

## راهبردها و الزامات دستیابی به تحول تأثیرگذار، ماندگار و پایدار حکمرانی داده‌های ارشد

مهدی عزیزی مهماندوست<sup>۱</sup>، محمد مهدی نژاد نوری<sup>۲</sup>، محسن آقایی<sup>۳</sup>

پذیرش مقاله: ۱۴۰۱/۰۹/۰۵

دریافت مقاله: ۱۴۰۱/۰۵/۲۱

### چکیده

داده‌های ارشد با تحکیم، استانداردسازی و تطبیق عناصر مشترک داده‌ها سبب دستیابی به نمایش پایدارتر سامانه‌ها در سازمان می‌شود. حکمرانی داده‌های ارشد رویکردی سازمان‌یافته به نظارت، پایش و واپایش مدیریت داده‌های ارشد دارد و یکی از مهم‌ترین اهداف کلیدی آن کیفیت مطلوب داده‌ها است. این در حالی است که بروز تغییرات و تحولات در سامانه‌ها و افزایش قدرت فناوری، فشار روزافزونی را به‌منظور اعمال حکمرانی بر داده‌های مربوط به سیاست‌گذاران و ارائه‌دهندگان خدمات تحمیل می‌کند. این پژوهش توصیفی - تحلیلی با شناسایی و طبقه‌بندی نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها به تحلیل راهبردهای (SWOT) الزامات دستیابی به تحول تأثیرگذار، ماندگار و پایدار حکمرانی داده‌ها با استفاده از تجزیه و تحلیل داده‌ها توسط الگوی ترکیبی SWOT-AHP و امتیازدهی هرکدام از آنها و اولویت‌بندی میان شاخص‌ها می‌پردازد. جامعه آماری پژوهش را ۴۲ نفر از خبرگان، مدیران، کارشناسان فناوری اطلاعات حوزه سایبری، فناوری اطلاعات و مدیریت راهبردی تشکیل داده که به‌عنوان نمونه انتخاب شده است. امتیازدهی شاخص‌ها از روش طیف ۹ درجه ساعتی انجام شد. پس از مشخص شدن امتیاز نهایی، تمام شاخص‌های فرصت‌ها، تهدیدها، نقاط قوت و نقاط ضعف به‌صورت زوجی با یکدیگر مقایسه شد. نتایج نشان داد مهم‌ترین زیرمعیار تأثیر وجود توانمندی‌های فنی، مدیریتی و... برای برنامه‌ریزی و سیاستگذاری حکمرانی داده‌های ارشد (S1) با وزن ۰,۲۴۳، بیشتر از دیگر شاخص‌ها است. هم‌چنین نتایج نشان داد که گروه ضعف با وزن ۰,۳۱۴، گروه قوت با وزن ۰,۲۶۴، گروه تهدید با وزن ۰,۲۴۱ و گروه فرصت با وزن ۰,۱۸۱ به‌ترتیب رتبه اول تا چهارم را به خود اختصاص داده است.

**واژگان کلیدی:** حکمرانی، داده ارشد، راهبرد، تحول، حکمرانی پایدار.

۱. دانشجوی دکتری مدیریت راهبردی فضای سایبری - دانشگاه عالی دفاع ملی، تهران، ایران

۲. دانشیار و عضو هیأت علمی دانشگاه عالی دفاع ملی، تهران، ایران

۳. عضو هیأت علمی دانشگاه عالی دفاع ملی، تهران، ایران

## مقدمه

در بیشتر الگوهای مرتبط با فضای سایبر، عرصه محتوا و داده از دیدگاه دانشمندان این عرصه به‌عنوان بخش غیر قابل چشم‌پوشی است. به‌طورکلی داده و اطلاعات از ارکان اصلی سازمان‌ها است و امروزه دولت‌ها برای مدیریت و حکمرانی داده‌ها در ارکان زیرساختی خود به طراحی و تدوین اسناد راهبردی اقدام کرده‌اند. منظور از مدیریت داده، طراحی و اجرای معماری‌ها، سیاست‌ها، اقدامات و رویه‌های لازم برای مدیریت تمامی نیازهای چرخه حیات داده در سازمان است. در رابطه با مبحث حکمرانی داده‌ها موضوعاتی مانند مدیریت دسترس‌پذیری، استفاده، یکپارچگی و امنیت داده‌های سازمان و همچنین تعیین سیاست‌ها، حقوق و مسئولیت‌ها در فرایندهای مرتبط با داده حائز اهمیت است. عصر کنونی، عصر اطلاعات و ارتباطات است؛ زیرا دسترسی مردم به اطلاعات و در نتیجه آگاهی و بصیرت آنها افزایش یافته و امروزه دسترسی عادلانه و قانونمند به داده‌ها یکی از مباحث مهم و مورد توجه حکومت‌های مردم‌سالار است و نیازمند مدیریتی است که دسترسی مردم به اطلاعات عمومی را فراهم و آسان کند و در عین حال اسرار دولتی، حریم خصوصی و اطلاعات خاص را که لازمه حفظ امنیت و انتظام ملی است از دسترسی عموم مردم محافظت کند (عصاریان‌نژاد و همکاران، ۱۳۹۶). از طرفی امنیت سامانه نیز شامل مجموعه‌ای از حفاظت‌های امنیتی مرتبط با نرم‌افزار، سخت‌افزار، کارکنان و سیاست‌های سازمانی است و از سامانه‌های اطلاعاتی در برابر تهدیدهای داخلی و خارجی محافظت می‌کند. در واقع، سرنوشت سازمان به سطوح فناوری اطلاعات و حفاظت اطلاعات آن سازمان وابسته است. حفاظت از داده‌های ارشد در برابر دسترسی‌های ناخواسته و غیرمجاز، حوادث غیرمترقبه و تخریب فیزیکی و غیر آن در برابر هر فرد مزاحم ضروری است. حفاظت پایدار تنها یک نمونه از مواردی است که در حوزه امنیت پایدار مورد نیاز است. تهدیدها امنیتی پایگاه‌های داده در سال‌های اخیر به‌طور چشمگیری افزایش یافته است. این در حالی است که امنیت داده‌ها و رازداری، یکی از نگرانی‌های اساسی است. موارد اشاره‌شده برخی از بخش‌های مرتبط با حکمرانی داده‌های ارشد است که تحقق وجوه مثبت و عدم تحقق وجوه منفی سبب ارتقای مواردی همچون مدیریت دسترس‌پذیری، استفاده، یکپارچگی و امنیت داده‌های سازمان و همچنین تعیین سیاست‌ها، حقوق و مسئولیت‌ها در فرایندهای مرتبط با داده می‌شود. نظر به اینکه دستیابی به این موارد از اهداف عمده در بخش داده‌های ارشد و دغدغه‌های مدیران سایبری و فناوری اطلاعات است و

ازسوی دیگر به دلیل اهمیت زیرساخت داده‌ها به‌عنوان یکی از زیرساخت‌های حیاتی، لازم است راهبردهای اصلی و مهم برای تحقق اهداف مرتبط با حکمرانی داده‌های ارشد مورد تدوین قرار گیرد؛ بنابراین مسئله این پژوهش تدوین راهبردهای تحول تأثیرگذار، ماندگار و پایدار در حکمرانی داده‌های ارشد است. اقدام به این پژوهش از این نظر اهمیت دارد که تصمیم‌سازان و تصمیم‌گیران حوزه سیاست‌گذاری سایبری و فناوری اطلاعات با استفاده از راهبردهایی مدون اقدام به تصمیم‌سازی و درنهایت برنامه‌ریزی عملیاتی برای اقدامات معطوف به اعمال حکمرانی داده‌های ارشد می‌کنند و از این نظر ضرورت برای انجام این پژوهش متصور است که انجام‌دادن آن روندی منفعلانه برای موضوع داده‌های ارشد ایجاد می‌کند و قدرت تصمیم‌گیری افول می‌کند و سبب ایجاد سرگردانی در برنامه‌ریزی‌های عملیاتی و کنترل داده‌های ارشد خواهد شد. به این منظور هدف اصلی این پژوهش تدوین و ارائه راهبردهای مربوط به الزامات تحول تأثیرگذار، ماندگار و پایدار در حکمرانی داده‌های ارشد است که در قالب اهداف فرعی همچون: تعیین نقاط قوت و ضعف، تعیین موارد فرصت و تهدید و تعیین راهبردها و اولویت‌سنجی آنها، اقدام خواهد شد. بر این اساس سؤال اصلی پژوهش این است که راهبردهای تحول تأثیرگذار، ماندگار و پایدار در حکمرانی داده‌های ارشد چیست؟ در این زمینه پژوهشگران به این سؤالات پاسخ می‌دهند:

۱. قوت‌ها و ضعف‌ها در اعمال حکمرانی داده‌های ارشد کدام است؟
۲. فرصت‌ها و تهدیدها در اعمال حکمرانی داده‌های ارشد کدام است؟
۳. راهبردهای تحول تأثیرگذار، ماندگار و پایدار در حکمرانی داده‌های ارشد کدام است؟

## مبانی نظری

### داده‌ها

ظرفیت فنی بشر برای اندازه‌گیری طیف وسیعی از رخدادها و فعالیت‌ها و هم‌چنین جمع‌آوری، ذخیره‌سازی و تحلیل نسخه‌های الکترونیکی چیزهایی که هیچ‌کدام قبلاً به‌عنوان داده در نظر گرفته نمی‌شد (ویدئوها، تصاویر، ضبط‌های صوتی، اسناد) توسعه یافته است و این توانایی به مرحله سنتز داده‌ها به‌صورت اطلاعاتی قابل استفاده وارد شده است. بهره‌برداری از گوناگونی داده‌ها بدون غرق‌شدن در حجم و سرعت زیاد آنها نیازمند اقدامات عملی قابل اعتماد و قابل گسترش در مدیریت داده‌ها است (Brian Lee, 2016 و Chalabi Mona, 2017).

