

نگاهی نو؛
به حکمرانی فضای مجازی

زاویه 



الزامات قانونگذاری در نظام حکمرانی داده

مروری بر قانون حکمرانی داده اتحادیه اروپا



الزامات قانونگذاری در نظام حکمرانی داده

مروری بر قانون حکمرانی داده اتحادیه اروپا



سیدعلی حسینی

نویسنده

امین زاده حسین

مدیر مطالعه

تیر ۱۴۰۲

تاریخ تنظیم

۶۶۹۰

تعداد کلمات

حکمرانی داده، داده نهادهای عمومی، دسترسی به داده،

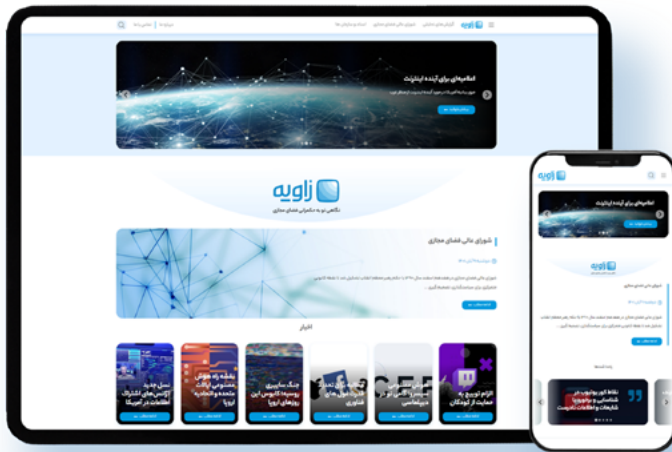
کلیدواژه‌ها

خدمات واسطه‌گری داده، داده عام‌المنفعه

محتوای انتشار یافته در این اثر،

لزوماً بیانگر دیدگاه مجموعه زاویه نیست.

نگاهی نو،
به حکمرانی فضای مجازی



فهرست مطالب

۱	خلاصه مدیریتی
۵	مقدمه (۱)
۱۱	چارچوب نظری قانون حکمرانی داده (۲)
۱۵	داده‌نهادهای عمومی (۳)
۱۶	بیان موضوع (۱-۳)
۱۷	الزامات (۲-۳)
۱۹	خدمات واسطه‌گری داده (۴)
۱۹	بیان موضوع (۱-۴)
۲۲	الزامات (۲-۴)
۲۵	داده‌عام‌المنفعه (۵)
۲۵	بیان موضوع (۱-۵)
۲۷	الزامات (۲-۵)
۳۱	جریان‌های بین‌المللی داده (۶)
۳۳	مقام صالح ملی (تنظیم‌گر) (۷)
۳۵	جمع‌بندی (۸)
۳۹	پیشنهادسیاستی (۹)
۴۱	منابع (۱۰)

خلاصه مدیریتی



حکمرانی داده رویکردی برای مدیریت داده‌ها و اطلاعات در یک نظام سیاسی است؛ به نحوی که امکان استفاده از داده‌ها^۱ برای اهداف عمومی و اقتصادی فراهم شده و در عین حال هرگونه سوءاستفاده از داده و نقض اصول حاکم بر انواع داده‌ها، کنترل شود. علی‌رغم تلاش بخش خصوصی و دولتی طی سال‌های گذشته برای توسعه اقتصاد دیجیتال در ایران، لیکن عدم اهتمام به پیاده‌سازی نظام حکمرانی داده در ساختارهای سیاست‌گذاری و تقنینی کشور، این حوزه را با چالش‌های فراوانی روبرو کرده است. خلأ قوانین و مقررات مورد نیاز برای سامان‌دهی و انتظام این حوزه، منجر به از دست دادن سرمایه داده‌های کشور و محرومیت از آثار و عواید اقتصادی و اجتماعی حاصل از آن شده است. در این گزارش به منظور معرفی تجربه نظام‌های حقوقی پیشرو در موضوع حکمرانی داده، «قانون حکمرانی داده» مصوب پارلمان اروپا که از سپتامبر ۲۰۲۳ لازم‌الاجرا خواهد بود، مورد بررسی قرار گرفته است.

۱. «استفاده از داده» یا «استفاده‌کننده از داده» در این نوشتار جایگزینی برای اصطلاح (Data User) است. این اصطلاح در ماده ۲ قانون حکمرانی داده تعریف گردیده است: استفاده‌کننده از داده هر شخص حقیقی یا حقوقی است که به داده‌های شخصی یا غیرشخصی خاصی دسترسی دارد و مجاز است از آن داده‌ها برای اهداف تجاری یا غیرتجاری استفاده کند.

اهم نکات قانون حکمرانی داده اتحادیه اروپا شامل موارد زیر می‌شود:

۱. اصول ۴ گانه داده مشتمل بر یافت‌پذیری، دسترس‌پذیری، هم‌کنش‌پذیری و قابلیت استفاده مجدد، چارچوب نظری قانون حکمرانی داده محسوب می‌گردد.
۲. نهادهای عمومی دولتی و غیردولتی (به‌جز استثنائات قانون مانند نهادهای نظامی، آموزشی و...) با رعایت تکالیف مندرج در قانون مکلف‌اند داده‌هایی را که با هزینه بودجه عمومی جمع‌آوری کرده‌اند، در دسترس استفاده‌کنندگان از داده قرار دهند.
۳. قانون حکمرانی داده با تعریف تکالیفی بر ارائه‌دهندگان خدمات واسطه‌ای داده، فعالیت آن‌ها را سازماندهی و کنترل می‌کند. این تکالیف شامل الزام به اخذ مجوز، رعایت الزامات و استانداردهای فنی، تفکیک حقوقی خدمات واسطه‌ای از غیر آن، اصول رقابت و... می‌شود.
۴. رسمیت‌بخشی به فعالیت مؤسساتی که در زمینه جمع‌آوری داده‌های عام‌المنفعه فعالیت می‌کنند، یکی دیگر از ابتکارات قانون حکمرانی داده است. الزامات فراتر از آنچه که برای واسطه‌های داده وجود داشت، سبب فعالیت نظام‌مند این مؤسسات خواهد شد.
۵. انتقال داده‌های موضوع قانون حکمرانی داده، اعم از داده‌های شخصی و غیرشخصی به خارج از اتحادیه اروپا ممنوع گردیده است.

همچنین با در نظر گرفتن وضعیت فعلی نظام حقوق ایران در موضوع حکمرانی داده، به طور خلاصه گزاره های سیاستی ذیل در خصوص آن پیشنهاد گردیده است:

۱. کاربست حکمرانی داده در ایران، بیش از هر اقدام تقنینی یا اجرایی، مستلزم تأیید و ابلاغ آن در بالاترین سطح سیاستی در نظام حقوقی کشور است. به نحوی که نهادهای نظامی و امنیتی نیز بر اجرای آن اتفاق نظر داشته باشند.
۲. حکمرانی داده اساساً قانونی پیشرفته محسوب می شود که تصویب و اجرایی سازی آن در نظام حقوقی هر کشور، مستلزم مجموعه ای از قوانین پیش نیاز و مکمل است؛ در وضعیت فقدان قوانین سنتی داده در ایران همچون اسرار دولتی، حریم خصوصی، اسرار تجاری و قوانین جدید حوزه داده مانند داده های باز، حفاظت از داده های شخصی و...، قانون حکمرانی داده قابلیت اجرایی نخواهد یافت.

۱) مقدمه

پذیرش فناوری‌های نوظهور در ایران و توسعه اقتصاد دیجیتال، ظرفیت‌های زیادی را برای رشد و شکوفایی اقتصاد کشور فراهم کرده است. داده به عنوان موتور پیشران اقتصاد دیجیتال، از اهمیت بسیار بالایی برخوردار است و دسترسی شرکت‌های فعال در این حوزه به انواع آن یک پیش‌نیاز اساسی به‌شمار می‌آید. داده منبعی برای محصولات و خدمات جدید در عرصه‌های مختلف مرتبط با فناوری اطلاعات و ارتقای آن‌ها محسوب می‌گردد. داده، فناوری‌های جدید را فعال، تولید را کارآمدتر و ابزارهایی را برای مبارزه با چالش‌های اجتماعی فراهم می‌کند. در زمینه هوش مصنوعی نیز، مدیریت و به‌اشتراک‌گذاری حجم عظیمی از داده‌ها برای یادگیری ماشین و توسعه هوش مصنوعی ضروری است. همچنین در موضوع نظام اداری، امکان اتخاذ سیاست‌گذاری صحیح و مطلوب، حکمرانی شفاف و ارائه خدمات عمومی عادلانه را برای سازمان‌های اداری فراهم می‌کند. در بخش صنایع نیز داده می‌تواند منبعی

