پژوهشگاه
فضای مجازی

دفتر آبی ۵

مجموعه گزارش‌های پژوهشی
آبان‌ماه ۱۴۰۳

مجموعه مطالعات تطبیقی

حکمرانیِ داده


بسم الله الرحمن

مجموعه مطالعات تطبیقی حکمرانیِ داده

دفتر آبی (Research Paper) شمارهٔ پنجم، **آبان ۱۴۰۳**

نویسنده: محمدحسین اعلمی
تهیه شده در ادارهٔ کل دبیرخانهٔ شورای عالی فضای مجازی کشور

نشانی: تهران، سعادت آباد، خیابان علامهٔ شمالی، کوچهٔ هجدهم غربی، پلاک ۱۷
تلفن: ۲۲۰۷۳۰۳۱-۰۲۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

مقالات پژوهشی (Research Paper) از مهم‌ترین ابزارهای توسعهٔ دانش هستند که با تکیه بر داده‌های تجربی به بررسی دقیق و جامع موضوعات تخصصی می‌پردازند. این مقالات معمولاً توسط پژوهشگران، استادان دانشگاه و محققان حرفه‌ای نوشته می‌شوند و به‌تفصیل از مشاهدات و داده‌های تحقیق بحث می‌کنند. مخاطب این مقالات نیز عمدتاً محققان و کارشناسان آن رشته است. امروزه در مسئلهٔ فضای مجازی و سایبری، به‌طور مرتب مقالات پرشماری توسط محققان و اندیشکده‌ها تولید می‌شود که به بررسی موشکافانهٔ مسائل جاری در این حوزه می‌پردازند. آگاهی از این مطالعات و رصد شرایط و ابعاد مختلف این حوزه از این رهگذر، برای کارشناسان و به‌خصوص قانون‌گذاران، حکمرانان و متولیان این عرصه ضروری است.

دفترهای آبی دسته‌ای از گزارش‌های تفصیلیِ تولیدشده در پژوهشگاه فضای مجازی، و محصول رصد مطالعات اندیشکده‌ها و نخبگان جهان و منطقه در این موضوع است.

پیشگفتار

«داده» ارزشمندترین کالای عصر تکنولوژی است و از این جهت، مسئلهٔ سیاست‌گذاریِ «داده» نیز اهمیت حیاتی پیدا کرده است و حکومت‌ها به دنبال آن‌اند که به‌راحتی این کالای باارزش را از دست ندهند و بر مسیرهای جریانِ داده و نیز به سرچشمه‌های آن تسلط داشته باشند. این مسئله در لایه‌های مختلفی اهمیت پیدا می‌کند، ازجمله در لایهٔ سیاست‌گذاری، ارزش‌گذاری، دسترسی به داده و اشتراک‌گذاری آن. در همین راستا، تعریف رابطهٔ حکمران و پلتفرم نیز (به‌عنوان جایگاه خلق داده و ابزار اصلی مدیریت آن) اهمیت ویژه دارد؛ طبیعتاً پلتفرم داده‌های خود را به‌راحتی با حکمران به اشتراک نمی‌گذارد، زیرا در این صورت بهره‌ای از جایگاه ویژهٔ خود نبرده است و از طرف دیگر اگر دسترسی و بهره‌برداری از داده در انحصار پلتفرم باشد، اوست که بر این عرصه حکمرانی خواهد کرد. لذا سیاست‌های این عرصه دارای اهمیت است و سیاست‌گذاریِ درست می‌تواند نسبت متعادلی میان بازیگران مختلف برقرار کند. در کشور ما نیز اهمیت این موضوع به‌درستی درک شده است و نسبت به از دست رفتن داده بی‌تفاوت نیستیم، اما هنوز نیازمند کارشناسی و تکمیل سیاست‌گذاری‌های خودیم.

میثم غلامی

سرپرست پژوهشگاه فضای مجازی

آبان ماه سال ۱۴۰۳

مقدمه

حکمرانی داده امروزه و با ظهور کسب‌وکارهای بزرگ دیجیتال که به جمع‌آوری، ذخیره‌سازی و پردازش داده‌های کاربران فضای مجازی اقدام می‌کنند. به یکی از موضوعات برجسته و مهم سیاست‌گذاری و حکمرانی دیجیتال تبدیل شده است. یکی از پیچیدگی‌های حکمرانی داده که در عین حال باعث اهمیت آن نیز می‌شود، داشتن ابعاد اقتصادی، فناورانه، سیاسی، امنیت و اجتماعی است که باعث شده است در کشورهای مختلف طیف مختلفی از قوانین و مقررات در این زمینه ایجاد شده و نهادسازی‌های منحصر به فردی انجام شود.

وضع قوانین مختلف مرتبط با داده‌های دیجیتال، در دنیا با سرعت و رویکردهای مختلفی صورت پذیرفته است و منجر به خلق الگوهای متفاوتی در کشورهای مختلف برای حکمرانی داده شده است؛ الگوهایی که اهداف مختلفی را دنبال کرده و از ابزارهای قانونی، فناورانه و سیاسی مختلفی بهره برده‌اند. به‌منظور تدوین یک چارچوب مناسب برای حکمرانی داده در ایران، ضروری است که مروری کلّی به تجربیات دنیا در این زمینه انجام شود و تجربیات کشورهای گوناگون مطالعه شود.

در ادامهٔ این گزارش، ابتدا مروری بر دسته‌بندی قوانین و مقررات حوزهٔ حکمرانی داده در دنیا، و آمار و ارقام مربوط به پیاده‌سازی آن‌ها در جهان انجام شده و سپس به مطالعهٔ موردی دو کشور منتخب هند و کرهٔ جنوبی و دلیل انتخاب آن‌ها خواهیم پرداخت.

نگاهی کلّی به حکمرانی داده در دنیا

دسته‌بندی قوانین و مقررات ذیل حکمرانی داده

همان‌طور که در مقدمه نیز اشاره کردیم، امروزه حکمرانی داده شامل طیف وسیعی از قوانین، مقررات و نهادسازی‌ها می‌شود که با دنبال‌کردن طیف مختلفی از اهداف اقتصادی، فناورانه، سیاسی، امنیتی و اجتماعی و استفاده از ابزارهای حقوقی و همچنین فناورانه، چارچوب‌هایی برای فعالیت کسب‌وکارهای دیجیتال، شهروندان و همچنین نهادهای عمومی و دولتی ایجاد کنند. ناظر به این تنوع قابل‌توجه در موضوعات ذیل چترکلّیِ حکمرانی داده، لازم است تا در ابتدا به دسته‌بندی‌های اساسی این موضوعات بپردازیم.

هرچند در ادبیات علمی و تخصصی دسته‌بندی‌های متفاوتی برای تقسیم‌بندی قوانین و مقررات مربوط به حکمرانی داده استفاده شده است، اما در ادامه از دسته‌بندی مورداستفادهٔ بانک جهانی در گزارش سالانهٔ سال ۲۰۲۱ این نهاد که موضوع اصلی آن سیاست‌گذاری داده است[1] استفاده شده است؛ به‌غیراز ارائهٔ یک دسته‌بندی، این گزارش به تحلیل داده‌های جمع‌آوری‌شده در زمینهٔ حکمرانی نیز پرداخته است که به برخی از موارد مرتبط و برجستهٔ آن در ادامه اشاره شده است.

1. World Development Report 2021: Data for Better Lives. World Bank Group (2021)

در گزارش مورد اشاره، حکمرانی داده به دو دستهٔ کلّی سیاست‌های حفاظتی[1] برای جلوگیری از استفاده‌های سوء از داده و آثار منفی آن و سیاست‌های تسهیل‌گرانه[2] برای فراهم‌کردن بسترِ به‌اشتراک‌گذاری داده و استفادهٔ مفید و مؤثر از آن تقسیم شده است.

- دستهٔ اول یا سیاست‌های حفاظتی خود به چهار دستهٔ ملموس‌تر تقسیم شده است: ۱. امنیت سایبری[3] و جرائم سایبری،[4] ۲. حفاظت از داده‌های شخصی[5] و حریم شخصی افراد، ۳. حفاظت از داده‌های غیرشخصی[6] و عمومی و ۴. قواعد مربوط به انتقال بین‌مرزی داده.[7]
- دستهٔ دوم یا سیاست‌های تسهیل‌گرانه نیز به سه دسته تقسیم شده است: ۱. ایجاد دسترسی به داده‌های عمومی (یا داده باز[8]) ۲. ایجاد دسترسی به داده‌های خصوصی (نظیر کلان‌داده‌های مفید برای جامعه) و ۳. قواعد تجارت الکترونیک.

در شکلی که در ادامه می‌آید، میزان پیاده‌سازی قوانین و مقررات در هر یک از این هفت دسته در میان دسته‌های مختلف کشورهای مورد مطالعه (برحسب درآمد سرانه) تصویرسازی شده است. می‌توان تفاوت میان کشورهای با درآمد بالا، درآمد متوسط و درآمد پایین را در میزان تلاش برای اعمال حکمرانی داده در موضوعات مختلف ذیل آن و همچنین تفاوت در میزان اهمیت موضوعات مختلف و قوانین وضع‌شده در قبال آن‌ها مشاهده کرد.

1. Safeguard
2. Enabler
3. Cybersecurity
4. Cybercrime
5. Personal data protection
6. Non-personal data
7. Cross-border data flow
8. Open data

میزان وضع قوانین و مقررات مرتبط با موضوعات ذیل حکمرانی داده در میان گروه های درآمدی مختلف کشورها، سال ۲۰۲۱

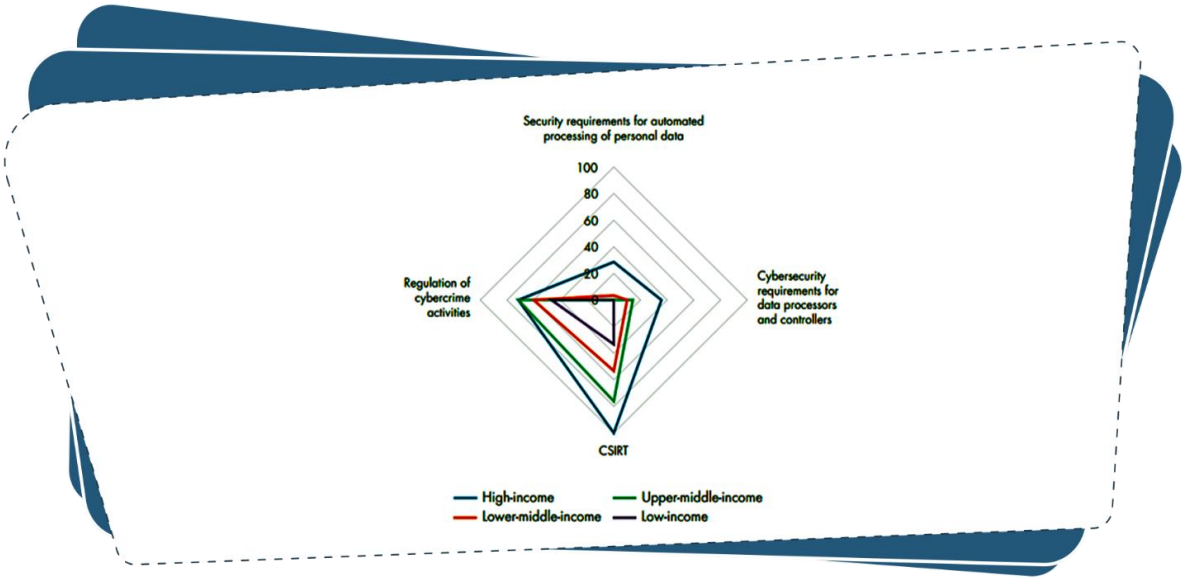
از میان این دسته‌بندی هفت‌گانه، چهار دسته بیشترین اهمیت را دارند و با اهداف و مضامین مدنظر سیاست‌گذاران در ایران نیز تناسب دارد: ۱. امنیت سایبری ۲. حفاظت از داده‌های شخصی ۳. داده باز ۴. قواعد انتقال بین‌مرزی داده

در ادامه مروری بر تعاریف این دسته‌بندی‌ها و برخی آمار و ارقام مرتبط با هر یک از آن‌ها خواهیم داشت.

امنیت داده

شاید در نگاه اول امنیت موضوعی فراتر از حکمرانی داده به نظر برسد، و جلوگیری از دسترسی‌های غیرمجاز و متخلفانه به داده که عمدتاً از طریق حملات سایبری، هک و نفوذ انجام می‌شود اهمیت بسیاری در زمینهٔ نگهداری امن و مطمئنِ داده دارد، می‌توان قواعد مربوط به امنیت سایبری را نیز از جهات قابل توجهی مرتبط با حکمرانی داده دانست. در بسیاری از اسناد

مربوط به حکمرانی داده نیز (شامل اسناد موردمطالعه در بخش مطالعهٔ موردی این گزارش) امنیت سایبری به‌عنوان یکی از ارکان حکمرانی داده برشمرده شده است. در ادامه، تصویری از میزان پیاده‌سازی قوانین و مقررات مربوط به امنیت سایبری در میان گروه‌های درآمدی مختلف کشورهای دنیا آمده است.



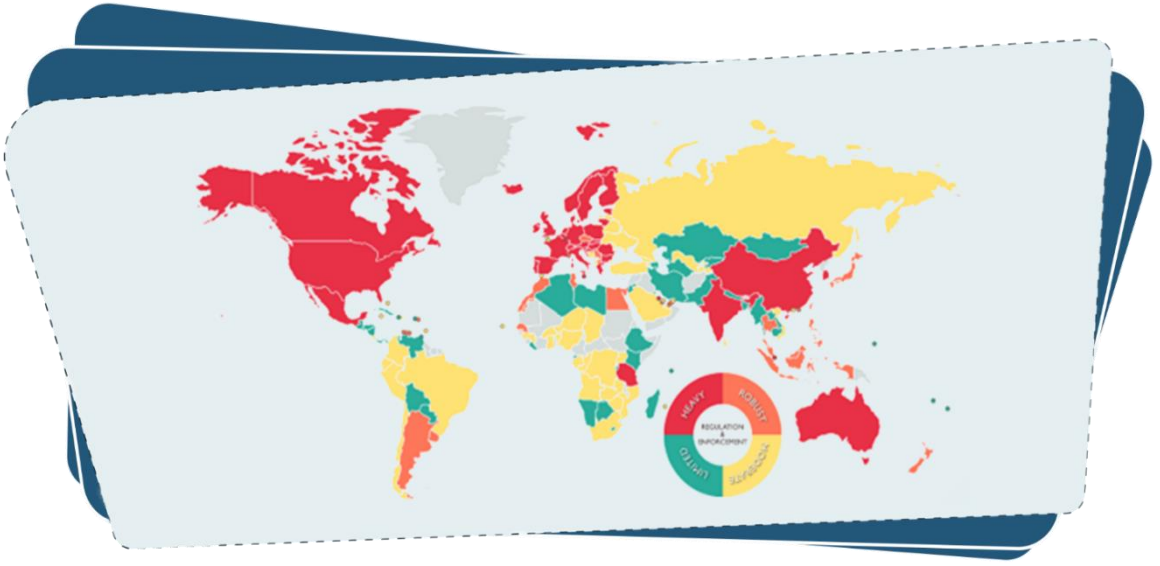
میزان وضع قوانین و مقررات مرتبط با امنیت سایبری در میان گروه های درآمدی مختلف کشورها در سال ۲۰۲۱

همان‌طور که مشاهده می‌شود، به‌غیراز قوانین مربوط به جرائم سایبری که در میان کشورهای مختلف نسبتاً رایج بوده، تأسیس یک مرکز ملّی مواجهه با حملات سایبری (CSIRT)[1] نیز نسبتاً موردتوجه بوده است. اما وضع قواعد امنیتی برای پردازشگرانِ داده و همچنین سامانه‌های خودکارِ پردازشِ داده موضوعاتی است که هنوز در دنیا به‌صورت گسترده موردتوجه قرار نگرفته است.

1. national Computer Security Incident Response Team

حفاظت از داده‌های شخصی

موضوع حفاظت از داده‌های شخصی در سالیان اخیر به یکی از داغ‌ترین موضوعات مورد بحث در زمینهٔ سیاست‌گذاری فناوری تبدیل شده و پس از تصویب و اجرای قانون GDPR[1] در اتحادیهٔ اروپا بسیاری از کشورها به وضع قوانین و مقررات مشابهی پرداختند. همان‌طور که در شکل زیر مشاهده می‌شود، این قوانین امروزه در دنیا رایج است و کشورمان ایران درحال تبدیل‌شدن به یکی از معدود کشورهایی است که قانون مشخصی در این زمینه تصویب نکرده است.

