

سناریوهای آینده سیستم‌های داده شهروند در افق ۱۴۱۰ و امنیت ملی

عبدالرحیم پدram^۱

محمدهادی قاسمی*^۲

نوع مقاله: پژوهشی

چکیده

در حال حاضر تولید داده‌های مربوط به افراد، شرکت‌ها و به‌طور ویژه داده‌های شهروندان و استفاده از آن، به‌سرعت رو به رشد است. امروزه بیش از هر زمان دیگری در اینترنت، مسافرت، تفریح، تجارت و تقریباً در همه جنبه‌های زندگی روزمره، ردپای دیجیتالی بر جای می‌گذاریم و این داده‌ها ارزش بالقوه و بسیار زیادی را برای مصرف‌کنندگان، شرکت‌ها، سازمان‌های دولتی و امنیتی فراهم می‌کنند. در عصر دیجیتال به‌راحتی می‌توان طیف متنوعی از داده‌ها و اطلاعات شهروندان را برای اهداف وسیع‌تر و موضوعاتی که در گذشته پیش‌بینی نشده بود، بکار برد، همچنین اتفاقات پیش‌بینی نشده در آینده مانند همه‌گیری بیماری کرونا نیز می‌تواند تأثیرات عمیق‌تری در استفاده و اشتراک‌گذاری داده‌های شهروندان و تغییر نگرش عمومی نسبت به این موضوع ایجاد کند. در پژوهش حاضر با جامعه آماری شامل خبرگان مرتبط با موضوع و ۱۲ نمونه آماری، ضمن استفاده از روش سناریو پردازی، چهار سناریو آینده پیرامون سیستم‌های داده شهروند ارائه شده است که این سناریوها بیان می‌دارند هنجارهای جهانی، مدل‌های تجاری، قوانین بین‌المللی و رویکردهای دولت‌ها در مورد داده‌های شهروندان می‌توانند توسعه پیدا کرده و تغییرات قابل توجهی داشته باشند. در برخی از سناریوها، همگرایی در حاکمیت داده‌ها وجود دارد و داده‌ها با آزادی بیشتری در سراسر جهان جابجا می‌شوند. در برخی دیگر، دولت‌ها رویکردهای واگرا و اغلب محدودکننده‌تری دارند و داده‌ها به‌طور فزاینده‌ای بومی‌سازی می‌شوند؛ لذا در فضای عدم قطعیت آینده، درعین حال که تشخیص می‌دهیم همکاری‌های بین‌المللی اجتناب‌ناپذیر است در کنار آن مدیریت داده‌های ملی نیز حیاتی است و باید مسیری را طی کنیم که امنیت ملی و منافع کشورمان به بهترین وجه تضمین شود.

واژه‌های کلیدی:

سناریو پردازی، سیستم‌های داده، امنیت ملی، سناریوهای آینده سیستم‌های داده شهروندی.

^۱ استادیار و عضو هیئت‌علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران.

^۲ دانشجوی دکتری آینده‌پژوهی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران.

* نویسنده مسئول: Email: mh.Ghasemi110@ut.ac.ir



مقدمه

جهان در آستانه یک انقلاب بزرگ داده قرار دارد و در هر ثانیه بر حجم اطلاعات دیجیتالی‌ای که بین مشاغل، دولت‌ها و مردم به سرعت در حال گسترش هستند، اضافه می‌شود. داده‌ها اکنون به‌طور فزاینده‌ای زیربنای زندگی روزمره ماست و از آن‌ها برای خرید آنلاین، نظارت بر فعالیت‌های کاری، امور بانکی و مدیریت حساب‌های شخصی و حتی فعالیت‌های ورزشی خود استفاده می‌کنیم. این داده‌ها و سامانه‌های مرتبط با آن تبدیل به جنبه‌های مهمی از تجارت بین‌المللی و جهانی شده است و حتی در حال حاضر به‌مثابه یک سلاح مهم در نبرد علیه ویروس کرونا مورد استفاده قرار گرفته است. این تحول دیجیتالی فرصت عظیمی برای کشورها و حکومت‌ها فراهم می‌آورد تا با استفاده از قدرت داده‌ها، بتوانند رشد اقتصادی و بهره‌وری را افزایش داده و نوآوری در حکمرانی را پیش ببرند، خدمات عمومی را بهبود بخشند، روابط بین‌الملل را بر اساس ظرفیت‌های جدید بازسازی کنند و در نهایت رضایتمندی بیشتری را برای شهروندان خود رقم بزنند (GOFS, 2020: 1). فن‌آوری‌های نوظهور، شوک‌های اقتصادی و اجتماعی، تغییرات ژئوپلیتیکی و بحران‌های جهانی - مانند شیوع بیماری کرونا - همگی توانایی تغییر قابل توجه در روندهای فعلی را دارند. از این منظر و با توجه به تحولات و نگرش جهانی‌ای که نسبت به داده‌ها وجود دارد باید از توانایی و استراتژی خودمان در مقابل شوک‌های اجتناب‌ناپذیر آینده و سازگاری مناسب آن با عدم قطعیت‌های پیش رو اطمینان حاصل کنیم. می‌بایست از اطلاعات و داده‌های افراد و جامعه خود محافظت کنیم و به‌طور هم‌زمان مانند برخی کشورها اقدام به تدوین راهبردهای داده‌های ملی نماییم چراکه یک سیستم داده موفق، نیاز به انعطاف‌پذیری و واکنش سریع نسبت به تغییرات دارد. این موارد می‌تواند در اثر بی‌توجهی و یا سو مدیریت، به افراد، جامعه و امنیت ملی آسیب برساند (GOFS, 2020: 4).

امروزه دولت‌ها می‌توانند از اهرم‌ها و سیاست‌های مختلف برای شکل دادن و بهره‌برداری از سیستم‌های داده داخلی استفاده کنند. این موارد می‌تواند شامل مقررات مربوط به حریم خصوصی و محافظت از داده‌ها، سیاست‌های اقتصادی مبتنی بر تحلیل داده‌های شهروندان، استفاده از داده‌ها برای امنیت ملی، نظارت‌های قانونی و به اشتراک‌گذاری داده‌های بخش دولتی باشد. رویکردهای منطقه‌ای برخی از کشورها در این خصوص تمایل به توسعه ارگانیک با توجه به هنجارهای موجود اما با اهداف ژئوپلیتیک سازگار با آینده است. در یک دسته‌بندی کلی می‌توان رفتارهای سه منطقه جغرافیایی متفاوت را در این خصوص به شکل زیر تفکیک کرد:

- دولت چین، کنترل قوی داده‌های شهروندان همراه با محدودیت در انتقال بین‌المللی، امنیت اقتصادی و اجتماعی ملی را در اولویت قرار داده است. چین با کمک سیستم

مبتنی بر داده‌های شهروندان با نام «سیستم اعتباری- اجتماعی ملی^۱» اهداف تعریف‌شده در امنیت ملی خود را شامل جمع‌آوری داده‌های مالی، انتظامی، تجاری، رسانه‌های اجتماعی و سایر داده‌ها به‌منظور نظارت بر انطباق شهروندان با تعهدات شهروندی، تعیین مجازات و تشویق برخی رفتارها، مدیریت می‌کند (Tanner, 2017).

- اتحادیه اروپا با اندکی تفاوت در بین برخی کشورهای عضو، رویکردهای امنیت ملی، حقوق شهروندی و رقابت در بازار داخلی را در اولویت قرار داده است. ایجاد سپر حریم خصوصی اتحادیه اروپا، توسعه قوانین و مقررات مربوط به داده‌ها مانند مقررات جامع عمومی حفاظت از داده‌ها^۲ از جمله اقداماتی بوده است که به نظر می‌رسد پیرامون حقوق و مسئولیت‌های جدید اعمال‌شده توسط این‌گونه آیین‌نامه‌ها در خصوص داده‌های شهروندان، به‌طور گسترده‌ای مورد استفاده قرار گرفته است (Scott & Cerulus, 2018).
- ایالات متحده آمریکا، مطابق با مواضع اقتصادی گسترده‌تر خود، رویکرد کاملاً مداخله‌جویانه‌تری نسبت به داده‌ها اتخاذ کرده است و به‌طور فعال در تلاش است از داده‌های شهروندی در حمایت از امنیت ملی استفاده کند. اگرچه در حال حاضر قانون جامع حفاظت از داده‌های فدرال وجود ندارد اما قوانینی مربوط به بخش‌های خاص وضع شده و علیرغم وجود تفاوت‌هایی در روش پیاده‌سازی قوانین فوق در بین ایالت‌های مختلف، با توجه ویژه‌ای از این قوانین پشتیبانی می‌شود (Noordyke, 2020).

همان‌طور که مشاهده می‌شود اولویت‌های مختلف دولت‌ها باعث شکل‌گیری سیستم‌های داده‌ای متفاوت در این سه منطقه شده است. همچنین ارزش‌های اجتماعی شهروندان ممکن است در شکل‌گیری سیستم‌های داده نقش داشته باشند. به‌عنوان مثال، شواهد نشان می‌دهد که مردم در چین معمولاً سطح بالاتری از اعتماد و نگرانی کمتری درباره استفاده از داده‌ها و حریم خصوصی را نسبت به کشورهای اتحادیه اروپا و آمریکا از خود نشان می‌دهند (GOFS, 2020: 4).

داده‌ها و به‌طور مشخص در این مقاله، داده‌های اشخاص که «داده‌های شهروندان» نامیده می‌شوند، از نظر حجم و تنوع به‌سرعت در حال افزایش است. استفاده و به اشتراک‌گذاری این داده‌ها می‌تواند مزایای زیادی برای اقتصاد، فرهنگ، سیاست و پویایی جامعه به همراه داشته باشد. مثلاً در طرح شناسایی دهک‌های مختلف جامعه برای تخصیص یارانه می‌توان از داده‌های

¹. Chinese Social Credit System

². General Data Protection Regulation (GDPR)

شهروندان و تجمیع آن‌ها به منظور کشف میزان توانگری اقتصادی و برنامه‌ریزی برای توزیع یارانه‌ها استفاده کرد اما همین اطلاعات در جای دیگر می‌تواند ملاک صدور برگه‌های مالیاتی برای افراد و مشاغل مختلف و بروز اعتراضاتی در خصوص ورود به حریم خصوصی گردد. لذا این مقاله در تلاش است تصمیمات دولت را با نگاه کل‌نگرانه نسبت به داده‌های شهروندان مورد بررسی قرار دهد. این بررسی می‌تواند در ایجاد چارچوب‌های حاکمیت داده، ارزش‌ها و رفتارهای عمومی، فناوری‌ها و مدل‌های تجاری متمرکز بر داده، توسعه دولت هوشمند و دولت الکترونیک، حفاظت از امنیت ملی و ارائه تضمین‌های قابل قبول در خصوص حفظ حریم خصوصی شهروندان و جلوگیری از غافلگیری در آینده مورد استفاده قرار گیرد.

