

Digitalism and the future of state surveillance; Studying how digitalism affects government surveillance in the Islamic Republic of Iran; The elites' viewpoin

Mohammad Babaei*

Assistant Professor of Faculty of Law and Political Science Kharazmi t University of Tehran, Iran,
mohammadbabaei@khu.ac.ir

Ahmad Vaezi

Master's degree in political science Abstrac Kharazmi t University of Tehran, Iran,
ahmad.vaezi27@gmail.com

Abstract

Purpose: The main objective of this article is to determine the positive/negative effects of digital transformation on the Islamic Republic of Iran's government. So, the study mainly examines the aspect of government's surveillance because of the broad scope of the topic.

Method: The research is qualitative and based on the grounded theory method. The data collection method used in the theoretical sections is documentary- library .A semi-structured interview method was also used with a sample population made up of professors, experts, as well as some staff in related fields in order to assess the collected data and their compliance with the Iranian government. Additionally, the information gathered from the interviews has been analyzed using three phases of qualitative coding.

Findings: The study's findings demonstrated that, although Iran remains significantly behind its regional and global rivals in this field, digitalism has had profoundly positive and negative effects on the government's surveillance in that country.

Conclusion: As a conclusion, it seems digital technologies will aid in ensuring the security of the society in a nation like Iran in terms of surveillance. Another point is that creating legal frameworks for data access and facilitating people activities in cyber spaces are both necessary for enhancing the government's capacity for digital surveillance. At last, taking into account the current state of Iran society, establishing trust between individuals through the legal frameworks is a crucial and fundamental tenet in the government's surveillance and use of data gathered

Keywords: Artificial Intelligence, Digitalism, Surveillance, Government, Technology Firms

Vaezi, Ahmad .(2023), Digitalism and the future of state surveillance; Studying . **Cite this article:** Babaei, Mohammad how digitalism affects government surveillance in the Islamic Republic of Iran; The elites' viewpoin, Volume8, NO.1, Spring & Summer 2023, 81-107

DOI: 10.30479/jfs.2023.18135.1447

Received on 5 December,2022 Accepted on 29 April,2023

Copyright© 2022, The Author(s).



Publisher: Imam Khomeini International University

Corresponding Author: Mohammad Babaei

E-mail: Mohammadbabaei@khu.ac.ir

دیجیتالی شدن و آینده نظارت دولت؛ تاثیر دیجیتالی شدن بر عملکرد نظارتی دولت در جمهوری اسلامی ایران از نگاه نخبگان

محمد بابایی

استادیار، گروه علوم سیاسی، دانشگاه خوارزمی تهران، ایران، نویسنده مسئول، M ohammadbabaei@khu.ac

احمد واعظی

دانش آموخته کارشناسی ارشد علوم سیاسی دانشگاه خوارزمی، تهران، ایران، ahmad.vaezi27@gmail.com

چکیده

هدف؛ هدف مقاله، شناسایی اثرات (مثبت یا منفی) تحول دیجیتال بر دولت در جمهوری اسلامی است. پرسش اصلی پژوهش این است که دیجیتالی شدن، چه تأثیراتی بر عملکرد نظارتی دولت خواهد داشت؟ با توجه به گستردگی دامنه بحث، پژوهش حاضر بر بُعد نظارتی دولت متمرکز است.

روش؛ پژوهش، از نوع کیفی و براساس روش گراند تئوری است. داده‌های بخش مبانی و نظری، به روش اسنادی گردآوری شده است. برای ارزیابی داده‌های گردآوری شده و انطباق آن‌ها با دولت در ایران، از تکنیک مصاحبه نیمه-ساخت یافته با جامعه نمونه؛ متشکل از استادان، متخصصان و شاغلان حوزه‌های مرتبط نیز استفاده شده است. داده‌های گردآوری شده از مصاحبه‌ها نیز از طریق کدگذاری سه مرحله‌ای پژوهش‌های کیفی، تجزیه و تحلیل شده‌اند.