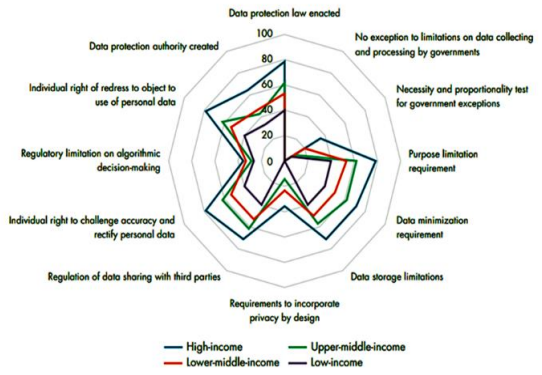


میزان شدت قوانین و مقررات کشورهای مختلف در زمینهٔ حفاظت از داده های شخصی

(منبع: مؤسسهٔ حقوقی DLA Piper[2])

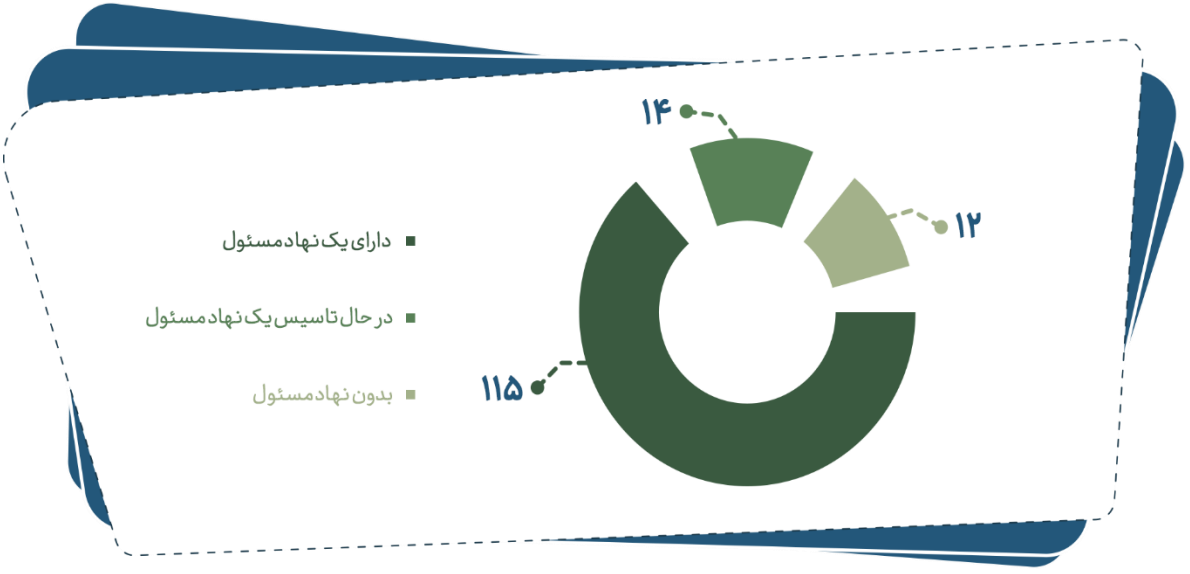
1. General Data Protection Regulation
2. Data Protection Laws of the World, DLA Piper website: dlapiperdataprotection.com/index.html

قواعد حفاظت از داده‌های شخصی معمولاً شامل ایجاد چارچوبی برای جمع‌آوری، ذخیره‌سازی، پردازش و به‌اشتراک‌گذاری داده‌های شخصی افراد توسط کسب‌وکارهای دیجیتال می‌شود. پس از تصویب قانون GDPR، این قانون به نوعی تبدیل به الگویی برای دیگر کشورها شد و عناصر به‌کاررفته در آن در بسیاری از قوانین استفاده شد؛ عناصری نظیر اطلاع‌رسانی و جلب رضایت افراد صاحب داده به هنگام جمع‌آوری و به‌اشتراک‌گذاری داده‌های شخصی آن‌ها، محدودکردن جمع‌آوری داده به موارد اطلاع‌رسانی شده و استفاده از داده به هدف طرح شده و.... وجود این عناصر مشترک را در تصویر زیر می‌توان مشاهده کرد.



وجود عناصر مختلف در قوانین و مقررات حفاظت از داده های شخصی گروه های مختلف درآمدی کشورها در سال ۲۰۲۱

یکی از مواردی نیز که در این مورد شایستهٔ توجه است وجود یک نهاد مسئول در زمینهٔ حفاظت از داده به‌عنوان یک الگوی غالب است. نهادهای مسئول در زمینهٔ حفاظت از داده وظیفهٔ نظارت بر پیاده‌سازی این قوانین توسط کسب‌وکارها را به عهده دارند و در صورت نقض تعهدات کسب‌وکارها، می‌توانند به بررسی فنی و حقوقی و رسیدگی به شکایات بپردازند. از میان ۱۴۱ کشور دارای قانون حفاظت از داده‌های شخصی، ۱۱۵ کشور یک نهاد مشخص مسئول در این حوزه دارند، ۱۴ کشور درحال تأسیس آن هستند و تنها ۱۲ کشور نهاد مشخص مسئولی ندارند.

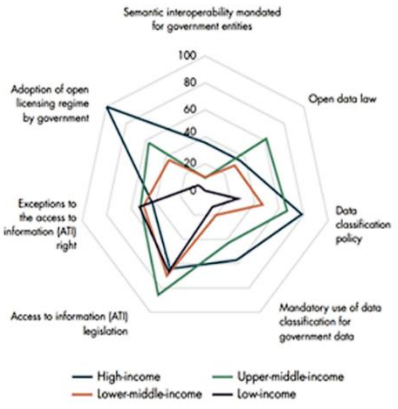


بود یا نبود نهاد مسئول حفاظت از داده های شخصی در میان ۱۴۱ کشور دارای قانون در سال ۲۰۲۲

داده‌باز

برجسته‌ترین رویکرد تسهیلگرانه کشورهای مختلف در زمینهٔ حکمرانی داده که رواج آن نیز در تصویر صفحهٔ ۵ قابل‌مشاهده است، سیاست‌های داده‌باز یا همان فراهم‌کردن دسترسیِ بازیگران مختلف، به‌خصوص کسب‌وکارهای دیجیتال به داده‌های عمومیِ جمع‌آوری‌شده و ذخیره‌شده توسط نهادهای عمومی و دولتی به منظور خلق ارزش از این داده‌هاست.

برخلاف حوزهٔ حفاظت از داده‌های شخصی که قوانین کشورهای مختلف اشتراکات بسیاری دارند و اغلب کشورها از قانون GDPR اتحادیهٔ اروپا الهام گرفته‌اند، در زمینهٔ داده‌باز جزئیات قانون اهمیت بسیاری دارد و طراحی آن ناظر به تفاوت‌های قابل توجهِ ساختار دولت و نهادهای عمومی در میان کشورهای مختلف انجام می‌شود. لذا هرچند شمایی از عناصر مختلف سیاست داده‌باز در شکل زیر قابل‌مشاهده است، اما نمی‌توان تفاوت‌های موجود در میان رویکردهای کشورهای مختلف را به‌درستی در آن مشاهده کرد.



وجود عناصر مختلف در قوانین و مقررات داده باز گروه های مختلف درآمدی کشورها در سال ۲۰۲۱

انتقال بین‌مرزیِ داده

انتقال بین‌مرزی داده که با عنوان محلّی‌سازیِ داده[1] نیز شناخته می‌شود، امروزه به یکی از موضوعات مناقشه‌برانگیز و محل چالش در تعاملات بین‌المللی کشورهای مختلف تبدیل شده است. منظور از انتقال بین‌مرزی داده، قواعدی است که انتقال داده‌های شهروندان یک کشور را جهت ذخیره‌سازی یا پردازش آن به خارج از مرزهای جغرافیایی کشور محدود می‌کند و کسب‌وکارهای دیجیتال را ملزم به ذخیره‌سازی دادهٔ شهروندان خود در داخل مرزهای جغرافیایی خود می‌کند.

ازآنجاکه محدودکردن انتقال بین‌مرزی داده با اهداف مختلفی نظیر حفاظت از حریم شخصی شهروندان، فراهم‌کردن امنیت داده‌های شهروندان، مزیّت‌بخشی به کسب‌وکارهای داخلی و یا فراهم‌کردن دسترسی به داده‌های شهروندان جهت نیازهای امنیتی صورت می‌گیرد، قواعد مربوط به این حوزه در کشورهای مختلف در یک قانون مشخص تبیین نشده است و بعضاً ذیل دیگر قوانین، نظیر قانون حفاظت از داده‌های شخصی تبیین شده‌اند.

1. Data Localization

مالکیت داده‌های شخصی در قوانین حفاظت از داده‌های شخصی

در پیش‌نویس سند حکمرانی داده، به این موضوع اشاره شده است که داده‌های جمع‌آوری‌شده و پردازش‌شده توسط نهادها و دستگاه‌ها در دو صورت در **مالکیتِ** آن‌ها نیست. فارغ از اینکه حدود مورد دوم (در برداشتنِ اطلاعات مهم) مشخص نیست، مورد اول (در برداشتنِ اطلاعات شخصی و خصوصیِ اشخاص جامعه از حیث انفرادی یا تجمیعی) شامل بخش عمده‌ای از داده‌های جمع‌آوری شده توسط بخش خصوصی و نهادهای عمومی می‌شود.

عدم مالکیت نهادهای جمع‌آوری‌کننده و پردازش‌کننده، موجب طرح این سؤال می‌شود که مالکیت این داده‌ها در اختیار کیست؟ اعطای مالکیت داده‌های شخصی و خصوصی افراد به آن‌ها، شاید در نگاه اول به‌عنوان راه‌حلّی برای جلوگیری از سوءاستفادهٔ نهادهای جمع‌آوری‌کننده و پردازشگر به نظر برسد، اما تبعات غیرمنتظرهٔ گسترده‌ای دارد و می‌تواند به اختلافات حقوقی پیچیده‌ای میان بازیگران مختلف صنعتِ داده منجر شود.

یکی از پیچیدگی‌های تعیین مالک برای داده، ماهیت غیررقابتی و غیرقابل تخصیص آن در مقایسه با کالاهای فیزیکی است. برخلاف کالاهای فیزیکی، همزمان تعداد زیادی از افراد می‌توانند به داده دسترسی داشته باشند و از آن بهره‌برداری کنند (غیررقابتی بودن). همچنین در شرایطی که داده به‌صورت عمومی در دسترس باشد، نمی‌توان کسی را از استفاده و بهره‌برداری از آن منع کرد (غیرقابل تخصیص بودن). این دو موضوع در کنار قابلیت تهیهٔ کپی از داده با هزینهٔ بسیار کم، باعث پیچیدگی‌های مختلفی برای تعیین مالک داده می‌شود.

با توجه به دخالت بازیگران متعدد در فرایند ایجاد، جمع‌آوری و پردازشِ داده و تعلق بسیاری از داده‌ها و پایگاه‌های دادهٔ موجود به بیش از یک شخص، تعیین مالک داده‌ها دشوار خواهد بود. در چنین شرایطی تصمیم‌گیری دربارهٔ سرنوشت داده‌ها و چگونگی پردازش و انتقال آن‌ها، نیازمند دخیل کردن همهٔ اشخاصی است که یک داده یا یک مجموعه داده به‌نحوی

دربردارندهٔ اطلاعات شخصی و خصوصی آن‌هاست و این مسئله بسیار چالش‌برانگیز خواهد بود و درست شبیه به ملکی است که در مالکیت چندین نفر باشد و به‌سبب چالش در تصمیم‌گیری دربارهٔ آن، رها شود.

خلع مالکیت از همهٔ بازیگران درگیر در ایجاد، جمع‌آوری و پردازش داده نیز موجب کاهش انگیزهٔ کسب‌وکارها می‌شود و نظام انگیزشی اقتصادِ داده را مختل خواهد کرد. ناظر به سلب مالکیت از نهادها و دستگاه‌های جمع‌آوری‌کننده و پردازشگرِ داده، این نهادها باید به‌ازای هرگونه عملِ مرتبط با داده، نسبت به جلب رضایت مالک داده اقدام کنند که ناظر به حقوق گستردهٔ مرتبط با مالکیت (درمقابلِ حقوق مشخصی که می‌تواند در قانون تدوین شود و حد و حدود آن برای اشخص و کسب‌وکارها تبیین شود)، این موضوع می‌تواند چالش‌های گسترده‌ای برای کسب‌وکارها ایجاد کند و انگیزهٔ آن‌ها برای جمع‌آوری و پردازش داده را کاهش دهد.

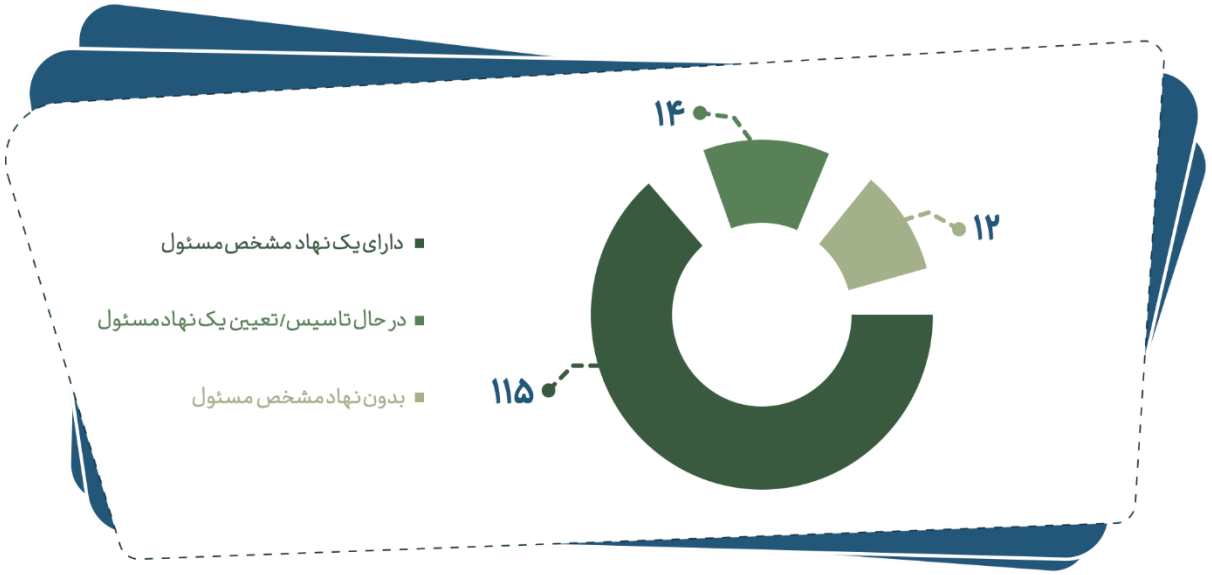
اعطای مالکیت داده به افراد می‌تواند منجر به ایجاد انگیزهٔ فروش مالکیت داده توسط اشخاص شود که اثراتی منفی بر حریم شخصی و امنیت داده‌ها خواهد داشت. شاید در نگاه اول اعطای مالکیت داده به افراد موجب افزایش کنترل آن‌ها بر داده و جلوگیری از سوءاستفادهٔ آن‌ها شود، اما از سوی دیگر این موضوع می‌تواند منجر به فروش و انتقال مالکیت داده بدون اطلاع از تبعات مختلف آن شود و به سوءاستفادهٔ گسترده بینجامد.

در نهایت، به نظر نمی‌رسد که الزامِ نهادها و کسب‌وکارها به رعایت موارد مورداشاره در سند، نیازی به سلب مالکیت داده از آن‌ها و یا اعطای مالکیت داده به اشخاص داشته باشد، اما در سوی مقابل، اشاره به مالکیت داده می‌تواند تبعات حقوقی گسترده و غیرمنتظره‌ای داشته باشد؛ موضوعی که در اشاره‌نکردن به این موضوع و مسکوت‌گذاشتن آن در قوانینِ حفاظت از داده در دنیا نیز بازتاب دارد.

مختصات نهادهای حفاظت از داده در قوانین حفاظت از داده‌های شخصی

نهادهای حفاظت از داده (Data Protection Authority) در کشورهای مختلف به‌تبعِ تصویب قوانین حفاظت از داده‌های شخصی و به‌منظور نظارت بر اجرای این قوانین در راستای حفاظت از حریم شخصی و حقوق اشخاصِ صاحب داده و جلوگیری از سوءاستفاده از داده‌های شخصی افراد شکل گرفتند.