مبانی نظری پژوهش

داده‌های شهروندی

داده‌ها در مورد افراد به‌طور مداوم از طریق تعامل با طیف عظیمی از خدمات دولتی و خصوصی، با و بدون آگاهی و رضایت ایشان تولید می‌شود. در اینجا، ما از اصطلاح «داده‌های شهروندی»^۱ استفاده می‌کنیم تا به هر داده‌ای که به هر فرد یا گروهی از افراد و در هر کشوری، مربوط می‌شود، تعمیم داده شود. این داده‌ها ممکن است توسط هر تعداد سازمان دولتی و یا بخش خصوصی نگهداری شوند. نمونه‌هایی از داده‌های شهروندان عبارت‌اند از:

- شناسه‌های منحصر به فرد (به‌عنوان مثال کد ملی یا شماره گذرنامه)؛
- شناسه‌های مشترک (به‌عنوان مثال نام، تاریخ تولد، آدرس)؛
- داده‌های بیومتریک (به‌عنوان مثال DNA^۲ و اثر انگشت)؛
- سوابق پزشکی، آموزشی یا موارد دیگر؛
- داده‌های تولید شده یا مشاهده شده از طریق تعامل با سرویس‌ها یا دستگاه‌ها مانند:
- تاریخچه مرور اینترنت، ردیابی کوکی‌ها و آدرس‌های IP^۳؛
 - داده‌های ویدئویی (به‌عنوان مثال تصاویر دوربین مداربسته)؛
 - داده‌های استفاده از ابزار (به‌عنوان مثال از کنتورهای هوشمند)؛
 - داده‌های تولید شده از طریق تعامل با دستگاه‌های اینترنت اشیا (به‌عنوان مثال صوت ضبط شده صدا)؛

^۱. Citizenship data

^۲. Deoxyribonucleic

^۳. شانی پروتکل اینترنت (Internet Protocol Address) یا به اختصار آدرس آی‌پی (IP Address) نشانی عددی است که به هر یک از دستگاه‌ها و رایانه‌های متصل به شبکه رایانه‌ای که بر مبنای نمایه TCP/IP (از جمله اینترنت) کار می‌کند، اختصاص داده می‌شوند.

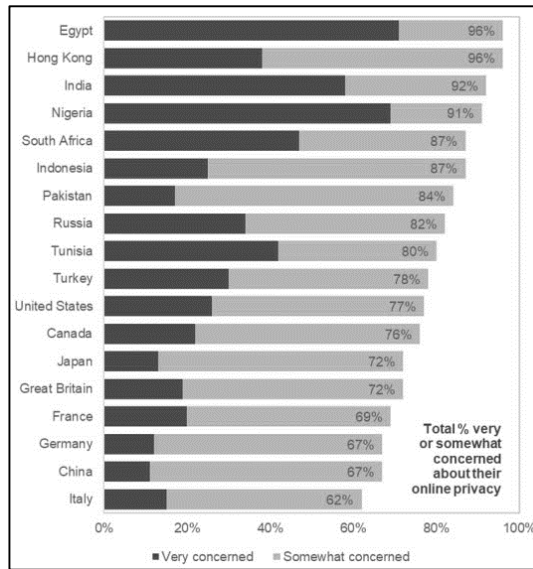
- داده‌های مصرف‌کننده (به‌عنوان مثال رفتار خرید آنلاین)؛
- داده‌های شبکه‌های اجتماعی؛
- داده‌های مکان (به‌عنوان مثال از طریق برنامه‌های ردیاب)؛
- فراداده مربوط به داده‌های متصل به افراد (مانند زمان و نحوه تولید داده‌ها مانند تراکنش‌های بانکی)؛ و
- داده‌های تجمیع شده و جمع‌آوری شده مانند اطلاعات سرشماری (Li & Mocko, 2020).

سیستم‌های داده

اصطلاح «سیستم داده»¹ برای افراد با پیشینه متفاوت کاری و دانشی، معانی متفاوتی خواهد داشت. در این مقاله دید گسترده‌ای از سیستم‌های داده داریم که شامل: افراد، فرایندها و فناوری‌های مربوط به جمع‌آوری، کشف، ذخیره‌سازی، تجزیه و تحلیل، پیوند دادن و به اشتراک‌گذاری داده‌های شهروندان است. این طیف گسترده شامل افرادی هم که داده‌ها را جمع‌آوری می‌کنند (به‌عنوان مثال در تعاملات پزشکی و بیمار)، حس‌گرها و سایر فناوری‌های تولید داده، استانداردهای فنی، سیستم‌هایی که داده‌ها را ذخیره و پردازش می‌کنند، چارچوب‌های قانونی و اخلاقی مرتبط با داده‌ها، نیز خواهد بود. انگیزه‌ها، ارزش‌ها، رفتار و سایر پویایی‌های بازیگران در این سیستم‌های گسترده نیز باید مورد توجه قرار گیرد. این اقلام می‌توانند شامل انتظارات شهروندان و رفتار آن‌ها در رابطه با جمع‌آوری و استفاده از داده‌ها، مشوق‌های تجاری و مدل‌های تجاری، انگیزه‌ها و اقدامات سایر بازیگران، از دولت‌ها گرفته تا گروه‌های لابی یا بازیگران مخرب همگی در تعریف جامعی از سیستم داده قرار می‌گیرند (GOFS, 2020: 14).

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

¹. Data System



نمودار (۱) ابراز نگرانی شهروندان برخی از کشورها در مورد حریم خصوصی آنلاین خود بر اساس نظرسنجی بین‌المللی انجام‌شده (CIGI-Ipsos, 2019)

چرا داده‌های شهروندان برای دولت‌ها مهم است؟

داده‌ها به‌طور کلی شامل جنبه‌های اقتصادی، امنیتی و اجتماعی هستند. افزایش حجم و تنوع داده‌ها در مورد افراد که توسط تعداد فزاینده‌ای از دستگاه‌های دیجیتال تولید می‌شود، یک فرصت بزرگ است. این پتانسیل برای افزایش بهره‌وری و تجارت (UNCTAD, 2019) و حمایت از مشاغل و ایجاد شغل‌های جدید (Deloitte, 2017)، افزایش کارایی و دامنه تحقیقات علمی و هدف‌گذاری بهتر سیاست‌ها و خدمات عمومی، دارای سودآوری برای جامعه است. علاوه بر این، موارد مهم‌تری در ارتباط با استفاده از داده‌های شهروندان هم در بُعد مثبت (تجمیع داده‌ها و ایجاد و ارزش‌افزوده جدید) و هم در بُعد منفی (نفوذ به حریم خصوصی) وجود دارد (Beagrie & Houghton, 2016). در نمودار (۱) میزان ابراز نگرانی شهروندان برخی از کشورها در مورد حریم خصوصی خود قابل مشاهده است.

امنیت ملی

واژه امنیت از جمله واژه‌هایی است که به لحاظ برخی شباهت‌ها، دارای مفهومی سیال، متنوع و صورتی متغیر بوده که گستره بسیار وسیعی در ابعاد مختلف فردی و اجتماعی را شامل می‌شود. طبیعی است ارائه تعریفی کامل و جامع برای این‌گونه مفاهیم کاری دشوار است (بخشی، ۱۳۹۵: ۴۲). می‌توان گفت امنیت ملی شامل تعقیب روانی و مادی ایمنی است و اصولاً جزء مسئولیت حکومت‌های ملی است تا از تهدیدات مستقیم خارجی نسبت به بقای رژیم‌ها، نظام شهروندی و

شیوه زندگی شهروندان خود ممانعت به عمل آورد (ماندل، ۱۳۸۷: ۵۲). در حال حاضر فضای سایبری و بخصوص اینترنت، دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس بودن، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد عادی به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آن‌ها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱). حمله سایبری چیزی متفاوت از جنگ سایبری است. حمله سایبری اختلال در صحت یا درستی داده‌ها و بانک‌های اطلاعاتی است که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، صورت می‌گیرد (Rodriguez, 2006: 9). تحلیل‌گران بر این باورند که اهمیت این «مسائل جدید» نه تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد. در عین حال، انتقادی که بر ادبیات موجود امنیت وارد است این است که اغلب این متون به تهدیدهای سایبری به‌عنوان یکی از چالش‌های امنیتی جدید که در این زمینه بسیار هم پراهمیت به نظر می‌رسد، توجه اندکی داشته‌اند (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱). لذا بحث درباره تهدیدهای سایبری تأثیر گرفته از انقلاب مداوم اطلاعات رایانه‌ای و سیستم‌های داده است که ناشی از پویایی انتشار اطلاعات و تکنولوژی‌های ارتباطات در همه جنبه‌های زندگی انسان است (Cavetly and Brunner, 2007: 15).

سناریو پردازی

سناریو^۱ نگاه به آینده از دریچه و چشم‌اندازی ویژه است که در چهارچوب آن، داستان تصویر شده دارای سازگاری منطقی است و رخدادهای بیرون از حقیقت‌نمایی و خردورزی در تاروپود آن، راهی ندارد. سناریو، یعنی داستانی درباره آینده که معمولاً شامل داستان‌هایی از گذشته و حال هم می‌شود (بل، ۱۳۹۲: ۵۴۹). در واقع، هدف از تدوین سناریوها، خلق فضای بررسی احتمالی آینده‌های ممکن^۲، به‌گونه‌ای است که بتوان پابرجایی سیاست‌ها را در برابر طیفی از چالش‌های

1. Scenario

2. Possible Futures

آینده‌آزمود؛ سناریوها به ما کمک می‌کنند تا عوامل شگفتی‌ساز^۱ را در چهارچوب چالش‌ها یا فرصت‌های بالقوه بشناسیم. دو اصل اساسی در آینده‌پژوهی وجود دارد؛ یکی اینکه آینده قطعی نیست و آینده‌های بدیل^۲ وجود دارد و دوم اینکه می‌خواهیم از غافلگیری پیشگیری کنیم و یک مطلوبیتی از آینده داشته باشیم (پدارم و زالی، ۱۳۹۷). آینده‌های بدیل در قالب سناریوها بررسی می‌شوند تا مطلوب یا نامطلوب بودن آن‌ها آشکار شود. سناریو، محصول آرمانی آینده‌پژوهی است (بیشاب و دیگران، ۱۳۸۸: ۴).

عدم قطعیت و انواع آن

عدم قطعیت^۳ به آن عواملی اشاره می‌کند که نتایج ناشناخته دارد و هنوز اتفاق نیفتاده است و نمی‌توان برای آن میزان احتمال وقوع خاصی را پیش‌بینی کرد. این عناصر همواره به‌طور ذاتی به عناصر نسبتاً مشخص مرتبط هستند و می‌توانید با به سؤال کشیدن مفروضات خود در زمینه این عناصر، آن‌ها را پیدا کنید (شوارتز، ۱۳۹۰: ۲۲۶).

پیشران‌ها

ساده‌ترین و شیواترین تعریف پیشران^۴، نیروهای بزرگ تغییر است. پیشران‌ها نیروهایی هستند که بر پیامد رویدادها تأثیر دارند. به‌عبارت‌دیگر عناصری که باعث حرکت و تغییر در طرح اصلی سناریوها شده و سرانجام داستان‌ها را مشخص می‌کنند (شوارتز، ۱۳۹۰: ۲۲۶). پیشران این پتانسیل را دارد که صحنه را با تحولی اساسی روبه‌رو سازد؛ پیشران‌ها از دو جهت برای ما دارای اهمیت هستند، از یک‌سو، در مقام توصیف، آینده را بر مبنای آن‌ها توصیف می‌کنیم و از سوی دیگر، در مقام تجویز و مبتنی بر پیشران‌ها، آینده را مطابق با میل خود تغییر می‌دهیم (پدارم و زالی، ۱۳۹۷).

کنشگران

اگر رخدادهای را به دو بخش طبیعی و انسان‌ساز تقسیم کنیم، هسته اصلی عموم پژوهش‌های سناریونویسی، مطالعه رفتار اجتماعی انسان‌ها و رخدادهای انسان‌ساز است. در حوزه مسائل امنیتی، سیاسی و فرهنگی، اهمیت مطالعه رفتار بازیگران بیشتر از حوزه‌های اقتصادی، علمی و فنی است. کنشگران تأثیرگذار آن‌هایی هستند که قدرت اثر گذاشتن بر معیارهای مطلوبیت سازمان را داشته باشند. این کنشگران می‌توانند دولتی، خصوصی، گروه‌های فراملی و فرو ملی،

1. Wild Cards

2. Alternative Futures

3. Uncertainty

4. Driving Force

سازمان‌های بین‌المللی و یا افراد باشند. رفتار و تصمیمات کنشگران می‌تواند بر آینده موضوع موردبررسی، اثرگذار باشد (پدram و احمدیان، ۱۳۹۴: ۱۸۶-۱۸۵).