برای رشد استارت‌آپ‌ها و شرکت‌های نوپا در حوزه فناوری باشد. تأثیر دسترسی به داده‌های هر بخش، آثار ذیل را در نظام اقتصادی و اجتماعی خواهد داشت:

- داده‌های سلامت: ارتقای خدمات درمانی، درمان‌های خانگی و درمان بیماری‌های نادر یا مزمن و واکنش‌های سریع به بیماری‌های پاندمی.
- داده‌های حمل‌ونقل: صرفه‌جویی در هزینه حمل‌ونقل، صرفه‌جویی در مصرف سوخت، کاهش بیماری‌های تنفسی ناشی از آلاینده‌های شهری و... با استفاده از حمل‌ونقل داده‌محور.
- داده‌های زیست‌محیطی: مبارزه با تغییرات آب‌وهوایی، کاهش انتشار دی‌اکسیدکربن و مبارزه با شرایط اضطراری، مانند سیل و آتش‌سوزی.
- داده‌های کشاورزی: استفاده کشاورزان از کلان داده‌ها برای به دست آوردن اطلاعات در مورد تغییر آب‌وهوا، میزان بارندگی، مصرف کود، میزان بارندگی و سایر عواملی که بر عملکرد محصول تأثیر می‌گذارند. همه این اطلاعات به کشاورزان در تصمیم‌گیری دقیق و قابل‌اعتماد کمک می‌کند که بهره‌وری آن‌ها را از کشت زمین به حداکثر می‌رساند.
- داده‌های مدیریت دولتی: ارائه آمار رسمی بهتر و قابل‌اعتمادتر و کمک به تصمیم‌گیری‌های کارشناسی شده و مبتنی بر آمار واقعی.
- و...

با در نظر گرفتن سهم اقتصاد دیجیتال و ارزش شرکت‌های بزرگ فناوری اطلاعات، در حال حاضر اراده حاکمیت سیاسی کشورها به این سمت رهنمون شده است که حداکثر استفاده از ظرفیت داده‌ها را در نظام‌های اقتصادی خود فراهم آورند که اجمالاً از آن به عنوان حکمرانی داده یاد می‌شود. وضعیت حکمرانی داده در ایران در وضعیت سکوت قانون‌گذار به سر می‌برد و شرکت‌های حوزه فناوری اطلاعات، با استفاده از داده‌هایی که خود استخراج می‌کنند یا از طرق غیرشفاف به داده‌های مورد

نیاز خود دسترسی می‌یابند، به فعالیت می‌پردازند. در حال حاضر بازار خرید و فروش و انتقال داده بین پلتفرم‌ها و شرکت‌های حوزه فناوری اطلاعات در ایران، بازاری کاملاً آزاد و بدون هرگونه دخالت حاکمیت تلقی می‌شود.

در نظام حقوقی ایران هنوز قانون حفاظت از داده‌های شخصی برای انتظام انتقال داده‌های شخصی و حساس به تصویب نرسیده است؛ این در حالی است که حتی نظام‌های حقوقی لیبرال نیز قوانین سخت‌گیرانه‌ای را برای این حوزه به تصویب رسانده‌اند. از حیث ایجابی حکمرانی داده که مستلزم زمینه‌سازی برای دسترسی امن کسب‌وکارها به داده‌ها می‌باشد، نیز نظام حقوقی ایران در وضعیت سکوت و ابهام به سر می‌برد. باید اذعان داشت که حجم عظیمی از داده‌های غیرشخصی در ایران، از سوی نهادهای عمومی دولتی و غیردولتی جمع‌آوری و نگهداری می‌شود که جریان آن در اقتصاد دیجیتال سبب توسعه درآمدهای ملی کشور می‌گردد.

حکمرانی داده به عنوان رویکردی برای توسعه اقتصاد دیجیتال ایران، یک امر حیاتی در برهه حاضر محسوب می‌شود و حصول آن مستلزم هنجارسازی قواعد مربوط به داده و تصویب قانون حکمرانی داده است. اما بدیهی است که قانون‌گذاری در موضوع داده و حکمرانی آن، به دلیل پیچیدگی‌ها و ابعاد فنی آن، علی‌الخصوص برای نظام قانون‌گذاری ایران که تجربه‌ای در این خصوص نداشته، امری دشوار خواهد بود. لذا اولین گام برای حکمرانی داده در ایران، مطالعه تطبیقی و تدقیق در تجارب قانون‌گذاری سایر نظام‌های حقوقی محسوب می‌شود. به همین منظور در این گزارش، تجربه اتحادیه اروپا در این موضوع مورد بررسی قرار گرفته است.

قانون حکمرانی داده^۱ تلاش پارلمان اتحادیه اروپا برای تسهیل اشتراک‌گذاری داده‌ها در کشورهای عضو به منظور استفاده کسب‌وکارها و مردم از ظرفیت عظیم داده‌ها است. گرچه منافع حاصل از دسترسی به داده‌ها برای اهداف اقتصادی و

۱. Data Governance Act (EU) 2022/868

اجتماعی کشورها مبرهن است، لیکن تاکنون این مهم در سطح اتحادیه اروپا بنا به دلائلی محقق نگردیده است. دلیل اول مربوط به بی‌اعتمادی مردم به پلتفرم‌های آنلاین است که اشتراک‌گذاری داده‌های شخصی خود در اختیار آنان را به‌عنوان تهدیدی علیه حقوق فردی خود محسوب می‌کنند. دلیل دوم محدودیت‌های مربوط به طبقه‌بندی اسناد دولتی و قوانین ملی مربوط به اسناد سری و محرمانه است که دسترسی به بخش عظیمی از داده‌ها را متوقف نموده است. دلیل بعدی نیز مربوط به محدودیت‌ها و ضعف‌های فنی برای حفاظت از امنیت اطلاعات و داده‌های شخصی است. بنا به دلائل مذکور دسترسی و به اشتراک‌گذاری داده‌ها در سطح اتحادیه اروپا با مشکل مواجه گردیده است.

منافع حاصل از تسهیل دسترسی به داده‌ها، پارلمان اروپا را بر آن نمود که قانونی به‌منظور کنترل آسیب‌های فوق تصویب نماید. قانون حکمرانی داده با در نظر گرفتن آسیب‌های فوق، نظام حکمرانی داده را مبتنی بر ۴ دسته از سازوکارهای حقوقی طراحی نموده است:

۱. سازوکارهایی برای تسهیل استفاده مجدد از برخی از داده‌های بخش عمومی که نمی‌توانند به‌عنوان داده‌های باز در دسترس قرار گیرند. به‌عنوان مثال، استفاده مجدد از داده‌های بهداشتی می‌تواند تحقیقات را برای یافتن درمان بیماری‌های نادر یا مزمن ارتقاء دهد.
۲. سازوکارهایی برای اطمینان از اینکه واسطه‌های داده به‌عنوان سازمان‌دهندگان قابل‌اعتماد اشتراک‌گذاری یا ادغام داده‌ها در فضاهای داده مشترک اروپایی عمل خواهند کرد.

۱. این اصطلاح معادل (re-use) است که در بند (۲) ماده ۲ قانون حکمرانی داده بدین نحوه تعریف گردیده است: «استفاده مجدد به معنای استفاده اشخاص حقیقی یا حقوقی از داده‌های در اختیار نهادهای عمومی است و هدف آن هر موضوع تجاری یا غیرتجاری به جز آن هدف عمومی است که اساساً داده برای تحقق آن ایجاد گردیده است. انتقال داده بین نهادهای دولتی برای ایفای وظایف اداری مشمول این تعریف نخواهد بود.»

۳. سازوکارهایی برای اینکه شهروندان و کسب و کارها بتوانند داده‌های شخصی خود را در راستای منافع عمومی در اختیار دیگران بگذارند.

۴. سازوکارهایی برای تسهیل اشتراک‌گذاری داده‌ها در بین کشورهای عضو.

ابزارهای فوق شاکله اصلی قانون حکمرانی داده را تشکیل می‌دهد. در این گزارش ضمن بررسی چارچوب نظری قانون حکمرانی داده، طی ۴ بخش مفهوم و دلالت‌های قانونی هریک از این ابزارهای فوق تبیین می‌گردد.



