مرکز پژوهش‌های مجلس شورای اسلامی
دفتر مطالعات مدیریت
مسلسل: ۲۰۴۲۰ ■ بهمن ۱۴۰۳

مطالعه تطبیقی قوانین و استانداردهای مرتبط با زنجیره ارزش داده در کشورهای منتخب


بسم الله الرحمن الرحيم

تاریخ انتشار:
۱۴۰۳/۱۱/۳۰

شماره مسلسل: ۲۰۴۲۰
کد موضوعی: ۲۹۰

مرکز پژوهش‌های مجلس شورای اسلامی

عنوان گزارش:
مطالعه تطبیقی قوانین و استانداردهای مرتبط با زنجیره ارزش داده در کشورهای منتخب

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

نام دفتر:
دفتر مطالعات مدیریت (گروه دولت الکترونیک و مدیریت داده)

تهیه و تدوین‌کنندگان:
محمدحسن طایفی نصرآبادی، اسمهان حکاک، عطیه یوسفی (مطالعات حکمرانی) ابوالقاسم یوسفی بابادی

مدیر مطالعه:
یحیی مرتب، سپیده شفیعا

ناظران علمی:
مهدی عبدالحمید، محمد عبدالحسین‌زاده (عضو هیئت علمی دانشگاه علم و صنعت)

اظهارنظرکننده:
سیدمجتبی شهرآیینی (مطالعات مدیریت)، اسماعیل عبدی، فهمیه محمدی هارونی (مطالعات بنیادین حکمرانی)، ابوالقاسم رجبی (مطالعات انرژی، صنعت و معدن)، یحیی مزروعی ابیانه (مطالعات حقوقی)

گرافیک و صفحه‌آرایی:
حمیده سادات وفایی
ساجده زارع مرزی

ویراستار ادبی:
مژگان کاظمی

تاریخ شروع مطالعه:
۱۴۰۳/۰۵/۰۱

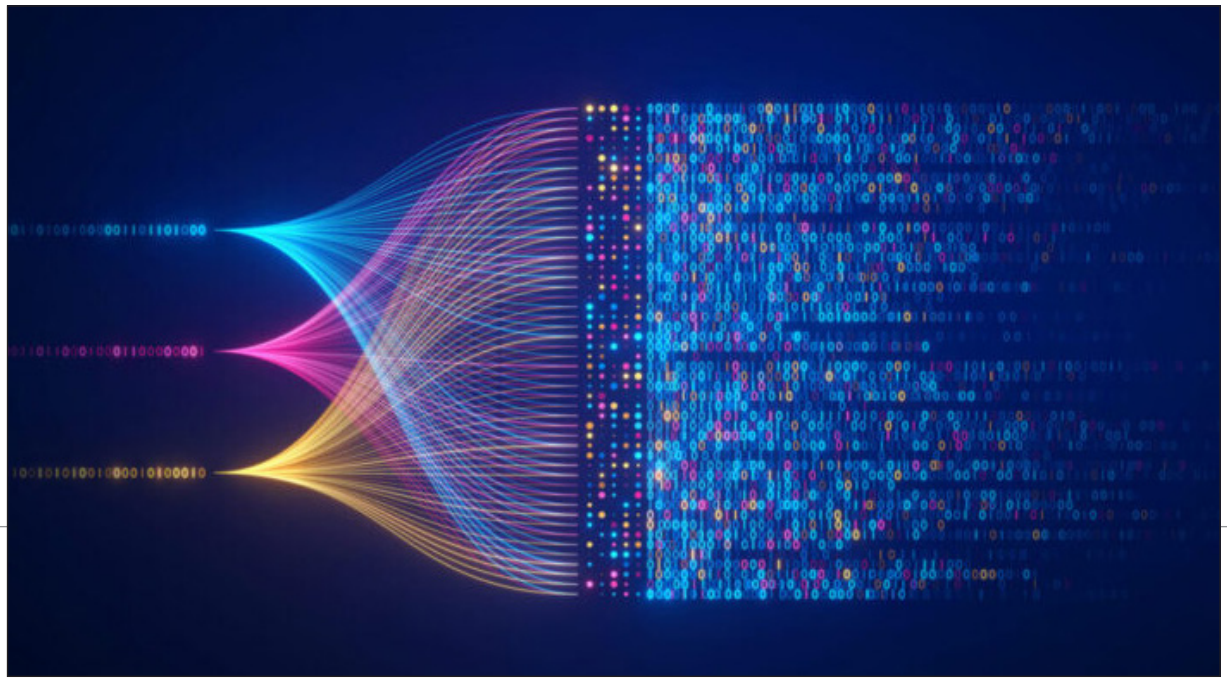
واژه‌های کلیدی:
۱. زنجیره تأمین داده
۲. یکپارچگی داده
۳. متولی داده
۴. توزیع داده
۵. امنیت اطلاعات

دفتر مطالعات مدیریت

فهرست مطالب

فهرست شکل ها

فهرست جداول



مطالعه تطبیقی قوانین و استانداردهای مرتبط با زنجیره ارزش داده در کشورهای منتخب

چکیده

داده و اطلاعات در توسعه کشـــورها و ایجاد مزیت رقابتی برای آنها نقش کلیدی دارند. ناتوانی در مدیریت داده همانند ناتوانی در مدیریت سرمایه به شمار رفته که نتیجه آن اتلاف منابع و از دست رفتن فرصت‌ها خواهد بود. یکی از اقدامات مهم در راستای مدیریت داده‌ها در کشور، سامان‌دهی به چرخه حیات داده‌ها، از ایجاد یا دریافت داده تا استفاده و در نهایت انهدام یا بایگانی آنهاست. چنین فرایندی در ادبیات با عنوان زنجیره ارزش داده شناخته می‌شـــود. **زنجیره ارزش داده**، چارچوبی را برای ایجاد سیاست‌های حکمرانی داده، تضمین کیفیت داده‌ها و حفظ امنیت و حریم خصوصی داده‌ها، که برای حفظ اعتماد و انطباق بسیار مهم هستند، فراهم می‌کند.

با توجه به ضرورت پرداختن به زنجیره ارزش داده در ایران با هدف ایجاد زیربنایی برای سامان‌دهی به جریان داده در کشور، پژوهش حاضر در نظر دارد با بررسی زنجیره ارزش داده در ۶ کشور کانادا، استرالیا، سنگاپور، مکزیک، انگلیس و نیوزلند و احصای استانداردها و قوانین حاکم در آن کشورها، سازوکاری را برای مقایسه زیست‌بوم داده در ایران و کشورهای مذکور فراهم کرده و چارچوبی را برای سامان‌دهی به جریان داده در کشور ارائه کرده است.

خلاصه مدیریتی

بیان / شرح مسئله

درنتیجه تبدیل فناوری‌ها و سیستم‌های نرم‌افزاری به ابزاری برای ارائه و تسهیل خدمات در بخش‌های مختلف صنعتی، اقتصادی، بهداشتی، حجم عظیمی از داده و اطلاعات تولید شده‌اند که مدیریت آنها امری کلیدی و حائز اهمیت در حکمرانی کشور است. ازاین‌رو، تعیین راهبرد مناسب برای تسهیل جریان داده در کشور ضروری بوده و امروزه به شاخصی برای سنجش قوت و ضعف هر کشور در مدیریت داده‌ها و اطلاعات خود تبدیل شده است. طراحی استراتژی‌های مناسب برای جریان داده در کشور نیازمند سامان‌دهی به مراحل مختلف حیات داده نظیر تولید داده، جمع‌آوری داده‌ها، ذخیره‌سازی داده‌ها و غیره است که ضرورت پرداختن به موضوع **زنجیره ارزش داده** را مشخص می‌کند. بررسی شرایط فعلی حاکم در کشور در زمینه چگونگی مدیریت زنجیره ارزش داده و قیاس آن با سایر کشورها، چارچوبی را برای سامان‌دهی به مراحل مختلف حیات داده فراهم می‌آورد.

نقطه نظرات / یافته‌های کلیدی

بررسی رویه‌ها، قوانین و مقررات موجود در جهان در نحوه مواجهه با موجودیتی به‌نام داده و اطلاعات نشان از آن دارد که بسیاری از کشورها و سازمان‌های بین‌المللی از سال‌ها قبل به اهمیت این موضوع پی برده و شیوه تعامل، قوانین و مقررات بالادستی مناسبی را در این زمینه تدارک دیده و در حال توسعه و به‌روزرسانی آنها هستند. با توجه به اهمیت داده‌ها و اطلاعات در توسعه تمامی زمینه‌های حکمرانی به‌ویژه حوزه فناوری، وجود چنین قوانین و مقرراتی، می‌تواند به جنبه‌ای از اقتدار در این کشورها اشاره کند.

پیشنهاد راهکارهای تقنینی سیاستی

در ایران قدم‌های اولیه‌ای به‌منظور سامان بخشیدن به نحوه مواجهه با حجم داده‌ها و اطلاعاتی که روزانه در حال تولید و انتشار هستند، برداشته شده است، اما این اقدام‌ها همچنان در مراحل اولیه خود هستند که از این میان می‌توان به قانون مدیریت داده‌ها و اطلاعات ملی اشاره کرد. اما با توجه به وضع موجود و فقدان یکپارچگی در زمینه مدیریت داده‌ها و اطلاعات، چه در بخش‌های دولتی و عمومی و چه در بخش خصوصی، نیاز است تا یک سازوکار جامع و عملیاتی در زمینه سامان‌دهی به فضای داده‌ها و اطلاعات در کشور طراحی شود. در این گزارش ویژگی‌های مورد نیاز برای طراحی چنین سازوکاری با جزئیات بیان شده است.

۱. مقدمه

امروزه ارزش داده و اطلاعات در کشورها به حدی بالاست که آن را برابر با دارایی‌های ارزشمندی همچون نفت می‌دانند، زیرا همان‌گونه که می‌توان از نفت در راستای توسعه کشور و کسب‌وکارهای موجود استفاده کرد از داده و اطلاعات نیز می‌توان در همین جهت بهره‌های فراوانی به‌دست‌آورد. در عصر اطلاعات، سیاستگذاری برای داده از یک اقدام لوکس به یک نیاز ضروری و محوری برای تمامی فعالیت‌ها تبدیل شده است. در چند سال اخیر و به مدد رشد رسانه‌های اجتماعی، گوشی‌های هوشمند، حسگرها و سایر فناوری‌های حوزه اینترنت اشیا، صفحات وب و نیز توسعه نرم‌افزارهای سازمانی، نرخ تولید داده و به‌تبع آن حجم داده‌ها با جهش عظیمی مواجه شده است؛ داده‌هایی که علاوه‌بر نیاز به ذخیره و پردازش، نیازها و ضرورت‌های جدیدی را هم با خود به ارمغان آورده‌اند.

ارزش‌آفرینی از داده‌ها همچون هر سرمایه دیگری نیازمند تبیین سازوکارها، استانداردها و قوانین مناسب برای جریان این سرمایه ارزشمند، از تولید تا انهدام تا بایگانی آن است که ضرورت پرداختن به مفهوم زنجیره ارزش داده را مشخص می‌کند. زنجیره ارزش داده[1] به مجموعه‌ای از مراحل و فرایندهای دخیل در تبدیل داده‌های خام به بینش‌های ارزشمند اشاره دارد [۱]. سامان‌دهی به زنجیره ارزش

1.Data Value Chain

داده نیازمند طراحی قوانین و استانداردهایی برای بخش‌های مختلف این فرایند نظیر تولید، جمع‌آوری و ذخیره‌سازی داده‌هاست.
با توجه به ضرورت پرداختن به مفهوم زنجیره ارزش و درنتیجه توسعه سیستم‌های اطلاعات مدیریت و افزایش روزافزون داده و اطلاعات تولید شده در این سیستم‌ها، از سال ۱۹۷۰، در اغلب کشورهای صنعتی، قوانین و مقرراتی برای سامان‌دهی به بخش‌های مختلف زنجیره ارزش داده و اطلاعات تدوین شده است. از سال ۲۰۰۰ به بعد نیز، تصویب قوانینی در راستای تکمیل قوانین اولیه و با هدف تحکیم چارچوب‌های حفاظت امنیت و حفظ حریم‌های خصوصی، در دستور کار دولت‌ها قرار گرفته است [۲].
علاوه‌بر اهمیت سامان‌دهی به جریان اطلاعات در سطح حاکمیت، تحقق کامل دولت الکترونیک به‌عنوان یکی از عوامل مهم در تسهیل خدمت‌رسانی دستگاه‌های اجرایی و افزایش رضایت‌مندی شهروندان نیز از بُعدی دیگر، ضرورت پرداختن به مفهوم زنجیره ارزش داده را مشخص می‌کند. تحقق کامل دولت الکترونیک، مستلزم وجود سامانه‌های مجتمع اطلاعاتی در تمامی بخش‌های عمومی و دولتی است. بنابراین با توسعه چنین سامانه‌هایی نیازمندی‌هایی همچون چگونگی نگهداری و یکپارچه‌سازی داده‌های تولید شده، چگونگی تبادل داده‌ها بین سامانه‌ها، چگونگی کنترل امنیت و صحت داده‌های تولید شده، چگونگی محافظت از حریم خصوصی و چگونگی افشای داده‌ها به‌وجود می‌آیند [۳].
در سطح جهانی تعدادی دستورالعمل و چارچوب در حوزه سامان‌دهی به بخش‌های مختلف زنجیره ارزش داده توسط سازمان‌های جهانی ایجاد و در اختیار کشورها قرار داده شده است. از آن جمله می‌توان به دستورالعمل «سازمان همکاری و توسعه اقتصادی»[1] و «کمیسیون اقتصادی و اجتماعی سازمان ملل متحد برای آسیا، اقیانوسیه و اتحادیه اروپا»[2] اشاره کرد. در این دستورالعمل‌ها، روش‌های پیشنهادی برای مراحل مختلف جریان داده ارائه شده است. همچنین در برخی از کشورها نیز اقدام‌هایی برای پیاده‌سازی حکمرانی داده طراحی شده است. برای مثال، برزیل از سال ۲۰۱۳ به‌عنوان یکی از حامیان اصلی قطعنامه‌های سازمان ملل در مورد حکمرانی داده، میزبان دو کنفرانس چندجانبه در انجمن حکمرانی اینترنتی بوده است. این کشور، قانونی را با عنوان قانون مدنی اینترنت نیز به تصویب رسانده‌است که ارکان آن به‌عنوان مرجع بین‌المللی مورد بهره‌برداری قرار می‌گیرد [۴]. اتحادیه اروپا، چارچوب بسیار سخت‌گیرانه‌ای را برای حفظ حریم خصوصی و حفاظت از داده‌ها، با مقررات عمومی حفاظت از داده‌ها در مرکز آن، اتخاذ کرده است و «حق فراموش شدن» و «حق انتقال داده‌ها» را برای افزایش کنترل افراد روی اطلاعات خودشان معرفی کرده است [۵]. علاوه‌بر این، کمیسیون اتحادیه اروپا راهبردی را برای ارتقای استانداردهای بین‌المللی حفاظت از داده‌ها تعیین کرده است [۶]. حتی در این مورد می‌توان به قانون شفاف‌سازی استفاده قانونی از داده‌ها در خارج از کشور توسط آمریکا اشاره کرد [۷].
در ایران طی سال‌های اخیر تنظیم‌گران درصدد ایجاد چارچوبی مشخص و قانونی بر جریان داده‌ها بوده‌اند. از جمله طرح‌های ارائه شده در مجلس شورای اسلامی مرتبط با حوزه حکمرانی داده می‌توان به طرح «صیانت از حقوق کاربران در فضای مجازی و سامان‌دهی پیام‌رسان‌های اجتماعی» و نسخه جدیدتر آن تحت عنوان طرح «حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی»، طرح «حمایت از توسعه و رقابت‌پذیری پلتفرم‌های ارائه‌دهنده خدمات پایه و کاربردی شبکه ملی اطلاعات»، «قانون مدیریت داده‌ها و اطلاعات ملی» و طرح «الزام به انتشار داده و اطلاعات» اشاره کرد.
با وجود تلاش‌هایی که در کشور ایران برای سامان‌دهی به جریان داده صورت گرفته است، اما مشاهده می‌شود که همچنان زیست‌بوم داده در کشور با مشکلات متعددی مواجه است. بر این اساس، در گزارش حاضر تلاش شده است تا قواعد، قوانین و استانداردهای مرتبط با بخش‌های مختلف زنجیره ارزش داده در هفت کشور ۱. کانادا، ۲. استرالیا، ۳. سنگاپور، ۴. مکزیک، ۵. انگلیس، ۶. نیوزلند، ۷. کره‌جنوبی بررسی و با شرایط زیست‌بوم داده در کشور ایران قیاس شود. بررسی این قوانین و استانداردها و تطبیق آن یا شرایط فعلی در کشور می‌تواند زمینه‌ای را برای سامان‌دهی به خلأهای فعلی فراهم آورد.
شایان ذکر است، در فرایند انتخاب کشورهای منتخب تلاش شده است تا کشورهایی از طیف‌های اقتصادی، جغرافیایی و فرهنگی

1.Organisation for Economic Co-operation and Development (OECD)
2.Economic and Social Commission for Asia and the Pacific

متفاوت مورد بررسی قرار بگیرند تا محتوای احصا شده برای شرایط کشور ایران قابل تعمیم باشد. به‌عنوان مثال، کشورهای سنگاپور و مکزیک پس از دستیابی به استقلال در حکمرانی و بدون وابستگی به منابع کشورهای ضعیف‌تر در مدت زمانی کوتاه و منطقی، توانسته‌اند تغییرات اولیه‌ای قابل قبولی را در شرایط مدیریت داده‌ها و اطلاعات خود ایجاد کنند که از این منظر می‌توانند به‌عنوان الگوهای عملیاتی برای کشور ایران در نظر گرفته شوند.

