شخص حقیقی یا حقوقی است که – صرف نظر از شکل قانونی آن – از طریق مشارکت و یا ایجاد انجمن‌هایی ایجاد می‌شود که به‌طور منظم در یک فعالیت اقتصادی مشغول فعالیت اقتصادی هستند.

گروه شرکت: مفهوم گروه شرکت[9] به‌معنای یک شرکت کنترل‌کننده و شرکت‌های تحت حمایت و متعهد به آن می‌باشد [۱۳].

مرجع نظارت: این مفهوم به‌معنای یک مرجع عمومی مستقل است که به موجب قانون تأسیس شده و وظیفه نظارت بر اجرای قوانین و مقررات حفاظت از داده‌ها را برعهده دارد.

مرجع نظارتی مرتبط: این مفهوم به معنای یک مرجع نظارتی است که دغدغه اصلی آن به دلایل زیر پردازش اطلاعات شخصی در موارد خاص است:

الف) کنترل‌کننده یا پردازشگر در قلمرو کشور دیگری تأسیس شده است.

ب) تعداد افراد قابل ملاحظه‌ای تحت تأثیر پردازش و کنترل داده در یک شرکت خاص باشند.

پردازش مرزی: پردازش مرزی[10] در شرایط زیر معنی می‌شود:

a) پردازش داده‌های شخصی که در چارچوب فعالیت‌های یک شرکت یا بنگاه اقتصادی که خارج از کشور فعالیت می‌کند و یا علاوه بر فعالیت در کشور، در سایر کشورها نیز فعال است.

۱. پردازش داده‌های شخصی که در قالب یک کنترل‌کننده و یا پردازش‌گر در داخل کشور فعالیت می‌کند ولی فعالیت‌های آن تأثیر قابل ملاحظه‌ای بر فعالیت‌های خارج از کشور دارد.

اعتراض مربوط و مستدل: این مفهوم به معنی اعتراض به تصمیماتی است که منجر به نقض قوانین و آیین‌نامه‌ها در حوزه حفاظت از داده‌ها، تداخل مقررات این حوزه با سایرحوزه‌ها و یا اختیارات پیش‌بینی شده در رابطه با کنترل‌کننده‌ها و پردازش‌گرها و نحوه فعالیت آن‌ها می‌شود.

خدمات جامعه اطلاعاتی: خدمات در جامعه اطلاعاتی یعنی هر خدمتی که به طور معمول در یک بنگاه اقتصادی برای سود / پاداش انجام می‌شود و از راه دور، از طریق وسایل الکترونیکی و به درخواست فرد دریافت‌کننده خدمات انجام می‌شود [۱۴].

در اینجا «از راه دور» بدان معنی است که این خدمات در اکثر موارد بدون حضور همزمان طرفین ارائه می‌شود. همچنین «از طریق الکترونیکی» به این معنی است که این سرویس در ابتدا با استفاده از تجهیزات الکترونیکی برای پردازش و ذخیره‌سازی داده‌ها در مقصد دریافت می‌شود و به‌طور کامل از طریق رابط سیمی،

[9] Group of Undertakings
[10] Cross-Border Processing

از طریق رادیو، به‌صورت نوری، الکترومغناطیسی و یا با هر وسیله دیگری منتقل و دریافت می‌شود. علاوه بر موارد فوق، «در صورت درخواست فرد دریافت‌کننده خدمات» نیز بدان معنی است که این خدمات از طریق انتقال داده به درخواست فردی ارائه می‌شود.

سازمان بین‌المللی: این مفهوم به معنای سازمان و نهادهای فرعی آن است که براساس قوانین بین‌المللی عمومی فعالیت می‌کند و یا هر نهادی که توسط دو یا چند کشور بوجود آمده باشد یا براساس قوانین آن‌ها ایجاد شده باشد.

موضوع داده: موضوع داده[11] به هر فرد مشخصی اطلاق می‌شود که به‌طور 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 [۱۴]. موضوع و افراد داده می‌توانند مشتریان، پیمانکاران، فروشندگان و حتی کارمندان یک سازمان باشند.

دسته‌بندی‌های ویژه از اطلاعات شخصی: برخی از داده‌ها از حساسیت‌های خاصی در استفاده و پردازش برخوردار هستند که در اینجا دسته‌بندی شده‌اند و محافظت از آن‌ها نیز تابع شرایط خاصی خواهد بود. به عبارت دیگر، انواع داده‌های شخصی زیر ممکن است به محافظت خاصی نیاز داشته باشند:

- نژاد و قومیت
- عقاید سیاسی، مذهبی یا فلسفی (از جمله عضویت در اتحادیه‌ها)
- سلامتی، زندگی فردی و گرایش جنسی
- داده‌های ژنتیکی و بیومتریک (به‌منظور شناسایی منحصر به فرد)

البته برای استفاده از این داده‌ها نیز شرایط خاصی را می‌توان طراحی کرد که رضایت شخصی، استفاده در مراحل شغلی قانونی، استفاده در شرایط پزشکی خاص و نیز استفاده برای تحقیق و توسعه از جمله این موارد هستند.

رضایت در استفاده از داده: «رضایت» از پردازش و بهره‌برداری از داده‌ها به‌معنای هرگونه نشان‌دادن آزادانه و آگاهانه و بدون ابهام در مورد استفاده از داده‌ها است که توسط فرد با یک بیانیه یا با امضای یک تأییدیه روشن، توافقی را برای پردازش داده‌های شخصی فرد ایجاد می‌کند.

[11] Data Subject

بهره‌گیری مشروع از داده: یکی از مفاهیم اساسی در پردازش داده‌ها، بهره‌برداری مشروع[12] 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.

مرجع محافظت از داده: مراجع محافظت از داده[13] معرف مقام رسمی مستقلی هستند که از طریق اختیارات تحقیق و تصحیح، بر اعمال قانون حمایت از داده‌ها نظارت می‌کنند. آن‌ها مشاوره تخصصی را در مورد مسائل مربوط به حمایت از داده‌ها ارائه می‌دهند و به شکایاتی که ممکن است قانون را نقض کرده باشند، رسیدگی می‌کنند. مرجع حفاظت از داده تضمین می‌کند که داده‌های شخصی به‌درستی نگهداری و با دقت محافظت می‌شوند، و نیز حفظ حریم خصوصی آینده‌ی کاربران را نیز تضمین می‌کند.

مدیر حفاظت از داده: کنترل‌کننده و پردازش‌گر داده‌ها باید از یک نفر به عنوان «مدیر حافظت از داده»[14] استفاده کنند. بهره‌گیری از این مدیر در موارد زیر ضروری است:

الف) پردازش داده‌ها توسط یک مقام یا نهاد عمومی انجام می‌شود.

ب) فعالیت‌های اصلی کنترل‌کننده یا پردازش‌گر شامل عملیات پردازش باشد که به دلیل ماهیت، دامنه و یا اهداف آن‌ها، نیاز به نظارت منظم بر داده‌ها در مقیاس بزرگ دارند.

ج) فعالیت‌های اصلی کنترل‌کننده یا پردازش‌گر شامل پردازش داده‌های شخصی در مقیاس وسیعی از دسته‌بندی‌های خاص و مربوط به محکومیت‌ها و جرائم کیفری باشد.

[12] Legitimate Interest
[13] Data Protection Authority
[14] Data Protection Officer

نقض داده: نقض داده‌ها[15] معرف یک مسئله امنیتی است که منجر به تخریب تصادفی یا غیرقانونی، از بین رفتن، تغییر، افشای غیرمجاز یا دسترسی به داده‌های محافظت‌شده می‌شود. اساساً هر چیزی که بر محرمانه بودن، صحت یا دسترس‌پذیری داده‌ها تأثیر بگذارد، نقض داده خوانده می‌شود. در برخی از قوانین حفاظت از داده‌ها، سازمان‌ها از نظر قانونی موظف هستند تا ظرف مدت زمان خاصی از نقض داده‌ها اطلاع یافته و آن‌را به مرجع حفاظت از داده‌ها گزارش دهند [۱۴].

