سال چهاردهم، شماره‌های ۵۱ و ۵۲ ، بهار و تابستان ۱۴۰۱

صص: ۱۷_۳۵

دو فصلنامه علمی

فناوری اطلاعات و ارتباطات ایران

سیاست‌گذاری دسترسی به داده‌های باز در داخل کشور از منظر صیانت از حریم خصوصی و مالکیت داده‌های شخصی

بهروز الیاسی* معصومه صادقی** نسرین دسترنج* مهدی حسین‌پور* طاهره میرسعیدقاضی**

*عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات

**پژوهشگر پژوهشگاه ارتباطات و فناوری اطلاعات

تاریخ دریافت: ۱۳۹۹/۱۲/۰۴ تاریخ پذیرش: ۱۴۰۰/۰۶/۰۳

نوع مقاله: پژوهشی

چکیده

تقویت دسترسی به داده‌های باز تضمینی برای باروری امر پژوهش و نوآوری و توسعه راهکارهای مقابله با چالش‌های پیچیده اجتماعی در داخل کشور است. سیاست‌های پیشنهادی OECD[۱] و دیگر محافل علمی، تاکیدی بر این راهبرد است. اما پیاده‌سازی آن‌ها قطعاً نیازمند برپایی سیستم‌های حکمرانی، فرایندهای شفاف‌سازی، و تضمین اعتماد به حوزه‌های پژوهشی و کسب‌وکاری است. بخش عمده و مهمی از ارزشمندترین منابع داده‌ای ماهیت شخصی دارند و گردآوری، ذخیره و پردازش آنها در فضای مجازی منبع سرشار درآمدزایی برای کسب‌وکارهای داده‌محور محسوب می‌گردد. از جمله چالش‌های اصلی در مسئله اعتمادسازی، اتخاذ سیاست‌های حفظ حریم خصوصی و تعیین حدود مالکیت این داده‌هاست. این مقاله با تبیین پیچیدگی مفهوم مالکیت در زیست‌بوم داده‌های شخصی، کارامدی سیاست‌های پیشنهادی همچون گزارشات OECD در زمینه تقویت دسترسی باز را به چالش می‌کشد. همچنین، به اجمال کاستی‌های موجود در قوانین تجارت الکترونیکی و جرائم رایانه‌ای کشور مطرح می‌شود. سپس، با هدف پیشنهاد یک سیاست دسترسی به داده‌های باز، عطف به حساسیت داده‌های شخصی، ابتدا نتایج تفصیلی یک مطالعه میدانی شامل معیارهای تحقق هدف و سیاست‌گذاری‌های ممکن به شیوه دلفی استخراج می‌گردند. پژوهش انجام شده حاکیست سطح آگاهی عمومی در کشور از قوانین حمایت‌کننده موجود در این زمینه، حتی در یک جامعه هدف متعالی، از وضع مطلوبی برخوردار نیست. همچنین، دیدگاه عمومی از امانتداری نسبت به داده‌های شخصی و امید به اجرای موثر قوانین در موارد تخلف رضایت‌بخش نیست. در انتها، با ارزیابی مجدد میدانی به شیوه FAHP[۲]، گزینه‌های سیاست‌گذاری مورد سنجش و تحلیل قرار می‌گیرند و الزامات ضروری برای اجرای سیاست منتخب پیشنهاد می‌شوند.

واژگان کلیدی: سیاست‌گذاری، دسترسی، داده‌های شخصی، حریم خصوصی، مالکیت.

۱. مقدمه

اهمیت داده‌ها برای علم، فناوری و نوآوری(STI[۳]) در دهه آینده بدون شک مسیر فزاینده‌ای را در پیش می‌گیرد. حجم داده‌های تولیدشده در کل جهان رقمی بالغ بر ۱۶ ZB تا سال ۲۰۱۶م. بوده که پیش‌بینی می‌شود تا ۲۰۲۵م. به ۱۶۳ ZB برسد. همچنین انتظار می‌رود اهمیت هوش مصنوعی در استفاده از این داده‌ها و کشفیات علمی جدید به رشد قابل‌ملاحظه‌ای برسد.

در سال‌های اخیر مفهومی بنام «داده‌های دولتی باز[۴]» در محافل علمی مورد توجه قرار گرفته که تعریف آن و شیوه‌های طبقه‌بندی و دسترسی به آن‌ها هنوز محل بحث است. اما بر سر این موضوع اتفاق-

نویسنده مسئول: بهروز الیاسی eliasi@itrc.ac.ir

[۱] Organization for Economic Co-operation and Development
[۲] Fuzzy Analytic Hierarchy Process
[۳] Science, Technology and Innovation
[۴] Open Government Data

نظر وجود دارد که تقویت دسترسی به داده‌های باز تضمین قابل‌توجهی برای افزایش باروری امر تحقیق و نوآوری، و توسعه راهکارهایی برای مقابله با چالش‌های پیچیده اجتماعی فراهم می‌آورد. اینکه داده‌های پژوهشی چه زمانی، چگونه و تحت چه شرایطی باید در دسترس قرار بگیرند، جزء پرسش‌های مهم از مقوله سیاست دسترسی و از زمره دغدغه‌های OECD بشمار می‌آید.

امروزه ورود مراکز رشد نیز به عنوان همراه نهادهای دولتی برای تهیه و/یا فراهم‌سازی داده‌های باز و فعال شدن کسب و کارهای سودمند مبتنی بر این داده‌ها توسط استارت‌آپ‌ها و شرکت‌های SME[1]، اکوسیستم تولید خدمات و محصولات مبتنی بر داده‌های باز را گسترده‌تر و فرایندهای حقوق مالکیت فکری را پیچیده‌تر نموده است[۱-۳]. این موضوع، اهمیت نیاز به تدوین برنامه‌ریزی‌های استراتژیک و چارچوب‌های سیاست-گذاری دقیق‌تر را دوچندان نموده است.

اصول مستخرج از کمیته OECD در حوزه سیاست‌گذاری برای علم و فناوری، چارچوب راهنمای توسعه سیاست و همکاری بین مجموعه‌های مختلف را با هدف کمینه‌سازی مخاطرات بالقوه ارائه می‌دهد[۴]. اما نظرسنجی‌هایی که در مورد همراستایی این توصیه‌ها با باز بودن داده‌های دولتی صورت گرفته، نشان می‌دهد وضعیت موجود هنوز با حالت ایده‌ال فاصله دارد[۵]. برخی از کشورها سیاست‌های علم باز و/یا استراتژی- های دسترسی باز به داده‌های دولتی را اتخاذ نموده‌اند، و برخی دیگر مانند کشورهای عربی حوزه خلیج فارس اخیراً در حال تلاش و اقدام برای آن هستند[۶] و [۷]. با وجود این، باز بودن دسترسی داده‌ها خود می‌تواند مفهومی باز داشته باشد و تحت شرایطی مانند ماهیت خاص داده‌ها و جمع ذینفعانی که با این مسئله درگیر هستند، با سیاست‌های متفاوتی تبیین گردد. به همین دلیل است که بعضاً کشورهایی مانند ایران هنوز در مورد این موضوع به اجماع نظر واحدی نرسیده‌اند. اما در کشورهای عضو OECD، بدرستی دسترسی و استفاده از داده‌های پژوهشی تابع محدودیت‌های قانونی معینی دانسته شده است. یکی از این محدودیت‌ها، حریم خصوصی و محرمانگی داده‌های شخصی و داده‌های دیگری است که موضوع آن‌ها انسان باشد. از اینرو، لزوم اقداماتی از سوی متصدیان امر برای بکارگیری روال‌های محرمانه‌سازی جهت اطمینان تا سطح مطلوب ضروری دانسته شده است[۴].

کارهای زیادی باید انجام بشود و در عین حال کارهای زیادی نیز انجام شده است[۸-۱۱]. از جمله کارهای مورد نیاز، کمک به ارائه تفسیر درستی از داده‌های باز برای شرایط جدیدی است که دانشگاه و صنعت طی سال‌های اخیر با آن روبرو خواهند شد. باز نمودن داده‌های پژوهشی دولتی به این معناست که بازیگران جدیدی قادر خواهند بود به تحلیل و تفسیر این داده‌ها از دیدگاه خود و نه الزاماً با عینیت‌یافتگی موردانتظار دانشمندان بپردازند. توسعه پاسخ‌گویی به نیازهای فناوری و انتظارات جامعه در عصر جدید ارتباطات و اطلاعات بدون شکل‌گیری کسب‌وکارهای نوین داده‌محور تقریباً قابل‌تصور نیست. با وجود منافع و فوایدی که در اینکار حاصل می‌شود، اما موانعی نیز بر سر راه وجود دارند [۲]. کاملاً طبیعی است که پذیرش خدمات نوآورانه این کسب‌وکارها از سوی جامعه، نمی‌تواند به بهای ورود بدون مجوز فعالان تجاری به حریم خصوصی و یا تضییع حقوق مالکیت افراد ممکن گردد. تشکیل پرونده‌های الکترونیکی از اسناد شخصی در فضای مجازی و تبادل یا به اشتراک‌گذاری آن‌ها با کسب‌وکارهایی که بر مبنای گردآوری، پردازش و تحلیل داده‌ها شکل گرفته و یا تقویت شده‌اند، ابعاد تازه‌ای به دامنه تعریف حفظ حریم خصوصی و حقوق مالکیت فکری و مادی افراد داده است. این دغدغه در سطح دنیا به طرز بارزی نمود یافته و کشور ما نیز از آن مستثنا نیست.

بنابراین، یکی از کارهای لازم در سطح سیاست‌گذاری مربوط به بسط قوانین موجود هر کشور برای حفظ حریم خصوصی و تعیین محدوده‌های مالکیت داده‌های شخصی، آنهم با توجه به تعابیر جدید و رو به تغییری است که فضای مجازی به مفهوم داده‌های باز داده است.

نتایج پژوهشی این مقاله به شیوه دلفی و طی دو مرحله ارائه گردیده است. در مرحله اول، ضمن مطالعه میدانی بازخورد قوانین موجود در کشور بر روی نمونه‌های یک جامعه هدف متعالی اخذ می‌شود. معیارها و سیاست‌گذاری‌های ممکن دسترس‌پذیری به داده‌های باز، با عطف به حساسیت داده‌های شخصی، در قالب بحث و مذاکره با جمعی از خبرگان بر روی پاسخ‌نامه‌ها تعیین می‌شوند. مرحله دوم، با به شور گذاشتن مجدد نظرات خبرگان در قالب ماتریس‌های زوجی ساختار توماس ال. ساعتی، با ارزیابی و سنجش این سیاست‌ها به روش FAHP آن‌ها را رتبه‌بندی می‌نماید. در انتها، الزامات راهبردی تحقق هدف برای اولویت منتخب تبیین می‌شوند.

در ادامه مقاله، بخش دوم به پیشینه پژوهش در این موضوع اختصاص یافته است و بخش سوم تحلیلی از موضوع مالکیت ارائه می‌دهد. در بخش چهارم، قوانین جرائم رایانه‌ای و تجارت الکترونیکی در حوزه حریم خصوصی و مالکیت داده‌های شخصی به‌ویژه در فضای مجازی مرور می‌شوند و برخی از معایب آن‌ها برشمرده می‌شوند. بخش پنجم به مرحله اول پژوهش میدانی و بخش ششم به مرحله

[1] Small and Medium Enterprises

دوم پژوهش می‌پردازد. استفاده از روش دلفی، بنا به ماهیت موضوع مقاله، در پژوهش‌هایی که روش‌های ریاضی سرراستی برای استخراج نتایج موجود نیست و تابع نظرات خبرگان می‌باشد، بسیار مرسوم و شناخته‌شده است. هدف از روش دلفی، ایجاد شیوه‌ای مبتنی بر نظرات خبرگی بوده تا با فراگردی تکراری، و از طریق پر نمودن پرسشنامه بر اساس تحلیل پاسخ‌های محرمانه از دورهای قبلی به نتایج واقعی نزدیک شود. همچنین استفاده از روش سلسله مراتبیAHP برای تصمیم‌سازی و انتخاب، در جاییکه داده‌های موجود از نظرات شفاهی برآمده‌اند، از چندین معیار تبعیت می‌کنند، و تحلیل ریاضی آن‌ها کار ساده‌ای نیست، روش جاافتاده‌ای است. با وجود این، برای آنکه نتایج تحلیل‌های انجام‌شده روی ساختار سلسله مراتبی به داده‌های انسانی شبیه‌تر باشند، تکنیک منطق فازی برای تبدیل پاسخ‌های کیفی به اعداد واقعی و نزدیک به نظرات انسانی نیز مورد استفاده قرار گرفته است.

نتایج و تحلیل‌های نهایی پژوهش در بخش هفتم ارائه شده و بخش هشتم به نتیجه‌گیری پایانی اختصاص یافته است.

۲. پیشینه پژوهش

اقدامات لازم برای دسترسی به داده‌های پژوهشی باز توسط OECD، در یک چارچوب رگولاتوری، سیاست‌گذاری و روال‌مند تجمیع شده‌اند و نهادهای پژوهشی، آژانس‌ها و دیگر شرکا آن‌ها را بکار می‌گیرند تا شرایط دسترسی و استفاده از این داده‌ها را فراهم سازند. مفهوم «باز بودن» در این دسترسی، با کمی تفصیل، چنین بیان شده است:

«داده‌های باز، داده‌هایی هستند که بدون هرگونه محدودیت فنی یا قانونی توسط هر فردی قابل‌دسترس و به‌طور مکرر قابل‌استفاده باشند. این امر الزاماً به معنای رایگان بودن داده‌ها نیست، اما این دسترسی باید برای جامعه پژوهشی بین‌الملل یکسان و با نازلترین بها، که ترجیحاً هزینه‌های نشر در آن دیده نشده باشد، ممکن گردد.»