پیشینه پژوهش

مطابق با بررسی‌های انجام‌شده مشخص شد در منابع فارسی، پژوهشی که ضمن شناسایی سیستم‌های داده شهروند به معرفی سناریوهای مرتبط با آن در آینده و اهمیت آن از منظر امنیت ملی بپردازد، انجام‌نشده است و لذا این پژوهش در نوع و موضوع خود در کشور منحصر به فرد است. در منابع لاتین و در پایگاه‌های اطلاعاتی و نشریات معتبر علمی، مواردی در بررسی‌های کتابخانه‌ای پیرامون موضوعاتی که به نوعی با این پژوهش مرتبط بوده‌اند، شناسایی شدند اما این منابع نیز همه متغیرها و ابعاد این پژوهش را باهم بررسی نکرده‌اند و در آن فقط به برخی از مؤلفه‌های مدنظر محققین این پژوهش توجه شده است. بخشی از یافته‌ها در خصوص پیشینه پژوهش در جدول (۲) قابل مشاهده است:

جدول (۲) بررسی پیشینه مرتبط با پژوهش

ردیف	پژوهشگر	عنوان اثر	تاریخ	چکیده
۱	روی زو	سازمان شبکه خدمات نمایندگی شهروند: راهی جدید برای بهبود سیستم آژانس شهروندی چین در عصر داده‌های بزرگ	۲۰۲۱	تقاضاهای زیاد شهروندان چینی در خصوص دادرسی‌های مدنی باعث شده است شبکه خدمات نمایندگی و کارگزاری با عنوان آژانس‌های شهروندی در این کشور راه‌اندازی شده و به صورت سازمانی شبکه‌ای به ارائه خدمات بر اساس تجمیع داده‌های بزرگ شهروندان بپردازند. این مقاله راهکارهای برداشت داده‌های شهروندان را در بهبود عملکرد آژانس‌های یادشده بررسی کرده است.
۲	هریس ریمر و همکاران	داده‌های شهروندان، نقطه مرکزی اتکای دولت و امنیت ملی استرالیا	۲۰۲۰	در این گزارش که توسط مرکز مطالعات استراتژیک و دفاعی دانشگاه ملی استرالیا تهیه شده است با اشاره به اهمیت داده‌های شهروندان، به نقش آن در نحوه بهره‌برداری دولت از این داده‌ها و اثربخشی آن بر روی امنیت ملی استرالیا پرداخته شده است. همچنین در بخش‌های بعدی این گزارش در خصوص چالش‌ها و عدم قطعیت‌ها پیرامون داده‌های شهروندی و نمونه‌هایی از مسائل به وجود آمده در کشورهای دیگر بحث شده است.
۳	وی نینگ وو	عوامل تعیین کننده داده‌های تولیدشده توسط شهروندان در یک شهر هوشمند	۲۰۲۰	این پژوهش نشان می‌دهد که چگونه داده‌های تولیدشده توسط شهروندان می‌توانند به پیشرفت شهرهای هوشمند و پایدار کمک کنند و از آنجاکه ابتکارات شهرهای هوشمند بر داده‌های شهروندان متمرکز است، مدیران

ردیف	پژوهشگر	عنوان اثر	تاریخ	چکیده
				دولتی باید استراتژی‌ها و برنامه‌هایی برای ارتقا شهروندی و همچنین درک چگونگی استفاده شهروندان از فناوری‌های شهرهای هوشمند برای توسعه شهرهای پایدار داشته باشند.
۴	ایولین راپرت	آینده‌های متفاوت داده‌ها: آزمایشی در داده‌های شهروندان	۲۰۱۹	در این مقاله آمده است: داده‌های بزرگ و شهروندان جدایی‌ناپذیر هستند؛ از تلفن‌های هوشمند، کنتورها، یخچال‌ها و اتومبیل‌ها تا سیستم‌عامل‌های اینترنت، اکثراً داده‌های فن‌آوری‌های دیجیتال داده‌های شهروندان است. مقاله علاوه بر طرح موضوعات سیاسی و اخلاقی حریم خصوصی و حفاظت از داده‌ها، خواستار تجدیدنظر در استفاده مجدد از کلان داده‌های مرتبط با شهروندان در تولید آمارهای رسمی و قابل‌اعتماد شده است.
۵	اکاراث پانیاتپ	مدلی از روند مدیریت سیستم داده‌های جامعه توسط مرکز جامعه دیجیتال و مشارکت شهروندان	۲۰۱۷	این رساله دکتری ضمن بررسی میزان داده‌های دیجیتال تولیدشده در نمونه آماری خود، با طراحی مدلی برای مدیریت سیستم داده‌های جامعه در خصوص نحوه توسعه داده‌ها و مدیریت آن و نیازمندی‌های این مدل و چشم‌انداز آن، جمع‌آوری و تعیین منبع داده‌ها و آینده سیستم داده‌های جامعه بحث شده است.

با توجه به بررسی پیشینه پژوهش که بخشی از آن در جدول فوق ارائه گردید، نکات زیر به صورت خلاصه مشاهده می‌شود:

- توجه ویژه برخی دولت‌ها به اهمیت سیستم‌های داده مبتنی بر اطلاعات شهروندان به منظور استفاده در مصارف مدیریت شهری، کنترل مقوله‌های امنیتی و اقتصادی؛
- ضرورت ایجاد سیستم‌ها و بانک‌های اطلاعاتی شامل رفتار و داده‌های شهروندان جهت پیش‌بینی، نظارت و استقرار حکمرانی مبتنی بر اطلاعات؛
- اهمیت نظارت بر داده‌های شهروندان در استقرار و استحکام امنیت ملی؛
- افزایش تعاملات بین‌المللی در آینده پیرامون تبادل داده‌های شهروندان کشورهای مختلف به منظور استقرار امنیت منطقه‌ای و جهانی و اثربخشی ایجاد سیستم‌های داده شهروندی بر امنیت ملی؛
- اهتمام برخی از کشورها به تدوین سند ملی امنیت داده‌ها و راه‌اندازی سامانه‌های مدیریتی و نظارتی مرتبط.

در مجموع می‌توان ادعا کرد رویکرد آینده‌نگری و تدوین آینده‌های محتمل در قالب سناریوهای باورپذیر پیرامون سیستم‌های داده شهروند در کنار توجه به مقوله امنیت ملی، نوآوری پژوهش

حاضر است و پژوهش منتشرشده قبلی در این زمینه وجود ندارد، لکن با مرور منابع و بررسی پیشینه پژوهش، تعدادی مؤلفه و عامل اثرگذار بر موضوع پژوهش شناسایی گردید که مهم‌ترین آن‌ها در جدول (۳) دسته‌بندی شده است. این موارد به‌منظور ایجاد دید و ترسیم فضای وسیع‌تر در قالب داده‌های اولیه در اختیار خبرگان پژوهش قرار گرفت. خبرگان با توجه به موارد احصا شده اقدام به تفکیک این عوامل در قالب عناوینی چون کنشگر، عامل کلیدی و پیشران نموده و سپس در پنل برگزارشده ضمن ترکیب، حذف یا اضافه نمودن برخی از موارد، به میزان اهمیت آن‌ها امتیاز دادند.

جدول (۳) مؤلفه‌ها و عوامل اثرگذار شناسایی‌شده طی بررسی پیشینه پژوهش

ردیف	پژوهشگر	عنوان اثر	مؤلفه‌ها و عوامل اثرگذار بر موضوع پژوهش
۱	روی زو	سازمان شبکه خدمات نماینده‌گی شهروند: راهی جدید برای بهبود سیستم آژانس شهروندی چین در عصر داده‌های بزرگ	<ul style="list-style-type: none"> • رسانه‌ها و شبکه‌های اجتماعی • گروه‌های مرجع • قوانین مالکیت معنوی داده‌ها • مقررات مربوط به حریم خصوصی • توسعه و ارائه پلتفرم‌های جدید
۲	هریس ریمر و همکاران	داده‌های شهروندان، نقطه مرکزی اتکای دولت و امنیت ملی استرالیا	<ul style="list-style-type: none"> • دولت‌های پیشرو در فناوری اطلاعات • نهادهای قانون‌گذاری و نظارت بین‌المللی • نهادهای حقوقی بین‌المللی • قدرت‌های منطقه‌ای و بین‌المللی • سیاست‌های امنیتی - اطلاعاتی • اعمال فشارهای بین‌المللی
۳	وی نینگ وو	عوامل تعیین‌کننده داده‌های تولیدشده توسط شهروندان در یک شهر هوشمند	<ul style="list-style-type: none"> • سازمان‌ها و انجمن‌های مردم‌نهاد • شرکت‌های بزرگ فناوری اطلاعات و ارتباطات • سیاست‌های استقرار دولت هوشمند • سیاست‌ها و قوانین نظارت بر تبادل داده‌ها • ایجاد بسترهای جدید تبادل داده در فضای مجازی
۴	ایولین راپرت	آینده‌های متفاوت داده‌ها: آزمایشی در داده‌های شهروندان	<ul style="list-style-type: none"> • نهادهای اجتماعی بین‌المللی • حقوق شهروندی و حریم خصوصی • ترویج سبک زندگی دیجیتالی • رسمیت بخشی به هویت دیجیتالی • توسعه اقتصاد مبتنی بر داده‌های شهروندان • فروش اطلاعات افراد و تحلیل رفتار مشتریان

ردیف	پژوهشگر	عنوان اثر	مؤلفه‌ها و عوامل اثرگذار بر موضوع پژوهش
۵	اکاراث پانیاتپ	مدلی از روند مدیریت سیستم داده‌های جامعه توسط مرکز جامعه دیجیتال و مشارکت شهروندان	<ul style="list-style-type: none"> • شرکت‌های بزرگ و صاحب برندهای معروف • شوک‌های اقتصادی و اجتماعی • منازعات، جنگ و بحران‌های سیاسی • مدیریت شکاف‌های اجتماعی ایجادشده پیرامون داده‌های افراد

روش‌شناسی پژوهش

پژوهش می‌تواند چهار هدف متفاوت را دنبال کند. گاهی هدف از پژوهش حل یک مسئله متداول و معمول در محیط کار است؛ گاهی هدف از آن ارتقای دانش در حوزه‌ای خاص است و گاهی اوقات هدف پژوهش بررسی اثرات پیشنهادی پژوهش‌های کاربردی و بعضاً توسعه پژوهش قبلی است (دانایی‌فرد و همکاران، ۱۳۹۶: ۳۲). این پژوهش از نظر تقسیم‌بندی نوع آن جزو پژوهش‌های کاربردی به شمار می‌رود و در آن تلاش شده با استفاده از زمینه و بسترهای شناختی و معلومات موجود، از نتایج حاصله برای رفع ابهامات و نادانسته‌ها و توسعه کاربردی موضوع موردپژوهش، استفاده شود. همچنین این پژوهش با رویکرد کیفی در پی گردآوری داده‌ها به منظور مفهوم‌سازی و ارائه تحلیل‌های تجویزی است. با توجه به اهمیت موضوع پژوهش و نظر به اینکه یکی از اهداف اصلی آن بسط نگاه راهبردی فرماندهان، مدیران و سیاست‌گذاران کلان کشور به ظرفیت نا اندیشیده در خصوص سیستم‌های داده شهروند و تأثیر آن بر امنیت ملی بوده است، سعی شده چالش‌های مرتبط با آن در حوزه‌های سیاسی، امنیتی، اجتماعی و اقتصادی، موردتوجه قرار گیرد؛ لذا شناسایی خبرگان مؤثر و کارآمد در این پژوهش نقش به‌سزایی داشته و به همین منظور جامعه آماری این پژوهش به‌صورت باز تعریف‌شده و شامل صاحب‌نظران و خبرگانی است که توانایی کمک تحلیلی به اهداف پژوهش را داشته باشند. در پژوهش حاضر از روش نمونه‌گیری هدفمند (انتخاب آگاهانه افراد یا عناصر مشخص برای پژوهش توسط پژوهشگر) و تعداد محدودی از افراد نمونه استفاده شده است. با توجه به محدود بودن تعداد افراد خبره در این حوزه و همچنین ویژگی‌های مدنظر برای جامعه آماری، از دیدگاه‌های ۱۲ نفر با مشخصات زیر که شامل اساتید دانشگاه‌های تهران و دانشگاه عالی دفاع ملی و برخی مدیران دولتی شاغل در وزارت کشور، صداوسیما، سازمان برنامه‌وبودجه و سازمان فناوری اطلاعات کشور بوده‌اند، استفاده گردید. ویژگی‌های انتخاب نمونه آماری بر اساس ملاک‌های زیر بوده است:

- داشتن نگاه راهبردی و عمیق به موضوع تحقیق؛
- دارا بودن تحصیلات عالی در حوزه‌های مدیریت، آینده‌پژوهی و فناوری اطلاعات؛

- داشتن بیش از ده سال سابقه در حوزه‌های مختلف تصمیم‌گیری و سیاست‌گذاری کلان؛
 - توانایی تحلیل و درک درست از موضوعات امنیتی و مقولات امنیت ملی؛ و
 - دارا بودن سابقه پژوهشی به‌منظور درک بیشتر و عمیق‌تر هدف از انجام پژوهش.
- در خصوص شیوه‌های گردآوری اطلاعات و روش تجزیه و تحلیل، ابتدا به‌منظور مرور ادبیات، بررسی کتابخانه‌ای علمی و تخصصی و سپس در مراحل بعدی از روش‌های ذهن‌انگیزی و پنل‌های خبرگان استفاده شده است. روش اصلی تجزیه و تحلیل پژوهش بر سناریو پردازی استوار بوده است.
- رویکردهای شکل‌دهی به فضای سناریوها**

سناریوها نمایندگان برگزیده‌شده از فضای آینده‌های بدیل هستند. برای شناسایی آینده‌های بدیل و تبدیل آن‌ها به مجموعه سناریوها سه رویکرد کلی پیشنهاد شده است: رویکردهای استقرایی، فزاینده و استنتاجی (پدرام و احمدیان، ۱۳۹۴: ۱۸۱). رویکردهای فزاینده و استقرایی به دلیل پیچیدگی‌های روش‌شناختی به‌شدت نیازمند تبحر و تجربه هستند. یکی دیگر از رویکردهای سناریو پردازی رویکرد استنتاجی^۱ است. این رویکرد کاربرد گسترده‌ای در سناریونویسی کیفی دارد و به شکلی منظم به تحلیل عدم قطعیت‌ها و سناریوها می‌پردازد (پدرام و زالی، ۱۳۹۷). بر پایه این رویکرد، الگوهای اجرایی متنوعی برای سناریو پردازی پیشنهاد شده است که مرسوم‌ترین آن‌ها در مکتب آمریکایی، الگوی «شبکه جهانی کسب‌وکار» معروف به GBN^۲ است که پیتر شوارتز^۳ در کتاب هنر دورنگری، این مراحل را به شرح زیر برمی‌شمارد:

- گام اول: شناسایی موضوع یا تصمیم اصلی؛
- گام دوم: شناسایی نیروهای کلیدی در محیط نزدیک؛
- گام سوم: شناسایی نیروهای پیشران؛
- گام چهارم: طبقه‌بندی بر اساس اهمیت و عدم قطعیت؛
- گام پنجم: انتخاب منطق سناریوها؛
- گام ششم: پربار کردن سناریوها؛
- گام هفتم: شناسایی پیامدها؛ و
- گام هشتم: انتخاب شاخص‌ها و علائم راهنما (شوارتز، ۱۳۹۰).

^۱. Deductive

^۲. Global Business Network

^۳. Peter Schwartz

در پژوهش حاضر مبتنی بر رویکرد استنتاجی، از الگوی شبکه جهانی کسب‌وکار به‌منظور سناریو پردازی و تجزیه و تحلیل داده‌های پژوهش استفاده شده است.

تجزیه و تحلیل داده‌ها و یافته‌های پژوهش

در پژوهش حاضر روش سناریونویسی از آن جهت انتخاب شد که می‌تواند به ما کمک کند تا با شناخت برخی از عناصر مهمی که احتمالاً در ساخت آینده تأثیر خواهند داشت، تصویرها و داستان‌هایی از آینده بسازیم. به همین منظور در گام نخست، مهم‌ترین و تأثیرگذارترین بازیگران مؤثر در موضوع پژوهش شناسایی و بررسی شدند. این بازیگران در اولین پیل، توسط خبرگان از نظر اهمیت مورد بررسی قرار گرفتند. در گام دوم، شناسایی مؤلفه‌ها و عوامل تأثیرگذار بر موضوع در دستور کار قرار گرفت. هدف از این گام ترسیم فضایی است که حداکثر تطابق را با واقعیت داشته باشد چراکه این عوامل نقش مهمی در تعیین داستان سناریو دارند. در گام سوم پیشران‌ها و عدم قطعیت‌های مرتبط با آن‌ها از طریق مرور اسناد، مصاحبه نیمه ساختاریافته و تحلیل آن‌ها در پیل با مشارکت خبرگان، بررسی و احصا شد. در گام چهارم مطلوب‌ترین آینده ممکن مورد بررسی خبرگان قرار گرفت و در گام پنجم، فضای کلی سناریوها ترسیم شد. در این گام کوشش شد تا سناریوهای اصلی (محتمل‌تر) برای آینده (در افق زمانی پژوهش) شناسایی شود. فرایند انجام کار تا رسیدن به سناریوهای نهایی بدین گونه بوده است که منطق شکل‌گیری سناریوها با استفاده از تحلیل نیروهای پیشران و عدم قطعیت‌های آن‌ها در دومین پیل خبرگان تبیین شده و درباره آن اجماع حاصل شد. در گام ششم، روایت توصیفی هر سناریو به نگارش درآمده و شاخص‌های راهنما، دورنمای مطلوب و پیش‌بینی‌های محیطی هر سناریو تهیه شد و در گام پایانی، با حضور جمع برگزیده‌ای از خبرگان، سناریوها مجدداً مورد ارزیابی و بازنگری نهایی قرار گرفتند. اهم یافته‌های پژوهش بر اساس گام‌های فوق از این قرار است:

الف. کنشگران تأثیرگذار بر آینده سیستم‌های داده شهروند در افق ۱۴۱۰

شناخت کنشگران از حیث توانمندی‌ها، اهداف، انگیزه‌ها، نقاط ضعف و مطلوبیت‌ها به ما کمک می‌کند تا بتوانیم شناخت بهتری از آینده موضوع مورد مطالعه به دست بیاوریم. پس از مشخص شدن فهرست و دسته‌بندی کنشگران، باید وزن آن‌ها در مسئله سازمان مشخص شود. معمولاً این وزن دهی به شکل نمادین (با ستاره دادن از ۰ تا ۳) یا با اعداد معادل نماها انجام می‌شود. برای مثال وزن کنشگران با عددی بین ۰ تا ۳ مشخص می‌شود که عدد ۳ معادل واژه «کلیدی»، عدد ۲ معادل واژه «بسیار مهم» و عدد ۱ معادل واژه «مهم» است. کنشگری که وزن صفر داشته باشد از فهرست اصلی کنار گذاشته می‌شود (پدارم و احمدیان، ۱۳۹۴: ۱۸۵). علت و ضرورت

شناسایی کنشگران را می‌توان در این دلایل دسته‌بندی کرد: ۱- پیشران، حاصل کنش کنشگران است لذا شناسایی کنشگران در تشخیص و شناسایی پیشران‌ها مؤثر است ۲- بررسی احتمالات رفتاری بازیگران کلیدی در نگارش سناریوها مهم است چراکه هر یک می‌توانند از ظرفیت‌های متعدد و متنوعی برخوردار باشند و این ظرفیت‌ها، تصمیمات و رفتار ایشان می‌تواند بر آینده موضوع اثرگذار باشد ۳- در روایت نویسی سناریوها از کنشگران و نقش و رفتار آن‌ها می‌توان استفاده کرد. نتایج حاصل از برگزاری پنل خبرگان در خصوص کنشگران تأثیرگذار بر آینده سیستم‌های داده شهروند در جدول (۴) منعکس شده است. خبرگان به وزن هر یک از کنشگران امتیازی بین ۰ تا ۳ را اختصاص داده‌اند و میانگین وزن‌های اعلام‌شده در ستون میزان اهمیت، آورده شده است.

جدول (۴) کنشگران مؤثر بر سیستم‌های داده شهروند

میزان اهمیت	کنشگران
۲,۲۵	دولت‌های پیشرو در فناوری اطلاعات (مانند ژاپن و ایالات‌متحده آمریکا)
۲,۳۸	نهادهای قانون‌گذاری و نظارت بین‌المللی (مانند سازمان ملل متحد)
۱,۸۸	نهادهای حقوقی بین‌المللی (مانند دیوان لاهه)
۲,۳۸	شرکت‌های بزرگ فناوری اطلاعات و ارتباطات (مانند گوگل، میکروسافت و ...)
۲,۷۵	رسانه‌ها و شبکه‌های اجتماعی با کاربران بسیار زیاد و پرمخاطب (مانند فیس‌بوک، توییتر و ...)
۲	قدرت‌های منطقه‌ای و بین‌المللی تأثیرگذار بر روابط بین کشورها
۲,۱۳	سازمان‌ها و انجمن‌های مردم‌نهاد و فعال بین‌المللی
۲,۱۳	گروه‌های مرجع شامل افراد شاخص سیاسی و اجتماعی بین‌المللی (مانند رهبران سیاسی مشهور، سلبریتی‌ها، چهره‌های سرشناس ورزشی و ...)
۱,۷۵	مجامع علمی و دانشگاهی معتبر جهانی
۱,۸۸	نهادهای اجتماعی بین‌المللی (مانند یونیسف)
۲,۵	شرکت‌های بزرگ و صاحب برندهای معروف اقتصادی

ب. نیروهای پیشران تغییر

روندهای نوظهور و مؤلفه‌های فناورانه، اقتصادی، اجتماعی، سیاسی و فرهنگی بسیار زیادی بر آینده موضوع اثر می‌گذارند. برخی از این مؤلفه‌ها دارای عدم قطعیت زیاد و برخی دیگر تا حدودی قابل پیش‌بینی‌اند. مؤلفه‌های دارای عدم قطعیت بالا، تصمیم‌گیری را برای مدیران در حوزه‌های ذی‌ربط، پیچیده و دشوار می‌سازد (رضایان و همکاران، ۱۳۹۶). پیشران‌ها از دو جهت برای ما

دارای اهمیت هستند، از یک‌سو در مقام توصیف، آینده را بر مبنای آن‌ها توصیف می‌کنیم و از سوی دیگر، تجویزهایی که برای تغییر در آینده ارائه می‌شوند نیز متکی به همین نیروهای پیشران است (پدارم و احمدیان، ۱۳۹۴: ۱۸۷). پیشران‌هایی که پیشامد آن‌ها می‌تواند سیستم‌های داده شهروندی را با تحولی جدی روبه‌رو سازد و به‌تبع آن بر آینده این سیستم‌ها تأثیرگذار باشد بر اساس پنل خبرگان در جدول (۵) احصا شده است. لیست اولیه پیشران‌های یادشده در ابتدا طی مرور اسناد، بررسی پیشینه پژوهش و مصاحبه با تعداد محدودی از خبرگان احصا شده و سپس با طرح آن‌ها در پنل خبرگان، موارد مشابه ادغام و مواردی نیز بر اساس نظر ایشان و با توجه به کنش احتمالی کنشگران شناسایی شده در آینده، اضافه شد. خبرگان حاضر در دومین پنل اجراشده، از نظر اهمیت به هریک از این نیروهای پیشران امتیازی بین ۰ تا ۳ داده‌اند.^۱ ممکن است در زمان پژوهش، پیشران‌ها بالفعل یا بالقوه باشند، مهم این است که آنچه نیروی تغییر آینده را دارد برشمرده باشیم. در جدول (۵) میانگین نظر خبرگان در مورد هر پیشران در ستون «اهمیت» نمایش داده شده است.