۲. درآمدی بر زنجیره ارزش داده در کشورهای منتخب و قیاس آن با کشور ایران

در این بخش در گام نخست، به تشریح استانداردها و قوانین مرتبط با بخش‌های مختلف حیات داده در هفت کشور منتخب پرداخته و سپس وضعیت تنظیم‌گری در ایران در حوزه داده و اطلاعات تشریح خواهد شد. گفتنی است که پژوهش حاضر صرفاً بر اقدام‌های اجرایی و روش‌شناسی موضوع تمرکز کرده و اقدام‌های فنی مورد توجه قرار نگرفته است. همچنین، محتوای احصا شده از منابع اطلاعاتی مختلف نیز در قالب بخش‌های مختلف زنجیره ارزش داده شامل مراحل زیر ارائه شده است:

- **منابع تولید داده، تجمیع و یکپارچه‌سازی داده:** فرایندها و قوانین مرتبط با تولید، ثبت و نگهداری داده؛
- **پردازش داده:** فرایندهایی شامل انجام تغییرات، اقدامات تحلیلی و محاسباتی، ایجاد گزارش، تجمیع و تفکیک و به‌روزرسانی داده؛
- **امنیت داده:** شامل فرایندها و قوانین مرتبط با رعایت جوانب فنی واستراتژی‌های نگهداری داده؛
- **توزیع داده:** شامل فرایندها و قوانین مربوط به ایجاد دسترسی و روش‌های افشای داده‌ها.

علاوه‌بر موارد مذکور، تلاش شده است تا متولی زنجیره ارزش و قوانین موجود در کشورهای مذکور نیز بررسی شود.

۲-۱. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور کانادا

۲-۱-۱. منابع تولید داده

در کانادا پایگاه‌های داده باز،[1] جزء اصلی پایگاه‌های داده‌ای قابل انتقال به شمار می‌روند. در این کشور، منابع اطلاعاتی مختلفی ایجاد شده است که از این میان می‌توان به بانک داده اداره آمار کانادا، شورای ملی تحقیقات کانادا، تحقیق و توسعه دفاعی کانادا، دبیرخانه هیئت خزانه‌داری کانادا، آژانس بهداشت عمومی کانادا، آژانس بازرسی مواد غذایی کانادا، بانک اطلاعاتی باز محیط زیست و تغییرات آب و هوایی، ساختمان‌ها، مراکز آموزشی، مراکز درمانی، مراکز فرهنگی و هنری، اطلاعات حمل‌ونقل کانادا، منابع‌طبیعی، شیلات و اقیانوس‌ها در کانادا و شبکه کتابخانه‌های علمی فدرال اشاره کرد. اغلب این منابع داده به‌صورت باز منتشر شده و برخی دیگر در حال آماده‌سازی جهت انتشار برای عموم هستند [۸].

۲-۱-۲. نحوه جمع‌آوری و یکپارچه‌سازی داده

در این کشور از روش‌های مختلفی برای جمع‌آوری داده‌ها استفاده می‌شود. از استفاده از ابزارهای ساده‌ای همچون نظرسنجی تا جمع‌آوری داده‌های اداری و داده‌های کلان با استفاده از هوش‌مصنوعی، گستره شناسایی شده در زمینه ابزارهای جمع‌آوری داده‌ها در کشور کاناداست [۹ و ۱۰].

همچنین در این کشور، از روش‌های متعددی برای ادغام داده‌ها از منابع مختلف اطلاعاتی استفاده می‌شود. از آنجاکه لازمه ادغام اطلاعات، اشتراک‌گذاری داده‌ها بین سازمان‌ها و یا حتی میان بخش‌ها یا شعبه‌های یک سازمان است، در برنامه‌های مرتبط با مدیریت داده در کانادا، به‌صورت مشخص برنامه‌هایی جهت مقابله با مخاطرات و فقدان قطعیت‌های ذاتی در اشتراک اطلاعات، تدوین شده است [۱۱].

1.https://science.gc.ca/

۳-۱-۲. رویکرد پردازش داده

در کشور کانادا برای پردازش داده، از رویکردهای متفاوتی همچون جداول و تجزیه‌وتحلیل داده‌های ایستا[1] و ابزارهایی برای ارزیابی استفاده مسئولانه از داده‌ها[2] استفاده می‌شود. به هر شهروند کانادایی این دسترسی داده شده که از داده‌های موجود در مرکز ملی آمار کانادا استفاده کرده و پردازش موردنظر خود را انجام دهند[۱۲]. علاوه‌بر این، مرکز ملی آمار کانادا نیز تحلیل‌های عمومی را از داده‌های موجود انجام داده و در اختیار عموم قرار می‌دهد.

۴-۱-۲. نحوه توزیع داده

الزامات و تعهدات خاص مربوط به توزیع داده‌ها ممکن است بسته به نوع داده، هدف از تحول و حوزه قضایی که سازمان در آن فعالیت می‌کند، متفاوت باشد. بر این اساس در کشور کانادا نیز به تناسب این جزئیات، قوانین مختلفی طراحی شده است که از این میان می‌توان به موارد زیر اشاره کرد:

۱. قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی:[3] PIPEDA قانون فدرال حریم خصوصی است که جمع‌آوری، استفاده و افشای اطلاعات شخصی توسط سازمان‌های بخش خصوصی را تنظیم می‌کند. براساس PIPEDA، سازمان‌ها باید قبل از جمع‌آوری، استفاده یا افشای اطلاعات شخصی خود از افراد رضایت بگیرند و باید از صحت، امنیت و مدیریت مناسب این اطلاعات اطمینان حاصل کنند. PIPEDA همچنین به افراد حق دسترسی و درخواست اصلاح اطلاعات شخصی خود را می‌دهد[۱۳].

۲. قوانین حریم خصوصی ایالتی: علاوه‌بر PIPEDA، برخی از ایالت‌های کانادا قوانین حفظ حریم خصوصی مختص خود را دارند که ممکن است برای انتقال داده‌ها اعمال شود، مانند:

- قانون حفاظت از اطلاعات شخصی آلبرتا (PIPA)[۱۴]،
- قانون حفاظت از اطلاعات شخصی بریتیش کلمبیا (PIPA)[۱۵]،
- قانون کبک در مورد احترام به حفاظت از اطلاعات شخصی در بخش خصوصی[۱۶].

۵-۱-۲. پرداختن به موضوع امنیت داده

چنانچه در گزارش پیشین مرکز پژوهش‌های مجلس نیز بیان شده است[۱۷]، با توجه به اینکه کشور، کانادا عضو سازمان همکاری و توسعه اقتصادی است، برای تأمین امنیت داده‌ها و حریم خصوصی داده اصول ۱۰ گانه‌ای را به‌عنوان اصول زیربنایی در قانون حریم خصوصی در نظر گرفته است. مهم‌ترین اصول حمایت از اطلاعات شخصی در قانون حمایت از حریم خصوصی کانادا عبارتند از:

- **اصل یکم. پاسخ‌گویی:** هر سازمان مسئول اطلاعات در اختیار خود است.
- **اصل دوم. مشخص کردن اهداف:** هدف از جمع‌آوری داده باید تعیین شود.
- **اصل سوم. رضایت:** احترام به حریم خصوصی افراد و اخذ رضایت از ایشان هنگام استفاده و افشای اطلاعات مربوط ضروری است.
- **اصل چهارم. محدودیت گردآوری:** جمع‌آوری داده صرفاً باید حول محور هدف تعیین شده در اصل دوم باشد.
- **اصل پنجم. محدودیت استفاده، افشا و نگهداری:** داده‌های جمع‌آوری شـــده صرفاً برای رسیدن به هدف تعیین شده در اصل دوم استفاده شده و داده‌ها تا زمان نیل به هدف موردنظر باید نگهداری شوند. برای استفاده در سایر اهداف باید مجدد رضایت افراد یا سازمان‌های مالک داده که داده‌ها متعلق به ایشان است اخذ شود.

1.Static Data Analysis
2.Responsible Data Use
3.Personal Information Protection and Electronic Documents Act (PIPEDA)

- **اصل ششم. دقت:** اطلاعات شخصی باید برای اهدافی که قرار است مورد استفاده قرار بگیرند دقیق و کامل بوده و در هنگام ضرورت به‌روزرسانی شود.
- **اصل هفتم. تدابیر حفاظتی:** اطلاعات شخصی باید با توجه به سطح حساسیت آنها، توسط تدابیر حفاظتی امنیتی مورد حفاظت قرار گیرد.
- **اصل هشتم. شفافیت:** یک سازمان باید اطلاعات خاص در مورد روش‌ها و سیاست‌های مربوط به مدیریت اطلاعات خود را در دسترس قرار دهد.
- **اصل نهم. دسترسی فردی:** هر فرد باید دسترسی لازم به داده‌های شخصی خود را داشته باشد و در صورت امکان آن را اصلاح و به‌روزرسانی نماید.
- **اصل دهم. تطابق:** هر فرد باید بتواند تطابق سازمان یا فرد / افراد مسئول حفاظت از اطلاعات شخصی خود در سازمان را با اصول فوق به چالش بکشد.

۲-۱-۶. متولی زنجیره تأمین داده

در طول صد سال گذشته، آمار مرتبط با کانادا در یک آژانس آماری با نام اداره ملی آمار کانادا[1] متمرکز شده است و از این آمار در جهت تصمیم‌گیری‌ها و سیاستگذاری‌های مبتنی‌بر داده‌ها و خدمات بهتر برای شهروندان کانادایی بهره برده می‌شود. نقش آژانس مذکور با رویکرد حاکمیتی برای مدیریت داده، اطمینان از در دسترس بودن داده‌های با کیفیت بالا و قابل‌اعتماد برای اطلاع‌رسانی به برنامه‌ها و خدمات حاکمیت است. این درحالی است که از اطلاعات و حریم خصوصی کانادایی‌ها محافظت می‌کند. همچنین این آژانس، متعهد به رهبری، یکپارچه‌سازی آمار و تقویت سیستم آماری ملی از طریق امکان استفاده استراتژیک از داده‌ها و ارائه بینش داده از طریق همکاری‌ها و مشارکت‌های نوآورانه است [۱۸].

۲-۱-۷ عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

مهم‌ترین عضویت کشور کانادا در ارتباط با داده و اطلاعات، عضویت این کشور در سازمان همکاری و توسعه اقتصادی است [۱۷]. علاوه‌بر این، در این کشور قوانین متعددی در زمینه داده و اطلاعات طراحی شده است که از این میان می‌توان به موارد ارائه شده در شکل ۱ اشاره کرد.

1.Statistics Canada

شکل ۱. مهم‌ترین قوانین کشور کانادا در زمینه داده‌ها و اطلاعات [۱۷]

قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی (PIPEDA)

- قانون فدرال حریم خصوصی است که بر جمع‌آوری، استفاده و افشای اطلاعات شخصی توسط سازمان‌های بخش خصوصی نظارت می‌کند.

قانون حفظ حریم خصوصی

- قانون حفظ حریم خصوصی یک قانون فدرال است که بر جمع‌آوری، استفاده و افشای اطلاعات شخصی توسط نهادهای دولتی فدرال حاکم است.

قانون ضدهرزنامه کانادا (CASL)

- CASL قانونی است که ارسال پیام‌های الکترونیکی تجاری از جمله ایمیل و پیام‌های متنی را در داخل کانادا و بین کانادا و سایر کشورها تنظیم می‌کند.

قانون آزادی اطلاعات

- قانون آزادی اطلاعات برای عموم مردم حق دسترسی به سوابق نگهداری شده توسط مؤسسات دولتی فدرال، مشروط به استثنائات معین را فراهم می‌کند.

قوانین حفاظت از اطلاعات سلامت

- چندین استان قوانین حفاظت از اطلاعات بهداشتی را وضع کرده‌اند که بر جمع‌آوری، استفاده و افشای اطلاعات سلامت شخصی حاکم است.

قوانین حریم خصوصی استانی

- برخی از استان‌ها قوانین مربوط به حریم خصوصی خود را دارند که بر جمع‌آوری، استفاده و افشای اطلاعات شخصی توسط سازمان های بخش عمومی نظارت می‌کند.

۲-۲. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور استرالیا

۲-۲-۱. منابع تولید داده

در استرالیا با هدف یکپارچه‌سازی داده، از داده‌های مربوط به ادارات و سازمانی‌های مختلف استفاده می‌شود که مهم‌ترین این منابع عبارتند از [۱۹]:

- داده‌های مرتبط با سلامت و سالمندی،
- پایگاه شواهد ملی آموزش و پرورش،
- داده‌های مرتبط با خدمات اجتماعی،
- داده‌های مرتبط با مهارت و اشتغال،
- داده‌های مرتبط با امور کشاورزی،
- داده‌های مرتبط با امور منابع آب و محیط زیست،
- داده‌های مرتبط با امور صنعت،
- داده‌های مرتبط با امور انرژی و منابع،
- داده‌های مرتبط با امور مالی،
- داده‌های مرتبط با امور اطلاعات ملی،
- سایر اطلاعات محافظت شده توسط دولت.

۲-۲-۲. نحوه جمع آوری و یکپارچه‌سازی داده

در کشور استرالیا، داده‌ها به‌صورت بر خط و مستقیم از مراکز تولید منابع داده دریافت می‌شود و در مرکزی تحت نظارت اداره آمار استرالیا[1] و مؤسسه بهداشت و رفاه استرالیا[2] نگهداری می‌شوند. یکپارچه‌سازی داده در استرالیا دارای چارچوب منحصربه‌فرد خود است که مطابق با اسناد پژوهشی درخصوص پروژه یکپارچه‌سازی داده در استرالیا موسوم به DIPA[3] به‌شرح زیر است [۲۰]:

۱ **زیرساخت و ادغام داده:** به‌منظور انجام این اقدام زیر ساخت‌های فنی امن و قابل دسترسی در کشور استرالیا ایجاد شده است.

۲ **تولید داده:** داده‌ها از مجاری و روش‌های مختلف که بر پایه سیستم‌ها و سامانه‌های عملیاتی است تولید می‌شوند.

۳ **تحلیل داده‌ها:** از تحلیل داده‌های یکپارچه برای حل مسائل پیچیده دولتی و حکومتی متشکل از چند موضوع مختلف، استفاده می‌شود. واحد تحلیل داده توسط وزارت خدمات اجتماعی، بهداشت، مهارت و اشتغال، دپارتمان‌های کشاورزی، منابع آب و محیط زیست، صنعت، انرژی و منابع، علوم و نخست وزیر راهبری می‌شود.

۴ **برقراری ارتباط و تعامل بهتر:** نحوه استفاده از داده‌ها توسط دپارتمان نخست وزیری[4] راهبری می‌شود.

۵ **بررسی فنی و مشاوره:** بررسی فنی و ارائه مشاوره توسط واحدی با نام Data 61 ارائه می‌شود. این واحد، نقش تضمینی و مشاوره‌ای برای کمک به سازمان‌های مشارکت‌کننده در یکپارچه‌سازی داده‌ها، برای تصمیم‌گیری آگاهانه با در نظر گرفتن آخرین داده‌های در دسترس و تحلیل آنها، دارد.

1.Australian Bureau of Statistics
2.Australian Institute of Health and Welfare (AIHW)
3.Data Integration Partnership for Australia
4.https://www.pmc.gov.au/

۲-۲-۳. رویکرد پردازش داده

یکی از اجزای اصلی یکپارچه‌سازی داده‌ها برای استرالیا، ایجاد واحدهای تحلیل داده‌ها هستند. پنج واحد تحلیل داده تحت DIPA وجود دارد که عبارتند از: ۱. واحد تحلیل اجتماعی، بهداشت و رفاه، ۲. شبکه تحلیل و داده‌های اقتصادی، ۳. شبکه تجزیه‌وتحلیل محیط فیزیکی، ۴. واحد تحلیل کسب‌وکار حاکمیتی و ۵. مرکز تجزیه‌وتحلیل مرکزی.

مرکز تحلیل مرکزی، با بررسی گزارش‌های سایر واحدهای تحلیل‌کننده، بینش‌ها و خط‌مشی‌های مناسب را برای سیاست‌های اولویت‌دار حاکمیت تعیین می‌کند و با در نظر گرفتن سیاست‌های تعیین شده توسط راهبر توزیع داده یعنی دفتر نخست وزیری، این اطلاعات را در اختیار سازمان‌ها و ادارات متقاضی قرار می‌دهد [۲۰].

۲-۲-۴. امنیت داده

در پروژه DIPA توجه خاصی به حریم خصوصی فردی و امنیت داده‌های حساس، مبذول شده است، زیرا DIPA دسترسی به داده‌های کنترل شده، شناسایی نشده و محرمانه را برای تجزیه‌وتحلیل سیاست‌ها و اهداف تحقیقاتی فراهم می‌کند. DIPA توسط فرایندها و قوانین آژانس‌ها، ازجمله قانون حفظ حریم خصوصی ۱۹۸۸، اداره می‌شود. در استرالیا به‌منظور یکپارچه‌سازی داده‌های سلامت و بهداشت و رفاه اجتماعی، پروژه‌ای توسط مؤسسه بهداشت و رفاه استرالیا انجام شده است. مؤسسه بهداشت و رفاه استرالیا یک محیط پیوند ایمن برای گردآوری تمامی داده‌های مورد توجه در محدوده پروژه فراهم کرده اســت. برای این منظور، مرکز خدمات یکپارچه‌سازی داده‌ها[1] راه اندازی شده است که متشکل از یک شبکه کامپیوتری مجزا بوده که به اینترنت یا هیچ سیستم دیگری متصل نیست و شامل پروتکل‌ها و رویه‌های سخت‌گیرانه برای امنیت فیزیکی، امنیت داده‌ها و بررسی خروجی‌ها توسط مدیر برای اطمینان از رعایت اصول اخلاقی است.

۲-۲-۵. متولی زنجیره تأمین داده

اداره آمار استرالیا و مؤسسه بهداشت و رفاه استرالیا، دو سازمان اصلی است که برای یکپارچه‌سازی داده‌ها و قابلیت‌های پیوند موجود آنها در استرالیا در نظر گرفته شده است. اداره آمار استرالیا با همکاری دپارتمان کشاورزی، آب و محیط زیست، وزارت صنعت، علوم، انرژی و منابع و همچنین شاخص موقعیت مکانی، ابزاری را برای ارائه یک سیستم استاندارد و قابل تکرار برای یکپارچه‌سازی داده‌ها در سراسر اقتصاد توسعه داد [۲۱].

۲-۲-۶. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

مهم‌ترین عضویت کشور استرالیا مرتبط با داده‌ها و اطلاعات را می‌توان عضویت این کشور در کمیسیون اقتصادی و اجتماعی سازمان ملل متحد برای آسیا و اقیانوسیه بیان کرد [۲۲]. جدول ۱ نیز مهم‌ترین قوانین کشوری در زمینه داده‌ها و اطلاعات را در کشور استرالیا نشان می‌دهد.