### داده‌های ارشد

داده‌های ارشد داده‌های کلیدی و حیاتی است که برای عملکرد سازمان ضروری است. این داده‌ها نشانگر سامانه‌های داده‌ای کلیدی و اشیای کسب‌وکاری است و به دلیل چگونگی به‌اشتراک‌گذاری و تعاملات داده‌ها، به عملیات درون سازمان و فنون تحلیل در آن حساس بوده و بر اساس آنها زمینه تراکنش‌های داده‌ها را فراهم می‌کند. داده‌های ارشد به‌طور طبیعی خود غیر تراکنشی است و معمولاً برای سازمان در دامنه‌های داده‌ای شناسایی و سازماندهی می‌شود که سامانه‌های کلیدی کسب‌وکار مانند مشتریان، شریکان، مواد، دارایی و کارکنان از آن استخراج می‌شوند. به بیان دیگر، داده‌های ارشد به اجزای داده‌های سازمان اطلاق می‌شود که شامل ارزشمندترین داده‌ها در این نهاد است و به اشتراک گذاشته می‌شود. این داده‌ها می‌تواند داده‌های مرجع ایستا، تراکنشی، غیر ساخت‌یافته، تحلیلی، سلسله‌مراتبی و یا فراداده‌ها باشد. سازمان می‌تواند از داده‌های ارشد در نرم‌افزارها یا سکوه‌های نرم‌افزاری گوناگون استفاده کند. انواع داده‌هایی که تحت عنوان داده‌های ارشد در سازمان در نظر گرفته می‌شود از یک سازمان و شرکت تا سازمان و شرکت دیگر و یا حتی بخش درون یک سازمان تا بخش دیگر در همان سازمان متفاوت خواهد بود. داده‌های ارشد روال به‌اشتراک‌گذاری داده‌ها را ساده‌تر می‌کند. این ساده‌سازی به کاهش هزینه و خطرپذیری در محیط‌های پیچیده منجر خواهد شد. درحالی‌که تمرکز نوآفرینی‌های سازمانی داده‌محور بر داده‌های تراکنشی (افزایش فروش یا سهم بازار، کاهش هزینه‌ها، نشان‌دادن انطباق) است؛ اما امکان استفاده از این نوع داده‌ها به‌شدت به دسترسی و کیفیت داده‌های مرجع و ارشد وابسته است. بهبودی در دسترس‌پذیری و کیفیت داده‌های مرجع و ارشد تأثیر قابل توجهی بر کیفیت کلی و همچنین محرمانگی کسب‌وکار در داده‌ها دارد. این فرایندها برای سازمان مزایای دیگری نیز به‌دنبال دارد؛ از جمله ساده‌سازی چشم‌انداز فناوری اطلاعات، کارایی و باروری بهبودیافته و به‌همراه این موارد، ظرفیت بهبوددادن به تجربه‌ای که مشتری کسب می‌کند (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱).



شکل ۱: وضعیت داده‌های ارشد در مقایسه با انواع دیگر داده‌ها (MDM, 2014)

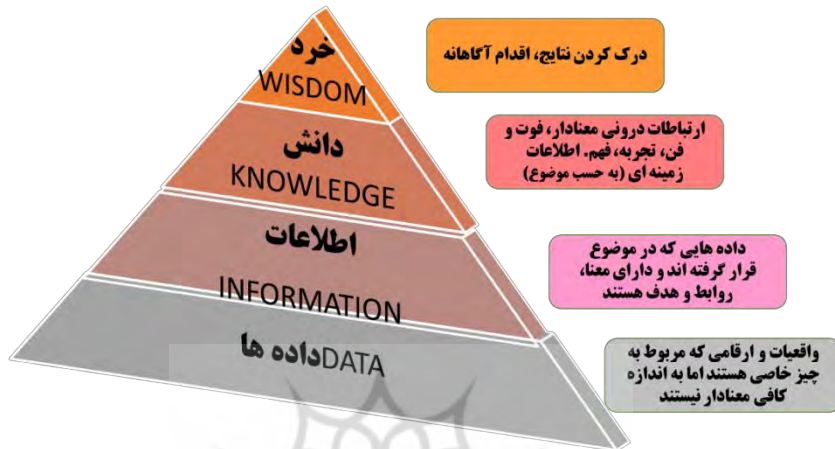
### چالش داده‌ها

چالش زیادی در داده‌های بزرگ در زمینه حفاظت از داده‌ها، جمع‌آوری و به اشتراک‌گذاری اطلاعات و استفاده از داده‌ها وجود دارد (Kerremans, 2016). از آنجا که داده‌های بزرگ حاوی اطلاعات خصوصی افراد و تاریخچه آنها است، محافظت از پایگاه داده در ارتباط با هک شدن، سرقت اینترنتی و فیشینگ اهمیت دارد. جایی که اطلاعات داده‌های سرقت شده می‌تواند با مبالغ زیادی فروخته شود (وبگاه آموزشی هاروارد و هلث لاین). به جز داده‌های پزشکی و سلامت و اطلاعات شخصی در سامانه‌های بهداشتی که می‌تواند هک یا ربوده شود، داده‌های بزرگ دیگری نیز در سازمان‌های تجاری مانند شرکت‌های مخابراتی، بانک‌ها و مؤسسات مالی نیز بدون آگاهی از مشتریان آسیب‌پذیر است. قبل از اینکه داده‌های بزرگ بتواند اجرا شود، لازم است اطمینان حاصل شود که مدیریت، حریم خصوصی و امنیت داده‌های بزرگ به خوبی محافظت می‌شود. حفاظت از اطلاعات بهداشتی از راه انتقال امنیت، احراز هویت چندلایه، استفاده از نرم‌افزار ضد ویروس، فایروال، رمزگذاری داده‌ها در واقع حیاتی است (Kruse, et.al, 2017).

### داده‌ها و اطلاعات

مطالب زیادی در مورد ارتباط بین داده‌ها و اطلاعات عنوان شده است. داده‌ها، «مواد خام اطلاعات» نامیده می‌شود، اطلاعات نیز «داده‌ها در بستر موضوع» است. این دو مفهوم گاهی با یکدیگر اشتباه گرفته می‌شود و به جای هم مورد استفاده قرار می‌گیرد؛ اما تفاوت ظریف و باریکی بین آنها هست؛ بنابراین مهم است که به هر کدام از این دو مفهوم به عنوان یک سامانه جدا نگریسته شود و رابطه آنها با هم و تفاوت آنها از یکدیگر درک شود. تعاریف بسیاری از داده‌ها در

واژه‌نامه‌ها، مقاله‌ها و کتاب‌ها آمده است که به‌طور مبنایی، داده‌ها را «نهادی از واقعیت با آیتمی از اطلاعات» معرفی می‌کند. بر اساس تعریف DAMA<sup>۱</sup>، داده‌ها عبارت است از «نمایش یک واقعیت به‌صورت متن، عدد، نمودار، تصویر، صدا یا ویدئو» (M. O. Enofe, 2017).



شکل ۲. هرم لایه‌ای یا الگوی DIKW (M. O. Enofe, 2017)

### الزامات مدیریت داده‌ها

مدیریت داده‌ها به‌معنای مدیریت کیفیت داده‌ها است: دستیابی به اطمینان از اینکه داده‌ها با اهداف همگون است، هدف اصلی مدیریت داده‌ها است. سازمان‌ها برای مدیریت کیفیت باید مطمئن شوند الزامات کیفی ذی‌نفعان را درک کرده‌اند و داده‌ها را براساس این الزامات بسنجند:

- انواع گوناگون داده‌ها، مشخصه‌های چرخه حیات متفاوتی دارد: به همین دلیل، الزامات مدیریتی متفاوتی دارد. شیوه‌های مدیریت داده‌ها باید این تفاوت‌ها را شناخته و به حد کافی منعطف باشد تا انواع گوناگون ملزومات چرخه حیات داده‌ها را برآورده سازد.
- مدیریت داده‌ها دربردارنده مدیریت ریسک‌های مرتبط با داده‌ها است: داده‌ها علاوه بر اینکه دارای است، برای سازمان خطرپذیری نیز به‌همراه می‌آورد. داده‌ها ممکن است گم شود، دزدیده شود یا از آنها سوء استفاده شود. سازمان‌ها باید التزام‌های اخلاقی به‌کارگیری از داده‌ها را مدنظر قرار دهند. ریسک‌های مرتبط با داده‌ها باید به‌عنوان بخشی از چرخه حیات داده‌ها مدیریت شود.

- ملزومات مدیریت داده‌ها باید تصمیمات فناوری اطلاعات را جهت‌دهی کند: داده‌ها و مدیریت داده‌ها به‌طور عمیق با فناوری اطلاعات و مدیریت فناوری اطلاعات درهم تنیده است. مدیریت داده‌ها نیازمند روشی برای دستیابی به این اطمینان است که فناوری به‌جای پیش‌راندن نیازهای راهبردی داده‌ای سازمان، در خدمت آن قرار گرفته است (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱).

#### تهدیدهای سایبری داده‌ها

امروزه تهدیدهای متنوع و در حال گسترشی داده‌های گوناگون در سطح جهان را تهدید می‌کند. به‌عنوان مثال یکی از شایع‌ترین حملات اخیر که مراکز داده را تحت تأثیر خود قرارداد، باج‌افزار و اناکرای بود. در نگاه اول به‌نظر می‌رسید که حملات رمزنگاری شده است و شرکت‌های مختلف را تحت تأثیر قرار داده است. برای اولین بار و اناکرای در تاریخ ۱۲ ماه می ۲۰۱۷ راه‌اندازی شد. در اولین حمله این تروجان بیش از ۲۰۰,۰۰۰ رایانه قربانی شد (Wakaskar, 2017).

#### حکمرانی داده‌ها

حکمرانی داده‌ها بخشی از یک نظام کامل‌تر است که به‌شکلی سنتی، مدیریت اطلاعات نهاد کسب‌وکاری نامیده می‌شود. در واقع، خاستگاه اصلی ابهامات موجود در مفهوم حکمرانی داده‌ها از دیدگاه‌های نسبتاً متفاوتی نشأت می‌گیرد که به‌چگونگی ارتباط آن با مدیریت اطلاعات مربوط می‌شود (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱). برای دستیابی به هدف کلی از ایجاد حکمرانی داده‌ها، لازم است برنامه حکمرانی داده‌ها سه ویژگی پایدار، جاسازی شده و سنجش‌پذیر داشته باشد (DAMA-DMBOK, 2017). هم‌چنین حکمرانی داده‌ها، سازماندهی و اجرای سیاست‌ها، روش‌ها، ساختارها، نقش‌ها و مسئولیت‌هایی است که قواعد مربوط، حقوق تصمیم‌گیری و مسئولیت‌ها را برای مدیریت مؤثر دارایی‌های اطلاعاتی ترسیم و اجرا می‌کند (DAMA-DMBOK, 2017).

#### ضرورت‌های حکمرانی داده‌ها

مؤسسه حکمرانی داده‌ها (DGI) چهار ضرورت ایجاد نظم حاکم بر داده‌های رسمی توسط سازمان‌ها را چنین معرفی می‌کند:

۱. وسعت سازمان به‌اندازه‌ای است که مدیریت سنتی توان پاسخگویی به فعالیت‌های متقابل کاربردی مربوط به داده‌ها را ندارد.
۲. سامانه‌های اطلاعات، سازمانی بسیار پیچیده‌ای دارد، به‌گونه‌ای که مدیریت سنتی قادر به پاسخگویی به فعالیت‌های متقابل کاربردی مرتبط با داده‌ها نیست.

۳. معماری داده‌های سازمان و هم‌چنین گروه‌های معماری سرویس‌گرا نیازمند پشتیبانی توسط یک برنامه عملیاتی متقابل است که به‌جای دیدگاه محدودیت‌های سازمانی، چالش‌ها و مسائل مرتبط به داده‌ها را در برگیرد.

۴. تدوین مقررات، توافقات و یا الزامات قراردادی در راستای کنترل و نظارت رسمی داده‌ها است (Fleissner, et.al, 2014).