یافته‌ها؛ یافته‌های پژوهش نشان داد؛ دیجیتالی شدن، تأثیرات عمیق مثبت و منفی و در ابعاد مختلف بر عملکرد نظارتی دولت در ایران خواهد داشت؛ مانند گسترش قلمرو و کیفیت نظارت بر مردم، ایجاد دغدغه در میان جامعه، تحدید حریم خصوصی و بروز رقیبان جدید برای دولت.

نتیجه‌گیری؛ نتایج نشان داد؛ به‌کارگیری فناوری دیجیتال در بعد نظارتی، نقشی حیاتی در تأمین امنیت در کشوری به وسعت ایران دارد. همچنین ارتقای توان نظارتی دیجیتال دولت، از سویی مستلزم تسهیل فعالیت شهروندان در فضای مجازی و از سوی دیگر، نیازمند ایجاد ساختارهای قانونی برای دسترسی به داده‌هاست و درنهایت با توجه به وضعیت جامعه، جلب اعتماد مردم از طریق تدوین ساختارهای قانونی، اصل لازم و بنیادی در نظارت و بهره‌گیری دولت از داده‌های گردآوری شده است.

واژگان کلیدی؛ هوش مصنوعی، نظارت، دولت، دیجیتالی شدن، شرکت‌های صاحب فناوری

*استناد: بابایی، محمد، واعظی، احمد. (۱۴۰۲)، دیجیتالی شدن و آینده نظارت دولت؛ تاثیر دیجیتالی شدن بر عملکرد نظارتی دولت در جمهوری اسلامی ایران از نگاه نخبگان دو فصلنامه علمی آینده پژوهی ایران، مقاله پژوهشی، دوره ۸، شماره ۱، بهار و تابستان ۱۴۰۲، ۸۱-۱۰۷
تاریخ دریافت مقاله: ۱۴۰۱/۹/۱۴ تاریخ پذیرش نهایی: ۱۴۰۲/۲/۹
ناشر: دانشگاه بین المللی امام خمینی (ره)

در طول تاریخ، ابداعات و اختراعات، معمولاً متأثر از دو نگرانی، با مخالفت مواجه شده‌اند. اول؛ نگرانی برخی جریان‌ها از تأثیر آن بر مردم و جامعه، دوم؛ نگرانی حکومت‌ها؛ اما تحولات نشان داد، نمی‌توان در برابر نوآوری‌ها و توسعه فناوری، ایستادگی نمود؛ به نحوی که امروزه توسعه سریع فناوری دیجیتال، تقریباً همه عرصه‌های جامعه انسانی را دربرگرفته است (کیسینجر، اشمیت و نوتنلوچر، ۱۴۰۱: ۵۷). به همین شکل، فناوری دیجیتال نیز با وجود شماری از مقاومت‌ها، موفق شد، افزون بر نمایش کارآمدی، از جهاتی حتی متمایز از فناوری‌های پیشین، خود را نمایان سازد. مهم‌ترین این تمایزات، کاستن تدریجی از میزان سهم هوش بشری در حل مشکلات حیات فردی و جمعی افراد است که به دنبال خود تغییر در مفهوم دانش و به تبع آن، معنای آموزش و یادگیری را سبب شده است (کیسینجر، اشمیت و نوتنلوچر، ۱۴۰۱: ۵۸-۵۴)؛ گستره تأثیرگذاری (تقریباً بر تمام عرصه‌های زندگی) و نیز تحول در نقش و جایگاه این فناوری در زندگی جمعی، از دیگر تمایزات آن است. فناوری‌هایی پیشین (دستگاه چاپ، ماشین بافندگی و یا ماشین بخار)، ابزاری در اختیار انسان بودند؛ اما فناوری دیجیتال، بخشی جدایی‌ناپذیر از زندگی است و این پیوستگی، هرچه عمیق‌تر شود؛ در نهایت به میزان در هم تنیدگی دولت‌ها با این فناوری باید اشاره کرد. در گذشته، شاید فناوری‌ها بر روی بخش‌هایی از سازمان دولت اثرگذار بودند؛ اما اکنون تمام وجوه و عملکرد دولت‌ها، متأثر از فرایند دیجیتالی شدن است (Delfanti and Arvidsson, 2019: 8-12) و بدون آن، تحقق کارویژه‌های دولت (مثلاً در اقتصاد داخلی یا خارجی)، نه فقط با چالش جدی مواجه خواهد شد؛ بلکه انزوای دولت را نیز در پی خواهد داشت (صفری و همکاران، ۱۳۸۲: ۵۴). بروز پدیده دولت الکترونیک، به‌عنوان بخشی از برنامه اصلاح بخش عمومی در جهان و از جمله در ایران