1.https://www.abs.gov.au/about/data-services/data-integration/data-integration-service

جدول ۱. مهم‌ترین قوانین کشوری مرتبط با داده در کشور استرالیا

عنوان	توضیحات
قانون حفظ حریم خصوصی ۱۹۸۸ [1]	اصول حفظ حریم خصوصی استرالیا که به‌نحوی به‌عنوان قانون اصلی حفاظت از داده‌ها در این کشور شناخته می‌شود.
قانون فقدان ثبت تماس ۲۰۰۶ [2]	محدودیت‌هایی را در رابطه با تماس‌های تلفنی ناخواسته اعمال می‌کند.
قانون هرزنامه ۲۰۰۳ [3]	قوانینی را در رابطه با پیام‌های تجاری تعیین می‌کند تا بتوان ارسال پیام‌ها و تبلیغات به اشخاص در فضای مجازی و سایبری را مدیریت کرد.
قانون مبارزه با پول‌شویی و مبارزه با تأمین مالی تروریسم ۲۰۰۶ [4]	شامل تمهیداتی در رابطه با انطباق با اصول حفظ حریم خصوصی استرالیا مرتبط با اطلاعات به‌دست آمده تحت این قانون است.

مأخذ: یافته‌های پژوهش.

همچنین در سطح ایالت و منطقه‌ای نیز قوانین مختلفی وجود دارد که برخی از این موارد در شکل ۲ ارائه شده است.

شکل ۲. برخی از قوانین ایالتی و منطقه‌ای کشور استرالیا در زمینه داده‌ها و اطلاعات

قوانین مرتبط با صنایع بانکی، بیمه و بازنشستگی	قوانین مرتبط با حفاظت از حریم خصوصی و اطلاعات شخصی	قوانین مرتبط با مخابرات	قوانین مرتبط با بخش سلامت
استاندارد احتیاطی CPS ۲۳۱	قانون محرمانگی اطلاعات ۲۰۱۴	قانون مخابرات ۱۹۹۷	قانون سوابق سلامت من ۲۰۱۲
استاندارد احتیاطی SPS ۲۳۱	قانون حریم خصوصی محل کار ۲۰۱۱	قانون مخابرات (رهگیری و دسترسی) ۱۹۷۹	قانون شناسه‌های مراقبت‌های بهداشتی ۲۰۱۰
استاندارد احتیاطی CPS ۲۳۴	قانون محرمانگی اطلاعات ۲۰۰۹		قانون سوابق سلامت و محرمانگی اطلاعات ۲۰۰۲
	قانون تجاوز به حریم خصوصی ۱۹۷۱		قانون سوابق سلامت (محرمانگی و دسترسی) ۱۹۹۷
	قانون اطلاعات ۲۰۰۲		قانون سوابق سلامت ۲۰۰۱
	قانون حفاظت از حریم خصوصی و داده ۲۰۱۴		
	قانون آزادی اطلاعات ۱۹۹۲		

مأخذ: همان.

1.Commonwealth Countries (Cth)
2.Do not Call Register
3.Spam Act
4.Anti-Money Laundering and Counter-Terrorism Financing Act

۳-۲. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور سنگاپور

۱-۳-۲. منابع تولید داده

در سنگاپور، سازمان‌های مختلف داده‌های خود را برای شفافیت بیشتر در اختیار عموم مردم و در اختیار یکدیگر قرار می‌دهند. مهم‌ترین منابع داده در این کشور عبارتند از [۲۳]:

- داده‌های مرتبط با امور اقتصادی،
- داده‌های مرتبط با امور آموزشی،
- داده‌های مرتبط با امور محیط زیستی،
- داده‌های مرتبط با امور دارایی، مالی و سرمایه‌گذاری،
- داده‌های مرتبط با امور بهداشت و سلامت،
- داده‌های مرتبط با امور زیر ساختی،
- داده‌های مرتبط با امور اجتماعی،
- داده‌های مرتبط با امور فناوری اطلاعات،
- داده‌های تکنولوژیکی،
- داده‌های مرتبط با امور حمل‌ونقل.

در سامانه پرتال داده سنگاپور[1] ۱۸۳۷ پایگاه داده مختلف در زمینه موضوعات فوق وجود دارد. این وب‌سایت اولین بار در سال ۲۰۱۱ به‌عنوان پرتال یک مرحله‌ای دولت برای مجموعه داده‌های در دسترس عموم از هفتاد سازمان عمومی راه‌اندازی شد. تا به امروز، بیش از صد برنامه با استفاده از داده‌های باز دولت ایجاد شده است. برخی از منابع تولید داده ملی سنگاپور عبارتند از [۲۳]:

۱ **داده‌های دولتی:** جمع‌آوری داده‌ها از منابع دولتی شامل داده‌های جمعیتی، داده‌های اقتصادی، داده‌های بهداشتی و داده‌های محیط زیستی.

۲ **داده‌های تجاری:** داده‌های تولید شده توسط شرکت‌های تجاری فعال در زمینه اقتصاد دیجیتال در این کشور.

۳ **داده‌های اجتماعی:** شهروندان سنگاپور از رسانه‌های اجتماعی و سایر پلتفرم‌های آنلاین برای تعامل با یکدیگر استفاده می‌کنند. این داده‌ها می‌توانند برای درک بهتر رفتارهای اجتماعی و ایجاد سیاست‌های عمومی مؤثر استفاده شوند.

اقدامات سنگاپور سبب شده است تا این کشور در زمینه حکمرانی داده در جهان جایگاه ویژه‌ای داشته باشد. برخی از دستاوردهای سنگاپور به‌شرح زیر است:

- براساس گزارش «دستورالعمل‌های حکمرانی داده جهانی ۲۰۲۳» که توسط مؤسسه بروکینگز منتشر شده است، سنگاپور در رتبه اول جهان در زمینه حکمرانی داده قرار دارد. این گزارش، سنگاپور را به‌دلیل «چارچوب قانونی و مقرراتی جامع و کارآمد، زیرساخت‌های فناوری اطلاعات و ارتباطات پیشرفته و فرهنگ احترام به حریم خصوصی» مورد تقدیر قرار داده است [۲۴].
- براساس گزارش «شاخص حکمرانی داده ۲۰۲۳» که توسط شرکت مشاوره مدیریت مکینزی منتشر شده است، سنگاپور در رتبه دوم جهان در زمینه حکمرانی داده قرار دارد. این گزارش، سنگاپور را به‌دلیل «تعهد قوی به حریم خصوصی داده‌ها، زیرساخت‌های فناوری اطلاعات و ارتباطات پیشرفته و فرهنگ خلاقانه و نوآورانه» تحسین کرده است [۲۵].
- براساس گزارش «شاخص حکمرانی داده جهان ۲۰۲۳» که توسط شرکت حقوقی و مشاوره DLA Piper منتشر شده است، سنگاپور در رتبه سوم جهان در زمینه حکمرانی داده قرار دارد. این گزارش سنگاپور را به‌دلیل «چارچوب قانونی و مقرراتی جامع، زیرساخت‌های فناوری اطلاعات و ارتباطات پیشرفته و فرهنگ احترام به حریم خصوصی» ستایش می‌کند [۲۶].

1. https://data.gov.sg

۲-۳-۲. نحوه جمع آوری و یکپارچه‌سازی داده

داده‌ها به دو طریق در آژانس فناوری دولتی سنگاپور[1] جمع‌آوری می‌شوند، یا به‌صورت دریافت گزارش آفلاین و آنلاین از سازمان‌ها و ادارات دولتی یا به‌صورت غیررسمی و از طریق همکاران غیررسمی با ارسال ایمیل‌های حاوی گزارش است. لازم به توضیح است صحت داده‌های دریافتی در روش دوم مورد بررسی قرار می‌گیرد. زیرا به نسبت روش اول، دارای کیفیت پایین‌تری است [۲۷].

برخی از اقدام‌های خاص سنگاپور برای جمع‌آوری و یکپارچه‌سازی داده ملی عبارتند از:

- دولت سنگاپور از یک پلتفرم داده ملی به‌نام NDS[2] برای جمع‌آوری و یکپارچه‌سازی داده‌های ملی از منابع مختلف استفاده می‌کنند.
- دولت سنگاپور از یک چارچوب مدیریت داده ملی به‌نام NDMP[3] برای اطمینان از اینکه داده‌های ملی به‌طور ایمن و مسئولانه مدیریت می‌شوند، استفاده می‌کند.
- دولت سنگاپور از یک برنامه سواد داده ملی به‌نام NDLI[4] که برای افزایش آگاهی شهروندان از اهمیت داده‌ها و نحوه استفاده مسئولانه از آنها استفاده می‌کند.

سنگاپور از طریق برنامه‌هایی مانند DS4PG[5] به‌دنبال توسعه زیرساخت‌های داده‌ای خود است. این برنامه‌ها، شامل جمع‌آوری داده‌های دولتی و خصوصی، ایجاد ابزارهای تحلیل داده و آموزش نیروی کار در حوزه داده‌های علمی است. این برنامه توسط اداره اطلاعات و ارتباطات ملی رهبری و با همکاری سایر نهادهای دولتی، بخش خصوصی و جامعه مدنی اجرا می‌شود [۲۸].

۲-۳-۳. رویکرد پردازش داده

در آژانس فناوری دولتی سنگاپور از روش‌های تقاطع‌گیری بین داده‌ها و تطبیق آماری برای یکپارچه‌سازی داده استفاده می‌شود. برای این منظور پس از شناسایی و ترکیب سوابق مربوط به سازمان‌ها و ادارات مختلف، از طریق روش‌های کنترل کیفیت داده، صحت داده‌های دریافتی را بررسی کرده و پس از قرارگیری در پایگاه داده موردنظر، در دسترس عموم قرار داده می‌شود. پردازش داده ملی در سنگاپور توسط آژانس ملی آمار[6] انجام می‌شود. NSO یک سازمان دولتی است که مسئول جمع‌آوری، تجزیه‌وتحلیل و انتشار داده‌های آماری در سنگاپور است. این سازمان داده‌ها را از منابع اطلاعاتی مختلف نظیر سرشماری‌ها، نظرسنجی‌ها، داده‌های ثبتی و داده‌های دولتی جمع‌آوری می‌کنند [۲۹].

۲-۳-۴. نحوه توزیع داده

در سنگاپور، داده‌های دریافتی از منابع فوق‌الذکر، با توجه به نوع داده و محرمانگی موجود، در وب‌سایت Data.gov.sg در دسترس سازمان‌ها و عموم مردم قرار دارد و سازمان یا فرد متقاضی با ثبت‌نام در پایگاه داده موردنظر، داده‌ها و اطلاعات مورد نیاز خود را دانلود می‌کند. توزیع داده ملی در سنگاپور توسط سازمان دولتی به‌نام DataGov انجام می‌شود. این سازمان در سال ۲۰۱۹ تأسیس شده است و مسئولیت مدیریت و توزیع داده‌های دولتی را برعهده دارد.

DataGov دارای یک پلتفرم آنلاین به‌نام MyData است که به شهروندان اجازه می‌دهد تا به داده‌های دولتی دسترسی داشته‌باشند و آنها را با دیگران به اشتراک بگذارند. این پلتفرم شامل داده‌هایی از سازمان‌های مختلف دولتی مانند وزارت بهداشت، وزارت آموزش و پرورش و وزارت کار است. DataGov همچنین یک برنامه مشارکتی به‌نام Data Innovation Lab را راه‌اندازی کرده است که به سازمان‌های خصوصی و دولتی کمک می‌کند تا از داده‌های دولتی برای توسعه محصولات و خدمات جدید استفاده کنند [۲۳].

1.https://www.tech.gov.sg/2 .Do Not Call Register
2.National Data Sharing Platform /4 .Anti-Money Laundering and Counter-Terrorism Financing Act
3.National Data Management Policy
4.National Digital Literacy Initiative
5.Data Science for Public Good
6.Natioonal statistical Office(NSO)

براساس گزارش Open Data Barometer ۲۰۲۳، سنگاپور در زمینه انتشـــار داده‌های دولتی رتبه اول را در جهان دارد. این کشور در سال ۲۰۲۳ بیش از هزار مجموعه داده را به‌صورت باز منتشر کرده است[۳۰].

۵-۳-۲. امنیت داده و متولی زنجیره تأمین داده

پایگاه داده ملی سنگاپور یک ابتکار ازسوی وزارت دارایی سنگاپور بوده است و هم‌اکنون توســـط آژانس فناوری دولتی[1] سنگاپور مدیریت می‌شود[۳۱].

متولی زنجیره تأمین داده ملی در سنگاپور، آژانس فناوری اطلاعات و ارتباطات (IDA) است. IDA یک آژانس دولتی است که مسئول توسعه و مدیریت زیرساخت‌های فناوری اطلاعات و ارتباطات در سنگاپور است. IDA مسئولیت‌های زیر را در زمینه زنجیره تأمین داده ملی برعهده دارد:

- ایجاد چارچوب سیاستی برای زنجیره تأمین داده ملی،
- تسهیل همکاری بین سازمان‌های دولتی و خصوصی برای توسعه و مدیریت زنجیره تأمین داده ملی؛
- ارائه حمایت فنی و مالی برای سازمان‌هایی که در زنجیره تأمین داده ملی مشارکت دارند.

IDA برای انجام این مسئولیت‌ها از یک چارچوب سیاستی برای زنجیره تأمین داده ملی خود استفاده می‌نماید که شامل اصول ارائه شده در شکل ۳ است. IDA درحال‌حاضر در حال توسعه یک برنامه پنج ساله برای زنجیره تأمین داده ملی است. این برنامه شامل اهداف و اقداماتی برای بهبود کارایی، امنیت و قابلیت دسترسی به داده‌های موجود در زنجیره تأمین داده ملی است.

شکل ۳. رویکردهای آژانس فناوری اطلاعات و ارتباطات سنگاپور [۳۱]

جامعیت	امنیت	کارایی	همکاری	حمایت
زنجیره تأمین داده ملی باید شامل تمام داده‌های دولتی و خصوصی باشد که برای توسعه و اداره کشور ضروری است.	داده‌های موجود در زنجیره تأمین داده ملی باید ایمن و محافظت شده باشد.	زنجیره تأمین داده ملی باید کارآمد و مقرون‌به‌صرفه باشد.	برای توسعه و مدیریت زنجیره تأمین داده ملی با سازمان‌های دولتی و خصوصی همکاری می‌کند. این همکاری از طریق کارگروه‌ها، انجمن‌ها و غیره انجام می‌شود.	برای سازمان‌هایی که در زنجیره تامین داده ملی مشارکت دارند، حمایت فنی و مالی شامل آموزش، مشاوره و غیره ارائه می‌گردد.

1.Government Technology Agency

۶-۳-۲.عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

عضویت در کمیسیون اقتصادی و اجتماعی سازمان ملل متحد برای آسیا و اقیانوسیه را می‌توان به‌عنوان یکی از مهم‌ترین اقدامات سنگاپور بیان کرد. در زمینه قوانین مرتبط با داده‌ها و اطلاعات، قانون حفاظت از داده‌های شخصی ۲۰۱۲[1] (PDPA) را می‌توان به‌عنوان قانون اصلی حفاظت از داده‌ها در سنگاپور معرفی کرد. PDPA یک قانون کلی حفاظت از داده‌هاست که برای همه سازمان‌های بخش خصوصی اعمال می‌شود. این قانون در دو نوامبر ۲۰۲۰ با اصلاحات جدیدی نظیر تعهدات سازمان‌ها را در رابطه با جمع‌آوری، استفاده، افشا، دسترسی، اصلاح، مراقبت، حفاظت، نگهداری، انتقال داده‌های شخصی و اطلاع‌رسانی در مورد نقض داده‌ها به‌روز شده است [۳۲]. سایر مقررات صادر شده تحت PDPA عبارتند از:

- مقررات حفاظت از داده‌های شخصی (۲۰۲۱)، که الزامات انتقال داده‌های شخصی به خارج از سنگاپور، شکل، نحوه و روش‌های درخواست دسترسی یا تصحیح داده‌های شخصی و افرادی که می‌توانند از حقوق مربوط به افشای اطلاعات شخصی افراد متوفی استفاده کنند را تعیین می‌کند.
- مقررات حفاظت از داده‌های شخصی (اعلان نقض داده‌ها) ۲۰۲۱ (مقررات اعلان نقض).
- مقررات حفاظت از داده‌های شخصی (ترکیب جرائم) ۲۰۲۱.
- مقررات حفاظت از داده‌های شخصی (فقدان ثبت تماس) ۲۰۱۳.
- مقررات حفاظت از داده‌های شخصی (اجرا) ۲۰۲۱.
- مقررات حفاظت از داده‌های شخصی (تجدیدنظر) ۲۰۲۱.

علاوه‌بر این، کمیسیون حفاظت از داده‌های شخصی (PDPC) چند دستورالعمل مشورتی صادر کرده است که تفسیر PDPA را روشن‌تر می‌کنند: قانون سوءاستفاده از رایانه ۱۹۹۳ چند مورد از تخلفات را تعیین می‌کند که شامل دسترسی یا تغییر غیرمجاز مطالب رایانه‌ای و همچنین استفاده یا رهگیری غیرمجاز از خدمات رایانه‌ای است.

قانون امنیت سایبری ۲۰۱۸ مالکان و اپراتورهای زیرساخت حیاتی اطلاعات را ملزم می‌کند که از خط‌مشی‌ها و استانداردهای امنیت سایبری پیروی کنند، ممیزی‌ها و ارزیابی‌های ریسک انجام دهند و اقدام‌های گزارش‌دهی حوادث را اجرایی سازند.

۲-۴. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور مکزیک

۱-۴-۲.منابع تولید داده

مهم‌ترین داده‌هایی که توسط منابع مختلف در مکزیک مورد توجه قرار می‌گیرد به‌شرح ذیل هستند: ۱. کشاورزی، ۲. رفاه، ۳. فرهنگ، ۴. دفاع ملی، ۵. مسکن، ۶. توسعه کشاورزی و ۷. اقتصاد. کلیه شهروندان مکزیک از طریق پرتال داده‌باز مکزیک[2] قادر خواهند بود به این داده‌ها دسترسی داشته‌باشند.