### وظایف و الگوی حکمرانی داده‌ها

واژه بنیادی در حکمرانی، حکمرانیدن است. حکمرانی داده‌ها را می‌توان از حکمرانی سیاسی استنباط کرد. این اصطلاح شامل وظایفی مشابه امور مقننه (تعریف سیاست‌ها، استانداردها و معماری داده‌های سازمان) و وظایفی مشابه امور قضایی (مدیریت مشکلات و ارجاع به مقام بالا) و وظایف اجرایی (حفاظت و خدمت‌رسانی، مسئولیت‌های مدیریتی) است. برای مدیریت بهتر خطر، بیشتر سازمان‌ها روش مبتنی بر نماینده را برای حکمرانی داده‌ها استفاده می‌کنند تا صدای تمام ذی‌نفعان شنیده شود. هر سازمان باید الگویی برای حکمرانی داده‌ها را اختیار کند که راه‌برد کسب‌وکار از آن پشتیبانی کرده و از دید فرهنگ سازمانی، برای افراد سازمان قابل فهم باشد. سازمان‌ها هم‌چنین باید برای ارتقای آن الگو به‌منظور رفع چالش‌های جدید آماده باشند. الگوها از نظر ساختار سازمانی، سطح رسمیت و روش تصمیم‌گیری با یکدیگر تفاوت دارد. برخی الگوها، سازمانی متمرکز دارد، درحالی‌که برخی دیگر توزیع‌یافته عمل می‌کند ( DAMA-DMBOK, 2017).



شکل ۳. نمایش «هفت‌گون» در جداسازی وظایف حکمرانی داده‌ها و مدیریت داده‌ها (J. Ladley, 2012)

### اقدامات حکمرانی داده‌ها

حکمرانی داده‌ها، مؤلفه‌ها و ابعاد گوناگونی به‌عنوان مدیریت داده‌های قوی و گسترده دارد. حکمرانی داده‌ها برای بسیاری از سازمان‌ها جدید است و لازم نیست تمام اجزای خط‌مشی را



برای شروع برنامه حاکمیتی مفید فراهم کند. به‌طور معمول در شروع این اقدام، سازمان‌ها ارزش زیادی را فقط با سازماندهی، آگاهی، نظارت و کیفیت داده‌ها و امکان درخشان احساس مدیریت چرخه اطلاعات برای جلوگیری از گسترش مجموعه اطلاعات رهاشده به‌دست می‌آورند (Fleissner, et al., 2014).

#### دسته‌بندی حکمرانی داده‌ها

در حکمرانی و مدیریت داده‌های دنیای واقعی، اشکال گوناگونی از چهار دسته‌بندی به چشم می‌خورد که در برخی منابع جداسازی‌های ریزتری از آنها همراه با ادغام تعدادی در یکی از چهار دسته دیگر، نشان داده شده است. با این حال، همه آنها به این چهار دسته کلی اشاره می‌کنند:

۱. داده‌های ارشد

۲. داده‌های تراکنشی

۳. داده‌های مرجع

۴. فراداده‌ها (Allen and D. Cervo, 2015)

#### مدیریت طبقه‌بندی حکمرانی داده‌ها

طبقه‌بندی تمام منابع و محتواها در کمترین زمان ممکن، از لحظه‌ای که توسط مالک آنها وارد می‌شود، تا هنگامی که مدیریت چرخه حیات اطلاعات، واپایش<sup>۱</sup> دسترسی و انطباق با مقررات را پشتیبانی کند، برای کسب‌وکار/ مباشر<sup>۲</sup> کاری حساس است. سطوح ممکن برای طبقه‌بندی از این قرار است:

- دولتی در برابر خصوصی
- دوره زمان‌بندی ماندگاری
- سطح امنیت
- واپایش‌های تنظیم‌گری قابل اعمال (PII،<sup>۳</sup> PCI) و محتوای غیر قانونی
- آزمون غیر مخرب برای برآورد/ طبقه‌بندی داده‌های مستقر، یا برآورد/ اجرا روی داده‌های

جاری

- 
1. Control
  2. Steward
  3. Personally Identifiable Information
  4. Payment Card Industry

- در صورت نبود وجود هرگونه واپاشی بر جریان ورودی، لازم است برای پیش و طبقه‌بندی هر آنچه از ناحیه مرزی عبور می‌کند، مؤلفه‌هایی در نظر گرفته شود. این کار برای کنارزدن هر داده‌ای که معیارهای قابل قبول را برآورده نمی‌کند، لازم است (حسین‌پور و همکاران، ۱۳۹۷).

#### **دسترسی به محتوا در حکمرانی داده‌ها**

از دیگر حیطه‌های مدیریت داده‌ها می‌توان به مدیریت دسترسی داده‌ها اشاره کرد. بخشی از این کار در مدیریت محتوا تعریف می‌شود که شامل برچسب‌گذاری روی داده‌های کلیدی اسناد و محتوا است. سازوکار این برچسب‌گذاری باید روی معماری محتوا تعریف شود. این سازوکار در موتورهای جستجو سبب آسان‌شدن دریافت محتوای مورد نظر خواهد شد، به‌ویژه محتوایی که از جنس داده‌های ساختارنایافته است (DAMA-DMBOK, 2017).

#### **امنیت و حریم خصوصی در حکمرانی داده‌ها**

ترکیب منابع داده‌ای نیز می‌تواند سبب افشای ناخواسته شود، مانند ترکیب نشانی‌های (IP) با اطلاعات جمعیتی یا در پژوهش پزشکی جایی که شناسه فرد به‌طور اتفاقی آشکار و سبب افشای علت بیماری می‌شود. از جنبه رقابتی، سازمان‌هایی که از داده‌های حساس محافظت می‌کنند و با افشاندن و انتخاب‌های گزیده، از حریم خصوصی مشتریان خود محافظت می‌کنند، جایگاه برتری در بازار می‌یابند (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱).

داده‌های ماشینی نیز یکی از عوامل دغدغه‌ساز در شرایطی است که اطلاعاتی را در مورد رفتار و عادات افراد فاش می‌کند. به‌طور مثال، داده‌های سنجش‌گر الکتریکی هوش می‌تواند الگوهای فعالیت خانگی را نشان دهد. در اینجا نیز، سیاست و قانون همگام با حقوق حریم خصوصی افراد وضع نشده است. با توجه به پنهان‌کاری و نیرنگ‌آفرینی‌ها، امنیت تبدیل به چالشی روزافزون شده است. موقعیت مکانی و به‌ویژه افزاره‌های GPS می‌تواند مکان افرادی را نشان دهد که در خطر جنایات خشن از قبیل خشونت‌های محلی یا اهداف بالقوه تروریستی هستند. تفکر روبه‌رشد این است که حکمرانی داده‌ها دیدگاه کلیدی برای مدیریت و به‌دست‌آوردن ارزش از داده‌ها است. پیش‌بینی مؤسسه گارتنر تا سال ۲۰۱۸ میلادی، حاکی است که ۲۵٪ سازمان‌های پیشرو، مدیریت تمام داده‌های ساختارنایافته خود را با استفاده از حکمرانی داده‌ها انجام خواهند داد. این رقم در سال ۲۰۱۳ میلادی فقط ۱٪ بوده است (C. Balard, C. Compert, 2014).

#### **حفاظت از اطلاعات در حکمرانی داده‌ها**

در توانایی حفظ اعتماد مشتریان، نگهداری از کیفیت داده‌ها و دسترسی کاری اساسی است.

- در حفاظت اطلاعات نباید به دلایلی همچون سودجویی، بی‌فکری و یا خطوط قرمز سهل‌انگاری شود. در صورت بروز شرایط هشدار، در مورد استثنائات باید گروه مناسبی از مدیریت تصمیم‌گیری کند و مراتب کار مکتوب شود.

- به‌عنوان واقعیت، باید سختی پیش‌بینی را پذیرفت در اینکه ریسک‌های جدید چگونه ممکن است خود را نشان دهد.

- نه فقط آنچه پیش روی مشتری قرار داده می‌شود، بلکه هر آنچه مشتری به آن ارجاع داده می‌شود و آنچه که سازمان برای مشتری نتیجه‌گیری می‌کند، همگی باید محافظت شود. مشتریان برای هرگونه شکستی در حفاظت آنها از پیوندهای بداندیش<sup>۱</sup>، سازمان را مقصر می‌دانند (حسین‌پور و همکاران، ۱۳۹۷).

#### مدیریت داده‌های حساس در حکمرانی داده‌ها

از لحاظ قانونی، سازمان‌ها ملزم به محافظت از حریم خصوصی هستند. این کار با شناسایی و حفاظت از اطلاعات حساس انجام می‌شود. امنیت و یا حکمرانی داده‌ها معمولاً تمهیدات مربوط به محرمانگی را برپا می‌دارد و دارایی‌های محرمانه یا با دسترسی محدود را شناسایی می‌کند. افرادی که به تولید یا سرهم‌بندی محتوا اقدام می‌کنند، باید این طبقه‌بندی را اعمال کنند. به‌عبارت دیگر، اسناد، صفحات وب و دیگر اجزای محتوا باید بر اساس سیاست‌ها و الزامات قانونی تعیین شود و مهر حساس بودن داشته باشد. پس از جداسازی داده‌های حساس، سازوکارهای لازم برای حفظ امنیت و حریم خصوصی در آنها به اجرا در می‌آید (DAMA-DMBOK, 2017).

#### مؤلفه‌های حکمرانی داده‌ها

مؤلفه‌های حکمرانی داده‌ها عبارت است از تمام عناصر لازم اعم از راهبردها، سیاست‌ها، استانداردها، ابزارها، پیش‌شرط‌ها، قوانین، حضور عوامل انسانی، نقشه راه و هر عامل دیگری که اجرای یک برنامه حکمرانی داده‌ها فقط با در کنار یکدیگر قراردادن همه آنها با هم امکان‌پذیر می‌شود (C. Ballard, C. Compert, 2014).

#### حکمرانی داده‌ها در سطح ملی

اهمیت موضوع حکمرانی داده‌ها به‌اندازه‌ای است که چالش ملی به‌شمار می‌رود. گرچه روند پژوهش‌ها بیشتر به‌سمت تدوین و اجرای این برنامه در سطح سازمانی و به‌طور معمول نهادهای کسب‌وکاری است، اما انجمن‌های علمی از نگاه ملی به این موضوع نیز غافل نیستند.

با وجود تمرکز بر ابعاد سازمانی این موضوع، پرداختن به آن در سطح ملی می‌تواند پایه‌ریز بسیج ملی در حوزه‌های گوناگون کسب‌وکار و فناوری اطلاعات کشور برای اهمیت دادن به مسئله حکمرانی داده‌ها در سطح مؤسسه، صنف، سازمان و یا نهاد کسب‌وکاری خود شود. آکادمی بریتانیا و انجمن پادشاهی کشور انگلیس در این زمینه ملاحظاتی دارد که محوری‌ترین آنها چهار اصل عملی و یک اصل راهبردی پنجم به‌عنوان اصل حاکم بر حکمرانی داده‌ها است. مبنای آن نمایی از جامعه نمونه قرن ۲۱ را برای خود ترسیم کرده که با تکیه بر داده‌های خود تبدیل به جامعه‌ای توانمند می‌شود.

۱. از حقوق و سلاقی فردی و جمعی حفاظت کند.

۲. اطمینان دهد که تمام آزمون و خطاهای متأثر از مدیریت و به‌کارگیری داده‌ها به‌صورت شفاف، پاسخگو و شمول‌پذیر باشد.

۳. طالب تجارب خوب باشد و از شکست و موفقیت درس بگیرد.

۴. با حفظ حقوق افراد جامعه، به توسعه فضای آزاد غنا ببخشد.