۱ - این ابداعات، به علت برخورداری از قابلیت تحول در توانایی‌های جامعه، عموماً از سوی حامیان نظم موجود، به‌ویژه دولت‌ها و نیروهای همسو، با مخالفت‌های شدید روبه‌رو شده است؛ مثلاً ابداع ماشین بافندگی در سال ۱۵۹۸ میلادی، به علت برهم زدن نظم موجود، با مخالفت شدید حاکمیت مواجه شد. در نخستین نمایش این دستگاه در حضور الزابت اول، ملکه انگلستان، ملکه به شدت با ایده ماشین بافندگی مخالفت کرد (میردامادی؛ نمیمی‌پور، ۱۳۹۳، ۲۴۵-۲۴۶)؛ زیرا روی آوردن بخش عظیمی از مردم برای کسب حداقل درآمد به شغل بافندگی، پایه‌های امپراتوری بریتانیا را به لرزه درمی‌آورد. از این رو، اعتراضات بسیاری در انگلستان و اروپای ابتدای قرن ۱۹ علیه مکانیزه شدن صنایع رخ دادند؛ مانند جنبش لودیت‌ها (Luddite) در قرن ۱۹ که در جریان شورش‌ها و اعتراضات آن‌ها، دستگاه‌های بسیاری خرد، افراد زیادی دستگیر و ده‌ها نفر اعدام شدند (Andrews, 2019, 1-2). لودیت‌ها، اعضای جنبش شورشی قرن ۱۹ در انگلستان بودند که در مخالفت با ماشین‌های بافندگی در سال ۱۸۱۱ و در شهر نانتینگهام، دست به اعتراض زدند (دانش‌نامه بریتانیکا).

نیز گواهی بر همین ادعاست. برخی این تحولات را انقلاب دیجیتال یا انقلاب پلتفرمی می‌نامند (Van Dijck, Poell, de Waal, 2018:4) که تأیید آن به معنای پذیرش تحولات عمیق در لایه‌ها و ساخت حیات جمعی است. انقلابی که در صورت گسترش، جامعه و دولت در ایران، گریزی از آن نخواهند داشت. امروزه و در عصر حکمرانی دیجیتال^۱، دولت الکترونیک تنها یک انتخاب نیست؛ بلکه عنصری حیاتی و غیرقابل اغماض در تداوم حضور دولت به‌ویژه در عرصه جهانی است (معمارزاده، مبینی و فقیهی، ۱۳۹۷: ۱۷). از همین روست که دولت‌ها درصددند، بخش‌های بیشتری از خدمات خود را مبتنی بر پلتفرم‌ها ارائه کنند. از جمله عرصه‌های مهمی که دولت‌ها، فناوری دیجیتال را در آن به‌کار می‌گیرند، حوزه نظارت است. مقاله حاضر نیز با همین ملاحظات و نظر به اهمیت تأثیر فناوری دیجیتال در حکمرانی، توجه خود را بر این وجه معطوف داشته است. یدیهی است؛ با توجه به گستردگی بحث، محوریت مقاله عملکرد نظارتی دولت و تأثیر فناوری دیجیتال بر آن خواهد بود. تمرکز مقاله، بر یکی از مهم‌ترین وجوه عملکردی دولت در ایران (نظارت دیجیتال بر مردم و جامعه) و شناخت عمیق‌تر تحولات این عرصه، به‌ویژه با توجه به کمبود ادبیات پژوهشی، از نوآوری‌های مقاله به‌شمار می‌رود.