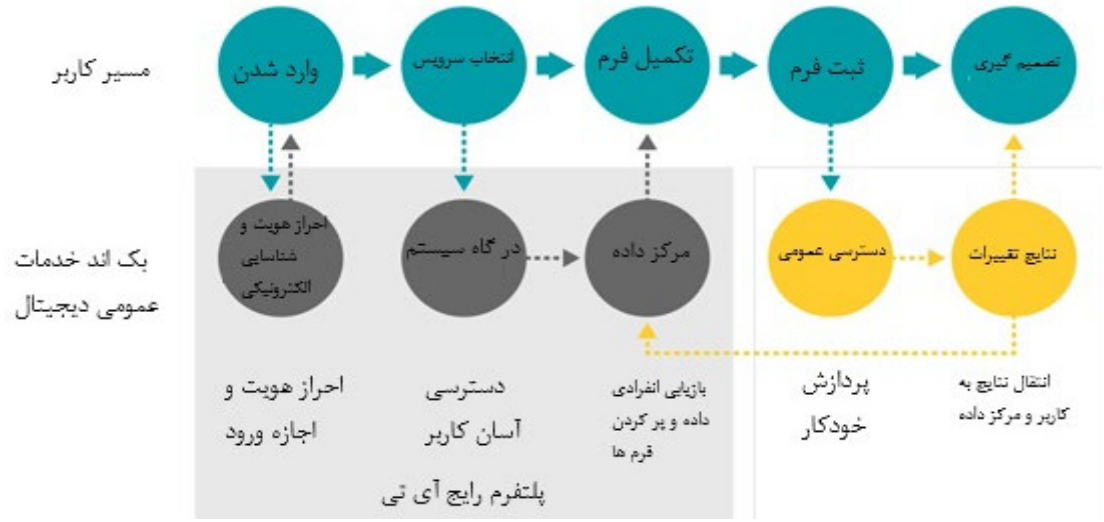
۲-۴-۲. نحوه جمع‌آوری و یکپارچه‌سازی داده

راه‌اندازی و مدیریت خدمات عمومی دیجیتال زمانی آسان‌تر است که بخش‌های مختلف فرایندهای بر خط شده ـ برای مثال، امکان ورود ایمن به یک فرم آنلاین ـ در دسترس همه ارگان‌های دولتی به‌عنوان واحدهای تولید داده و اطلاعات، مجزا و قابل استفاده باشد. به‌دلیل هزینه و پیچیدگی‌های موجود، برای ارگان‌های حاکمیتی اینکه به‌تنهایی زیرساخت‌های فناوری و مدیریت لازم را ایجاد کنند، تقریباً غیرعملی است. دولت‌ها در عوض می‌توانند به ایجاد پلتفرم‌های مشترک فناوری اطلاعات کمک کرده که همه ارگان‌های حاکمیتی از آنها استفاده کنند.

با در نظر گرفتن موارد مذکور، دولت مکزیک، ۳ برنامه کاربردی ویژه شامل ۱. مدیریت هویت الکترونیکی، ۲. دسترسی آسان به خدمات دیجیتال برای شهروندان و ۳. تبادل یکپارچه داده‌ها بین ارگان‌های دولتی را در نظر گرفته است (شکل ۴) [۳۳].

1.The Personal Data Protection Act 2012 (PDPA)
2.https://datos.gob.mx/

شکل ۴. چرخه ایجاد، نگهداری، یکپارچه‌سازی و بازیابی داده [۳۳]



۳-۴-۲ رویکرد پردازش داده

قانون حفاظت از داده‌ها و امنیت سایبری در مکزیک،[1] اصلی‌ترین قانون مرتبط با حفاظت از داده‌ها در کشور مکزیک است که دو نقش پردازشگر داده و کنترل‌کننده داده را با شرح وظایف زیر به رسمیت می‌شناسد:

- **پردازشگر داده:** موجودیت مرتبط یا شخص حقوقی که داده‌های شخصی را از طرف کنترل‌کننده داده، پردازش می‌کند.
- **کنترل‌کننده داده:** موجودیت مرتبط یا شخص حقوقی که در مورد پردازش داده‌های شخصی تصمیم می‌گیرد.

رابطه این دو نقش باید از طریق بندهای قراردادی یا سایر اسناد قانونی به‌گونه‌ای برقرار شود که وجود، دامنه و ماهیت چنین رابطه‌ای را ثابت کند. طبق قانون حفاظت از داده‌ها، اصولی که باید توسط کنترل‌کننده‌ها و / یا پردازشگرها در پردازش داده‌های شخصی رعایت شود به‌شرح زیر است [۳۴]:

- **مشروعیت:** داده‌های شخصی باید به روشی قانونی جمع‌آوری و پردازش شوند.
- **رضایت:** موجودیت مرتبط داده باید رضایت خود را برای پردازش داده‌های شخصی خود ارائه دهد.
- **اطلاعات:** از طریق یک اعلامیه حفظ حریم خصوصی، کنترل‌کننده داده باید موضوع داده‌ها را در مورد وجود و ویژگی‌های پردازش داده‌های شخصی آنها مطلع کند.
- **کیفیت:** این اصل زمانی است که داده‌های شخصی مستقیماً توسط موضوع داده ارائه می‌شود. در غیر این صورت، کنترل‌کننده داده‌ها باید اندازه‌گیری‌هایی را انجام دهد تا اصل کیفیت را برآورده کند و سازوکارهایی را اتخاذ کند که برای اطمینان از دقت، جامعیت، به‌روز و صحیح بودن داده‌ها ضروری است.
- **هدف:** داده‌های شخصی فقط برای اهداف تعیین شده در دستورالعمل حریم خصوصی قابل پردازش هستند.
- **وفاداری:** داده‌های شخصی باید برای حفاظت از منافع افراد موضوع داده و انتظار منطقی از حریم خصوصی پردازش شوند.
- **مسئولیت:** کنترل‌کنندگان داده‌ها باید از پردازش داده‌های شخصی در اختیارشان و همچنین داده‌هایی که به یک پردازشگر داده منتقل می‌شوند، اطمینان حاصل کنند.

علاوه‌بر این، الزامات قانونی زیر باید هنگام پردازش داده‌های شخصی در نظر گرفته شوند [۳۵]:

- داده‌های شخصی باید مطابق با مقررات تعیین شده توسط قانون حفاظت از داده‌ها و سایر مقررات قابل اجرا به روشی قانونی جمع‌آوری و پردازش شوند.

1.Data Protection and Cybersecurity Laws in Mexico

- داده‌های شخصی نباید از راه‌های فریبنده یا متقلبانه به‌دست آید.
- در تمامی پردازش‌های داده‌های شخصی، فرض بر این است که انتظار معقولی از حفظ حریم خصوصی وجود دارد، که به‌عنوان اعتمادی که هر شخص به دیگری نسبت به داده‌های شخصی ارائه شده برای رسیدگی به آنها براساس توافق طرفین در شرایط مقرر در قانون می‌کند، درک می‌شود.
- داده‌های شخصی نباید بیش از مدتی که برای انطباق با اهدافی که داده‌های شخصی برای آن نگهداری شده‌اند، لازم باشد. کنترل‌کنندگان داده‌ها باید رویه‌های نگهداری، از جمله حذف و / یا مسدود کردن داده‌های شخصی را با در نظر گرفتن ماهیت داده‌ها ایجاد و مستند کنند.

۴-۴-۲. نحوه توزیع داده

برای چندین دهه، شهروندان مکزیکی که خواستار دریافت المثنی از شناسنامه خود بودند، باید یک فرایند طولانی، خسته‌کننده و نامشخص را دنبال می‌کردند. آنها باید گواهی تولد والدین خود را بازیابی نموده، سندی را که توسط نماینده وزارت بهداشت مکزیک امضا شده بود، دریافت و به یک دفتر محلی ثبت احوال مراجعه می‌کردند. زمان لازم برای صدور گواهی مذکور بین دو هفته تا دو ماه بود و گاهی اوقات اشتباهاتی در نام، تاریخ تولد و حتی جنسیت وجود داشت. بااین‌حال، امروزه مکزیکی‌ها می‌توانند با ورود به gob.mx، یک پرتال یک مرحله‌ای که ۳۴۰۰۰ پایگاه‌داده از ۲۵۰ مؤسسه دولتی و ۵۴۰۰ سرویس عمومی را ادغام می‌کند، در عرض چند دقیقه یک نسخه ایمن، تأیید شده و بدون خطا از شناسنامه خود دریافت کنند.

طبق قانون حفاظت از داده‌ها در مکزیک، چنانچه کنترل‌کنندگان داده‌ها قصد دارند داده‌های شخصی را به اشخاص ثالث منتقل کنند، باید یک اعلامیه حفظ حریم خصوصی و اهدافی که موضوع داده‌ها برای آنها پردازش داده‌ها را محدود می‌کند، به آنها ارائه کنند. ارگان مرتبط با داده باید از طریق اعلامیه حفظ حریم خصوصی با چنین انتقالی موافقت کند. قرارداد فرعی ممکن است شامل پردازش داده‌های شخصی توسط پیمانکار فرعی شود، پردازشگر داده باید از کنترل‌کننده داده اجازه بگیرد، سپس پردازشگر داده باید با پیمانکار فرعی قراردادی منعقد کرده و پیمانکار فرعی همان تعهدات مورد نیاز برای پردازشگرهای داده را براساس قانون حفاظت از داده‌ها و سایر قوانین قابل اجرا برعهده بگیرد. در این مرحله نیاز است که حق پردازشگر داده برای قرارداد فرعی فعالیت‌های پردازش، در قرارداد بین کنترل‌کننده داده و پردازشگر داده مشخص شود. اگر این حق در آن قرارداد گنجانده نشده باشد، پردازشگر داده باید رضایت خاصی را از کنترل‌کننده داده به‌منظور قرارداد فرعی فعالیت‌های پردازشی بخواهد. انتقال بین‌المللی داده‌های شخصی باید مورد موافقت موجودیت مرتبط داده باشد و اهداف چنین انتقال‌هایی باید در اعلامیه حفظ حریم خصوصی گنجانده شود، اما درخصوص موارد ذیل نیازی به دریافت رضایت نیست:

- براساس قانون یا معاهده‌ای که مکزیک عضو آن است نیاز به دریافت رضایت نباشد،
- برای تشخیص یا پیشگیری پزشکی، ارائه مراقبت‌های بهداشتی، درمان پزشکی یا مدیریت خدمات بهداشتی، دریافت داده‌ها ضروری باشد؛ ارائه داده به گروه شرکت‌ها[1]، شرکت‌های تابعه یا وابسته تحت کنترل مشترک کنترل‌کننده داده، یا به شرکت مادر یا هر شرکتی از همان گروه کنترل‌کننده داده که تحت فرایندها و سیاست‌های داخلی یکسانی فعالیت می‌کنند؛
- به موجب قراردادی که به نفع موضوع داده منعقد شده بین کنترل‌کننده داده و شخص ثالث اجرا شده یا باید اجرا شود؛
- دسترسی به داده برای حفظ منافع عمومی یا اجرای عدالت ضروری یا قانونی لازم باشد؛
- برای شناسایی، اعمال یا دفاع از یک حق در دادرسی قضایی نیاز به داده باشد؛
- برای حفظ یا تحقق یک رابطه حقوقی بین کنترل‌کننده داده و موضوع داده دسترسی به داده ضروری باشد [۳۶].

1. National Institute of Statistics and Geography (INEGI)

۵-۴-۲. امنیت داده

کنترل کنندگان داده و پردازشگر داده‌ها ملزم به ایجاد و حفظ اقدامات اداری، فیزیکی، امنیتی و در صورت لزوم، فنی برای حفاظت از داده‌های شخصی هستند. در توسعه اقدام‌های امنیتی، کنترل کننده داده باید حداقل موارد زیر را در نظر بگیرد [۳۴]:

- خطر ذاتی با توجه به نوع داده‌های شخصی،
- حساسیت داده‌های شخصی،
- تحولات فناوری‌های مرتبط و تأثیرگذار،
- عواقب بالقوه نقض برای صاحبان داده،
- تعداد موضوع‌های داده‌ها،
- آسیب‌پذیری‌های قبلی در سیستم‌های پردازش،
- ارزش داده برای یک شخص ثالث غیرمجاز،
- سایر عواملی که ممکن است بر سطح خطر تأثیر بگذارند یا ناشی از سایر قوانین و مقررات قابل اجرا باشد.

مقررات حفاظت از داده‌ها، اقدام‌هایی را که کنترل کنندگان داده می‌توانند برای رعایت الزامات امنیتی انجام دهند را به‌شرح زیر تعیین کرده است:

- تهیه فهرستی از داده‌های شخصی،
- تعیین وظایف و تعهدات شخص (هایی) که داده‌های شخصی را پردازش خواهند کرد،
- انجام تجزیه‌وتحلیل ریسک داده‌های شخصی شامل شناسایی خطرها و برآورد خطرها،
- ایجاد تدابیر امنیتی لازم،
- شناسایی شکاف بین اقدامات امنیتی موجود و موارد مورد نیاز برای هر نوع داده و هر سیستم پردازشی،
- انجام بازنگری و / یا ممیزی،
- آموزش نیروهایی که داده‌های شخصی را پردازش می‌کنند.

۶-۴-۲. متولی زنجیره تأمین داده

گرچه هیچ استراتژی مشخصی در زمینه دولت الکترونیک در مکزیک در دهه ۱۹۹۰ وجود نداشت، اما درنتیجه استفاده دولت از فناوری اطلاعات و ارتباطات، مؤسسه آمار و جغرافیا[1] مسئولیت سیاست فناوری اطلاعات دولت مکزیک را برعهده گرفت. در سال ۲۰۰۱، چارچوب قانونی برای دولت الکترونیک توسط رئیس‌جمهور ابلاغ شد، که این موضوع در (مواد ۶ تا ۱۶) قانون اساسی مکزیک نیز آمده است. همچنین مقررات مربوطه در سال ۲۰۱۰ در قانون فدرال برای حفاظت از اطلاعات شخصی نگهداری شده توسط نهادهای خصوصی، منتشر شده است و مؤسسه ملی شفافیت، دسترسی به اطلاعات و حفاظت از داده‌های شخصی[2] مرجعی است که مسئول نظارت بر قانون است. علاوه‌بر موارد فوق، وزارت اقتصاد مسئول اطلاع‌رسانی و آموزش تعهدات مربوط به حفاظت از داده‌های شخصی بین شرکت‌های ملی و بین‌المللی با فعالیت‌های تجاری در قلمرو مکزیک است [۳۷].

۷-۴-۲. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

مکزیک عضو سازمان همکاری و توسعه اقتصادی بوده و در رتبه‌بندی کشورها در شاخص توسعه خدمات آنلاین محلی[3] دارای رتبه بیستم در جهان و در قاره آمریکا دارای رتبه دهم است [۳۸].

1.National Institute of Statistics and Geography (INEGI(
2.Institute National Access Information
3.Local Online Service Index

۲-۵. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور انگلستان

۲-۵-۱. منابع تولید داده

مهم‌ترین داده‌هایی که توسط منابع مختلف در انگلیس مورد توجه قرار می‌گیرد عبارتند از [۳۹]:

- داده‌های مرتبط با ادارات دولتی،
- داده‌های مرتبط با شوراهای محلی،
- داده‌های مرتبط با مدارس، کالج‌ها و دانشگاه‌ها،
- داده‌های مرتبط با مراکز درمانی، بیمارستان‌ها و جراحی‌های پزشکان،
- داده‌های مرتبط با موزه‌های با بودجه عمومی،
- داده‌های مرتبط با پلیس،
- داده‌های مرتبط با نهادهای عمومی غیربخشی، کمیته‌ها و نهادهای مشورتی.

کلیه شهروندان طی قوانین آزادی اطلاعات[1] امکان ثبت درخواست و دریافت اطلاعات ثبت شده را دارند.

۲-۵-۲. نحوه جمع آوری و یکپارچه‌سازی داده

کشور انگلیس تا پیش از خروج از اتحادیه اروپا اقدامات مربوط به حفاظت از داده‌ها را براساس مقررات عمومی حفاظت از داده‌ها موسوم به جی‌دی‌پی‌آر[2] انجام می‌داد که پس از خروج از اتحادیه اروپا تغییرات اندکی در این مقررات صورت گرفت.

بررسی قوانین کشور انگلستان نشـــان از آن دارد که GDPR اصلی‌ترین قانون در این زمینه است که برای صیانت از حریم خصوصی افراد و محافظت از داده‌های شخصی آنها، طراحی شده است. موضوع GDPR فقط داده‌های شخصی است و اصول مرتبط با پردازش داده‌های شخصی را بررسی می‌کند. با وجود این ابعاد ارائه شده در آن می‌تواند دیدگاهی در زمینه نحوه قانونگذاری برای سایر داده‌ها ارائه کنند. ازاین‌رو، در ادامه جهت آشنایی با این مقررات، بخشی از تعاریف مفاهیم مرتبط، اصول و قواعد جی‌دی‌پی‌آر بیان شده است [۴۰]:

۱.مفاهیم مرتبط با مقررات عمومی حفاظت از داده‌ها

- **داده شخصی:**[3] هر گونه اطلاعات فردی است که به‌طور مستقیم یا غیرمستقیم شناسایی می‌شود.
- **پردازش داده:**[4] هر عملی که بر روی داده‌ها، چه خودکار و چه دستی انجام می‌شود.
- **مالک داده:**[5] کسی که داده شخصی خودش را در اختیار قرار می‌دهد.
- **کنترل کننده داده:**[6] فردی که تصمیم می‌گیرد که چطور و چگونه داده‌های شخصی پردازش شود.
- **پردازشگر داده:**[7] شخص ثالث است که اطلاعات شخصی را از طرف یک کنترل کننده داده پردازش می‌کند.

۲.اصول هفت‌گانه GDPR

- **اصل اول، قانونی بودن، منصف و شفاف بودن:** پردازش داده‌ها باید برای مالک داده‌ها قانونی، منصفانه و شفاف باشد.
- **اصل دوم، محدودیت هدف:** داده‌ها باید براساس اهداف قانونی که به‌طور صریح به آنها اشاره شده است، جمع‌آوری و پردازش گردد.

1 .Freedom of Information (FOI)
2. General Data Protection Regulation (GDPR)
3. Personal Data
4. Data Processing
5. Data subject
6. Data Controller
7.Data processor

- **اصل سوم، به حداقل رساندن داده‌ها:** باید فقط داده‌هایی را که برای اهداف مشخص شده کاملاً ضروری است، جمع‌آوری و پردازش گردد.
- **اصل چهارم، دقت:** باید اطلاعات شخصی به‌صورت دقیق و به‌روز نگهداری گردد.
- **اصل پنجم، محدودیت ذخیره‌سازی:** شرکت‌ها فقط می‌توانند داده‌های شناسایی شخصی را تا زمانی که برای هدف مشخص مورد نیاز است ذخیره نمایند.
- **اصل ششم، یکپارچگی و محرمانه بودن:** پردازش باید به‌گونه‌ای انجام شود تا به‌طور مناسب امنیت، یکپارچگی و محرمانگی را تضمین نماید (مانند استفاده از روش‌های رمزنگاری).
- **اصل هفتم، حسابرسی:** کنترل‌کننده داده، مسئول تطابق اقدامات انجام شده براساس جی‌دی‌پی‌آر، با تمام این اصول است.