۲) چارچوب نظری قانون حکمرانی داده

هدف اتحادیه اروپا از وضع قانون حکمرانی داده، ترویج اشتراک‌گذاری داده‌ها و تضمین اجرایی نمودن اصولی است که نظام سیاست‌گذاری اتحادیه اروپا، برای داده‌ها ترسیم کرده است. یافت‌پذیری^۱، دسترس‌پذیری^۲، هم‌کنش‌پذیری^۳ و قابل‌استفاده مجدد بودن^۴ داده‌ها - که به اختصار FAIR نامیده می‌شوند- اصولی هستند که ابتدا در مجامع علمی و دانشگاهی طرح و بررسی گردید و نهایتاً در «استراتژی اتحادیه اروپا برای داده»^۵ مورد اجماع مراجع تصمیم‌گیر در اتحادیه اروپا قرار گرفت. قانون حکمرانی داده به‌عنوان آخرین دستاورد قانون‌گذاری پارلمان اروپا

۱. Findable
۲. Accessible
۳. Interoperable
۴. Re-usable
۵. A European Strategy for Data

در موضوع داده، انطباق حداکثری با اصول FAIR را در دستور کار قرار داده است؛ به طوری که وبسایت اتحادیه اروپا در معرفی استراتژی اروپا برای داده، قانون حکمرانی داده را اساساً بخشی از فرایند تحقق این استراتژی قلمداد کرده است.^۱ در سال‌های اخیر سایر قوانین، مقررات و دستورالعمل‌هایی که از سوی اتحادیه اروپا مورد تصویب قرار گرفت، نشان می‌دهد که این اصول به‌عنوان یک سیاست تقنینی در حوزه داده‌ها، از سوی پارلمان اروپا اتخاذ گردیده است. لازم به ذکر است که سایر اسناد اخیرالتصویب در اروپا مانند مقررات عمومی حفاظت از داده‌های شخصی^۲، دستورالعمل داده‌های باز^۳، قانون خدمات دیجیتال^۴ و... از اصول مذکور تبعیت می‌نمایند.

در این قسمت اختصاراً مفهوم هر یک از اصول FAIR بیان می‌گردد^۵:

۱. **یافت‌پذیری:** گام نخست در استفاده از داده‌ها یافتن آن‌هاست. یافتن فراداده‌ها و داده‌ها باید برای انسان و رایانه امکان‌پذیر باشد. به همین منظور با استفاده از شناسه‌های جهانی مانند DOI جستجوی سریع داده امکان‌پذیر می‌گردد.
۲. **دسترس‌پذیری:** هنگامی که کاربر داده‌های موردنیاز را پیدا کرد، باید بداند چگونه می‌توان به آن‌ها دسترسی داشت. این مهم از طریق ایجاد یک پروتکل ارتباطی جهانی که به‌صورت رایگان و باز پیاده‌سازی می‌گردد، محقق می‌شود. پروتکل ارتباطی بایستی موارد ذیل را در خصوص داده‌ها و فراداده‌ها تأمین نماید:

۱. <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>; last seen at 2023-06-15.

۲. (EU) 2016/679

۳. (EU) 2019/1024

۴. (EU) 2022/2065

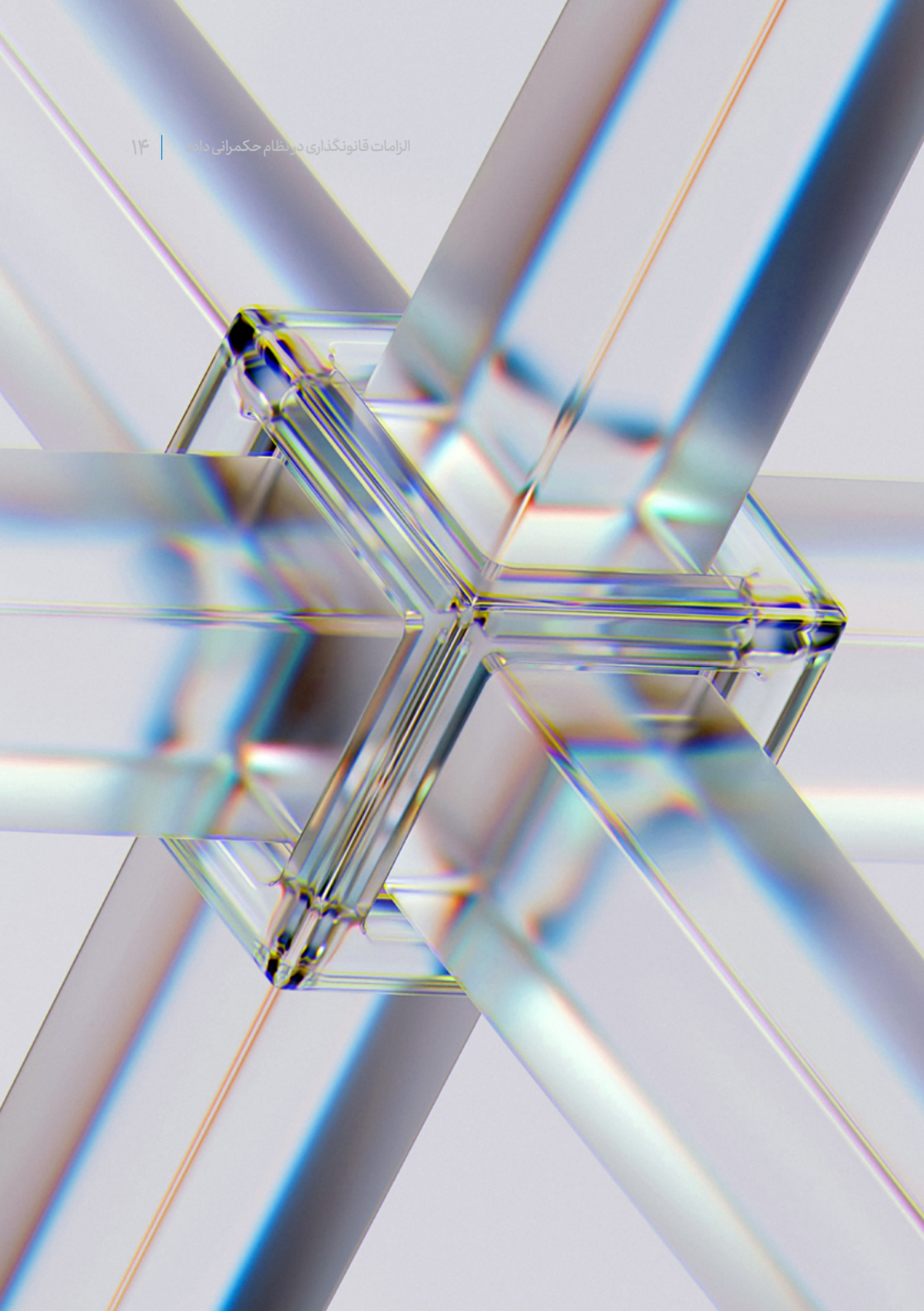
۵. Mark D. Wilkinson et al, (2016).

- داده یا فراداده را با استفاده از شناسه یکتای آن، قابل بازیابی نماید.
- امکانی برای احراز هویت و اخذ مجوز دسترسی به داده یا فراداده ایجاد کند.
- امکان دسترسی به فراداده را، حتی در صورت در دسترس نبودن داده فراهم نماید.

۳. **تعامل پذیری:** به این معنی که داده‌ها را بتوان با استفاده از فرمت‌های باز، در برنامه‌های کاربردی و سیستم‌های مختلف ردوبدل کرده و از آن استفاده نمود. همچنین براساس این اصل امکانی برای ادغام داده‌هایی که در یک موضوع و دسته‌بندی خاص قرار دارند، وجود داشته باشد.

۴. **قابل استفاده مجدد:** هدف نهایی اصول داده، بهینه‌سازی استفاده مجدد از داده‌ها است. برای دستیابی به این هدف، فراداده‌ها و داده‌ها باید با استفاده از ویژگی‌های زیر توصیف شوند تا امکان استفاده مجدد از آن‌ها تأمین گردد:

- داده به همراه مجوزهای دسترسی به آن منتشر گردد.
- منشأ داده مشخص گردد.
- داده با استانداردهای نام‌های دامنه منطبق باشد.





۳) داده‌های عمومی

منظور از این عنوان داده‌هایی است که توسط نهادهای عمومی جمع‌آوری گردیده و نگهداری می‌شوند. بند ۱۷ ماده ۲ قانون حکمرانی داده، در تعریف «نهاد عمومی» بیان می‌کند: «نهادهای حاکمیتی ملی، استانی یا محلی که براساس قوانین حقوق عمومی فعالیت می‌نمایند و همچنین نهادهای غیردولتی که توسط نهادهای حاکمیتی مذکور تأسیس یافته و براساس قوانین حقوق عمومی فعالیت می‌کنند». در دسترس قرار گرفتن داده‌هایی که توسط نهادهای عمومی نگهداری می‌شوند، مبتنی بر این اصل در حقوق اتحادیه اروپا است که نهادهای عمومی دولتی یا غیردولتی، به‌موجب بودجه عمومی کشورها اداره می‌شوند و داده‌هایی را که جمع‌آوری نموده‌اند در فرایند ارائه خدمات عمومی بوده است. لذا به همان ترتیبی که داده‌های مذکور از محل اعتبارات عمومی و ارائه خدمات عمومی به‌دست آمده است، عواید حاصل از آن نیز باید در اختیار عموم قرار گیرد. بند ۶ مقدمه قانون

حکمرانی داده ضمن بیان این اصل حقوقی در رویه قانون‌گذاری اتحادیه اروپا، قواعد دستورالعمل داده‌باز مصوب ۲۰۱۹ را نیز متکی به همان اصل می‌داند.