از میان **۱۴۱ کشورِ دارای قانون مصوّب** در زمینهٔ حفاظت از داده‌های شخصی، **۱۱۵ کشور** یک نهاد مشخصِ حفاظت از داده ایجاد کرده‌اند یا مسئولیت‌های متناظر با آن را به یک نهاد مشخصِ موجود سپرده‌اند، **۱۴ کشور** درحال تأسیس/تعیین یک نهاد مشخص بوده‌اند و **تنها ۱۲ کشور** نهاد مشخصی برای پیاده‌سازیِ قانونِ حفاظت از داده‌های شخصیِ خود تأسیس یا تعیین نکرده‌اند. (براساس داده‌های بانک جهانی در سال ۲۰۲۲)



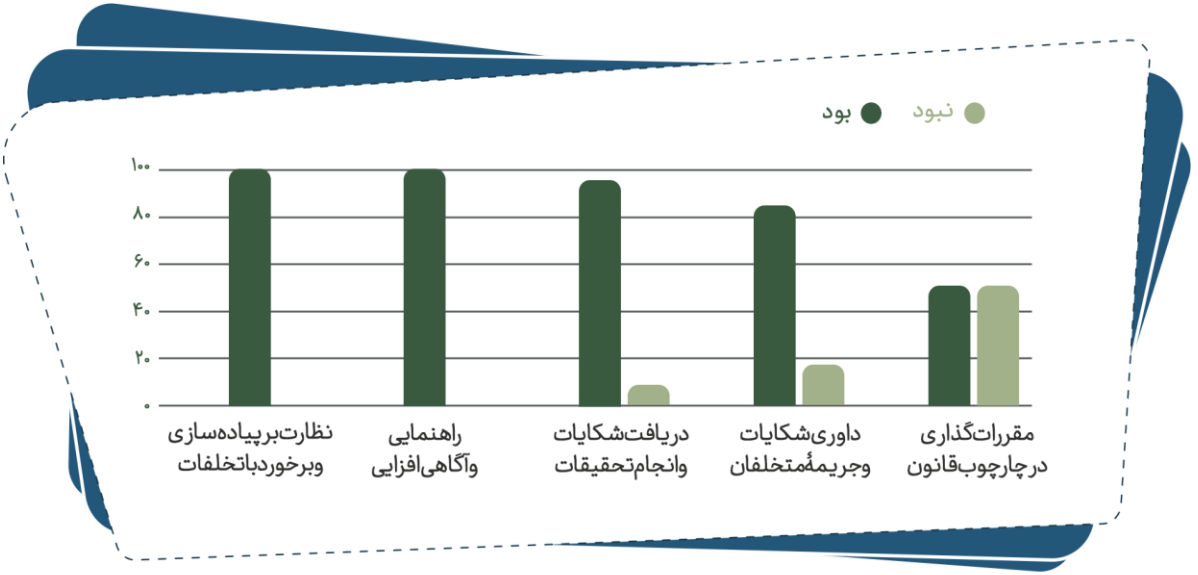
بود یا نبود یک نهاد مسئول در زمینهٔ حفاظت از داده های شخصی در سال ۲۰۲۲

می‌توان وظایف و اختیارات این نهادها را به پنج دسته تقسیم کرد:

۱. نظارت بر پیاده‌سازی قانون و برخورد با تخلفات، ۲. راهنمایی چگونگی پیاده‌سازی قانون و آگاهی‌افزایی عمومی، ۳. دریافت شکایات صاحبان داده و انجام تحقیقات دربارهٔ آن‌ها، ۴. داوری شکایات و جریمه‌کردن متخلّفان و ۵. مقررات‌گذاری در چارچوب قانون.

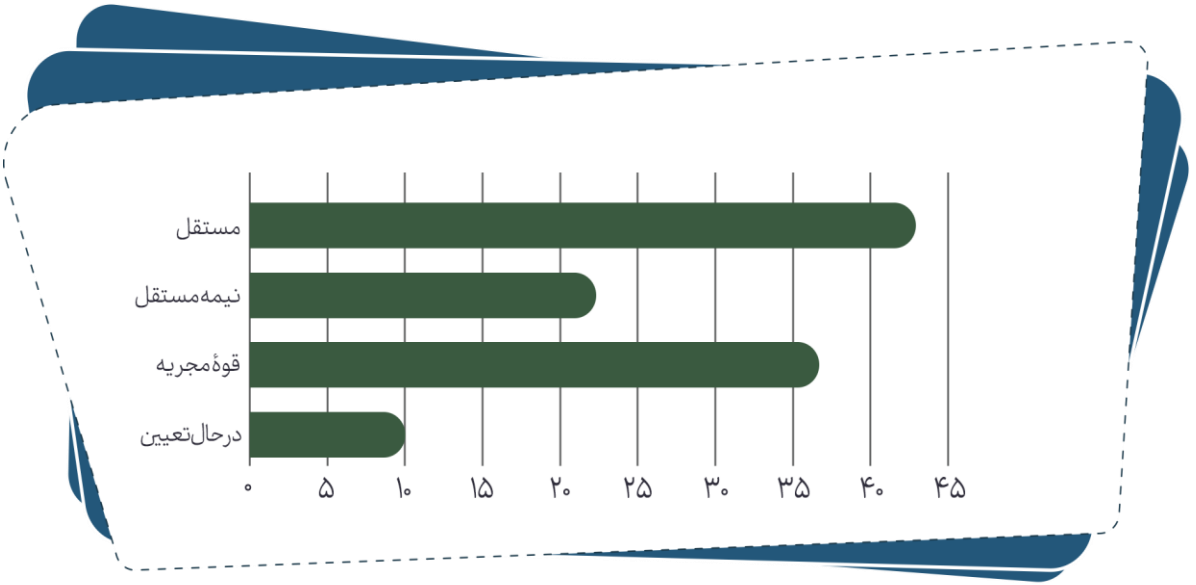
به منظور بررسی وجود این وظایف و اختیارات در نهادهای حفاظت از داده در کشورهای مختلف، داده‌های گردآوری‌شدهٔ مؤسسات حقوقیِ معتبر و همچنین داده‌های عمومیِ دردسترس دربارهٔ قوانین کشورهای مختلف و نهادهای حفاظت از دادهٔ آن‌ها جمع‌آوری شد و سپس این داده‌های خام (عمدتاً متون قانون و تحلیل‌های حقوقی و برای ۹۹ کشور) توسط هوش مصنوعی تحلیل شد و سپس با تطبیق موردیِ آن، از صحت این تحلیل اطمینان حاصل شد.

وجه مشترک تمامی نهادهای حفاظت از داده، نظارت بر پیاده‌سازی قانون توسط کسب‌وکارها و برخورد با تخلّفات آن‌ها در زمینهٔ پیاده‌سازی قانون و همچنین راهنمایی کسب‌وکارها و آگاهی‌افزایی در جامعه است. نهادهای حفاظت از داده در بیش از ۹۰ درصد از کشورها نسبت به دریافت شکایات اشخاص درصورت نقض حقوق خود در قانون اقدام می‌کنند و در نزدیک به ۸۵ درصد از کشورها نسبت به داوری این شکایات و جریمه‌کردنِ متخلّفان اقدام می‌کنند. درواقع تنها وظیفه‌ای که تنوع قابل‌توجهی در قبال آن وجود دارد، توانایی وضع مقررات جدید (در چارچوب قانون) توسط نهاد حفاظت از داده است.



وظایف و اختیارات نهاد حفاظت از داده در میان کشورهای مورد بررسی در سال ۲۰۲۴

همچنین با تحلیل داده‌های گردآوری‌شده با شیوه‌ای مشابه، جایگاه نهادیِ نهادهای حفاظت از داده در ۹۹ کشورِ موردبررسی استخراج شد. الگوی غالب که بیشتر کشورهای اروپایی ذیل چارچوب قانونیِ اتحادیهٔ اروپا، و بسیاری از دیگر کشورها اقدام به پیاده‌سازی آن کرده‌اند کمیسیون یا کمیسیونرهای مستقل است. اما از سوی دیگر در بسیاری از کشورها نهاد حفاظت از داده ذیل یک وزارت‌خانه یا مستقیماً زیر نظر رئیس جمهور یا نخست‌وزیر قرار دارد و در برخی کشورها نیز حدی از استقلال به نهادی ذیل قوهٔ مجریه اعطا شده که در دستهٔ نیمه‌مستقل گنجانده شده‌اند.



توزیع انواع نهاد حفاظت از داده در میان کشورهای مورد بررسی در سال ۲۰۲۴

برای شفافیت بیشتر، توضیحاتی دربارهٔ هریک از دسته‌بندی‌های نهاد حفاظت از داده ارائه شده‌است:

- **مستقل:** الگوی مستقل نهادهای حفاظت از داده که عمدتاً در کشورهای اروپایی مشاهده‌می‌شود، وبخشی‌ازآن‌هانیزذیل‌چارچوب‌قانون GDPR به‌آن‌ملزم‌شده‌اند، مشتمل بر انتخاب یک کمیسیون/کمیسیونر توسط پارلمان است تا دولت و قوهٔ مجریه چه در فرایند انتخاب و چه در عملکرد این نهاد، توانایی اعمال نفوذ بر آن را نداشته‌باشند. همان‌طورکه ذکر شد این الگو غالباً در اروپا پیاده‌سازی می‌شود، اما در خارج‌از این قاره‌ودرکشورهایی نظیرکانادا واروگوئه نیزپیاده‌سازی شده‌است.

- **قوهٔ مجریه:** در بسیاری از کشورها در دیگر قاره‌ها غیر از اروپا، نهاد حفاظت از داده همانند بسیاری از دیگر نهادهای نظارتی ذیل قوهٔ مجریه و وزارت‌خانهٔ مرتبط با حوزهٔ فناوری اطلاعات و یا مستقیماً زیر نظر رئیس جمهور یا نخست‌وزیر فعالیت می‌کند و دولت توانایی تغییر مسئول این نهاد (یا پنل/کمیسیون تصمیم‌گیر آن) را دارد و درنتیجه نهاد حفاظت از داده بیش از اینکه ماهیت یک نهاد مستقل از دولت را داشته باشد، یک سازمان تخصصی دولتی است. این الگو در کشورهایی نظیر روسیه، چین، قطر، آرژانتین و مالزی پیاده‌سازی شده است.
- **نیمه‌مستقل:** در برخی از کشورها، نهاد حفاظت از داده نه کاملاً از دولت مستقل است و نه کاملاً یک سازمان زیر نظر دولت محسوب می‌شود. برای مثال، در بسیاری از کشورهایی که نهاد حفاظت از داده در آن‌ها نیمه‌مستقل دسته‌بندی شده است رئیس یا اعضای کمیسیون/پنل نهاد حفاظت از داده توسط رئیس‌جمهور، نخست‌وزیر یا یکی از وزرا منصوب می‌شوند اما انتصاب آن‌ها برای بازه‌های زمانی مشخصی است که پیش از اتمام آن، دولت یا به‌کلّی امکان برکناری و تغییر رئیس/اعضای کمیسیون را ندارد یا برای این کار با موانع مختلفی روبه‌روست که در عمل استقلالی نسبی در تصمیم‌گیری تخصصی و بدون منظورکردنِ ملاحظات و اهداف سیاسیِ دولت به این نهاد اعطا می‌کند. و دشوارسازی و جلوگیری از مداخلهٔ دولت در عملکرد این نهاد، به غیر از فرایند انتصاب و برکناری، در استقلال عملکرد، تصمیم‌گیری و بودجه‌ریزی نیز بروز و ظهور دارد و در برخی از کشورها با اینکه نهادِ حفاظت از داده ذیل دولت تعریف شده، اما با داشتن چنین استقلال‌هایی نیمه‌مستقل محسوب می‌شود. می‌توان این الگو را در کشورهایی نظیر انگلیس، ترکیه، ژاپن، استرالیا و برزیل مشاهده کرد.

حدود و اهداف محلّی‌سازیِ داده به‌همراه بررسی نمونهٔ موردیِ تیک‌تاک

- منظور از محلّی‌سازی داده‌ها (Data Localization) یا محدودسازی جریان بین‌مرزیِ داده (Cross-border Data Flow)، مجموعه‌ای از سیاست‌هاست که دولت‌ها برای حفظ داده‌های شخصی شهروندان کشور در درون محوطهٔ جغرافیایی کشور، در راستای اهداف مختلف اقتصادی، امنیتی و سیاسی دنبال می‌کنند.
- اهداف مختلف محلّی‌سازی داده‌ها:
  - **اقتصادی:** محلّی‌سازی داده‌ها به‌نوعی شبیه به تعرفه‌ها و ممنوعیت‌های تجاری به‌دنبال مزیّت‌بخشی به کسب‌وکارهای داخلی نظیر مراکز داده و همچنین کسب‌وکارهای پردازش‌گر داده است. به‌مانند تعرفه‌ها و ممنوعیت‌های تجاری، محلّی‌سازی داده‌ها اثرات دوگانه‌ای داشته و به‌غیراز مزیّت‌بخشی به بازیگران داخلی، هزینه‌های بازیگران خارجی و حتی همکاری با بازیگران داخلی با بازیگران خارجی را بالا برده و می‌تواند در برخی موارد منجر به خروج آن‌ها از بازار یک کشور شود. ناظر به این موضوع، امروزه محلّی‌سازی داده به یکی از موضوعات موردتوجه در تفاهم‌نامه‌ها و توافق‌نامه‌های تجاری کشورها با یکدیگر تبدیل شده است.
  - **سیاسی/اجتماعی:** ذخیره‌سازی داده‌های شخصی شهروندان در خارج از مرزهای کشور، درصورت نبود زیرساخت‌های فنی و حقوقی مناسب در کشور مقصد، می‌تواند منجر به نقض حریم شخصی شهروندان شود (در قالب اتفاقاتی نظیر نشتِ داده و یا سوءاستفاده و فروش غیرقانونی داده‌ها). ناظر به این موضوع، کشورها نسبت به محدودکردن ذخیره‌سازی و پردازش داده‌های شهروندان خود در کشورهایی که ارزیابی مطلوبی از زیرساخت‌های حقوقی و فنی آن‌ها ندارند اقدام می‌کنند.

- **امنیتی/انتظامی**: استدلال‌های امنیتی پشتیبان محلّی‌سازی داده‌ها به دو دسته تقسیم می‌شود:
  ۱. دسترسی نهادهای امنیتی و انتظامی داخلی به داده‌های شهروندان در مواردموردنیاز
  ۲. جلوگیری و یا دشوارسازی دسترسی نهادهای امنیتی کشور مقصد به داده‌های شهروندان

عمده استدلال‌های امنیتیِ طرح‌شده برای محلّی‌سازیِ داده‌ها، دسترسی نهادهای امنیتی و انتظامی داخلی به داده‌های شهروندان است، اما بعضاً به جلوگیری یا دشوارسازی نهادهای امنیتی خارجی به داده‌های شهروندان نیز به‌عنوان هدف پرداخته می‌شود (مثلاً ذخیره‌سازی داده‌ها توسط کسب‌وکارهای داخلی در خارج از کشور).

- **محلّی‌سازی داده تنها محدود به ممنوعیت خروج داده‌های شخصی شهروندان از کشور نیست** و با ابزارهای مختلفی دنبال می‌شود؛ نظیر الزام به نگهداری یک نسخه (Mirror) از داده‌های شخصی شهروندان در داخل کشور یا صدور مجوّز برای خروج داده‌ها، بسته به برخی پارامترهای فنی، حقوقی و سیاسی در کشور مقصد.
- **محلّی‌سازی داده‌ها عمدتاً مربوط به داده‌های شخصی شهروندان و نه همهٔ داده‌های یک کسب‌وکار است**، مثلاً در پلتفرمی مانند تیک‌تاک، داده‌های شخصی جمع‌آوری‌شده نظیر آدرس ایمیل، آدرس IP، داده‌های جغرافیایی و دیگر داده‌های شخصی نظیر سن، جنسیت و نام؛ و نه داده‌هایی نظیر ویدئوهای به‌اشتراک‌گذاشته‌شده توسط کاربران که به‌صورت عمومی در دسترس هستند. **یکی از چالش‌های محلّی‌سازی داده، داده‌های شخصی هستند که به‌نحوی به دو نفر مربوط می‌شوند، مانند پیامی شخصی که بین دو کاربر از دو کشور مختلف ردوبدل شده است.**

آیا جلوگیری از دسترسی نهادهای امنیتی یک کشور خارجی به داده‌های شخصی داخلی که توسط کسب‌وکارهای آن کشور جمع‌آوری شده، امکان‌پذیر است؟

به‌صورت خلاصه، در اغلب موارد خیر. در بسیاری از مدل‌های کسب‌وکاری، شرکت‌ها برای ارائهٔ خدمات و بهبود کیفیت آن، به دسترسی و پردازش مستمرِ داده‌های کاربران نیاز دارند. حتی درصورت ذخیره‌سازی داده‌های شخصی شهروندان در داخل کشور، ممانعت کامل از دسترسی کسب‌وکار خارجی به این داده‌ها امکان‌پذیر نیست و نهادهای امنیتی کشور مقصد نیز می‌توانند از این طریق به موارد مدنظر خود دسترسی داشته باشند؛ **هرچند محلّی‌سازی داده می‌تواند برخی دسترسی‌های نامتعارف را شناسایی و ردیابی کند و دسترسی خارجی را دشوارتر کند.**