قواعد GDPR

- کنترل‌کننده داده باید با اقدامات مناسب اثبات کند که با مقررات و اصول جی‌دی‌پی‌آر سازگار است.
- امنیت داده را با تکنیک‌های فنی و معیارهای سازمانی تأمین کند.
- در طراحی و به‌صورت پیش‌فرض باید اصول حفاظت از داده را در نظر بگیرد.
- موارد قانونی ذخیره‌سازی و پردازش داده در نظر گرفته شود و در هیچ شرایطی از داده، استفاده‌ای به غیر از هدف عنوان شده نکند، مگر در مواردی که مالک داده این اجازه را به‌صراحت داده باشد.
- قوانین مربوط به رضایت مالک داده به‌طور کامل اجرا شود. برای مثال صراحت در ارائه هدف استفاده و اخذ رضایت صریح و مشخص از مالک داده.
- در شرایط خاص باید افسر حفاظت از داده وجود داشته باشد.
- حقوق مشخصی برای فرد صاحب داده‌ها وجود دارد که شـــامل: ۱. حق دریافت اطلاعات، ۲. حق دسترسی، ۳. حق اصلاح، ۴. حق پاک شدن، ۵. حق محدود کردن پردازش، ۶. حق دسترسی به داده‌ها، ۷. حق اعتراض و غیره است.

۳-۵-۲. نحوه توزیع داده

همان‌طور که پیش‌تر نیز اشاره شد، کلیه شهروندان طی قوانین آزادی اطلاعات[1] امکان ثبت درخواست و دریافت اطلاعات ثبت شده را دارند.

۴-۵-۲. امنیت و پردازش داده

همان‌طور که اشاره شد، قانون GDPR متعالی‌ترین قانون در کشور انگلستان در زمینه داده‌ها و اطلاعات است که برخی از ابعاد آن در بخش قبلی ارائه شد. این قانون در زمینه امنیت و پردازش داده‌ها نیز قواعد خاصی را در نظر گرفته است که برای جلوگیری از طولانی شدن گزارش از بیان آنها در این بخش خودداری شده است.

۵-۵-۲. متولی زنجیره تأمین داده

پس از خروج انگلیس از اتحادیه اروپا و تغییرات اعمال شده در GDPR برای اجرای قانون در این کشور، متولی اصلی داده، کمیسیونر اطلاعات[2] معرفی شده است [۴۱].

1.Freedom of Information (FOI)
2.Information Commissioner's Office (ICO)

۶-۵-۲. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

عضویت در سازمان همکاری و توسعه اقتصادی را می‌توان مهمترین عضویت این کشور در سازمان‌های مرتبط دانست همچنین، علاوه‌بر

۶-۲. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور نیوزلند

GDPR، توافق‌های با عناوین قوانین حفاظت از داده[1] و توافق‌نامه تجارت و همکاری[2] را می‌توان به‌عنوان مکمل‌های GDPR معرفی کرد [۴۰].

۶-۲-۱. منابع تولید داده

شهروندان نیوزلندی با مراجعه به سایت اصلی دسترسی به داده در این کشور[3] می‌توانند برای استفاده از داده‌های موجود در چهل گروه و ۱۷۹ سازمان موجود در این سایت، درخواست خود را ثبت کند. مهم‌ترین داده‌هایی که در این وب‌سایت در اختیار عموم مردم و سازمان‌ها قرار داده شده شامل موارد زیر است [۴۲]:

- داده‌های مرتبط با امور زمین،
- داده‌های مرتبط با امور محیط زیست،
- داده‌های مرتبط با امور تحصیلات،
- داده‌های مرتبط با امور زمین لرزه،
- داده‌های مرتبط با امور بازرگانی، تجارت و صنعت.

۶-۲-۲. نحوه جمع آوری و یکپارچه‌سازی داده

در نیوزلند، قانون حفظ حریم خصوصی [۴۳] قانون متعالی در این کشور در زمینه داده‌ها و اطلاعات است که همچون GDPR شامل مفاهیمی شبیه به کنترل کننده‌ها و پردازش کننده‌هاست. قانون حفظ حریم خصوصی در مورد تمام اطلاعات شخصی، جمع آوری شده، ذخیره شده یا نگهداری شده توسط یک مؤسسه اعمال شده و به نوع داده‌ها و نحوه ثبت داده‌ها متکی نیست. علاوه‌بر این، قانون حفظ حریم خصوصی برای همه سازمان‌ها و اشخاص حقیقی و حقوقی چه در بخش‌های مختلف دولتی و چه در بخش‌های خصوصی اعمال می‌شود.

کلیه سازمان‌های موجود در نیوزلند موظف به همکاری با مؤسسات نیازمند به داده و اطلاعات با در نظر گرفتن حساسیت‌های موجود در خصوص داده‌های مرتبط با برخی سازمان‌ها و افراد حقیقی و حقوقی هستند. برای مثال، اطلاعات مربوط به اعضای مجلس، دادگاه‌ها و دادگاه‌های قضایی و رسانه‌های خبری در هنگام انجام فعالیت‌های خبری خود از این قانون مستثناست. علاوه‌بر این، افرادی که اطلاعات شخصی را برای امور شخصی، خانوادگی یا خانگی خود جمع‌آوری یا نگهداری می‌کنند، شامل الزامات این قانون نمی‌باشند (اگرچه در مواردی که جمع‌آوری، افشا یا استفاده برای یک فرد معقول عادی، بسیار توهین‌آمیز باشد، این قانون اعمال نمی‌شود).

قانون حفظ حریم خصوصی برای حفظ محرمانگی «اطلاعات مربوط به یک فرد قابل شناسایی»، از اصطلاح «اطلاعات شخصی» استفاده کرده و دربرگیرنده برخی اطلاعات مانند ثبت تولد، فوت، ازدواج و... است. «اطلاعات» در قانون حفظ حریم خصوصی تعریف نشده، اما در تفسیر سایر قوانین مربوط گفته شده است که «اطلاعات» محدود به کلام مکتوب نیست، بلکه شامل هر دانشی، اعم از ایجاد یا نگهداری می‌شود.

جمع‌آوری، استفاده و افشای اطلاعات شخصی توسط سازمان‌های بخش دولتی و خصوصی باید با ۱۳ اصل حفظ حریم خصوصی مندرج در قانون حفظ حریم خصوصی مطابقت داشته باشد که این اصول را می‌توان به‌عنوان تعهدات زیر خلاصه کرد:

۱. جمع‌آوری اطلاعات برای یک هدف قانونی (فقط تا حدی که برای آن هدف ضروری است) از طریق ابزارهای قانونی و مستقیماً از موجودیت

1 .Data Production Act (DPA)
2. Trade and Cooperation Agreement (TCA)
3. data.govt.nz

مرتبط با داده با رعایت استثنائات ارائه شده است.

۲. هدف قانونی جمع‌آوری و گردآوری اطلاعات را شناسایی و به موجودیت مرتبط داده‌ها اطلاع دهد.

۳. حفاظت از اطلاعات در برابر از دست دادن، دسترسی، استفاده، اصلاح، افشا و سایر سوءاستفاده‌ها و حفظ اطلاعات به‌گونه‌ای که آژانس بتواند وجود اطلاعات را تأیید یا تصحیح یا دسترسی به اطلاعات را بنابه درخواست موجودیت مرتبط داده فراهم کند.

۴. اقداماتی جهت حصول اطمینان از دقت، به‌روز، کامل، مرتبط و گمراه‌کننده نبودن اطلاعات.

۵. اطلاعات را فاش نکند، مگر اینکه قانون این امکان را منع نکرده باشد. در مورد افشای اطلاعات به یک سازمان خارج از کشور، تنها درصورتی که آژانس دریافت‌کننده تدابیری مشابه با موارد مندرج در قانون حفظ حریم خصوصی باشد، امکان مبادله را خواهد داشت.

در ارتباط با اصول سیزده‌گانه تلخیص شده فوق، برخی استثناها به‌شرح زیر وجود دارد:

- قانون حفظ حریم خصوصی تنها تا حدی اعمال می‌شود که با قانون دیگری از پارلمان مغایرت نداشته باشد.
- در شرایط خاص، کمیسیونر حریم خصوصی می‌تواند به آژانس‌ها اجازه دهد تا اطلاعات را جمع‌آوری، استفاده یا افشا کنند، حتی زمانی که این اطلاعات معمولاً اصول حریم خصوصی مشخص شده را نقض می‌کند.
- هنگام پردازش اطلاعات شخصی در مورد کارمندان، برخی قوانین اضافی وجود دارد. با این حال، الزامات UEMA [1] در شرایطی که فرستنده و گیرنده رابطه خاصی دارند و پیام حاوی اطلاعات مربوط به آن رابطه است، مانند اطلاعات مربوط به استخدام یا مزایای خاص، اعمال نمی‌شود.
- هر سازمان دولتی و خصوصی باید حداقل یک افسر حفظ حریم خصوصی (از داخل یا خارج از سازمان) داشته باشد. قانون حفظ حریم خصوصی مسئولیت‌های افسر حفظ حریم خصوصی را مشخص کرده است که از مهم‌ترین آنها می‌توان به موارد زیر اشاره کرد:
  - تشویق آژانس به پیروی از اصول حفظ حریم خصوصی،
  - رسیدگی به درخواست‌های ارائه شده به آژانس تحت قانون حفظ حریم خصوصی (مانند درخواست برای دسترسی به اطلاعات شخصی، یا تصحیح اطلاعات شخصی)،

همکاری با دفتر کمیسر حریم خصوصی در رابطه با تحقیقات انجام شده براساس شکایات ارائه شده تحت قانون حفظ حریم خصوصی در رابطه با آژانس، در غیر این صورت از انطباق آژانس با قانون حفظ حریم خصوصی اطمینان حاصل شود.

- دفتر کمیسر حریم خصوصی همچنین توصیه می‌کند که یک افسر حفظ حریم خصوصی باید:
  - از نحوه استفاده از اطلاعات شخصی با رعایت اصول حفظ حریم خصوصی در قانون حفظ حریم خصوصی و هر قانون دیگری، آشنایی داشته باشد.
  - به شکایت مشتریان آژانس در مورد نقض احتمالی حریم خصوصی رسیدگی کند.
  - سایر کارکنان آژانس را برای برخورد صحیح با حریم خصوصی آموزش دهد.
  - مدیران را در مورد چگونگی اطمینان از مطابقت شیوه‌های تجاری آژانس با الزامات حریم خصوصی، تأثیرات حریم خصوصی، تغییرات در رویه‌های تجاری آژانس و تحلیل بهبود کسب‌وکار در اثر بهبود شیوه‌های حفظ حریم خصوصی، راهنمایی کند.
- کمیسر حریم خصوصی همچنین می‌تواند از یک آژانس بخواهد که نام و اطلاعات تماس افسران حریم خصوصی آژانس را ارائه کند تا بتواند به درخواست‌های عمومی درباره اطلاعات شخصی آژانس پاسخ دهد.

اصل (۵) حریم خصوصی از قانون حفظ حریم خصوصی، سازمان‌ها را ملزم می‌کند از اطلاعات شخصی با این گونه تدابیر امنیتی محافظت کنند تا در شرایط موردنیاز در برابر از دست دادن، دسترسی، استفاده، اصلاح، افشا و سایر سوءاستفاده‌ها، تصمیم‌های مناسب اتخاذ شود. اگر باید اطلاعات به شخص ثالث داده شود، آژانس باید تمام توان خود را مبذول دارد تا از استفاده غیرمجاز یا افشای غیرمجاز اطلاعات توسط شخص ثالث جلوگیری شود.

1 .Unsolicited Electronic Messages Act (UEMA)

قانون خاص حاکم بر پردازش توسط نمایندگان شخص ثالث (پردازنده‌ها) قانون حفظ حریم خصوصی است که حاوی قوانین خاص در مورد الزامات امنیتی است و در آن اطلاعات توسط یک عامل شخص ثالث پردازش می‌شود. با این حال، همان‌طور که در بالا ذکر شد، در مواردی که یک آژانس اطلاعات شخصی را به‌عنوان نماینده یا برای صرفاً پردازش اطلاعات از طرف یک آژانس دیگر نگهداری می‌کند و یا از اطلاعات برای اهداف خود استفاده یا افشا نمی‌کند، اطلاعات در اختیار آژانس قرار می‌گیرد که از طرف آن نگهداری یا پردازش می‌شود. علاوه‌بر این، قانون حفظ حریم خصوصی مقرر می‌دارد که یک مدیر مسئول در قبال اعمال یا کوتاهی‌های نماینده خود در مورد پردازش اطلاعات شخصی است، مگر اینکه این کار بدون مجوز صریح یا ضمنی آژانس (اصلی) انجام یا حذف شود[۴۲].

بر این اساس، هنگامی که یک سازمان یک نماینده شـــخص ثالث را برای پردازش اطلاعات شخصی از طرف خود منصوب می‌کند، سازمان مربوطه تحت قانون حفظ حریم خصوصی مسئول باقی خواهد ماند تا اطمینان حاصل شود که اصول حفظ حریم خصوصی اطلاعات (ازجمله الزامات امنیتی در اصل (۵)) همچنان رعایت می‌شود.

در ۸ اوت ۲۰۱۱ دولت نیوزلند اصول جدیدی را برای مدیریت داده‌ها و اطلاعاتی که در اختیار دارد تصویب کرد که جایگزین چارچوب سیاست ۱۹۹۷ برای اطلاعات دولتی شد. این اصول برای اطمینان از مدیریت با کیفیت بالای داده که دولت به نمایندگی از مردم در اختیار دارد، ایجاد شده اســـت. دولت نیوزلند اعلان می‌دارد که به‌طور خلاصه، داده‌ها و اطلاعات دولتی باید باز، به‌راحتی در دسترس، به‌خوبی مدیریت شده، دارای قیمت مناسب و قابل استفاده مجدد باشد.

این قانون دارای اصولی در زمینه مدیریت داده‌ها و اطلاعات است که در ادامه به بیان آنها پرداخته شده است:

۱ **اصل اول: باز باشد:** داده‌ها و اطلاعاتی که توسط دولت نگهداری می‌شود باید برای دسترسی عموم باز باشد، مگر اینکه دلایلی برای امتناع یا محدودیت‌هایی براساس قانون اطلاعات رسمی یا سایر سیاست‌های دولتی وجود داشته باشد. در چنین مواردی باید از آنها محافظت کرد.

۲ **اصل دوم: محافظت شده باشد:** داده‌ها و اطلاعات شخصی، محرمانه و طبقه‌بندی شده محافظت می‌شوند.

۳ **اصل سوم: به‌راحتی در دسترس باشد:** داده‌ها و اطلاعات باز به‌صورت فعال و بدون تبعیض منتشر می‌شوند. آنها قابل رؤیت و در دسترس هستند و به‌صورت آنلاین منتشر می‌شوند.

۴ **اصل چهارم: مورد اعتماد و معتبر باشد:** داده‌ها و اطلاعـــات از اهدافی که برای آنها جمع‌آوری شده‌اند پشتیبانی می‌کنند و در آن زمینه دقیق، مرتبط، به‌موقع، سازگار و بدون سوگیری هستند. در صورت امکان، یک منبع واحد معتبر شناسایی شده وجود دارد.

۵ **اصل پنجم: به‌خوبی مدیریت شوند:** داده‌ها و اطلاعات نگهداری شده و متعلق به دولت، عملاً متعلق به عموم مردم نیوزلند است. این داده ها دارایی استراتژیک مردم هستند که توسط دولت به‌عنوان امانتدار، از طرف مردم نگهداری می‌شود. دولت ملزم است که سیاست هایی را در جهت تولید یا جمع آوری داده ها مشخص سازد.

نهادهای حاکمیتی، حافظ داده‌ها و اطلاعات دولتی هستند و باید شیوه‌های مناسبی را برای مدیریت داده‌ها و اطلاعات در طول چرخه عمر خود فراهم کنند ، ازجمله مراقبت از داده ها و حفظ و دسترسی طولانی‌مدت به آنها. همکاری با سایر مؤسسات و مردم، تسهیل دسترسی، تقویت آگاهی و حمایت از همکاری بین‌المللی نیز از دیگر الزامات و وظایف نهادهای حاکمیتی است که بصورت روزانه باید مراعات گردد.

۶ **اصل ششم: قیمت مناسب داشته باشد:** انتظار می‌رود استفاده و استفاده مجدد از داده‌ها و اطلاعات دولتی رایگان باشد و پرداخت هزینه بابت دریافت دسترسی به داده، ممنوع است. قیمت‌گذاری برای پوشش هزینه‌های انتشار تنها زمانی مناسب است که بتوان به‌وضوح نشان داد که این قیمت‌گذاری به‌عنوان مانعی برای استفاده یا استفاده مجدد از داده‌ها عمل نمی‌کند. اگر هزینه‌ای برای دسترسی به داده‌ها اعمال می‌شود، باید شفاف، سازگار، معقول و برای همه درخواست‌کنندگان هزینه یکسان باشد.

۷ **اصل هفتم: قابل استفاده مجدد باشد:** داده‌ها و اطلاعات منتشر شده را می‌توان در طول زمان و از طریق تغییرات فناوری کشف و به اشتراک گذاشت و برای عموم استفاده کرد. متقاضیان مطابق با چارچوب دسترسی آزاد و مجوز دولت نیوزلند، امکان ذخیره‌سازی داده‌های موجود را برای استفاده مجدد دارند. انواع روش‌های انتشار داده به‌شرح زیر است:

- در قالب قابل استفاده مجدد و قابل خواندن توسط ماشین،
- با ابر داده مناسب،
- درصورتی‌که نتوان آنها را در حالت اولیه منتشر کرد، به‌صورت مجموع یا اصلاح شده.

داده‌ها و اطلاعات منتشر شده در قالب‌های اختصاصی نیز در قالب‌های باز و غیراختصاصی منتشر می‌شوند. فناوری‌های حقوق دیجیتال بر مواردی که برای استفاده مجدد در دسترس هستند تحمیل نمی‌شوند[۴۴].