۳ مقررات و قوانین در ایران در حوزه 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 حوزه حفاظت از داده‌ها است.

چنین شرایطی توجه تصمیم‌سازان و سیاست‌گذاران دولتی را بیش از پیش به موضوع حفاظت از داده‌ها معطوف داشته است و دولت‌ها نیز نقش مهمی در این روند ایفا خواهند کرد. دولت به عنوان یک تسهیل‌کننده به ایجاد یک محیط مساعد برای بازیگران صنعت – از طریق اصلاحات رگولاتوری، ایجاد مهارت و ظرفیت‌سازی، استانداردسازی، توسعه قابلیت همکاری، زیرساخت‌ها و نیز اقدامات امنیتی – می‌پردازد[۱۰]. در همین راستا همکاری صنعت و دولت برای حصول اطمینان از ایجاد یک محیط مساعد برای توسعه مناسب و کارآمد قوانین و مقررات حفاظت از داده و اجرای آن امری اجتناب‌ناپذیر است. در جدول ۱ برخی از قوانین و مقررات ایران اشاره‌شده که با این حوزه ارتباط دارند.

از این‌رو بررسی مجموعه راهبردها و گام‌های 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 [۶]. 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.

۴ کلیات تحقیق

۱.۴ ضرورت انجام تحقیق

باتوجه به مجموعه موارد فوق، بدون داشتن درک و آگاهی از خط‌مشی‌ها و راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای توسعه‌یافته و در حال توسعه (نظیر جمهوری اسلامی ایران) احتمال تحمیل هزینه‌های فرصت به تصمیم‌سازان این حوزه در کشور افزایش می‌یابد. بنابراین نیاز است تا یک چارچوب

[15] Data Breach

جدول ۱: برخی از قوانین و مقررات مرتبط با حفاظت از داده‌ها در ایران

ردیف	عنوان	موضوع کلیدی مطرح‌شده
۱	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.
۲	ماده ۱۳۰ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۳۸۳)	لایحه «حفظ و ارتقاء حقوق شهروندی و حمایت از حریم خصوصی افراد، در راستای اجرای اصل بیستم (۲۰) قانون اساسی جمهوری اسلامی ایران» توسط قوه قضائیه تدوین می‌شود.
۳	مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب شورای‌عالی انقلاب فرهنگی (۱۳۸۰)	وظایف ISPها دربرگیرنده حریم خصوصی کاربران و تعیین جرایم افشاء است.
۴	قانون برنامه پنجساله پنجم توسعه جمهوری اسلامی ایران (۱۳۹۴-۱۳۹۰)	تبصره ماده ۲۰۶ – عدم افشاء اطلاعات بند الف ماده ۳۵ – صیانت از اطلاعات پزشکی
۵	بند ۱ منشور حقوق شهروندی	تفکیک حریم عمومی از حریم خصوصی و نهادینه کردن خدمت در هر دو حریم که متاسفانه جزئیاتی پیرامون آن اشاره نشده است.
۶	بند «ب» اساسنامه سازمان بیمه سلامت ایران	تشکیل و صیانت از پرونده الکترونیکی سلامت افراد مدنظر است.
۷	بند ۴ ماده ۱۲ دستورالعمل تشکیل بانک اطلاعات هویت ژنتیک ایران	دستورالعمل حفاظت از اطلاعات ژنتیکی در آزمایشگاه‌ها را مدنظر قرار داده است.
۸	مصوبه شورای عالی اداری در خصوص منشور حقوق شهروندی (۱۳۹۵)	تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان توسط قوه قضائیه مدنظر قرار گیرد.

مفهومی برای شناسایی و بیان گزینه‌های راهبردی کشور در مواجهه با این حوزه ارائه شود. براین‌اساس، ضرورت‌های انجام تحقیق حاضر به‌شرح زیر هستند:

- درک بهتر رهیافت‌ها و راهبردهای مرتبط با توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف جهان
- تصمیم‌سازی در حوزه توسعه قوانین و مقررات حفاظت از داده‌ها در کشور مبتنی بر درس‌های آموخته و بهترین تجارب منتشرشده در سایر کشورها
- ارائه یک سازوکار پشتیبان تصمیم جهت شناسایی و تبیین راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها در کشور

۲.۴ سؤالات تحقیق

بر اساس مجموعه موارد مطرح‌شده، سؤال اصلی این پژوهش عبارت است از:

- چارچوب مفهومی برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشور دارای چه ابعادی است؟

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

- ابعاد/ گزینه‌های راهبردی توسعه قوانین و مقررات حفاظت از داده‌ها در سایر کشورها چیست؟
- چارچوب مفهومی مناسب برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشور کدام است؟
- اهمیت هریک از ابعاد / گزینه‌های راهبردی در چارچوب پیشنهادی به چه میزان است؟

۳.۴ اهداف تحقیق

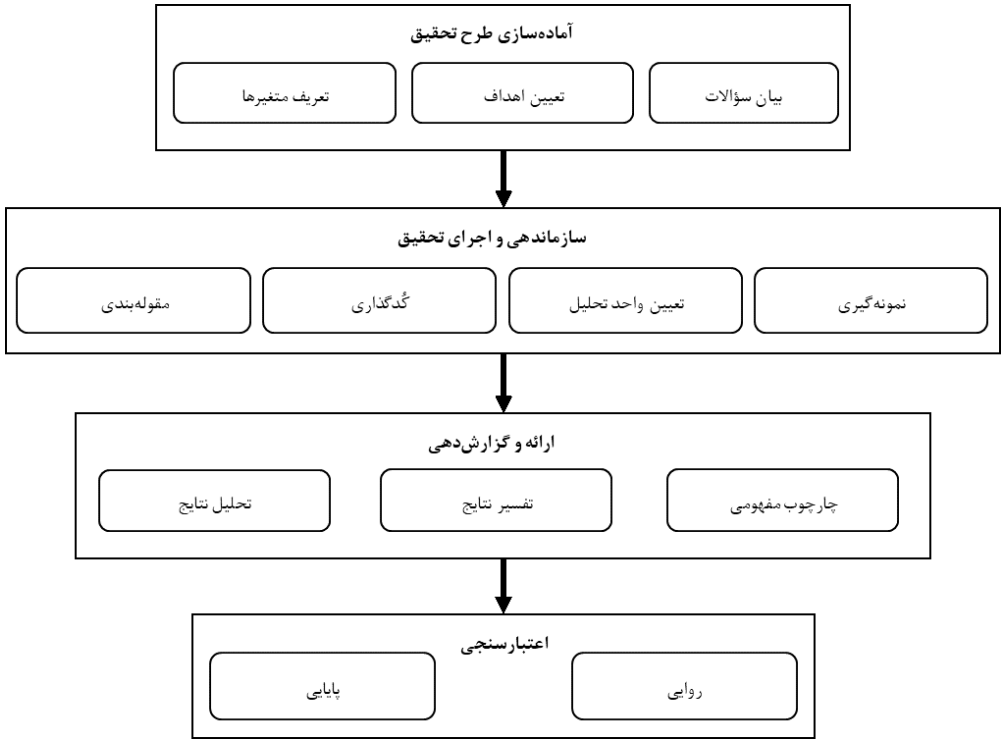
هدف اصلی در این پژوهش مطالعه مقایسه‌ای راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها باهدف «ارائه یک چارچوب مفهومی برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها» است. اهداف فرعی شامل موارد ذیل می‌باشد:

- بررسی رهیافت و نگرش کشورهای مختلف نسبت به قوانین و مقررات حفاظت از داده‌ها
- شناسایی و تحلیل ابعاد / گزینه‌های راهبردی توسعه قوانین و مقررات حفاظت از داده‌ها در سایر کشورها
- بررسی و انتخاب یک چارچوب کاربردپذیر جهت شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها مبتنی بر درس‌های آموخته

۵ چارچوب پیشبرد تحقیق

محقق در راستای ارائه یک چارچوب مفهومی اقدامات کلان توسعه قوانین و مقررات حفاظت از داده‌ها نسبت به بررسی مقایسه‌ای راهبردهای منطقه‌ای، ملی و بخشی این حوزه در قالب یک چارچوب نظام‌مند تحقیق اقدام نموده است. این چارچوب در قالب شکل ۱.۵ ارائه شده‌است [۱۵].