پشتیبانی از بینش‌های علمی جدید در لوای نظام‌های ممکن، تاثیرگذاری بر قابلیت بازتولید در نتایج علمی، و همچنین تسهیل نوآوری موجب می‌شود تا تقویت دسترسی به داده‌ها به منزله یک توانمندساز کلیدی برای STI صورت امکان بخود بگیرد. اما حقیقت حاکی از آنست که بسیاری از کشورها تا توسعه روش‌های جامع برای تقویت دسترسی به داده‌ها راه زیادی در پیش دارند. از جمله معضلات سیاستی خاص و موجود در برابر تقویت به اشتراک‌گذاری داده‌ها، موارد زیر برشمرده شده‌اند[۵]:

الف- پرورش حکمرانی داده‌ها، به منظور ایجاد اعتماد و توازن منافع و مخاطرات به اشتراک‌گذاری داده‌ها.

ب- توسعه و پیاده‌سازی استانداردها و شیوه‌های فنی.

ج- تعریف مسئولیت و مالکیت داده‌ها

د- تغییر سیستم‌های تشویق و پاداش به منظور ترغیب دانشمندان برای به اشتراک‌گذاری داده‌ها.

ه- پیاده‌سازی مدل‌های کسب و کار و حمایت مالی بلندمدت برای تامین داده.

و- توسعه سرمایه‌ها و مهارت‌های انسانی برای پشتیبانی به اشتراک‌گذاری و تحلیل داده‌ها.

از آنجا که جریان‌های پژوهشی و تحقیقاتی در سال‌های اخیر بشدت به وجود داده‌ها بستگی پیدا نموده‌اند و مقوله کلان‌داده‌ها در تمام حوزه‌های علمی رو به گسترش بوده است، تعمیق این دسترسی اولویت اصلی سیاست‌گذاران گردیده است. توصیه‌نامه‌های OECD از سال ۲۰۰۶م. به بعد گام مهمی در تلاشهای چندجانبه برای پیشبرد اهداف دسترسی باز به داده‌ها در STI به‌شمار می‌رود. طیف وسیعی از سیاست‌ها در پاسخ به این توصیه‌نامه‌ها بسرعت راه‌اندازی گردید. برخی از کشورها قوانین و سیاست‌های جامعی را معرفی کردند و برخی دیگر بیانیه‌هایی دال بر وضعیت جاری و برنامه‌هایی که برای آینده در نظر گرفته‌اند، صادر کرده‌اند. بررسی OECD در ۲۰۱۷م. تعدادی بالغ بر ۱۸۱ مورد از تازه‌های سیاست‌گذاری با هدف تقویت دسترسی را در بین سیاست‌گذاران ۲۷ کشور شناسایی نموده است. در این بررسی از پاسخ‌دهندگان خواسته شده بود تا ارزیابی خود را در مورد ۱۳ اصل توصیه‌نامه سال ۲۰۱۶م. از OECD توضیح دهند. جدای از اصول سیزده‌گانه فوق، اصول FAIR[۱] نیز از سوی ذینفعان اضافه شدند که توسط دیگران مرجع قرار گرفت [۱۲]. در بین کلیه اقدامات، ۷۴ مورد(٪۴۲) به زیرساخت‌های پژوهش، شامل درگاه‌های ارائه‌دهنده دسترسی باز به نشریات؛ مخازن و آرشیوهای داده‌های علمی؛ موتورهای جستجو؛ شبکه‌های مجازی؛ و فضاهای ابری اتصال‌دهنده به مخازن فیزیکی مجزا مربوطند. مثال‌هایی از این موارد شامل اَبرِ اروپایی علم باز، و زیرساخت داده‌های پژوهشی برای علم باز در ژاپن هستند. در مواردی مانند استرالیا، استونی، فنلاند و فرانسه، زیرساخت داده‌های باز در ذیل یک استراتژی ملی بر روی زیرساخت‌های پژوهش در نظر گرفته شده‌اند. همچنین، ۸ مورد (٪۴) مربوط به بُن‌سازه‌های[۲] شبکه‌سازی و همکاری مشترک برای تسهیل دسترسی باز به داده‌ها هستند. ۵۵ مورد (٪۳۳) نیز مربوط به

[۱] Findability, Accessibility, Interoperability, Reusability

[۲] platforms

استراتژی‌ها و سیاست‌های ملی برای دسترسی باز به داده‌ها و نشریات هستند و ۵ مورد (۳٪) عهده‌دار مشاوره‌های رسمی گروه‌های ذینفعان، شامل گروه‌های کارشناسی هستند. ۱۳ مورد (۷٪) نیز با هدف ایجاد یا اصلاح یک بدنه حکمرانی برای ترویج دسترسی باز بوجود آمده‌اند. و بالاخره، درصدی از این اقدامات بدنبال جمع‌آوری داده‌هایی در مورد محققان، پروژه‌ها و سیاست‌های تحقیقاتی بوده‌اند[۵].

بررسی OECD با توجه به سیاست تقویت دسترسی به داده‌های دولتی برای STI ، شش حوزه کلیدی را شناسائی نموده که دو مورد از آن‌ها به موضوع این مقاله مرتبط هستند[۵]:

- حکمرانی داده‌ها برای اعتمادسازی - توازن منافع به اشتراک‌گذاری داده‌ها با ریسک‌ها
- تعریف مسئولیت‌پذیری و مالکیت

۱,۲ حکمرانی داده‌ها برای اعتمادسازی - توازن منافع به‌اشتراک‌گذاری داده‌ها با ریسک‌ها

متوازن نمودن منافع عمومی بالقوه با مخاطرات به اشتراک‌گذاری داده‌های پژوهشی یک دغدغه اساسی برای حکمرانی داده‌هاست. برای اطمینان از اعتماد هر دو طرف تامین‌کننده و کاربران داده‌ها و ارتقاء فرهنگ به اشتراک‌گذاری، با هدف «باز نگه‌داشتن حتی‌الامکان داده‌ها» و «بسته ماندن آنها در حد لازم»، نیاز به یک حکمرانی سالم داده‌هاست.

به‌اشتراک‌گذاری داده‌ها سبب چندین ریسک می‌شود که به موارد زیر مربوط می‌شوند:

۱) حریم خصوصی فردی (به عنوان مثال: در مورد داده‌های کلینیکی فرد).
۲) سوءاستفاده (به عنوان مثال: داده‌هایی در مورد گونه‌های نادر یا خطرناک، یا مواد معدنی کمیاب).
۳) بدفهمی (به ویژه در مورد مجموعه‌های دادگان با کیفیت نامعین، و/یا فقدان فراداده‌های مناسب).
۴) امنیت ملی (به عنوان مثال: داده‌های پژوهشی با کاربردهای بالقوه نظامی). داده‌های با جزئیات بیشتر، اغلب ارزش پژوهشی بالقوه بیشتری دارند اما به همان اندازه ریسک هم افزایش می‌یابد.

از اینجاست که پیوند داده‌های پژوهشی با داده‌های شخصی نیز گره می‌خورد. تامین دسترسی به داده‌های شخصی یا داده‌های با موضوعیت انسانی، همیشه چالش‌برانگیز بوده است. اگرچه تکنیک‌های گمنام‌سازی می‌توانند اطلاعات قابل‌شناسائی شخصی را از مجموعه‌های دادگان فردی حذف نمایند، اما ارزش پژوهش داده‌های شخصی اغلب از توان پیوند خوردن آن به مشخصات فردی ناشی می‌شود. به عنوان مثال: در انگلستان پیوند اطلاعات بیمارستان‌ها با مخزن داده‌های سرطانی و داده‌های بدست آمده از آزمون‌های مختلف غربالگری، امکان پیشنهاد تغییراتی در آیین‌نامه‌های پزشکی که احتمالاً موجب بهبود نرخ نجات از سرطان بشود را، ممکن ساخته است.

با وجود این، رضایت آگاهانه رُکن اصلی دسترسی به داده‌های شخصی در امر پژوهش است. جلب رضایت در بسیاری از کشورها حق شناخته‌شده‌ای است و در قانون‌هایی همچون GDPR[۱] محترم شمرده شده است[۹]. تمرکز GDPR روی داده‌های شخصی است و دسته‌بندی خاصی از آن‌ها را، که به آن داده‌های حسّاس هم اطلاق می‌شود، مورد توجه قرار می‌دهد. داده‌های شخصی موردنظر این قانون، حاوی اطلاعاتی در مورد منشأ نژادی یا اخلاقی داده‌ها، دیدگاه‌های سیاسی، باورهای مذهبی یا فلسفی، سلامت فیزیکی یا روانی، زندگی جنسی، داده‌های ژنتیک و بیومتریک، یا عضویت اشخاص در یک اتحادیه تجاری هستند. این داده‌ها همچنین ممکن است دربرگیرنده پیشینه جنایی یا روال محتوایی محکمه‌های جنایی علیه افراد مرتبط با آن داده‌ها باشند. پردازش این دسته خاص از داده‌های شخصی نیازمند شکل‌گیری شرایط خاصی است که از ماهیت این داده‌ها و محل کاربرد و استفاده از آنها برمی‌خیزد. به علاوه، تصریح بر اینست که داده‌های شخصی باید به صورت قانونی، مطلوب و در ارتباط با موضوع داده‌ها پردازش شوند.

اما در پژوهش موقعیت‌هایی وجود دارد که جلب رضایت برای استفاده از داده‌ها برای مقاصد پژوهشی خاص غیرممکن یا دست‌نیافتنی است، به ویژه اگر این مقاصد زمانیکه ابتدائاً گردآوری می‌شده قابل تصور نبودند. به عنوان مثال، هنگام تحلیل اَشکالِ جدیدی از داده‌های شبکه‌های اجتماعی به روش‌هایی که در تصور جمع‌کننده داده‌ها نمی‌گنجیده است، ممکن است ارجاع به کلیه افراد برای کسب رضایت از آنها غیرممکن باشد. خاطرنشان می‌سازد که اصول GDPR در امور پژوهشی استثنائاتی برای استفاده از داده‌ها در نظر گرفته و رضایت‌مندی در آن‌ها یک ملاحظه بشمار رفته، اما به عنوان مبنای قانونی برای استفاده از داده‌ها به صورت حکم در نیامده است. OECD اخیراً بر لزوم تشکیل بدنه‌های بازبینی موازین اخلاقی (ERB[۲]) به صورت مستقل و تعیین نقش آنها در ارزیابی برخی کاربردهای مورد حمایت دولت که با مقاصد پژوهشی به داده‌های شخصی دسترسی می‌یابند، تاکید ورزیده است. روش اتخاذ

[۱] General Data Protection Regulations

[۲] Ethics Review Bodies

شده توسط دولت استرالیا که هدفش نیل به ایجاد ارزش با داده‌های باز در حالیست که ریسک‌ها را به صورت شفاف مدیریت نماید، یکی از موارد مثالی است که در این مسیر گام برداشته‌اند[۵].

۲,۲ چالش‌های مسئولیت‌پذیری و مالکیت

مسئولیت‌پذیری و مالکیت، از جمله حق چاپ و مالکیت فکری، به هنگام تقویت دسترسی به داده‌های پژوهشی باز نیازمند بررسی مجدد هستند، چرا که می‌توانند الزامات مهمی بر نحوه استفاده از داده‌ها و اینکه چه کسانی می‌توانند از آن‌ها استفاده نمایند، داشته باشند. ایجادکنندگان داده‌ها ممکن است الزاماً دارای حقوق مالکیت فکری(IPR[۱]) داده‌هایی که جمع نموده‌اند، نباشند. قوانین و قواعد مدیریت داده‌های پژوهشی در بین سازمان‌ها و کشورها فرم یکدست و هماهنگی ندارد. متصدیان داده‌ها اغلب تحت چارچوب‌های قانونی مختلفی که حاکم بر مجموعه داده‌های پژوهشی و نحوه استفاده از آنهاست، عمل می‌کنند. سیاست‌های متفاوتی در موضوع IPR به‌کار گرفته شده‌اند و اشارات زیادی دال بر عدم توجه کافی در پروتکل‌های حکمرانی داده به موضوع مالکیت، دسترسی و همچنین مقوله پاسخگویی و اهمیت به اصول اخلاقی در این زمینه شده است[۱۳] و [۱۴].

مالکیت، طیف وسیعی از موضوعات استفاده از داده‌ها در فضای مجازی را با خود درگیر می‌سازد و رسیدگی به این موضوع در دنیا سابقه کمی ندارد. مطالعه‌ای که [۱۵] در مورد دغدغه‌های مهم مالکیت بر پایگاه‌های داده در ایالات متحده و اروپا انجام داده و به کاستی‌های قوانین در برخورد با اقدامات کسب‌وکاری مجرمانه پرداخته، نمونه‌ای از این دست مطالعات است. در بسیاری از این موارد، اهمیت و لزوم توجه به موضوع مالکیت داده بیشتر از منظر حکمرانی داده‌ها در سطح سازمان و نهادهای کسب‌وکاری مورد توجه قرار گرفته و کمتر مشاهده شده این موضوع با مسئله مالکیت شخصی افراد بر داده‌ها و حقوق حریم خصوصی آن‌ها پیوند خورده باشد[۱۶] و [۱۷].

با وجود این، در سال‌های اخیر موضوع مالکیت به داده‌های شخصی بیشتر گره زده شده و در برخی از مطالعات ردپای آن دیده شده است. [۱۸] تلاش کرده تا در بستر قانون اتحادیه اروپا مرز سنتی بین داده‌های شخصی از غیرشخصی را بررسی نموده و در مورد تفکیک مفهوم دقیق بین داده‌های شخصی و اطلاعات شخصی بحث نماید. از همین منظر، مفهوم مالکیت را نیز به بحث کشیده است که نشان دهد تا چه حد می‌توان این مفهوم را به داده‌های شخصی اطلاق نمود.