اصل پنجم که بر دیگر اصول حکمرانی داده‌ها غالب است، عبارت است: «سامانه‌های حکمرانی داده‌ها، باید سبب ارتقای پیشرفت بشر شود». اصولی که ازسوی آن انجمن معرفی شده است وارد جزئیات عملی کار نمی‌شود و بیشتر نقش هدایتگری، واپایش و نشانه‌هایی را بازی می‌کند که می‌تواند برای به‌کارگیری در بخش‌ها و کاربردهای گوناگون، کمابیش تغییر شکل داده شود. این اصول باید تمام ابزار و الگوهای حکمرانی مختص به هر زمینه یا بخش را که در قلمروهای گوناگون عملی - خواه به شکل نشانه‌هایی از علوم اخلاق، فنی، استانداردهای عملیاتی یا مقننه و یا راهکارهای فناورانه‌ای همچون شخصی‌سازی حریم خصوصی - به‌کار می‌رود، پشتیبانی کند (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱).

### سیاست حکمرانی داده‌ها

در بخش مفاهیم، از تعریف و مفهوم سیاست گفته شد. این واژه خود به‌تنهایی مؤلفه حکمرانی داده‌ها به‌شمار می‌آید. سیاست‌ها در واقع فرایندهای تعریف‌شده‌ای است که از پشتوانه محکمی برخوردار است. به بیان روشن، سیاست‌ها روش تدوین اصول است و استانداردها را در بر می‌گیرد؛ حوزه‌ای که کارکنان فناوری اطلاعات هنگام تحقق‌یافتن حکمرانی داده‌ها حساسیت زیادی به آن نشان می‌دهد. می‌توان گفت، به‌احتمال بسیار زیاد، بیشتر سیاست‌های ممکن به‌شکلی ازهم‌گسیخته در فناوری اطلاعات، داده‌ها یا انطباق با قوانین و مقررات حضور دارد. به‌عبارت

دیگر، سیاست بدون اینکه مورد توجه قرار گیرد، مانند بسیاری از موقعیت‌های دیگر راحت در کتابچه‌های یادداشت خاک می‌خورد و زندگی جریان عادی خود را طی می‌کند. با پیوند سیاست‌ها و اصول به یکدیگر، می‌توان در برنامه حکمرانی داده‌ها از این اتفاق جلوگیری کرد. سیاست حکمرانی داده‌ها حول محور تنظیم و اجرای سیاست‌های مرتبط با مدیریت داده‌ها، فراداده‌ها، دسترسی، امنیت و کیفیت دور می‌زند (DAMA-DMBOK, 2017).

### **راهبرد حکمرانی داده‌ها**

تعیین خط‌مشی‌ها و راهبردها در حکمرانی داده‌ها، به نیازهای سازمانی بستگی دارد، اما ویژگی‌های آن در بیشتر سازمان‌ها از وجوه اشتراک زیادی با یکدیگر برخوردار است. تعریف، اطلاع‌رسانی و پیش‌بردن اجرای راهبردهای داده‌ها و راهبردهای حکمرانی داده‌ها از زمره این وجوه مشترک است. راهبردها؛ مجموعه‌ای از گزینه‌ها و تصمیماتی است که در کنار یکدیگر برای انجام عملی، یک نمودار از دید بالا برای آن ترسیم می‌کند. حال اگر راهبرد در سطح یک برنامه باشد، عبارت از یک دوره عملیات سطح بالا است که به منظور دستیابی به اهداف سطح بالا صورت می‌پذیرد (DAMA-DMBOK, 2017).

### **مزیت راهبردی حکمرانی داده‌ها**

مزیت راهبردی و اصلی حکمرانی داده‌ها این است که داده‌ها را می‌توان به روشی بسیار مؤثر و قابل اطمینان، پیدا، تبیین و مدیریت کرد. پیشران‌های کسب‌وکاری بیشتری نیز هست که عبارت است از بهبود انعطاف‌پذیری سازمان، چابکی کسب‌وکار و کاهش خطرپذیری کسب‌وکار. با حکمرانی داده‌ها، راهبرد کسب‌وکار بسیار متمرکز و ترویج استفاده راهبردی از فناوری اطلاعات نیز امکان‌پذیر است. به‌علاوه، سبب رشد داده‌ها با نرخ مشخص می‌شود که مزیت‌های فراوانی برای سازمان دارد.

علاوه بر این موارد، حکمرانی داده‌ها سبب بهبود کارایی کلی سازمان، افزایش درآمد و سهم بازار، افزایش درک سازمانی در مورد اقدامات اطلاعاتی قابل انجام با داده‌های موجود، اعتماد عمومی به محصولات اطلاعاتی و پذیرش هزینه‌های مالی طرح‌های مدیریت اطلاعات می‌شود (Christian Bruck, 2017).

### **تعیین نقشه راه حکمرانی داده‌ها**

از آنجا که اجرای موفق برنامه حکمرانی داده‌ها، مستلزم رعایت قواعد نقشه راه است؛ به همین دلیل چند فعالیت در تعیین نقشه راه ضرورت دارد:

۱. یکپارچه‌سازی حکمرانی داده‌ها با دیگر کارها
۲. طراحی سنجه‌های حکمرانی داده‌ها و گزارش‌دهی ملزومات
۳. تعریف ملزومات پایداری
۴. طراحی برنامه مدیریت تغییر
۵. تعریف اجرای عملیات حکمرانی داده‌ها (Anthony Chalker, 2014)

#### داده‌های ارشد و حکمرانی داده‌ها

از آنجا که داده‌های ارشد و مرجع از نوع داده‌های اشتراکی در سازمان است، حکمرانی و نظارت بر این نوع داده‌ها لازم و ضروری است. در حوزه داده‌های ارشد و مرجع، فرایند حکمرانی داده‌ها شامل تصمیم‌گرفتن دربارهٔ موارد زیر است:

- یکپارچه‌سازی منابع داده
- اجرای قوانین کیفیت داده‌ها
- شرایط اجرای قوانین
- فعالیت پایش داده‌ها و زمان این پایش
- اولویت و سطح پاسخگویی فعالیت‌های مباحثی داده
- چگونگی ارائه داده‌ها به‌منظور برآورده شدن نیاز ذی‌نفعان
- ارائه چارچوب کلی و انتظارات برای توسعه مدیریت اسناد و محتوا (ISO Standards)

#### تحول حکمرانی داده‌ها

هر سازمان می‌تواند در راستای برنامه حکمرانی داده‌ها بنا به صلاح‌دید، در رفتار سازمانی، فرهنگ و حتی اصول سازمانی خود تغییراتی ایجاد کند، اما خودداری از اصول ملی حکمرانی داده‌ها به‌سادگی مدیریت در داخل سازمان نیست و جرایم قانونی به‌همراه دارد. ازسویی، تأثیرگذاری سازمان‌ها در اصلاح قوانین و اصول ملی مربوط، از روش ساده و مستقیمی برخوردار نیست و نیازمند حمایت و توجه دولت به پیشنهادهایی است که ازسوی نهادهای کسب‌وکاری و فناوری اطلاعات ارائه می‌شود (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱). اصول بنیادین با ارائه مبنایی برای تصمیم‌گیری‌ها به گروه راهبری و راهی برای اطلاع‌رسانی مقاصدشان به بخش‌های پایین‌تر سازمان، به آنها کمک می‌کند. با درک مناسب از این اصول، تصمیمات مورد نیاز در طول دوره‌های با بهره‌وری زیاد، احتمالاً در راستای مقاصد کمیته حکمرانی داده‌های سازمان باقی می‌ماند (C. Balard, C. Compert, 2014).

### تحول در برابر تکامل حکمرانی داده‌ها

اجرای حکمرانی داده‌ها کاری است که ضمن اجرای دقیق و مطابق با طراحی، نیاز به بارها تکرار دارد. دانستن اینکه حکمرانی چگونه انجام شود، یک ویژگی فطری نیست و نیاز به یادگیری دارد. همه سازمان‌ها حاضر نیستند از سیر طولانی انتقال در برنامه حکمرانی داده‌ها استقبال کنند. این کار نیازمند حجم فعالیت زیادی از استانداردسازی و قانونمندکردن پایگاه‌های مدیریت داده‌ها است. فقط سازمان‌هایی حاضر به تحمل این شرایط می‌شوند که در حرفه کسب‌وکاری خود بسیار مأیوس شده‌اند و سرسختانه در برابر قبول شکست، از خود پایداری و مقاومت نشان می‌دهند. در این حالت، سازمان برای حفظ بقا و احیای ارزش‌افزایی خود از راهکارهای پیشنهادی مانند حکمرانی داده‌ها نیز استقبال می‌کند، هرچند سخت باشد.

نگاه منطقی به حرکت در راستای اجرای حکمرانی داده‌ها این تلقی را سبب شده که هنوز اطمینانی از چگونگی انجام آن به‌وجود نیامده است. یادگیری چگونگی انجام حکمرانی داده‌ها، نیازمند به تکامل رسیدن آن در طول یک فرایند است. چهار مرحله جداگانه برای یادگیری هست که برای سازمان‌ها (همچون افراد) به‌کار گرفته می‌شود:

۱. عادت: تکرار، اما نه ادراک و فهم - سازمان می‌تواند تعاریف مفاهیم حکمرانی داده‌ها را بیان کند.

۲. فهم: سازمان می‌تواند طبیعت و اهمیت حکمرانی داده‌ها را درک کند (تعداد زیادی از برنامه‌های حکمرانی داده‌ها در این مرحله متوقف می‌شود).

۳. کاربرد: سازمان به‌اندازه کافی می‌داند که شروع به اعمال مفاهیم حکمرانی داده‌ها کند، اما فقط در پاسخ مستقیم به یک عامل پیشران (به‌طور مثال، اگر کیفیت داده‌ها ضعیف باشد ممکن است شروع به حکمرانی بر کیفیت داده‌ها متقاعدکننده باشد).

۴. همبستگی: سازمان می‌تواند مفاهیم را خلاقانه و برای موقعیت‌های پیچیده‌تر اعمال کند (به‌طور مثال، به تغییر و بازسازی حکمرانی به‌گونه‌ای پردازد که برای برنامه‌ریزی منابع یک نهاد کسب‌وکاری یا مدیریت داده‌های ارشد در آن که از ابتدا بد پیش رفته است، مناسب باشد). (الیاسی و همکاران، ۱۳۹۹: ۲۶۴ - ۱).

### ویژگی پایدار بودن در حکمرانی داده‌ها

برنامه حکمرانی داده‌ها یک طرح نیست که پایان داشته باشد. فرایندی پیوسته و در حال انجام است که نیازمند تعهد سازمانی است. حکمرانی داده‌ها نیازمند ایجاد تغییرات در چگونگی مدیریت

و استفاده از داده‌ها است. این مطلب همیشه به معنای تحول شگرف سازمانی نیست؛ بلکه منظور مدیریت تغییر به شکلی است که ورای اجرای اولیه هر عنصر از حکمرانی داده‌ها، پایدار بماند. حکمرانی داده‌های پایدار به هدایت کسب‌وکار، حمایت مالی و مالکیت بستگی دارد (DAMA-DMBOK, 2017).

