



رویکرد راهبردی به مسائل حکمرانی داده :
نظام مسائل حکمرانی داده جمهوری اسلامی
ایران

پیش‌نویس اولیه گزارش راهبردی

گروه حکمرانی عصر دیجیتال
آذر ۱۴۰۰





دیدگاه تخصصی	نوع سند
گروه حکمرانی عصر دیجیتال	حوزه تخصصی
رویکرد راهبردی به مسائل حکمرانی داده: نظام مسائل حکمرانی داده جمهوری اسلامی ایران	برنامه
سیما رفسنجانی نژاد	عنوان
دکتر حسین میرزاپور- عمادالدین پاینده	نگارنده/نگارندگان
آذر ۱۴۰۰	ناظر کیفی
شورای راهبردی روابط خارجی	تاریخ انتشار
	مخاطب

جملات کلیدی

کلمات کلیدی

حکمرانی داده، حکمرانی اینترنت، صیانت از داده، راهبردهای حکمرانی داده

مقدمه

استعاره‌ی جدید «داده در عصر جدید مانند نفت در زمان قدیم است»، به نقش مهم داده در توسعه اقتصاد دیجیتال اشاره دارد. پیشرفت فناوری‌های نوظهور باعث می‌شود داده‌ها با روش‌هایی جدید و بی‌سابقه و با سرعت و حجمی فوق‌العاده جمع‌آوری، ایجاد، استفاده، پردازش، تحلیل، اشتراک‌گذاری، منتقل، کپی و ذخیره‌سازی شوند. کشورهای منطقه خاورمیانه امروزه به سرعت در حال طرح‌ریزی برنامه‌هایی برای مبدل شدن به سرآمد در زمینه فناوری‌های نوین و بالاخص دیجیتالی در بازار رقابتی داغ منطقه هستند. نبودن ایران در حلقه ارزش جهانی و عدم پیوند اقتصاد دیجیتال ایران به بازار منطقه‌ای و جهانی، موانعی پیش‌روی تعامل کشور با نظام بین‌الملل ایجاد خواهد کرد. بررسی شاخص‌های مرتبط با حکمرانی داده نشان‌دهنده فاصله ایران با کشورهای همسایه است؛ برای مثال دیدبان داده باز^۱ در آخرین گزارش خود (۲۰۲۰) ایران را در جایگاه ۱۳۱ در بین ۱۸۷ کشور قرار داده است که در مقایسه با برخی از کشورهای منطقه همچون امارات (۱۶) و عمان (۱۱) نیز اختلاف فاحشی به نظر می‌آید. ضرورت دارد از فرصت فناوری‌های نوظهور در راستای تجاری شدن کلان‌داده‌ها و ایفای نقش فعال در فرایند «دیجیتالی شدن خاورمیانه» نهایت استفاده صورت گیرد.

تعریف مفاهیم

الف. **حکمرانی بر داده:** عبارت است از اصول و خط‌مشی‌های کلان حاکمیت در زمینه تضمین حداکثری منافع ملی و امنیتی مرتبط با داده که مسائلی از قبیل: مالکیت داده، تعیین انواع داده (حساس، عادی، تجاری، عمومی و ...)، مدیریت جریان‌های داده در کشور، کیفیت داده، دسترسی‌پذیری داده، کیفیت انتشار داده، انحصار داده، شبکه ملی اطلاعات، تدوین الزامات بومی‌سازی داده، دستورالعمل‌های پردازش و آزادسازی داده‌های عمومی، تحدید بهره‌برداری‌های مجاز از داده‌ها و مدیریت پایگاه‌های اطلاعات ملی و ... در این دامنه قرار می‌گیرد.