در گام اول و براساس مسئله تحقیق تعریف‌شده، محقق به بیان اهداف، سوالات و متغیرهای تحقیق می‌پردازد. لازم به ذکر است که متغیرهای تحقیق حاضر همان راهبردها و اقدامات کلان ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف هستند. در گام دوم تحقیق، نمونه‌گیری (براساس روش‌های نمونه‌گیری هدفمند و در دسترس)، تعیین واحد تحلیل و زمینه (براساس کلمات، عبارت‌ها و مضامین معرف گزاره‌های راهبردی هدف تحقیق) و نیز کُدگذاری و مقوله‌بندی (براساس دستورالعمل کُدگذاری دو مرحله‌ای باز و مبتنی بر رویکرد استقرایی و داده‌رانده) در دستورکار محقق قرار می‌گیرد. در گام سوم، محقق نسبت به ارائه چارچوب مفهومی پیشنهادی (براساس کُدگذاری و مقوله‌بندی برخاسته از داده) و نیز تحلیل و بررسی یافته‌ها (براساس تحلیل فراوانی کُدها و مقوله‌ها، تحلیل‌های درون و بین موردی و نیز بررسی‌های مقایسه‌ای) می‌پردازد. در گام چهارم نیز محقق به بررسی اعتبار چارچوب پیشنهادی خواهد پرداخت.



شکل ۱: چارچوب پیشبرد تحقیق

۱.۵ روش تحقیق

در این پژوهش از روش تحلیل محتوای کیفی استفاده شده است که یکی از روش‌های انجام پژوهش کیفی است. تحلیل محتوای کیفی در جایی که تحلیل کمی به محدودیت‌هایی می‌رسد، نمود می‌یابد. بنابراین تحلیل محتوی کیفی را می‌توان روش تحقیقی برای تفسیر ذهنی محتوایی داده‌های متنی – از طریق فرایندهای طبقه‌بندی نظام‌مند کُدبندی و تم‌سازی یا طراحی الگوهای شناخته‌شده – دانست [۱۵].

با تحلیل کیفی می‌توان یک رویکرد تجربی روش شناسانه و کنترل‌شده مرحله به مرحله را با رعایت عناصر مورد مطالعه در نظر گرفت. عینیت نتایج به‌وسیله وجود یک فرآیند کُدبندی نظام‌مند تضمین می‌شود. این روش، تِم و الگوهایی که آشکار و یا پنهان هستند را به‌صورت محتوای آشکار می‌آزماید [۱۶].

هم اکنون سه رویکرد: سنتی (متعارف)[۱۶] ، هدایت‌شده[۱۷] ، جامع[۱۸] برای کاربرد تحلیل محتوا مطرح است. در تحلیل محتوی به روش متعارف طبقات به گونه مستقیم از متن داده‌ها استخراج می‌شوند. ستون فقرات تحقیق حاضر مبتنی بر روش تحلیل محتوای متعارف بنا نهاده شده است. در این روش، محقق به دنبال تفسیر ذهنی محتوای متنی از طریق فرآیندهای طبقه‌بندی نظام‌مند، کُدگذاری، مقوله‌بندی و نیز ارائه یک چارچوب مفهومی شناخته‌شده است [۱۸]. پیش‌فرض محقق پیرامون استفاده از این روش تحقیق، جدید بودن پدیده مورد مطالعه (یعنی قوانین و مقررات حفاظت از داده‌ها) و محدود بودن منابع نظری پیرامون آن است. در این شرایط، محقق از به‌کارگیری مقوله‌های از پیش تعریف‌شده پرهیز می‌نماید و به دنبال بکارگیری رویکردی داده‌رانده برای شناسایی مقوله‌ها است. براساس روش پایه انتخابی (تحلیل محتوای متعارف)، محقق مجموعه‌ای از فعالیت‌های مستقل اما به‌هم‌پیوسته را در قالب چهار گام برای پیشبرد تحقیق حاضر پیش‌بینی نموده است. این گام‌ها در قالب شکل ارائه شده‌است.

البته محقق برای غنابخشی به یافته‌های تحقیق از مجموعه‌ای از روش‌ها و تکنیک‌های تحقیق در مرحله سوم (ارائه و گزارش‌دهی) استفاده نموده است. در این گام و برای تحلیل یافته‌های تحقیق –مبتنی بر چارچوب مفهومی پیشنهادی – از تکنیک‌های بررسی درون موردی و بین موردی و نیز بررسی مقایسه‌ای راهبردی استفاده شده است. در بررسی مقایسه‌ای راهبردی، محقق به دنبال هدف‌هایی فراتر از توصیف بوده و این‌کار متضمن داوری و ارزش‌گذاری آزمودنی‌ها است. در این نگاه، محقق برای بهبود یافته‌ها از بررسی مقایسه‌ای می‌تواند با هدف تصمیم‌گیری در سطح ملی و بخش بهره‌برداری نماید [۱۵]. علاوه بر این، در تحلیل‌های درون موردی و بین موردی – مبتنی بر ساختار حاکم بررسی موردی چندگانه مطرح‌شده در تحقیق حاضر – محقق به دنبال مقایسه دیدگاه‌های حاکم در کشورهای مختلف و نیز دلیل پرداخت یا عدم پرداخت به برخی از نمونه‌های موردی مبتنی بر شرایط آن کشور است [۱۵].

[16] Conventional
[17] Directed
[18] Summative

۲.۵ جامعه و نمونه آماری تحقیق

جامعه آماری تحقیق حاضر متشکل از گزارش‌های منطقه‌ای (قاره‌ای و بین قاره‌ای)، ملی و بخشی متنشرشده در زمینه راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها است. محقق برای تأمین جامعیت تحقیق حاضر نسبت به انتخاب هدفمند اسناد فوق اقدام نموده است؛ به‌گونه‌ای که کلیه اسناد راهبردی (منطقه‌ای، ملی و بخشی) مشتمل بر ۳۸ نمونه موردی دسترس‌پذیر تا سال ۲۰۲۱ در قالب روش سرشماری جمع‌آوری و مورد تحلیل عمیق قرار گرفته‌اند. علاوه بر این، جهت سنجش روایی اسناد مورد بررسی پنل خبرگی ۶ نفره با حضور اعضای هیات علمی و خبرگان حوزه فناوری در پژوهشگاه ارتباطات و فناوری اطلاعات، دانشگاه تهران، دانشگاه شهید بهشتی و دانشگاه علم و صنعت – که در مجموع سابقه انجام ۶ پروژه راهبردی، کاربردی و توسعه‌ای در زمینه قوانین و مقررات حفاظت از داده‌ها طی ۳ سال گذشته را داشته‌اند – تشکیل گردید.

۳.۵ روش گردآوری و تحلیل داده‌های تحقیق

واحد تحلیل در این پژوهش، کل متن اسناد شناسایی شده‌است. پس از انتخاب واحد تحلیل، به تدوین مقوله‌ها و زیرمقوله‌های اسناد پرداخته شده و متغیرهای پژوهش از این طریق شناسایی شده‌اند. جهت تحلیل اسناد مقوله، اختصاص داده شده است. هر یک از مقوله‌ها دارای یک یا چند واحد است. با شناسایی راهبردهای کلیدی در متن اسناد و کُدگذاری داده‌ها امکان بررسی و تحلیل راهبردها فراهم شده‌است. در این روش دو عنصر اصلی مطرح هستند: واحد تحلیل و مقوله تحلیل.