البته مطالعه صورت گرفته، دامنه این پژوهش را به داده‌های اینترنت اشیاء(IoT[۲]) محدود نموده است و دستاورد نهایی آن ارائه نسخه‌ای جدیدی از تئوری مالکیت داده‌های شخصی در بسترIoT برای کارهای آینده و بحث در سطوح سیاست‌گذاری و رگولاتوری آن بوده است. همچنین، [۱۹] پیچیدگی تعیین مالکیت در سطح فضای مجازی را از منظر موفقیت در نوآوری برای کارآفرینان در این فضا مطرح نموده و با طرح مسئله در دو لایه محتوا و بُن‌سازه مجازی، الزامات نظری و عملی برای کارآفرینان مجازی را موردنظر قرار داده است. موضوع جالب توجه در این مقاله نیز ابهام مالکیت در بین کلیه نقش‌آفرینان فعال در یک بُن‌سازه مشترک است. مثالی از این بُن‌سازه، می‌تواند فضای بازی‌های برخط چندنفره باشد. رُشد این فضا موجی از خلاقیت و کارآفرینی بر مبنای مهارت‌ها و دانش افرادی را می‌طلبد که هر یک به نوعی در ارتقاء کسب‌وکار از جمله در طراحی محصول، گردشگری مجازی، زیباسازی فضا و محیط، شبیه‌سازی و تبادلات اجتماعی موثر هستند. در واقع، فقدان یک مالکیت شفاف می‌تواند بر موفقیت در نوآوری افراد تاثیر منفی بگذارد. این موضوع یکی از جنبه‌های مهم مالکیت داده‌های شخصی است که در مقاله مذکور مورد توجه قرار گرفته و الزامات نوآوری موفق در فضای مجازی را در این شرایط تبیین نموده است. بر این اساس، کاربران نوآور با ورود به فرایند نوآوری در محصول، پیشنهاداتی برای بهبود محصولات ارائه می‌نمایند که پیشتر از دید تامین‌کننده محصول پنهان مانده بود. در نتیجه، با اینکار کاربر نوآور در فرایند بهره‌وری اقتصادی خدمات‌دهنده ورود پیدا می‌کند و برای خود نیز، ولو در قالب دریافت جوایز، فایده اقتصادی می‌خرد. بدین‌ترتیب، مالکیت ابزار اصلی استخراج فایده اقتصادی از پیگیری کارآفرینانه کاربران مجازی است.

توسعه مفهوم مالکیت داده‌های شخصی و حفظ حریم خصوصی افراد در حین استفاده از آن‌ها، نه فقط در کارهای پژوهشی بلکه به‌طور جدی توسط شرکت‌ها، انجمن‌ها و نهادهای علمی نیز مورد توجه قرار گرفته است. نسخه پیشنهادی سال ۲۰۱۸م. در [۲۰]، راهنمای عملی برای سازمان‌هایی است که مایل به نشر داده‌های باز هستند. در این مرجع به موضوع مالکیت و حفظ حریم خصوصی بر داده‌های شخصی افراد تاکید شده است. این تاکید در قالب پروژه مشترکی به نام درگاه اروپایی داده‌ها[۳] بین کنسرسیومی از چندین نهاد علمی مستقیماً مورد بررسی و تحلیل قرار گرفته است[۲۱].

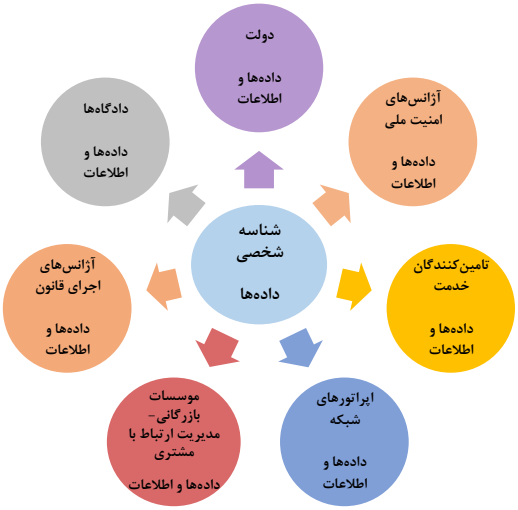
[۱] Intellectual Property Rights
[۲] Internet of Things
[۳] European Data Portal

۳. تحلیلی بر مالکیت

ابهام در مالکیت، بیشتر از ابهام در ماهیت داده‌ها ناشی می‌شود. واقعیت این است که داده‌ها چیزی بیش از مفهوم چند کاراکتر و بیت نیستند و تا زمانی‌که در بستر کاربردی خود دیده نشوند، هیچ مفهومی ندارند. داده‌ها در واقع چیزی هستند که ما برای تهیه یکسری اطلاعات از آنها استفاده می‌کنیم. تا قبل از این کار، نه داده‌ها ارزشی دارند و نه چالشی در مورد مالکیت آنها وجود دارد. اما از این نقطه به بعد، دولت‌ها و نهادهای بخش دولتی، داده‌ها را به عنوان یک موجودی عمومی تلقی می‌کنند. تمایل سازمان‌ها به این است که داده‌های شخصی ما را داده‌های شرکتی تلقی کنند و مدعی می‌شوند که بدون این داده‌ها قادر به انجام وظایف خود نخواهند بود. امروزه حجم این داده‌ها در سازمان‌ها به صورت وحشتناکی رو به فزونی است. اینجاست که موضوع مالکیت داده‌ها از دو دیدگاه شخصی و سازمانی در برابر یکدیگر قرار می‌گیرند و اهمیت آن را در مقوله حکمرانی داده‌ها دوچندان می‌کند.

سؤالی که باید به آن پاسخ داد اینست که منظور ما از عبارت «داده‌های شخصی» چیست؟ آیا می‌توان اطلاعات خانوادگی و مربوط به دوستانی را که نگه می‌داریم، یا اطلاع‌رسانی‌ها و برگه‌های اعتباری بانکی ارسال‌شده از سوی بانک را شخصی تلقی نمود؟ یا مثلاً اظهارنامه مالی ارسال‌شده توسط یک شرکت به فرد به عنوان یک سهامدار، می‌تواند برای آن فرد در حکم «داده‌های شخصی» تلقی شود؟ کدامیک خصوصی تلقی می‌شوند و اَشکال مختلف استفاده از کدامیک منوط به کسب اجازه و رضایت صاحبان آنست؟ کمی بعد، در ادامه پرسش دیگری در مورد منبع مالکیت مطرح خواهد شد.

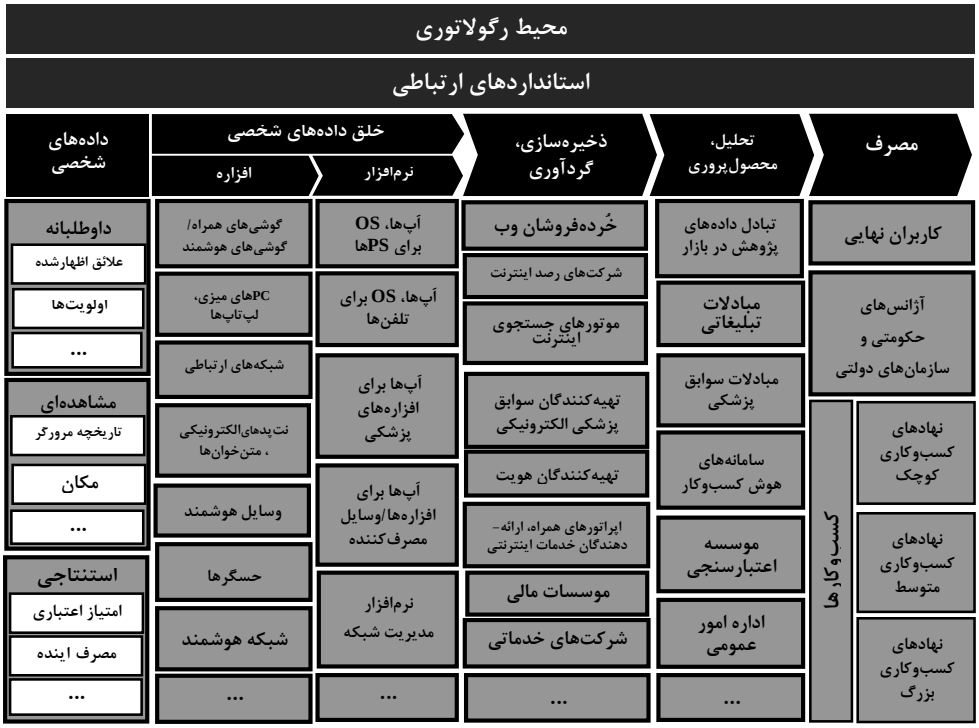
برخی از دیدگاه‌ها بر این باورند که مفهوم «داده‌های شخصی» فقط دربردارنده ویژگی‌ها و مشخصات فردی شخص است نه چیزی بیشتر! در حقیقت، ویژگی‌های شخصی فرد را از نظر فیزیکی، منطقی، یا هیجانی، تنها داده‌ای می‌دانند که به او تعلق دارد. در توضیح و تثبیت این نظریه، گفته می‌شود هنگامی که داده‌های خود را به اشتراک می‌گذاریم و حجم تراکنش‌های داده‌ای مربوط به ویژگی‌های شخصی خود را افزایش می‌دهیم، مالکیت خود بر آن داده‌ها را در اختیار دیگری می‌گذاریم. با این کار، مالکان داده نیز با هر بار مشارکت مجدد افزایش پیدا می‌کنند. شکل(۱) این به‌اشتراک‌گذاری داده‌ها را بین مدعیان مختلف مالکیت نشان می‌دهد[۲۲].



شکل ۱. تصویری از مدعیان بالقوه مالکیت داده‌های شخصی[۲۲].

بر اساس این دیدگاه‌هاست که مفهوم داده‌های باز تلاش می‌کند دسترسی شهروندان، شرکت‌ها و واحدهای کسب و کاری و جامعه مدنی را به داده‌ها تسهیل نماید. مراکز پژوهشی نیز از این امر مستثنا نیستند. بخش اعظم داده‌های ارزشمند پژوهشی بر مبنای گردآوری، ذخیره، پردازش داده‌های شخصی و بازتولید خدمات یا محصولات فکری از آن‌ها احصاء شده و می‌شوند. نشر این داده‌ها به هر شکل و صورتی می‌تواند حریم خصوصی افراد را در جامعه با تهدید مواجه سازد. در حقیقت، در اغلب موارد نشر داده‌های شخصی به صورت باز غیرقانونی است. راههای متعددی از جمله گمنام‌سازی مجموعه دادگان وجود دارند که ماهیت شخصی داده‌ها را مخفی نگه دارند، اما ویژگی برگشت‌پذیری در آن ضریب اطمینان این روش را پایین می‌آورد. به علاوه، همچنانکه داده‌های بیشتر و بیشتری از منابع مختلف یکپارچه‌سازی می‌شوند، بکارگیری این تکنیک‌ها در عمل بسیار مشکل‌تر می‌شود. گرچه قواعد و قوانین می‌توانند بازدارنده رخنه در گمنام‌سازی گردند، اما مشوق‌های مالی که به این موضوع کمک نمایند ممکن است در صنایع بخصوصی بالا باشند و نظام‌های حقوقی لازم برای پیاده‌سازی، در قلمرو اختیارات ملی، بسیار سخت و ناممکن باشد.

در مجموع، یک برنامه موفق و پایدار برای داده‌های باز بر سه رُکن استوار است. به لحاظ اخلاقی، ناشر داده باید حریم خصوصی موضوعات داده‌ای را حفظ نماید. به لحاظ قانونی، به قانون حفاظت از داده‌ها احترام بگذارد. و به طور عملی، اعتماد عمومی را جلب نماید[۲۱].



شکل ۲. مثالی از زیست‌بوم داده‌های شخصی: شبکه‌ای مرکب از خلق داده‌ها تا مصرف آنها[۲۲].

از سوی دیگر، سازمان‌ها در روال عادی کار خود قادر هستند به شیوه‌های مختلفی داده‌های شخصی را بدست بیاورند. هر نوع داده شخصی اعم از داوطلبانه، مشاهده‌ای، یا استنتاجی را می‌توان از چندین منبع (افزاره و نرم‌افزارهای کاربردی) ایجاد نمود، ذخیره کرد، و توسط چندین تأمین‌کننده (خرده‌فروشان فضای وب، موتورهای جستجو، یا شرکت‌های خدماتی) جمع‌آوری نمود و سپس به مقاصد متفاوت و برای کاربران مختلف (کاربران نهایی، کسب‌وکارها، و سازمان‌های دولتی) مورد تحلیل قرار داد. شکل(۲) زیست‌بوم ایجاد این داده‌های شخصی را نشان می‌دهد[۲۲].