ب. **حکمرانی با داده:** به طور مشخص اینکه در شرایط انقلاب صنعتی چهارم و ارزشمند شدن داده به عنوان مهمترین ابزار تنظیم‌گری، نظارت و پایش شئون مختلف حکمرانی، چگونه می‌توان با استفاده از داده (علی‌الخصوص کلان‌داده) به بهبود، هوشمندسازی، روزآمدسازی و کارآمدسازی تحقق اهداف حکمرانی کمک نمود. مسائلی همچون: توسعه قطب‌های منطقه‌ای و تعاملات بین‌المللی داده، ملی‌سازی داده، ارتقاء شاخص‌های هوشمندسازی، تحقق حکمرانی داده‌محور، تحقق سیاستگذاری شواهدمحور، تقویت مراکز داده و خدمات ابری کشور، گذار به رویکرد خودتنظیمی، دولت الکترونیک، پرتال‌های داده باز، کاربست فناوری در جهت افزایش اشراف حاکمیت بر فضای مجازی به جای تصدی‌گری، بررسی راهکارهای مشارکت بخش خصوصی در نوآوری‌های بخش عمومی و ... در این دسته ملاحظه می‌شود.

ج. **صیانت از داده:** بر سیاست کشور برای صیانت هرچه کارآمدتر از حقوق شهروندان و حریم خصوصی کاربران در برابر تهدیدات و سوءاستفاده‌های امنیتی، اقتصادی، اجتماعی، فرهنگی و سیاسی بخش خصوصی (شرکت‌های ارائه‌دهنده خدمات داده‌محور خارجی و داخلی) دلالت دارد. برخی از مسائل برجسته ذیل این دسته عبارت‌اند از: روزآمدسازی قوانین بالادستی حریم خصوصی، مسئولیت پلتفرم‌ها، سیاست پناهگاه امن^۲، وضع جرایم بازدارنده، امنیت داده، مالکیت فکری، مشارکت و مطالبه‌گری نهادهای مدنی در حوزه حریم خصوصی، سواد دیجیتال و داده.

¹ Open Data Watch

² Safe Harbor Privacy Principles

رویکرد کشورهای پیشرو در بحث حکمرانی داده

به طور کلی سه رویکرد در رابطه با حکمرانی داده در دنیا برجسته هستند:

۱- الگوی دولت-محور چین و روسیه: در رویکرد چینی و روسی کنترل کامل فضای اینترنت و داده توسط دولت‌ها انجام می‌شود. براساس رویکرد مذکور، داده‌های جمع‌آوری شده توسط بخش خصوصی را باید یک دارایی ملی قلمداد کرد که دولت براساس نیاز به آن دسترسی داشته یا دسترسی به آن را محدود کند. در رابطه با جریانات داده برون‌مرزی نیز برخی کشورها مانند چین و روسیه انتقال بیشتر انواع داده را محدود کرده‌اند. برای مثال قانون امنیت سایبری چین می‌گوید اطلاعات شخصی و داده‌های مهم کاربران باید فقط در داخل کشور جمع‌آوری و نگهداری شود.

۲- الگوی حریم خصوصی محور اتحادیه اروپا: رویکرد اروپایی در مورد حکمرانی داده رویکردی است که قانون‌نویسی و مقررات‌گذاری جامع را در دستور کار قرار می‌دهد. در این نگاه، قوانین جامع و فراگیر در زمینه حمایت از داده‌ها، تعیین مراجع عمومی برای ثبت داده‌ها، پایگاه داده، حل اختلاف، اخذ رضایت قبلی در مورد پردازش برخی داده‌ها و... مدنظر قرار می‌گیرد. احترام به حریم خصوصی شهروندان و حقوق بشر مهم‌ترین دغدغه این الگوی حکمرانی است. در این زمینه اروپا اقداماتی از جمله تصویب «مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»³ GDPR در زمینه حفظ حریم خصوصی انجام داده است. مقررات حفاظت از داده اتحادیه اروپا، شرکت‌ها را ملزم می‌کند تا برای بهره‌برداری از اطلاعات شخصی کاربران از آنها رضایت صریح بگیرند و همه مزایا و معایب به‌اشتراک‌گذاری داده را به کاربران اطلاع دهند. در رابطه با جریانات داده برون‌مرزی نیز می‌گوید که انتقال داده فقط به کشورهایی مجاز است که سیستم حفاظت از داده مناسبی داشته باشند. این رویکرد البته، با محدودیت‌های قابل توجهی نیز همراه است که عمدتاً به ظرفیت و توان اجرایی‌سازی قوانین عریض و طویل مذکور بر می‌گردد. کاربران معمولاً بخش سیاست‌های حریم خصوصی را مطالعه نمی‌کنند و وقتی متوجه دسترسی غیرمجاز به داده‌هایشان می‌شوند، هیچ اقدامی در برابر آن انجام نمی‌دهند. به همین دلیل، رویکرد مذکور در حل مشکلات مربوط به داده چندان موفق نبوده است.