واحد تحلیل معرف کوچک‌ترین جزء پیکره‌ی متن است که برای رسیدن به هدف تحقیق، اندازه‌گیری و شمارش می‌شود. واحد تحلیل می‌تواند در برگیرنده کلمه، جمله، پاراگراف و... باشد که این واحدها وابسته به نوع متن و هدف پژوهش انتخاب می‌شوند.

هنگامی که واحدها معین شدند باید مشخص گردد که واحدهای استخراج و شمارش‌شده چگونه دسته‌بندی می‌شوند. عناوین این دسته‌بندی‌ها معرف مقوله تحلیل هستند. در نهایت واحدها براساس مقوله‌های تحلیل دسته‌بندی می‌شوند تا مراحل شمارش و تحلیل اطلاعات صورت گیرد [۱۵].

۶ بررسی اقدامات راهبردی تدوین مقررات حفاظت از داده‌های عمومی در واحدهای تحلیل

همانطور که پیش از این اشاره شد، واحد تحلیل در این پژوهش کلیه اسناد راهبردی (منطقه‌ای، ملی و بخشی) مشتمل بر ۳۸ نمونه موردی دسترس‌پذیر تا سال ۲۰۲۱ است. در ادامه و به‌منظور بررسی تفصیلی موضوع نسبت به ارائه خلاصه کلی از اهداف کلیدی و برنامه‌های پیش‌بینی‌شده در ۵ نمونه منتخب اقدام می‌گردد.

۱.۶ ایالات متحده امریکا

ایالات متحده امریکا یکی از معدود کشورهای جهان است که نهاد دولتی برای محافظت از داده‌های فدرال ندارد. با این وجود ایالات متحده رهبر جهانی در زمینه حفظ حریم خصوصی در جهان از جنس کارکردی

و ساختاری محسوب می‌شود. قانون گزارش اعتباری منصفانه[۱۹]، مصوب سال ۱۹۷۰ در آن زمان به عنوان اولین قانون مدرن برای حفظ حریم خصوصی، پاسخی به اتوماسیون روبه‌رشد داده‌های شخصی در ایالات متحده تلقی شد.

اما امروز اروپا در حمایت از داده‌های مصرف‌کننده از ایالات متحده پیشی گرفته و آیین‌نامه حمایت از داده‌های عمومی که از سال ۲۰۱۸ به اجرا در آمد، حقوق اساسی افراد را تقویت می‌کند و مصرف‌کنندگان را مجدداً بر سرنوشت داده‌های شخصی خود مسلط می‌کند و این حقوق را به اشخاص می‌دهد که در صورت نقض (در مدت ۷۲ ساعت) اطلاع‌رسانی کنند و از حقوق مصوب در این قانون بهره‌مند گردند [۱۹]. در این شرایط، در کشور آمریکا قوانین متعددی تدوین و ارائه شده است که در جدول ۲ به برخی از آن‌ها اشاره می‌شود.

۲.۶ اقدامات کانادا

کانادا مدت‌هاست که با تصویب «قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی[۲۴]» (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 دربر می‌گیرد. امروزه، این اصول همچنین در آیین‌نامه حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) نیز دیده می‌شود [۲۰].

در PIPEDA به ۱۰ اصل اساسی حفاظت از داده‌ها اشاره شده‌است. در عین حال سازمان‌ها در هر زمان مسئولیت حفاظت از اطلاعات شخصی را برعهده دارند و موظف هستند که اطمینان حاصل کنند که هرگونه 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.

۳.۶ اقدامات اتحادیه اروپا

مقررات حفاظت از داده‌های عمومی اتحادیه اروپا[۲۵] (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 شده‌است. 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 [۱۰].

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

[19] Fair Credit Reporting Act
[24] Personal Information Protection and Electronic Documents Act
[25] General Data Protection Regulation

جدول ۲: برخی از قوانین و مقررات ایالات متحده امریکا در حوزهٔ حفاظت از داده‌ها

ردیف	عنوان	موضوع مورد توجه
۱	قانون گرام لیچ بیلی [۲۰]	حمایت از اطلاعات شخصی در دست بانک‌ها، شرکت‌های بیمه و سایر شرکت‌های حوزه خدمات مالی
۲	قانون گزارش اعتباری منصفانه [۲۱]	محدودسازی استفاده از اطلاعات دارای اعتبار مربوط به اعتبار فردی، جایگاه اعتباری، ظرفیت اعتباری، شخصیت و شهرت عمومی
۳	استانداردهای امنیت داده‌های صنعت کارت پرداخت (PCI-DSS)	مجموعه‌ای از استانداردهای امنیتی که توسط شرکت‌های بزرگ کارت اعتباری به‌منظور محافظت از داده‌های دارندگان کارت‌های پرداخت تهیه شده‌است.
۴	قانون قابلیت انتقال و پاسخگویی بیمه سلامت (HIPAA)	بهبود بهره‌وری در مراقبت‌های بهداشتی و نتایج مراقبت از بیمار با تشویق جریان آزاد اطلاعات بهداشتی در ایالات متحده و حراست از حریم خصوصی اطلاعات بهداشتی فرد
۵	قانون حمایت از مصرف‌کنندگان تلفن	آیین‌نامه‌های مرتبط با تماس‌ها و پیام‌های متنی تلفن‌های همراه و قوانین مربوط به تماس با تلفن‌های ثابت برای اهداف بازاریابی یا استفاده از سیستم‌های شماره‌گیری خودکار یا پیام‌های از پیش ضبط‌شده
۶	قانون آموزش حقوق و حفظ حریم خصوصی خانواده	ایجاد حق بازرسی و تجدید نظر در سوابق دانش آموزان و ممنوعیت افشای این سوابق یا سایر اطلاعات شخصی دانش‌آموزان، بدون رضایت وی و یا خانواده وی
۷	قانون حریم خصوصی مصرف‌کننده در کالیفرنیا	لایحه‌ای برای حفظ حقوق حریم شخصی و حمایت از مصرف‌کننده افراد مقیم ایالت کالیفرنیا
۸	قانون حفاظت از حریم خصوصی ویدیو	قانون حذف اطلاعات شناسایی شخصی در ویدئوها در شرکت‌های اجاره ویدیو حداکثر یک سال پس از آن که اطلاعات دیگر برای هدف جمع‌آوری‌شده آن ضروری نیست.
۹	قانون اوراق بهادار فدرال	قوانین کنترل اوراق بهادار فدرال در عرضه و فروش اوراق بهادار و تجارت اوراق بهادار، فعالیت‌های متخصصان خاص در صنعت، شرکت‌های سرمایه‌گذاری، پیشنهادات مناقصه، اظهارنامه‌های حقوقی و مقررات شرکت‌های عمومی کاربرد دارند.
۱۰	قانون حفاظت از حریم خصوصی آنلاین کودکان (COPPA)	حفاظت از داده‌ها و حریم خصوصی کودکان در فضای اینترنت
۱۱	قانون حفظ حریم خصوصی ارتباطات الکترونیکی [۲۲] (ECPA)	محافظت از ارتباطات برخط، شفاهی و الکترونیکی در زمان برقراری ارتباطات، حمل و نقل و ذخیره آنها را مدنظر قرار می‌دهد.
۱۲	قانون تقلب و سوءاستفاده رایانه‌ای [۲۳] (CFAA)	قانونی برای حفاظت از سیستم‌های کامپیوتری در مقابل قانون‌شکنی و حملات سایبری
۱۳	قانون کمیسیون تجارت فدرال (قانون FTC)	قانونی برای جلوگیری از استفاده از روش‌های ناعادلانه رقابت و اعمال یا اقدامات ناعادلانه یا فریبنده مؤثر بر تجارت
۱۴	قانون حمایت مالی از مصرف‌کننده (CFPA)	قانون ایجاد نقطه پاسخگویی برای اجرای قوانین مالی مصرف‌کننده فدرال و حمایت از مصرف‌کنندگان در بازار مالی
۱۵	چارچوب سیاست حفظ حریم خصوصی داده‌های پیشنهادی دولت ترامپ	مجموعه‌ای از اهداف حفظ حریم خصوصی «کاربر محور» برای حمایت از مصرف‌کنندگان در مقابل اقدامات نهادهای دولتی مرتبط با حریم خصوصی

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. به‌عنوان 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 به‌صورتی 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 PEPEDA	فرد می‌تواند انطباق یک سازمان با اصول PEPEDA را به چالش کشیده و چالش خود را به مسئول امور حفظ حریم خصوصی شرکت – که مسئولیت انطباق با PEPEDA را بر عهده دارد – ارائه کند.