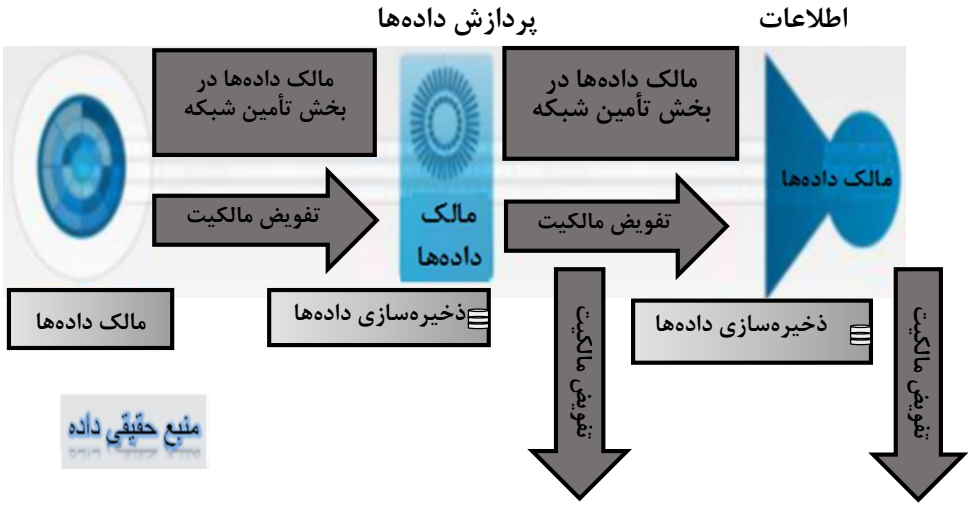
در حقیقت، این منابع مختلف هستند که از روی این داده‌ها به ایجاد داده‌های شخصی ارزشمند دیگری مبادرت می‌ورزند و این کار زیست‌بوم داده‌ها را از منظر مالکیت داده‌های شخصی جدیداً بوجودآمده پیچیده‌تر می‌کند. مدل مفهومی شکل(۳) بیانگر این ادعاست که منبع حقیقی و مالکیت داده‌های شخصی ورودی به زیست‌بوم داده‌ها، همچنانکه در مراحل مختلف منجر به تولید داده‌های دیگری می‌شود، در هر مرحله تغییر می‌کند.

دیدگاه مالکیت، از بُعد فرهنگی، قومی، نژادی، مذهبی و جغرافیایی ممکن است چالش‌های زیادی به همراه بیاورد. تخطی از حقوق مالکین اصلی هر داده در هر سطحی از مدیریت داده و در هر محیطی اعم از اجتماعی، پژوهشی یا کسب‌وکارهای داده‌محور، ممکن است زیرپاگذاشتن اصول اخلاقی نیز تلقی شود و اجازه اعلام شکایت برای مالکین محفوظ می‌ماند. اما سیاست‌ها و قوانین کشورها، تابع شرایط فرهنگی، اجتماعی و امنیتی جامعه در عمل ممکن است تدوین متفاوتی از حقوق مالکیت و حفظ حریم خصوصی افراد ارائه دهند.

در برابر چنین فضای آشفته‌ای از تولید داده‌ها و استنباط‌هایی که از مالکیت تفویض‌شده به میان آمده است، پرسش اینست: جایگاه مالکیت دقیقاً کجاست؟ اینکه منبع ذیصلاح برای تأیید داده‌ها و صحت اطلاعات «مالک حقیقی» داده‌هاست، محل برخورد و کشمکش است. اینجا مفهوم جدیدی شکل گرفته که باید دید چه کسی حق استفاده از اطلاعات و داده‌هایی که شخص در ارائه یا ایجاد آنها دخالتی نداشته اما به نوعی به داده‌های شخصی اولیه او مربوط هستند، دارد.

با توجه به نکات بالا موضوع تقویت دسترسی باز به داده‌ها از بُعد حفظ حریم خصوصی و حقوق مالکیت افراد و سازمان‌ها یا نهادهای

کسب‌وکاری بر داده‌های شخصی نیازمند توجه و دقت بیشتری است. OECD رسیدگی به این امر را به دلیل اهمیت و جایگاه فراتر موضوع، در قالب قانون عمومی حفاظت از داده‌های شخصی (GDPR)، عمدتاً در سطح کشورهای عضو آورده است[۲۳].



شکل ۳. ابهام در ماهیت منبع حقیقی مالکیت داده‌های شخصی[۲۲].

با وجود این، تمرکز این قانون عمدتاً بر حفاظت از داده‌های شخصی و با توجه به حفظ حریم خصوصی است و موضوع مالکیت داده‌های شخصی هنوز در محافل علمی مختلف محل بحث است که در بخش دوم به پیشینه برخی پژوهش‌ها در این زمینه اشاره شد. با این نگرش، انتظار می‌رود صاحب‌نظران و متخصصین داخلی دست‌اندرکار حوزه علوم داده، شرکت‌ها و سازمان‌های کسب‌وکاری مرتبط، نهادهای تنظیم مقررات و قوانین حوزه فضای مجازی، نهادهای حقوقی و...، با انجام مطالعات پژوهشی و برگزاری طوفان‌های فکری، در بازتعریف، تبیین و توسعه زیست‌بوم داده‌های شخصی به حل این موضوع بپردازند.

نه تنها به قوانین و ضوابط توافق‌شده در سطح ملی نیاز است، بلکه باید بسیار فراگیر باشند. لازم است در بخش‌های درون‌سازمانی نیز قابل‌اعمال بوده و برای حفاظت از حریم خصوصی بر گستره‌ای وسیع‌تر از صرفاً کمینه‌سازی گردآوری، ذخیره‌سازی و استفاده از داده‌ها متمرکز شوند. اصول توسعه زیست‌بوم داده‌های شخصی باید سرلوحه کار قرار بگیرند. برخی از این اصول در [۲۲] پیشنهاد شده‌اند که در تدوین سیاست‌گذاری‌های راهبردی و قوانین مربوطه می‌توان از آن‌ها بهره گرفت. بخش بعدی، به وضعیت قوانین این موضوع در داخل کشور می‌پردازد.

۴. بررسی و تحلیل قوانین مالکیت و حفظ حریم خصوصی در کشور

در نظام حقوقی ایران، حفظ حریم خصوصی اشخاص و حمایت از حقوق مالکیت مادی/معنوی بر داده‌های شخصی در فضای مجازی از سه مسئله رنج می‌برد:

- شمولیت نداشتن قوانین موجود بر کلیه مصادیق مالکیت مادی/معنوی داده‌های شخصی(ضعف سیاست‌گذاری).
- ضعف در ضمانت اجرایی قوانین(ضعف نظارت).
- به‌روز نبودن و عدم‌تناسب قوانین فعلی با الزامات کسب و کاری در نظام تحول دیجیتال(ضعف سیاست‌گذاری).

بدلیل کاستی‌های بالا اغلب شاهد مواردی از نقض حریم خصوصی افراد، تخریب حیثیت اجتماعی آن‌ها و سرقت حقوق مادی/معنوی دستاوردهای اشخاص حقیقی/حقوقی (افراد یا نهادهای کسب‌وکاری) بوده و هستیم. دو اصل قانون اساسی جمهوری اسلامی و فرمان هشت‌ماده‌ای در مواردی نقض یا نادیده گرفته می‌شوند. به‌علاوه، به نظر می‌رسد نقض حریم خصوصی در جامعه ریشه‌ای عمیق در فرهنگ کشور داشته و در مواردی که بی‌غرض صورت می‌گیرد، امری عادی تلقی می‌شود.

مادامیکه قانون‌گذار دامنه این تخلفات را روشن نسازد و برای متجاوزین به این حریم مجازات مناسبی در نظر نگیرد و بدون تبعیض و چشم‌پوشی آنرا به اجرا درنیاورد، شاهد تغییر اساسی در این حوزه نخواهیم بود[۲۴]. در آخرین اقدام که به سال ۱۳۹۵ منشور حقوق شهروندی تدوین شده و به امضاء ریاست جمهوری رسید، بنظر می‌رسید در راستای ارتقاء حقوق شهروندان در زمینه حق حریم خصوصی و انواع مالکیت، به لحاظ اجرایی گام‌های مهمی از سوی نهادهای ذیربط برداشته شود[۲۵]. انتظار بر این بود آیین‌نامه‌های اجرایی در حوزه فضای مجازی نیز بهبود داده شوند. مفاد این منشور با دستورالعمل ۹۵/۴۶ کنوانسیون مصوب ۱۹۸۱م. اتحادیه اروپا برای حمایت از افراد در پردازش خودکار داده‌های شخصی چنانکه در [۲۴] به آن پرداخته است، تناظرهای نزدیکی دارد. منشور حقوق شهروندی از حق دسترسی شهروندان به اطلاعات شخصی خود، حق درخواست اصلاح در اطلاعات اشتباه وارد شده، و ارائه اطلاعات با رضایت مالک داده‌ها به دیگران حمایت کرده است (ماده ۳۱). همچنین، به موضوع حق حریم خصوصی و حق مالکیت افراد بر داده‌های شخصی نیز مواد جداگانه‌ای را اختصاص داده است. در موضوع حق حریم خصوصی، تفتیش، گردآوری، پردازش، به‌کارگیری، افشاء و یا انتشار اطلاعات خصوصی و داده‌های شخصی و ... در رسانه‌ها و تریبون‌های مختلف، بدون رضایت آگاهانه مالکین یا مگر به تشخیص قانون، ممنوع اعلام شده است. مرتکبین طبق مقررات قانونی مسئول و موظف به جبران خسارت می‌باشند (مواد ۳۶-۴۲). به‌علاوه، انواع مالکیت فکری افراد از جمله مالکیت ادبی، هنری، و صنعتی با رعایت قانون محترم و مورد حمایت قرار گرفته است(ماده ۷۶). با وجود این، مصادیق این منشور در موضوع حریم خصوصی و مالکیت به ویژه در فضای مجازی هنوز روشن نیست.

بخش دیگری از حقوق شهروندی سندی است که به تاریخ نهم بهمن ۱۳۹۵ ویژه نظام اداری تدوین گردیده است. در بند دوم و سوم از ماده هفت این حقوق تاکید شده استفاده از اطلاعات شخصی افراد فقط به حد کفایت و در مصارف هدفی باشد که اطلاعات برای آن جمع‌آوری گردیده است[۲۶]. شاید بتوان این قانون را به هر نوع اطلاعات شخصی اعم از داده‌های ثبت‌شده افراد در مجموعه دادگان اداری موجود در فضای مجازی نیز اطلاق نمود. لیکن کاربرد این قوانین به حیطه نظام اداری محدود گردیده شامل محیط‌های اجتماعی و شرکت‌های کسب‌وکاری داده‌محور مجازی که دارنده مجموعه دادگانی از افراد حقیقی و حقوقی هستند، نمی‌شود.

حمایت از حقوق مالکیت شهروندان در بخش اصناف کشور، از جمله مولفان، مُصَنِّفان، و هنرمندان سابقه‌ای بیش از منشور حقوق شهروندی دارد[۲۷]. حقوق مالکیت مادی/معنوی این طیف از کسب‌وکارها بدون در نظر گرفتن شیوه یا روش بیان و انتشار و ایجاد آن‌ها (مواد ۱-۲)، محفوظ دانسته شده است و حق انحصاری نشر و پخش و عرضه و اجرای اثر و حق بهره‌برداری مادی و معنوی از نام و اثر در تملک صاحب اثر دانسته شده است (مواد ۳-۴) و متخلفین مشمول مجازات‌ها و جرائم مذکور در مواد ۲۳-۳۳ این قانون خواهند بود. گرچه ماده ششم این قانون حفظ حقوق بر آثار حاصل از همکاری مشترک را برای کلیه همکاران اثر لحاظ نموده است، لیکن در مورد زنجیره‌ای از آثار بعدی و بدست‌آمده از محصول اولیه، به‌ویژه آنگونه که در این مقاله به مسئله پردازش‌های چندباره داده‌های شخصی و ابهام در مالکیت پرداخته شد، سخنی به میان نیاورده است. این موضوع اما در آیین‌نامه اجرایی و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای که به سال ۱۳۷۹ه. ش. به تصویب رسیده است، صرفاً برای تولیدات نرم‌افزاری دیده شده است. در مواد ۹ و ۱۰ این آیین‌نامه، از حقوق پدیدآورنده حمایت نموده و ماده ۱۱ صراحتاً به حقوق اشخاص متعددی که در این فرایند مشارکت داشته باشند، تاکید ورزیده است. به‌علاوه، ماده ۱۲ و ۱۳ آیین‌نامه در موضوع پدیدآوری نرم‌افزارهای ثانوی با استفاده از نرم‌افزارهای موجود را مجاز شمرده، حقوق آنرا متعلق به پدیدآورندگان جدید می‌داند. در واقع، قانون این عمل را ناقض حقوق پدیدآورندگان نرم‌افزارهای واسط، جز در موارد استفاده از نرم‌افزار آن‌ها بدون کسب رضایت ایشان، نمی‌داند[۲۸]. با این حال، قانون یادشده نیز محدود به محصولات و کسب و کارهای نرم‌افزاری است و اشاره‌ای به ارزش حقوقی پدیدآورندگان یا دارندگان داده‌های شخصی ندارد. به‌علاوه، جرائم مالی تعیین شده در قانون مذکور بر مبنای شرایط تورمی در اقتصاد کشور به هیچ‌وجه بازدارنده نیستند. قانون تجارت الکترونیکی مصوبه دی ماه سال ۱۳۸۲ ه. ش. طبق ماده یک آن، مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسط‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود[۲۹]. در این قانون برای اولین بار به تعریف عبارت «داده پیام» و «داده پیام شخصی» اشاره شده است. موادی که در قانون حمایت از حقوق مولفان، مصنفان و هنرمندان برای حفظ حقوق ایشان در آثار منتشرشده در فضای مجازی به صراحت بیان نشده‌اند، در مواد ۶۲-۶۳ قانون تجارت الکترونیکی پوشش داده شده است. از طرفی، ملاحظات تفصیلی این قانون در فصل سوم نیز تحت عنوان حمایت از داده پیام‌های شخصی، به حق درخواست شخص برای دسترسی، اصلاح یا امحاء پرونده‌ها و داده‌های شخصی خود در هر زمان صحه گذاشته است (ماده ۵۹، بندهای د - ه). همچنین، تاکید شده میزان داده پیام فقط باید متناسب با اهدافی که در هنگام جمع‌آوری برای شخص مالک شرح داده شده صورت

پذیرد(ماده ۵۹ بند ب). با وجود این، مفاد مذکور در این فصل درصدد مقابله با سوءاستفاده‌های شخص در برابر شخص که خارج از حیطه‌های کسب‌وکاری رخ می‌دهد، برنیامده است. مهمتر آنکه نه در اینجا و نه در قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای ۱۳۷۹، مشخص نیست مرزبندی و کیفیت استفاده سوء از نرم‌افزار یا داده‌های شخصی اولیه در خلق و ایجاد نرم‌افزار یا داده‌های شخصی ثانوی چگونه تعیین می‌شود. به عبارتی، قانون هم در نحوه این تشخیص و هم در معرفی متولی این امر سکوت نموده است. بدیهی است میزان جرائم تخلفات در اینکار نیز به همین نسبت از جزییات لازم برخوردار نیست.