بسیاری از کشورهای غیراروپایی همچون استرالیا، کانادا، کره جنوبی، ژاپن و... نیز به تقلید از رویکرد اروپایی به تدوین قانونی جامع برای حفاظت از حریم خصوصی کاربران در فضای مجازی پرداخته‌اند.

۳- الگوی «آزاد» ایالات متحده آمریکا: الگوی حاکم در آمریکا مبتنی بر الگوی آزاد بوده است؛ هرچند این الگو طی سال‌های اخیر دچار تغییراتی شده است. در این رویکرد، دولت مداخله نمی‌کند و اختیار در دست شرکت‌های بزرگ است. یعنی سیاست‌های دولت منتج از رشد شرکت‌های بزرگ است. در ایالات متحده آمریکا قانون جامعی برای جمع‌آوری و استفاده از داده‌های شخصی وجود ندارد و فقط چند قاعده و دستورالعمل پایه دیده می‌شود. مثلاً در ماساچوست، شرکت‌ها باید برای انتقال داده در شبکه‌های عمومی، داده‌های شخصی کاربران را رمزگذاری کنند. قانون نوآورانه «حریم خصوصی مصرف‌کننده کالیفرنیا» (CCPA) نیز قوانین متعددی را برای شرکت‌ها در نظر گرفته است. ایالات متحده آمریکا به دلیل اتخاذ روش موردی برای قانون‌گذاری در خصوص حریم خصوصی و رویکرد خودتنظیمی در بخش‌های مختلف حکمرانی اینترنت، فاقد قانونی جامع در این زمینه است.

رویکرد سازمان‌های بین‌المللی در بحث حکمرانی داده

۱- اجلاس جهانی جامعه اطلاعاتی (WSIS) و انجمن حکمرانی اینترنت (IGF)

موضوع حکمرانی اینترنت و حکمرانی داده از موضوعات مهم در دستور کار جهانی است که با فشار کشورهایمانند چین و روسیه وارد ادبیات سازمان ملل متحد شده و متعاقباً منجر به نهادسازی در این حوزه شده است. شکل‌گیری اجلاس جهانی جامعه اطلاعاتی (WSIS) در سال ۲۰۰۳ اولین نتیجه تلاش این کشورها برای گسترده کردن دامنه شرکت‌کنندگان در زمامداری اینترنت بود. سازمان ملل در سال ۲۰۰۵ در تونس اقدام به برگزاری دوره دوم اجلاس جهانی جامعه اطلاعاتی نمود. در این

³ General Data Protection Regulation

اجلاس، به منظور تسهیل گفت‌وگوی بین‌المللی حول مسائل حکمرانی اینترنت، تصمیم به ایجاد مجمع و انجمنی چندملیتی گرفته شد. درخواست تشکیل این انجمن به دبیر کل سازمان ملل ارسال شد و پس از موافقت، **انجمن حکمرانی اینترنت**^۴ (IGF) تأسیس شد. این انجمن جایگاه حقوقی برای تصمیمات الزام‌آور ندارد، بلکه محلی برای تبادل نظر آزاد و برابر افراد درباره مسائل اصلی و مهم اینترنت در جهان باشد.