جدول (۵) وزن دهی به پیشران‌های مؤثر بر سیستم‌های داده شهروند

کنشگران	پیشران‌ها	اهمیت
دولت‌های پیشرو در فناوری اطلاعات	سیاست‌های استقرار دولت هوشمند و دولت الکترونیک	۲
	سیاست‌های غلبه فناوریانه و اقتصادی بر سایر کشورها	۱,۷۵
	ایجاد روال‌های مرتبط با سیستم‌های داده و اقتضانات آن	۱,۸۸
	مدیریت بهره‌مندی از سیستم‌های داده	۱,۵
نهادهای قانون‌گذاری و نظارت بین‌المللی	سیاست‌ها و قوانین نظارت بر تبادل داده‌ها	۱,۸۸
	سیاست‌های توسعه یا محدودسازی استفاده از داده‌ها در محاکم بین‌المللی	۱,۷۵
	قوانین مالکیت معنوی داده‌ها	۱,۸۸
	رسمیت بخشی به هویت دیجیتالی افراد	۲,۲۵
نهادهای حقوقی بین‌المللی	ارائه خدمات دانشی به کشورهای عقب‌افتاده	۱,۳۸
	مقررات مربوط به حریم خصوصی و محافظت از داده‌ها	۲,۲۵
	چارچوب‌گذاری در تبادل و استعلام داده‌های افراد بین دولت‌ها	۲
	وضع قوانین مرتبط با جرائم سایبری	۲
	هماهنگ‌سازی قوانین سایبری با نیازهای روز بین‌المللی	۱,۷۵
تجاری‌سازی فن‌آوری‌های نوظهور برای دولت‌ها و شرکت‌ها	۲	

^۱ در ارتباط با دسته‌بندی پیشران‌ها باید گفت که پیشران‌ها را می‌توان به پیشران‌های بالقوه و بالفعل و یا پیشران‌های مثبت و منفی تقسیم کرد. سپس به پیشران‌ها نیز مشابه بازیگران ستاره می‌دهیم (از صفر تا سه ستاره). روشن است پیشران‌هایی که ستاره بیشتری می‌گیرند، کلیدی‌تر هستند. تکنیک وزن دهی می‌تواند مشابه وزن دهی کنشگران باشد. منظور از وزن و اهمیت پیشران، همان قدرت اثرگذاری آن بر مسئله است.

اهمیت	پیشران‌ها	کنشگران
۲,۱۳	ایجاد خدمات مبتنی بر ارزش افزوده داده‌ها	شرکت‌های بزرگ فناوری و ارتباطات
۲,۵	کاربرد و عمومی کردن فناوری‌های نوین مانند اینترنت اشیا در سطح جوامع	
۲,۳۸	ارائه خدمات جدید محاسباتی و تحلیل داده‌ها و مبتنی بر هوش مصنوعی برای مشتریان خاص	
۲,۲۵	توسعه و ارائه پلتفرم‌های جدید مبتنی بر فناوری اطلاعات	رسانه‌ها و شبکه‌های اجتماعی با کاربران بسیار زیاد و پرمخاطب
۲,۶۳	تغییر ذائقه کاربران در اشتراک‌گذاری و تولید محتوا	
۲	عوامل انگیزشی برای تولید داده و اشتراک‌گذاری اطلاعات شخصی کاربران	
۱,۷۵	ایجاد داده‌های حجیم از اطلاعات کاربران و در اختیار گذاردن آن به دولت‌ها و مشتریان خاص	
۲	افزایش کارآمدی و هم‌افزایی رسانه‌های اجتماعی در خصوص تبیین آینده داده‌های افراد	
۲,۳۸	ایجاد بسترهای جدید تبادل داده در فضای مجازی	قدرت‌های منطقه‌ای و بین‌المللی تأثیرگذار بر روابط بین کشورها
۲	سیاست‌های اقتصادی و سیاسی	
۱,۸۸	سیاست‌های امنیتی - اطلاعاتی و سلطه‌جویانه	
۲,۱۳	توسعه حکمرانی دیجیتالی بر جهان	
۱,۶۳	اعمال تحریم‌های شدید برای برخی از کشورها در خصوص تبادل و جایجایی داده‌ها	
۱,۵	اعمال فشارهای بین‌المللی بر کشورهای مورد تخاصم	سازمان‌ها و انجمن‌های مردم‌نهاد و فعال بین‌المللی
۱,۸۸	ایجاد مطالبات و ساختارهای حمایتی از حقوق دیجیتالی اشخاص	
۱,۷۵	توسعه ارزش‌های اجتماعی- شبکه ای شهروندان	
۲,۱۳	مطالبه مباحث حقوق شهروندی و حریم خصوصی	
۲,۱۳	ایجاد موج‌های اعتراض‌آمیز به استفاده از داده‌های خصوصی توسط دولت‌ها	
۲	تشکیل کمپین‌ها و تجمعات در خصوص مالکیت معنوی داده‌ها و حریم خصوصی	گروه‌های مرجع شامل افراد شاخص سیاسی و اجتماعی بین‌المللی
۱,۶۳	هم‌افزایی و همراهی با نهادهای بین‌المللی در خصوص بهره‌برداری مناسب از داده‌های اشخاص	
۱,۷۵	اقناع‌سازی افکار عمومی پیرامون سیاست‌های کلان وضع شده در مورد داده‌های دیجیتال	
۱,۵	حمایت یا عدم‌حمایت از روندهای جاری در خصوص توسعه و بهره‌برداری از داده‌های شهروندی	
۱,۸۸	ترویج سبک زندگی دیجیتالی	
۲	الگوسازی برای هویت دیجیتالی مخاطبان	رسمیت بخشی به هویت دیجیتالی و داده‌های افراد
۲,۱۳		

اهمیت	پیشران‌ها	کنشگران
۲,۵	توسعه سیستم‌ها و فناوری‌های مبتنی بر داده‌کاوی	مجامع علمی و دانشگاهی معتبر جهانی
۱,۸۸	وضع سیاست‌های اجتماعی پیرامون حقوق سایبری اشخاص	نهادهای اجتماعی بین‌المللی
۱,۷۵	ایجاد سیاست‌های رفاهی و حمایتی در خصوص داده‌های اشخاص	
۱,۳۸	مدیریت شکاف‌های اجتماعی ایجادشده پیرامون داده‌های افراد	
۱,۸۸	کاهش فاصله‌های طبقاتی ایجادشده در عصر دیجیتال	
۱,۸۸	انگیزه‌های تجاری در استفاده از داده‌ها	شرکت‌های بزرگ و صاحب برندهای معروف اقتصادی
۲,۳۸	توسعه اقتصاد مبتنی بر داده‌های شهروندان	
۲	ذائقه شناسی و تغییر ذائقه مشتریان بر اساس تحلیل داده‌های در دسترس	
۲,۱۳	فروش اطلاعات افراد و تحلیل رفتار مشتریان	
۲	ایجاد سبک زندگی مبتنی بر فضای مجازی	پیشران‌های محیطی جهانی
۱,۳۸	تغییرات اقلیمی (خشک‌سالی، ریزگردها و ...) و ژئوپلیتیکی	
۲,۲۵	بحران‌های جهانی (مانند همه‌گیری بیماری کرونا)	
۲,۲۵	شوک‌های اقتصادی و اجتماعی	پیشران‌های اقتصادی جهانی
۲	سیاست‌های توزیع عادلانه منافع اقتصاد دیجیتال	
۲,۱۳	توسعه اقتصاد دیجیتالی	
۱,۶۳	منازعات، جنگ و بحران‌های سیاسی	پیشران‌های سیاسی منطقه‌ای و بین‌المللی
۱,۷۵	درگیری‌ها، شورش‌ها و انقلاب‌های منطقه‌ای	

در رویکرد برنامه‌ریزی مبتنی بر سناریوها، برای شناسایی سناریوهای تنها از پیشران‌هایی استفاده می‌شود که آینده آن‌ها با عدم قطعیت آمیخته است. با توجه به میزان اهمیت اعلام‌شده برای هر پیشران توسط خبرگان پژوهش و بر اساس جدول فوق، ده مورد از پیشران‌هایی که بالاترین امتیاز را داشتند جداشده و مجدداً نظر جمع برگزیده‌ای از خبرگان در خصوص مهم‌ترین و مؤثرترین پیشران‌های مؤثر بر موضوع پژوهش در افق ۱۴۱۰، موردبررسی قرار گرفت و درنهایت موارد زیر با اجماع نظر خبرگان انتخاب شدند:

- تغییر ذائقه کاربران در اشتراک‌گذاری و تولید محتوا؛
- توسعه سیستم‌ها و فناوری‌های مبتنی بر داده‌کاوی؛
- کاربردی و عمومی کردن فناوری‌های نوین؛
- ارائه خدمات جدید محاسباتی و تحلیل داده‌ها و مبتنی بر هوش مصنوعی؛
- ایجاد بسترهای جدید تبادل داده در فضای مجازی؛ و
- توسعه اقتصاد مبتنی بر داده‌های شهروندان.

پ. عدم قطعیت‌های کلیدی و تدوین چارچوب سناریوها

به‌منظور شناسایی عدم قطعیت‌های کلیدی، با توجه به پیشران‌های بااهمیت شناسایی‌شده در پنل خبرگان، حالت‌های احتمالی آینده این پیشران‌ها بررسی شد. بر اساس نظر خبرگان، چند شرط برای شناسایی عدم قطعیت‌های کلیدی در نظر گرفته شد: ۱- عدم قطعیت‌ها با توجه هم‌زمان به دو فاکتور بالاترین اهمیت و بیشترین تأثیرگذاری تعیین شوند. ۲- این اطمینان به وجود آید که عدم قطعیت‌های کلیدی حداکثر فضای نا اطمینانی را پوشش می‌دهند و ۳- به ویژگی بارز عدم قطعیت یعنی پیش‌بینی‌ناپذیری توجه شود و اگر رویدادی حتی با احتمال نه‌چندان زیاد، قابل پیش‌بینی است دیگر عدم قطعیت به شمار نمی‌آید. با منطبق ترسیم‌شده، عدم قطعیت‌های کلیدی با اجماع خبرگان در سه دسته اصلی تقسیم‌بندی شد:

- حمایت/عدم‌حمایت هنجارهای اجتماعی و ذائقه کاربران از اشتراک‌گذاری داده؛
- تأکید/عدم تأکید مقررات داخلی و بین‌المللی بر استفاده از داده‌های افراد؛ و
- رشد/عدم رشد مدل‌ها و مشوق‌های تجاری برداشت از داده‌ها.

از برهم‌کنش این سه عدم قطعیت کلیدی، هشت فضای نا اطمینانی آینده به دست می‌آیند که با کمک خبرگان و صاحب‌نظران در خصوص باورپذیری یا باورناپذیری آن‌ها، ارزیابی‌های لازم صورت گرفت. خبرگان با استناد به نظر و تجربه تخصصی خود و نیز با توجه به کلان‌روندهای ترسیم‌شده برای آینده سیستم‌های داده شهروند (Katherine et al, 2020) و بر اساس گزارش‌های تخصصی منتشرشده پیرامون چشم‌انداز آینده این سیستم‌ها (GOFS, 2020) احتمال وقوع هر حالت و باورپذیری آن را تعیین کردند. در جدول (۶) جمع‌بندی نظرات خبرگان ارائه شده است.