### الزامات پایداری حکمرانی داده‌ها

اولین گام برای مدیریت تغییراتی که باید رخ دهند، برنامه‌ریزی برای آن است. اگر سازمان درصدد اجرای موفق برنامه حکمرانی داده‌ها باشد، لازم است مؤلفه‌های فرهنگی بسیاری را مورد توجه قرار بدهد. این فعالیت، مؤلفه‌ها و چگونگی هماهنگی آنها را تعیین می‌کند. گروه حکمرانی داده‌ها، ارزیابی ظرفیت تغییر، تحلیل ذی‌نفعان و یافته‌های دیگری را بررسی می‌کند که طی فعالیت پیشین به قصد توسعه الزامات برای اطمینان از پایداری برنامه حکمرانی داده‌ها جمع‌آوری شده است. اولین حرکت طبیعی به‌طور تقریب اجرای هر چیزی است، بدون آنکه در نظر گرفته شود طی یکی دو سال آینده در طول مسیر چه اتفاقی خواهد افتاد. علاوه بر آموزش و ارتباط‌گرفتن با افراد که امری بدیهی است، به اندازه‌گیری پیوسته میزان و مقدار تغییر و هم‌چنین رفتار و روحیه گروه حکمرانی داده‌ها و ذی‌نفعان نیز نیاز است. تلاش برای تغییر نیازمند حمایت درازمدت است؛ لذا گروه حکمرانی داده‌ها به‌دنبال فردی به‌عنوان حامی این تغییرات خواهد بود (Anthony Chalker, 2014).

یکی از اهداف مهم برنامه حکمرانی داده‌ها، حفاظت از الزامات ذی‌نفعان داده‌ها (اشخاص یا گروه‌هایی که بر داده‌ها تأثیر می‌گذارند و یا از آنها تأثیر می‌پذیرند) است. این اشخاص یا گروه‌ها شامل ایجادکنندگان داده، کاربران داده و کسانی می‌شوند که قواعد و الزامات داده را وضع می‌کنند. حفظ حریم خصوصی، محرمانگی و یکپارچگی داده‌های شخصی شهروندان از راه انطباق با GDPR محقق می‌شود. (GDPR به‌عنوان یک قانون در استفاده از داده‌ها، برای سازمان‌ها و شرکت‌های اروپایی در زمینه پیاده‌سازی برنامه‌های حکمرانی داده‌ها، نقش مهمی ایفا می‌کند. تمرکز GDPR روی داده‌های شخصی است و هم‌چنین دسته‌بندی خاصی از داده‌های شخصی را که به آن داده‌های حساس هم گفته می‌شود). (Microsoft GDPR, 2017)



### مدیریت الزامات بلندمدت و ماندگار حکمرانی داده‌ها

«سیاست‌ها» و «استانداردها» سازوکارهایی است که مدیریت به‌واسطه آنها الزامات بلندمدت و ماندگار کسب‌وکار خود را اطلاع‌رسانی می‌کند. این الزامات برای برنامه حکمرانی کارآمد، بسیار اساسی است:

- طرح‌هایی که بر سبک دستیابی، ذخیره‌سازی یا جابه‌جایی داده‌ها تأثیر گذار است، باید به تمام سیاست‌ها و استانداردها قابل اعمال باشد. وجود سیاست‌ها و استانداردها در الزامات کسب‌وکاری باید به‌صورت یکسان مورد توجه قرار گیرد.

- هنگام راه‌اندازی طرح کلان‌داده، ممکن است به سیاستی برای کلان‌داده (یا بازبینی سیاست‌های موجود) نیاز باشد تا معلوم شود چه کارهایی صورت می‌گیرد و چه فرصت‌های عرضه/ارزش‌آفرین منحصربه‌فردی خلق می‌شود. قواعد باید بازبینی شود؛ چرا که کلان‌داده‌ها شرایط را تغییر می‌دهد.

- باید این فکر را کنار گذاشت که کلان‌داده‌ها ظرفیت کمتری به مداخله انسان می‌دهد و روش‌های جدید پاسخ‌دهی را شناسایی کرد.

- باید فرایندهای وقفه برای پرهیز از فرایندهای گریز به‌وجود بیاید و این‌گونه رخدادها پایش شود. گروه‌ها باید برای وجود سازوکارهای بازخورد طرح داشته باشند، تا میزان تغییر را برای جلوگیری از ناتوانی کامل در برابر فرایند گریز یا موتور تصمیم، واپایش کنند (حسین‌پور و همکاران، ۱۳۹۷).

### ویژگی‌های حکمرانی پایدار

حکمرانی پایدار هشت ویژگی به شرح ذیل دارد:

۱. حکمرانی پایدار مبتنی بر الگوواره‌های پایداری محور و مدیریت توسعه پایدار است.
۲. کلیمنز در طبقه‌بندی خود از حکمرانی، حکمرانی پایدار را فراتر از حکمرانی خوب تعریف و تلقی می‌کند.
۳. در حکمرانی پایدار توسعه پدیده چندبعدی تلقی می‌شود که مردم تعریف‌کننده آن هستند.
۴. شاخص موفقیت در حکمرانی پایدار، توجه به پایداری است.
۵. در حکمرانی پایدار انسان هدف و اصل است، مسئولیت جمعی مورد تأکید است. منابع طبیعی بستر حیات و توسعه است.
۶. پاسخ‌گویی همه‌جانبه نسبت به جوامع محلی و بین‌المللی محور تأکید حکمرانی پایدار است.

۷. در حکمرانی پایدار، نقش دولت ایجاد چارچوب‌های قانونی، تواناسازی، مشوق همکاری‌ها و فعالیت‌های مردم و نهادهای مردمی است.

۸. در حکمرانی پایدار، سرمایه در ابعاد گوناگون سرمایه اقتصادی، سرمایه سیاسی، سرمایه زیست‌محیطی مطرح است (مرزبان و همکاران، ۱۳۹۶: ۸۵ - ۵۵).

### الگوی حکمرانی پایدار

طی سالیان متمادی آزمون و خطا درباره شیوه‌های حکمرانی، بیشتر الگوواره‌های حکمرانی به ناپایداری منجر شده است؛ از جمله رشدمحوری، دولت رفاه، دولت‌های سوسیالیستی، دولت مدیریتی، دولت کوچک، دولت پیمانکار، دولت قدرتمند، دولت نظارت‌کننده و غیره. کمابیش همه این الگوها نظام‌هایی بودند که از سوی نهادهای بین‌المللی برای کشورهای در حال توسعه تجویز می‌شد؛ اما در عمل بیشتر به دلیل فراهم نبودن شرایط زمینه‌ای و نگاه جامع نداشتن به محیط محکوم به شکست یا به ناپایداری منجر شده است (ابراهیم‌پور و خلیلی، ۱۳۹۰: ۷). چالش‌های ناشی از این الگوواره‌ها به ظهور الگوواره‌های جایگزین با محوریت پایداری منجر شد؛ بنابراین الگوی حکمرانی پایدار مورد توجه قرار گرفت. همراه شدن حکمرانی با توسعه پایدار و پایداری بر این واقعیت صحنه می‌گذارد که فعالیت‌های هر دو بخش دولتی و خصوصی نیازمند بازنگری و اصلاح است. این مفهوم به‌اندازه توسعه پایدار تکامل نیافته است و توسعه پایدار نیز با وجود ابهاماتی که دارد، اکنون به‌عنوان هنجار پذیرفته شده در خط‌مشی‌گذاری‌ها مورد توجه است. حکمرانی پایدار به معنی ایجاد تناسب بین سه بخش اجتماعی (دولتی، خصوصی و نهادهای مدنی) است. با مبانی فکری و فلسفی انسان‌شناختی و توسعه پایدار که مبتنی بر الگوواره تفسیرگرا است، الگوواره‌های پایداری محور و الگوواره مدیریت توسعه پایدار که از اقتصاد، سیاست، فرهنگ، آموزش، محیط‌زیست، اخلاق، عدالت و... می‌کند تا در تعامل با هم و با احترام به مختصات و فرهنگ‌های ملل مختلف به زندگی بشری معنای انسانی بخشند، از یک سو در کنار حکمرانی خوب به‌عنوان راهبردی برای تحقق آرمان‌های توسعه پایدار از سوی دیگر، ظهور یافت. امروزه تفکر حاکم بر حکمرانی این الگوواره‌ها است و تحقق توسعه پایدار نیز در سایه عملی کردن این الگوواره‌ها است؛ بنابراین استفاده از الگوواره پایداری به‌عنوان مغزافزار و استفاده از مبانی حکمرانی خوب به‌عنوان نرم‌افزار و رویکرد اجرا می‌تواند کارساز باشد (نقیبی منفرد، ۱۳۹۸: ۱۴۱). با توجه به ترکیب دو عبارت حکمرانی و پایداری می‌توان حکمرانی پایدار را این‌گونه تعریف کرد: حکمرانی به معنی

توزیع قدرت بین بخش‌های گوناگون اجتماعی و دخالت‌دادن آنها در سیاست‌گذاری‌های اجتماعی است. این بخش‌ها عبارت است از: بخش دولتی، خصوصی و نهادهای مدنی. پایداری به معنی توسعه متوازن و متناسب چهار بعد دارد. این چهار بعد عبارت است از: بعد اقتصادی، بعد اجتماعی، بعد زیست‌محیطی و بعد سیاسی (ابراهیم‌پور و خلیلی، ۱۳۹۰: ۱۰). در نتیجه حکمرانی مبتنی بر پایداری تحقق تناسب توأم بین بخش‌ها و ابعاد چهارگانه است. در اثر این تناسب، در نهادها و بخش‌های یادشده نسبت به اجرایی کردن تصمیمات تعهد به وجود می‌آید و در همه ابعاد، توسعه متناسب و پایدار ایجاد می‌شود.

### پیشینه تجربی

در زمینه حکمرانی داده‌ها مطالعات و پژوهش‌های فراوانی در سطح جهان انجام شده و پژوهشگران از جنبه‌های گوناگون این مسئله را بررسی کرده‌اند که مرتبط‌ترین و جدیدترین آنها به شرح ذیل است:

- در مقاله ارائه‌شده توسط مجید الرویت<sup>۱</sup>، الحاج بن خلیفه<sup>۲</sup> و خاور حامد<sup>۳</sup> با عنوان «طراحی چارچوب مفهومی برای حکمرانی داده‌ها در محاسبات ابری» در سیزدهمین کنفرانس بین‌المللی سیستم‌های تلفن همراه و محاسبات فراگیر (MobiSPC, 2016) که در سال ۲۰۱۶ در نشریه علمی ELSEVIER منتشر شد، چارچوب ارائه‌شده به دنبال حمایت از مصرف‌کنندگان ابری است که به طراحی حکمرانی داده‌ها نیاز دارند. نظارت بر رایانش ابری در سازمان‌های آنها با پوشش رویه‌های عمومی در طراحی حکمرانی داده‌ها برای خدمات رایانش ابری، امری ضروری است. طراحی حکمرانی داده‌ها برای رایانش ابری به‌طور بالقوه پیچیده است. برای رفع این پیچیدگی، چارچوب پیشنهادی بر اساس نظریه تحلیلی استوار است. به نقل از نظریه تحلیلی بوریس اوتو (۲۰۱۱) برای سازماندهی موضوع پژوهش حکمرانی داده مفید است. بعد از تجزیه و تحلیل دقیق در ادبیات، چارچوب پیشنهادی در این مقاله بر پنج فرایند کلیدی برای حکمرانی داده‌ها در ابر تمرکز دارد که محاسبه موارد ذیل است:

۱. ساختار حکمرانی داده

- 
1. Majid Al-Ruithe
  2. Elhadj Benkhelifa
  3. Khawar Hameed

۲. ارزیابی حکمرانی داده

۳. عملکرد حکمرانی داده

۴. مذاکره

۵. توافقنامه سطح اطمینان داده

روش پنج مرحله‌ای برای طراحی حکمرانی داده‌ها برای محاسبات ابری و همچنین مقدمه‌ای برای ارائه چارچوب مفهومی طراحی حکمرانی داده‌ها برای محاسبات ابری را نشان می‌دهد.