در سال ۲۰۲۰، انجمن حکمرانی اینترنت به موضوع «دموکراتیزه کردن تولید داده و کاربرد داده» پرداخت؛ به طوری که خود کاربران، قوانین خودشان را وضع کنند و خودشان در مورد اینکه داده‌هایشان چگونه استفاده می‌شوند، تصمیم بگیرند. در گردآوری داده، نباید حریم خصوصی شخصی و حریم خصوصی جمعی جامعه به خطر بیفتد. از جمله مباحث دیگر انجمن این بود که مزایای فناوری‌های داده‌محور باید در دسترس همه قرار داشته باشد نه فقط دولت‌ها و بخش خصوصی. برای این منظور مردم باید به وسایل دیجیتال و اتصال و نیز مهارت سواد دیجیتال دسترسی داشته باشند تا از فناوری‌های داده‌محور استفاده کامل کنند.

۲- «گروه کارشناسان دولتی» و «گروه کاری باز ملل متحد»: دو سازوکار دیگری که در چارچوب ملل متحد در رابطه با موضوعات مرتبط با اینترنت شکل گرفته است گروه کارشناسان دولتی^۵ (GGE) با تعداد محدود (۲۵ دولت انتخاب‌شده توسط دبیر کل ملل متحد) و پروژه کارگروهی آزاد^۶ (OEWG) با امکان مشارکت تمامی دولت‌ها عضو ملل متحد در سال ۲۰۱۸ می‌باشند. هر دو گروه در زمینه‌ی امنیت اطلاعات در فضای سایبر، توسط روسیه ایجاد شده است. هدف از تشکیل گروه‌های مذکور، افزایش نقش دولت‌ها برای تضمین امنیت و ثبات بین‌المللی است که می‌تواند توسط فضای سایبر دچار مشکل گردد.

۳- سازمان همکاری‌های اقتصادی آسیا - پاسیفیک: سازمان همکاری‌های اقتصادی آسیا - پاسیفیک (APEC) شامل ۲۷ کشور می‌شود که «سیستم قوانین حریم خصوصی برون‌مرزی» (CBPR) را توسعه داده است. CBPR چارچوبی قاعده‌محور است که می‌تواند هم حریم خصوصی و هم جریانات داده را بهبود بخشد.

۴- توافقنامه پاریس: امانوئل مکرون «فراخوان اعتماد و امنیت در فضای سایبری» را پایه‌گذاری کرد که اعلامیه‌ای نمادین جهت افزایش فعالیت‌های امنیت سایبری و استانداردهای بین‌المللی برای اینترنت است. تعداد ۶۷ کشور از جمله کل اتحادیه اروپا به اضافه ۳۵۸ شرکت و ۱۳۹ سازمان اجتماعی شهری و بین‌المللی این توافقنامه را امضا کردند. آمریکا، چین و روسیه به توافقنامه پاریس نپیوسته‌اند.

۵- «کنوانسیون دیجیتال ژنو»: طرح پیشنهاد «کنوانسیون دیجیتال ژنو»^۷ در سال ۲۰۱۷ توسط رئیس شرکت مایکروسافت داده شد و پس از آن «توافقنامه فنی امنیت سایبری» و ائتلاف ۳۴ شرکت از مجموعه شرکت‌های فناوری، با شعار مقابله با حملات سایبری دولت‌ها و حفاظت از کاربران و شرکت‌ها اعلام شد. این حرکت با هدایت دولت آمریکا و با محوریت شرکت‌های بزرگ زیرساخت و فناوری سایبری شکل گرفته است و هنجارسازی در حوزه امنیت سایبری با استفاده از دیپلماسی غیررسمی و ظرفیت‌های غیردولتی به یکی از اولویت‌های اصلی آمریکا که به دنبال رهبری جهانی در حوزه اینترنت است، تبدیل شده است.