جدول (۶) سازگاری عدم قطعیت‌ها و باورپذیری سناریوها

نام سناریو	مطلوبیت	رشد مدل‌ها و مشوق‌های تجاری برداشت از داده‌ها	تأکید مقررات داخلی و بین‌المللی بر استفاده از داده‌های افراد	حمایت هنجارهای اجتماعی و ذائقه کاربران از اشتراک‌گذاری داده	باورپذیری
انتهای قدرت	مطلوب	بلی	بلی	بلی	+
ابر و خورشید	مطلوب نسبی	خیر	بلی	بلی	+
ایستاده در غبار	مطلوب نسبی	بلی	خیر	بلی	+

نام سناریو	مطلوبیت	رشد مدل‌ها و مشوق‌های تجاری برداشت از داده‌ها	تأکید مقررات داخلی و بین‌المللی بر استفاده از داده‌های افراد	حمایت هنجارهای اجتماعی و ذائقه کاربران از اشتراک‌گذاری داده	باورپذیری
ایستگاه متروک	نامطلوب	خیر	خیر	خیر	+
		خیر	خیر	بلی	-
		بلی	بلی	خیر	-
		خیر	بلی	خیر	-
		بلی	خیر	خیر	-

ت. تدوین سناریوها

سناریوها، توصیف موقعیت‌های آینده و حوادث ممکن در آن موقعیت‌ها هستند، به‌گونه‌ای که شخص بتواند از موقعیت کنونی خود به‌سوی آینده‌های بدیل حرکت نماید. به دیگر بیان، سناریو یک طرح یا نمای کلی است و باید یک کلان تصویر از آینده فراهم کند (Son, 2012). در این پژوهش از مدل کلاسیک و پرکاربرد برنامه‌ریزی بر مبنای سناریو بهره گرفته‌شده است و روش سناریونویسی از آن جهت انتخاب شد که می‌تواند به ما کمک کند تا با شناخت برخی از عناصر مهمی که احتمالاً در ساخت آینده تأثیر خواهند داشت، تصویرها و داستان‌هایی از آینده بسازیم (Bostron, 2009) و از طریق این تصویرها و توصیف‌ها، درک جامع‌تری از آینده‌های ممکن و چگونگی تلاش برای هم‌سویی با برخی یا دوری از برخی دیگر به دست آوریم (Bishop, 2007). در این پژوهش با تحلیل عوامل کلیدی، کنشگران بااهمیت و پیشران‌های مؤثر بر موضوع و در نظر گرفتن عدم قطعیت‌های کلیدی، می‌توان سناریوهای آینده سیستم‌های داده شهروند را توسعه داد. سناریوها بر اساس طیف وسیعی از احتمالات نیروهای پیشران و تعاملات بین آن‌ها حاصل شده است و اسامی چهار سناریو به‌دست آمده که به‌صورت نمادین از فیلم‌های سینمایی ایرانی انتخاب شده است. در ادامه فرآیند پس از شناسایی نیروهای پیشران و عدم قطعیت‌های مرتبط با آن‌ها از طریق مرور اسناد، مصاحبه و تحلیل آن‌ها در پنل خبرگان، باورپذیری سناریوها موردبررسی قرار گرفت و کوشش شد تا سناریوهای اصلی و محتمل‌تر برای آینده در افق زمانی پژوهش شناسایی شود. سپس منطق شکل‌دهی به سناریوها با استفاده از تحلیل نیروهای پیشران و عدم قطعیت‌های آن‌ها تبیین شد و بعد از تدوین اولیه سناریوها، نتایج حاصل با حضور شماری از خبرگان مطرح و درباره آن اجماع حاصل شد. در پایان نیز شاخص‌های راهنمای هر سناریو تهیه شد. منطق معرفی شاخص‌های راهنما بر این اصل استوار بوده است که این شاخص‌ها،

رویدادهایی هستند که در هر سناریو بیشترین احتمال رخ دادن را داشته و در صورت وقوع، باید سناریوی مرتبط با آن شاخص‌ها مبنای عمل قرار گیرد.

سناریوی اول: انتهای قدرت

در راستای صیانت مؤثر از امنیت ملی، دولت‌ها اقدام به راه‌اندازی بانک‌های اطلاعاتی و سامانه‌های داده‌ای مبتنی بر رفتار و اطلاعات شهروندان نموده‌اند و با گذشت زمان، حجم و تنوع داده‌های شهروندان در سامانه‌های اطلاعاتی مختلف به سرعت در حال افزایش است. اشتراک‌گذاری این داده‌ها مزایای زیادی به همراه آورده است و تبادل امن داده‌ها و تحلیل آن، تمایل سازمان‌های امنیتی را به استفاده بیشتر از داده‌ها، افزایش داده است. حفاظت از امنیت ملی و رشد خدمات دولت هوشمند، باعث شده، افکار عمومی موافق استفاده از داده‌های خود باشند و با استقرار سیستم‌های اطلاعات داده محور، پیگیری سریع جرائم سایبری، مبارزه با پول‌شویی و برخورد قضایی با ناقضین حقوق شهروندی و حفظ حریم خصوصی در کنار ارائه خدمات شهر هوشمند و شهروند الکترونیک به راحتی امکان‌پذیر گردد. این سامانه‌ها مانند بازوی قدرتمندی برای حفظ و افزایش ضریب امنیت ملی عمل می‌کنند و با استفاده از آن‌ها امکان اعمال نظارت‌های قانونی نهادهای امنیتی افزایش یافته است. در کنار این موضوع، بهره‌وری در حوزه تجارت افزایش یافته و امکان تولید محصولات نوآورانه، بهبود خدمات عمومی و توسعه تحقیقات علمی فراهم شده است.

از سویی دیگر، توسعه سامانه‌های داده شهروند در کنار نظارت و پایش مدام داده‌ها، به سازمان‌های امنیتی اجازه می‌دهد در شناسایی و مواجهه با تهدیدات سایبری موفق‌تر باشند و در پرتو فضای سایبری امن ایجادشده، شرکت‌های تولیدکننده سخت‌افزارها و نرم‌افزارهای رایانه‌ای، هرروز بر سرعت ارائه محصولات خود می‌افزایند و خدمات جذابی مانند خرید آنلاین، سرویس‌های جاده هوشمند، خدمات الکترونیک سفر، آموزش مجازی، گردشگری، سلامت الکترونیک و ... ارائه می‌دهند. دولت‌ها به راحتی طرح‌هایی مانند شهر الکترونیک، مالیات هوشمند، خدمات هوشمند بیمه‌ای و شهروندی و ... را مبتنی بر سابقه داده‌های شهروندان به اجرا می‌گذارند. تعاملات بین‌المللی اشتراک‌گذاری داده‌ها در بسیاری از کشورها گسترش یافته و افزایش تبادلات داده‌ای، اثرات بسیار مؤثری در مقابله با تروریسم سایبری و مبارزه با جرائم سازمان‌یافته بین‌المللی داشته است. این هم‌افزایی باعث شده میزان مشارکت کشورها در حل منازعات و مسائل بین‌المللی مانند بحران‌های سیاسی - امنیتی و حتی مسائلی مانند بحران کم‌آبی و مشکلات محیط‌زیست، بیشتر و موفق‌تر باشد.

شاخص‌های راهنما

- رشد فزاینده اعتماد افکار عمومی در جمع‌آوری و استفاده از داده‌های شهروندی در قبال تقویت امنیت ملی و افزایش خدمات دولت هوشمند؛
- افزایش شاخص‌های توسعه امنیت ملی و مبارزه مؤثر دولت‌ها با جرائم سایبری؛
- حمایت قوانین و نهادهای بین‌المللی از تبادل داده بین کشورها برای حل مسائل جهانی و وضع قوانین سخت‌گیرانه در خصوص جرائم و تروریسم سایبری.

سناریوی دوم: ابر و خورشید

قوانین بین‌المللی و مقررات داخلی بسیاری از کشورها از حاکمیت داده‌ها و ایجاد سامانه‌های مبتنی بر داده‌های شهروندان در کنار ایجاد نقاط دسترسی تحت شبکه‌های اطلاعاتی بین‌المللی حمایت می‌کنند. ایالات متحده آمریکا، چین و اتحادیه اروپا به‌عنوان سه بلوک اصلی کنترل جریان داده‌های بین‌المللی، هریک استانداردهایی را وضع کرده‌اند و می‌کوشند کشورهای کمتر توسعه‌یافته را با استانداردهای خود و در قبال خرید و استقرار سیستم‌های داده غیربومی، همراه سازند. فرصت حضور و مشارکت سایر کشورها در فضای دیجیتال شدن حکمرانی جهانی و ایجاد امنیت پایدار بیشتر شده اما این به معنای توان نقش‌آفرینی برای آن‌ها نیست و کشورهای خارج از سه بلوک فوق می‌بایست برای بسیاری از تعاملات و تبادلات بین‌المللی در حوزه‌های مختلف امنیتی، اقتصادی، تجاری و اجتماعی، به دادن امتیازاتی تن دهند که شاید در آینده به چالش‌هایی برای امنیت ملی آن‌ها تبدیل شود.

اگرچه توافقنامه‌های بین‌المللی اشتراک‌گذاری داده‌ها، امکان حل بسیاری از مسائل جهانی مانند بحران‌های سیاسی، جنگ، مخاصمات منطقه‌ای و منازعاتی چون کم‌آبی و آلودگی هوا را راحت‌تر کرده است اما وابستگی‌های فناورانه به کشورهای خاص، ایجاد شکاف در ساختار امنیت ملی و بروز تهدیدات امنیتی و سایبری جدی‌ای را در آینده گوشزد می‌کند. شرکت‌های بزرگ تولیدکننده فناوری‌های دیجیتالی، بازارهای خوبی را در سایر کشورها به دست آورده‌اند و پذیرش اجتماعی حضور این فناوری‌ها در زندگی روزمره مردم دنیا در حال افزایش است. با این حال دولت‌هایی که دارای نوآوری فناوری و تجاری کمتری هستند برای ادامه حیات اقتصادی و تأمین امنیت ملی خود مجبورند به سمت کشورهای پیشرو در فناوری‌های اطلاعاتی و ارتباطی متمایل شوند. توسعه اقتصاد دیجیتالی و ظهور پول ارزهای دیجیتالی باعث شده است در برخی کشورهای ضعیف‌تر شوک‌های اقتصادی و به‌تبع آن ناآرامی‌های اجتماعی دیده شود. شرکت‌های بزرگ غربی مانند فیس‌بوک، گوگل و ... با ارائه سرویس‌های متنوع و ارائه خدمات شهروند محور، مرزهای جغرافیایی را کنار زده و فعالیت‌های خود را در کشورهای دیگر به‌سرعت افزایش داده‌اند و این

وابستگی شهروندان کشورهای مختلف به سرویس‌های این شرکت‌ها در امور روزمره، به تهدیدی برای امنیت ملی تبدیل شده است و عملاً نبض داده‌های کشورهای ضعیف‌تر در اختیار شرکت‌های بزرگ بین‌المللی قرار دارد. ادامه این روند، نگرانی‌های زیادی را برای مدیران امنیتی و سازمان‌های اطلاعاتی ایجاد کرده است.

شاخص‌های راهنما

- شکل‌گیری تفاهم‌نامه‌ها و معاهده‌های بین‌المللی در خصوص تبادل داده‌ها؛
- ایجاد چارچوب‌های قانونی و حقوقی بین‌المللی جهت حمایت از حریم خصوصی با تأکید بر اشتراک‌گذاری داده‌ها در مواقع ضروری بین کشورها؛ و
- پیدایش روند رو به افزایش بهره‌وری دولت‌ها و کاهش هزینه‌های خدمات عمومی به سبب جایگزین شدن خدمات الکترونیک با برخی خدمات سنتی.