۲-۶-۳. رویکرد پردازش داده، توزیع داده و امنیت داده

در زمینه پردازش، توزیع و امنیت داده نکاتی در بخش قبلی بیان شده است، اما از بیان نکات تکمیلی از قانون حفظ حریم خصوصی[۴۳] برای جلوگیری از طولانی شدن گزارش خودداری می‌شود.

۲-۶-۴. متولی زنجیره تأمین داده

طبق قانون حریم خصوصی مصوب ۱ دسامبر ۲۰۲۰، دفتر کمیسر حریم خصوصی متولی داده‌های عمومی است. که زیر نظر بالاترین مقام نیوزلند قرار دارد.

۲-۶-۵. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

نیوزلند هم عضو سازمان همکاری و توسعه اقتصادی و هم عضو کمیسیون اقتصادی و اجتماعی سازمان ملل متحد برای آسیا و اقیانوسیه است.

۲-۷. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور کره‌جنوبی

۲-۷-۱. منابع تولید داده

براساس نقشه داده‌های ملی کره‌جنوبی می‌توان به اصلی‌ترین منابع داده‌ای این کشور به‌شرح زیر اشاره کرد[۴۵]:

- علم و فناوری،
- حمل‌ونقل،
- رفاه اجتماعی،
- مسکن و شهرسازی،
- سلامت و درمان،
- قوانین و امور حقوقی،
- و....

۲-۷-۲. جمع‌آوری و یکپارچه‌سازی داده

پردازش داده ملی در کره‌جنوبی توسط «کمیته ملی به اشتراک‌گذاری و دسترسی به داده‌های عمومی»[1] انجام می‌شود. این سازمان دولتی در سال ۲۰۱۳ تأسیس شده است و مسئولیت توسعه و اجرای سیاست‌های داده ملی، ایجاد چارچوب‌های قانونی و اخلاقی برای استفاده از داده‌های عمومی و ترویج اشتراک و دسترسی به داده‌های عمومی را برعهده دارد[۴۶].

1 .National Committee for Public Data Sharing and Accessibility (NCPDI)

۳-۷-۲.پردازش داده

NCPI از یک چارچوب پردازش داده ملی شامل چهار لایه ارائه شده در شکل ۵ استفاده می‌کند.

شکل۵.چارچوب پردازش داده‌ملی کره‌جنوبی[۴۷]

NCPI از فناوری‌های مختلفی برای پردازش داده ملی نظیر فناوری‌های زیر استفاده می‌کند:

۱ **یادگیری ماشین:** یادگیری ماشین برای تجزیه‌وتحلیل داده‌ها و شناسایی الگوها استفاده می‌شود.

۲ **هوش‌مصنوعی:** هوش‌مصنوعی برای اتوماسیون وظایف پردازش داده استفاده می‌شود.

۳ **رایانش ابری:** ابر محاسبات برای ذخیره و پردازش داده‌های بزرگ استفاده می‌شود.

۴-۷-۲.نحوه توزیع داده

توزیع و اشتراک‌گذاری داده ملی در کره‌جنوبی در پرتال ملی داده‌باز کره جنوبی[1] انجام شده و به‌عنوان یکی از مهم‌ترین پلتفرم‌های داده ملی در جهان شناخته می‌شود که به سازمان‌ها و افراد اجازه می‌دهد، داده‌های دولتی را به‌صورت رایگان دانلود و استفاده کنند.

در سال ۲۰۱۷، NCPI پلتفرم اشـــتراک داده‌های عمومی کره‌جنوبی را راه‌اندازی کرد. این پلتفرم به سازمان‌های دولتی و خصوصی اجازه می‌دهد تا داده‌های عمومی را به اشتراک بگذارند. درحال‌حاضر بیش از ۱۵۰ میلیون رکورد داده از صد سازمان دولتی را در خود جای داده است. این پلتفرم به دولت کره‌جنوبی کمک کرده است تا داده‌های دولتی را به‌صورت شفاف و قابل دسترس برای عموم مردم منتشر کند[۴۵].

۵-۷-۲.امنیت داده

این کشور در سال ۲۰۱۹ قانون امنیت داده ملی[2] (DSN)، را تصویب کرده است که چارچوب قانونی لازم برای محافظت از داده‌های ملی را فراهم می‌کند. همچنین، کره‌جنوبی در حال توسعه زیرساخت‌های امنیتی خود برای مقابله با تهدیدات سایبری است.

براساس قانون امنیت داده ملی کره‌جنوبی (DSN)، نظارت بر امنیت داده‌های خصوصی در کره‌جنوبی برعهده سازمان ملی امنیت اطلاعات (NIS) است. NIS نهادی مستقل است که مسئولیت امنیت ســـایبری در کره‌جنوبی را برعهده دارد. این سازمان در زمینه امنیت داده ملی

1. https://www.data.go.kr/en/index.do
2. Data Protection Law in South Korea

اقداماتی مانند نظارت بر امنیت زیرساخت‌های اطلاعاتی دولتی و خصوصی را نیز برعهده دارد[۴۸]. براساس DSN، دولت کره‌جنوبی مسئول حفاظت از داده‌های خصوصی شهروندان است. این مسئولیت شامل جمع‌آوری، ذخیره، پردازش، و انتقال داده‌ها می‌شود. دولت کره‌جنوبی برای انجام این مسئولیت، یک سازمان ذیل وزارت اطلاعات و ارتباطات به‌نام آژانس امنیت و اینترنت کره[۱] را ایجاد کرده است.

KISA مسئول اجرای DSN و نظارت بر امنیت داده‌های خصوصی در کره‌جنوبی است. این سازمان برای انجام این مسئولیت، اقدامات زیر را انجام می‌دهد[۴۹]:

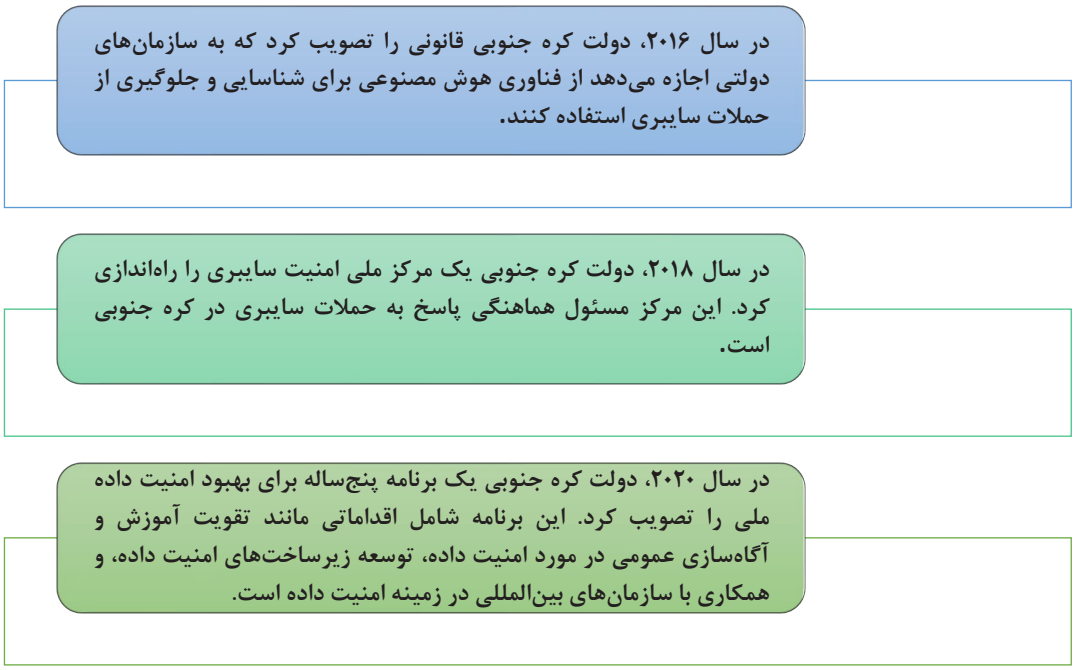
- توسعه و اجرای استانداردهای امنیت داده،
- آموزش و آگاه‌سازی عمومی در مورد امنیت داده،
- انجام تحقیقات و مطالعات در زمینه امنیت داده،
- همکاری با سازمان‌های بین‌المللی در زمینه امنیت داده.

KISA همچنین یک پایگاه داده مرکزی از داده‌های شخصی شهروندان کره‌جنوبی را اداره می‌کند. این پایگاه داده شامل اطلاعات هویتی، آدرس، شماره تلفن، و سایر اطلاعات شخصی شـــهروندان اســـت. KISA از این پایگاه داده برای نظارت بر دسترسی به داده‌های شخصی و جلوگیری از دسترسی غیرمجاز استفاده می‌کند.

شکل ۶ برخی از اقدامات خاص دولت کره‌جنوبی برای بهبود امنیت داده ملی را ارائه می‌کند.

با این حال، هنوز چالش‌هایی در زمینه امنیت داده ملی در کره‌جنوبی وجود دارد. یکی از چالش‌ها، افزایش حجم داده‌های دیجیتالی است که باید محافظت شوند. چالش دیگر، پیشرفت سریع فناوری است که می‌تواند تهدیدات جدیدی را برای امنیت داده‌ها ایجاد کند[۴۷].

شکل ۶. چارچوب پردازش داده ملی کره‌جنوبی[۵۰]



۲-۷-۶. متولی زنجیره تأمین داده

متولی زنجیره تأمین داده ملی در کره‌جنوبی، آژانس ملی آمار کره[1] است. KOSTAT یک سازمان دولتی است که مسئول جمع‌آوری، تجزیه‌وتحلیل و انتشار داده‌های آماری در کره‌جنوبی است. این سازمان همچنین مسئول توسعه و اجرای سیاست‌های آماری در کشور است[۵۱].

۲-۷-۷. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

کره‌جنوبی عضو چندین سازمان بین‌المللی داده است که ازجمله آنها می‌توان به موارد زیر اشاره کرد[۵۲]:

سازمان بین‌المللی استاندارد:[2] کره‌جنوبی در سال ۱۹۵۵ عضو ISO شده است و درحال‌حاضر در بیش از دویست کمیته فنی ISO مشارکت دارد. این کشور همچنین عضو هیئت مدیره ISO و چندین کمیته فرعی آن است.

سازمان توسعه صنعتی ملل متحد:[3] کره‌جنوبی در سال ۱۹۶۶ عضو UNIDO شده است و درحال‌حاضر در چندین برنامه و پروژه این سازمان مشارکت دارد. این کشور همچنین عضو هیئت مدیره UNIDO و چندین کمیته فنی آن است.

سازمان همکاری اقتصادی و توسعه:[4] کره‌جنوبی در سال ۱۹۹۶ عضو OECD شده است و درحال‌حاضر عضو شورای اقتصادی و اجتماعی OECD و چندین کمیته فنی آن است.

سازمان همکاری و توسعه اقتصادی آسیا و اقیانوسیه:[5] کره‌جنوبی یکی از اعضای بنیانگذار APEC است و درحال‌حاضر عضو شورای اقتصادی و تجاری APEC و چندین کمیته فنی آن است.

اتحادیه بین‌المللی مخابرات:[6] کره‌جنوبی در سال ۱۹۵۹ عضو ITU شده است و درحال‌حاضر در چندین کمیته فنی ITU مشارکت دارد. این کشور همچنین عضو هیئت مدیره ITU و چندین کمیته فرعی آن است.

سازمان جهانی مالکیت معنوی:[7] کره‌جنوبی در سال ۱۹۶۶ عضو WIPO شده است و درحال‌حاضر در چندین کمیته فنی WIPO مشارکت دارد. این کشور همچنین عضو هیئت مدیره WIPO و چندین کمیته فرعی آن است.

کره‌جنوبی از طریق مشارکت در کمیته‌های فنی ISO، UNIDO، OECD، APEC، ITU و WIPO، در تدوین استانداردهای بین‌المللی داده نقش فعالی ایفا می‌کند. این استانداردها به ایجاد یکپارچگی در زمینه داده‌ها در سطح بین‌المللی کمک می‌کنند.

۲-۸-۱. منابع تولید داده

۲-۸. بررسی متولیان و نحوه عملکرد بخش‌های مختلف زنجیره ارزش در کشور ایران

براساس قانون مدیریت داده‌ها و اطلاعات ملی، درحال‌حاضر نزدیک به ۲۷ پایگاه داده عمومی و اطلاعات پایه در سازمان‌ها و ادارات دولتی رایج است، که هرکدام به‌صورت جزیره‌ای تولید شده و به‌جز تعداد اندکی از آنها، مابقی هیچ‌گونه ارتباطی با همدیگر ندارند.

۲-۸-۲. نحوه جمع‌آوری و یکپارچه‌سازی داده

نهادهای مختلفی در کشور در حال جمع‌آوری و تولید داده‌ها هستند، اما این اطلاعات به‌صورت یکپارچه تنظیم و مدیریت نمی‌شود.

بررسی به عمل‌آمده در مورد منابع تولید داده و ذی‌نفعان مرتبط نشان از آن دارد که برخی از پایگاه‌های داده فعال در کشور درحالی‌که با یکدیگر ارتباط سیستمی براساس مرکز ملی تبادل داده دارند، اما خارج از این مرکز نیز در حال تبادل داده هستند! ولیکن این امر به‌صورت

1 .Korea Internet and Security Agency (KISA)
2 .International Organization for Standardization (ISO)
3 .United Nations Industrial Development Organization (UNIDO)
4 .Organization for Economic Co-operation and Development (OECD)
5 .Asia-Pacific Economic Cooperation (APEC)
6 .International Telecommunication Union (ITU)
7 .World Intellectual Property Organization (WIPO)

موردی مشاهده شده است. در برخی سازمان‌ها صرفاً اندک اطلاعاتی به‌صورت دسترسی عموم وجود دارد. از جمله این موارد می‌توان به استعلام اشتغال[1] اشاره کرد. همچنین مرکز ملی آمار ایران[2] و بانک مرکزی ایران،[3] برخی اطلاعات عمومی را در اختیار عموم مردم قرار داده است.

موضوع یکپارچه‌سازی اطلاعات ملی با هدف ارائه خدمات منسجم به مردم از جمله اهداف «طرح یکپارچه‌سازی داده و اطلاعات ملی» است که در نیمه دوم سال ۱۳۹۹ در مجلس شورای اسلامی اعلام وصول و در آبان‌ماه ۱۴۰۱ تحت‌عنوان قانون مدیریت داده‌ها و اطلاعات ملی به تصویب مجلس شورای اسلامی رسیده است. براساس این قانون، شورای عالی فضای مجازی متولی سیاستگذاری در حوزه حکمرانی داده به‌طور خاص داده‌های عمومی خواهد بود. در این قانون، پایگاه داده و اطلاعات پایه، کلیه پایگاه‌داده‌ها و اطلاعاتی است که در ایجاد و ارائه خدمات الکترونیکی و هوشمند و اجرای فرایندهای الکترونیکی نقش پایه‌ای دارند.

همچنین براساس ماده (۷) این قانون، تبادل داده‌ها و اطلاعات بین دستگاه‌ها و نهادهای مشمول این قانون با دستگاه‌های اجرایی و یا کسب‌وکارها با رعایت اصول حفاظتی و امنیتی برعهده، مرکز ملی تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات است.

با وجود وظایف محول شده به دو نهاد مذکور، بررسی‌های تکمیلی نشان از آن دارد که اقدام‌های این دو نهاد کفایت لازم را برای سامان‌دهی به جمع‌آوری و یکپارچه‌سازی داده به‌همراه نداشته است. همچنین براساس تصویب‌نامه در خصوص ایجاد مرکز داده دولت به همراه نظام به‌روزرسانی مستمر و بر خط داده‌ها و اطلاعات مصوب ۱۳۹۵/۱۰/۱۲ هیئت وزیران در آدرس DATA.GOV.IR مرجع نظام داده‌ای دولت ایجاد شده است.

۳-۸-۲. رویکرد پردازش داده

در قانون مدیریت داده‌ها و اطلاعات ملی به ذکر این تکلیف بسنده شده که دستگاه‌ها و نهادهای مشمول این قانون که براساس شرح وظایف مقرر در قوانین مربوطه و نیز تکالیف ناشی از این قانون موظف به تولید، نگهداری، پردازش داده و اطلاعات می‌باشند مکلف شده‌اند که در امر تولید، نگهداری، پردازش، حفظ امنیت و صیانت از داده‌های شخصی و تبادل و اشتراک‌گذاری و تکمیل و به‌روزرسانی داده‌ها و اطلاعات ملی، سیاست‌ها و نظامات مصوب شورای عالی فضای مجازی و مصوبات کمیسیون داده‌ها و اطلاعات ملی (دوام) را اعمال و اجرا کنند. همچنین در مصوبه شماره دو، نود و ششمین جلسه شورای عالی فضای مجازی مورخ ۱۴۰۲/۰۸/۲۳ با عنوان «ایجاد سامانه ملی و جامع داده‌ها» مقرر شده مرکز ملی فضای مجازی کشور موظف است ظرف مدت ۳ ماه، سامانه ملی سنجش و پایش داده‌ای فضای مجازی را در تمامی لایه‌های فضای مجازی (لایه‌های زیرساخت و خدمات شبکه ملی اطلاعات، خدمات کاربردی و محتوا) ایجاد نماید. کلیه دستگاه‌ها، سازمان‌ها، نهادها و تنظیم‌گران بخشی موظفند براساس درخواست مرکز ملی فضای مجازی کشور، ظرف مدت یک‌ماه، دسترسی به داده‌ها و سامانه‌های مرتبط با فضای مجازی درخواست شده را فراهم نمایند.

۴-۸-۲. نحوه توزیع داده

در زمینه دسترسی آزاد به داده‌ها و اطلاعات، مجلس شورای اسلامی در بهمن ماه سال ۱۳۸۷، قانون انتشار و دسترسی آزاد به اطلاعات را در ۲۳ ماده به تصویب رسانده است. در ماده (۵) این قانون آمده است که مؤسسات عمومی مکلفند اطلاعات موضوع این قانون را در حداقل زمان ممکن و بدون تبعیض در دسترس مردم قرار دهند.

درحال‌حاضر از طریق سامانه ملی انتشار و دسترسی آزاد به اطلاعات[1] امکان ثبت درخواست برای دریافت نوع مشخصی از داده فراهم شده است. البته این سامانه با مشکلاتی از لحاظ عملیاتی مواجه است. همچنین مرکز ملی آمار ایران و بانک مرکزی و دیگر نهادها و دستگاه‌ها براساس ماده (۳) قانون ارتقای سلامت نظام اداری و مقابله با فساد، ملزم به ارائه اطلاعات قراردادها در سامانه‌ای مشخص شده‌اند.