۲. مبانی نظری

مبانی نظری، مطالعه حاضر از چند نظریه استخراج شده است. اول؛ نظریه مانوئل کاستلز (۲۰۰۹)، مبنی بر شکل‌گیری قدرت شبکه‌ای است. در نگاه کاستلز، فناوری‌های دیجیتال منجر به ایجاد شبکه‌هایی متشکل از گره‌های ارتباطی بین بخش‌های اصلی تبادل‌کننده داده در جامعه می‌گردند که تولید‌کننده قدرت‌اند. از این رو، شکل‌گیری جامعه شبکه‌ای و دولت شبکه‌ای، امری محتمل است. دولت شبکه‌ای، در چنین بستری از ظرفیت‌هایی برخوردار می‌شود که آن را قادر می‌سازد، با بهره‌گیری از داده‌ها و کنترل آن‌ها، جامعه را مدیریت کند. از نگاه کاستلز، چنین شیوه‌ای از اعمال قدرت، همواره سبب ایجاد مقاومت نیز خواهد شد (Castells, 2009:47-53). این شبکه-

1- Platform revolution
2- Digital Governance

۳- وجه دیگر قدرت دولت یعنی بعد «مدیریت» و تأثیر فناوری دیجیتال بر آن، در مقاله بعدی نویسندگان بررسی خواهد شد.

ها، دو عنصر اصلی دارند: اول؛ هستی‌شناسی متشکل از عناصر فزاینده شبکه‌ای که در جایگاه تبیین نباید از آن غفلت کرد. دوم؛ نظریه قدرت که بر اساس آن، قدرت به شکلی فزاینده در مجتمع‌های فناورانه - رسانه‌ای فراملی متمرکز می‌شود (Schroeder, 2018:2). افزایش توان نظارتی دولت برای نظارت شبکه‌ای و گسترده، مهم‌ترین شاخص برگرفته از این دیدگاه است که در بخش تجزیه و تحلیل دادها، آن را به کار می‌گیریم. نظریه دیگر، جبرگرایی فناورانه است. مارشال مک لوهان و هرولد اینیس، نظریه پردازان این رویکرد، برآنند که فناوری گاه ممکن است عاملیت اصلی را در تحولات بر عهده بگیرد و سبب بروز دگرگونی‌های مهم در جامعه شود؛ اما در نقد عاملیت فناوری، گفته شده است که فناوری، تنها عامل تعیین کننده نیست؛ بلکه شکل‌گیری آن نیز متأثر از شرایط اجتماعی جامعه است (Van loon, 2008:22-25&42-43). این نگاه انتقادی، در عین حال بیانگر این واقعیت است که شاید نتوان تصور نمود، فناوری همه‌جا نتایج یکسان به بار آورد. شاخص مهمی که از این دیدگاه برای به‌کارگیری در مطالعه حاضر سودمند است، تعامل فناوری و جامعه و اجتناب از نگاه جبرفناوری است. از سویی، در مباحث شناخت دولت، عموماً چهار چهره برای دولت قائل می‌شوند: ۱- وجه ایدئولوژیک ۲- وجه اجبار ۳- وجه عمومی (تأمین خدمات و کار ویژه‌های عمومی) ۴- وجه خصوصی یا چهره اقتصادی (بشیریه، ۱۳۹۶: ۳۷-۳۳). فناوری دیجیتال، در هریک از این عرصه‌ها، فرصت و چالش‌های نو ایجاد می‌کند. در وجه اجبار (اِزاری، ساختاری و ایدئولوژیک)، به‌کارگیری فناوری دیجیتال در ساختار ارتش، پلیس، زندان‌ها و نیروهای امنیتی، امکان نظارت و کنترل بیشتر بر شهروندان را فراهم می‌کند. در اجبار ساختاری، با استفاده از امکانات کلان‌داده و نظارت وسیع بر فضای مجازی، می‌توان از مخالفت‌ها و نارضایتی‌ها، آگاه و پیش از گسترش، مانع آن‌ها شد. در اجبار ایدئولوژیک، این امکان فراهم است که با تبلیغات هوشمند، به خواسته شهروندان جهت داد تا خواست دولت و احزاب سیاسی، تبدیل به باور عمومی شود و ضرورتی به اجبار ساختاری و اِزاری نباشد (خرازی، ۱۳۹۹: ۱۰۹). در وجه ایدئولوژیک، دولت‌ها با آگاهی از عقاید و انتظارات جامعه، قادرند مشروعیت مناسب برای هر نسل را تبیین کنند. مثلاً در یک نسل، مشروعیت سنتی انتساب به خداوند و نمایندگان او و در نسلی دیگر، مشروعیت دموکراتیک و یا مشروعیت کارآمدی پذیرفتنی است. در چهره عمومی، دولتی که از فناوری‌های دیجیتال بهره‌بردار، توانایی موثرتری در نظارت بر مشکلات اجتماعی و ارائه راهکار برای تقویت هم‌بستگی اجتماعی خواهد داشت. از منازعات زودتر مطلع