سناریوی سوم: ایستاده در غبار

شرکت‌های رایانه‌ای معروف و صاحب‌برند با ارائه مشوق‌ها و خدمات ویژه، سعی در جذب بازارهای بین‌المللی و جمع‌آوری داده‌های اشخاص به‌منظور تحلیل رقبا و افزایش سود خود بر اساس ذائقه‌های مشتریان دارند. از آنجاکه خاستگاه این شرکت‌ها، کشورهای قدرتمند و فرصت‌طلب است طبیعی است که جمع‌آوری داده‌ها در سطحی وسیع توسط آن‌ها در کنار تنوع محصولات و سرویس‌های رایگان یا ارزان‌قیمت ایشان (که هم‌فشار فناوری و هم‌کشش بازار مصرف را با خود به همراه دارد)، می‌بایست دغدغه‌ای جدی برای مدیران و نهادهای امنیتی باشد. در این شرایط تقریباً نظارت دولت‌ها کنار گذاشته و شهروندان با استقبال چشمگیر خدمات متنوع این شرکت‌ها، به مشتریان وفاداری برای آنان تبدیل شده‌اند و این ارتباط دوسویه ایجادشده و بدون امکان نظارت جدی نهادهای مسئول، باعث شده است شبکه‌های اجتماعی، پایگاه‌های خبری و اطلاع‌رسانی، سامانه‌های تبادل پول‌های دیجیتالی و... همگی برای دولت‌هایی که زیرساخت‌های فناورانه مدیریت و نظارت بر داده‌ها را ندارند به مسائل امنیت ملی تبدیل شوند. برخی دولت‌ها از وضع فعلی رضایت نداشته و این تبادلات که حدود مرز مشخصی ندارد را برخلاف استقلال و امنیت ملی خود می‌دانند. لذا رویکرد ایشان با اعمال محدودیت‌های بسیار و فیلترینگ دسترسی به سایت‌ها و سامانه‌های الکترونیکی و شبکه‌های بین‌المللی همراه شده است. با افشای اطلاعات مهم و یا بروز حملات سایبری گاه‌وبیگاه، آرام‌آرام حفظ امنیت عمومی و حریم خصوصی با چالش جدی مواجه شده و این مسائل استعداد تبدیل شدن به دغدغه امنیت ملی را در خود ایجاد می‌کنند. ضعف در ردیابی تهدیدهای سایبری، کمبود قوانین پیشگیرانه و مؤثر،

ضعف هماهنگی دولت و بخش خصوصی، همگی باعث شده‌اند سیاست‌های سخت‌گیرانه برخی دولت‌ها تشدید شده و با تداوم این محدودیت‌ها، کسب‌وکارهای کوچک رو به ورشکستگی گذارند. هم‌زمان با افزایش میزان نفوذ فناوری اطلاعات در بین شهروندان، جرائم و کلاهبرداری‌های سایبری نیز رشد کرده و کشورهای آسیب‌پذیر، مجبور به اتخاذ سیاست‌های انقباضی و تقابل با خواسته‌های شهروندان و محدودسازی آزادی‌های ایشان، شده‌اند. تداوم این رویه در کنار اعمال فشارهای بین‌المللی برای توسعه آزادی‌های مدنی، می‌تواند کشورهای ضعیف‌تر را با مشکلاتی چون آسیب‌پذیری سایبری، شکاف اجتماعی و فروریزش سرمایه‌های اجتماعی همراه سازد.

شاخص‌های راهنما

- رشد بسیار سریع تعداد کاربران در رسانه‌ها و شبکه‌های اجتماعی غیردولتی و غیربومی؛
- ناکافی بودن زیرساخت‌های حقوقی بین‌المللی و قوانین حاکم بر تبادلات داده‌ها در کنار افزایش تهدیدات و حملات سایبری به علت ضعف قوانین پیشگیرانه؛ و
- پررنگ‌تر شدن نقش و دخالت دولت‌ها در نظارت بر تبادل داده‌ها و ایجاد بسترهای ملی برای حفظ و رصد داده‌های بومی، در راستای کاهش تهدیدات مربوط به امنیت ملی.

سناریوی چهارم: ایستگاه متروک

نقض حریم خصوصی شهروندان توسط برخی دولت‌ها باعث ایجاد بی‌اعتمادی بسیار زیادی نسبت به استفاده از سامانه‌های اینترنتی و شبکه‌های اجتماعی بومی و حتی اشتراک‌گذاری اطلاعات در فضای مجازی شده است و شهروندان، عضویت در شبکه‌های اجتماعی خارجی و نامطمئن را بر سرویس‌های ایجادشده داخلی ترجیح می‌دهند. نارضایتی‌های مدنی رو به افزایش یافته و این مخالفت‌ها از طرق مختلف و توسط سازمان‌های مردم‌نهاد و سایر ابزارهای در دسترس جامعه، ابراز می‌شود. تداوم این نارضایتی‌ها به بی‌اعتبار شدن برخی دولت‌ها در فضای بین‌المللی و کاهش تعامل سایر کشورها با ایشان منجر شده و به‌طور هم‌زمان نهادهای بین‌المللی مانند سازمان ملل متحد با اخطارهای مختلف به ایجاد محدودیت‌های شدید در تبادل اطلاعات و بومی‌سازی غیرقانونی داده‌ها، اعتراض نموده‌اند. بر اثر شکل‌گیری جبهه بین‌المللی علیه این کشورها، دسترسی ایشان به میزان قابل‌توجهی به داده‌های ضروری بین‌المللی مانند اطلاعات هواشناسی، محیط‌زیست، پیگردهای قضایی و ... محدود و یا قطع شده است. اتخاذ برخی سیاست‌های سخت‌گیرانه در واکنش به حضور محصولات و نرم‌افزارهای شرکت‌های بزرگ خارجی، باعث شده یا شرکت‌های فوق‌متهم به جاسوسی فناوریانه شده و یا شهروندان این کشورها فشارهای روانی بیشتری را بر اثر اعمال محدودیت در اینترنت و شبکه‌های ارتباطی تجربه کنند.

برخی از کشورها تقریباً به‌طور کامل از اینترنت جهانی جدا شده‌اند و فقط نقاط دسترسی کنترل شده و محدودی در اختیار شهروندان قرار داده‌اند. این امر در کنار کاهش سطح تعاملات جهانی، برخلاف تصور اولیه، منجر به رشد میزان تهدیدات سایبری و جرائم امنیتی و بروز نارضایتی‌های مدنی شده است و روابط تجاری، حفظ سهم بازار، روابط فرهنگی و اجتماعی با سایر کشورها را با بی‌ثباتی جدی‌ای روبرو کرده است. تداوم روند به وجود آمده، حکمرانان این کشورها را بر سر دوراهی تعامل آزاد با دنیا و یا آمادگی برای انزوای بیشتر قرار داده است. کشورهایی که به دلایل مختلف مرزهای اطلاعاتی و شبکه‌ای خود را مسدود و یا تحت نظارت شدید درآورده‌اند با چالش‌های جدی در تجارت و سایر مناسبات بین‌المللی و نیز مطالبات مدنی و اجتماعی شهروندان خود مواجه هستند. این مسئله باعث شده همواره چالش‌های متفاوت امنیت ملی و دوگانگی برخورد با شبکه‌های اطلاع‌رسانی و محصولات جدید فناوری اطلاعات مشاهده شده و هزینه‌های سیاسی و اجتماعی زیادی بابت اتخاذ این رویه تحمل شود.

شاخص‌های راهنما

- کاهش شدید اعتماد افکار عمومی به دولت‌ها به علت اجرای سیاست‌های مداخله‌جویانه در حریم خصوصی و افزایش جرائم سایبری؛
- اعمال سیاست‌های اجباری بومی‌گرایی داده‌های ملی توسط دولت‌ها و کاهش مرادات بین‌المللی در زمینه پیگیری جرائم قضایی، توریسم، تجارت الکترونیک و ...؛
- انزوای برخی کشورها در تبادلات تجاری و مناسبات بین‌المللی در بستر شبکه‌های مرسوم اطلاعاتی، رشد میزان تهدیدات امنیتی و افزایش تروریسم و جاسوسی سایبری.

نتیجه‌گیری و پیشنهادها

هدف از تدوین سناریوها، خلق فضای بررسی احتمال آینده‌های ممکن، به‌گونه‌ای است که بتوان پابرجایی سیاست‌ها را در برابر طیفی از چالش‌های آینده آزمود. سناریوها همچنین به ما کمک می‌کنند تا عوامل شگفتی‌ساز را در چهارچوب چالش‌ها یا فرصت‌های بالقوه بشناسیم، زیرا سناریوها، ابزارهایی ارزشمند برای جست‌وجو در محیط و زمانی هستند که در آن، راهبردها و سیاست‌های ما به اجرا درخواهند آمد. اشاره گردید که دو اصل اساسی در آینده‌پژوهی وجود دارد؛ یکی اینکه آینده قطعی نیست و آینده‌های بدیل وجود دارد و دوم اینکه می‌خواهیم از غافلگیری پیشگیری کنیم و یک مطلوبیتی از آینده داشته باشیم؛ تنها روشی که به این دو اصل هم‌زمان، پاسخ می‌دهد، سناریو پردازی است، زیرا یک وحدت روش‌شناسی هم برای آینده‌پژوهی

به همراه می‌آورد. بنابراین، در این مقاله، مبتنی بر روش سناریو در رویکرد استنتاجی، تلاش شد ضمن شناسایی کنشگران مهم و اثرگذار بر آینده سیستم‌های داده شهروند، پیشران‌های مؤثر و عدم قطعیت‌های مرتبط نیز با استفاده از نظرات خبرگان شناسایی شود. بر اساس یافته‌های فوق امکان نگارش سناریوهای باورپذیر فراهم‌شده و درنهایت چهار سناریو برای آینده موضوع موردپژوهش در افق ۱۴۱۰ تهیه شود. یافته‌های پژوهش نشان داد کنشگران کلیدی اثرگذار شامل «رسانه‌ها و شبکه‌های اجتماعی با کاربران بسیار زیاد و پرمخاطب»، «شرکت‌های بزرگ و صاحب برندهای معروف اقتصادی» و دو کنشگر «تهادهای قانون‌گذاری و نظارت بین‌المللی» و «شرکت‌های بزرگ فناوری اطلاعات و ارتباطات» بوده و مهم‌ترین پیشران‌ها نیز «تغییر ذائقه کاربران در اشتراک‌گذاری و تولید محتوا»، «توسعه سیستم‌ها و فناوری‌های مبتنی بر داده‌کاوی» و «کاربردی و عمومی کردن فناوری‌های نوین» بوده‌اند. بر اساس نظر خبرگان با شناسایی سه عدم قطعیت کلیدی با عناوین «حمایت/عدم‌حمایت هنجارهای اجتماعی و ذائقه کاربران از اشتراک‌گذاری داده»، «تأکید/عدم تأکید مقررات داخلی و بین‌المللی بر استفاده از داده‌های افراد» و «رشد/عدم رشد مدل‌ها و مشوق‌های تجاری برداشت از داده‌ها»، هشت فضای نا اطمینانی به دست آمد که با بررسی باورپذیری آن‌ها، نگارش سناریوها انجام شد. در سناریوی مطلوب، دولت می‌تواند با مداخله در حریم خصوصی و پایش داده‌های شهروندان و به‌کارگیری آن در بانک‌های اطلاعاتی، هم خدمات دولت هوشمند را توسعه دهد و هم هزینه‌های خود را کاهش داده و از این ابزار برای توسعه حکمرانی و اعمال نظارت‌های بیشتر در حوزه‌های سیاسی و امنیتی بهره‌مند شود و در یک کلام، امنیت ملی را تقویت نماید. از سویی دیگر وجود قوانین ملی و بین‌المللی مرز این مداخله را تنظیم کرده و در فضایی وسیع‌تر، دولت‌ها با تبادل و اشتراک‌گذاری این اطلاعات، امنیت بین‌المللی، تجارت، فرهنگ، سیاست و مسائل اجتماعی را توسعه داده و به استقرار نظم و حل مسائل جهانی در موضوعاتی چون جرائم سایبری، مبارزه با تروریسم، محیط‌زیست، بحران کم‌آبی، قاچاق مواد مخدر و پیشگیری از فعالیت‌های مخرب سازمان‌یافته و ... مبادرت می‌ورزند. در عصر انقلاب اطلاعات و پویایی انتشار اطلاعات آنچه مهم است حفظ و پایداری امنیت ملی است و پیچیدگی تهدیدات سایبری باعث می‌شود دولت‌ها بیشتر به فکر نظارت بر این تهدیدات از طریق راه‌اندازی سیستم‌های مدیریت داده‌ها و رفتار شهروندان و ردیابی اقدامات مجرمانه و خطرآفرین برای امنیت ملی خود باشند.