درمورد تیک‌تاک، مطالبات سیاستمداران آمریکایی فراتر از محلّی‌سازی داده‌ها است. تیک‌تاک از سال ۲۰۲۲ به‌صورت داوطلبانه اقدام به ذخیره‌سازی داده‌های شهروندان آمریکایی بر روی ابر شرکت Oracle در آمریکا کرده است، اما این اقدام نیز نتوانست مانع از تصویب قانون کنگره علیه آن در سال ۲۰۲۴ شود. درواقع تیک‌تاک حاضر شده بود در قالب طرحی به نام «پروژهٔ تگزاس»، فراتر از محلّی‌سازی داده‌های شهروندان آمریکایی، تیمی اختصاصی از میان شهروندان آمریکایی (و نه چینی یا خارجی) برای مدیریت داده‌های شهروندان آمریکایی تشکیل دهد و سیاست‌های بسیار محدودی برای خروج داده‌ها از آمریکا وضع کند. تیک‌تاک حتی این پیشنهاد را نیز مطرح کرده بود که کمیتهٔ سرمایه‌گذاری‌های خارجی آمریکا (CFIUS) و شرکت اوراکل به‌عنوان متخصصِ معتمد، بر فرایندهای مرتبط با داده‌های شهروندان آمریکایی و سیاست‌های مدیریت محتوای تیک‌تاک نظارت کنند، **اما درنهایت این مجموعه پیشنهادها که فراتر از محلّی‌سازی داده‌ها بود نیز نتوانست سیاستمداران آمریکایی را از تصمیم خود برای قطع ارتباط کامل تیک‌تک (divestment) با مالک چینی‌اش منصرف کند؛ تصمیمی که در کنگره تصویب شد.**

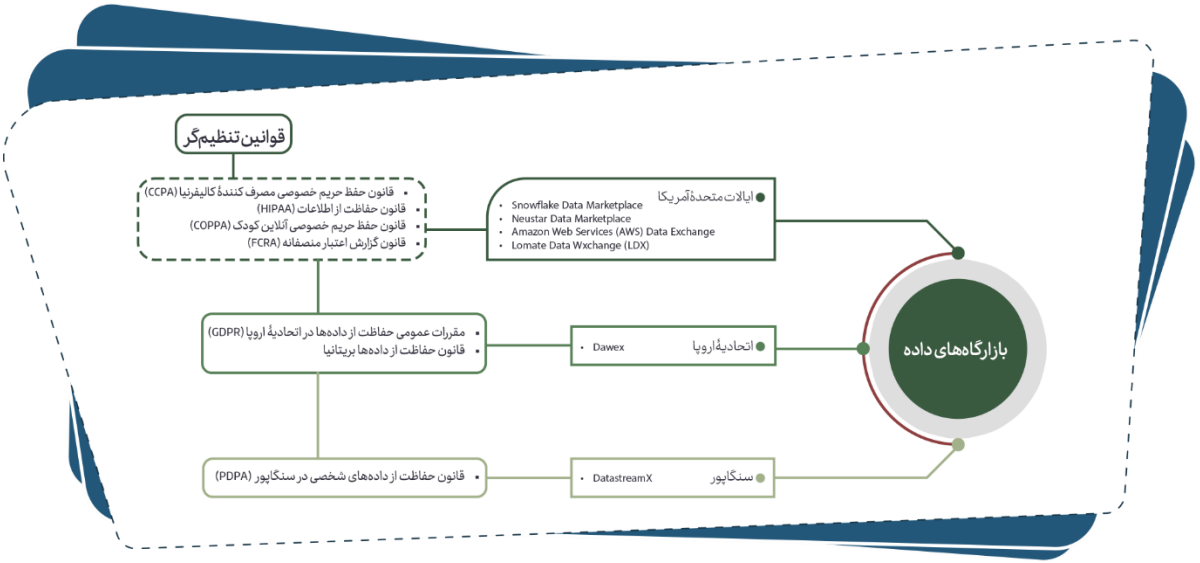
خدمات ابری از اندک صنایعی است که محلّی‌سازی داده‌ها در آن به‌نحوی که حتی شرکت ارائه‌دهندهٔ خدمات نیز به داده‌های شخصی در آن دسترسی نداشته باشند ممکن است. از جایی که در مدل کسب‌وکاریِ خدمات ابری، شرکت ارائه‌کنندهٔ زیرساخت، نظیر گوگل یا

مایکروسافت، نیازی به محتویات استفادهٔ شما از زیرساختِ ابری ندارد، پروتکل‌های فنی خاصی با استفاده از رمزنگاری توسعه داده شده است که می‌تواند تضمین کند به‌غیر از شخصِ استفاده‌کننده از خدمت ابری، بازیگر دیگری امکان دسترسی به چگونگی استفاده از زیرساخت ابری را ندارد. **هرچند این مدل از ارائهٔ خدمات ابری رایج نیست، اما با توجه به فناوری‌اش گران‌قیمت است و عمدتاً برای شرکت‌های بزرگ دارای حجم زیادی از داده‌های شخصی حساس، نظیر اپراتورهای اینترنت، استفاده می‌شود.**

بازارگاه‌های داده: زیرساخت ساماندهی و تسهیل مبادلهٔ داده

بازارگاه داده، عبارت است از یک زیرساخت دیجیتال که در آن، داده به‌مثابهٔ یک کالا که ارزش اقتصادی دارد، ذیل چارچوب‌های حقوقی مشخصی مبادله می‌شود. این شبیه به زیرساخت بورس برای دیگر دارایی‌های اقتصادی است. چنین سامانه‌ای دارای مکانیسم‌هایی برای قانونمندکردن، اعتباربخشیدن و اعتمادسازی‌کردن به‌منظور پشتیبانی از تراکنش‌هایی است که بازیگران مختلف انجام می‌دهند؛ این بازیگران می‌توانند فروشندگانِ داده، خریداران یا مصرف‌کنندگانِ داده باشند و خدمات دهندگان نیز طرف سوم باشند. به عبارتی، بازارگاه داده یک پلتفرم چندجانبه[1] است که به‌عنوان یک پلتفرم، کنشگران مختلف را به یکدیگر وصل می‌کند. چنین پلتفرمی ازطریق ایجاد بستر تبادل و کاهش اختلال در تراکنش‌ها و تخصیص کارآمد منابع و جورسازی[2] عرضه و تقاضا، ارزش ایجاد می‌کند.

1. multi-sided platform
2. matching



نمونه های بازارگاه های داده در آمریکا، اروپا و سنگاپور به همراه زیرساخت حقوقی فعالیت آن ها

این بازارگاه‌ها به‌طور کلّی سه نقش زیر را ایفا می‌کنند:

- پیوند عرضه و تقاضا؛
- تأمین زیرساخت‌های انعقاد قراردادهای فروش؛
- تسهیل تراکنش‌ها و حمایت از نقل‌وانتقالات محصولات داده‌ای و پرداخت‌ها در شرایط ایمن.

امروزه داده را می‌توان به‌منزلهٔ مهم‌ترین سوخت محرّک برای بسیاری از سازمان‌ها به حساب آورد. متأسفانه به‌سبب فقدان معماری مناسب و ضعف در سیستم‌های پردازش بسیاری از داده‌ها، فرصت ایجاد خلق ارزش از آن‌ها از دست می‌رود. بازارگاه‌های داده تلاش دارند با تسهیل تبادل داده، خلق ارزش از آن را امکان‌پذیر کنند. برای تبیین این موضوع بهتر است به این واقعیت اشاره کنیم که بخش عمدهٔ کلان‌داده‌ها در سیستم‌هایی نظیر سیلوها، انبارها و دریاچه‌های داده، بی‌استفاده باقی می‌مانند یا به‌منظور خلقِ آنیِ ارزش، تصمیم‌گیری‌های سازمانی نیاز به سفارشی‌سازی شدن توسط تحلیلگران یا توسعه‌دهندگانِ داده با صرف وقت و هزینهٔ بالا دارند. چالش‌های مذکور موجب پیدایش مفهوم داده-بازار یا بازارگاه‌های داده در طی سال‌های اخیر شده است.

به‌طور کلّی بازارگاه‌های داده را می‌توان بر سه اساس دسته‌بندی کرد:

۱. **محصولات و خدمات**: محصولات و خدمات یک بازارگاه داده که به نوعی برای ذی‌نفعان ارزش ایجاد می‌کنند شامل این موارد می‌شوند:

- محصولات داده‌ای: داده‌های خام، غنی‌سازی‌شده، طولی، کلان‌داده‌ها، فرادادە، داده‌های تحلیلی، بینش حاصل از تحلیل داده‌ها؛
- محصولات فناوری‌محور: الگوریتم‌های استفاده از داده و تحلیل آن، نرم‌افزارهای دسترسی به داده؛
- خدمات زیرساختی: زیرساخت‌های ذخیره‌سازی و ایجاد فضای انبارشِ داده، ایجاد زیرساخت‌های محاسباتی؛
- خدمات بروکری: تسهیل‌کنندهٔ معاملات داده‌ای، واسطه‌گری، بازارسازی و جورسازی طرفین عرضه و تقاضا؛
- خدمات اپراتوری: انجام عملیات اجرایی تبادل داده به‌مثابهٔ اصلی‌ترین کالای اقتصادی مورد معامله؛

- خدمات پشتیبانی: تسهیل تراکنش‌ها از طریق مکانیسم‌های عقد قرارداد و پشتیبانی لجستیک در جهت انتقال سالم داده و پرداخت پایا، ایجاد مکانیسم‌های قانونمندسازی، اعتمادسازی و حمایت از حریم خصوصی در کلیهٔ تراکنش‌ها.

۲. **نوع مالکیت داده و جهت‌گیری تراکنش:** از این منظر دو حالت زیر می‌تواند اتفاق بیفتد:

- رویکرد سلسله‌مراتبی: تراکنش ممکن است توسط مالک بازارگاه داده تنظیم و قیمت‌گذاری شود. در این حالت فروشندگان و خریدارانِ داده با اجازهٔ مالک بازارگاه وارد معامله می‌شوند.
- رویکرد بازارمحور: در این حالت بازار و قوانین حاکم بر آن به تراکنش‌ها نظم می‌دهند. تراکنش‌ها از طریق انعقاد قراردادهای دوجانبه میان فروشندگان و خریدارانِ داده صورت می‌پذیرند و قیمت‌ها با توافق طرفین تنظیم می‌شوند. در این حالت مالک بازارگاه داده به‌عنوان خدمات‌دهندهٔ مستقل، از تراکنش‌ها پشتیبانی می‌کند.

۳. **مکانیسم جورسازی[1] فروشنده و خریدار:** داده‌بازارها را از نظر مکانیسم‌های اتصال دو طرفِ فروشنده و خریدار به چهار دسته به شرح زیر تقسیم می‌کنند:

- *داده‌بازارگاه‌های یک‌به‌یک:*[2] همان‌طور که از عنوانش پیداست، در این‌گونه بازارگاه‌های داده، یک فروشنده به یک خریدار متصل می‌شود و هر دو طرف معاملهٔ خود را در چارچوب بازارگاه انجام می‌دهند. نمونه‌ای از این مکانیسم جورسازی شرکت لایورمپ[3] (آکسیوم[4] سابق) و همچنین بروکرهای داده هستند.

1. matching mechanism
2. One-to-one
3. LiveRamp
4. Acxiom

- *بازارگاه‌های دادهٔ یک‌به‌چند:*[1] در این نوع بازارگاه‌های داده یک فروشنده محصول داده‌ای خود را هم‌زمان با چند خریدار معامله می‌کند. در چنین حالتی، مفاد استاندارد تبادل از طریق واسط‌های برنامه‌نویسی کاربردی[2] اجرا می‌شوند. مصداقی از این مکانیسم جورسازی، واسط برنامه‌نویسی کاربردی توییتر است.
- *داده‌بازارهای چندبه‌یک:*[3] در اینگونه بازارگاه‌ها، چند فروشندهٔ داده، محصولات خود را به یک خریدار پیشنهاد می‌دهند و در عوض خدمات رایگانی را ازطرف خریدار دریافت می‌کنند. این وضعیت در پلتفرم‌های رسانهٔ اجتماعی بسیار مشاهده می‌شود، مانند سرویس‌های گوگل.
- *بازارگاه‌های چندبه‌چند:*[4] این نوع بازارگاه‌ها معمولاً چندجانبه هستند. در این‌گونه بازارگاه‌های چندجانبه، فروشندگان متعددی که شاید همگی مالکیت داده را نداشته باشند (مثلاً بروکر داده یا واسطه‌گر باشند) با خریداران وارد معامله می‌شوند. در این حالت، مالکان داده‌بازار صرفاً خدمات طرف سوم را ارائه می‌دهند و از تراکنش‌ها پشتیبانی می‌کنند. بازارگاه مایکروسافت آزور نمونه‌ای از این مکانیسم جورسازی است.

1. One-to-many
2. Application Programming Interface(API)
3. Many-to-one
4. Many-to-many

مطالعهٔ موردی حکمرانی داده در هند و کرهٔ جنوبی

نکتهٔ جالب دربارهٔ دو کشور هند و کرهٔ جنوبی که مطالعهٔ تجربهٔ حکمرانی آن‌ها در حوزهٔ داده را ارزشمند می‌سازد، **فاصله‌داشتن آن‌ها از الگوهای تبدیل‌شده به کلیشهٔ آمریکایی** (الگوی بازارمحور و متمرکز بر اهداف اقتصادی)، **اروپایی** (الگوی کاربرمحور و متمرکز بر حقوق شهروندان و حریم شخصی) **و چینی** (الگوی دولت‌محور و متمرکز بر اهداف امنیتی و سیاسی) است؛ به‌نحوی که می‌توان ردپای ابزارهای هر سه الگوی مذکور را در این دو کشور یافت و رویکرد هند و کرهٔ جنوبی به حکمرانی داده را نوعی **رویکرد ترکیبی و منحصربه‌فرد** در این زمینه دانست که می‌تواند به اتخاذ نگاهی واقع‌بینانه و عملگرا به حکمرانی داده در ایران کمک کند.

در ادامه و براساس چندین مطالعهٔ معتبرِ منتشرشده دربارهٔ تجربهٔ حکمرانی داده در این دو کشور، به مرور ابعاد مختلف حکمرانی داده، خصوصاً در نسبت با چهار محور مطرح‌شده در بخش قبل خواهیم پرداخت.

داده‌باز

داده‌باز یکی از حوزه‌های حکمرانی داده است که با فراهم‌کردن دسترسی بازیگران مختلف، شامل شهروندان و کسب‌وکارها، با مجموعه‌ای از داده‌ها سروکار دارد که عمدتاً شامل داده‌های عمومی و دولتی می‌شود. البته گاهی گسترهٔ داده‌های مربوط به این حوزه از این نیز فراتر می‌رود که در ادامه و در نمونهٔ هند به آن اشاره می‌کنیم.

کشور هند اقدام به فراهم‌کردن دسترسی به داده‌های دولتی ازطریق سیاست ملّیِ به‌اشتراک‌گذاری و دسترسی به داده[1] کرده است که همهٔ دستگاه‌های دولتی را موظّف به انتشار داده‌های غیرحساس و غیرشخصیِ جمع‌آوری‌شده به‌وسیلهٔ منابع عمومی کرده است. این داده‌ها در یک درگاه ملّی با نام «سکوی داده‌های دولت باز»[2] و در قالب‌های استاندارد مختلف

1. The National Data Sharing and Access Policy
2. Open Government Data Platform

منتشر شده است و ساختارهای پرداخت متناسبی جهت تشویق دستگاه‌های دولتی به انتشار این داده‌ها تعبیه کرده است.

به‌غیر از این برنامه که تاکنون اجرا شده و دسترسی شهروندان هندی به دادگان‌های متعددی را فراهم کرده است، دولت هند برای اصلاح و بهبود سیاست ملّیِ به‌اشتراک‌گذاری و دسترسی به داده، دست به راه‌اندازی یک ادارهٔ مدیریت داده[1] زده است؛ اداره‌ای که وظیفهٔ جمع‌آوری داده‌های کلان در سطح ملّی، ایجاد استاندارد برای جمع‌آوری و ذخیره‌سازی این داده‌ها و همکاری با بخش خصوصی در این زمینه را خواهد داشت.

یکی از ایده‌های منحصربه‌فرد دولت هند در پیش‌نویس قانون حفاظت از داده‌های شخصی این کشور طرح شده بود فراهم‌کردن دسترسی نه تنها به داده‌های عمومی و دولتی، بلکه به داده‌های غیرشخصیِ[2] جمع‌آوری‌شده توسط بخش خصوصی بود. هدف از این اقدام فراهم‌کردن دسترسی گروه‌های اجتماعی مختلف به داده‌های جمع‌آوری‌شده از آن‌ها به‌عنوان حقوق این گروه‌ها از یک سو و افزایش توانایی دولت برای سیاست‌گذاری شواهدمحور و ارائهٔ خدمات به شهروندان مطرح شده بود. در نهایت این ایده پیش از تصویب قانون حفاظت از داده‌های شخصی از این قانون کنار گذاشته شده شد.