چالش‌های حکمرانی داده در ایران

• فقدان یا نقص قوانین حکمرانی داده

فقدان قوانین و اصول حقوقی در حوزه‌های «حریم خصوصی»، «امنیت داده»، «طبقه‌بندی داده‌های حساس» و همچنین «مالکیت فکری» و «فقدان مقررات مربوط به دسترسی به داده و محرمانگی و چالش در دسترسی به داده‌ها» از جمله دلایل عدم تحقق حکمرانی داده در کشور است. برای نمونه در مرداد ۱۳۹۷ «پیش‌نویس لایحه صیانت از داده‌های شخصی»، نهایی شد و

^۴ Internet Governance Forum

^۵ Group of Governmental Experts

^۶ Open-ended working group

^۷ Digital Geneva Convention

اردیبهشت ۱۳۹۸ روی میز مجلس شورای اسلامی قرار گرفت؛ اما تصویب لایحه صیانت از داده‌های شخصی در این سال‌ها به تاخیر افتاده است. لایحه بخش‌های مختلفی دارد و در مجموع سعی کرده تمام فرایندهای مربوط به داده را نظام‌مند کند. مسائلی از جمله اینکه داده چیست، داده‌های شخصی و حیاتی کدام‌اند و چطور باید آنها را جمع‌آوری کرد، نحوه نگهداری و پایش داده‌ها، مسئولیت‌پذیری کسانی که با آنها سروکار دارند، محصولات جدیدی که با داده‌ها ایجاد می‌شود، نحوه تعامل سازمان‌ها با صاحب داده، شیوه انعقاد قراردادها، مجوزها و ضمانت اجرایی جزو مواردی است که در این لایحه گنجانده شده است.

همچنین در تیرماه سال ۱۴۰۰ نمایندگان طرحی به نام «قانون یکپارچه‌سازی داده‌ها و اطلاعات ملی» پیشنهاد کردند. طرح مذکور، ضمن ترسیم «نگاشت نهادی زیست‌بوم داده»، سیاست‌گذاری نظام نگهداری، پردازش، دسترسی، یکپارچه‌سازی، تبادل و امنیت داده‌ها و اطلاعات ملی را به عهده «شورای عالی فضای مجازی» قرار داده‌اند. برای اجرای سیاست‌های شورای عالی فضای مجازی، نمایندگان پیشنهاد داده‌اند تا «کارگروه تعامل‌پذیری دولت الکترونیکی» موضوع مصوبه ۵۴ شورای عالی فضای مجازی به «کمیسیون داده‌ها و اطلاعات ملی» یا کمیسیون دوام «تغییر نام پیدا کند. با توجه به موارد ذکر شده، لازم است نقشه راه و نگاشت نهادی زیست‌بوم داده کشور ترسیم شده و ارتباط اجزا، نقش و جایگاه نهادهای متولی با یکدیگر، مشخص گردد تا از عدم همکاری، هم پوشانی و بخشی‌گرایی در بحث حکمرانی داده ممانعت به عمل آید.

• نامشخص بودن مسئله مالکیت داده

به منظور تحقق حکمرانی داده، شفاف شدن بحث «مالکیت داده» ضرورت دارد. در بحث مالکیت داده‌های بخش عمومی، بسیاری از دستگاه‌های اجرایی با فرض گرفتن اختیارات قانونی برای ارائه خدمات و دریافت هزینه آن از محل بودجه عمومی یا به طور مستقیم از مردم، تصور می‌کنند مالکیت داده‌های عمومی با دستگاه است. لیکن به نظر می‌رسد دستگاه، مدیریت داده‌ها را بر عهده داشته و مالکیت تنها با دولت است. نظیر اموال غیرمنقول دولت که مالکیت آنها با دولت است و داده‌ها نیز جزئی از اموال و دارایی‌های دولت بوده و ارزش اقتصادی به مراتب بیشتری دارد. با توجه به اینکه برای تولید داده‌ها از بودجه عمومی کشور استفاده می‌شود بنابراین داده‌ها، ملی محسوب شده و به دولت تعلق دارد، لذا هر دستگاه موظف است اطلاعات خود را در اختیار پنجره واحد دولتی قرار دهد. منظور از مالکیت عمومی و «ملی‌سازی داده‌ها»، دولتی‌سازی داده‌ها نیست بلکه به این معناست که کسب و کارها و مردم بتوانند از آن منتفع شوند.