- در مقاله‌ای که با موضوع الگوی ارزیابی حکمرانی داده باز به‌عنوان شاخص توسعه در کشور تایلند که توسط Chatipot Srimuang, Nagul Coocharojanane, Uthai Tanlamai و Achara Chandrachai در کنفرانس بین‌المللی IEEE در زمینه فناوری ارتباطات پیشرفته (ICACT, 2017) ارائه شد، روش چهار مرحله‌ای زیر ارائه شده است:

مرحله ۱: بررسی وضعیت موجود و پیشرفت ارزیابی حکمرانی داده‌ها که بر روی نمایش حکمرانی داده‌های باز و در دسترس بودن بر اساس اصل داده‌های باز تمرکز دارد.

مرحله ۲: تعیین اینکه آیا مؤلفه‌های ارزیابی حکمرانی داده‌های باز برای بافت تایلند مناسب خواهد بود یا نه؟

مرحله ۳: بررسی‌های تجربی مربوط به مصاحبه عمیق با پنج نفر متخصص که در زمینه حکمرانی داده‌های باز در ادارات دولتی تایلند مشغول کار هستند.

مرحله ۴: خلاصه و توسعه الگوی ارزیابی

مقاله به شاخص‌ها و موارد گوناگونی در این زمینه طی دو جدول بازبینی ارزیابی حکمرانی داده‌های باز و الگوی جدید ارزیابی حکمرانی داده‌های باز پرداخته که به این قرار است:

۱. سیاست و برنامه ۲. قوانین و مقررات ۳. سازماندهی ۴. قابلیت‌های شخصی ۵. زیرساخت فناوری ۶. اصل علمی حکمرانی داده باز ۷. نوآوری ۸. مشارکت.

- در مقاله دیگری در مجله بین‌المللی پیش‌بینی فنی و تغییر اجتماعی ELSEVIER تحت عنوان «حکمرانی همکاری‌های کلان‌داده: چگونگی تعادل سازگاری با قوانین و نوآوری‌های زیانبار» که توسط Anne Fleur van Veenstra و Tijds van den Broek ارائه شده است، ضمن بررسی نظریه‌هایی در این زمینه به مواردی مانند داده‌های کلان به‌عنوان فناوری زیانبار، نقش انطباق در نوآوری‌های کلان‌داده، نظام حکمرانی بین‌سازمانی، حکمرانی سامانه بین‌سازمانی، مطالعه موردی

به اشتراک‌گذاری داده‌های بین‌سازمانی (بازاریابی شخصی، داده‌های باز، پایگاه داده مراقبت‌های بهداشتی، سکوی داده انرژی) پرداخته است و در انتها نتیجه گرفته می‌شود که نوع داده‌ها به شدت در معرض نظام حاکمیت برای داده‌های باز بیشتر با رویکردهای غیرمتمرکز و برای داده‌های حساس با رویکردهای متمرکز است.

## روش پژوهش

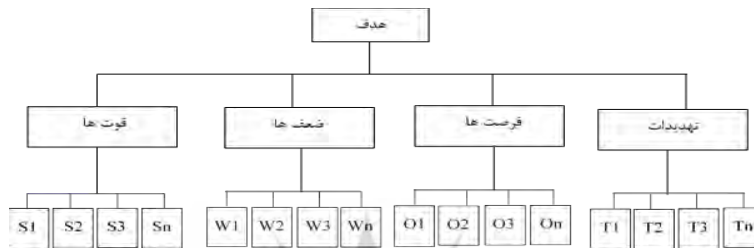
فرایند سلسله‌مراتبی AHP یکی از معروف‌ترین روش‌های تصمیم‌گیری چندشاخه است که اولین بار در دهه ۱۹۷۰ توسط تواس ال ساعتی نوآوری شد (قدسی‌پور، ۱۳۸۱). فرایند سلسله‌مراتبی یکی از روش‌هایی است که اگر هنگام تصمیم‌گیری با چند گزینه و شاخص تصمیم‌گیری روبه‌رو شویم، می‌تواند مفید باشد. این روش بر اساس مقایسه زوجی است. فرایند رتبه‌بندی و اولویت‌بندی گزینه‌ها در روش فرایند سلسله‌مراتبی AHP سه مرحله دارد که عبارت است از:

۱. تشکیل درخت سلسله‌مراتبی
  ۲. مقایسه زوجی معیارها و زیر معیارهای پژوهش
  ۳. تعیین نرخ ناسازگاری.
- در روش AHP میزان نرخ ناسازگاری قابل قبول کمتر از ۰/۱ است.

## رویکرد تلفیقی AHP-SWOT

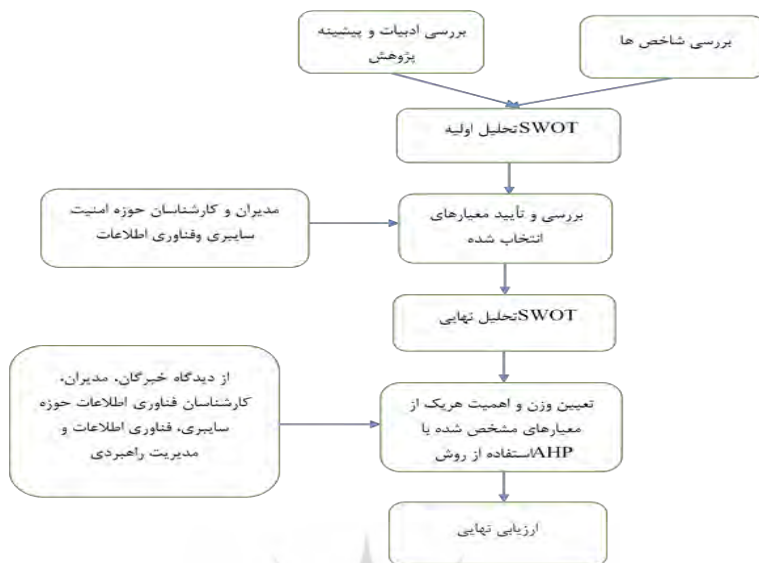
برای تجزیه و تحلیل اطلاعات و ارائه راهبردی مناسب با توجه به وضعیت و شرایط تحول تأثیرگذار، ماندگار و پایدار راهبرد حکمرانی داده‌های ارشد در فضای سایبری در این مطالعه با اولویت‌بندی راهبردهای اجرایی از روش تحلیلی AHP-SWOT استفاده شد. با بررسی محیط داخلی و خارجی مؤثر در فضای سایبری فهرستی از نقاط ضعف، نقاط قوت، فرصت‌ها و تهدیدها شناسایی و سپس با استفاده از نظر کارشناسان وزندهی بر روی هر کدام انجام شد و با تنظیم عوامل داخلی و خارجی مؤثر نسبت به تهیه و تنظیم ساختار سلسله‌مراتبی عوامل در محیط AHP با هدف تعیین، اولویت‌بندی و اتخاذ بهترین راهبردها اقدام شد. این رویکرد تلفیقی در سه‌گام به‌کار گرفته می‌شود. در گام اول فهرستی از زیرمعیارهای مربوط به نقاط قوت و ضعف قابل توجه

داخلی و فرصت‌ها و تهدیدهای خارجی و انجام تجزیه و تحلیل‌های SWOT تهیه شد؛ در گام دوم از مقایسه زوجی برای تعیین وزن هر یک از معیارهای SWOT استفاده می‌شود. در گام سوم نیز از روش AHP به منظور تعیین اهمیت نسبی هر کدام از معیارهای SWOT استفاده شد؛ سپس اهمیت تمام زیرمعیارها از راه ضرب میزان اهمیت هر کدام در وزن معیار اصلی مربوط، محاسبه و رتبه‌بندی می‌شود. ساختار سلسله‌مراتبی ماتریس SWOT در شکل ۴ نشان داده شده است.



شکل ۴. ساختار سلسله‌مراتبی ماتریس SWOT

در فرایند محاسباتی روش AHP و به منظور رتبه‌بندی و اولویت‌بندی راهبردهای مشخص شده در الگوی SWOT از نرم‌افزار Expert Choice استفاده شده است. در این مطالعه برای اولویت‌بندی معیارهایی که از روش تجزیه و تحلیل SWOT در تهران و از بین خبرگان، مدیران، کارشناسان فناوری اطلاعات حوزه سایبری، فناوری اطلاعات و مدیریت راهبردی انتخاب شد، از روش AHP استفاده شد. ابتدا معیارها شناسایی و سپس به صورت سلسله‌مراتبی ساختار بندی شد، پس از آن از روش رویکرد اولویت‌بندی اهمیت نسبی هر یک از معیارها تعیین شد. در هر سطح زیرمعیارها به صورت دوجه دو بر اساس میزان تأثیر و نفوذشان و بر اساس معیارهایی که تعیین شد در سطوح بالاتر مورد مقایسه قرار گرفت. جامعه آماری این پژوهش را ۴۲ نفر از این متخصصان تشکیل می‌دهند که به صورت تصادفی برای بررسی موضوع پژوهش انتخاب شدند. مراحل اصلی روش‌شناسی تحقیق در شکل ۵ نشان داده شده است.



شکل ۵. مراحل روش پژوهش

باتوجه به روش پژوهش، در ابتدا بر اساس شاخص‌ها، ویژگی‌ها و عوامل مؤثر بر تحول اثرگذار، ماندگار و پایدار راهبرد حکمرانی داده‌های ارشد در فضای سایبری معیارهای مربوط به هرکدام از گروه‌های نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها شناسایی و با مطالعه پیشینه پژوهش مرتبط با SWOT در درجه اول تحلیل ابتدایی معیارهای اصلی انجام شد. این فرایند از روش ایجاد کمیته تخصصی از بین کارشناسان و مدیران حوزه امنیت سایبری و اطلاعات و فناوری برای هر کدام از این گروه‌ها انجام شد. در مرحله دوم معیارهای SWOT مورد تحلیل نهایی و تأیید قرار گرفت. این فرایند توسط کارشناسان و مدیران متخصص در این حوزه انجام شد. در مرحله سوم برای تعیین وزن و اهمیت هر عامل با استفاده از روش AHP اقدام شد. در این مرحله ابتدا ماتریس‌های مقایسه زوجی معیارها و زیرمعیارهای SWOT توسط گروه متخصص که ۴۲ نفر از خبرگان، مدیران، کارشناسان فناوری اطلاعات حوزه امنیت سایبری، فناوری اطلاعات و مدیریت راهبردی بودند، با استفاده از مقیاس ۱ الی ۹ تکمیل و بر مبنای آن میزان اهمیت هر کدام تعیین شد.