خواهد شد و سریع‌تر اقدام خواهد کرد. در وجه خصوصی، با گسترش نفوذ فناوری دیجیتال، وابستگی دولت به شرکت‌های صاحب فناوری افزایش می‌یابد. هم‌زمان این خطر هست که دولت تضعیف شود و به جای نمایندگی کردن افراد، به نمایندگان شرکت‌های صاحب فناوری تبدیل شود. با توجه به سهم قابل توجه فناوری‌های دیجیتال در آینده، این نگرانی مطرح است که اقتصاد، ارتش، جامعه و آموزش، تحت نفوذ این شرکت‌ها قرار گیرند؛ زیرا به مهم‌ترین شریک دولت در حکمرانی و اعمال قدرت تبدیل می‌شوند. مثلاً گسترش فناوری دیجیتال سبب شده است، آمریکا در جایگاه ابرقدرت مالی جهان، نسبت به آینده سيطرة مالی خود در تجارت جهانی، احساس خطر کند (Meredith, 2021, 1-2) و برای محدودسازی و کنترل معامله با ارز دیجیتال، وارد عمل شود. با کاهش نقش دولت در ارائه خدمات و تفویض آن به شرکت‌های خصوصی و صاحب فناوری، آسیب‌پذیری دولت در برابر حملات سایبری افزایش می‌یابد؛ زیرا این شرکت‌ها اغلب توجهی به پروتکل‌های امنیتی ندارند. هک شدن خطوط انتقال سوخت آمریکا در سال ۲۰۲۱ و از کار افتادن ۸۹۰۰ کیلومتر خط انتقال سوخت و افزایش بی‌سابقه قیمت، گواهی بر این ادعاست (Tidy, 2021, 1-2). در جمهوری اسلامی نیز از جمله حوزه‌هایی که در آن، بیشترین بهره‌گیری از فناوری‌های دیجیتال صورت گرفته، نظارت بر شهروندان است. نظارت در این حوزه، البته بدون چالش نبوده است. از این رو، برای مواجهه با آن‌ها، اقداماتی؛ نظیر تصویب قانون جرایم رایانه‌ای،^۱ تشکیل شورای عالی فضای مجازی، تشکیل کارگروه تعیین مصادیق محتوای مجرمانه، شکل‌گیری پلیس فضای تولید و تبادل اطلاعات فراجا، ارتش سایبری ایران و قرارگاه دفاع سایبری صورت گرفت. از این رو، با توجه به قرابت معانی وجوه دولت با آنچه مورد نظر این مطالعه است، در این مطالعه، چهره اول و دوم دولت، ذیل مفهوم نظارت در نظر گرفته شده است.

فناوری دیجیتال

فناوری دیجیتال، عموماً به رایانه‌ها، نظارت رایانه‌ای، جریان داده و شبکه سوئیچینگ تلفن مبتنی بر رایانه اشاره دارد. (Yates & Rice, 2020, 39). در تعریفی ساده شامل ابزارآلات الکترونیکی،

۱. این قانون مشتمل بر ۵۶ ماده و ۲۵ تبصره، پنجم خرداد ۱۳۸۸ در مجلس شورای اسلامی تصویب شد و بیستم خرداد همان سال به تأیید شورای نگهبان رسید.