از دیگر نقاط ضعف قانون تجارت الکترونیکی، ذکر جرائم سَبُک و متناسب نبودن مبالغ آن با شرایط اقتصادی روز کشور در مواد ۶۹-۷۳ و همچنین اشاره صرف به ذکر جرائم در خصوص تخلف افراد صرفاً از منظر خسران مالی وارده به مالکان داده پیام است (ماده ۶۷). این در حالیست که بسیاری از جرائم فضای مجازی ناشی از زیرپاگذاشتن اصول اخلاقی در شبکه‌ها و پیام‌رسان‌های اجتماعی است و پرداخت جزای نقدی معادل مال ماخوذه مذکور در ماده ۶۷ این قانون سنخیتی با خسارات وارده به حیثیت و شان اجتماعی اشخاص ندارد.

قانون جرائم رایانه‌ای در کشور (۱۳۸۸ ه. ش.) سند دیگری حاوی مصادیق مجرمانه و مجازات‌های تعیین شده برای آن‌هاست که عمدتاً با رویکرد حفاظت از داده‌های طبقه‌بندی-شده، محرمانه در برابر جاسوسی، تخریب، و تخلف توسط افراد در نهادهای دولتی تدوین شده است[۳۰]. با این‌حال، موارد معدودی از مفاد آن مانند ماده ۱۶ و ۱۷ از فصل پنجم این قانون، اشاره‌ای عام به مجرمانه بودن عمل تغییر یا تحریف و نشر بدون رضایت مالک داده‌ها به صورت صوت، تصویر، یا فیلم منجر به هتک حیثیت نموده است. با مقداری خوش‌بینی، بنظر می‌رسد قلمرو دو ماده مذکور علاوه بر مصادیق مجرمانه در سیستم‌های رایانه‌ای شخصی و عمدتاً دولتی و خصوصی، می‌تواند به محتواهای منتشرشده توسط مالکین داده‌های شخصی در بستر شبکه‌ها و پیام‌رسان‌های اجتماعی نیز تعمیم یابد. با وجود این، هنوز ابهام در مصادیق مالکیت داده‌ها بعد از پردازش‌های زنجیره‌ای داده‌های شخصی و متناسب بودن میزان جرائم تعیین‌شده با زمان تصویب قوانین، در این قانون نیز به چشم می‌خورد و به هیچ‌وجه مانع پیش‌گیری از بروز تخلفات نمی‌گردد.

ضعف قوانین موجود بدلیل اینکه برخی از آن‌ها پیشینه‌ای بیش از طول عمر فضای مجازی دارند، امری قابل‌درک است. به‌ویژه، موضوع مالکیت داده‌های شخصی زمانی قوت گرفت که با ظهور مفاهیمی همچون تحول دیجیتال نقش داده‌ها به عنوان منابع ایجاد ارزش و ظهور کسب‌وکارهای داده‌محور کلیدی‌تر شد، به گونه‌ای که کاربران و مصرف‌کنندگان نهایی خود نیز جزیی از زنجیره ارزش و کسب درآمد گردیده‌اند.

متاسفانه با قوانین موجود، رسیدگی بسیاری از موارد تخلف بدلیل عدم وضوع در مفاد قانون با مشکل ضمانت اجرایی روبرو می‌شود.

رشد شبکه‌ها و پیام‌رسان‌های اجتماعی به عنوان منبع عظیمی از داده‌های شخصی، شکل دیگری از علوم تحلیل داده‌ها و همچنین شیوه‌های تبلیغاتی جدید را در دسترس کسب‌وکارهای مجازی قرار داده است. دریافت تبلیغات پیامکی، بازشدن ناخواسته انواع کانال در پیام‌رسان‌های اجتماعی، و یا باز شدن پنجره‌های تبلیغی متعدد در صفحات وب‌سایت‌ها، صرفنظر از اینکه هزینه بیشتری بابت مصرف اینترنت را به مشتریان فضای مجازی تحمیل می‌کنند، در موارد زیادی موجب برخی مزاحمت‌ها و در نتیجه بازخوردهای جدی از سوی اشخاص و خانواده‌ها می‌شوند. تبلیغات و پیشنهادات دریافتی منعکس‌شده از رفتار یا سلائق پیدا و پنهان کاربران فضای مجازی، می‌تواند احساس ناامنی و تحت پایش بودن در کلیه موقعیت‌های فضای مجازی را به آن‌ها القا نماید و در مجموع حس امنیت اجتماعی در جامعه را کاهش می‌دهد.

در این شرایط، رویکرد سیاست دسترسی باز به داده‌ها در کنار مسائلی که در خصوص مالکیت داده‌ها و حریم خصوصی اشخاص در اینجا بررسی شدند، نیازمند برخی الزامات راهبردی در سطح سیاست‌گذاری است. تعیین این الزامات در پاسخ به سوالاتی ضرورت پیدا نموده که روشن‌سازی پاسخ آن‌ها می‌تواند از یک سو راهگشای توسعه دانش مبتنی بر داده در سطح مراکز پژوهشی کشور و نوآوری و کارآفرینی در حوزه‌های کسب و کار گردد و از سوی دیگر، این سیاست‌گذاری کلان را در برابر چالش‌های پیش‌روی خود، از منظر صیانت از حریم خصوصی و حقوق مالکیت داده‌های شخصی قابل‌قبول نماید. اهم این سوالات عبارتند از:

- راهبردها و سیاست‌های کلان دستگاه حاکمه برای حمایت از دسترسی به داده‌های باز توسط واحدهای پژوهشی و کسب وکاری کشور با اهداف سالم توسعه، کدامند؟
- دیدگاه عمومی در کشور راجع به سیاست‌گذاری‌های حمایتی از حریم خصوصی اشخاص و حفظ حقوق مالکیت فردی(مادی و معنوی) افراد در فضای مجازی چیست؟
- ضمانت‌های اجرایی قوانین حفظ حریم خصوصی و حقوق مالکیت داده‌های شخصی در فضای مجازی داخل کشور تا چه حد مورد اعتماد جامعه است؟

در گام اول، بررسی نتایج یک مطالعه میدانی از میزان رعایت حفظ حریم خصوصی و احترام به حقوق فردی اشخاص در یک جامعه هدف، اهمیت و جایگاه این موضوع را بیش از پیش در کشور نمایان می‌سازد. پژوهش انجام شده، سپس با گذر از مرحله دوم تلاش می‌کند به مرحله سیاست‌گذاری در این زمینه نیز ورود پیدا کند.

۵. پژوهش میدانی – مرحله ۱: وضعیت موجود در کشور - استخراج معیارهای انتخاب و گزینه‌های سیاست دسترس‌پذیری به داده‌های باز

پژوهش در مرحله اول به دنبال بررسی وضعیت موجود در داخل کشور از منظر کاربران، در مورد چگونگی صیانت از حریم خصوصی اشخاص و مالکیت آن‌ها بر داده‌های شخصی خود در فضای مجازی کشور می‌باشد. معیارها و سیاست‌گذاری‌های ممکن دسترس‌پذیری به داده‌های باز در این مرحله شناسایی می‌شوند. در مرحله دوم، با رتبه‌بندی این سیاست‌گذاری‌ها و تحلیل نتایج پژوهش، الزامات راهبردی پیشنهاد می‌شوند. هدف از این امر، تسهیل بهره‌برداری حوزه‌های پژوهشی و کسب و کاری از بستر داده‌ها و اطلاعات شخصی در فضای مجازی برای کمک به توسعه و ایجاد خدمات و محصولات نوین و رونق کارآفرینی‌های جدید در عصر تحول دیجیتال در داخل کشور می‌باشد.

مدل مفهومی شکل(۴)، صورت مسئله را با روند تحلیل در این پژوهش، برای تحقق اهداف سیاست‌گذاری نشان می‌دهد.

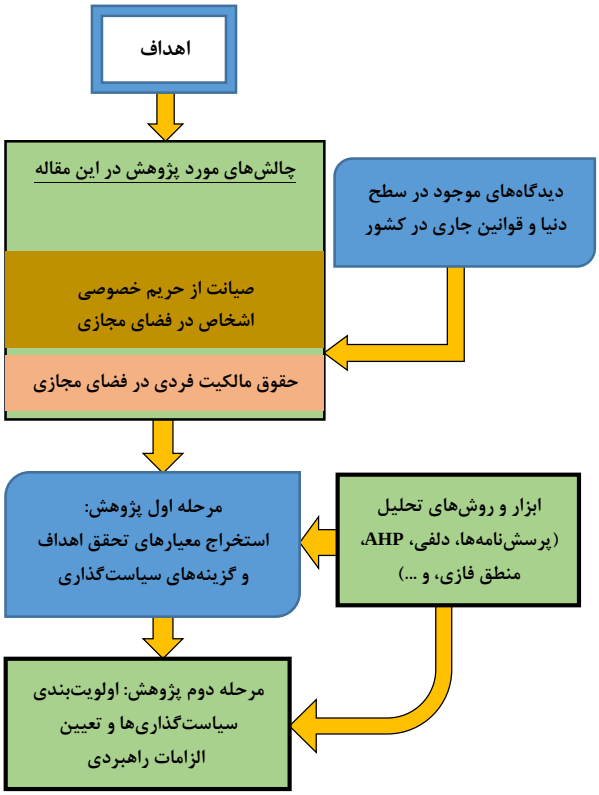
۱،۵ جامعه هدف

این مطالعه به روش دلفی و بر روی یک جامعه هدف با مشخصات زیر صورت گرفته است:

- تعداد نمونه‌ها ۵۸ نفر بوده است.
- پرسشنامه حاوی ۱۸ پرسش بوده که تعداد گزینه‌های پاسخ در هر پرسش از ۳ تا ۴ متفاوت بوده و در یک پرسش ۸ گزینه شامل انتخاب از یک تا هر هشت گزینه وجود داشت.
- نمونه‌ها طیفی از مهارت‌ها یا تخصص‌های مرتبط با تامین یا تحلیل دانش‌های مربوط به توسعه فضای مجازی را با توزیع زیر دربرمی‌گیرند(به همین دلیل آنرا جامعه متعالی می‌نامیم):
  - ✓ ۱۹ نفر از حوزه فناوری اطلاعات
  - ✓ ۱۲ نفر از حوزه ارتباطات
  - ✓ ۹ نفر از حوزه شبکه و امنیت اطلاعات
  - ✓ ۹ نفر از حوزه‌های دفتری مرتبط با ICT
  - ✓ ۹ نفر از حوزه خدمات‌دهندگان اینترنتی
- مهارت یا تخصص نمونه‌ها صرفاً ملاک قضاوت نبوده و در جمع‌آوری پاسخنامه‌ها با اغلب نمونه‌ها مذاکره انجام گرفته تا ابهامات احتمالی مرتفع شوند.
- معدودی از پرسش‌ها جنبه تخصصی‌تر داشتند تا در این پژوهش انتخاب بهتری از مصاحبه‌شوندگان صورت بگیرد.
- هرگاه نتیجه‌گیری روشنی حاصل نمی‌شد، پاسخنامه از فهرست داده‌های آماری حذف می‌شد.

چهار پاسخنامه، بدلیل معتبر نبودن محتوای پاسخ‌ها و نتایج مذاکره با پاسخ‌دهندگان بی‌اعتبار دانسته شد و حذف گردیدند.

لازم به توضیح است که گرچه انتخاب نمونه‌ها هدفمند بوده است اما فرض شده احتمال پاسخ‌های اشتباه وجود دارد. زیرا در جامعه‌ای با مشخصات فرهنگی کشور ما اغلب دیده شده است افراد حتی در صورت عدم آگاهی کافی به موضوع، از گفتن واژه «نمی‌دانم» اجتناب دارند. بر این اساس، معدودی از پرسش‌ها جنبه تخصصی‌تر داشتند تا در این پژوهش انتخاب بهتری از مصاحبه‌شوندگان صورت بگیرد.



شکل ۴. مدل مفهومی موضوع سیاست‌گذاری دسترسی به داده‌های باز، در برابر چالش‌های صیانت از حریم خصوصی و مالکیت داده‌های شخصی در فضای مجازی.