• قابلیت دسترس‌پذیری داده‌ها

یکی از ویژگی‌های سیاست‌گذاری و حکمرانی مبتنی بر داده، قابلیت دسترس‌پذیری داده‌ها است. این ویژگی به معنای دسترسی آسان به داده‌ها و اطلاعات و در دسترس بودن داده‌ها و اطلاعات به صورت تفصیلی و تفکیک‌شده است. همچنین به روز بودن داده‌ها و اطلاعات و انتشار به موقع داده‌ها ضروری است. براساس آیین‌نامه‌های اجرایی «قانون دسترسی آزاد به اطلاعات» مصوب سال ۱۳۹۳، «سامانه انتشار و دسترسی آزاد به اطلاعات» در سال ۱۳۹۶ راه‌اندازی و اداره این سامانه به عهده دبیرخانه «کمیسیون انتشار و دسترسی آزاد به اطلاعات» قرار گرفت. این کمیسیون باید هر ساله گزارشی درباره رعایت قانون مذکور در مؤسسات مشمول این قانون و فعالیت‌های خود را به مجلس شورای اسلامی و رئیس‌جمهور تقدیم کند. همه دستگاه‌های حاکمیتی عضو کمیسیون مذکور هستند و در قانون پیش‌بینی شده است حتی نهادهایی که زیر نظر رهبری هستند شامل این کمیسیون هستند. ضرورت دارد کمیسیون انتشار و دسترسی آزاد به اطلاعات، سالانه گزارشی از وضعیت پیوستن دستگاه‌های دولتی و شهرداری‌ها به سامانه و میزان همکاری نهادهای سازمان‌ها ارائه دهد.

• نگرانی در رابطه با کیفیت انتشار داده‌ها

«کیفیت داده»‌های منتشر شده از جمله مباحث حائز اهمیت در بحث حکمرانی داده است. داده‌ها به لحاظ کیفیت انتشار در پنج سطح طبقه‌بندی می‌شوند. سطح اول شامل داده‌های دارای قابلیت خوانش انسانی و ذخیره‌سازی مانند داده‌های PDF، سطح

دوم داده‌های ساختار یافته با قابلیت خوانش و ویرایش مانند DOC و HTML، سطح سوم داده‌های دارای قابلیت خوانش، ویرایش و پردازش گروهی مانند XML، سطح چهارم داده‌های دارای قابلیت اتصال به سایر داده‌ها مانند API و سطح پنجم داده‌های شبکه شده (دارای اتصال دوطرفه) به سایر داده‌ها و دارای قابلیت پردازش یعنی «داده باز متصل»^۸ است. با این تعریف و سطح‌بندی، داده‌هایی که در قالب‌هایی مانند PDF یا قالب‌های تصویری مبادله می‌شوند، داده استاندارد نیستند. «داده باز متصل» مرحله نهایی فرایند داده باز است. در این مرحله تمام داده‌های باز در ارتباط با یکدیگر قرار گرفته و به تکمیل هم کمک می‌کنند. این توانایی موجب می‌شود که بتوان اطلاعات گسترده‌ای را بین تمامی سامانه‌ها به اشتراک گذاشت و روی آنها کاوش‌های گوناگونی را اعمال کرد.