سامانه‌ها و دستگاه‌هایی است که داده‌ها را تولید، پردازش و ذخیره می‌کنند. از این رو، فناوری دیجیتال، افراد را قادر می‌سازد در داده‌ها جستجو کنند، داده ایجاد کنند، آنها را به اشتراک بگذارند و یا به روزرسانی کنند (Yates & Rice, 2020,59). با این تعریف، طیف گسترده‌ای از ابزارهایی که روزانه استفاده می‌کنیم، در شمول ابزارآلات دیجیتال قرار می‌گیرند.

نظارت

نظارت دولت بر شهروندان، از ابتدای تشکیل دولت وجود داشته است. از جمله قدیمی‌ترین ساز و کارهای منسجم نظارت دولت، نظارت در دوره حاکمیت دودمان هان در چین است (افشار، ۱۳۹۹: ۱۹). اکنون آنچه به‌ویژه در قرن ۲۱ تغییر کرده، ابزار و شیوه‌های آن است. از این رو، نظارت و معنای آن، دستخوش تحولات تاریخی است؛ مثلاً از نگاه نهادهای مدنی، بهره‌گیری دولت از فناوری دیجیتال، برای نظارت (فیلترینگ، کنترل رایانه‌های شخصی از دور، کنترل وب‌کم‌ها، استفاده از بدافزار^۱ و اپلیکشن‌های موبایلی برای دسترسی به داده) نقض حریم خصوصی است (Arrigo, 2018, 42)؛ اما در مقابل، دولت‌ها بر این نظرند که افزایش توان نظارتی از این طریق، مانع بروز بی‌نظمی، حملات تروریستی و مراقبت از امنیت می‌شود (Snowden, 2019: Video File). نظیر همین اختلاف نظر، در تعریف نظارت دولتی هم هست. دانشنامه کمبریج^۲، آن را «زیر نظر گرفتن با دقت فرد و یا مکان، از سوی پلیس یا نیروی نظامی، به علت فعالیت مجرمانه و یا انتظار عملی مجرمانه» تعریف کرده است. تامسون، آن را «گردآوری و پردازش داده‌های آشکار و پنهان افراد، با هدف تحت تأثیر قرارداد و یا مدیریت آن‌ها» بیان می‌کند (Thomsen, 2019: 702). هاگرتی و ساماتاس، آن را «شیوه‌های زیر نظر گرفتن افراد و اماکن، با هدف مداخله در امور» توصیف می‌کنند (Haggerty & Samatas, 2010: 2) و بلابی نیز معنایی گسترده شامل: «فعالیت دوربین‌های مداربسته و نظارت پنهان تا نظارت بر داده^۳ و داده‌کاوی^۴ در موضوعاتی؛ همانند هویت، مسیرهای رفت و آمد، نزدیکان، شغل و...» را مطرح می‌کند (Bellaby, 2012: 105). به نظر می‌-

۱. Han dynasty: دومین خاندان بزرگ چین که بین سال‌های ۲۰۶ قبل از میلاد تا ۲۲۰ میلادی (در حدود ۴۰۰ سال) در چین قدرت حاکم بوده است.

۲. malware

۳. Cambridge Dictionary

۱. Dataveillance

۲. Data mining

رسد؛ با همه ملاحظات بالا، می‌توان نظارت را چنین تعریف کرد: تشکیل پروفایل دیجیتال برای افراد، از طریق کنار هم قراردادن داده‌های گردآوری شده درباره آن‌ها از منابع مختلف دولتی و غیردولتی، با هدف مداخله و مدیریت. این تعریف، افزون بر تصریح وجه دیجیتالی نظارت و داده-محور بودن آن، بر بُعد حاکمیتی با قصد مداخله نیز دلالت دارد. بدیهی است؛ چنین رویکردی به موضوع، روش پژوهش مناسب خود را می‌طلبد.