## یافته‌های پژوهش

با استفاده از مرحله اول و دوم روش‌شناسی در این پژوهش و پیشینه، معیارهای مربوط به هرکدام از گروه‌های نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها شناسایی و در گروه‌های SWOT طبقه‌بندی شد. نتایج این مرحله در جدول ۱ نشان‌داده شده است. همان‌طور که در این جدول مشاهده می‌شود، گروه‌های نقاط قوت و نقاط ضعف هفت زیرمعیار و گروه‌های فرصت و تهدید هرکدام هشت زیرمعیار دارد.

جدول ۱. ماتریس SWOT

نقاط ضعف	نقاط قوت
W1 نبود برنامه‌ریزی و سیاستگذاری برای حکمرانی داده‌های ارشد	S1 وجود توانمندی‌های فنی، مدیریتی و... برای برنامه‌ریزی و سیاستگذاری حکمرانی داده‌های ارشد
W2 نبود تجهیزات و زیرساخت‌های مورد نیاز برای اعمال حکمرانی بر داده‌های ارشد	S2 تعهد دولت به عملیاتی‌کردن و توسعه شبکه ملی اطلاعات
W3 کمبود بودجه و اعتبارات لازم برای تأمین زیرساخت‌ها و تجهیزات مورد نیاز برای اعمال حکمرانی بر داده‌های ارشد	S3 مدیریت کیفیت، شفافیت و صحت داده‌های ارشد
W4 تعامل‌نداشتن مالکان و صاحب‌اختیاران داده‌های ارشد برای اشتراک‌گذاری و تبادل داده‌های ارشد	S4 تسهیل در جمع و پایش داده‌های ارشد
W5 نبود ساختارهای مورد نیاز برای تولید، ذخیره، انتقال و تبادل داده‌های ارشد	S5 یکپارچگی و آسان‌سازی در دسترسی به داده‌های ارشد
W6 عملیاتی‌نشدن شبکه ملی اطلاعات	S6 افزایش توان حریم خصوصی و امنیت داده‌های ارشد
تهدیدها	فرصت‌ها
T1 امکان نقض مالکیت داده‌های ارشد	O1 ایجاد بخش عمده زیرساخت‌های شبکه ملی اطلاعات
T2 امکان ایجاد تعارض منافع ناشی از افشای داده‌های ارشد	O2 کاهش هزینه‌های جمع‌آوری و پایش داده‌های ارشد
T3 آگاهی‌نداشتن و نبود فرهنگ تعامل در راستای تحقق حکمرانی داده‌های ارشد	O3 دسترسی عمومی به شبکه اینترنت برای اشتراک‌گذاری و تبادل داده‌های ارشد
T4 امکان دسترسی غیر مجاز و سوء استفاده از داده‌های ارشد	O4 افزایش سطح دسترسی به پایگاه‌های داده
T5 تهدیدهای سایبری در راستای حذف، تغییر، سرقت و تخریب داده‌های ارشد	O5 افزایش سرعت و سطح دسترسی به داده‌های ارشد
T6 نبود برنامه راهبردی در سطح ملی برای حکمرانی داده‌های ارشد	O6 افزایش کمی و کیفی داده‌های ارشد



پس از به‌کارگرفتن مرحله سوم روش پژوهش، نتایج این مرحله در جدول ۲ تا ۷ نشان‌داده شده است. اعداد داخل هرکدام از جدول‌ها بیانگر ترجیحات و اهمیت عامل سطر و عامل ستون است. این مقادیر از راه محاسبه میانگین هندسی نظر ۴۲ نفر از خبرگان، مدیران، کارشناسان فناوری اطلاعات حوزه سایبری، فناوری اطلاعات و مدیریت راهبردی به‌دست آمد. در جدول ۲ مقایسه زوجی هرکدام از گروه‌های اصلی تجزیه‌وتحلیل SWOT ارائه شده است. ستون اهمیت نیز بیانگر وزن و اهمیت هرکدام از عوامل چهارگانه است.

جدول ۲. مقایسه زوجی گروه‌های SWOT

میزان اهمیت	قوت (S)	فرصت (O)	ضعف (W)	تهدید (T)	معیار اصلی (SWOT)
۰/۲۴۱	۱/۰۴۰	۱/۰۲۴	۱/۰۶۸	۱	تهدید (T)
۰/۳۱۴	۱/۱۶۶	۲/۱۵۱	۱		ضعف (W)
۰/۱۸۱	۱/۵۶۱	۱			فرصت (O)
۰/۲۶۴	۱				قوت (S)
IR = ۰/۰۲					

همان‌طور که در نتایج جدول ۲ مشاهده می‌شود گروه نقاط ضعف (W) با وزن ۰/۳۱۴، بیشترین اهمیت را از نظر متخصصان به خود اختصاص داده است. هم‌چنین گروه‌های فرصت (O) با وزن ۰/۱۸۱ در رتبه آخر قرار گرفته است. همان‌طور که نتایج نشان می‌دهد نرخ ناسازگاری این ماتریس برابر با ۰/۰۲ به‌دست آمد که چون کوچکتر از ۰/۱ است می‌توان گفت که قضاوت و مقایسه زوجی از سازگاری مناسب برخوردار است. جدول ۳ مقایسه زوجی بین زیرمعیارهای گروه قوت را نشان می‌دهد. در این جدول زیرمعیار وجود توانمندی‌های فنی، مدیریتی و... برای برنامه‌ریزی و سیاستگذاری حکمرانی داده‌های ارشد (S1) با وزن ۰/۲۴۳ بیشترین اهمیت و زیرمعیار تعهد دولت به عملیاتی‌کردن و توسعه شبکه ملی اطلاعات (S2) با وزن ۰/۱۱۸ کمترین اهمیت را از نظر متخصصان داشته است. نرخ ناسازگاری این ماتریس برابر با ۰/۰۶ و چون کوچکتر از ۰/۱ است، می‌توان گفت که قضاوت و مقایسه زوجی از سازگاری مناسب برخوردار است.

## جدول ۳. ماتریس مقایسه زوجی زیرمعیارهای گروه نقاط قوت

نقاط قوت		S1	S2	S3	S4	S5	S6	میزان اهمیت
S1	وجود توانمندی‌های فنی، مدیریتی و... برای برنامه‌ریزی و سیاستگذاری حکمرانی داده‌های ارشد	۱	۱/۸۵۳	۱/۸۸۶	۱/۸۶۳	۱/۵۸۵	۱/۴۵۹	۰/۲۴۳
S2	تعهد دولت به عملیاتی‌کردن و توسعه شبکه ملی اطلاعات		۱	۱/۰۴۷	۱/۱۹۲	۱/۵۰۴	۱/۶۹۴	۰/۱۱۸
S3	مدیریت کیفیت، شفافیت و صحت داده‌های ارشد			۱	۲/۳۳۴	۱/۵۵۸	۱/۸۹۰	۰/۱۵۵
S4	آسان‌سازی در تجمیع و پایش داده‌های ارشد				۱	۱/۴۴۷	۱/۳۹۸	۰/۱۵۲
S5	یکپارچگی و آسان‌سازی در دسترسی به داده‌های ارشد					۱	۱/۹۴۹	۰/۱۷۳
S6	افزایش توان حریم خصوصی و امنیت داده‌های ارشد						۱	۰/۱۶۰
IR = ۰/۰۶								

جدول ۴ مقایسه زوجی بین زیر معیارهای گروه ضعف را نشان می‌دهد. در این جدول زیرمعیار نبود برنامه‌ریزی و سیاستگذاری برای حکمرانی داده‌های ارشد (W1) با وزن ۰/۲۳۹ بیشترین اهمیت و زیرمعیار عملیاتی‌نشدن شبکه ملی اطلاعات (W6) با وزن ۰/۱۱۶ کمترین اهمیت را از نظر متخصصان داشته است. همان‌طور که نتایج نشان می‌دهد نرخ ناسازگاری این ماتریس برابر با ۰/۰۳ است. از آنجا که این مقدار کوچک‌تر از ۰/۱ است؛ لذا می‌توان گفت که قضاوت و مقایسه زوجی از سازگاری مناسب برخوردار است.

## جدول ۴. ماتریس مقایسه زوجی زیرمعیارهای گروه ضعف

نقاط قوت		W1	W2	W3	W4	W5	W6	میزان اهمیت
W1	نبود برنامه‌ریزی و سیاستگذاری برای حکمرانی داده‌های ارشد	۱	۱/۰۴۳	۱/۶۹۷	۲/۳۶۱	۲/۰۶۰	۱/۳۲۷	۰/۲۳۹
W2	نبود تجهیزات و زیرساخت‌های مورد نیاز برای اعمال حکمرانی بر داده‌های ارشد		۱	۱/۰۶۸	۲/۳۲۱	۱/۴۴۵	۱/۲۷۰	۰/۱۸۸
W3	کمبود بودجه و اعتبارات لازم برای تأمین زیرساخت‌ها و تجهیزات مورد نیاز برای اعمال حکمرانی بر داده‌های ارشد			۱	۲/۳۳۸	۱/۴۵۴	۲/۰۸۸	۰/۲۰۵
W4	تعامل نداشتن مالکان و صاحب‌اختیاران داده‌های ارشد برای اشتراک‌گذاری و تبادل داده‌های ارشد				۱	۱/۴۱۵	۲/۰۱۶	۰/۱۳۴
W5	نبود ساختارهای مورد نیاز برای تولید، ذخیره، انتقال و تبادل داده‌های ارشد					۱	۱/۲۱۳	۰/۱۱۹
W6	عملیاتی‌نشدن شبکه ملی اطلاعات						۱	۰/۱۱۶
IR = ۰/۰۳								

جدول ۵ مقایسه زوجی بین زیر معیارهای گروه فرصت‌ها را نشان می‌دهد. در این جدول زیرمعیار ایجاد بخش عمده زیرساخت‌های شبکه ملی اطلاعات (O1) با وزن ۰/۲۳۹ بیشترین اهمیت و زیرمعیار افزایش سرعت و سطح دسترسی به داده‌های ارشد (O5) با وزن ۰/۱۲۰ کمترین اهمیت را از نظر متخصصان داشته است. همان‌طور که نتایج نشان می‌دهد نرخ ناسازگاری این ماتریس برابر با ۰/۰۲ است. از آنجا که این مقدار کوچک‌تر از ۰/۱ به دست آمد؛ لذا می‌توان گفت که قضاوت و مقایسه زوجی از سازگاری مناسب برخوردار است.