از طریق طراحی و به‌طور پیش فرض» باشند؛ یعنی اطلاعات شخصی باید با استفاده از مستعارسازی یا بی‌نام‌سازی ذخیره شود و حداکثر محرمانگی به‌طور پیش‌فرض در نظر گرفته شود؛ به‌گونه‌ای که داده‌ها بدون رضایت صریح به‌طور عمومی در دسترس نباشد و بدون اطلاعات اضافی جداگانه برای تعیین هویت اشخاص قابل استفاده نباشد. براین 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 [۱۰].

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 درآمد. اعمال این قانون نیازمند تصویب قانون جداگانه در کشورهای عضو اتحادیه نمی‌باشد و به‌طور خودکار در همه آن‌ها لازم‌الاجرا است.

۴.۶ اقدامات کره جنوبی

مشابه ساختار مقررات عمومی حفاظت از داده مصوب اتحادیه اروپا در کشور کره جنوبی نیز قانونی در رابطه با محافظت از اطلاعات شخصی (قانون حمایت از اطلاعات شخصی[۲۶] (PIPA))، از سپتامبر ۲۰۱۱ تصویب و اجرا گردید. بدین ترتیب که «قانون حمایت از اطلاعات شخصی» کره جنوبی در ۲۹ مارس ۲۰۱۱ به تصویب مجلس قانونگذاری این کشور رسید و در ۳۱ مارس ۲۰۱۲ توسط دولت این کشور اجرایی شد. این قانون سخت‌گیرانه‌ترین و جامع‌ترین قانون حفاظت از حریم خصوصی کاربران در فضای مجازی در میان کشورهای دنیا شناخته می‌شود (گرینلیف و پارک، ۲۱۱۲). این قانون شامل تمامی سازمان‌های بخش دولتی نیز می‌شود و علاوه بر جامع بودن، دارای ویژگی‌های زیر است [۲۱]:

- کمیسیون حفاظت از اطلاعات شخصی که ۱۵ عضو مستقل دارد.
- الزام بنگاه‌های تجاری و سازمان‌های دولتی به نصب مأموران حافظ انطباق با قوانین حریم خصوصی.
- لزوم اطلاع‌رسانی به افراد آسیب‌دیده و نیز نهادهای نظارتی در صورت بروز هرگونه مسائل امنیتی و نشر داده‌های شخصی افراد.
- لزوم انجام ارزیابی آثار حریم خصوصی برای سامانه‌های بخش دولتی آسیب‌پذیر.
- الزام سازمان‌ها به اخذ رضایت آشکار افراد برای مقاصد بازاریابی با استفاده از پایگاه‌های داده خود سازمان‌ها.

[26] Personal Information Protection Act

۵.۶ اقدامات روسیه

در ۲۲ ژوئیه ۲۰۱۴ بود که اصلاحات قابل توجهی در قانون روسیه به تصویب رسید و در تاریخ ۱ سپتامبر ۲۰۱۵ لازم‌الاجرا گردید. این اصلاحات به کلیه اپراتورهایی که از داده‌های شخصی استفاده می‌کنند، الزام می‌کند که هرگونه اطلاعات شخصی افراد روس را در پایگاه‌های داده مستقر در روسیه ذخیره و پردازش کنند. مجازات نقض این شرط می‌تواند منجر به مسدود کردن وب‌سایت‌ها و کسب‌وکار شود. پیگیری حقوقی متخلفان از قانون حفاظت از داده‌های شخصی توسط سرویس فدرال با نظارت بر محتوا، ارتباطات و فناوری‌ها ایجاد می‌شود و این سرویس ممکن است برای مسدودکردن وب‌سایت‌ها اقدام کند.

تیم واکنش اضطراری به حوادث رایانه‌ای بخش مالی[۲۷] به‌عنوان زیرمجموعه‌ای از اداره‌کل امنیت و حفاظت از اطلاعات بانک روسیه تأسیس شده است و به‌عنوان مرکز دارای صلاحیت تبادل اطلاعات بین بانک روسیه، بانک‌ها و مؤسسات مالی غیربانکی (NBFIs)، شرکت‌های یکپارچه‌ساز ، فروشندگان آنتی ویروس و ارائه‌دهندگان خدمات ارتباطاتی و اپراتورها و به‌طور خاص برای اجرای قانون در سراسر جامعه فعالیت می‌کند و مقام نظارت بر امنیت سایبری در سراسر صنعت روسیه را برعهده دارد.

۷ یافته‌های تحقیق

پس از تعیین متن اسناد راهبردی شناسایی‌شده –به‌عنوان واحد تحلیل– محقق نسبت به تدوین مقوله‌ها و زیرمقوله‌های اسناد پرداخته و متغیرهای پژوهش از این طریق شناسایی شده‌است. این نتایج در قالب جدول ۴ ملاحظه می‌شود. جهت تحلیل اسناد ۳۸ مقوله اختصاص داده شده است. هر یک از مقوله‌ها دارای یک یا چند واحد ثبت است. با شناسایی پیام‌ها و گزاره‌های کلیدی موجود در مقاله‌ها و کُدگذاری داده‌ها امکان بررسی و تحلیل فراهم شده‌است. در بررسی واحدهای تحلیل، ۴۲۵ زیرمقوله شناسایی گردید. سپس در جلسات خبرگی این زیرمقوله‌ها مورد بازبینی قرارگرفته، کُدگذاری شده و در ۳۸ مقوله سازماندهی شده‌اند. نتایج این فعالیت در قالب جدول ۴ ارائه شده‌است.

جدول ۴: کُدگذاری داده واحدهای تحلیل

ردیف	مقوله	فراوانی
۱	حق تعریف اطلاعات و داده‌های شخصی	۳۳
۲	مسئولیت‌پذیری	۳۳
۳	محدودیت در پردازش اضافه‌تر	۳۱
۴	حفظ کیفیت اطلاعات	۳۱
۵	حق اعلام جمع‌آوری	۳۰
۶	حق حمل و نقل داده‌ها	۳۰
۷	حق اعلان نقض اطلاعات	۳۰
۸	محدودیت پردازش و استفاده	۳۰
۹	اعلان نقض در داده‌ها	۳۰
۱۰	اطلاعات شخصی حساس	۳۰
۱۱	مشخص نمودن هدف از پردازش	۲۹

[27] FinCERT

ردیف	مقوله	فراوانی
۱۲	الزام مسئول حفظ داده‌ها	۲۸
۱۳	حفظ محدودیت‌های انتقال داده‌های مرزی	۲۸
۱۴	عدم استفاده در بازاریابی مستقیم	۲۸
۱۵	حق تعریف داده‌های حساس	۲۷
۱۶	محدودیت در جمع‌آوری داده	۲۷
۱۷	انجام اقدامات امنیتی و استفاده از اشخاص ثالث	۲۷
۱۸	حق انتقال اطلاعات	۲۴
۱۹	مشارکت‌دادن و ایجاد دسترسی برای موضوع داده	۲۴
۲۰	حفظ حریم خصوصی آنلاین	۲۴
۲۱	باز بودن داده‌ها	۲۳
۲۲	حق درخواست دسترسی	۲۱
۲۳	استفاده و افشای داده	۱۸
۲۴	حفظ امنیت داده‌ها	۱۸
۲۵	حق حفظ حریم خصوصی آنلاین	۱۸
۲۶	نگهداری و از بین‌بردن داده‌ها	۱۷
۲۷	انتقال اطلاعات	۱۷
۲۸	حفظ کیفیت اطلاعات	۱۷
۲۹	محدودیت پردازش و استفاده	۱۷
۳۰	مشخص‌بودن هدف از جمع‌آوری داده‌ها	۱۷
۳۱	عدم پردازش بیش از توافق اولیه	۱۶
۳۲	مشخص‌بودن و اعلام نحوه جمع‌آوری	۱۵
۳۳	اعلام تغییر در داده‌های جمع‌آوری‌شده	۱۵
۳۴	عدم جمع‌آوری بیش از توافق اولیه	۱۵
۳۵	حق درخواست تعلیق پردازش	۱۵
۳۶	باز بودن داده‌ها	۱۴
۳۷	حق فراموش‌شدن	۱۴
۳۸	مأمور محافظت از داده	۱۳