با وجود تصویب سند چارچوب تعامل‌پذیری و ریل‌گذاری اولیه در این خصوص و معرفی استانداردهای مشخص در حوزه داده‌ها، دستگاه‌ها بدون توجه به استانداردهای داده و کیفیت داده‌ها، سامانه‌های خود را توسعه داده و مبادرت به اخذ اطلاعات از کاربران (خدمات گیرندگان) کرده‌اند. تدوین چارچوب قانونی برای داده‌های دولت باز به منظور تنظیم اشتراک داده‌های دولت در قالب‌های باز و قابل خواندن توسط ماشین در چارچوب قانون محافظت از اطلاعات و حریم خصوصی، ضروری است.

• چالش‌های حفاظت و امنیت داده

از جمله مهم‌ترین مباحث در حکمرانی داده، موضوع «امنیت داده» و الزام سازمان‌ها به اجرای الزامات حفاظتی از تمام سامانه‌های فناوری اطلاعات است. بحث امنیت داده با شروع پاندمی کرونا و هک اطلاعات کاربران و مواردی مشابه هک سامانه هوشمند سوخت بیشتر مورد توجه قرار گرفت. در سال ۲۰۲۱ ایران در شاخص جهانی امنیت سایبری (GCI) در بین ۱۸۲ کشور جهان رتبه ۵۴ را به دست آورد. به نظر می‌رسد نوعی تشنگی در سازمان‌های مسئول امنیت سایبری و امنیت داده در کشور وجود دارد. در آبان ۹۶ شورای عالی فضای مجازی، «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی» را تصویب کرد که براساس آن حملات سایبری که در حوزه عمومی به وقوع می‌پیوندد، توسط نیروی انتظامی مورد رسیدگی قرار خواهد گرفت و حوادثی که در سازمان‌ها رخ می‌دهد از طریق وزارت ارتباطات و فناوری اطلاعات رسیدگی خواهد شد. همچنین سازمان پدافند غیرعامل در حوزه نهادها و سامانه‌های حساس، مسئولیت دارد. تعدد بروز اتفاقات مشابه در کشور نشان می‌دهد که پیشگیری و مقابله با تهدیدات سایبری و مدیریت مخاطرات فضای مجازی در داخل کشور دارای ضعف جدی بوده و سند شورای عالی فضای مجازی برای تقسیم وظایف دستگاه‌ها در «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی» ناکارآمد است.

• عدم تحقق اهداف کلان و معماری شبکه ملی اطلاعات:

سند/قانون اهداف کلان و معماری شبکه ملی اطلاعات خط‌مشی کلان برجسته‌ای در زمینه حکمرانی بر داده مقرر داشته که تاکنون سازوکار نهادی و اجرایی تحقق آن‌ها در کشور مشخص نگردیده است؛ به عبارت بهتر، اهدافی از قبیل:

۱. الزام به ذخیره‌سازی، میزبانی و پردازش داده‌های خدمات اثرگذار (موسوم به خدمات پایه‌کاربردی) در داخل کشور به منظور جلوگیری از فراتحلیل ذائقه کاربران ایرانی و در نتیجه داشتن ابزاری مهم در جنگ نرم علیه ملت ایران

۲. ایجاد قطب‌های منطقه‌ای تبادل داده و تجاری‌سازی جریان‌های داده‌ای استراتژیک

۳. یکپارچه‌سازی/درگاه واحد درخواست داده از پلتفرم‌های داخلی در موارد امنیتی همچنان در مرحله نقد و تبادل نظر ماهوی میان نهادهای ذی‌نفع مختلف باقی مانده است.

از سوی دیگر عدم اجرای تکالیف ناشی از ماده ۴۶ برنامه پنجم توسعه مبنی بر تکمیل پایگاه‌های داده‌ها و اطلاعات دستگاه‌های اجرایی و سایر الزامات قانونی منجر به تنوعی از نقص‌های اطلاعاتی شده است که به واسطه این ناهمگونی، زنجیره خدمات دولت با چالش زیرساخت داده‌ای و تعامل‌پذیری روبه‌رو شده است.