۲,۵ محتوای پرسش‌نامه‌ها و نتایج مستخرج

پرسش‌های مطرح‌شده حول موضوعات زیر بوده‌اند:

- تعریف کاربران اینترنتی از اطلاعات شخصی که جزء حریم خصوصی یا در مالکیت مادی/معنوی آنها است. مواردی از قبیل محتواهای بارگذاری‌شده/بارگیری‌شده، کامنت‌های کاربران در صفحات مجازی، خدمات یا محصولات نرم‌افزاری شخصاً تولید/عرضه‌شده در فضای مجازی، افشاء حضورهای پنهان در شبکه‌های اجتماعی و ...حتی پروفایل شخصی، شماره‌های تماس و آدرس ایمیل جزو پاسخ‌های نمونه‌های جامعه هدف بوده است.
- از نظر پاسخ‌دهندگان در مورد اجازه دسترسی دولت و کسب‌وکارهای داخل کشور به داده‌های شخصی به منظور استفاده سالم و ایجاد بازارهای جدید پرسش شده است.
- در مورد لزوم کسب اجازه کاربران عادی از صاحبان داده‌های شخصی در فضای مجازی برای بازنشر آن‌ها یا هر فعالیت سالم دیگری پرسش شده است.
- در مورد وضعیت جاری کشور به اینکه آیا در حال حاضر داده‌های شخصی توسط خدمات‌دهندگان اینترنتی دولتی /خصوصی مورداستفاده یا در بین ایشان مبادله می‌شود، پرسش شده است.
- در مورد اینکه آیا بازاستفاده از اطلاعات شخصی کاربران در فضای مجازی موجب مراجعات مکرر و مزاحمت کسب و کارهای مختلف جهت تبلیغ یا فروش خدمات و/یا محصولات گردیده یا خیر، پرسش شده است.
- در مورد اینکه آیا شکایاتی در مورد تضییع حقوق مالکیت مادی/معنوی یا تجاوز به حریم خصوصی کاربران صورت گرفته، و از نتیجه دادرسی به این شکایات پرسش شده است.
- آگاهی پاسخ‌دهندگان به وجود قوانینی در سطح دنیا و/یا در کشور، ویژه کسب و کارها با هدف مشتری‌مداری و صیانت از اطلاعات شخصی و حریم خصوصی کاربران و حقوق مالکیت افراد در فضای مجازی، از موارد پرسش بوده‌اند.

در این پژوهش، داده‌های امنیتی که منظور داده‌های طبقه‌بندی شده در سطح کشور هستند و به طور مثال شامل پرونده‌های سیاسی اشخاص، اقدامات امنیتی مجاز توسط افراد رده بالای دستگاه حاکمه، و .... نیز می‌باشند، موضوع این مقاله نبوده‌اند. همچنین، داده‌های حساس تجاری نیز که حاوی اطلاعات حساس و کاملاً خصوصی و یا پرونده‌های محرمانه مربوط به اشخاص هستند، از حوزه مطالعه این پژوهش خارج هستند.

دو نکته جالب‌توجه و مهم در پاسخ‌ها وجود داشت. اول اینکه، بجز ۵۸ نمونه مذاکره شده به صورت موفق، برخی از پاسخ‌دهندگان به حقوق بدیهی خود بر داده‌های شخصی واقف نبودند و حتی پرداختن به محتوای پرسشنامه را به حدی حساس تلقی می‌کردند که از پر نمودن آن خودداری نمودند. نکته دوم اینکه، عموم پاسخ‌ها نشان می‌داد حتی در بین نمونه‌های یک جامعه متعالی تعداد افراد آگاه به قوانین موجود و مرتبط با حریم و حقوق مالکیت داده‌های شخصی در کشور از جمله: آیین‌نامه اجرایی و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، قانون تجارت الکترونیکی، و قانون جرائم رایانه‌ای، از تعداد انگشتان یک دست هم کمتر است.

با وجود این، دیدگاه‌های تخصصی و مهارتی نمونه‌های جامعه هدف برای اهداف سیاست‌گذاری در این مقاله مفید واقع شدند. معیارهای تحقق و سیاست‌های مناسب برای دسترس- پذیری به داده‌های باز در کشور، از ماحصل این دیدگاه‌ها به وضعیت جاری کشور در موضوع حفظ حریم خصوصی و حقوق مالکیت تعیین شدند(جدول ۱).

به علاوه، از جمع‌بندی آرا و پاسخ‌ها این واقعیت مشهود بود که استقبال عمومی شرط لازم برای انتخاب یک سیاست دسترس‌پذیری به داده‌های باز است، اما کافی نیست. عدم اطلاع اغلب نمونه‌ها از وجود قوانین مناسبی در این زمینه در داخل کشور، و بازخوردهای منفی ایشان از مقابله ناکارامد با موارد تخلفی که در فضای مجازی رخ داده، حاکی از ناامیدی ایشان در بازدارندگی جرائم و اجرای موثر قانون در بحث صیانت از حریم خصوصی و حفظ حقوق مالکیت افراد بوده است. در بین سیاست‌گذاری‌های ممکن و مستخرج از این نظرسنجی، مطابق جدول(۱)، پنج گزینه مطرح می‌باشد.

پس از تعیین گزینه‌های ممکن سیاست‌گذاری، نظرسنجی از خبرگان برای اولویت‌بندی و انتخاب سیاست‌گذاری مناسب، تکرار شد. این کار در مرحله دوم پژوهش به شیوه FAHP انجام گرفت.

جدول ۱. معیارهای تحقق و سیاست‌های ممکن از منظر خبرگان برای دسترس‌پذیری مراکز پژوهشی و کسب‌وکارهای داده‌محور به داده‌های باز در فضای مجازی.

هدف	انتخاب سیاست دسترس‌پذیری داده‌های باز در حوزه‌های پژوهشی و کسب‌وکارهای داده‌محور در فضای مجازی - با عطف به حساسیت داده‌های شخصی
معیارهای تحقق هدف	استقبال عمومی
	جامعیت قوانین حفظ

	حریم خصوصی اشخاص
	جامعیت قوانین حفظ منافع شخصی مالکان داده
	اجرای موثر قوانین
سیاست‌های دسترس‌پذیری به داده‌های باز	گزینه ۱: دسترس‌پذیری باز به انواع داده‌های عمومی، شامل داده‌های شخصی (به جز امنیتی و داده‌های حساس تجاری)
	گزینه ۲: همان گزینه یک، به شرط جلب رضایت از مالک داده به حسب هر مورد.
	گزینه ۳: همان گزینه یک، به شرط دریافت منفعت مادی توسط مالک اصلی داده، درحالیکه ماحصل کسب و کار و بهره‌برداری دیگری بوده است.
	گزینه ۴: همان گزینه یک، به اضافه شروط گزینه‌های دوم و سوم.
	گزینه ۵: همان گزینه یک، به جز داده‌های شخصی، امنیتی، و داده‌های حساس تجاری.

۶. پژوهش میدانی - مرحله ۲: تحلیل اولویت‌های سیاست‌گذاری به روش FAHP و راهبردهای تحقق هدف.

این مرحله هدف اصلی مقاله را برای انتخاب و پیشنهاد یک سیاست مناسب دسترسی‌پذیری به داده‌های باز در کشور دنبال می‌کند. ابتدا، ساختار AHP مشتمل بر یک هدف، چهار معیار تحقق هدف، و پنج گزینه سیاست‌گذاری تشکیل شد. معیارها از یکدیگر مستقل هستند و ارتباطات افقی در AHP وجود ندارد. کلیه محاسبات در محیط اکسل یا نرم‌افزارهای موجود، مانند سوپردسیژن[۱]، و حتی به صورت دستی قابل انجام هستند.

این مرحله با گزینش ۹ نفر از بین خبرگان جامعه هدف آغاز گردید. معیار گزینش خبرگان در این مرحله کسانی بودند که به پرسش‌های تخصصی‌تر پرسشنامه آگاهی داشتند و برای تبیین الزامات راهبردی تحقق هدف، در طی مذاکرات مشارکت علمی موثری داشتند. فرایند تکمیل ۴۵ ماتریس زوجی، با شفاف‌سازی نکات مبهم و دریافت نقطه‌نظرات خبرگان به انجام رسیده است.

از خبرگان خواسته شد برای تکمیل ماتریس‌های زوجی (شامل یک ماتریس ۴×۴ در سطح اول و چهار ماتریس ۵×۵ در سطح دوم) پاسخ‌های خود را با متغیرهای کلامی فازی ارائه دهند. سپس تبدیل لازم بر طبق اعداد فازی مثلثی طیف لیکرت ۵ درجه صورت گرفت (جدول ۲) و از روش مینکوفسکی (معادله ۱) فازی‌زدایی پاسخ‌ها انجام شد. از مجموعه نظرات خبرگان، بدلیل گسترده بودن طیف پاسخ‌های داده‌شده، میانگین هندسی گرفته شد و سپس وزن‌دهی ماتریس‌های زوجی بدست‌آمده به روش میانگین حسابی انجام گرفت. در ادامه، به روش مقادیر ویژه، نرخ ناسازگاری برای ماتریس‌های زوجی محاسبه گردید.

جدول ۲. اعداد فازی مثلثی طیف لیکرت ۵ درجه[۳۱].

متغیر کلامی	مقدار فازی	عدد فازی مثلثی (l,m,U)
خیلی کم	$\tilde{۱}$	(۰ ، ۰ ، ۰/۲۵)
کم	$\tilde{۲}$	(۰ ، ۰/۲۵ ، ۰/۵)
متوسط	$\tilde{۳}$	(۰/۲۵ ، ۰/۵ ، ۰/۷۵)
زیاد	$\tilde{۴}$	(۰/۵ ، ۰/۷۵ ، ۱)
خیلی زیاد	$\tilde{۵}$	(۰/۷۵ ، ۱ ، ۱)

$$X = m + \frac{U-l}{۴} \qquad (۱)$$

$\boldsymbol{X}$ مقدار فازی‌زدایی شده پاسخ‌های خبرگان می‌باشد.

در گام آخر، رتبه‌بندی گزینه‌های پنج‌گانه سیاست‌گذاری از حاصل‌ضرب دو ماتریس زیر محاسبه شدند:

$$W_t = W_O \times W_c \qquad (۲)$$

که در آن W_c بردار ستونی وزن معیارها و W_Oماتریس ۴ × ۵ است که ستون‌های آنرا به‌ترتیب بردارهای وزن گزینه‌ها، یعنی $W_{O۱}$ تا $W_{O۴}$، تشکیل می‌دهند. جدول(۴) بردار وزن تحقق هدف، یعنی W_t ، و رتبه‌بندی در پنج گزینه سیاست‌گذاری را نشان می‌دهد. ستون آخر نیز ضریب فاصله چهار گزینه را نسبت به گزینه منتخب با رتبه یک نشان می‌دهد.

جدول ۳. وزن‌دهی و نرخ ناسازگاری ماتریس‌های زوجی.

عناوین ماتریس‌های زوجی	بردارهای وزن هر ماتریس		نرخ ناسازگاری
هدف: انتخاب سیاست دسترس‌پذیری داده‌های باز	W_c	۰/۰۹۵	۰/۰۶۱
		۰/۲۴۶	

[۱] super decisions

عناوین ماتریس‌های زوجی	بردارهای وزن هر ماتریس		نرخ ناسازگاری
در حوزه‌های پژوهشی و کسب‌وکارهای داده‌محور در فضای مجازی - با عطف به حساسیت داده‌های شخصی		۰/۲۱۴	
		۰/۴۴۵	
معیار ۱: استقبال عمومی	W_{O1}	۰/۰۳۴	۰/۰۲۴
		۰/۱۴۱	
		۰/۱۳۵	
		۰/۳۲۹	
		۰/۳۶۱	
معیار ۲: جامعیت قوانین حفظ حریم خصوصی اشخاص	W_{O2}	۰/۰۳۴	۰/۰۷
		۰/۲۰۵	
		۰/۰۹۶	
		۰/۲۷۷	
		۰/۳۸۹	
معیار ۳: جامعیت قوانین حفظ مناقع شخصی مالکان داده	W_{O3}	۰/۰۳۷	۰/۰۴۵
		۰/۰۹۴	
		۰/۲۳۱	
		۰/۳۳۴	
		۰/۳۰۴	
معیار ۴: اجرای موثر قوانین	W_{O4}	۰/۰۶	۰/۰۴۱
		۰/۱۳۹	
		۰/۱۴۷	
		۰/۲۷۴	
		۰/۳۸	

جدول ۴. رتبه‌های پنج گزینه سیاست‌گذاری دسترسی به داده‌های باز- عطف به حساسیت داده‌های شخصی.

گزینه‌های سیاست‌گذاری (رجوع به جدول ۱)	بردار وزن تحقق هدف (W_t)	رتبه گزینه‌های سیاست‌گذاری	ضریب فاصله از گزینه منتخب
گزینه ۱	۰/۰۴۶۲	۵	۷/۹
گزینه ۲	۰/۱۴۵۸	۴	۲/۵
گزینه ۳	۰/۱۵۱۳	۳	۲/۴
گزینه ۴	۰/۲۹۲۸	۲	۱/۲
گزینه ۵	۰/۳۶۴۱	گزینه منتخب با رتبه یک	

۷. نتایج پژوهش و تحلیل

مقادیر نرخ ناسازگاری بدست‌آمده (جدول۳) برای کلیه ماتریس‌ها بسیار مطلوب و کمتر از آستانه ۰/۱ قرار دارند و این مطلب حاکی از سازگاری و هماهنگی نتایج جمع‌آرا بوده است. بنظر می‌رسد دومرحله‌ای کردن این پژوهش میدانی و پیگیری‌ها و مذاکرات مجدد با پاسخ‌دهندگان در هر دو مرحله، به کاهش تناقض در پاسخ‌ها و اعتبار مطلوب نتایج این پژوهش کمک بسزایی نموده است.

نتایج این پژوهش بیانگر این واقعیت است که جامعه هدف با دادن رتبه ۱ به گزینه پنج و رتبه‌های ۲ تا ۵ بترتیب به گزینه‌های چهار تا یک، دیدگاه بسته و بسیار محتاطانه‌ای را اتخاذ نموده است. فاصله تقریباً ۸ برابری گزینه یک (با رتبه ۵) و حدود ۲/۵ برابری گزینه‌های دوم و سوم از گزینه پنج (با رتبه ۱) ، موید این مطلب می‌باشد. نظری به نتایج فرعی این پژوهش، درک این دیدگاه را منطقی و ساده‌تر خواهد نمود.