همچنین برای حمایت از کسب‌وکارهای دیجیتال در آیین‌نامه حمایت از سکوها و کسب‌وکارهای اقتصاد رقومی (دیجیتال) مصوب ۱۴۰۱/۰۸/۱۰ هیئت‌وزیران بحث‌های زیرساختی مورد توجه قرار گرفته است.

1 .estelam.msrt.ir
2.https://amar.org.ir/
3.https://www.cbi.ir/

۵-۸-۲. پرداختن به موضوع امنیت داده

در زمینه امنیت داده، اسناد مختلفی در کشور طراحی شده است. در این اســناد تلاش شده است تا موضوع امنیت داده از مناظر مختلف تحت بررسی قرار گیرد. برای مثال، ماده (۳۵) منشور حقوق شهروندی، اظهار دارد که «حق شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند». همچنین ماده (۳۷) این منشور بیان می کند: «تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیرالکترونیکی، اطلاعات و داده‌های شخصی و نیز سایر مرسولات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند اینها ممنوع است مگر به‌موجب قانون». در ماده (۳۰) نیز به الزام حفظ و حراست اطلاعات شخصی افراد که در نزد سازمان‌ها و نهادهای مختلف است، تأکید می‌شود. اهمیت پرداختن به حفظ حریم خصوصی تا جایی مطرح است که مطابق با ماده (۸۲) منشور حفظ حقوق شهروندی، گزینش و اشتغال افراد از روش‌های ناقض حریم خصوصی ممنوع شده است[۵۳].

در قانون انتشار و دسترسی آزاد به اطلاعات نیز استثنائاتی در زمینه دسترسی به اطلاعات بیان شده است که از این میان می‌توان به اسرار دولتی و حریم خصوصی مطرح در قانون (مگر در شرایطی که دارنده آن اجازه انتشار داده باشد یا خواهان اطلاعات، ولی، قیم یا وکیل او باشد و غیر این صورت تهدیدی بر امنیت و آسایش عمومی محسوب می‌شود) اشاره کرد. در ماده (۱۴) این قانون نیز مستقیماً اشاره به حریم خصوصی، اطلاعات تحصیل شده از روش‌های ناقض حریم خصوصی شده و آن را ممنوع کرده و بیان شده است: «چنانچه اطلاعات درخواست شده مربوط به حریم خصوصی اشخاص باشد و یا در زمره اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود».

علاوه بر موارد فوق، فصل سوم قانون تجارت الکترونیک (مصوب ۱۳۸۲/۱۰/۱۷) به‌صورت خاص به امنیت داده و حمایت از داده پیام‌های شخصی در ماده‌های (۵۸) تا (۶۱) پرداخته است.

در نهایت، در ماده (۶) قانون مدیریت داده‌ها و اطلاعات ملی، اعمال تدابیر حفاظتی و امنیتی جهت صیانت از داده‌ها و اطلاعات و حفظ محرمانگی داده‌ها و اطلاعات اشخاص برعهده دستگاه‌ها و نهادهای مشمول این قانون و ارائه‌دهندگان خدمات ذیل تنظیم‌گران بخشی است که مسئول تولید، نگهداری یا پردازش کننده داده‌ها و اطلاعات هستند. همچنین مطابق ماده (۸) همین قانون، برای صیانت و حفظ یکپارچگی در داده‌ها و اطلاعات ملی و صرفه‌جویی در تبادل داده‌ها و اطلاعات، دولت می‌تواند متناسب با کارکرد و نحوه و تواتر به‌روزرسانی آنها در مراکز داده دولت، براساس مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی، این داده‌ها را نگهداری نماید. دستگاه‌ها و نهادهای مشمول این قانون موظف به به‌روزرسانی بر خط این پایگاه‌های اطلاعاتی هستند. تعیین سطح دسترسی به این پایگاه‌های اطلاعات به‌موجب مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی است.

همچنین دستورالعمل سامان‌دهی خدمات میزبانی در فضای مجازی کشور مصوب یکصد و بیست و هشتمین جلسه کمیسیون عالی تنظیم مقررات فضای مجازی کشور براساس وظایف و اختیارات مصرح در بندهای «۳۲۱» و «۵۲۳» سند شرح وظایف، اختیارات و ترکیب اعضای کمیسیون عالی تنظیم مقررات فضای مجازی کشور (مصوب هشتاد و یکمین جلسه مورخ ۱۴۰۱/۰۲/۲۷ شورای عالی فضای مجازی کشور)» و در راستای اجرای سند «نظام هویت معتبر در فضای مجازی» (مصوب پنجاه و نهمین جلسه مورخ ۱۳۹۸/۰۶/۰۹ شورای عالی فضای مجازی کشور)، با هدف سامان‌دهی احراز هویت و تشکیل پایگاه شناسنامه اشخاص حقیقی و حقوقی متقاضی فضای میزبانی در ابرها و مراکز داده داخلی، تصویب شده است.

۶-۸-۲. متولی زنجیره تأمین داده

مقام معظم رهبری در اسفندماه ســال ۱۳۹۰، ضمن تأکید بر اهمیت راهبری و مدیریت فضای مجازی کشور، دستور تشکیل شورای عالی فضای مجازی را صادر نمودند و در فروردین‌ماه سال ۱۴۰۱، با تصویب قانون مدیریت داده‌ها و اطلاعات ملی توسط مجلس شورای اسلامی، شورای عالی فضای مجازی متولی سیاستگذاری و تصویب راهبردهای کلان نظام تولید، نگهداری، پردازش، دسترسی، یکپارچه‌سازی، تبادل و امنیت داده و اطلاعات ملی با هدف افزایش قدرت حکمرانی، سامان‌دهی و انسجام‌بخشی به نظام تبادل داده‌ها و اطلاعات، گسترش تبادل اطلاعات میان دستگاه‌ها و نهادهای مشمول این قانون و تسهیل دسترسی به اطلاعات پایه برای کسب‌وکارهای بخش خصوصی شده است.

1.Iranfoia.ir

همچنین در ماده (۱۸)، قانون انتشار و دسترسی آزاد به اطلاعات بیان شـــده است که، برای حمایت از آزادی اطلاعات و دسترسی همگانی به اطلاعات موجود در مؤسسات عمومی و مؤسسات خصوصی که خدمات عمومی ارائه می‌دهند، تدوین برنامه‌های اجرایی لازم در عرصه اطلاع‌رسانی، نظارت کلی بر حُسن اجرا، رفع اختلاف در چگونگی ارائه اطلاعات موضوع این قانون از طریق ایجاد وحدت رویه، فرهنگ‌سازی، ارشاد و ارائه نظرات مشورتی، کمیسیون انتشار و دسترسی آزاد به اطلاعات به دستور رئیس‌جمهور با ترکیب، وزیر فرهنگ و ارشاد اسلامی (رئیس کمیسیون)، وزیر ارتباطات و فناوری اطلاعات یا معاون ذی‌ربط، وزیر اطلاعات یا معاون ذی‌ربط، وزیر دفاع و پشتیبانی نیروهای مسلح یا معاون ذی‌ربط، رئیس سازمان مدیریت و برنامه‌ریزی کشور یا معاون ذی‌ربط، رئیس دیوان عدالت اداری، رئیس کمیسیون فرهنگی مجلس شورای اسلامی و دبیر شورای عالی فناوری اطلاعات کشور تشکیل شده است.

براساس قانون مدیریت داده‌ها و اطلاعات ملی، تبادل داده و اطلاعات بین دســـتگاه‌ها و نهادهای مشمول این قانون با دستگاه‌های اجرایی و یا کسب‌وکارها با رعایت اصول حفاظتی و امنیتی برعهده مرکز ملی تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات خواهد بود. برای صیانت و حفظ یکپارچگی در داده‌ها و اطلاعات ملی و صرفه‌جویی در تبادل داده‌ها و اطلاعات، دولت می‌تواند متناســـب با کارکرد و نحوه و تواتر به‌روزرسانی آنها در مراکز داده دولت، براساس مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی، این داده‌ها را نگهداری نماید. دستگاه‌ها و نهادهای مشمول این قانون موظف به به‌روزرسانی بر خط این پایگاه‌های اطلاعاتی هستند. تعیین سطح دسترسی به این پایگاه‌های اطلاعات به موجب مصوبه کارگروه تعامل‌پذیری دولت الکترونیکی است. همچنین مطابق ماده (۲) «قانون مدیریت داده‌ها و اطلاعات ملی، سیاستگذاری و تصویب راهبردهای کلان نظام تولید، نگهداری، پردازش، دسترسی، یکپارچه‌سازی، تبادل و امنیت داده‌ها و اطلاعات ملی با هدف افزایش قدرت حکمرانی، سامان‌دهی و انسجام بخشی به نظام تبادل داده‌ها و اطلاعات، گسترش تبادل اطلاعات میان دستگاه‌ها و نهادهای مشمول این قانون و تسهیل دسترسی به اطلاعات پایه برای کســـب‌وکارهای بخش خصوصی برعهده «شورای عالی فضای مجازی» است. براساس ماده (۳) همین قانون، «کارگروه تعامل‌پذیر دولت الکترونیکی» مصوب شورای عالی فضای مجازی موظف است در تصمیم‌گیری‌های خود به استثنای امر قضا نسبت به اعمال سیاست‌ها و راهبردهای کلان و نظارت و مدیریت بر نحوه نگهداری، پردازش، دسترسی، یکپارچه‌سازی، امنیت و به‌ویژه تبادل و به اشتراک‌گذاری داده‌ها و اطلاعات موضوع این قانون اقدام نماید.

۷-۸-۲. عضویت در سازمان‌های مرتبط بین‌المللی و قوانین مرتبط

ایران عضو کمیسیون اقتصادی و اجتماعی سازمان ملل متحد برای آسیا و اقیانوسیه است[۱۷].

۳. جمع‌بندی و نتیجه‌گیری

حکمرانی بر داده به طیفی از رویکردهای اتخاذ شده توسط دولت‌های مختلف برای کنترل داده‌های تولید شده در زیرساخت اینترنت ملی یا داده‌هایی که از آن عبور می‌کند، اشاره دارد. تحقق این مفهوم در کشور به چرخه حیات داده و ارزش‌آفرینی از آن گره خورده است. داده‌ها و اطلاعات، زیربنای قدرت نرم و مهم‌ترین رکن اداره کشورها هستند. امروزه، فناوری‌های نوینی همچون هوش‌مصنوعی و اینترنت اشیا همراه با رویکردهای نوین اداره کشورها نظیر دولت هوشمند، شهر هوشمند و اقتصاد هوشمند بر پهنه مفهوم تحول دیجیتال بنا شده و به مبنایی برای سیاستگذاری کشورها تبدیل شده است. بر این اساس، برای جمهوری اسلامی ایران پرداختن به این اقدامات از یک اقدام آینده‌نگرانه به یک ضرورت تبدیل شده است. بسیاری از معضلات و مسائل پیش‌روی کشور با تغییر نظام حکمروایی داده‌ها و اطلاعات قابل رفع و بهبود است، اما ساختارهای اجرایی کشور و رویکردهای سنتی مواجهه با داده‌ها و اطلاعات، منجر به جزایری از فناوری‌های غیرمتصل شده است که گویی نه‌تنها از هم فاصله دارند بلکه بی‌اطلاع از یکدیگر نیز هستند.

با توجه به ضرورت پرداختن به مبنایی پیشینی در زمینه حکمرانی داده همچون زنجیره ارزش داده و احصای قواعدی برای سامان‌دهی به جریان داده و اطلاعات در کشور، در این گزارش تطبیقی تلاش شد تا استانداردها و قوانین مرتبط با جریان داده و اطلاعات در ۶ کشور منتخب

مورد بررسی قرار گیرد. همچنین در این گزارش، گزاره‌های سیاستگذاری برای برنامه‌ریزی و اجرا در زیست‌بوم داده در کشور، با در نظر گرفتن ویژگی‌های خاص هر کدام از کشورهای تحت بررسی، ارائه شده است.

لازم به توضیح است با مقایسه و بررسی جمعیت کشورهای مورد بررسی مشاهده می‌شود که میزان جمعیت تأثیری بر عزم حاکمیت آنها برای مدیریت داده‌های ملی و عمومی نداشته‌است (جدول ۲). برای مثال کشوری مانند نیوزلند با پنج میلیون جمعیت دارای ۱۷۹ سیستم متمرکز بوده که دربرگیرنده کلیه فرایندهای جاری در عرصه عمومی نیوزلند است. این آمار، نشانه‌ای است بر این امر که قطعاً یکی از ابتدایی‌ترین عوامل متمرکز کردن سیستم‌های اطلاعاتی در این کشورها، تسریع در خدمت‌رسانی به شهروندان است. بررسی‌های تکمیلی از اطلاعات، کشورها نشان از آن دارد که عوامل مهم‌تر و حیاتی‌تری نظیر استفاده‌های اقتصادی و امنیتی از داده‌ها و اطلاعات نیز انگیزه‌ای برای سامان‌دهی به جریان داده و اطلاعات در کشورهای مذکور بوده است. زیرا حکومت‌ها دریافته‌اند جا ماندن در روش‌های قدیمی صنعتی و تولیدی برطرف‌کننده نیاز آینده آنها نخواهد بود و چرخه تولید و انتقال اطلاعات و داده در فضای کنونی دنیا بسیار بااهمیت‌تر و قابل توجه‌تر از گذشته شده است. چنانچه به تولید ناخالص ملی کشورهای مورد بحث نیز توجه شود، مشاهده می‌شود در برخی کشورها مانند نیوزلند یا سنگاپور، به‌رغم اینکه تولید ناخالص ملی به مراتب کمتری از ایران دارند، اما وضعیت زنجیره تأمین داده آنها دارای چارچوب منظم‌تری است، به‌عبارت‌دیگر می‌توان اذعان کرد کشورهای مذکور در محدوده کوچک خود (نسبت به ایران) توجه خاص به موضوعات حائز اهمیتی مانند داده دارند.

با توجه به تجربیات جهانی بررسی شده، برخی از عوامل موفقیت در حکمرانی ملی داده عبارتند از [۵۴]:

۱. تعریف استراتژی‌ها و سیاست‌های جامع در حوزه داده‌ها؛
۲. ایجاد قوانین و مقررات ملی برای حفاظت از داده‌های شخصی و امنیت اطلاعات؛
۳. ترویج داده‌های باز و شفافیت در دسترسی به اطلاعات؛
۴. ایجاد سازمان‌ها و مراکز مسئول حکمرانی داده؛
۵. همکاری بین‌المللی و تبادل تجربیات در این حوزه.

کشورهای در حال توسعه مانند ایران با چالش‌های متعددی در حوزه حکمرانی داده‌ها روبه‌رو هستند. برخی از این چالش‌ها عبارتند از [۵۵]:

- نبود قوانین و مقررات کافی و مناسب برای حفاظت از داده‌ها و حریم خصوصی شهروندان؛
- نبود سیاست‌های ملی و راهبردهای کارآمد برای جمع‌آوری، نگهداری و انتشار داده‌های دولتی؛
- نبود زیرساخت‌های لازم برای جمع‌آوری، ذخیره‌سازی و پردازش داده‌های بزرگ (کلان داده)؛
- نبود استانداردهای مشترک و یکپارچه برای جمع‌آوری، پردازش و انتشار داده‌های دولتی موجود در سازمان‌ها و وزارتخانه‌ها؛
- نبود تضمین حقوقی برای دسترسی عمومی به داده‌های دولتی؛
- نبود توانایی و دانش کافی برای استفاده از داده‌ها برای تصمیم‌گیری‌های سیاسی و اقتصادی و کمبود و توزیع نابرابر استعدادها و نیروهای مرتبط با حوزه دیجیتال؛
- تمرکز ناکافی بر ایجاد اعتماد و ایمنی و محدودیت‌های بودجه‌ای موجب نبود همکاری بین دولت، بخش خصوصی و سایر ذی‌نفعان در حوزه حکمرانی داده و پراکندگی نظام‌های حکمرانی داده در کشور.

با توجه به مطالب مطرح شده در این گزارش می‌توان بر نکات قابل توجه هر کدام از کشورهای منتخب در مطالعات تطبیقی به‌شرح ارائه شده در شکل ۷ اشاره کرد. توضیحات تکمیلی از اطلاعات هر کشور نیز در جدول ۲ ارائه شده است.

در ایران فارغ از اقدامات انجام شده در زمینه سامان‌دهی به چارچوب داده، مشاهده می‌شـــود که همچنان چالش‌های جدی در این حوزه وجود دارد. از طرفی زیست‌بوم داده در حوزه‌های متنوعی به‌ویژه در بخش خصوصی و در شرایط خلأهای قانونی نظیر حقوق مالکیت معنوی، حریم خصوصی و ... به‌نحو غیرمنضبط شکل گرفته است و هرگونه اقدام آتی در جهت ســـامان‌دهی به این زیست‌بوم، موجب نارضایتی و اعتراض خواهد شد. ازسوی‌دیگر کشور ضرورتاً نیازمند یک محیط منضبط داده است و ناگزیر از ایجاد زیرساخت‌های تأمین حریم خصوصی

و زیرساخت‌های جریان و به گردش در آمدن داده است. زیرساخت‌هایی که هم حقوق مردم را تأمین می‌کند و هم بازار را برای عملکرد پویای خویش مبتنی‌بر تبادل داده آماده می‌سازد.

شکل ۷. نکات قابل توجه هر کدام از کشورهای منتخب در زمینه سامان‌دهی به جریان داده‌ها و اطلاعات

مأخذ: یافته‌های پژوهش.

با توجه به مطالعات انجام شده و بررسی وضعیت زیست‌بوم داده در ایران، پیشنهادهای زیر برای تحقق کامل دولت الکترونیک کامل و به‌دنبال آن دولت دیجیتال پیشنهاد می‌شود. شایان ذکر است، پس از تعیین موارد زیر می‌توان ارکان حکمرانی داده در کشور را طراحی و راه‌اندازی کرد:

- **اصلاح نگرش به داده برای تغییر دیدگاه در سطوح تصمیم‌ساز و تصمیم‌گیر در کشور:** با تبیین جایگاه ویژه کنونی داده و اطلاعات در سطح حکمرانی، می‌توان از مزیت‌های داده به‌عنوان عوامل تولید ثروت، قدرت و امنیت در سطح داخلی و بین‌الملل استفاده و همچنین خطرهای احتمالی فقدان توجه به این مهم را در ابعاد سیاسی، امنیتی، اقتصادی و اجتماعی رفع کرد. به‌عبارت‌دیگر همانند سایر کشورهای پیشرو، داده به‌عنوان یک دارایی دارای ارزش‌افزوده در نظر گفته شود. همچنین در راستای ایجاد سازوکار مناسب و کارآمد در جهت حکمرانی داده‌محور، طی کردن مسیر پیشنهادی زیر براساس شکل ۸ به‌ترتیب و براساس اولویت‌های عنوان شده لازم است، تا بتوان قدم‌هایی مطمئن در راستای دستیابی به حکمرانی براساس داده و اطلاعات به‌وجود آید.