جدول ۵. ماتریس مقایسه زوجی زیر معیارهای گروه فرصت‌ها

میزان اهمیت	O6	O5	O4	O3	O2	O1	نقاط قوت
۰/۲۳۹	۲/۱۱۰	۱/۸۲۶	۱/۸۰۷	۱/۳۴۴	۲/۲۴۶	۱	ایجاد بخش عمده زیرساخت‌های شبکه ملی اطلاعات
۰/۱۴۱	۱/۳۲۶	۱/۰۷۷	۲/۰۹۷	۱/۱۵۶	۱		کاهش هزینه‌های جمع‌آوری و پایش داده‌های ارشد
۰/۲۰۲	۲/۰۴۱	۱/۳۲۴	۱/۷۸۴	۱			دسترسی عمومی به شبکه اینترنت برای اشتراک‌گذاری و تبادل داده‌های ارشد
۰/۱۶۱	۱/۱۹۹	۱/۴۵۵	۱				افزایش سطح دسترسی به پایگاه‌های داده
۰/۱۲۰	۱/۵۲۵	۱					افزایش سرعت و سطح دسترسی به داده‌های ارشد
۰/۱۳۶	۱						افزایش کمی و کیفی داده‌های ارشد
IR = ۰/۰۲							

جدول ۶ مقایسه زوجی بین زیرمعیارهای گروه تهدیدها را نشان می‌دهد. در این جدول زیرمعیار نبود برنامه راهبردی در سطح ملی برای حکمرانی داده‌های ارشد (T6) با وزن ۰/۲۰ بیشترین اهمیت و زیرمعیار امکان ایجاد تعارض منافع ناشی از افشای داده‌های ارشد (T2) با وزن ۰/۱۳۶ کمترین اهمیت را از نظر متخصصان داشته است. همان‌طور که نتایج نشان می‌دهد نرخ ناسازگاری این ماتریس برابر با ۰/۰۶ است. از آنجا که این مقدار کوچک‌تر از ۰/۱ است؛ لذا می‌توان گفت که قضاوت و مقایسه زوجی از سازگاری مناسب برخوردار است.

جدول ۶. ماتریس مقایسه زوجی زیر معیارهای گروه تهدیدها

نقاط قوت		T1	T2	T3	T4	T5	T6	میزان اهمیت
T1	امکان نقض مالکیت داده‌های ارشد	۱	۱/۲۴۴	۱/۴۸۴	۲/۲۷۸	۱/۰۶۶	۲/۰۲۹۱	۰/۱۶۳
T2	امکان ایجاد تعارض منافع ناشی از افشای داده‌های ارشد		۱	۱/۰۶۴	۱/۳۷۹	۱/۵۰۲	۱/۱۰۴	۰/۱۳۶
T3	آگاهی نداشتن و نبود فرهنگ تعامل در راستای تحقق حکمرانی داده‌های ارشد			۱	۱/۰۰۸	۲/۱۸۸	۱/۲۱۸	۰/۱۹۴
T4	امکان دسترسی غیر مجاز و سوء استفاده از داده‌های ارشد				۱	۱/۹۳۶	۱/۰۴۵	۰/۱۴۰
T5	تهدیدهای سایبری در راستای حذف، تغییر، سرقت و تخریب داده‌های ارشد					۱	۱/۳۲۳	۰/۱۶۶
T6	نبود برنامه راهبردی در سطح ملی برای حکمرانی داده‌های ارشد						۱	۰/۲۰۰
IR = ۰/۰۶								

سرانجام بر اساس وزن نهایی هر کدام از زیرمعیارها با توجه به وزن معیار اصلی گروه SWOT محاسبه شد. نتایج بررسی در جدول ۷ نشان داده شده است. همان‌طور که نتایج جدول ۷ نشان می‌دهد نبود برنامه‌ریزی و سیاستگذاری برای حکمرانی داده‌های ارشد (W1) با وزن نهایی ۰/۰۷۲ مهم‌ترین زیرمعیار بین همه زیرمعیارهای مورد نظر بوده است. این زیرمعیار در گروه ضعف قرار دارد که با وزن ۰/۳۱۴ مهم‌ترین گروه به‌شمار می‌رود.

جدول ۷. وزن نهایی زیرمعیارها

گروه SWOT	وزن معیار	زیرمعیارهای SWOT	وزن زیرمعیار در گروه	وزن نهایی هر زیرمعیار
قوت	۰,۲۶۴	S1	۰,۲۴۳	۰,۰۶۴
		S2	۰,۱۱۸	۰,۰۳۱
		S3	۰,۱۵۵	۰,۰۴۱
		S4	۰,۱۵۲	۰,۰۴۰
		S5	۰,۱۷۳	۰,۰۴۶
		S6	۰,۱۶۰	۰,۰۴۲
ضعف	۰,۳۱۴	W1	۰,۲۳۹	۰,۰۷۲
		W2	۰,۱۸۸	۰,۰۵۷
		W3	۰,۲۰۵	۰,۰۶۲
		W4	۰,۱۳۴	۰,۰۴۱
		W5	۰,۱۱۹	۰,۰۳۶
		W6	۰,۱۱۶	۰,۰۳۵
فرصت	۰,۱۸۱	O1	۰,۲۳۹	۰,۰۵۲
		O2	۰,۱۴۱	۰,۰۳۱
		O3	۰,۲۰۲	۰,۰۴۴
		O4	۰,۱۶۱	۰,۰۳۵
		O5	۰,۱۲۰	۰,۰۲۶
		O6	۰,۱۳۶	۰,۰۳۰
تهدید	۰,۲۴۱	T1	۰,۱۶۳	۰,۰۴۱
		T2	۰,۱۳۶	۰,۰۳۴
		T3	۰,۱۹۴	۰,۰۴۹
		T4	۰,۱۴۰	۰,۰۳۵
		T5	۰,۱۶۶	۰,۰۴۲
		T6	۰,۲۰۰	۰,۰۵۱

### جمع‌بندی و نتیجه‌گیری

از بررسی موارد ضعف، قوت، فرصت، تهدید و همچنین تحلیل ماتریس سوات حکمرانی داده‌های ارشد چنین استنباط می‌شود که مغفول‌ماندن این موضوع با اهمیت ضمن محرومیت از مزیت‌ها و فرصت‌های فراوانی که ایجاد می‌کند، سبب می‌شود که از طریق مورد سوء استفاده قرارگرفتن نقاط ضعف، آسیب‌ها و تهدیدهای بالفعل و بالقوه‌ای که امروزه در فضای سایبری همواره در شرف

تغییر ماهیت و افزایش است، صدمات جبران‌ناپذیری به امنیت داده‌ها، تحمیل هزینه‌های دوباره‌کاری و اقدامات جزیره‌ای، حریم خصوصی و مالکیت مادی و معنوی وارد خواهد ساخت؛ لذا سیاست‌گذاران و تصمیم‌گیران سایبری و مدیران عرصه داده‌ها و فناوری اطلاعات می‌توانند با استفاده از راهبردهای ارائه‌شده در این پژوهش حکمرانی بر داده‌های ارشد را اعمال و محقق کرده و گام مهمی در برنامه‌ریزی راهبردی، تدوین دستورالعمل‌ها، الزامات و استانداردهای محرمانگی و امنیت داده‌های این حوزه بردارند. در انتها با توجه به میران اهمیت داده‌های ارشد پیشنهاد می‌شود تمام نهادها و دستگاه‌های حاکمیتی مانند شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، سازمان فناوری اطلاعات ایران و... در راستای تأمین امنیت و منافع ملی با مشارکت یکدیگر نسبت به تدوین قوانین و مقررات، تقسیم کار ملی و تبیین ساختارها و فرایندهای لازم برای ایجاد تحول تأثیرگذار، ماندگار و پایدار در اعمال حکمرانی و نگهداری داده‌های ارشد اقدام مقتضی را به‌عمل آورند.



پژوهشگاه علوم انسانی و مطالعات فرهنگی  
پرتال جامع علوم انسانی

## فهرست منابع

- ابراهیم‌پور، حبیب و خلیلی، حسن (۱۳۹۰). از حکمرانی خوب تا حکمرانی پایداری، کنفرانس بین‌المللی مدیریت.
- حسین‌پور، مهدی و همکاران (۱۳۹۷). تعیین ابعاد فنی، حقوقی، مقرراتی و تدوین پیش‌نویس لایحه حکمرانی داده در کشور، تهران: پژوهشگاه ارتباطات و فناوری اطلاعات.
- عصاریان‌نژاد، حسین و شریفی زارچی، احمدعلی (۱۳۹۶). ضرورت مدیریت اطلاعات عمومی در جمهوری اسلامی ایران و تأثیر آن در ارتقای امنیت ملی، فصلنامه امنیت ملی، س ۷، ش ۲۴.
- قدسی‌پور، سید حسن (۱۳۸۱). فرایند تحلیل سلسله‌مراتبی AHP، تهران: انتشارات دانشگاه امیرکبیر.
- مرزبان، نازنین؛ عیوضی، محمدرحیم و صالحی، معصومه (۱۳۹۶). از بررسی حکمرانی خوب تا الگوی حکمرانی پایدار، فصلنامه راهبرد، س ۲۶، ش ۸۵: ۸۵ - ۵۵.
- نقیبی مفرد، حسام (۱۳۸۹). حکمرانی مطلوب در پرتوی جهانی‌شدن حقوق بشر، تهران: مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
- الیاسی، بهروز؛ حسینی‌نسب، مهدی؛ سلیمی کوچی، فهیمه و حسین‌پور، مهدی (۱۳۹۹). حکمرانی داده‌ها: مبانی استقرار حکمرانی داده‌ها، تهران: انتشارات آوای قلم.

- “ISO Standards,” [Online]. Available: <https://www.iso.org/standards.html>
- Anthony Chalker, Data Governance Overview, protiviti Consulting Co., 2014 .
- Brian Lee, Do You Really Have Big Data, Or Just Too Much Data?, 2016.
- C. Balard, C. Compert, T. Jesionowski, I. Milman, B. Plants, B. Rosen and H. Smith, Information Governance Principles and Practices for a Big Data Landscape, 2014.
- Chalabi Mona, Making sense of too much data, [www.ted.com/speakers/mona\\_chalabi?referrer=playlist-making\\_sense\\_of\\_too\\_much\\_data](http://www.ted.com/speakers/mona_chalabi?referrer=playlist-making_sense_of_too_much_data), February 2017
- Christian Bruck, "Challenges and opportunities of Data Governance in private and public organizations," 2017.
- DAMA-DMBOK: Data Management Body of Knowledge, Second edition ed., Basking Ridge, New Jersey: 2017.
- Data Governance for GDPR Compliance: Principles, Processes, and Practices, Microsoft, 2017.
- J. Ladley, Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program, 1st edition ed., Waltham, MA: Morgan Kaufmann, 2012.
- Kerremans GR (2016) Big data in Healthcare. J Health Commun 1: 4.
- Kruse SC, Smith B, Vanderlinden H, Nealand A (2017). J Med Syst 41: 127.
- M. Allen and D. Cervo, Multi-Domain Master Data Management: Advanced MDM and Data Governance in Practice, 1 edition ed., Waltham, MA: Morgan Kaufmann, 2015.
- M. O. Enofe, "Data Management in an Operational Context: A study at Volvo Group Trucks Operations," 2017.
- Master Data Management (MDM) Reference Architecture (RA), California: 2014.
- The Importance of Data Governance in Healthcare ‘An Encore Point of View ‘By Bill Fleissner; Kamalakar Jasti; Joy Ales, MHA, BSN, RN; Randy Thomas, FHIMSS ؛ October 2014

Wakaskar RR (2017) Cancer Therapy with Drug Delivery Systems. J Pharmacogenomics 8: e158.