در ادامه پیشنهادی پژوهش به شرح زیر مطرح می‌شود:

۱. با توجه به سرعت و تنوع تولید داده‌ها، داشتن سیاست فعال برای مواجهه با شرایطی که این داده‌ها در آینده به وجود خواهند آورد برای دستگاه‌های اجرایی و نهادهای حاکمیتی مرتبط

در کشور ضروری است. از یک سو انباشت و تولید حجم عظیمی از داده‌ها به‌طور خواسته یا ناخواسته نیازمند سیستم‌های مدیریت داده‌ها برای بهره‌برداری از آن‌هاست و از سوی دیگر بی‌توجهی به افسارگسیختگی این حجم عظیم تولید داده‌ها، می‌تواند در آینده مشکلاتی را برای امنیت ملی و عمومی کشور ایجاد کند. لذا ضروری است سیاست‌گذاران کشور و نهادهای امنیتی به‌طور هم‌زمان، هم بر ایجاد بسترهای قانونی و حقوقی نظارت بر داده‌ها از طریق ایجاد قانون در مجلس شورای اسلامی مبادرت نمایند و هم اعتبارات ریالی مناسبی را برای توسعه زیرساخت‌های شبکه و ایجاد مراکز داده (دیتاسنتر) در نظر بگیرند و با راه‌اندازی سامانه‌های مرتبط جهت شناسایی و ردیابی تهدیدات سایبری، چالش‌های امنیتی این حوزه را به حداقل برسانند.

۲. حضور پررنگ محصولات مبتنی بر فناوری‌های نوین در جامعه ایرانی که با نقش‌آفرینی شرکت‌های بزرگ صاحب‌نام خارجی مانند تلگرام، فیس‌بوک، واتس‌آپ و... در حال انجام است باعث می‌شود مدیریت و کنترل گردش داده‌ها در اختیار شرکت‌های یادشده قرار گرفته و در آینده این شرکت‌ها و محصولاتشان تعیین‌کننده شرایط و اقتضائات ما باشند. این محصولات از تلفن همراه گرفته تا لوازم خانگی و اداری، خودروها و رایانه‌های شخصی و دولتی و... بیشتر شئون زندگی جامعه ایرانی را دربر گرفته‌اند و در کنار خدماتی که ارائه می‌دهند فرهنگ، سیاست و ادبیاتی را وارد کشور می‌کنند که می‌تواند تضادهایی با منافع ملی ما داشته و یا در برهه‌هایی از زمان، به‌عنوان تهدیدی جدی عمل کنند. لذا مدیران راهبردی امنیتی و دفاعی کشور از هم‌اکنون باید برای پیش‌گیری فعالانه از غافلگیری اقدام کنند و با توجه به پیچیدگی تهدیدات سایبری و ضعف نظارت بر بخش خصوصی، اشراف اطلاعاتی و توان دفاعی خود را در این زمینه افزایش دهند.

۳. به‌منظور تبادل داده‌ها چه در بُعد تجاری و چه سایر ابعاد سیاسی، امنیتی و اجتماعی، معاهده‌ها و توافقنامه‌های حقوقی در جامعه بین‌المللی در حال شکل‌گیری است. عضویت یا عدم عضویت در این توافقات بستگی به نقشه راه آینده و سیاست‌های ما در قبال واگرایی و یا همگرایی پیرامون داده‌های تولیدشده بومی دارد. لذا ضروری است قبل از قبول تعهدات بین‌المللی، وضعیت آینده سیاست‌های ما در بالاترین سطوح امنیت ملی مانند شورای عالی امنیت ملی مشخص شده باشد تا از تحمیل شروط نامطلوب در آینده بر کشور و ایجاد محدودیت‌های قانونی و بین‌المللی آتی جلوگیری شود.

۴. در برخی کشورها با توجه به اهمیت داده‌های شهروندی و ضرورت مدیریت این داده‌ها تصمیم‌های خاصی عملی شده است. در بعضی کشورها «سند ملی تبادل داده‌ها»، «راهبردهای ملی آینده داده‌ها» و یا عناوین مشابهی تهیه و تصویب شده است که سازوکارهای لازم برای مواجهه با فضای عدم قطعیت مرتبط با داده‌های بومی آن کشورها در سندهای یادشده تعریف شده است. لذا ضروری است شورای عالی امنیت ملی، مرکز ملی فضای مجازی، مجلس شورای اسلامی و سایر نهادهای حاکمیتی کشور، به این موضوع توجه ویژه داشته و اقدامات مؤثری و پیش‌دستانه برای مواجهه با آینده داشته باشند.
۵. حضور سرویس‌ها و پلتفرم‌های شبکه‌های اجتماعی خارجی و ورود بیش‌ازپیش آن‌ها در زندگی روزمره ایرانیان، در آینده می‌تواند در ابعاد سیاسی و اجتماعی، زمینه‌های لازم برای بروز اغتشاشات و ناامنی‌های اجتماعی را فراهم کند. با توجه به ضریب نفوذ بالای اینترنت در کشور و میانگین نسبتاً بالای استفاده ایرانیان از این نرم‌افزارها و سرویس‌های غیربومی به‌صورت روزانه، امکان استفاده از داده‌های تجمیع شده ایرانیان و تحلیل آن‌ها تسهیل شده و این امر اطلاعات ناب و گران‌قدری را در اختیار کشورهای متخاصم قرار خواهد داد. تجربه شناسایی و ترور دانشمندان هسته‌ای کشور یا ایجاد اختلالات شبکه‌ای وسیع در سامانه‌های خدمت‌رسان مانند سامانه سوخت و ... نشان می‌دهد این موضوع در آینده استعداد تبدیل شدن به مسئله امنیت ملی کشور را دارد.

قدردانی

از مشارکت و همراهی اساتید و خبرگان توانمندی که در مراحل مختلف این پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان قرار دادند، تشکر و قدردانی می‌نماییم.

منابع

- امانیان، حسین. (۱۳۹۵). چالش‌های امنیتی ج.ا.ا از پیروزی انقلاب اسلامی تا حال حاضر، فصلنامه اندیشه انقلاب اسلامی، (۶): ۲۱۱-۲۳۲.
- بخشی، عبدالله. (۱۳۹۵). اطلاعات و امنیت در کتاب و سنت، چاپ اول، تهران: موسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.
- بل، وندل. (۱۳۹۲). مبانی آینده‌پژوهی: تاریخچه، اهداف و دانش، ترجمه مصطفی تقوی و محسن محقق، چاپ اول، تهران: مرکز آینده‌پژوهی علوم و فناوری دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

- بیشاب، پیتر. هاینز، اندی. و کولینز، تری. (۱۳۸۸). وضعیت کنونی سناریونویسی؛ مرور اجمالی تکنیک‌ها، ترجمه مسعود منزوی، چاپ اول، تهران: مرکز آینده‌پژوهی علوم و فناوری دفاعی، نشر مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- پدارم، عبدالرحیم. و احمدیان، مهدی. (۱۳۹۴). *آموزه‌ها و آموزه‌های آینده‌پژوهی*، چاپ اول، تهران: نشر موسسه افق راهبردی.
- پدارم، عبدالرحیم. و زالی، سلمان. (۱۳۹۷). الگویی نوین برای سناریونویسی در موضوعات راهبردی مطالعه موردی: سناریوهای آینده بحران سوریه، *فصلنامه مطالعات سیاسی جهان اسلام*، ۷(۲): ۲۶-۱.
- خلیلی‌پور رکن‌آبادی، علی. و نورعلی وند، یاسر. (۱۳۹۱). تهدیدات سایبری و تأثیر آن بر امنیت ملی، *فصلنامه مطالعات راهبردی*، ۱۵(۵۶): ۱۹۶-۱۶۷.
- دانایی‌فرد، حسن. الوانی، سید مهدی. و آذر، عادل. (۱۳۸۳). *روش‌شناسی پژوهش کیفی در مدیریت: رویکردی جامع*، چاپ اول، تهران: انتشارات صفار.
- دانایی‌فرد، حسن. الوانی، سید مهدی. و آذر، عادل. (۱۳۹۶). *روش‌شناسی پژوهش کمی در مدیریت: رویکردی جامع*، چاپ دوازدهم، تهران: انتشارات صفار.
- رضایان قیه‌باشی، احد. پور عزت، علی اصغر. و سرمست، بهرام. (۱۳۹۶). ارائه چارچوبی برای مطالعه شگفتی‌سازهای نظامی - دفاعی پیش‌روی جمهوری اسلامی ایران، *فصلنامه آینده‌پژوهی دفاعی*، ۲(۷): ۱۲۸-۱۰۳.
- شوارتز، پیتر. (۱۳۹۰). *هنر دورنگری: برنامه‌ریزی برای آینده در دنیایی با عدم قطعیت*، ترجمه عزیز علیزاده، چاپ اول، تهران: مرکز آینده‌پژوهی علوم و فناوری دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- صالح نیا، علی. و بختیاری، حسین. (۱۳۹۷). اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله مراتبی، *فصلنامه مطالعات راهبردی سیاست‌گذاری عمومی*، ۸(۲۷): ۲۷۷-۲۵۵.
- ماندل، رابرت. (۱۳۸۷). *چهره متغیر امنیت ملی*، چاپ سوم، تهران: پژوهشکده مطالعات راهبردی.
- Beagrie, N., & Houghton, J. (2016). The value and impact of the European bioinformatics institute.
- Chertoff, M. (2008). *The cyber security Challenge, Regulation & Governance*. Congressional Research Service (CRS) (2008), Botnets, Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, available at: www.crs.org, (accessed by July 23, 2011).

- CIGI-Ipsos. (2019). *2019 CIGI-Ipsos Global Survey on Internet Security and Trust*. www.cigionline.org/internet-survey-2019.
- Deloitte, L. L. P. (2017). Assessing the value of TfL's open data and digital partnerships.
- Dunn Caveltly, M., & Brunner, E. (2007). Introduction: Information, Power, and Security: An Outline of Debates and Implications. In *Power and security in the information age* (pp. 1-18). Ashgate.
- GOFS, A. (2020). *Evidence and scenarios for global data systems, Government office for science Report, UK*. <https://doi.org/10.1038/d41586-018-02386-3>.
- Li, J., & Mocko, M. (2020). Machine learning for a citizen data scientist: an experience with JMP.
- Mansted, K., & Logan, S. (2020). Citizen data: a centrepiece for trust in government and Australia's national security. *Fresh Perspectives in Security*, 6-12.
- Noordyke, M. (2020). US state comprehensive privacy law comparison. International association of privacy professionals. [Google Scholar].
- Rodriguez, Carlos A. (2006). *Cyber terrorism*, Inter-American Defense College as a prerequisite for the Diploma approved.
- Scott, M., & Cerulus, L. (2018). Europe's new data protection rules export privacy standards worldwide. Retrieved March 18, 2018.
- Tanner, M. S. (2017). Beijing's New National Intelligence Law: From Defense to Offense. *Lawfare*, July 20.
- UNCTAD. (2019). *Digital Economy Report 2019. Value creation and capture: implications for developing countries*. United Nations Conference on Trade and Development.