شکل ۸. لایه‌های حکمرانی داده

مأخذ: همان.

- **شناخت تمامی عناوین داده‌ای موجود در سطح کشور به‌عنوان یک موجودیت:** اگر داده را به‌عنوان مصالح اولیه برای ساخت بانک‌های اطلاعاتی در سطح ملی بدانیم، باید تا عناوین و انواع دسته‌بندی داده‌های موجود در سطح کشور احصا و تعریف شوند.
- **شناخت تمامی فرایندهای اطلاعاتی در سطح ملی و عمومی:** پس از شناخت عناوین داده‌ها و ایجاد یک دسته‌بندی بومی براساس عناوین داده‌ها، برای امکان مدیریت فرایند تولید داده در کشور، باید تمامی فرایندهایی که طی آنها داده‌ای تولید می‌شود (براساس انواع داده‌هایی که به حکمرانی داده در کشور مرتبط است) شناسایی شده و مورد نظارت و بهبود مداوم قرار گیرد.
- تولید سند استانداردها و قوانین بومی مرتبط با چرخه حیات داده و اطلاعات در ایران براساس انواع داده‌ها و فرایندهای داخلی.
- تحلیل انواع داده و فرایندهای شناخته شده و مشخص کردن ارتباط بین موجودیت‌های داده‌ای با فرایندها در راستای اجرای سند استانداردهای بومی کشور.
- مهندسی مجدد سامانه‌های عمومی و ملی براساس سند استانداردهای بومی.
- ایجاد قوانین و استانداردها برای نظارت بر شناسایی نیاز، تولید و نگهداری سامانه‌های اطلاعاتی جهت استفاده در بخش‌های ملی، عمومی و خصوصی.
- ایجاد قوانین و دستورالعمل‌های مناسب جهت برقراری هماهنگی بین منابع تولید داده براساس یافته‌های بند «۵-۳».
- ایجاد شفافیت در بخش متولی‌گری داده در کشور.
- اصلاح و تقویت قانون انتشار و دسترسی آزاد به اطلاعات جهت تمایز میان داده‌های شخصی و عمومی و تشریح رویه‌های اجرایی مربوط به هر دسته از منظر هرکدام از اجزای زنجیره تأمین داده.
- تعریف انواع داده و تحلیل روش‌های برخورد با هر نوع در طول زنجیره تأمین داده.
- تدوین و تصویب استانداردها، دستورالعمل‌ها و رویه‌های اجرایی هرکدام از گام‌های حکمرانی داده اعم از تولید، توزیع، یکپارچه‌سازی، امنیت و انتشار داده.
- امکان اندازه‌گیری میزان بلوغ کشورها در حوزه داده است که این امر نیازمند طراحی یک مدل بومی است

جدول ۲. اطلاعات تکمیلی در زمینه کشورهای تحت بررسی

		ایران	کره‌جنوبی	کانادا	استرالیا	سنگاپور	مکزیک	انگلیس	نیوزلند
اطلاعات کلی	جمعیت در ۲۰۲۲ (نفر)	۸۴،۳۵۵،۰۱۵	۷۷,۰۰۰,۰۰۰	۳۸،۳۰۱،۲۰۷	۲۵,۷۵۰,۱۹۸	حدود ۵/۶۸۶ میلیون	حدود ۱۲۸/۹ میلیون	حدود ۵۵/۹۸ میلیون	حدود ۵/۰۸۴ میلیون
	تولید ناخالص ملی (میلیارد دلار)	۱۱۰۵	۱،۸۱۱	۱۸۰۵	۴۱۲/۲۷۰	۴۹۱/۷	۲۳۴۳	۷۱۵/۹۹۲	۲۱۸/۸
	تراز تجاری (میلیارد دلار)	منفی ۲/۱	۹/۵ مثبت	مثبت ۲/۳	مثبت ۹/۴۲	مثبت ۳۲/۷	مثبت ۲۴/۴۲	مثبت ۲۱/۳	مثبت ۰/۳۸۵

مأخذ: همان.

جدول ۳. جمع‌بندی اقدامات کشورهای تحت بررسی در زمینه ساماندهی به جریان حیات داده

نام کشور / بخش‌های زنجیره ارزش داده	ایران	کره‌جنوبی	کانادا	استرالیا	سنگاپور	مکزیک	انگلیس	نیوزلند
جمع‌آوری و یکپارچه‌سازی	نبود یکپارچگی داده‌ها و وجود قوانین پراکنده ازجمله فصل سوم قانون تجارت الکترونیک	پردازش داده ملی در کره‌جنوبی توسط نهاد ملی (NCPI) انجام می‌شود.	استفاده از روش‌هایی نظیر: • نظرسنجی • هوش‌مصنوعی • روش‌های مدرن ادغام داده • توجه به فقدان قطعیت داده‌ها	به‌صورت بر خط و مستقیم مطابق پروژه DIPA	• دریافت گزارش ازسوی سازمان‌ها • دریافت غیررسمی از افراد • دستورالعمل و خطوط راهنمایی درخصوص یکپارچه‌سازی داده	• انتشار اطلاعات توسط سایت‌های دولتی انجام می‌شود • طراحی چارچوب فن برای ارتباط دیتابیس‌ها	• اصلاحیه قانون GDPR • سیاست CMA	• تحت نظر قوانین داخلی • افشا تمام اطلاعات کشور در چهل گروه تجمیع شده • راه‌اندازی آژانس‌های متولی تجمیع داده‌ها
پردازش	نبود وجود قوانینی مرتبط با موضوع – وجود قوانین پراکنده ازجمله قانون تجارت الکترونیک و جرائم رایانه‌ای.	دارای یک‌مدل چهار لایه‌ای	استفاده از جداول و تجزیه‌وتحلیل داده‌های ایستا	استفاده از واحد تحلیل داده	استفاده از روش‌های تطبیق آماری	طراحی قوانین پردازش داده به تفکیک هر سامانه	اصلاحیه قانون GDPR	دارای آژانس‌های متولی پردازش که مجوز ذخیره داده را ندارند.

نام کشور / بخش‌های زنجیره ارزش داده	ایران	کره‌جنوبی	کانادا	استرالیا	سنگاپور	مکزیک	انگلیس	نیوزلند
توزیع	راه‌اندازی سامانه انتشار و دسترسی آزاد به اطلاعات (iranfoia.ir) که نیازمند اصلاح‌های عملیاتی است.	توزیع و اشتراک‌گذاری داده ملی در کره‌جنوبی توسط یک پلتفرم آنلاین انجام می‌شود.	• بهره‌مندی از چارچوب استفاده مجدد از داده • استفاده از چارچوب استراتژی داده	تحت قانون ملی	انتشار در پرتال داده‌باز سنگاپور (Data.gov.sg)	• طراحی قانون برای ارتباط متولی داده و شخص ثالث • طراحی قانون اجازه دسترسی شرکت‌های خصوص به تمامی داده‌ها • طراحی قانون جابه‌جایی داده با کشورهای دیگر	مقررات آزادی اطلاعات (FOI) برای دسترسی به اطلاعات عمومی	• افشار تمامی داده‌های کشور در دسترس عموم با وجود برخی استثنا (مجلس، دادگاه‌ها و رسانه‌های خبری) • قانون اجازه دسترسی شرکت‌های خصوص به‌تمامی داده‌ها
امنیت	وجود قوانین پراکنده ازجمله آیین‌نامه موضوع تبصره «۲» ماده (۷۳۲) کتاب پنج قانون مجازات در مورد داده‌ها سری و دارای طبقه‌بندی تدوین نشده است.	این کشور در سال ۲۰۱۹ قانون امنیت داده ملی را تصویب کرد که چارچوب قانونی لازم برای محافظت از داده‌های ملی را فراهم می‌کند.	اصول دهگانه امنیت داده منتشر شده توسط OECD	براساس قانون حفظ حریم خصوصی ۱۹۸۸ نگهداری DISC	تحت قانون ملی	قوانین خاص امنیت داده	• اصلاحیه قانون GDPR • الزام به افسر حفاظت داده در شرایط خاص	• کمیسیون حریم خصوصی • الزام به افسر حفاظت داده در همه شرایط

نام کشور / بخش‌های زنجیره ارزش داده	ایران	کره‌جنوبی	کانادا	استرالیا	سنگاپور	مکزیک	انگلیس	نیوزلند
متولی زنجیره تأمین داده	شورای عالی فضای مجازی	متولی زنجیره تأمین داده ملی در کره‌جنوبی کره‌جنوبی، آژانس ملی آمار کره (KOSTAT) است.	اداره ملی آمار کانادا	اداره آمار استرالیا • مؤسسه بهداشت و رفاه استرالیا	آژانس فناوری دولتی	وزارت اقتصاد	کمیسیون ICO زیر نظر ملکه	زیر نظر پادشاه
عضویت در سازمان‌های مرتبط	ESCAP	• ISO • UNIDO • OECD • APEC • WIPO	OECD	ESCAP	ESCAP	OECD	• OECD • توافق‌های TCA و DPA	• OEC • ESCAP

منابع و مآخذ

[1] Curry, E. (2016). The big data value chain: definitions, concepts, and theoretical approaches. New horizons for a data-driven economy: A roadmap for usage and exploitation of big data in Europe, 29-37.

The Data Value Chain: Moving from Production to Impact. Open [2] Open Data Watch. (2018, February 8). ./Data Watch. https://opendatawatch.com/publications/the-data-value-chain-moving-from-production-to-impact

[3] Twizeyimana, J. D., and Andersson, A. (2019). The public value of E-Government – A literature review. Government Information Quarterly,2)36), pp. 167–178.

[4] Santoro, M., and Borges, B. (2017). Brazilian Foreign Policy Towards Internet Governance. Revista Brasileira de Política Internacional, 60(1).

[5] EDPS. (2018, May 25). The History of the General Data Protection Regulation European Data Protection Supervisor. Www.edps.europa.eu. https://www.edps. europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[6] European Commission. (2018). Data protection in the EU. Commission.europa.eu. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.

[7] H.R.4943 - 115th Congress (2017-2018): CLOUD Act. (2017). Congress.gov. https://www.congress.gov/bill/115th-congress/house-bill/4943.

[8] Arora, Anil and Rohinton P. Medhora. (2020). Now More than Ever, the World Needs Data Stewards. Opinion, Centre for International Governance Innovation, October 12. www.cigionline.org/articles/nowmore-ever-world-needs-data-stewards-0.

[9] Statistics: Power from Data! Types of data collection. (n.d.). Www150.Statcan.gc.ca. https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch2/types/5214777-eng.htm.

[10] Artificial intelligence at Statistics Canada. (n.d.). Www.statcan.gc.ca. https://www.statcan.gc.ca/en/trust/collecting-your-data/artificial-intelligence.

[11] Girard, Michel, (2021). A Canadian Framework for Data Reuse, Centre for International Governance Innovation, License type: CC BY-NC-ND, Series: IGI Papers No. 251, Post date: 27 Apr 2021.

[12] CIOSC. 2020. “National Standards of Canada Standards Proposal: Data governance: Responsible data stewardship.” November. https://ciostrategycouncil.com/wp-content/ uploads/2020/11/CIOSC_StandardsProposal_Data-Stewardship_v1.pdf.

[13] Legislative Services Branch. (2019). Personal Information Protection and Electronic Documents Act. Justice.gc.ca. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/.

[14] Personal Information Protection Act - Open Government. (n.d.). Open.alberta.ca. https://open.alberta.ca/publications/p06p5.

[15] Personal Information Protection Act. (n.d.). Www.bclaws.gov.bc.ca. https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01.

[16] Act respecting the protection of personal information in the private sector. (n.d.). Www.legisquebec.gouv.qc.ca. https://www.legisquebec.gouv.qc.ca/en/document/ cs/p.39.1.

[۱۷] مرکز پژوهش‌های مجلس (۱۳۹۷). «بررسی قوانین حفاظت از داده‌های کاربران در کشورهای منتخب»، شماره مسلسل: ۱۵۸۷۷.

[18] Statistican of Canada. (2022). Statistics Canada Data Strategy-Delivering insight through data for a better Canada.

[19] Department of the Prime Minister and Cabinet (2019). Pmc.gov.au. https://www.pmc.gov.au/.

[20] Jensen, L. R. (2022). Using Data Integration to Improve Health and Welfare Insights. International Journal of Environmental Research and Public Health, 19(2), p. 836.
[21] Department of the Prime Minister and Cabinet (2019). Pmc.gov.au. https://www.pmc.gov.au/.
[22] Welcome to United Nations ESCAP | United Nations ESCAP. (2019). Unescap.org. https://www.unescap.org/.
[23] Data.gov.sg. (2010). Data.gov.sg; Data.gov.sg. https://data.gov.sg/.
[24] Rwanda's data governance: Navigating data governance in the public sector. (n.d.). Brookings. Retrieved May 16, 2024, from https://www.brookings.edu/articles/ rwandas-data-governance-navigating-data-governance-in-the-public-sector/.
[25] Petzold, B., Roggendorf, M., Rowshankish, K., and Sporleder, C. (2020, June 26). Designing data governance that delivers value | McKinsey. Www.mckinsey.com. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/designing-data-governance-that-delivers-value.
[26] Data (2024). Data Hub - Lexology. Globaldatareview.com. https://globaldatareview .com/.
[27] Data.gov.sg. (2024). Www.tech.gov.sg. https://tech.gov.sg/products-and-services/data-gov-sg/.
[28] Data Science and Artificial Intelligence. (2024, March 22). Singapore Government Developer Portal. https://www.developer.tech.gov.sg/products/collections/data-science-and-artificial-intelligence/.
[29] Singapore Department of Statistics (DOS) (2018). Singapore Department of Statistics (DOS). Base. https://www.singstat.gov.sg.
[30] Open Data Barometer. (n.d.). Opendatabarometer.org. https://opendatabarometer.org/.
[31] Personal Data Protection Commission (2021). Trusted Data Sharing Framework.
[32] PDPC (2022). PDPA Overview. http://Www.pdpc.gov.sg. https://www.pdpc.gov.sg/ Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.
[33] Daub, M., Domeyer, A., Klier, J., and Lundqvist, M. (2018) . Digitizing the state: Five tasks for national governments. BUSINESS.
[34] Martínez, H. G. (2020). Data Protection and Cybersecurity Laws In Mexico. CMC-Low-Tax-Future. https://cms.law/.
[35] Law in Mexico - DLA Piper Global Data Protection Laws of the World. (n.d.). Www.dlapiperdataprotection.com. https://www.dlapiperdataprotection.com/ index.html?t=lawandc=MX.
[36] Cesar, M., Chaia, A., Vaz, A. O., Garcia-Muñoz, G., and Haugwitz, P. (2018). How Mexico Can Become Latin America's Digital-Government Powerhouse. mckinsey Digital. https://www.mckinsey.com/.
[37] Arceo, A. D, Alcocer, G. (2019). ICLG Data Protection 2019. https://www.olivares.mx/.
[38] EGOVKB | United Nations> Data> Country Information. (2022). Un.org. https://publicadministration.un.org/egovkb/en-us/data/country-information/id/110-mexico.
[39] Find open data - data.gov.uk. (2019). Data.gov.uk. https://data.gov.uk/.
[40] GDPR.EU. (2019). Complete guide to GDPR compliance. GDPR.eu. https://gdpr.eu/.
[41] Andrews, S. K., Gabat, J., Jolink, G., and Klugman, J. (2021). DLA Piper/New Perimeter.
[42] Discover and use data - data.govt.nz. (n.d.). Data.govt.nz. https://data.govt.nz/.
[43] New Zealand Legislation. (2020). Privacy Act 2020. Www.legislation.govt.nz. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html.
[44] Findlay, B. (2020). Data Protected-New Zealand. Linklaters. https://www.linklaters.com/.
[45] OPEN DATA PORTAL. (n.d.). Www.data.go.kr. https://www.data.go.kr/en/index.do.
[46] PIPC, Korea. (n.d.). Www.pipc.go.kr. https://www.pipc.go.kr/eng/index.do.

[47] Park, K. B. (2021). South Korea - Data Protection Overview. DataGuidance. https://www.dataguidance.com/notes/south-korea-data-protection-overview.
[48] DataGuidance. (n.d.). DataGuidance. Retrieved May 17, 2024, from https://dataguidance.com/notes/south-korea-data-protection-overview.
[49] KISA. (n.d.). Www.kisa.or.kr. https://www.kisa.or.kr/EN.
[50] nitroeye-jdh. (2024). National Cyber Security Center. Ncsc.go.kr. https://www.ncsc.go.kr:4018/eng/mainPage.do.
[51] Korea, S. (2023). Statistics Korea. Statistics Korea. https://kostat.go.kr/anse/.
[52] Foreign relations of South Korea. (2020, May 7). Wikipedia. https://en.wikipedia.org/wiki/Foreign_relations_of_South_Korea#:~:text=South%20Korea%20is%20a%20member.
[53] President.ir. (2024). https://president.ir/fa/96859.
[54] Lee, E., Park, H., Kim, Y. (2019). Success Factors for National Data Governance. .Journal of Future Generation Communication and Networking, 12(1), pp. 9-14
[55] Ramezani, M., Nematollahi, M. and Javadian Kootanaee, A. (2018). Government Open Data in Iran: Challenges and Opportunities for Government Transparency and Accountability. Journal of Information Technology and Politics, 15(4), pp. 329-345. doi: 10.1080/19331681.2018.1537949.

کزیده سیاستی

در عصر اطلاعات، بهره‌مندی از داده‌ها، به عنصری، کلیدی در توسعه کشورها و ایجاد مزیت رقابتی برای آنها تبدیل شده است. استفاده از داده‌ها و ارزش‌آفرینی از آنها در گام نخست نیازمند سامان‌دهی به چرخه حیات داده‌ها، از ایجاد یا دریافت داده تا استفاده و در نهایت انهدام یا بایگانی آنهاست.

مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاسداران، روبروی پارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

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

وب سایت: rc.majles.ir