۱-۳ بیان موضوع

دستورالعمل داده‌های باز (EU) 2019/1024)) بخش زیادی از داده‌هایی را که دولت در اختیار دارد، در دسترس عموم قرار می‌دهد. در عین حال، دولت حجم زیادی از داده‌های محافظت‌شده (مانند داده‌های شخصی و داده‌های محرمانه تجاری) را در اختیار دارد که نمی‌توان آن‌ها را به‌عنوان داده‌های باز مجدداً استفاده کرد. اما می‌توان بدون به خطر انداختن ماهیت محافظت‌شده آن داده‌ها، از آن‌ها مجدداً استفاده نمود. فصل دوم قانون حکمرانی داده، امکان استفاده مجدد از این نوع داده‌ها را با تکلیف به کار بستن برخی ابزارهای محافظتی امکان‌پذیر می‌نماید.

الزام نهادهای عمومی به ارائه داده‌ها امری بی‌سابقه نبوده و در برخی از کشورهای اروپایی مطابق قوانین ملی، تکلیفی قانونی محسوب می‌گردد. به‌عنوان نمونه در حال حاضر در کشور فنلاند، پایگاه Findata به‌عنوان مرکز تبادل اطلاعات تخصصی در حوزه بهداشت فعالیت می‌کند. مؤسسات و نهادهای دولتی در حوزه بهداشت و تأمین اجتماعی در فنلاند مانند مؤسسه بیمه اجتماعی، نهاد ثبت احوال بازنشستگی و ثبت جمعیت این کشور وظیفه دارند، داده‌های عمومی را به این مرکز انتقال دهند. Findata نیز وظیفه دارد که درخواست‌های اشخاص حقیقی و کسب‌وکارها برای استفاده مجدد از داده‌ها را بررسی نموده و اجازه دسترسی به داده‌ها را در صورت احراز شرایط قانونی اعطا نماید.

ناگفته نماند که الزام نهادهای عمومی برای اشتراک‌گذاری داده‌های عمومی، مطلق نبوده و دارای استثنائاتی است که از آن جمله داده‌های شرکت‌های دولتی،

برودکسترها، مؤسسات فرهنگی، داده‌های آموزشی و مدارس، داده‌های نظامی و امنیتی و... را می‌توان ذکر نمود.

۲-۳) الزامات

- **الزامات فنی برای نهادهای عمومی:** قانون حکمرانی داده کشورهای عضو را ملزم می‌کند که نهادهایی را به منظور اعمال ابزارهای فنی بر داده‌هایی که از سوی نهادهای عمومی به اشتراک گذارده می‌شود، ایجاد نمایند. به موجب ماده (۷) قانون حکمرانی داده، این نهادها وظیفه دارند که به کار بستن طیف وسیعی از ابزارها مانند ابزارهای فنی از قبیل بی‌نام‌سازی^۱، مستعارسازی^۲ یا دسترسی به داده‌ها در محیط‌های پردازش امن (مانند اتاق‌های داده^۳) را در سامانه‌ها و داده‌های نهادهای عمومی تضمین کنند. یکی دیگر از ابزارهایی که به همین منظور در مقدمه ۱۱ قانون پیش‌بینی شده، الزام به انعقاد قراردادهای محرمانگی و فعال ساختن مسئولیت قراردادی اشخاصی است که داده‌ها را از نهادهای عمومی اخذ می‌کنند.
- **معاذت نهادهای عمومی:** باتوجه به اینکه بخش مهمی از داده‌ها مانند برخی از داده‌های شخصی و تمامی داده‌های مربوط به اسرار تجاری، تنها با جلب رضایت شخص یا اشخاص موضوع داده مجاز خواهد بود، ممکن است دولت بنا به محدودیت‌های قانونی یا امثالهم قادر به در اختیار گذاشتن این دسته از داده‌ها نباشد. در چنین مواقعی دولت‌های عضو به موجب جزء (c) بند (۲) ماده ۷ وظیفه دارند که کسب رضایت از اشخاص موضوع داده‌های فوق را برای استفاده‌کنندگان مجدد داده، تسهیل نمایند.

۱. Anonymisation
 ۲. Pseudonymisation
 ۳. Data Rooms

- **ممنوعیت انعقاد قراردادهای انحصاری:** برای اینکه داده‌های عمومی بیشتری برای استفاده مجدد در دسترس باشد، ماده ۴ قانون حکمرانی داده، نهادهای عمومی را از انعقاد قراردادهای انحصاری با استفاده‌کنندگان مجدد از داده منع می‌کند تا منافع حاصل از دسترسی به داده‌ها شامل عموم گردد.
- **هزینه معقول:** نهادهای عمومی به‌منظور در اختیار گذاشتن داده‌ها ممکن است درآمدهایی را از استفاده‌کنندگان مجدد از داده اخذ نمایند. این درآمدها نباید از هزینه‌های ضروری برای ایجاد دسترسی به داده‌ها تجاوز نماید. همچنین در خصوص استفاده مجدد در حوزه تحقیقات علمی و سایر اهداف غیرانتفاعی و همچنین استفاده استارت‌آپ‌ها و شرکت‌های نوپا، نهادهای عمومی نباید هزینه‌ای دریافت کنند.
- **مهلت پاسخ به درخواست:** نهاد عمومی حداکثر ۲ ماه فرصت دارد تا در مورد درخواست استفاده مجدد از داده تصمیم بگیرد.
- **نقطه دسترسی واحد اروپایی داده:** برای اینکه استفاده‌کنندگان مجدد داده به راحتی بدانند که چه اطلاعاتی توسط کدام یک از نهادهای عمومی نگهداری می‌شود، برابر حکم ماده ۸ قانون حکمرانی داده، کشورهای عضو ملزم به ایجاد یک نقطه اطلاعاتی واحد خواهند بود. کمیسیون برای تسهیل بیشتر استفاده مجدد از داده‌ها در بازار داخلی و فراتر از آن، یک نقطه دسترسی واحد اروپایی (با یک ثبت قابل جستجو از اطلاعات گردآوری شده توسط نقاط اطلاعات واحد ملی) ایجاد خواهد کرد.

Cost per conversion

573.27

+ 0.2%

Quality Score

9.38

↓ -0.1%

۴ خدمات واسطه‌گری داده

یکی دیگر از اجزای مهم قانون حکمرانی داده، نقش واسطه‌های داده^۱ است. در حال حاضر داده‌ها به‌عنوان محصول در فروشگاه‌های داده در اروپا معامله می‌شوند. اما این بازار اندازه کمی دارد و اتحادیه اروپا با استفاده از تعیین الزامات حاکم بر فعالیت در این حوزه، پیش‌بینی می‌کند که وسعت این بازار افزایش یابد.

۱-۴ بیان موضوع

در حال حاضر بسیاری از شرکت‌ها اشتراک‌گذاری داده‌های خود را برابر با از دست دادن مزیت رقابتی و خطر سوءاستفاده دیگران می‌دانند. قانون حکمرانی داده مجموعه‌ای از قوانین را برای ارائه‌دهندگان «خدمات واسطه‌گری داده» تعریف نموده است که براساس آن واسطه‌های مذکور به‌عنوان یک فعالیت اقتصادی حرفه‌ای و

۱. Data Intermediation Services

تحت نظارت و تنظیم‌گری نهادهای صالح دولتی عمل می‌کنند. واسطه‌های داده یک دسته جدید از ارائه‌دهندگان هستند که به اشتراک‌گذاری داده‌ها را تسهیل می‌کنند و هدف آن ایجاد روابط تجاری بین چندین دارنده داده^۱ و استفاده‌کنندگان از داده^۲ است.