از ویژگی‌های مهم مرحله اول این پژوهش، قرار دادن طیف وسیع اطلاعات خصوصی با ذکر مصادیق آن پیش روی پاسخ‌دهندگان بوده است. پاسخ‌ها به خوبی نشان می‌دهند که جز تعداد بسیار اندکی، غالب کاربران استفاده، تحلیل یا نشر این اطلاعات را به هر وسیله‌ای نیازمند کسب اجازه از صاحبان آن‌ها می‌دانند. موارد بارزی از مصادیق خصوصی بودن اطلاعات شخصی در شبکه‌ها و پیام‌رسان‌های اجتماعی و یا در پایگاه‌های داده دولتی /خصوصی، که با نظر کثیری از پاسخ‌دهندگان حتی استفاده سالم از آن‌ها نیاز به کسب رضایت از صاحبان اطلاعات دارد، عبارتند از:

- آدرس محل سکونت و محل کار.
- تصاویر، ویدیوها، پیامک‌ها و کامنت‌های خانوادگی یا غیرخانوادگی.
- خدمات و محصولات نرم‌افزاری عرضه‌شده برای فروش.
- پرونده‌های شخصی(پزشکی، قضایی، شغلی، و ...).
- افشاء حضورها یا روابط پنهان اشخاص در محیط‌های مجازی.

پاسخ‌دهندگان مجاز بودند تا در مورد هر یک از موارد بالا جداگانه نظر بدهند. بسیاری از پاسخ‌دهندگان حتی استفاده، تحلیل، یا بازنشر اطلاعات عمومی نظیر شماره تماس، آدرس ایمیل، و در مواردی پروفایل شخصی که اغلب فقط حاوی رزومه تحصیلی یا شغلی افراد و مشخصات عمومی آن‌هاست، را منوط به کسب رضایت صاحبان آن‌ها می‌دانستند. این نکته می‌تواند حاکی از حس ناامنی باشد که در اثر رشد جرائم اینترنتی به جوامع دست داده است و کشور ما نیز از آن مستثنا نیست. در موارد اندکی هم، یک مورد مثال در پاسخ‌ها خبر از تمهیداتی می‌داد که اپراتورهای ارتباطات همراه در مقابل ارسال پیامک‌های ناخواسته، امکان ارسال پیام دریافت/عدم‌دریافت اینگونه پیامک‌ها را در اختیار مشترکین خود گذاشته‌اند. با وجود این،

مواردی از دریافت مجدد چنین پیامک‌هایی پس از گذشت مدتی کوتاه خبر داده شده است.

نکته مفید و در خور تعمق دیگری که حضور گزینه ۵ را در رتبه اول منطقی نشان می‌دهد، وزن‌های داده شده به چهار معیار تحقق هدف هستند. مقادیر بردار وزن W_c در جدول(۳) نشان می‌دهد دیدگاه عمومی از ضعف اجرای قوانین بیش از تببین جامع قوانین و استقبال عمومی نگران است. به عبارت دیگر، حتی در صورتیکه دو معیار دوم و سوم بخوبی محقق گردیده باشند، یکی از دغدغه‌های اصلی عدم اجرای موثر قوانین خواهد بود.

این واقعیات نشانگر این حقیقت است که وضع قوانین دسترسی حوزه‌های پژوهشی و کسب و کاری داده‌محور به داده‌های باز، اگر جامع و کامل نباشند و یا موثر اجرا نشوند، نه فقط با استقبال عمومی روبرو نمی‌شود، بلکه خالی از بروز چالش‌ها و مخاطرات اجتماعی نخواهد بود. با وجود این، وزن‌های بدست‌آمده در W_c حاکی از آنست که بازخوردهای منفی در مورد جامعیت قوانین حفظ حریم خصوصی اشخاص (معیار دوم با وزن ۰/۲۴۶) نسبت به جامعیت قوانین حفظ منافع شخصی مالکان داده (معیار سوم با وزن ۰/۲۱۴) فقط کمی بیشتر است. این تفاوت اندک می‌تواند این نکته ظریف را به ذهن متبادر سازد که کسب منفعت مادی در ازای بهره‌برداری سالم و مُولّد از داده‌های شخصی افراد در جامعه، می‌تواند برخی از آحاد جامعه را راضی کند تا دست‌کم دایره مصادیق اطلاعات خصوصی خود را کوچکتر نمایند. اما به هیچ‌وجه نمی‌توان گفت این گرایش در جامعه ناشی از وسعت‌یابی فرهنگ و بینش اشخاص به مقوله توسعه دسترس‌پذیری به داده‌های باز است. چه بسا، انگیزه‌های مادی برای رضایت به کاربرد اطلاعات شخصی ولو به نحو سالم، در جامعه‌ای با ریشه‌های فرهنگی/مذهبی کشور ما ناشی از گسترش شرایط بد اقتصادی حتی در بین طبقه متوسط در سال‌های اخیر بوده باشد.

ابهاماتی در تبیین زمینه‌های سالم و ناسالم نیز وجود دارند که مرزهای این انتخاب را برای افراد با شرایط مختلف اقتصادی و با عقاید و باورهای متنوع جابجا می‌نمایند. این واقعیات می‌توانند در مواردی منجر به بروز آسیب‌های اجتماعی گردند. نتایج این پژوهش، آندسته از اقشار آسیب‌پذیر جامعه را که در ازای کسب منفعت مادی یا به اجبار و زور، حتی در برابر استفاده‌های ناسالم از داده‌های شخصی خود شکایتی ندارند، در برنمی‌گیرد.

از دیگر نتایج جانبی و جالب‌توجه در این پژوهش، دریافت پیشنهاداتی از سوی برخی نمونه‌های خبرگان در سطح عملیاتی است که به غنی‌ترشدن الزامات راهبردی داده شده در سطح سیاست‌گذاری کمک می‌نمایند. به طور مثال، یکی از موارد پیشنهادی لزوم دسته‌بندی و قابلیت برچسب‌گذاری بر اطلاعات واردشده از سوی کاربران در پیام‌رسان‌ها و شبکه‌های اجتماعی است که به آن‌ها به عنوان مالکین داده‌ها امکان دهد بازنشر اطلاعات در گروه‌ها یا صفحات را به حسب مورد، مجاز یا غیرمجاز نمایند(در حال حاضر، این گزینه بیشتر به حسب شخص تعبیه شده است). به‌علاوه، استفاده از گمنام‌سازی برای اهداف پژوهشی و نه کسب‌وکاری ضروری دانسته شد. همچنین، بهره‌برداری مالکین داده و انتفاع مادی آن‌ها در حوزه‌های کسب‌وکاری ولو به نحوی غیرمستقیم، مثلاً بهبود زیرساخت‌های شهری یا اهداء امتیازات و هدایا به مشترکین فعال، جزء مطالبه‌گری‌ها بود.

۱,۷ الزامات راهبردی تحقق هدف

با وجودیکه دیدگاه غالب در انتخاب یک سیاست دسترس‌پذیری باز بسیار محتاطانه است(گزینه ۵)، ولیکن فاصله بین گزینه پنج و چهار(با ضریب ۱/۲ برابر)، نشان از جایگاه بسیار نزدیک این دو گزینه به یکدیگر دارد. لذا با توجه به محدودیت‌زایی وافر گزینه پنج، بنظر می‌رسد با اعمال موثر شرایط مورد اشاره در گزینه چهارم امکان تسهیل سیاست دسترس‌پذیری به داده‌های باز و تعمیم آن به حوزه داده‌های شخصی نیز عملی باشد. این کار، با تبیین الزامات راهبردی مناسب تقویت می‌گردد. لازم است نهادهای فرهنگ‌سازی و قانون‌گذاری به ارتقاء بینش عمومی جامعه در گسترش فضای سالم و مفید پژوهش و کسب و کار کمک نمایند. همچنین، سیاست‌های بازدارنده جدی باید به اجرا درآیند که با سوءاستفاده از داده‌های شخصی در فضای مجازی بشدت و با قاطعیت برخورد شود.

با اشاره به ابهامات و همچنین موارد پیشنهادی ذکر شده توسط خبرگان، مهمترین الزامات راهبردی که برای تحقق هدف با سیاست‌گذاری نزدیک به شرایط گزینه چهار ضرورت توجه می‌یابند، عبارتند از:

- مسئله تبیین حقوق و حریم شهروندی بر داده‌های شخصی هنوز در حوزه فناوری اطلاعات مورد پژوهش جدی پژوهشگران و جامعه علمی کشور قرار نگرفته است و لازم است این موضوع در فراخوان سمپوزیوم‌ها و کنفرانس‌های علمی مشخصاً جزء محورهای فراخوان قرار داده شود.
- حمایت از سیاست‌گذاری‌های دسترسی باز به داده‌های دولتی/خصوصی با اهداف پژوهشی یا کسب‌وکارهای داده‌محور، به شرط استفاده از شیوه‌های مناسب محرمانه-سازی و تعیین مصادیق جرم و تعیین مجازات متناسب با شرایط اقتصادی روز کشور، می‌تواند به بارورشدن فضای دیجیتال کشور کمک موثری نماید.

- شناخت و مطالبه حقوق شهروندی، بدلیل عدم اعتماد به پاسخ‌گویی جدی ارکان نظارت، بندرت و با ناامیدی دنبال می‌شود. در نتیجه، نگه‌دارندگان منابع داده‌های شخصی سوءاستفاده از حقوق شهروندی را برای خود سهل می‌بینند. بنابراین، نهادهای قانون‌گذار و متولیان نظارتی نیازمند بازنگری جدی در روال‌های نظارتی خود هستند.
- کسانی که با دسته‌بندی داده‌های شخصی و تشخیص نیازها و بازارهای جدید موافق بوده‌اند، از زمره افرادی هستند که با صورت کسب‌وکارهای مجازی به شکل نوین آن در دنیا آشنا هستند و آنرا برای اشتغال جوانان و کارآفرینی مفید می‌دانند. در اغلب موارد دیگر، مخالفت‌ها جدی است و رسیدگی جهت رفع این چالش، نیازمند فرهنگ‌سازی، آموزش و اعتمادسازی در سطوح مختلف جامعه است.
- عمده کسانی که با کسب درآمد از محل داده‌های شخصی موافق بوده‌اند، با دانش فناوری اطلاعات و ارزش داده‌ها در مسیر تحول دیجیتال کمابیش آشنا بوده‌اند. بنابراین، لازم است آگاهی‌رسانی از زمینه‌های اشتغال بر بستر اینترنت و ترغیب جوانان به یادگیری مهارت‌های ساده در حوزه وب و فناوری اطلاعات در سطح جامعه نیز گسترش یابد.
- هویت شخص یا بنگاه تبلیغاتی و شرکت/موسسه‌ای که بازاریابی به نفع اوست و از اطلاعات شخصی افراد جامعه استفاده می‌کند، باید روشن و قابل‌دسترس باشد.
- گرچه ذخیره‌سازی و پردازش پیام‌های شخصی افراد که مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی آن‌ها یا وضعیت جسمانی، روانی و یا جنسی اشخاص باشد، و توزیع نتایج حاصله بدون رضایت صریح آن‌ها و به هر عنوان غیرقانونی اعلام شده است، اما لازم است مصادیق آن در فضای مجازی، شامل پیام‌رسان‌ها، شبکه‌های اجتماعی، و پایگاه‌های داده‌های دولتی/خصوصی نیز تبیین گردد.
- تعیین مجازات و جبران ضرر و زیان ناشی از تخلفات مرتکب شده در قانون کشور ذکر شده است، اما باید متناسب با شرایط اقتصادی روز کشور انعطاف‌پذیر باشند. همچنین، به نحوی برطرف‌کننده خسارات وارد آمده روحی و فکری به شاکیان باشد.
- اجرای مجازات‌های تعیین‌شده از جنبه عمومی جرم نیز، حتی در صورت رضایت شاکیان، باید کاملاً به‌روز بوده و تاثیر بازدارنده داشته باشد.
- حتی با وجود مجازات‌های مادی سنگین برای موارد تخلف، بروز این گونه جرائم از سوی طبقات مُرفَّه جامعه می‌تواند ادامه یابد. پیشنهاد اکید توسعه راهکارهای جدی و قاطع‌تر برای برخورد با طیف‌های مختلف جامعه است.

۸. نتیجه‌گیری

نیاز جامعه در کشور به حفظ حریم خصوصی اشخاص و مالکیت بر داده‌های شخصی در محیط‌های مختلف فضای مجازی، در حالی احساس می‌شود که هنوز استفاده عمومی از شبکه‌های اجتماعی و پیام‌رسان‌های خارجی در کشور ما جایگاه قانونی ندارند. علی‌رغم این، بسیاری از کسب‌وکارهای اینترنتی داخلی در این محیط‌ها راه‌اندازی شده‌اند و حجم زیادی از اطلاعات شخصی افراد در این محیط‌ها، منبع بروز تخلفات و جرائم اینترنتی در داخل و البته خارج از کشور نیز شده است. این در حالیست که نسخه‌های داخلی شبکه‌های اجتماعی یا پیام‌رسان‌ها هنوز در بستر شبکه ملی اطلاعات کشور، بدلیل آماده نبودن زیرساخت‌های فنی و امنیتی لازم، پاسخگوی نیاز کاربران و کسب‌وکارهای داده‌محور در کشور نیستند. از طرفی، مسئله دسترسی باز از طریق فضای مجازی به داده‌های خصوصی اشخاص در پایگاه‌های داده دولتی/خصوصی نیز از نظام قانونی روشنی برخوردار نیست. مسئله مهمتر اینکه فرهنگ داده‌پردازی بر اطلاعات پرونده‌های خصوصی افراد جامعه با حفظ محرمانگی و سلامت پژوهش هنوز نهادینه و مدیریت نشده است. بنابراین، یکی از پایه‌های بنیادی سیاست‌گذاری در بحث حفظ حریم خصوصی و مالکیت داده‌های شخصی افراد در فضای مجازی، نخست روبرو شدن قانون‌گذار با واقعیات فضای مجازی است که سال‌هاست در جامعه به شکل غیررسمی مورداستفاده کاربران حقیقی/حقوقی قرار گرفته است. در گام دوم، ضرورت وجودی چنین بسترهایی لازم می‌دارد سیاست‌گذاران و قانون‌گذاران برای ایجاد بسترهای مشابه داخلی مانند شبکه ملی اطلاعات و شبکه‌های اجتماعی و پیام‌رسان‌های بومی، از بُعد زیرساختی و امنیتی تلاش زیادی برای حمایت از توانمندی‌های داخلی و بالا بردن اعتماد عمومی در جامعه نمایند. این اعتماد لازم است به نحوی ایجاد گردد که کلیه نیازهای کسب‌وکاری، پژوهشی، و استفاده‌های عمومی کاربران عادی در حد عرف جامعه آزاد باشد و به صورتی امن و با کیفیت فراهم گردد.