کرهٔ جنوبی به‌رغم پیشرفت‌های قابل‌توجه در زمینهٔ داده‌باز، درحال حاضر با سه چالش عمده در زمینهٔ فراهم‌کردن دسترسی شهروندان و بخش خصوصی به داده‌های مفید مواجه شده است:

- **تداخل وظایف، رقابت دستگاه‌های مختلف و خلأ یک نهاد تصمیم‌گیر:** درحال حاضر در کرهٔ جنوبی سه نهاد دولتی، شامل وزارت کشور[3] در کنار وزارت علوم و اطلاعات و

---

1. The Indian Data Management Office

۲. Non-personal Data: منظور از داده‌های غیرشخصی در اینجا داده‌هایی که به یک شخص خاص مربوط نیست یا اینکه به مجموعه‌ای از اشخاص مرتبط است که به شیوه‌ای ناشناس‌سازی‌شده که نمی‌توان اطلاعات اشخاص را از آن استخراج کرد.

3. Ministry of the Interior and Safety

ارتباطات[1] و همچنین مرکز آمار کرهٔ جنوبی[2] و چندین شورا و کمیتهٔ سطح بالا و قدرتمند دارای مسئولیت‌هایی متفاوت ولی درعین‌حال متداخل در زمینهٔ حکمرانی داده هستند و هیچ نهادی وجود ندارد که بتواند تصمیم نهایی را به‌نحوی اتخاذ کند که دیگر دستگاه‌ها از آن پیروی کنند.

در نتیجهٔ این موضوع، نهادهای عمومی و اداراتی که بایستی داده‌های خود را در اختیار شهروندان و بخش خصوصی بگذارند از یک سو دچار ابهام در زمینهٔ انتخاب میان دستورالعمل‌ها و مقررات هر یک از دستگاه‌های تصمیم‌گیر شده‌اند و از سوی دیگر می‌توانند با مانوردادن در میان سیاست‌های موازی و متناقض نهادهای مختلف از زیر انجام مسئولیت‌های خود شانه خالی کنند.

- **اولویت‌های متعارض در زمینهٔ حفاظت از داده و دسترسی آزاد به آن:** ادارات و نهادهای عمومی مختلف در کرهٔ جنوبی، باید از یک سو مطابق با سیاست‌ها و دستورالعمل‌های داده‌باز عمل کرده و از سوی دیگر از قوانین و مقررات حفاظت از داده‌های حساس پیروی کنند. در خلأ یک نهاد تصمیم‌گیر بالادستی در زمینهٔ حکمرانی داده، نهادهای عمومی کرهٔ جنوبی نسبت به تبعات ناشی از ایجاد دسترسی به داده‌های خود نگران‌اند و در نتیجه ترجیح می‌دهند خطر نکنند و داده‌های خود را محرمانه نگه دارند یا درصورت فراهم‌کردن دسترسی، آن‌ها را طوری منتشر کنند که استفاده از آن‌ها دشوار باشد.
- **ضعف مهارتی و نیروی انسانی در سازمان‌های عمومی:** در نهایت، و در صورت رفع هر دو چالشی که تشریح شد، یک مانع بزرگ پیش‌روی سازمان‌های دولتی کره‌ای برای پیاده‌سازی سیاست‌های داده‌باز وجود دارد: ضعف نیروی انسانی و مهارت در این سازمان‌ها که از شیوه‌های منحصربه‌فرد استخدام و نگه‌داشت نیروی انسانی در دیوان‌سالاری کره‌ای ناشی می‌شود که در آن مستخدمان به جابه‌جایی‌های مکرر در میان نقش‌ها و ادارات مختلف وادار می‌شوند و مشتاق رشد و دستیابی به

1. Ministry of Science and Information and Communications Technology
2. Statistics Korea

جایگاه‌های مدیریتی هستند. این ویژگی امکان جذب نیروهای متخصص فنی را دشوار می‌کند.

حفاظت از داده

حفاظت از داده‌های شهروندان، یکی دیگر از شئون حکمرانی داده است که عمدتاً متمرکز بر رعایت حقوق و حریم شخصی شهروندان است؛ هرچند به دلیل ارتباط نزدیک با دیگر حوزه‌های حکمرانی داده نظیر محلّی‌سازی داده‌ها (که در ادامه به آن می‌پردازیم) بعضاً قوانین حفاظت از داده شامل طیف مختلفی از تدابیر در حوزه‌هایی نظیر محلّی‌سازی داده نیز هستند.

در گزارش‌های مورد مطالعه، قوانین کرهٔ جنوبی در حفاظت از داده به تفصیل مورد بررسی قرار نگرفته و در نتیجه به اختصار به آن اشاره می‌شود، اما هند در زمینهٔ قوانین حفاظت از داده، ابتکارات جالبی پیاده کرده است که در ادامه به آن‌ها می‌پردازیم.

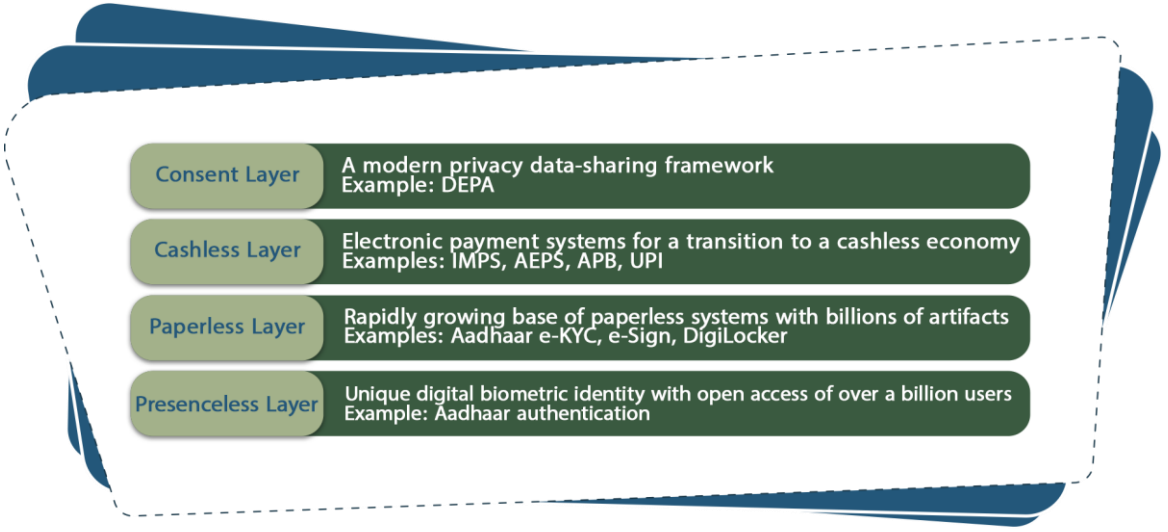
نسخهٔ اولیهٔ قانون هند در زمینهٔ حفاظت از داده‌های شخصی در سال ۲۰۱۸ برای دریافت بازخورد از متخصصان و افکارعمومی منتشر شد و در سال ۲۰۱۹ دولت لایحهٔ خود را تقدیم مجلس کرد. این لایحه تا سال ۲۰۲۱ در مجلس بررسی شد اما در سال ۲۰۲۲ دولت این لایحه را پس گرفت و لایحهٔ جدیدی را با تغییرات قابل‌توجهی به مجلس تقدیم کرد. در نهایت، این لایحه در سال ۲۰۲۳ تحت عنوان قانون حفاظت از داده‌های دیجیتال شخصی (DPDP)[1] در مجلس هند تصویب شد.

قانون مصوّب شامل بندهای رایج و مشابه با دیگر قوانین حفاظت از داده در دنیاست: از یک سو جلب رضایت قبل از جمع‌آوری و پردازش داده‌های شخصی (جالب رضایت والدین برای افراد زیر ۱۸ سال)، حق دسترسی، تصحیح و از بین بردن داده برای اشخاص در کنار حق انتصاب یک نماینده و از سوی دیگر الزاماتی برای تأمین امنیت داده‌ها و اطلاع‌رسانی به هنگام جمع‌آوری، پردازش و انتقال داده‌ها و جبران خسارت‌های احتمالی.

1. Digital Personal Data Protection

اما قانون مصوّب هند شامل برخی ویژگی های جالب است که در ادامه به آن ها می پردازیم:

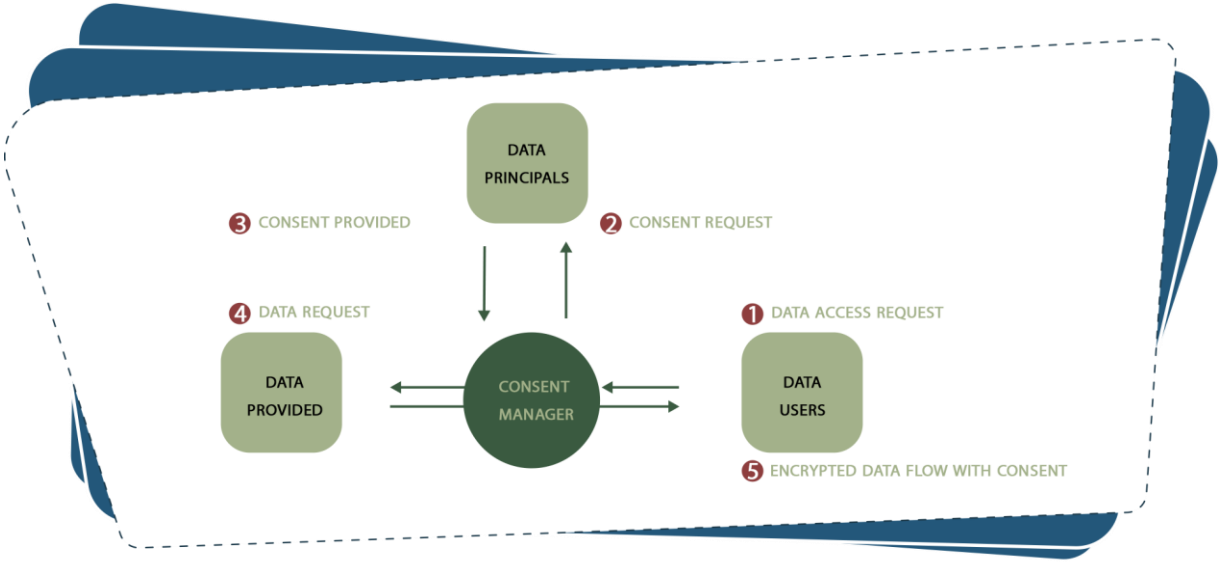
تکیه بر زیرساخت فناورانهٔ بومی: با توجه به گسترش شتابان اقتصاد دیجیتال در آن، به مرور زمان زیرساخت های فناورانهٔ منحصر به فردی با کمک دولت و بخش خصوصی شکل گرفته اند. در لایهٔ زیرین، دولت هند اقدام به راه اندازی یک **سامانهٔ هویت دیجیتال و احراز هویت ملّی** به نام Aadhaar کرده است که امروزه بیش از ۹۵ درصد جمعیت هند تحت پوشش آن قرار گرفته اند. در لایهٔ بعدی و مبتنی بر این زیرساخت هویتی، **زیرساخت امضای دیجیتال** و انجام امور اداری به صورت دیجیتال برای شهروندان فراهم شده است. در لایهٔ بعد و مشابه با خدمت شاپرک در ایران، شرکت ملّی پرداخت های هند[1] اقدام به راه اندازی یک **سوییچ مرکزی برای اتصال سامانه های مالی** بانک های مختلف هندی کرده است که گسترش آن منجر به استفادهٔ بازیگران بین المللی نظیر آمازون، گوگل و متا از آن نیز شده است.



لایه های زیرساخت فناورانهٔ توسعه داده شده توسط دولت هند و بخش خصوصی آن که به دلیل منحصر به فرد و بومی بودن با عنوان پشتهٔ هند یا India Stack شناخته می شوند (منظور از پشته یا Stack مجموعه ای از فناوری های دیجیتال مرتبط با یک دیگر است)

1. National Payments Corporation of India

اما لایه‌ای که بیش از همه با موضوع حکمرانی داده مرتبط است، ساختار توانمندسازی و حفاظت از داده (DEPA)[1] است که کارکرد اصلی آن ایجاد یک استاندارد برای به‌اشتراک‌گذاری داده‌های شهروندان توسط واسطه‌های حرفه‌ای با جلب رضایت آن‌هاست. این زیرساخت دیجیتال که تاکنون در صنعت مالی هند پیاده‌سازی شده و مورداستفاده قرار گرفته است، امکان پدیدآمدن موجودیت‌هایی تحت‌عنوان «میانجیان رضایت»[2] را فراهم می‌کند که کاربران می‌توانند آن‌ها را به‌عنوان میانجی و واسط در زمینهٔ به‌اشتراک‌گذاری اطلاعات شخصی خود معرفی کنند. درصورتی که -به‌عنوان مثال- یک بانک بخواهد به اطلاعات مالی یک شخص که نزد یک مؤسسهٔ بیمه ذخیره شده است جهت اعتبارسنجی آن شخص دسترسی داشته باشد، به میانجی رضایتی که کاربر او را واسط خود معرفی کرده مراجعه می‌کند و پس از ثبت درخواست، میانجی رضایت شخص را به صورت الکترونیکی جویا شده و درصورت کسب رضایت، اطلاعات شخص را به‌صورت امن و رمزنگاری‌شده از مؤسسهٔ بیمه‌ای به بانک منتقل می‌کند.



نمایی از نحوهٔ فعالیت میانجیان رضایت در به اشتراک‌گذاری و انتقال داده‌های شخصی کاربران هندی

1. Data Empowerment and Protection Architecture
2. Consent

در قانون جدیدالتصویب حفاظت از داده‌های شخصی هند، این زیرساخت فناورانه به‌عنوان شیوهٔ به‌اشتراک‌گذاری داده مورد تأکید قرار گرفته است.

- **عقب‌نشینی از مداخلهٔ گسترده:** در نسخهٔ اولیهٔ لایحهٔ حفاظت از دادهٔ دولت هند، یک رگولاتور مستقل و قدرتمند برای نظارت بر پیاده‌سازی سیاست‌های حفاظت از داده تعبیه شده بود[1] که در نسخهٔ نهایی این قانون، دولت هند با عقب‌نشینی از این موضع اقدام به ایجاد یک شورای دولتی با اختیارات بسیار کمتر[2] نسبت به یک نهاد تنظیم‌گر قدرتمند کرده است. می‌توان این اقدام دولت هند را به‌نوعی سیگنالی در راستای پیاده‌سازی محافظه‌کارانه‌تر و با شدت کمترِ قانون حفاظت از داده‌های شخصی دید که به‌نوعی نگرانی‌های بخش خصوصی از مداخلهٔ شدید دولت در این حوزه را کمتر کرده است.

  برخلاف تنظیم‌گر تعبیه شده در قانون اولیه، اعضای شورای حفاظت از داده‌های شخصی توسط دولت منصوب شده و حتی ساختار جزئی آن نیز پس از تصویب قانون توسط دولت طراحی می‌شود. همچنین این شورا برخلاف نهاد تنظیم‌گر قانون اولیه، اختیارات بسیار محدودی برای سیاست‌گذاری، صدور دستورالعمل‌های مختلف و نظارت فعالانه بر کسب‌وکارها دارد و اختیارات آن بیشتر مربوط به پاسخگویی به شکایات و همچنین انجام بازرسی در مواردی است که پرونده‌ای برای نقض قوانین توسط یک کسب‌وکار طرح می‌شود.

- **قائل شدن اختیارات وسیع برای نهادهای امنیتی و انتظامی و همچنین دولت:** یکی از ویژگی‌های قانون حفاظت از دادهٔ هند که آن را در مقایسه با قوانین اروپایی و به‌صورت کلّی غربی متمایز می‌کند، قائل‌شدن بسطِ ید قابل‌توجه برای نهادهای امنیتی و انتظامی در زمینهٔ دسترسی و پردازش داده‌های شهروندان به وسیله ذکر مکرر استثنائاتی برای محدودیت‌های مختلف ذکرشده در قانون است؛ استثنائاتی که با

1. Data Protection Authority
2. Data Protection Board

ارائه اصطلاحات کلی و تفسیرپذیر نظیر« حفظ حاکمیت ملی هند[1]، امنیت ملی[2]، روابط دوستانه با دیگر کشورها[3]، حفظ نظم عمومی[4]»عملا به نهادهای نظارتی هندی امکان دسترسی به داده‌های مورد نظر خود را در شرایط مختلف و بدون مزاحمت خاصی از جانب این قانون می‌دهد.

همچنین در یک استثناء عجیب دیگر، امکان اعطای معافیت از قانون برای برخی کسب‌وکارهای مشخص و یا گروه‌هایی از کسب‌وکارها توسط دولت هند تا پیش از پنج سال از اجرای این قانون را می‌دهد. شاید این موضوع از یک سو امکان انعطاف و تطبیق پیاده‌سازی قانون با شرایط مختلف را به دولت بدهد، اما از سوی دیگر قائل شدن چنین اختیار گسترده‌ای برای دولت در کنار وابستگی کامل شورای نظارتی این قانون به دولت امکان برخورد سلیقه‌ای برای دولت را در موارد مختلف فراهم کرده است که از سوی تحلیل‌گران بسیار نگران‌کننده است و ممکن است به اجرای مؤثر این قانون لطمه وارد کند.