در ادامه، با شناسایی گزاره‌های راهبردی کلیدی در متن اسناد و کُدگذاری داده‌ها امکان بررسی و تحلیل راهبردها فراهم شده است. همانطور که در جدول ۵ مشاهده می‌شود، ۳۸ مقوله شناسایی‌شده در قالب ۳ موضوع راهبردی اصلی دسته‌بندی شده است و فراوانی موضوعات راهبردی نشان داده شده‌است. باید توجه داشت که موضوعات راهبردی معرف محورهای تعریف اصول و الزامات کلان، راهبردها و خط‌مشی‌های حفاظت از داده در اسناد و مقررات سایر کشورها بوده‌است.

۸ ارزیابی و صحت‌سنجی یافته‌های تحقیق

یکی از بهترین روش‌ها برای سنجش روایی، کسب نظر خبرگان است. در این پژوهش و برای تأیید اسناد ورودی جهت تحلیل محتوا از یک پنل خبرگی ۶ نفره با حضور اعضای هیات علمی و خبرگان حوزه فناوری در پژوهشگاه ارتباطات و فناوری اطلاعات، دانشگاه تهران، دانشگاه شهید بهشتی و دانشگاه علم و صنعت استفاده شده‌است. این افراد طی سال‌های ۱۳۹۷ تا ۱۳۹۸ مسئولیت مجری‌گری و راهبری ۶ پروژه کاربردی و راهبردی در حوزه تنظیم‌گری در حوزه ارتباطات و فناوری اطلاعات را برعهده داشته‌اند. در این راستا، جلسات مستمری تشکیل و اعتبار اسناد ورودی برای انجام تحلیل به تأیید خبرگان رسیده است.

جدول ۵: مقوله‌بندی و تبیین موضوعات راهبردی

موضوع راهبردی	گزاره راهبردی (مقوله)	فراوانی
داده	جمع‌آوری و اعلام	۱۹۶
	استفاده و افشای داده	
	تگهداری و از بین بردن داده‌ها	
	حفظ امنیت داده‌ها	
	اعلان نقض در اطلاعات	
	انتقال اطلاعات	
	باز بودن داده‌ها	
	حفظ کپیت اطلاعات	
	محدودیت در پردازش و استفاده	
	مشخص بودن هدف از جمع‌آوری داده‌ها	
	محدودیت در پردازش اضافی	
کاربر	حق تعریف اطلاعات و داده‌های شخصی	۲۴۲
	حق حفظ حریم خصوصی افراد	
	حق تعریف داده‌های حساس	
	حق اعلام جمع‌آوری	
	حق فراموش شدن	
	حق درخواست دسترسی	
	حق درخواست تعلیق پردازش	
	حق حمل و نقل داده‌ها	
	حق اعلان نقض اطلاعات	
	حق انتقال اطلاعات	
سازمان کنترل کننده	مامور محافظت از داده	۴۳۶
	مسئولیت‌پذیری	
	محدودیت پردازش و استفاده	
	عدم جمع آوری بیش از توافق اولیه	
	مشخص نمودن هدف از پردازش	
	عدم پردازش بیش از توافق اولیه	
	باز بودن داده‌ها	
	حفظ کپیت اطلاعات	
	ایجاد اقدامات امنیتی و استفاده از اشخاص ثالث	
	مشارکت دادن و ایجاد دسترسی برای موضوع داده	
	الزام مسئول حفظ داده‌ها	
	اعلام تغییر در داده های جمع آوری شده	
	حفظ محدودیت‌های انتقال داده‌های مرزی	
	عدم استفاده در بازاریابی مستقیم	
	حفظ حریم خصوصی افراد	
	پردازش اطلاعات شخصی حساس	

برای سنجش پایایی در فضای تحقیق حاضر نیز روش‌های متفاوتی معرفی شده‌است که توافق درصدی، روش هولستی و... از عمده این موارد هستند [۲۰]. در این روش‌ها می‌توان کُدگذاری‌ها را به دو صورت تکرار نمود: یا کُدگذاری توسط خود پژوهشگر با فاصله زمانی معناداری انجام می‌شود؛ و یا درخواست از فرد دیگری که دارای تخصص مشابه است خواسته می‌شود که نتایج حاصله را مقایسه کند [۱۶]. در این پژوهش برای تعیین پایایی کُدگذاری‌های اسناد از ضریب درون موضوعی کاپا[۲۸] – برای کُدگذاری توسط فرد خبره و مقایسه آن نتایج به‌دست آمده – استفاده شده‌است. از طریق این ضریب می‌توان میزان توافق دو اندازه‌گیری را ارزیابی نمود [۲۰]. با توجه به مراتب اعتمادپذیری مقادیر گوناگون ضریب کاپا در تعیین میزان توافق بین کُدگذاری‌ها، نتیجه بالای 0.6 مقداری قابل قبولی محسوب می‌شود که در پژوهش حاضر نتیجه 0.62 حاصل شده که در سطح قابل‌قبول می‌باشد [۱۸][۲۲].

۹ تحلیل و استنباط پیرامون یافته‌های تحقیق

نتایج حاصل از بررسی سیر موضوعی اسناد راهبردی و فراوانی آن‌ها با ارائه جداولی مشخص شده‌است. در ادامه گرایش‌های اصلی راهبردی در اسناد مشخص و رویکرد کشورها در تدوین نظام ملی تنظیم مقررات و قوانین حفاظت از داده‌ها بیان شده‌است. همانطور که در جدول ۶ مشاهده می‌شود، در میان مقوله‌های شناسایی‌شده، بیشترین گزاره‌های راهبردی مربوطه به‌منظور شناسایی موضوعات راهبردی تعیین و در قالب جدول ۶ ارائه شده‌است.

[28] Interclass correlation Kappa

شکل ۲: اولویت و تمرکز موضوعات راهبردی در اسناد مطالعه‌شده

جدول ۶: مقوله مورد تمرکز و راهبرد مرتبط

اولویت	گزاره راهبردی (مقوله)	فراوانی	موضوع راهبردی مربوطه
۱	حق تعریف اطلاعات و داده‌های شخصی	۳۳	کاربر
۲	مسئولیت‌پذیری	۳۳	سازمان کنترل‌کننده
۳	محدودیت در پردازش اضافه‌تر	۳۱	سازمان کنترل‌کننده
۴	حفظ کیفیت اطلاعات	۳۱	سازمان کنترل‌کننده
۵	حق اعلام جمع‌آوری	۳۰	کاربر
۶	حق حمل و نقل داده‌ها	۳۰	کاربر
۷	حق اعلان نقض اطلاعات	۳۰	کاربر
۸	محدودیت پردازش و استفاده	۳۰	سازمان کنترل‌کننده
۹	اعلان نقض در داده‌ها	۳۰	داده
۱۰	پردازش اطلاعات شخصی حساس	۳۰	سازمان کنترل‌کننده

همچنین با توجه به نتایج به‌دست آمده، اولویت و تمرکز موضوعات راهبردی – براساس مجموع فراوانی گزاره‌های راهبردی (مقوله‌ها) در اسناد – به ترتیب در قالب شکل ۲ به‌تصویر کشیده شده‌است.