در حال حاضر نیز در اروپا، داده‌ها به‌عنوان یک محصول در فروشگاه‌های داده معامله می‌شوند. به‌عنوان مثال یکی از مؤسساتی که در سطح اروپا، به ارائه خدمات واسطه‌ای داده اشتغال دارد، شرکت Dawex است که خود را به‌عنوان بازار داده جهانی توصیف می‌کند. البته این شرکت خود به‌صورت مستقیم به خرید و فروش داده‌ها نمی‌پردازد، بلکه صرفاً بازاری را فراهم کرده است تا عرضه‌کنندگان داده و استفاده‌کنندگان از داده بتوانند داده‌های موردنظر خود را خرید یا عرضه نمایند. به‌طور کلی شرکت‌هایی که در حال حاضر در موضوع ارائه خدمات واسطه‌ای داده توسعه یافته‌اند، در قالب یکی از دو دسته زیر فعالیت می‌کنند:

۱. **بازارهای داده:** شرکت‌هایی هستند که داده‌های عرضه‌شده توسط دارندگان داده را در معرض فروش می‌گذارند. علاوه بر Dawex بازارهایی مانند Microsoft Azure Marketplace، Statista یا Advaneo در همین دسته جای می‌گیرند.
۲. **پلتفرم‌های داده:** سرویس ارائه خدمات واسطه‌ای داده ممکن است به‌صورت یک پلتفرم ارائه گردد. در این صورت برعکس دسته قبل، مدیریت و فروش داده‌ها به‌صورت غیرمتمرکز و توسط خود کاربران انجام خواهد شد. کاربران این پلتفرم‌ها، داده‌های خود را در فضای ذخیره‌سازی پلتفرم به اشتراک گذاشته و در عوض از منابع داده‌ای اشتراکی پلتفرم استفاده می‌نمایند. علاوه بر این در اتاق‌های داده نیز کاربران می‌توانند داده‌های خود را به‌طور اختصاصی با یکدیگر به اشتراک بگذارند.

۱. Data Holders

۲. Data Users

قانون حکمرانی داده به این دسته‌بندی بی‌توجه بوده و مبنای تقسیم‌بندی انواع واسطه‌های داده را با رویکرد طرفین معامله داده و ماهیت انواع داده مورد معامله تقسیم نموده است. به موجب ماده ۹ قانون حکمرانی داده، واسطه‌گری داده شامل فعالیت‌های زیر می‌شود:

الف) ارائه سرویس واسطه‌ای داده فی‌مابین اشخاص حقوقی که داده‌ها را در اختیار دارند؛ استفاده‌کنندگان از داده

ارائه خدمات واسطه‌ای داده مطابق این بند شامل انتقال داده از شرکت‌های بزرگ فناوری می‌شود که حجم وسیعی از داده‌ها را در اختیار دارند. ایجاد پلتفرم یا پایگاه داده‌ای که اجازه بهره‌برداری استفاده‌کنندگان از داده را فراهم نماید، مشمول این بند از ماده ۹ است.

ب) ارائه سرویس واسطه‌ای فی‌مابین اشخاص موضوع داده‌ای که داده‌های شخصی خود را به اشتراک می‌گذارند؛ استفاده‌کنندگان از داده

الزامی که در خصوص این دسته از سرویس‌های واسطه‌ای داده وجود دارد، تکلیف آنان به رعایت الزامات GDPR است که شرایط سخت‌گیرانه‌ای را برای پردازش داده‌های شخصی ایجاد نموده است. با توجه به وسعت و عمومیت تعریف «پردازش» در GDPR، ارائه این سرویس واسطه‌ای مشمول مسئولیت‌های مربوط به کنترل‌گر داده می‌شود.

ج) انجمن (تعاونی) داده

تعاونی‌های داده از عضویت اشخاص موضوع داده، شرکت‌های کوچک فناوری اطلاعات و سایر اشخاص حقوقی تشکیل می‌گردد. تعاونی به نمایندگی از اشخاص موضوع داده و شرکت‌ها، در خصوص شرایط انتقال و پردازش داده‌های اشخاص مزبور، اهداف پردازش داده و نحوه اعطای رضایت شخص موضوع داده، با استفاده‌کنندگان از داده مذاکره می‌نماید.

۲-۴) الزامات

تکلیف ارائه‌دهندگان خدمات واسطه‌ای داده مطابق ماده ۱۱ قانون حکمرانی داده تعیین گردیده است که در محورهای زیر قابل بررسی است:

- **مجوز فعالیت:** واسطه‌های داده مکلف‌اند که قصد خود را برای ارائه خدمات واسطه‌ای داده، به نهاد صالح ملی اعلام کنند. نهاد صالح ملی نیز مکلف است در رسیدگی به اعلام ارائه‌دهنده خدمات واسطه‌ای داده، اصل عدم تبعیض را رعایت نماید. پس از تأیید اعلام از سوی نهاد صالح ملی، ارائه‌دهنده خدمات واسطه‌ای می‌تواند فعالیت خود را به صورت قانونی آغاز کند. وی همچنین ملزم است تا از نماد «ارائه‌دهنده خدمات واسطه‌ای ثبت شده در اتحادیه» در تمامی مکاتبات و فعالیت‌های تجاری خود استفاده کند.
- **تک خدمتی بودن سرویس اشتراک‌گذاری:** ماده ۱۱ هرگونه استفاده از داده برای سرویس واسطه‌ای را ممنوع نموده است. براین اساس ارائه‌دهنده خدمت واسطه‌ای بایستی از لحاظ حقوقی تنها موضوع فعالیت شرکت خود را ارائه خدمات واسطه‌ای قرار دهد. سرویس واسطه‌ای مجاز نیست خود از داده‌ها استفاده نماید و صرفاً باید داده را به دیگران (استفاده‌کنندگان) انتقال دهد.
- **شرایط استفاده از فراداده:** فراداده‌ای که در نتیجه ارائه سرویس واسطه‌ای و در بستر عملیات انتقال داده از دارندگان داده، برای ارائه‌دهنده سرویس واسطه‌ای حاصل گردیده است، صرفاً بایستی برای توسعه همان سرویس واسطه‌ای استفاده گردد.
- **اصول حاکم بر ارائه سرویس:** این اصول شامل اصل انصاف، شفافیت، عدم تبعیض در دسترسی به خدمات و قیمت عادلانه خدمات واسطه‌ای می‌باشد که بایستی در خصوص دارنده داده و استفاده‌کننده از داده رعایت گردد.

- **تعامل‌پذیری داده:** با هدف تعامل‌پذیری^۱ داده‌ها، ارائه‌دهنده سرویس واسطه‌ای مکلف است داده‌هایی را که از دارندگان داده دریافت می‌کند، به فرمت‌هایی که توسط دستورالعمل‌های اتحادیه یا قوانین و مقررات ملی اعلام می‌گردد، تبدیل کند.
- **استمرار خدمات:** ارائه‌دهنده سرویس واسطه بایستی تداوم فعالیت خود را تضمین نماید. به‌موجب این تکلیف، کشورهای عضو می‌توانند در قوانین خود ضمانت‌نامه‌هایی را برای ارائه‌دهندگان این سرویس‌ها تعیین نمایند.
- **داده‌های غیرشخصی:** در خصوص داده‌های غیرشخصی که انتقال آن‌ها به‌موجب قوانین اتحادیه اروپا، غیرمجاز محسوب می‌گردد، ارائه‌دهنده سرویس واسطه‌ای مکلف است تمهیدات فنی، قانونی و قراردادی و حفاظت سازمانی لازم را به‌منظور حفاظت از آن داده‌ها انجام دهد. لازم به توضیح است که منظور از داده‌های غیرشخصی در این حکم، داده‌هایی است که خارج از شمول GDPR بوده لیکن به‌موجب سایر اسناد و قوانین مستلزم حفاظت و محرمانگی است، مانند اسرار تجاری.
- **اقدامات فنی:** سرویس واسطه‌ای باید تمامی استانداردهای فنی ابلاغی از سوی نهاد صالح ملی را در خصوص ذخیره‌سازی و نگهداری از داده و همچنین انتقال داده، پیاده‌سازی کند.
- **رقابت:** ارائه‌دهنده سرویس باید رعایت الزامات رقابت و رویه‌های اتخاذی در این خصوص را تضمین کند. به‌عنوان مثال براساس اصول رقابت در اتحادیه اروپا، ارائه‌دهنده سرویس واسطه‌ای داده، مجاز نیست که قیمت خدمات خود را برای مشتریانی که از خدمات سایر سرویس‌های رقیب نیز استفاده می‌کنند، افزایش دهد.

۱. Interoperability





۵) داده عام‌المنفعه

مؤسسات داده عام‌المنفعه، فعالیت چشمگیری در اروپا ندارند و هنوز استقبال چندانی از این مؤسسات از سوی مردم به عمل نیامده است. اما قانون حکمرانی داده با وضع موادی، به صورت تفصیلی تکالیف این دسته از فعالان حوزه داده را تعیین نموده است. پارلمان اروپا با این ابتکار عمل به دنبال افزایش دسترسی به داده با اهداف غیرتجاری، به صورت رایگان و در خدمت منافع عمومی است.