همچنین در نسخه اولیه قانون، به‌غیراز موارد جالب مطرح شده، دو تدبیر جالب دیگر نیز وجود داشت که در لایحه نهایی حذف شد. نخست، امکان دسترسی به داده‌های غیرشخصی بود که در قسمت پیشین و ذیل عنوان داده باز به آن پرداختیم. تدبیر دوم، محدودکردن انتقال فرامرزی داده در قبال برخی از گروه‌های مشخص داده بود که در نهایت به اعطای اختیاری به دولت برای محدودکردن انتقال فرامرزی داده به برخی کشورهای مشخص با اطلاع قبلی تغییر کرد، موضوعی که به تفصیل در بخش بعدی به آن می‌پردازیم.

1. sovereignty and integrity of India
2. security of the state
3. friendly relations with foreign states
4. maintenance of public order

محلّی‌سازی داده[1]

یکی دیگر از شئون حکمرانی داده، محلّی‌سازی داده است که در مقایسه با دو حوزهٔ دیگری که تا به اینجا تشریح شد پیچیده‌تر است و از چشم‌اندازها و با توجه به اهداف مختلفی به آن پرداخته می‌شود. منظور از محلّی‌سازی داده، ذخیره‌سازی داده‌های شهروندان (و بعضاً کاربران ساکن در یک کشور) در سرورهایی در درون همان کشور و قابل دسترسی برای مقامات آن کشور است. البته نسخه‌هایی از محلّی‌سازی داده به ذخیره‌سازی نسخه‌های مشابه در داخل کشور به غیر از نسخه‌های ذخیره شده در خارج از کشور نیز رضایت می‌دهند.

این حوزه از حکمرانی داده که ذیل ادبیات محدودیت‌های انتقال فرامرزیِ داده[2] نیز به آن پرداخته می‌شود، با افزایش اهمیت داده به عنوان یکی از ارکان اقتصادی و امنیتی دنیای امروز به یکی از مباحث سیاست‌گذاری در بسیاری از کشورهای توسعه‌یافته و درحال توسعه تبدیل شده است و ذیل گفتمان‌هایی نظیر «حاکمیت دیجیتال»[3] یا «حاکمیت داده»[4] و با تأکید بر لزوم حفظ استقلال و یا بهره‌برداری از مزایای اقتصادی داده‌های شهروندان مطرح می‌شود.

در دو کشور هند و کرهٔ جنوبی، باوجود مطرح‌بودنِ مسئلهٔ محلّی‌سازی داده در هر دو کشور، این موضوع با اهداف و رویکردهای بسیار متفاوتی دنبال می‌شود. هرچند هند و کرهٔ جنوبی چه در شیوهٔ پیاده‌سازی این سیاست و چه در اهداف آن اشتراکاتی نیز داشته باشند، اما وجوه تفاوت آن‌ها به مراتب برجسته‌تر است. در ادامه به رویکرد منحصربه‌فرد هر دو کشور در قبال موضوع محلّی‌سازی داده‌ها می‌پردازیم:

1. Data Localization
2. Cross-border data flow
3. Digital sovereignty
4. Data sovereignty

غلبهٔ اهداف نظارتی-امنیتی و گفتمان خودکفایی و حاکمیت دیجیتال در هند

در میان کشورهای با بیشترین محدودیت بر انتقال فرامرزیِ داده، پس از چین، هند جایگاه دوم را به خود اختصاص داده است و سیاست‌های متعددی در راستای محدودسازی انتقال فرامرزیِ انواع خاصی از داده‌ها توسط نهادهای عمومی مسئول در حوزه‌های مختلف اعمال کرده است. نکتهٔ جالب دربارهٔ هند این است که این اتفاق درحالی در هند رخ داده که اقتصاد این کشور تکیهٔ قابل‌توجه بر دسترسی به داده‌های دیگر کشورها برای توسعهٔ اقتصاد دیجیتال (علی‌الخصوص در همکاری با کسب‌وکارهای آمریکایی در حوزه‌های مختلف) دارد و همچنین هند به کشورهای غربی نزدیک است (برخلاف چین که می‌توان محلّی‌سازی شدید داده‌ها در این کشور را در چارچوب روابطش با سایر کشورها تحلیل کرد).

در کشور هند، عامل اصلی پیش‌برندهٔ سیاستِ محلّی‌سازی داده‌ها، دغدغهٔ نهادهای نظارتی، اعم از دستگاه‌های امنیتی و انتظامی و همچنین نهادهای حوزهٔ مالی، امکان دسترسی به داده‌های موردنیاز برای نظارت بر پیاده‌سازی قوانین و مقررات این کشور است. هند کشوری با جمعیت بسیار زیاد است که با توجه به گسترش اقتصاد دیجیتال، مردم آن از طیف مختلفی از خدمات دیجیتال استفاده می‌کنند و داده‌های خود را با آن‌ها به اشتراک می‌گذارند. به‌منظور نظارت بر قوانین و مقررات در چنین شرایطی، نهادهای نظارتی هندی نیاز به دسترسی به حجم زیادی از داده‌های ذخیره‌شده نزد کسب‌وکارهایی خواهند داشت که بسیاری از آن‌ها در داخل هند نیستند و فرایند رسمی درخواست دسترسی به این داده‌ها از کانال‌های حقوقی و بین‌المللی دشوار خواهد بود.

با توجه به دسترسی گستردهٔ نهادهای نظارتی هندی به داده‌های شهروندان، به نظر حریم شخصی و آزادی بیان جزو اولویت‌های سیاست‌گذاران هندی نیست، بلکه دسترسی بازیگران خارجی و امکان رصد داده‌های شهروندان هندی از اولویت بیشتری برای دولت هند برخوردار است. یکی از موضوعاتی که در نسبت با محلّی‌سازی داده‌ها طرح می‌شود، حریم شخصی و آزادی بیان کاربران بومی است؛ موضوعی که از سوی بخش‌هایی از جامعهٔ مدنی هند دنبال

می‌شود و یکی از پشتوانه‌های سیاست‌های محلّی‌سازی داده در هند است. اما به نظر در مجموع، این موضوع در مقایسه با دغدغه‌های امنیتی نقش پررنگی در پیشبرد این سیاست‌ها ندارد.

یکی از کاربردهای محلّی‌سازی داده فراهم‌کردن فرصت بهره‌برداری از داده‌های شهروندان هندی برای کسب‌وکارهای داخلی جهت بهبود جایگاه آن‌ها در رقابت با شرکت‌های خارجی است. اما تبعات اقتصادی این سیاست تنها تقویت کسب‌وکارهای داخلی نیست و می‌تواند از جهاتی منجر به آسیب به اقتصاد دیجیتال هند شود. در زمینهٔ اقتصادی، واضح است که دسترسی گستردهٔ بازیگران خارجی برجسته (نظیر گوگل) به داده‌های شهروندان هند و دیگر کشورها و متمرکزشدن این داده‌ها نزد این بازیگران یکی از عوامل اصلی موفقیت اقتصادی آن‌ها بوده است. اما اعمال محدودیت بر انتقال فرامرزی داده‌ها می‌تواند اثرات سوء داشته باشد و به خروج بسیاری از بازیگران بین‌المللی از بازار هند منجر شود که به‌غیر از کاهش سرمایه‌گذاری و سرریز دانش و فناوری در هند، می‌تواند به اخلال در فعالیت کسب‌وکارهای بومی نیز که از خدمات همین بازیگران به‌عنوان زیرساخت و اجزای خدمات خود بهره می‌بردند کشیده شود.

دیپلماسی نیز یکی دیگر از پیشران‌های سیاست محلّی‌سازی داده‌ها بوده است. هند به‌عنوان نمایندهٔ کشورهای درحال توسعه و جنوب جهانی جایگاه خود را در مخالفت با آزادی کامل انتقال فرامرزیِ داده که موضع کشورهای توسعه‌یافته و غربی و از جهات مختلف به ضرر کشورهای درحال توسعه است ترسیم کرده است. هند یکی از اعضای گروه G20 است که در نشست سال ۲۰۱۹ آن در ژاپن، موضوع آزادی انتقال فرامرزی داده مطرح شد و با موافقت بسیاری از اعضا حتی چین همراه شد. اما هند به همراه دو کشور درحال توسعهٔ دیگر یعنی اندونزی و آفریقای جنوبی با این موضوع مخالفت کردند. همچنین هند مخالفت خود با این موضوع را در سازمان تجارت جهانی نیز ابراز کرده است.

در مجموع و با وجود عوامل مذکور، هند هنوز به سمت اعمال یک سیاست کلّی و جامع در زمینهٔ محلّی‌سازی داده‌ها حرکت نکرده و به‌غیر از اختیار اعطاشده به دولت برای محدودسازی

انتقال فرامرزیِ داده به برخی کشورهای خاص در قانون جدیدالتصویب حفاظت از داده‌های شخصی، به محدودیت‌های بخشی در بارهٔ انواع مشخصی از داده‌های حساس اکتفا کرده است.

غلبهٔ اهداف اقتصادی و منافع کسب‌وکارهای داخلی بر اهداف نظارتی در کرهٔ جنوبی

در کرهٔ جنوبی، پیشران‌های سیاست محلّی‌سازی با هند متفاوت است و ریشه‌های اقتصادی عجیب و نامتعارفی دارد. این کشور نیز مانند هند در برخی حوزه‌های مشخص انتقال فرامرزی داده‌ها را محدود کرده است (مانند داده‌های با دقت بالای جغرافیایی)، اما در این زمینه فاصله قابل توجهی با هند دارد. اما با این وجود، مباحثات در بارهٔ پیاده‌سازی و تقویت سیاست‌های محدودسازی داده در کرهٔ جنوبی ادامه دارد و امکان قانون‌گذاری و مقررات‌گذاری در این زمینه وجود دارد.

پیشران اصلی محلّی‌سازی داده در کرهٔ جنوبی، مقررات گستردهٔ اعمال‌شده بر کسب‌وکارهای بومی است که امکان اعمال آن‌ها بر رقبای خارجی وجود ندارد. به‌جای مسدودسازی، سیاست‌گذاران کره‌ای قصد دارند با بومی‌سازی داده‌ها کسب‌وکارهای خارجی را برای پیروی از این مقررات و در نتیجهٔ برای تقویت جایگاه اقتصادی کسب‌وکارهای داخلی تحت فشار قرار دهند. کرهٔ جنوبی طیف گسترده‌ای از مقررات پیچیده برای کسب‌وکارهای دیجیتال خود وضع کرده است که پیاده‌سازی و پیروی از آن‌ها، کسب‌وکارهای کره‌ای را برای رقابت با کسب‌وکارهای خارجی با پیچیدگی‌های متعددی مواجه کرده و آن‌ها را در موضع ضعف قرار داده است؛ مقرراتی نظیر لزوم فعالیت کاربران با نام واقعی، توقف خدمات بازی در ساعات نیمه‌شب و اعمال فیلترهای مشخصی پیش از بارگذاری محتوای تصویری. در شرایطی که پیاده‌سازی این مقررات کسب‌وکارهای داخلی را در موضع ضعف برای رقابت با کسب‌وکارهای خارجی قرار داده، سیاست‌گذاران کره‌ای دو راه را پیش روی خود می‌بینند: مسدودسازی کسب‌وکارهای خارجی (که به‌دلیل هزینه‌های زیاد امکان‌پذیر نیست) و یا محلّی‌سازی داده‌های کسب‌وکارهای خارجی با نیت به‌دست‌آوردن کنترل و اهرم فشار بیشتر برای پیاده‌سازی این مقررات بر آن‌ها. **این راهکار کرهٔ جنوبی از این جهت نامتعارف است که مطابق با قوانین سازمان**

تجارت جهانی، اِعمال مقررات داخلی جهت مداخله در رقابت کسب‌وکارهای داخلی با خارجی غیرمجاز است.

هرچند در کرهٔ جنوبی نیز دغدغه‌های نظارتی و امنیتی با بحث محلّی‌سازی داده‌ها مرتبط است، اما به‌دلیل سابقه و تصورات منفی مردم نسبت به نهادهای نظارتی در کره، پیشبرد این سیاست با این پشتوانه موجب افزایش نارضایتی شده و توسط دولت و نهادهای نظارتی پیگیری نمی‌شود. همانند دیگر کشورهای دنیا، دولت کرهٔ جنوبی و دستگاه‌های نظارتی آن از بابت امکان دسترسی به داده‌های شهروندان برای امور امنیتی و انتظامی و همچنین جلوگیری از دسترسی بازیگران خارجی به این داده‌ها ترجیح می‌دهند تا داده‌های شهروندان کره‌ای به‌صورت بومی ذخیره شود. اما نگاه منفی مردم به مداخلات دستگاه‌های نظارتی در حوزهٔ دیجیتال (که خود را در مهاجرت آن‌ها به پلتفرم‌های خارجی پس از طرح‌شدن اخبار مبتنی بر نظارت این نهادها بر کسب‌وکارهای داخلی نشان داده است) باعث شده است تا از یک سو دولت کرهٔ جنوبی پیگیر سیاست محلّی‌سازی را از این زاویه دنبال نکرده و از سوی دیگر مردم این کشور خواهان محلی‌سازی داده‌ها جهت بهبود حریم شخصی خود نباشند.

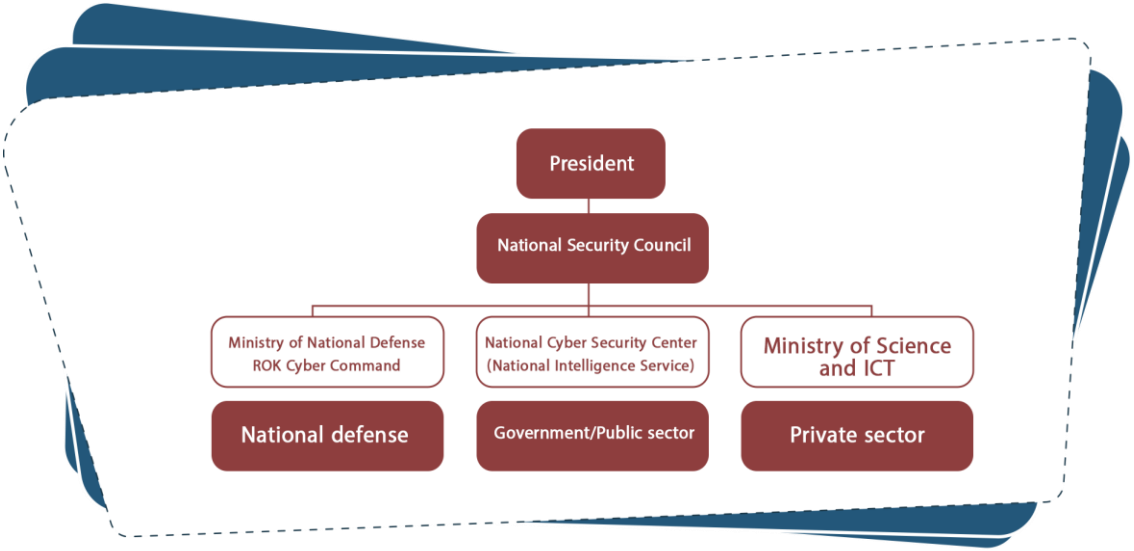
امنیت داده در کرهٔ جنوبی

کرهٔ جنوبی به‌عنوان یکی از کشورهای با نرخ بالای اتصال دیجیتال، مانند دیگر کشورهای مشابه در برابر حملات سایبری آسیب‌پذیر بوده است. مشخصاً ناظر به روابط میان دو کره، حملات سایبری ابزار مناسب و در دسترسی برای کرهٔ شمالی برای واردکردن خسارت به کرهٔ جنوبی و دستیابی به اهداف مختلف سیاسی، امنیتی و حتی اقتصادی بوده است. در پاسخ به این حملات سایبری، کرهٔ جنوبی در طول سالیان گذشته اقدام به اصلاحاتی در لایهٔ حکمرانی و سیاست‌گذاری خود کرده است که در ادامه به آن‌ها می‌پردازیم.

حکمرانی امنیت سایبری در کرهٔ جنوبی از طریق سه نهاد مختلف انجام می‌شود: مرکز ملّی امنیت سایبری (NCSC)[1] ذیل سرویس اطلاعاتی کرهٔ جنوبی در حیطهٔ دولتی و بخش عمومی،

1. National Cybersecurity Center

وزارت علوم و ICT برای بخش خصوصی و فرماندهی سایبری وزارت دفاع کره برای بخش‌های نظامی. در میان این سه نهاد، مرکز ملّی امنیت سایبری نقش محوری و هماهنگی را بر عهده داشته و ناظر به وجود بیش از ۷۰ درصد زیرساخت‌های اطلاعاتی حساس کرۀ جنوبی در بخش عمومی و دولتی، اغلب وظایف بر عهدۀ آن است. درنهایت این سه نهاد با محوریت NCSC، زیر نظر شورای امنیت ملّی کرۀ جنوبی که خود زیر نظر رئیس جمهور قرار دارد، فعالیت می‌کنند.