در این مقاله، دو محور مالکیت داده‌های شخصی در زنجیره ارزش کسب‌وکارهای داده‌محور فضای مجازی و همچنین مسئله چالش‌برانگیز حفظ حریم خصوصی در سیاست دسترسی باز به داده‌های پژوهشی به روش توصیفی - تحلیلی بررسی و وضعیت سیاست‌گذاری در این دو مقوله و قوانین موجود در داخل کشور مورد

بررسی و نقد قرار گرفت. روش دلفی محوریت کار قرار گرفت و با یک مطالعه میدانی در مرحله اول نشان داده شد که برای اجرای سیاست‌های دسترس‌پذیری به داده‌های باز در داخل کشور، معیارهای تحقق هدف و گزینه‌های ممکن کدامند. روشن شد که قوانین موجود در کشور با رشد روزافزون مطالبات حوزه‌های پژوهشی به دسترسی باز به داده‌ها و همچنین کسب‌وکارهای داده‌محور در بستر فضاهای مجازی همخوانی ندارند. نقاط ضعف موجود از چهار منظر اهمیت دارند:

- شمول‌ناپذیری قوانین موجود بر مصادیق جرم در صیانت از حریم خصوصی و حقوق مالکان داده‌های شخصی.
- نادیده‌انگاری حقوق کاربران و مصرف‌کنندگان به عنوان بخشی از زنجیره ارزش.
- به‌روز نبودن مجازات‌ها با شرایط اقتصادی کشور
- عدم ضمانت اجرایی کافی در برخورد با تخلفات.

در مرحله دوم، سیاست‌گذاری‌های ممکن برای تحقق هدف مورد سنجش قرار گرفتند و رتبه‌بندی آن‌ها بدست آمد. نتایج رتبه‌بندی گویای این واقعیت است که مسئله اصلی در تحقق هدف موردنظر در این پژوهش، ابتدا عدم‌اطمینان به اجرای موثر قوانین و سپس جامعیت نداشتن قوانین صیانت از حریم خصوصی اشخاص و احترام به مالکیت حقوق آن‌ها در فضای مجازی است.

به نظر می‌رسد کشور ما هنوز با گرایش جهانی به سمت تحول دیجیتال و ایجاد فضای دسترسی باز به داده‌های پژوهشی، که امروزه بخش بزرگی از آن داده‌های شخصی نیز محسوب می‌شوند، همسو نیست و بدلایل اجتماعی و فرهنگی عمیقی که از آن سراغ داریم از آمادگی لازم برخوردار نیست. باید تاکید نمود عدم‌رسیدگی به سیاست‌گذاری‌ها و قوانین جامع و کامل برای ساماندهی و نظارت موثر بر فعالیت‌های کسب‌وکاری در فضای مجازی، موجب رشد بی‌رویه و افسارگسیخته بسیاری از مشاغل کاذب با ماهیت‌های ناهنجاری از نوع واسطه‌گری، اقدامات غیراخلاقی، مجرمانه، و فریبکاری در این فضا خواهد گردید. این مقاله تلاش نمود با اتخاذ رویکرد راهبردی، سیاست‌های ممکن و الزامات قانونی برای تحقق دسترس‌پذیری کاربران حقوقی/حقیقی به داده‌های باز در فضای مجازی را، عطف به حساسیت داده‌های شخصی پیشنهاد دهد.

مراجع

[۱] Open Data Institute, Startups & fostering innovation, ۲۰۲۲.
https://theodi.org/service/startups-fostering-innovation/opportunities-for-startups/startup-accelerator.

[۲] Kitsios F., N. Papachristos and M. Kamariotou, "Business Models for Open Data Ecosystem: Challenges and Motivations for Entrepreneurship and Innovation", Proceedings of ۱۹th IEEE International Conference on Business Informatics (CBI'۱۷), Thessaloniki, Greece, pp. ۳۹۸-۴۰۸, ۲۰۱۷, DOI: ۱۰,۱۱۰۹/CBI.۲۰۱۷,۵۱
https://ieeexplore.ieee. Org/document/۸۰۱۰۷۴۴/.

[۳] Djaghloul Y., Martin S., Turki S, "T۱,۱,۱ State of the art report on methodologies", Ver. ۱,۰, Interreg-North West Europe (EU), Dec. ۳۰, ۲۰۱۶.

[۴] OECD, "OECD Principles and Guidelines for Access to Research Data from Public Funding", OECD Publications, ۲, rue André-Pascal, ۷۵۷۷۵ Paris Cedex ۱۶, Printed in France, ۲۰۰۷

[۵] OECD, "OECD Science, Technology and Innovation Outlook ۲۰۱۸: Adapting to Technological and Societal Disruption", Chap. ۶, page ۱۴۵, OECD Publishing , Paris, ۱۹ Nov. ۲۰۱۸.
Annual ISSN: ۲۵۱۸۶۱۶۷ (online):
https://doi.org/۱۰,۱۷۸۷/sti_in_outlook-۲۰۱۸-en

[۶] Katbi A. K., Al-Ammary J., "Open Government Data in Kingdom of Bahrain: Towards an Effective Implementation Framework", Colledge of Information Technology, Univ. of Bahrain, Zallaq, Kingdom of Bahrain., Springer Nature Switzerland AG ۲۰۱۹ Á. Rocha et al. (Eds.): WorldCIST'۱۹ ۲۰۱۹, AISC ۹۳۰, pp. ۶۹۹–۷۱۵, ۲۰۱۹. https://doi.org/۱۰,۱۰۰۷/۹۷۸-۳-۰۳۰-۱۶۱۸۱-۱_۶۶.

[۷] Saxena S., "Evaluation of the National Open Government Data (OGD) Portal of Saudi Arabia", Politics and Technology in the Post-Truth Era, Emerald Publishing Limited, ISBN: ۹۷۸-۱-۷۸۷۵۶-۹۸۴-۳, eISBN: ۹۷۸-۱-۷۸۷۵۶-۹۸۳-۶, ۷ May ۲۰۱۹.

[۸] Aarshi S. et al., "Dimensions of Open Government Data Web Portals: A Case of Asian Countries", International Journal of Advanced Computer Science and Applications (IJACSA), pp. ۴۵۹-۴۶۹, Vol. ۹, No. ۶, ۲۰۱۸.

[۹] European Commission, "Regulation (EU) ۲۰۱۶/ ۶۷۹ of the European Parliament and of the Council, – of ۲۷ April ۲۰۱۶ – 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 ۹۵/ ۴۶/EC (General Data Protection Regulation)", Official

Journal of the European Union, Document ۳۲۰۱۶R۰۶۷۹, ۲۰۱۶. http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:۳۲۰۱۶R۰۶۷۹&from=EN

[۱۰] Lavoie, B., "The Open Archival Information System (OAIS) Reference Model: Introductory Guide (۲nd Edition)", Principal Investigator for the Series Neil Beagrie. Retrieved ۰۷ ۰۳, ۲۰۱۴. https://www.Dpconline .org/docs/technology-watch-reports/۱۳۵۹-dpctw۱۴-۰۲/file

[۱۱] OECD, "Towards New Principles for Enhanced Access to Public Data for Science, Technology and Innovation", Joint CSTP-GSF Workshop, Paris, March ۱۳, ۲۰۱۸.

[۱۲] Wilkinson, M. et al., "The FAIR Guiding Principles for scientific data management and stewardship", Scientific Data ۳, Article No. ۱۶۰۰۱۸, Nature Communications, ۲۰۱۶.

http://dx.doi.org/۱۰. ۱۰۳۸/sdata.۲۰۱۶,۱۸

[۱۳] OECD, "Draft Policy Framework on Sound Public Governance", GOV/PGC (۲۰۱۸) ۲۶/REV ۱, page ۵۹, ۲۰۱۸.

[۱۴] M., Luke, J., Ferdinand, A. & Chamravi, D., "An Evaluation Framework to Improve Aboriginal and Torres Strait Islander Health", The Lowitja Institute, Melbourne, page ۳۸, Feb. ۲۰۱۸.

[۱۵] Harison E., "Who owns enterprise information? Data ownership rights in Europe and the U.S.", Elsevier, Information & Management, Vol. ۴۷, pp. ۱۰۲–۱۰۸, ۴ Jan. ۲۰۱۰, DOI: ۱۰,۱۰۱۶/j.im.۲۰۰۹,۱۲,۰۰۱.

[۱۶] Vilminko-Heikkinen R., Pekkola S., "Changes in roles, responsibilities and ownership in organizing master data management", International Journal of Information Management Vol. ۴۷, pp. ۷۶-۸۷, August ۲۰۱۹.

https://doi.org/۱۰,۱۰۱۶/j.ijinfomgt.۲۰۱۸,۱۲,۰۱۷

[۱۷] Dyche J. and Polsky A., "۵ Models for Data Stewardship: a SAS Best Practice white paper", SAS Institute Inc., ۲۰۱۳.

[۱۸] V. Janeˇcek, "Ownership of personal data in the Internet of Things", Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol: ۳۴, Issue ۵, pp. ۱۰۳۹-۱۰۵۲, October ۲۰۱۸.

https://doi.org/۱۰,۱۰۱۶/j.clsr.۲۰۱۸,۰۴,۰۰۷

[۱۹] Zhou, M., Technovation, "Ownership in the virtual world and the implications for long-term user innovation success", ۲۰۱۸.

https://doi.org/۱۰,۱۰۱۶/j.technovatio n.۲۰۱۸,۰۶,۰۰۲

[۲۰] Carrara W., Enzerink S., Oudkerk F., Radu C. & van Steenbergen E. "Open Data Goldbook for Data Managers and Data Holders", Jan. ۲۰۱۸.

http://www.europeandataportal.eu

[۲۱] Simperl E., O'Hara K. & Gomer R., "Open Data and Privacy", Electronics and Computer Science, University of Southampton, June ۲۰۱۶.

http://www.europeandataportal.eu/

[۲۲] Ali M. Al-Khouri, "Data Ownership: Who Owns 'My Data'?", The British Institute of Technology and E-Commerce, London, UK, International Journal of Management & Information Technology, ISSN: ۲۲۷۸-۵۶۱۲ Vol. ۲, pp. ۲-۳, No ۱, Nov. ۲۰۱۲

[۲۳] EU Regulation, Intersoft Consulting, "General Data Protection Regulation", ۲۰۱۸

https://gdpr-info.eu/

[۲۴] کروبی، محمدتقی، "اتحادیه اروپا و بحث حمایت از داده‌های شخصی و حریم خصوصی در ارتباطات الکترونیکی"، مرکز تحقیقات مخابرات ایران، تهران، ناشر: بقعه، صفحات ۳۱-۳۲، ۱۳۸۴ ه. ش.

[۲۵] بیانیه رئیس جمهوری اسلامی ایران، "منشور حقوق شهروندی"، معاونت حقوقی ریاست جمهوری، آذر ماه ۱۳۹۵ ه. ش.

[۲۶] مصوبه جلسه شورای عالی اداری، "حقوق شهروندی در نظام اداری"، ۹ بهمن ماه ۱۳۹۵ ه. ش.

[۲۷] قانون حمایت حقوق مولفان و مصنفان و هنرمندان، مصوبات مجلس شورا، مرکز پژوهش‌های مجلس شورای اسلامی، ماده ۳۳، دوره ۲۲، چاپ ۱، شماره جلد ۸، شماره صفحه ۴۱۴۵، تاریخ تصویب ۱۳۴۸/۱۰/۱۱ ه. ش.

[۲۸] آیین‌نامه اجرایی و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوبات مجلس شورا، مرکز پژوهش‌های مجلس شورای اسلامی، ماده ۱۷، دوره ۶، جلد ۱، تاریخ تصویب ۱۳۷۹/۱۰/۴ ه. ش.

[۲۹] قانون تجارت الکترونیکی ۱۳۸۲/۱۰/۱۷ ه. ش. مجلس شورا، مرکز پژوهش‌های مجلس شورای اسلامی.

[۳۰] قانون جرائم رایانه‌ای مصوبات مجلس شورا، مرکز پژوهش‌های مجلس شورای اسلامی، ماده ۵۶، دوره ۸، شماره ابلاغیه: ۱۶۳۰۶/۱۲۱، ۱۳۸۸/۰۳/۰۵ ه. ش.

[۳۱]حبیبی آ. ، ایزدیار ص. ،"تصمیم‌گیری چندمعیاره فا" ، ناشران: سیمای دانش، آذر، ۱۳۹۳، ص ۳۲.