۱-۵) بیان موضوع

پارلمان اروپا در قانون حکمرانی داده مفهوم جدیدی را در خصوص داده وضع نموده است که هدف از آن ترغیب به اشتراک‌گذاری رایگان داده از سوی دارندگان آن، با اهداف بشردوستانه و عام‌المنفعه بوده است. براساس فصل چهارم از

قانون، داده‌عام‌المنفعه در مورد افراد و شرکت‌هایی است که رضایت یا اجازه خود را برای در دسترس قرار دادن داده‌هایی که تولید می‌کنند؛ به صورت داوطلبانه و رایگان، جهت استفاده در راستای منافع عمومی در دسترس استفاده‌کنندگان از داده قرار می‌دهند. چنین داده‌هایی پتانسیل بسیار زیادی برای پیشبرد تحقیق و توسعه محصولات و خدمات بهتر از جمله در زمینه‌های بهداشت، محیط‌زیست و حمل‌ونقل دارد. به‌عنوان مثال Smart Citizen پلتفرمی است که به منظور جمع‌آوری داده‌های زیست‌محیطی با هدف ارائه این اطلاعات به مراجع دولتی و سیاست‌گذاری تشکیل شده است. کاربران سنسورهایی را در محیط زندگی خود قرار می‌دهند و رضایت می‌دهند که داده‌های ضبط شده بوسیله سنسورها مانند وضعیت جوی، آلاینده‌ها، آلودگی صوتی و ... را به پایگاه داده این پلتفرم ارسال نمایند!

تحقیقی که در سراسر اتحادیه اروپا انجام پذیرفته است، حاکی از آن است که شرکت‌ها و اشخاص حقیقی در اصل تمایل به اشتراک‌گذاری داده‌های خود را دارند، لیکن در عمل به دلیل فقدان سازوکاری قانونی که نظارت کافی بر استفاده از داده داشته باشد، تحقق این امر با مانع روبرو می‌شود. به این ترتیب، هدف قانون حاکمیت داده، ایجاد ابزارهای قانونی قابل‌اتکایی است که امکان اشتراک‌گذاری داده‌ها با اهداف عام‌المنفعه را به روشی آسان فراهم می‌کند. پارلمان اروپا ادعا دارد احکام فصل چهارم قانون حکمرانی داده این تضمین را به اشخاص حقیقی و حقوقی می‌دهد که داده‌هایی که در دسترس دیگران قرار می‌دهند، توسط نهادهای قانونی، براساس اصول اتحادیه اروپا مدیریت می‌شود. پیش‌بینی می‌شود، بستری که قانون حکمرانی داده برای تحقق داده‌عام‌المنفعه ایجاد می‌کند، حجم عظیمی از داده را در اختیار فناوری‌های مبتنی بر هوش مصنوعی قرار دهد تا امکان تجزیه و تحلیل داده‌ها و یادگیری ماشین، در سراسر اتحادیه اروپا فراهم شود.

۵-۲) الزامات

۵-۲-۱) الزامات ناظر بر تأسیس و فعالیت:

- **ثبت نام:** مؤسساتی که داده‌های عام‌المنفعه را جمع‌آوری می‌کنند، بایستی در سامانه‌های ملی که کشورهای عضو به همین منظور راه‌اندازی می‌کنند، ثبت‌نام نموده و نمایندگان قانونی و مشخصات شرکت خود را ثبت کنند. این شرایط در بند ۴ ماده ۱۹ قانون حکمرانی داده ذکر شده است که شامل اطلاعاتی همچون نام مؤسسه، وضعیت حقوقی، اساسنامه، درآمد و منابع مالی، آدرس دفتر مرکزی و... است. کمیسیون اروپایی به‌منظور تسهیل در شناسایی این مؤسسات، لوگو یا نماد واحدی را برای مؤسساتی که در زمینه داده‌های عام‌المنفعه فعالیت می‌کنند، تعیین می‌نماید. نماد مذکور به همراه یک کد QR امکان اتصال به سامانه یکپارچه استعلام مؤسسات عام‌المنفعه داده و شناسایی هریک از آن مؤسسات را فراهم خواهد کرد.
- **تک‌خدمتی بودن سرویس داده عام‌المنفعه:** همان الزامی که در خصوص سرویس‌های واسطه‌ای داده مطرح شد، برابر ماده ۱۸ قانون، بر مؤسسات عام‌المنفعه نیز حاکم است. در صورتی که واحدی چندین خدمت و از جمله سرویس عام‌المنفعه داده را ارائه می‌دهد، بایستی سرویس اخیر را از لحاظ استقلال حقوقی از سایر خدمات خود تفکیک نماید.
- **غیرانتفاعی بودن:** ارائه این سرویس بایستی به‌صورت غیرانتفاعی باشد، به عبارتی مؤسسات مذکور که داده‌ها را به‌صورت رایگان از اشخاص دریافت می‌کنند، باید آن را به‌صورت رایگان در اختیار استفاده‌کنندگان از داده قرار دهند.
- **شفافیت:** الزامات مربوط به شفافیت در قانون حکمرانی داده، در دو موضوع ثبت سوابق و گزارش سالانه وضع شده است.

- **ثبت سوابق:** مؤسسه عام المنفعه بایستی سوابق ذیل را ثبت کند تا در صورت درخواست مقام ذیصلاح در اختیار وی بگذارد:
 - مشخصات اشخاص حقیقی یا حقوقی که داده‌های عام المنفعه در دسترس آنان قرار گرفته است؛
 - تاریخ انتقال داده؛ و مدت زمانی که از داده استفاده نموده‌اند
 - هدفی که برای پردازش داده اعلام نموده‌اند؛
 - هزینه‌هایی که از سوی استفاده‌کنندگان از داده به مؤسسه پرداخت گردیده است.
- **گزارش سالانه:** گزارش سالانه حاوی شرحی از موارد زیر می‌باشد که بایستی در پایان سال مالی به نهاد ذیصلاح ملی ارائه گردد:
 - فعالیت مؤسسه در طول سال، اهداف عمومی که داده‌ها به منظور تحقق آن جمع‌آوری گردیده است؛
 - گزارشی از اهداف عمومی استفاده‌کنندگان مجدد داده؛ تکنیک‌ها و ابزارهای فنی که برای حفاظت از حریم خصوصی و رعایت الزامات حفاظت از داده‌های شخصی در سند GDPR مورد استفاده مؤسسه.
 - گزارشی از منابع مالی مورد استفاده مؤسسه عام المنفعه.

۵-۲-۲) الزامات ناظر بر حفاظت از حقوق اشخاص موضوع داده و دارندگان داده

قانون حکمرانی داده به موجب ماده ۲۱، تکالیفی را برای مؤسسات عام‌المنفعه داده ایجاد کرده است تا حفاظت از حقوق اشخاص موضوع داده‌های شخصی و همچنین سایر دارندگان داده را تضمین کند:

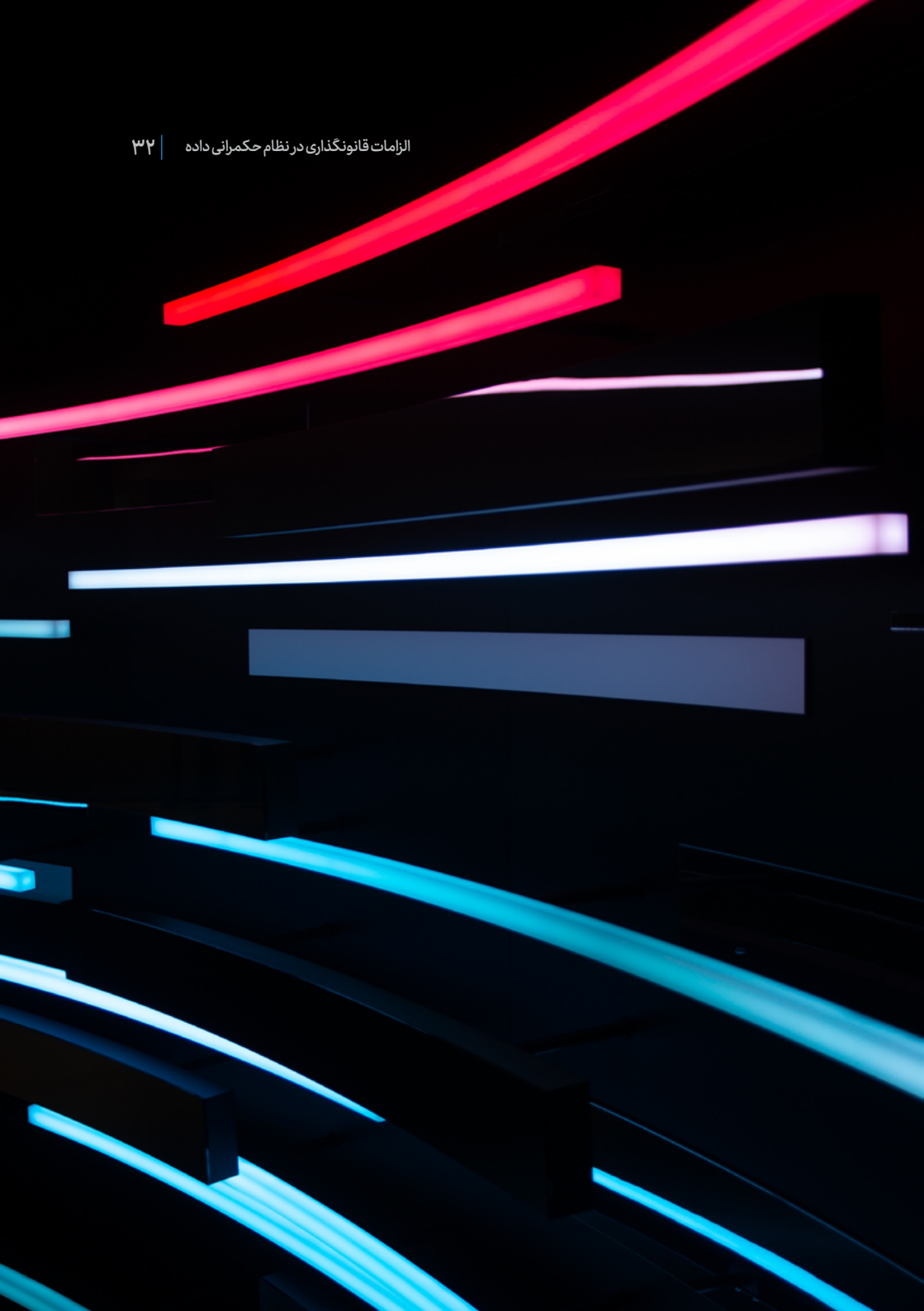
- **حق انصراف از رضایت:** مؤسسه عام‌المنفعه بایستی حق انصراف از رضایت شخص موضوع داده و دارنده داده را به رسمیت بشناسد.
- **حق آگاهی:** مؤسسه عام‌المنفعه باید هدف عمومی را که از پردازش داده دنبال می‌کند، به اشخاص موضوع داده یا دارندگان داده اطلاع دهد. وجه دیگر حق آگاهی اشخاص موضوع داده یا دارندگان داده، زمانی است که مؤسسه عام‌المنفعه از پردازش غیرمجاز یا خلاف رضایت آنان اطلاع یابد. در این صورت مکلف است جزئیات این موضوع را به اشخاص موضوع داده شخصی یا دارندگان داده غیرشخصی اطلاع دهد.
- **هدف عمومی:** مؤسسه عام‌المنفعه تنها برای اهداف عمومی حق جمع‌آوری و پردازش داده را دارد. حتی در صورتی که این داده در اختیار استفاده‌کنندگان داده نیز قرار می‌گیرد، مؤسسه عام‌المنفعه ملزم است که هدف عمومی استفاده‌کننده از داده را بررسی و احراز نماید.
- **اقدامات فنی:** مؤسسه عام‌المنفعه باید تمامی استانداردهای فنی ابلاغی از سوی نهاد صالح ملی را در خصوص ذخیره‌سازی و نگهداری از داده و همچنین انتقال داده را پیاده‌سازی نماید.





۶ جریان‌های بین‌المللی داده

پیش از قانون حکمرانی داده، الزامات GDPR در خصوص هرگونه درخواست دسترسی از سوی کشورهای ثالث به داده‌های شخصی در اروپا، لازم‌الرعايه بود. حال قانون حکمرانی داده، الزامات اتحادیه اروپا در خصوص دسترسی کشورهای ثالث به داده‌های غیرشخصی را نیز، لازم‌الاتباع دانسته است. قانون حکمرانی داده استفاده‌کنندگان داده از کشورهای غیرعضو را ملزم به تبعیت از تکالیف قانونی اتحادیه اروپا در زمینه محافظت از داده‌های اروپایی کرده است. این تکلیف تنها در بعد تنظیم مقررات خلاصه نمی‌شود و کشورهای ثالث به شرطی می‌توانند از داده‌های اروپایی استفاده کنند که صلاحیت قضائی مراجع اروپایی را در رسیدگی به دعاوی و تخلفات پذیرفته باشند. نقطه مقابل این امر نیز در خصوص هرگونه اعمال صلاحیت مراجع اداری و دادگاه‌های کشور ثالث در موضوع داده‌های اروپایی نامعتبر قلمداد گردیده است. البته طبق ماده ۳۱ قانون حکمرانی داده، حاکمیت قوانین اتحادیه اروپا و صلاحیت قضائی آن، در صورت وجود یک توافقنامه دو یا چند جانبه مستثنی گردیده است.



REGULATIONS

RULES

۷) مقام صالح ملی (تنظیم‌گر)

براساس قانون حکمرانی داده، اجرای الزامات این قانون در وهله اول برعهده نهادهایی است که به موجب قانون، تعیین گردیده و در هریک از حوزه‌های مقرر در این قانون به تنظیم مقررات و نظارت بر اجرای قانون خواهند پرداخت. نظارت بر پردازش داده‌های شخصی نیز مطابق همان سازوکار قبلی خواهد بود که به موجب GDPR برعهده کشورهای عضو قرار گرفته است.

- **مجوزدهی:** صلاحیت مجوزدهی جهت آغاز و ادامه فعالیت انواع سرویس‌های داده‌ای که در این قانون ذکر شد، برعهده نهاد صالح ملی قرار دارد. به عنوان مثال مطابق ماده ۱۷ قانون حکمرانی داده، در خصوص مؤسسات عام‌المنفعه داده، نهادهای صالح ملی وظیفه دارند شرایط درخواست‌کننده ارائه خدمات عام‌المنفعه داده را بررسی و در صورت احراز شرایط لازم درخواست آنان را تأیید

نمایند. در این صورت مؤسسه عام‌المنفعه می‌تواند به‌عنوان یک مؤسسه ثبت‌شده در سراسر اتحادیه اروپا فعالیت نماید.

- **انطباق:** نهادهای ملی همچنین وظیفه نظارت بر انطباق^۱ فعالیت سرویس‌های ثبت‌شده در اتحادیه اروپا با الزامات قانونی و تکالیفی قانون حکمرانی داده و سایر قوانین از جمله GDPR را برعهده دارند. مطابق ماده ۲۴ قانون حکمرانی داده، در صورتی که مؤسسه عام‌المنفعه داده پس از اخطار از سوی نهاد ملی، تخلف ارتكابی را رفع نکند، نهاد صالح ملی مجوز آن شرکت را ابطال می‌نماید که در این صورت مؤسسه موردنظر حق استفاده از نماد (لوگو) اعطایی از سوی اتحادیه اروپا را نخواهد داشت.

- **رسیدگی به شکایات:** نهادهای ملی مرجع رسیدگی به شکایات از عملکرد مؤسسات واسطه‌ای، عام‌المنفعه و نهادهای دولتی در خصوص داده‌های عمومی خواهد بود. قانون حکمرانی داده مجالس قانون‌گذاری ملی را مکلف نموده است که در ملی‌سازی قانون حکمرانی داده، صلاحیت اعمال جریمه‌های مناسب و کافی را برای نهادهای صالح ملی موضوع این قانون قرار دهند. باین‌حال، اگر موضوع نقض در مورد پردازش داده‌های شخصی باشد، براساس مقررات (GDPR) عمل خواهد شد.

CONCLUSION

۱) جمع‌بندی

۱. اتحادیه اروپا به دنبال تسهیل استفاده از داده‌ها به منظور توسعه اقتصاد دیجیتال و تحقق اهداف اجتماعی و خدمات شهری است. این سیاست در سند «استراتژی اروپا برای داده» در سال ۲۰۱۹ توسط شورایی از ارکان اصلی اتحادیه اروپا، اتخاذ گردید. براساس این سند، اصول داده FAIR سیاست‌های فوق‌الذکر برای اتحادیه اروپا را عملی خواهد ساخت. لذا قانون حکمرانی داده براساس اصول چهارگانه یافت‌پذیری، دسترس‌پذیری، تعامل‌پذیری و قابلیت استفاده از داده، بنیان نهاده شد. بدین معنا که قواعد مندرج در قانون حکمرانی داده تحقق اصول مذکور را با استفاده از ابزارهای قانونی مندرج در این سند، الزام‌آور نموده است.
۲. در دسترس قرار دادن داده‌های نهادهای عمومی، براساس اصلی در حقوق اتحادیه اروپا که استفاده مجدد از داده‌های حاصله از هزینه‌کرد بودجه عمومی را الزام‌آور می‌داند، در قانون حکمرانی داده پیش‌بینی گردیده است. این مهم

از طریق الزام نهادهای عمومی و استفاده‌کنندگان مجدد از داده به رعایت استانداردهای فنی و ایمنی در تبادل و نگهداری داده، ممنوعیت انعقاد قراردادهای انحصاری انتقال داده برای نهادهای عمومی، معاضدت نهادهای عمومی برای کسب رضایت استفاده مجدد از داده، تعیین مهلت پاسخ به درخواست‌های داده از نهادهای عمومی، تعیین قاعده اخذ هزینه معقول در قبال در اختیار نهادن داده و همچنین ایجاد یک پایگاه واحد برای یافت‌پذیری داده‌ها تحقق می‌یابد.