ساختار حکمرانی امنیت سایبری در کرۀ جنوبی

در سال ۲۰۱۹، استراتژی ملّی امنیت سایبری توسط دفتر امنیت ملّی به‌عنوان مهم‌ترین سند سیاستی کرهٔ جنوبی در زمینه امنیت سایبری منتشر شد. انتشار این سند، با یک نقشهٔ راه ملّی امنیت سایبری برای کرهٔ جنوبی همراه بود که در آن ۱۰۰ وظیفه[1] برای انجام شده در دو الی سه سال آینده فهرست شده بود؛ وظایفی که برخی از آن‌ها از جنس فناوری و عمدهٔ آن‌ها از جنس وظایف سیاستی بود. همچنین در سال ۲۰۲۰ نیز با بازبینی قانون سرویس اطلاعاتی کرهٔ جنوبی، جایگاه محوری این نهاد اطلاعاتی را در زمینهٔ امنیت سایبری تحکیم کرد.

کرهٔ جنوبی در بازهٔ زمانی پس از همه‌گیری کووید-۱۹، در عین رشد بی‌سابقهٔ خدمات دیجیتال و برخط، دچار رکودی اقتصادی شد که دولت را وادار به تدوین برنامه‌ای تحت عنوان Korean New Deal[2] برای ایجاد تغییر در افق اقتصادی و اجتماعی کرهٔ جنوبی کرد. این برنامه که بر سه حوزهٔ فناوری‌های دیجیتال، فناوری‌های سبز[3] و تقویت تورهای ایمنی اجتماعی[4] جامعهٔ کره متمرکز است، در محور یکپارچه‌سازی شبکه‌های داده و هوش مصنوعی، بر امنیت سایبری تأکید دارد و از میان چهار پروژهٔ تعریف شده در این بخش، دو پروژه از جنس امنیت سایبری است.

می‌توان اثر تغییرات در نگاه به مقولهٔ امنیت سایبری را در ادبیات علمی و آکادمیک کرهٔ جنوبی نیز مشاهده کرد. با بررسی کلیدواژه‌های مربوط به حوزهٔ سایبری در نشریات معتبر علمی کرهٔ جنوبی، می‌توان دید که در گذر زمان، کلیدواژه‌های مرتبط با حوزهٔ امنیت سایبری به تدریج به جایگاه‌های بالاتری در فهرست دست پیدا کرده‌اند و در اخیرترین بازهٔ موردبررسی، هر چهار کلیدواژهٔ نخستِ پراستفاده، به حوزهٔ امنیت سایبری مربوط است.

---

1. Task

۲. با الهام از برنامهٔ New Deal پیاده‌سازی شده در آمریکا پس از رکود بزرگ

۳. فناوری‌های مرتبط با انرژی‌های پاک و تجدیدپذیر

4. Social Safety Net

Period	2001-2003 (n = 13)	2004-2009 (n = 62)	2010-2014 (n = 162)	2015-september 2019 (n = 173)
1	Information protection	Information protection	Information protection	Information protection
2	Informatized society	Information security	Information security	Information security
3	Information Disclosure Act	Personal information protection	Personal information protection	Cybersecurity
4	Mass media social ethics	Privacy	Security policy	Cybersecurity (as related to information protection)
5	Mass media freedom of speech	Self-regulation	Information protection governance	Internet of things (IOT) security
6	Encryption	RFID	Information protection management system	Basic law
7	Information disclosure	Governmental regulation Pro	Personal Information Protection Law	personal information protection
8	Criminal law	Risk analysis	Cybersecurity	Cyber terror
9	Secret sharing scheme	Bio authentication	Authentication	Privacy
10	-	Encryption	Policy compliance	Cyber crime

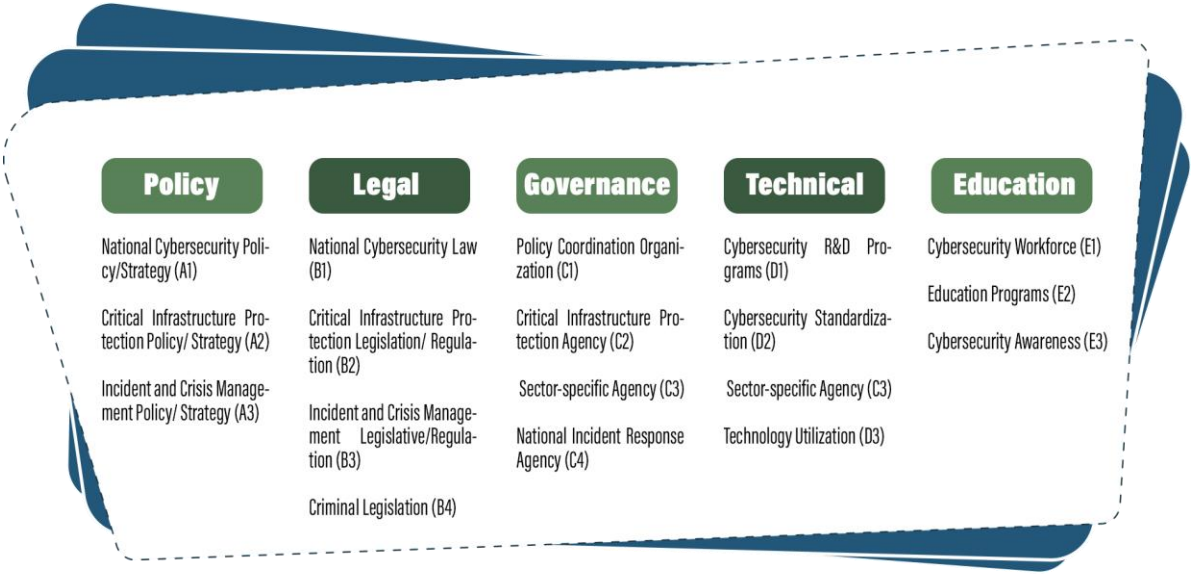
میزان تکرار کلیدواژه های مرتبط با امنیت سایبری در میان کلیدواژه های سایبری در نشریات علمی معتبر کرۀ جنوبی

یکی دیگه از اقدامات منحصر به فرد کرۀ جنوبی، برگزاری رویدادی تحت عنوان «تمرین درگیری سایبری»[1] است که توسط سرویس امنیتی کرۀ جنوبی و مؤسسۀ ملّی پژوهشی امنیت (NSR)[2] که بر اقدامات مؤثر به‌هنگام وقوع یک حمله و بحران سایبری متمرکز است؛ نظیر ارائۀ گزارش وضعیت[3] برای شناسایی علل بحران و تدبیر راه‌حل و همچنین طراحی پاسخ‌های رسانه‌ای[4] جهت جلوگیری از تشدید اثرات بحران سایبری به‌صورت آبشاری و گسترش آن به بخش‌های

1. Cyber Conflict Exercise
2. National Security Research Institute
3. Situation reporting
4. Media response

مختلف جامعه. در مجموع، در این رویداد در قالب بازی‌های شبیه‌سازی‌شده تلاش می‌شود تا چگونگی برقراری ارتباط مؤثر و تصمیم‌گیری حین حملات سایبری آموزش داده شود.

با درنظرداشتن چارچوب تشریح‌شده در قسمت قبلی و تدابیر اتخاذشده توسط سیاست‌مداران کره‌ای، مواجههٔ کرهٔ جنوبی با مسئلهٔ امنیت سایبری نقاط قوّت و ضعفی داشته است که در ادامه به آن می‌پردازیم. پژوهشگران کره‌ای به‌منظور اندازه‌گیری و بررسی توانایی امنیت سایبری کشورهای مختلف و مقایسهٔ آن با توانایی کره، اقدام به ایجاد چارچوبی تحت عنوان «ارزیابی توانمندی امنیت سایبری جهانی» (GCCA)[1] کرده‌اند. این چارچوب، توانمندی‌های امنیت سایبری هر کشور را ذیل معیارهایی که در پنج دستهٔ سیاست‌گذاری، حقوقی، حکمرانی، فنی، و آموزشی دسته‌بندی‌شده‌اند ارزیابی کرده و تصویری جامع دربارهٔ توانمندی‌های سایبری یک کشور ارائه می‌دهد.



توانمندی‌های مورد ارزیابی در چارچوب GCCA کرهٔ جنوبی و دسته‌بندی پنج‌گانهٔ آن‌ها

1. Global Cybersecurity Capability Assessment

ارزیابی‌های انجام‌شده توسط این ابزار، کرهٔ جنوبی را در بُعد فنی (مشخصاً در زمینه‌های تدوین استانداردهای فنی حفاظت از زیرساخت‌ها و پیاده‌سازی فناوری‌های پیشرفتهٔ امنیت سایبری) دارای توانمندی قابل توجهی می‌داند. اما از سوی دیگر توانمندی کره جنوبی در زمینه حکمرانی و همچنین آموزش‌های مرتبط با حوزهٔ امنیت سایبری ضعیف ارزیابی شده است.

یکی از ویژگی‌های مهم حکمرانی کرهٔ جنوبی در زمینهٔ امنیت سایبری، تعلّقِ بیش از ۷۰ درصد از زیرساخت‌های حیاتی به بخش دولتی است. برای مثال، زیرساخت‌های انرژی، آب و حمل‌ونقل که در برخی کشورها همگی به بخش خصوصی واگذار شده‌اند، در کرهٔ جنوبی همگی توسط دولت اداره می‌شوند. این موضوع به دولت کرهٔ جنوبی امکان پیاده‌سازی سیاست‌های مختلف مربوط به امنیت سایبری را بدون مواجه شدن با مقاومت بخش خصوصی فراهم می‌کند.

در مواجهه با حملات سایبری مختلف، دولت کرهٔ جنوبی در هر مورد اقدام به اتخاذ تدابیر مشخصی کرده است که در ادامه به آن‌ها می‌پردازیم. در نتیجهٔ حملهٔ سایبری سال ۲۰۰۳ که منجر به اختلال در اینترنت کرهٔ جنوبی شد، سیاستی برای بک‌آپ‌گیری مستمر معرفی شد که پس از تهیهٔ ابزارهای مناسب توسط دولت، این موضوع برای همه نهادهای دولتی شامل دولت‌های محلّی اجباری شد. همچنین پس از مواجهه با حملات DDoS در سال‌های ۲۰۰۹ و ۲۰۱۱، دولت کرهٔ جنوبی اقدام به ایجاد یک سیستم پاسخ‌دهی فعال به این حملات شامل چگونگی مواجهه با سیستم‌های زامبی[1] کرد. درحال حاضر برنامه‌های مقابله با DDoS در سراسر شبکهٔ کرهٔ جنوبی نصب شده‌اند و تمرین‌های منظمی جهت بررسی میزان آمادگی سیستم انجام می‌شود.

یکی دیگر از سیاست‌های برجستهٔ پیاده‌سازی شده در کرهٔ جنوبی، اصطلاحاً «نت‌سپ»[2] یا همان جداسازی شبکهٔ داخلی سازمان‌ها از اینترنت است. این سیاست در سال ۲۰۰۶ برای وزارت‌خانه‌های دولت کرهٔ جنوبی معرفی شد و تا سال ۲۰۱۰ در کل دستگاه‌های بخش عمومی کرهٔ جنوبی پیاده شد. پس از حملات سایبری سال ۲۰۱۱، دامنهٔ این مقررات به بخش خصوصی نیز

---

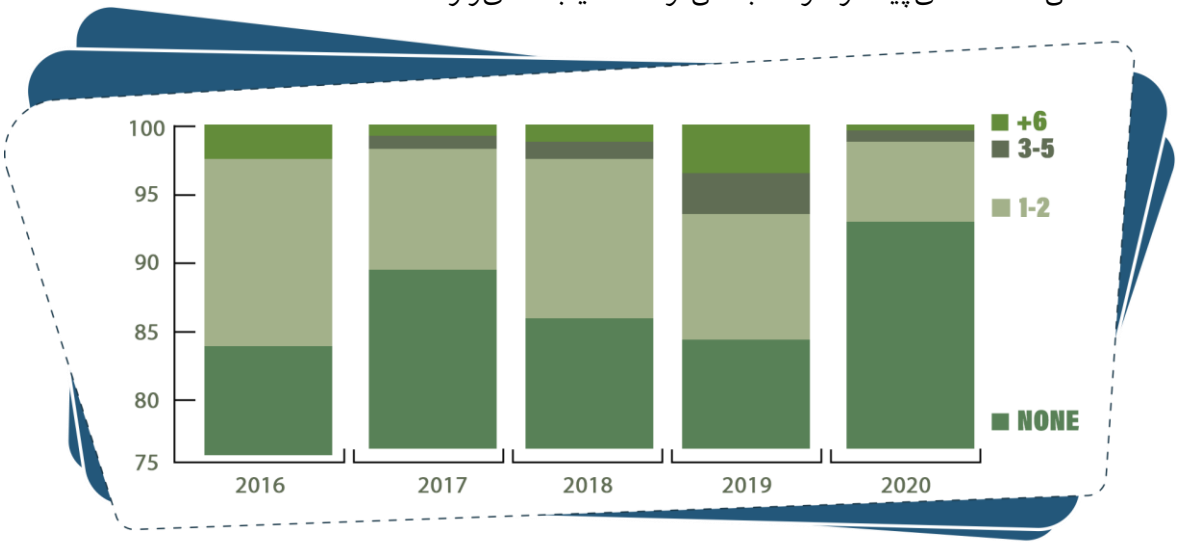
۱. سیستم‌ها و کامپیوترهایی که توسط ویروس آلوده شده و به‌عنوان عاملی برای حملات سایبری شامل DDoS استفاده می‌شوند.

2. NetSep–Network Seperation

گسترش پیاده کرد و شرکت‌های بزرگ و ارائه‌دهندهٔ خدمات مالی نیز موظف به پیاده‌سازی سطح مشخصی از جداسازی شبکه‌های داخلی خود از اینترنت شدند.

یکی دیگر از نقاط آسیب‌پذیری کرهٔ جنوبی، برگزاری رویدادهای بزرگ و بین‌المللی بوده است که به جهت پوشش رسانه‌ای و بین‌المللی هدف مناسبی برای حملات سایبری بوده‌اند. در پاسخ به این موضوع دولت کرهٔ جنوبی پیش از برگزاری چنین رویدادهایی تدابیر مضاعفی اتخاذ می‌کند. برای نمونه، پیش از برگزاری المپیک زمستانهٔ ۲۰۱۸ در کرهٔ جنوبی، تمرین‌های هک با شدت بالا، آزمون نفوذ به شبکه و طیف مختلفی از آموزش‌ها و بررسی‌ها انجام شد. با وجود همهٔ این تدابیر، در نهایت سامانه‌های اطلاعاتی مرتبط با این رویداد ورزشی در یک حملهٔ سایبری از نوع APT (Advanced Persistent Threat) آسیب دیدند و بخش قابل توجهی از خدمات برای مدتی متوقف شد.

اما درمجموع و در گذر زمان، کرهٔ جنوبی توانسته میزان آسیب حملات سایبری را مدیریت کند و باوجود افزایش کلّیِ تعداد حملات سایبری، حملاتی که به اهداف زیادی آسیب وارد می‌کنند کاهش پیدا کرده و اغلب نمی‌توانند آسیب خاصی وارد کنند.



توزیع حملات سایبری انجام شده در هر سال بر اساس تعداد نهادها و دستگاه‌های آسیب دیده از حملات در هر سال

باوجود تدابیر اتخاذشده، شامل استفاده از فناوری‌های مختلف و پیاده‌سازی سیستم‌های مقابله با حملات سایبری که منجر به کاهش آسیب‌های واردشده توسط حملات سایبری در کرهٔ جنوبی شده است، کرهٔ جنوبی هنوز از ضعف‌های متعددی در زمینهٔ مقابله با این حملات رنج می‌برد. برجسته‌ترین ضعف کرهٔ جنوبی در زمینهٔ امنیت سایبری، در لایهٔ حکمرانی است که برجسته‌ترین نمونهٔ آن نبود یک نقشهٔ جامع و یک نهاد هماهنگ‌کننده در سطح بالا در طی سالیان گذشته بوده است.

این ضعف منجر به برخوردهای موردی با حملات سایبری می‌شد و به جای وجود یک رویکرد جامع و کلّی، پس از هر حملهٔ سایبری، مجموعه‌ای از تدابیر مرتبط با تجربهٔ همان حمله اتخاذ می‌شد که لزوماً با تدابیر قبلی هماهنگ نبوده و بعضاً با آن‌ها هم‌پوشانی داشتند. هم‌اکنون و پس از انتشار استراتژی ملّی امنیت سایبری کرهٔ جنوبی در سال ۲۰۱۹، باید دید که این استراتژی چقدر می‌تواند در ایجاد یک رویکرد جامع به امنیت سایبری مؤثر باشد.