• رویکرد سیلویی/سازمانی به حکمرانی داده و جزیره‌ای بودن داده‌ها در دستگاه‌های اجرایی

⁸ linked Open Data

«تبادل داده» بین دستگاه‌ها زمینه‌ساز شکل‌گیری حکمرانی داده است. در شرایط فعلی هر چند «کارگروه تعامل پذیری دولت الکترونیکی» سعی کرده دستگاه‌ها را به سمت تبادل اطلاعات از طریق مرکز ملی تبادل اطلاعات سوق دهد؛ اما بسیاری از دستگاه‌ها به بهانه‌های مختلف از جمله عادت به روال گذشته، دلایل امنیتی، مسائل فنی و فقدان اطلاعات از تبادل داده از طریق این بستر اجتناب کرده‌اند. «جزیره‌ای بودن داده‌ها» و حاکم بودن رویکرد سیلویی، چالش‌های متعددی در زمینه حکمرانی داده ایجاد کرده است.

توصیه‌های سیاستی

- ✓ تصویب قوانین به‌روز، منعطف و مبتنی بر تجربیات بین‌المللی با رویکرد صیانت از حریم خصوصی و استفاده تجاری از کلان داده‌ها در مسیر توسعه اقتصاد ملی و مانع‌زدایی فزاینده از کسب و کارها. ضروری است در تصویب طرح‌های مرتبط با صیانت از داده‌های شخصی و حمایت از حقوق کاربران در فضای مجازی، ملاحظات و رویکردهای ذکر شده مورد توجه قرار گیرد. همچنین، در این راستا اهتمام (اولویت‌بخشی) نسبت به تصویب و اجرایی‌سازی طرح پیشنهادی نمایندگان مجلس شورای اسلامی با عنوان «قانون یکپارچه‌سازی داده‌ها و اطلاعات ملی» از اهمیت بسزایی برخوردار است.
- ✓ انجام همکاری و مشارکت بین دولت و بخش‌های خصوصی، بین کشورهای منطقه و بین تیم‌های ملی دیجیتال به منظور تقویت وزنه راهبردی جمهوری اسلامی ایران در حوزه حکمرانی بر داده؛ به عبارت دیگر، اتخاذ رویکردی جهانی با در نظر چشم انداز نوین تمدنی جمهوری اسلامی ایران و حمایت از ائتلاف‌های راهبردی منطقه‌ای و بین‌المللی ضرورت دارد.
- ✓ جایگزین کردن «حلقه‌های بازار» با نگاه‌های پروژه‌محور و موقت فعلی به بحث حکمرانی داده؛ برای مثال، در حوزه دولت الکترونیک، سکوی مرکز تبادل اطلاعات با چنین منطقی به وجود آمد که بازاری برای فعالان بخش ایجاد کند تا همدیگر را در یک سکو ملاقات، به یکدیگر خدمت‌رسانی و از یکدیگر دریافت خدمت کنند تا در کنار آن درآمدزایی و ایجاد ارزش افزوده بومی بر محوریت داده محقق گردد. ضرورت دارد رویکرد مبتنی بر ایجاد حلقه بازار در تنظیم‌گری حکمرانی داده مورد توجه قرار گیرد.
- ✓ بررسی کنوانسیون‌ها و توافقنامه‌های بین‌المللی در حوزه داده نشان می‌دهد که روند همکاری کشورها در زمینه مسائل مرتبط با داده و امنیت سایبری به سمت «توافقنامه‌های فنی و ابتکار عمل‌های دو یا چندجانبه» در حال افزایش است. اهتمام دستگاه دیپلماسی کشور بر عضویت و جلب حمایت در قالب گروه‌های کارشناسان دولتی (GGE) سازمان ملل متحد و اتخاذ رویکرد فعال به «دیپلماسی سایبری» جمهوری اسلامی ایران نیز در این زمینه قابل توجه است.