۳. خدمات واسطه‌گری داده، به‌عنوان یک بازار نوظهور و حائز اهمیت در اتحادیه اروپا ملزم به اعلام فعالیت و کسب تأیید نهادهای صالح ملی گردیده‌اند. علاوه بر این رعایت الزامات و استانداردهای فنی از سوی نهاد تنظیم‌گر ملی، التزام به اصل تعامل‌پذیری در ارائه داده‌ها، رعایت اصول شفافیت و ... برای ارائه‌دهندگان خدمات واسطه‌ای الزام‌آور شده است.

۴. مؤسسات داده‌عام‌المنفعه داده‌های شخصی و غیرشخصی را به‌صورت رایگان برای استفاده در اهداف منافع عمومی دریافت می‌نمایند. این مؤسسات در حال حاضر به‌صورت محدود فعالیت می‌کنند که ابتکارات قانون حکمرانی داده و قانونی نمودن فعالیت در حوزه داده‌عام‌المنفعه، سبب توسعه این مؤسسات خواهد شد. به دلیل غیرانتفاعی بودن این سرویس و امکان سوءاستفاده بیشتر از اهداف خیرخواهانه اشخاص موضوع داده در این سرویس، پارلمان اروپا اهداف سخت‌گیرانه‌ای را برای فعالیت این مؤسسات در نظر گرفته است که در دو محور الزامات ناظر بر تأسیس و فعالیت و الزامات ناظر بر حفاظت از داده‌های شخصی تقسیم می‌شود. در احکام مربوط به فعالیت، افزون بر الزاماتی که برای واسطه‌های داده ذکر شد، مؤسسات عام‌المنفعه ملزم به ثبت سوابق و ارائه گزارش‌های سالانه به نهاد تنظیم‌گر ملی هستند. همچنین حق آگاهی از پردازش، حق انصراف از پردازش و استفاده

از داده در راستای اهداف عمومی حقوقی است که مؤسسات عام‌المنفعه بایستی در قبال اشخاص موضوع داده و دارندگان داده رعایت کنند.

۵. در خصوص انتقال فرامرزی داده به خارج از اتحادیه اروپا، اصل بر غیرقانونی بودن انتقال داده و ارائه خدمات موضوع قانون حکمرانی داده به کشورهای ثالث می‌باشد. البته امکان استثنا از این اصل در صورت انعقاد موافقت‌نامه‌های دو یا چندجانبه پیش‌بینی گردیده است.





۹) پیشنهاد سیاستی

حکمرانی داده در ایران مفهومی نوپدید محسوب می‌شود که در حال حاضر به صورت محدود در سطح مجامع علمی و دانشگاهی طرح گردیده است و هنوز در دستور کار مراجع سیاست‌گذاری و قانون‌گذاری کشور قرار نگرفته است. حکمرانی داده یک خط‌مشی کلان و راهبردی نسبت به داده و نحوه مدیریت آن محسوب می‌گردد و نقش اساسی در توسعه اقتصاد دیجیتال ایفا می‌کند. همان‌طور که ذکر شد، اتحادیه اروپا نیز پیش از آن‌که قانون حکمرانی داده را وضع نماید، استراتژی اروپا برای داده را در سال ۲۰۱۹ تصویب و خطی‌مشی‌ها و رویکردهای کلان نسبت به نحوه مدیریت و حکمرانی داده را تعیین کرده است. لذا در ایران نیز پیش از آنکه مجلس شورای اسلامی یا نهادهای اجرایی کشور در این خصوص به وضع هنجارهای عمومی بپردازند، بایستی شورای عالی فضای مجازی به عنوان نقطه کانونی سیاست‌گذاری در فضای مجازی کشور، رویکرد نظام حکمرانی ایران را نسبت به نحوه مدیریت داده را تعیین نماید.

موضوع دیگر، ضرورت ایجاد نظام جامعی از قوانین و مقررات در حوزه داده است که هریک نقش مکمل یا پیش‌نیاز را برای قانون حکمرانی داده ایفا می‌کنند. قانون‌گذاری اتحادیه اروپا در خصوص مدیریت داده، با یک سیر منطقی از سال ۱۹۹۵ و هم‌زمان با تصویب دستورالعمل حفاظت از داده^۱، آغاز گردید و پس از آن قوانین و مقررات متعددی را در موضوعات مرتبط با داده تصویب نمود. قانون حکمرانی داده نیز به‌عنوان آخرین دستاورد قانون‌گذاری پارلمان اروپا در این موضوع، به‌صورت صریح ارجاعات متعددی را به قوانین و مقررات سابق اتحادیه اروپا مانند دستورالعمل داده‌های باز، مقررات عمومی حفاظت از داده‌های شخصی، قوانین طبقه‌بندی اسناد دولتی و... می‌دهد.

لذا مدیریت داده، موضوعی نیست که بتوان با صرف‌نظر از سایر موضوعات و به‌صورت مستقل قانونی در خصوص آن تصویب نمود و انتظار اجرایی شدن آن را داشت. با درنظر گرفتن موضوع فوق، به نظر می‌رسد که بحث از تصویب چنین قانونی در ایران با دشواری‌های فراوانی همراه خواهد بود. زیرا در ایران حتی قوانین سنتی که مبنای بسیاری از قوانین و مقررات فضای مجازی قرار می‌گیرد، هنوز به تصویب نرسیده است. ازجمله می‌توان قوانین اسرار دولتی، حریم خصوصی، اسرار تجاری، مالکیت فکری و... را نام برد که پایه‌های هرگونه قاعده‌گذاری در موضوعات نوین فضای مجازی و فناوری اطلاعات محسوب می‌گردند. به همین ترتیب قوانین حفاظت از داده‌های شخصی، باز بودن داده، سرویس‌های دیجیتال و... نیز هنوز در ایران طرح و تصویب نشده است. با عنایت به همین موضوع پیش‌بینی می‌شود که تصویب قانون حکمرانی داده در ایران به دلیل عدم تمهید بسترهای لازم در نظام حقوقی کشور، قابلیت اجرایی نخواهد یافت.

۱. Directive 95/46/EC

۱۰ منابع

1. Leistner, M. (2021). The Commission's vision for Europe's digital future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer. *Journal of Intellectual Property Law & Practice*, 16(8), 778-784. <https://doi.org/10.1093/jiplp/jpab054>
2. “Data Governance Act: Mediating between the EU Regulations and the Industry – Gaia-X: A Federated Secure Data Infrastructure.” 2022. <https://gaia-x.eu/news/latest-news/data-governance-act-mediating-between-the-eu-regulations-and-the-industry/> (June 21, 2023).
3. “Knowledge Centre Data & Society – European Union – Data Governance Act.” <https://data-en-maatschappij.ai/en/policy-monitor/europese-unie-data-governance-act> (June 21, 2023).

4. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance). 2022. 152 OJ L <http://data.europa.eu/eli/reg/2022/868/oj/eng> (June 22, 2023).
5. Richter, Heiko. 2023. "Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing." *GRUR International* 72(5): 458-70.
6. Ruohonen, Jukka, and Sini Mickelsson. 2023. "Reflections on the Data Governance Act." *Digital Society* 2(1): 1-9.
- 7.
8. Ruohonen, J., Mickelsson, S. Reflections on the Data Governance Act. *DISO* 2, 10 (2023). <https://doi.org/10.1007/s44206-023-00041-7>
9. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) 2022)
10. Heiko Richter, Dr, Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing, *GRUR International*, Volume 72, Issue 5, May 2023, Pages 458-470, <https://doi.org/10.1093/grurint/ikad014>

11. Mark D. Wilkinson; Michel Dumontier; IJsbrand Jan Aalbersberg; et al. (15 March 2016). "The FAIR Guiding Principles for scientific data management and stewardship". *Scientific Data*. 3 (1): 160018. doi: 10.1038/SDATA.2016.18
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
13. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information
14. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
15. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data
16. <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>; last seen at 2023-06-15.
17. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

پایان

نگاهی نو،
به حکمرانی فضای مجازی



تهران، ضلع غربی میدان فلسطین، خیابان آیت الله طالقانی، پلاک ۳۹۷
۰۲۱-۸۶۰۵۴۲۹۱

www.zaviehmag.ir

[@zaviehmag](#)

نشانی

تلفن

وبسایت

شبکه‌های اجتماعی