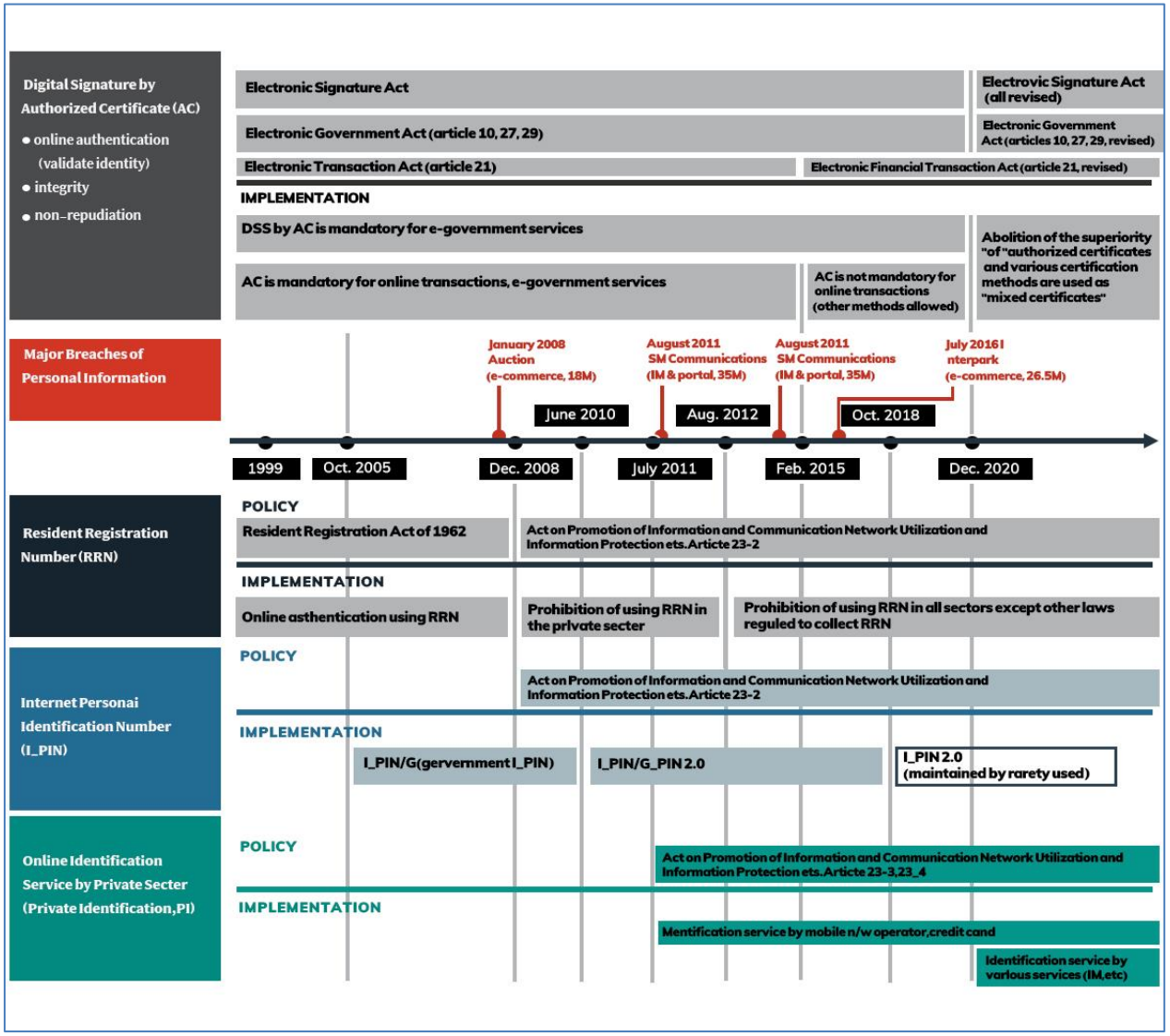
توسعهٔ زیرساخت‌های دیجیتال در کرهٔ جنوبی

به‌طور خلاصه، تجربهٔ کرهٔ جنوبی در زمینهٔ زیرساخت احراز هویت و امضای آنلاین، مبتنی بر ورود ابتدایی دولت به این حوزه‌ها و تلاش برای راه‌اندازی یک زیرساخت متمرکز ملّی بوده است که پس از سطحی از فراگیرشدن و آزمون و خطاهای مختلف، درنهایت زیرساخت‌های دولتی جای خود را به زیرساخت‌های متکثّر ولی درعین‌حال با کارایی و تأثیر بیشترِ بخش خصوصی داده‌اند.

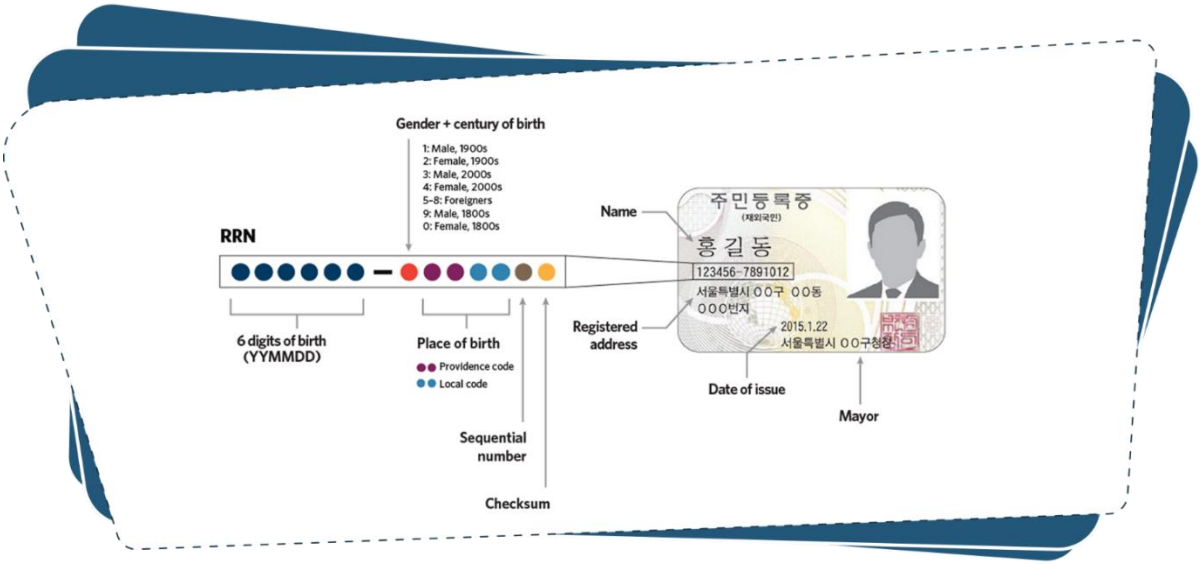
در این مسیر نقش دولت به‌عنوان یک بازیگر قدرتمند، انجام سرمایه‌گذاری اولیه و تسریع پذیرش[1] این فناوری‌های مهم در جامعه بوده است. اما در گذر زمان ناکارایی زیرساخت‌های دولتی بروز پیدا کرده و سیاست‌گذاران کره‌ای به این نتیجه رسیدند که بایستی به‌تدریج نقش دولت را به حداقل برسانند و زمینهٔ فعالیت بخش خصوصی را به‌منظور ارائهٔ کیفیت بالاتری از خدمات فراهم کنند. در ادامه و پس از مشاهدهٔ نمایی کلّی از تطوّر تدابیر کرهٔ

1. Technology adoption

جنوبی در قبال این دو موضوع، به‌صورت جزئی‌تر به تجربهٔ کره جنوبی در این دو حوزه می‌پردازیم.



کرۀ جنوبی در ابتدا در اغلب زیرساخت‌های دولتی خود برای احراز هویت کاربران، از شمارۀ یکتایی تحت عنوان RRN[1] استفاده می‌کرد. این شماره درواقع معادل کدملّی موجود در کارت‌های ملّی در ایران است، کارت‌هایی که از آن‌ها با عنوان اختصاری RRC[2] یاد شده است. شیوۀ تدوین کد RRN به‌نحوی است که نمی‌توان هویت صاحب کد را از آن تشخیص داد، اما می‌توان تشخیص داد که آیا این یک کد RRN معتبر است یا نه. ناظر به این موضوع، بخش خصوصی کره و وب‌سایت‌های مختلف کره‌ای شروع به استفاده از RRN به‌عنوان یکی از اطلاعات ثبت‌نام کاربران کرده و به‌دلیل یکتایی این شماره برای شهروندان کره‌ای، از آن به‌عنوان کلید شناسایی کاربران در پایگاه‌های دادۀ خود استفاده می‌کردند.



تصویری از کارت RRC شهروندان کرۀ جنوبی و کد RRN موجود در آن

1. Resident Registration Number
2. Resident Registration Card

این استفادهٔ گسترده از RRN به‌عنوان ابزار احراز هویت، منجر به یک هک و نشت گستردهٔ اطلاعات در سال ۲۰۰۸ شد که در نتیجهٔ آن دولت کره به‌تدریج و درنهایت در سال ۲۰۱۲ جمع‌آوری کد RRN شهروندان برای کسب‌وکارهای دیجیتال کره‌ای (به‌غیراز در مواردی که قانون صریحاً به‌آن اشاره کرده است) ممنوع شد.

البته پیش از این واقعه، دولت کرهٔ جنوبی به‌تدریج و از سال ۲۰۰۶ اقدام به معرفی جایگزینی مطمئن‌تر برای RRN تحت عنوان I-PIN[1] کرده بود. I-PIN درواقع خروجی یک فرایند رمزنگاری بود که با دریافت اطلاعات مختلفی از کاربر (شامل RRN) شمارهٔ یکتا و به‌مراتب امن‌تری از RRN برای احراز هویت در سایت‌های کره‌ای ارائه می‌کرد. به‌دلیل پیچیدگی‌های فنی I-PIN نیازمند نصب نرم‌افزارهای مشخصی بر روی کامپیوترهای شخصی بود که استفاده از آن را برای بسیاری از کاربران دشوار می‌ساخت. در نتیجهٔ این مسئله، به I-PIN در مقایسه با RRN اقبال چندانی نشد. اما با وجود مکانیزم‌های امنیتی پیشرفته‌تر، یکی از سرویس‌های صدور I-PIN نیز در سال ۲۰۱۵ هک شد که در نتیجهٔ آن، تمامی I-PIN‌های موجود دوباره از ابتدا صادر شد و بازهٔ عمر یک‌ساله‌ای برای هر I-PIN تعیین شد؛ تصمیماتی که با خلق پیچیدگی بیشتر منجر به دشواری بیشتر در استفاده از این مکانیزم شد و اقبال مردم به آن را کاهش داد.

درنهایت، کرهٔ جنوبی موفق‌ترین مکانیزم احراز هویتِ برخط را در بخش خصوصی خود یافت. در سال ۲۰۱۲ و پس از نشت داده‌های RRN و عدم اقبال به I-PIN، دولت کرهٔ جنوبی به سه اپراتور تلفن همراه مجوّز ارائهٔ خدمت احراز هویت اعطا کرد؛ خدمتی که ابتدا بر پایهٔ رفت‌وبرگشت‌های پیامکی انجام می‌شد و به‌تدریج و با گسترش تلفن‌های همراه هوشمند، از فناوری‌هایی نظیر کیوآر کد و احراز هویت زیست‌سنجی[2] بهره‌مند شد. پس از موفقیت این ابتکار، دولت کرهٔ جنوبی در سال ۲۰۱۷ تصمیم به اعطای این مجوّز به هفت شرکت کارت اعتباری نیز گرفت و در سال ۲۰۲۱ نیز با منسوخ شدن رسمی سرویس I-PIN، خدمات احراز هویت بخش خصوصی به شیوهٔ اصلی و رسمی احراز هویت برخط در کرهٔ جنوبی تبدیل خواهند شد.

---

1. Internet Personal Identification Number
2. Biometric

پیش از دستیابی به این موفقیت، کرهٔ جنوبی یک ابتکار دیگر را نیز در زمینهٔ احراز هویت کاربران اینترنت آزمود: لزوم استفاده از نام واقعی کاربران در سایت‌های پربازدید کره‌ای. این ابتکار که با هدف سالم‌سازی محیط اینترنت در سال ۲۰۰۷ پیاده‌سازی شد، میزان محتوای ناسالم سایت‌های مورد هدف (مشخصاً فروم[1]های اینترنتی) را اندکی کاهش داد. اما از یک سو استفادهٔ کلّی از خدمات اینترنتی را نیز کاهش داده و از سوی دیگر با مقاومت جدّیِ وب‌سایت‌های خارجی مواجه شد. یوتیوب پس از قرارگرفتن ذیل این قانون در سال ۲۰۰۹، ارائهٔ خدمت به کاربران کره‌ای را متوقف کرد که این موضوع باعث عقب‌نشینی مقامات کره‌ای شد؛ این عقب‌نشینی خود موجب شکایت وب‌سایت‌های داخلی به دلیل مورد تبعیض واقع‌شدن در مقایسه با وب‌سایت‌های خارجی شد. درنهایت در سال ۲۰۱۲ دادگاه قانون اساسی کرهٔ جنوبی[2] این ابتکار را خلاف قانون اساسی تشخیص داد و الزام آن را رفع کرد؛ تصمیمی که یکی از عوامل مؤثر بر آن، ترک‌کردن کسب‌وکارهای داخلی توسط کاربران و تبعیض علیه این کسب‌وکارها بود.

همانند حوزهٔ احراز هویتِ برخط، دولت کرهٔ جنوبی از دههٔ ۹۰ میلادی با هدف فراهم‌کردن بستر توسعهٔ اقتصاد دیجیتال به سمت ایجاد زیرساختی برای امضای برخط حرکت کرد. در سال ۲۰۰۱ میلادی و پس از تصویب قوانینی برای رسمیت‌بخشیدن به امضای الکترونیک و ایجاد پشتوانهٔ قانونی برای آن، یک خدمت PKI[3] ملّی مبتنی بر فناوری رمزنگاری برای پیاده‌سازی امضای الکترونیک راه‌اندازی شد. ذیل این خدمت، سازمان اینترنت و امنیت کرهٔ جنوبی یا KISA[4] در کنار پنج سازمان خصوصی دیگر که به‌عنوان مقام‌های اعطاکنندهٔ گواهی (CA)[5] تعیین شده بودند، گواهی‌های دیجیتالی[6] برای کاربران صادر می‌کردند که در قالب فایل‌های

1. Forum
2. Constitutional Court of Korea
3. Public key infrastructure
4. Korea Internet & Security Agency
5. Certificate Authority
6. AC (Authorized Certifticate)

مشخصی بر روی کامپیوتر کاربران ذخیره می‌شد و هنگام نیاز برای امضای الکترونیک به کسب‌وکار ارائه‌دهندهٔ خدمت الکترونیک، (مثلاً به یک بانک) ارائه می‌شد.

این ابتکار در سالیان آغازین پیاده‌سازی خود بسیار موفق بود و تا سال ۲۰۱۰ نیز روش اصلی امضای الکترونیک در کرهٔ جنوبی بود، اما به‌تدریج وابستگی آن به زیرساخت‌های نرم‌افزاریِ مشخص (نظیر الزام به استفاده از اینترنت اکسپلورر و ActiveX) موجب دشواری استفاده از آن در یک دنیای دیجیتالِ درحال تحول و همچنین موجب نمایان‌شدن برخی از ضعف‌های امنیتی این زیرساخت شد، تا جایی که سیاست‌مداران کره‌ای در سالیان میانی دههٔ ۲۰۱۰ از حذف الزام به استفاده از این زیرساخت برای جلب محبوبیت استفاده می‌کردند و درنهایت نیز تا سال ۲۰۱۷ تمامی الزام‌های استفاده از این زیرساخت، به‌عنوان مثال در خدمات بانکی رفع شد.

درنهایت در حوزهٔ امضای الکترونیک نیز دولت کرهٔ جنوبی راهکار نهایی خود را در روی‌آوردن به بخش خصوصی و پذیرفتن تکثّر در خدمات امضای الکترونیکِ ارائه‌شده توسط شرکت‌های بزرگِ خصوصی دید. در سال ۲۰۲۰، دولت کرهٔ جنوبی به خدمات امضای الکترونیکِ اپراتورهای مخابراتی و همچنین مؤسسه‌های مطرح مالی خود اعتبار بخشید و امکان استفادهٔ گسترده از آن‌ها را فراهم کرد؛ تصمیمی که منجر به افزایش تنوع و کیفیت خدمت امضای الکترونیک در اقتصاد دیجیتال کرهٔ جنوبی شد.

RESEARCH PAPERS

دفترهای آبی

مقالات پژوهشی (Research Papers) از مهم‌ترین ابزارهای توسعهٔ دانش هستند که با تکیه بر داده‌های تجربی به بررسی دقیق و جامع موضوعات تخصصی می‌پردازند.

دفترهای آبی دسته‌ای از گزارش‌های تفصیلیِ تولیدشده در پژوهشگاه فضای مجازی، و محصول رصدِ مطالعات تحقیقی اندیشکده‌ها و نخبگان جهان در موضوعات مرتبط با فضای مجازی است.

پژوهشگاه فضای مجازی