به منظور بررسی رویکرد مورد تمرکز در اسناد راهبردی ملی، محقق مقوله‌ها/ گزاره‌های راهبردی برجسته در هر نمونه موردی را به تفکیک واحدهای تحلیل در قالب جدول ۸ ارائه نموده‌است.

با بررسی رویکرد کشورها در موضوعات راهبردی شناسایی شده در اسناد و بررسی نتایج تحلیل کیفی مندرج در جدول ۸، مشاهده می‌شود که گزاره‌های راهبردی (مقوله‌های) ذیل بیش از ۵۰ درصد واحدهای تحلیل تکرار و مورد تاکید بوده است. تکرارپذیری این مقوله‌ها بیانگر اهمیت این موضوعات در امر برنامه‌ریزی و اخذ استراتژی‌های در امر توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف را نشان می‌دهد.

تحلیل بین‌موردی و درون موردی راهبردهای توسعه قوانین و مقررات حفاظت از داده‌های عمومی در نمایی متفاوت و به تفکیک واحدهای تحلیل در قالب جدول (۵) ارائه شده‌است. بررسی میزان تکرار و توجه به راهبردها در کشورهای مختلف بیانگر آن است که میزان توجه به مقوله‌ها در کشورهای مختلف، متفاوت است.

بررسی مقوله‌های ۳۸گانه در کشورهای منتخب که به بیش از ۲۰ مورد از مقوله‌ها توجه کرده‌اند، نشان می‌دهد اکثر کشورها به رعایت مقوله‌ها در قوانین و مقررات حفاظت دادهٔ کشور خود اهمیت داده‌اند. در عین حال مقولهٔ استفاده از مأمور حفاظت از داده که ناظر به اجرای دقیق در سمت کنترل‌کننده‌ها است، به علت

ایجاد بار اجرایی کمتر مورد توجه بوده است و در واقع فقط ۷ مورد از کشورها و یا به عبارت دیگر نیمی از کشورهای منتخب به آن توجه کرده‌اند.

جدول ۷: گزاره‌های راهبردی / مقوله مورد تمرکز به تفکیک واحدهای تحلیل

واحد تحلیل	مقوله مورد تمرکز	واحد تحلیل	مقوله مورد تمرکز
امریکا	• حق تعریف اطلاعات و داده‌های شخصی • مسئولیت‌پذیری • محدودیت پردازش و استفاده • حق اعلان نقض اطلاعات • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • محدودیت در پردازش اضافه‌تر • حق اعلام جمع‌آوری	کانادا	• محدودیت پردازش و استفاده • مسئولیت‌پذیری • پردازش اطلاعات شخصی حساس • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • محدودیت در پردازش اضافه‌تر • حق اعلام جمع‌آوری
اتحادیه اروپا	• حق تعریف اطلاعات و داده‌های شخصی • مسئولیت‌پذیری • محدودیت پردازش و استفاده • حق اعلان نقض اطلاعات • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • محدودیت در پردازش اضافه‌تر • حق اعلام جمع‌آوری	کره جنوبی	• حق تعریف اطلاعات و داده‌های شخصی • مسئولیت‌پذیری • محدودیت پردازش و استفاده • حق اعلان نقض اطلاعات • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق اعلام جمع‌آوری
روسیه	• محدودیت پردازش و استفاده • مسئولیت‌پذیری • پردازش اطلاعات شخصی حساس • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری	ژاپن	• مسئولیت‌پذیری • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق اعلام جمع‌آوری

واحد تحلیل	مقوله مورد تمرکز	واحد تحلیل	مقوله مورد تمرکز
اسپانیا	• مسئولیت‌پذیری • حق تعریف اطلاعات و داده‌های شخصی • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری	سنگاپور	• مسئولیت‌پذیری • حق تعریف اطلاعات و داده‌های شخصی • محدودیت پردازش و استفاده • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری
تایوان	• مسئولیت‌پذیری • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری	هند	• مسئولیت‌پذیری • پردازش اطلاعات شخصی حساس • اعلان نقض در داده‌ها • محدودیت پردازش و استفاده • حق اعلام جمع‌آوری
فرانسه	• حق تعریف اطلاعات و داده‌های شخصی • محدودیت پردازش و استفاده • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری	نروژ	• مسئولیت‌پذیری • حق اعلان نقض اطلاعات • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق حمل و نقل داده‌ها • حق اعلام جمع‌آوری
نیجریه	• حق اعلان نقض اطلاعات • محدودیت پردازش و استفاده • حق اعلام جمع‌آوری	استرالیا	• حق تعریف اطلاعات و داده‌های شخصی • مسئولیت‌پذیری • محدودیت پردازش و استفاده • اعلان نقض در داده‌ها • حق اعلام جمع‌آوری

در بخش‌های مختلف بیشترین توجه کشورها به جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس معطوف بوده‌است.

در حوزه توجه به مقوله‌هایی که در دسته‌بندی «داده» قرار می‌گیرند، بیشترین توجه به جمع‌آوری و اعلام (۱۴ مورد)، اعلان نقض در اطلاعات (۱۳ مورد)، محدودیت پردازش و استفاده (۱۴ مورد) و محدودیت در جمع آوری داده (۱۴ مورد) بوده است. در این بخش کمترین توجه به مقوله نگهداری و از بین بردن داده‌ها

جدول ۸: بررسی مقولات به تفکیک واحدهای تحلیل در کشورهای منتخب

مقوله ها / کشورها	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱	۳۲	۳۳	۳۴	۳۵	۳۶	۳۷	۳۸	میزان توجه به مقولات در کشورهای منتخب
	جمع آوری و اعلام	استفاده و افشای داده	نگهداری و از بین بردن داده ها	حفظ امنیت داده ها	اعلان نقض در اطلاعات	انتقال اطلاعات	باز بودن داده ها	حفظ کیفیت اطلاعات	محدودیت پردازش و استفاده	محدودیت در جمع آوری داده	مشخص بودن هدف از جمع آوری داده ها	محدودیت در پردازش اضافه تر	حق تعریف اطلاعات و داده های شخصی	حق حفظ حریم خصوصی آنلاین	حق تعریف داده های حساس	حق اعلام جمع آوری	حق درخواست دسترسی	حق فراموش شدن	حق درخواست تعلیق پردازش	حق حمل و نقل داده ها	حق اعلان نقض اطلاعات	حق انتقال اطلاعات	مأمور محافظت از داده	مسئولیت پذیری	محدودیت پردازش و استفاده	عدم جمع آوری بیش از توافق اولیه	مشخص نمودن هدف از پردازش	عدم پردازش بیش از توافق اولیه	حفظ کیفیت اطلاعات	باز بودن داده ها	انجام اقدامات امنیتی و استفاده از اشخاص ثالث	مشارکت دادن و ایجاد دسترسی برای موضوع داده	الزام مسئول حفظ داده ها	اعلام تغییر در داده های جمع آوری شده	حفظ محدودیت های انتقال داده های مرزی	عدم استفاده در بازاریابی مستقیم	حفظ حریم خصوصی آنلاین	پردازش اطلاعات شخصی حساس	
امریکا	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	۳۶
کانادا	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	۳۷
اتحادیه اروپا	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	۳۷
کره جنوبی	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	۳۴
روسیه	✓	×	✓	×	×	✓	×	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	×	✓	×	×	✓	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	✓	۲۰
اسپانیا	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	۳۱
ژاپن	✓	×	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	✓	✓	۳۱
تایوان	✓	×	×	×	✓	✓	×	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×	✓	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	۲۸
سنگاپور	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×	✓	✓	×	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	۲۹
فرانسه	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	✓	✓	✓	۲۸
نروژ	✓	✓	×	✓	✓	×	×	×	✓	✓	×	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	✓	×	×	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓	۲۶
نیجریه	✓	×	×	✓	✓	✓	×	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	✓	×	✓	✓	✓	×	×	✓	✓	✓	×	✓	✓	۲۵
هند	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓	×	×	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓	۳۰
استرالیا	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	✓	×	✓	×	✓	✓	×	✓	×	✓	✓	✓	×	✓	✓	✓	×	✓	✓	۲۹
فراوانی مقوله در کشورهای منتخب	۱۴	۹	۸	۱۰	۱۳	۱۱	۹	۱۰	۱۴	۱۴	۹	۱۰	۱۴	۱۰	۹	۱۴	۱۳	۹	۱۰	۹	۱۰	۱۳	۷	۱۴	۱۰	۱۱	۱۰	۱۳	۹	۱۱	۸	۹	۱۳	۱۳	۱۳	۱۱	۱۳	۱۴	

(با ۸ مورد) بوده است. در حوزه توجه به مقوله‌هایی که در دسته‌بندی «کاربر» قرار می‌گیرند، بیشترین توجه به حق تعریف اطلاعات و داده‌های شخصی (۱۴ مورد)، حق اعلام جمع‌آوری (۱۴ مورد)، حق درخواست دسترسی (۱۳ مورد) و حق انتقال اطلاعات (۱۴۳ مورد) بوده است.

در حوزه توجه به مقوله‌هایی که در دسته‌بندی «سازمان کنترل‌کننده» قرار می‌گیرند، بیشترین توجه به مسئولیت‌پذیری (۱۴ مورد)، پردازش اطلاعات شخصی حساس (۱۴ مورد)، حفظ حریم خصوصی آنلاین (۱۳ مورد)، الزام مسئول حفظ داده‌ها (۱۳ مورد) و حفظ محدودیت‌های انتقال داده‌های مرزی (۱۳ مورد) بوده است. در این بخش کمترین توجه به مقولهٔ مأمور محافظت از داده (۷ مورد) و انجام اقدامات امنیتی و استفاده از اشخاص ثالث (۸ مورد) بوده است. از سوی دیگر در بین کشورهای منتخب کانادا، اتحادیه اروپا (در قوانین جدید GDPR)، امریکا و کره جنوبی بیشترین توجه را به مقوله‌های حفاظت از داده‌ها داشته‌اند. از سوی دیگر روسیه و نیجریه در ابتدای راه طراحی و اجرای سیاست‌ها و قوانین مربوط به حفاظت از داده‌ها بوده و در حال توسعهٔ آن‌ها هستند.

۱۰ جمع‌بندی و نتیجه‌گیری

براساس 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 داده‌ها، مفاهیم متعددی در کشورهای مختلف مورد توجه واقع شده است. با توجه بررسی کشورهای مختلف، در جدول زیر مهمترین مفاهیم مورد توجه در کشورهای مختلف

شکل ۳: چارچوب مفهومی اقدامات کلان

در قالب یک مدل مرجع دسته‌بندی شده است. در ادامه یافته‌های تحلیل مورد واکاوی قرار گرفت تا مورد توافق و اجتماع خبرگان قرار گیرد. نتایج این پژوهش و اشباع نظری تحت عنوان «چارچوب مفهومی اقدامات کلان» در قالب شکل ۳ ارائه شده‌است.

همانطور که مشاهده می‌شود نتایج برآمده از تحلیل اسناد، به سه موضوع راهبردی بنیادی برای سیاست‌گذاری منتج شد که ملاحظات سیاست‌گذاران و نیز اقتضائات و نیازهای توسعه قوانین و مقررات حفاظت از داده‌های عمومی در کشورهای مختلف را پوشش می‌دهد. در این بین تحلیل یافته‌ها براساس تحلیل محتوای انجام‌شده اهمیت توجه به مقوله‌هایی چون جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس را نشان می‌دهد.

آنچه بیش از مدل تبیین شده حایز اهمیت است، نحوه اجرایی ساختن این موضوعات راهبردی است که افزون بر پاره‌ای رویکردهای شناختی و ملاحظات فناورانه، مستلزم توجه به بلوغ ساختاری و سیاست‌گذارانه در حوزه فناوری است که چالش عمده بسیاری از کشورهای توسعه‌یافته در این زمینه محسوب می‌شود. وزن این موضوعات از یک کشور به کشور دیگر دستخوش تغییر می‌شود. به‌عنوان مثال، در کشور ایران به‌واسطه وجود قوانین و مقررات خاص و ساختار حاکمیتی خاص کشور، مطمئناً مقوله‌های تحقیق و توسعه و نیز تنظیم و اعمال مقررات (با نگاه رگولاتوری و سازماندهی اکوسیستم) در اولویت قرار خواهند گرفت. در واقع، چارچوب مفهومی پیشنهادی –برگرفته از بررسی مقایسه‌ای راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌های عمومی– می‌تواند در نقش ساختار پشتیبان تصمیم و نیز پرتفوی خط‌مشی‌های کلان، راهبردها و نیز اقدامات کلان برای تدوین نقشه‌راه و نیز سیاست‌گذاری‌های این حوزه کاربرد داشته باشد.

بنابراین، فرموله نمودن نقشه راهبردی تدوین قوانین و مقررات حفاظت از داده‌های عمومی کشور و تدوین حوزه‌های کاربردپذیر می‌تواند به‌عنوان فعالیت‌های آتی پیشنهادی پژوهش حاضر مدنظر قرار گیرند.

مراجع

[1] Tamburri, D. A. Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 2019.

[2] Slepchuk, Alec N. and Milne, George R. Informing the design of better privacy policies. *Privacy and disclosure, online and in social interactions*, 2019.

[3] Sana, S. and Tahar, K. Sensitive and private data analysis: A systematic review. *ICFNDS*, 2019.

[4] Purtova, N. The law of everything. broad concept of personal data and future of eu data protection law. *Law, Innovation and Technology*, 2018.

[5] Van O., I. and U. V., Helena. Does the GDPR enhance consumers' control over personal data? an analysis from a behavioural perspective. *Journal of Consumer Policy. Springer.*, 2018.

[6] Gauthier, Ch. The impact of the eu general data protection regulation on scientific research. *Ecancermedicalscience*, 2017.

[7] Clarke, R. Privacy impact assessment: Its origins and development. *Computer law and security review*, 2009.

[8] Clarke, R. An Evaluation of Privacy Impact Assessment Guidance Documents. *International Data Privacy Law*, 1(2): 111-120, 2011.

[9] Commission Nationale de l'Informatique et des Libertes (CNIL). Privacy Impact Assessment (PIA) Methodology, 2015. URL: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

[10] European Commission. Special Eurobarometer 423 Cyber Security. Report 978 DR-01-15-143-EN-N, European Commission, 2015.

[11] ISO/IEC 29134 information technology – security techniques — privacy impact assessment – guidelines.

[12] Oetzel, M.C. and Spiekermann, S. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 2014.

[13] Office of the Australian Information Commissioner. *Guide to undertaking privacy impact assessments*, 2014.
URL: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

[14] Markos, E., Milne, GR., and Peltier, JW. Information sensitivity and willingness to provide continua: acomparative privacy study of the united states and brazil. *JPublic Policy Mark*, 2017.

[15] Saadatmand, F. A. S. Configurations of platform organizations: Implications for complementor engagement. 2019.

[16] Zhang, Yan. Qualitative analysis of content. 1966.

[17] H. H.-F. a. S. SE. Three approaches to qualitative content analysis. 2005.

[18] Ghorra-Gobin, C. The comparative social science approach. 2008.

[19] Shejy, G. Data privacy and security in social networks. *Smart Innovation, Systems and Technologies*, 2020.

[20] Hsieh, Hsiu-Fang and Shannon, Sarah E. Three approaches to qualitative content analysis. *Qual Health Res.*, 2005.

[21] Ko, M. J. and Lim, T. H. *Journal of the Korean Medical Association*, 2020.

[22] P. and Baxter, J. S. Qualitative case study methodology. *Study design and implementation for novice researchers*, 2008.