روش تحقیق

با توجه به ماهیت موضوع، پژوهش از نوع کیفی و بر اساس روش گراند تئوری است. انتخاب این روش، از آن روست که تاکنون در ارتباط با موضوع مقاله، نظریه‌پردازی مدونی صورت نگرفته است. همچنین به علت جدید و پویا بودن موضوع، گردآوری داده‌های به‌روز، مستلزم مصاحبه با افراد مطلع است. از این رو، به‌منظور گردآوری داده‌های اصلی، مصاحبه‌های عمیق به شکل نیمه-ساخت‌یافته با جامعه نمونه، متشکل از سه دسته افراد صورت گرفت: ۱- نخبگان دانشگاهی (استادان، شاغلان به تحصیل و دانش‌آموختگان حوزه مهندسی نرم‌افزار، سخت‌افزار، هوش مصنوعی و فناوری اطلاعات، علوم سیاسی، جامعه‌شناسی، آینده‌پژوهی) که درباره موضوع مطالعه عمیق و یا پژوهش داشته‌اند. گزاره‌های این افراد، با کد IN-F در جداول مشخص شده است. ۲- کارشناسان: افرادی که با وجود پیشینه مطالعاتی متعدد، اما در حوزه کارشناسی مرتبط با موضوع این پژوهش، در شرکت‌ها و سازمان‌ها فعالیت دارند. گزاره‌های ایشان، با کد IN-SP مشخص شده است. ۳- شاغلان حوزه جمع‌آوری داده از فضای مجازی؛ یعنی افرادی که در حوزه نظارت و یا مدیریت دولتی، با استفاده از فناوری‌های دیجیتال، فعال‌اند و به‌روزترین اطلاعات را در اختیار دارند. گزاره‌های این افراد نیز با کد IN-B در جداول متمایز شده است.

برای شناسایی افراد در مصاحبه‌های اولیه، از نمونه‌گیری هدفمند و پس از آن، به شیوه نمونه-گیری شبکه‌ای به‌منظور شناسایی افرادی با داده‌های سرشار^۱ و ارزشمند عمل شد. با توجه به این که در تحقیقات کیفی، حجم نمونه نباید کمتر از ۲۰ نفر باشد (محمدپور، ۱۳۹۸: ۶۲۶) در ابتدا، جامعه نمونه ۲۰ نفره در نظر گرفته شد؛ اما در فرایند مصاحبه، بعد از نفر دهم مشخص شد، دیدگاه

نظری جدیدی مطرح نمی‌شود. با این حال، با اصلاح شیوه طرح برخی پرسش‌ها به منظور گردآوری داده‌های جدیدتر، تا ۱۵ نفر مصاحبه ادامه یافت. به منظور تحلیل داده‌های به دست آمده از روش کدگذاری سه مرحله‌ای (کدگذاری باز، کدگذاری محوری، کدگذاری گزینشی یا انتخابی)، گرداندن تئوری استفاده شده است. به منظور آزمون روایی پرسش‌ها، از نظر متخصصان، اساتید دانشگاهی و کارشناسان خبره استفاده شده است. همچنین در مرحله طراحی پرسش‌ها، با انجام مصاحبه‌های پایلوت و کسب نظرات مصاحبه شونده‌گان، اصلاحات لازم در پرسش‌ها اعمال شد؛ لذا اطمینان حاصل گردید که پرسش‌ها، موضوع مورد نظر را می‌سنجند. به منظور تعیین پایایی، در پایان کدگذاری، پاسخ‌های به دست آمده از پنج نفر (حدود ۳۰ درصد) از اعضای جامعه نمونه خواسته شد. کدگذاری پاسخ‌ها را صحت‌سنجی کنند که بیش از هفتاد درصد کدگذاری‌ها مورد تأیید منتخبان جامعه نمونه بود و مواردی هم مطابق نظرات ایشان اصلاح شد. جدول شماره (۱) سیمای مصاحبه شونده‌گان را ارائه می‌کند.

جدول ۱- سیمای مصاحبه شونده‌گان

ردیف	کد مصاحبه شونده	مشخصات مشارکت کننده
۱	IN-SP-01	مرد- دکترای علوم اعصاب شناختی گرایش رایانش و هوش مصنوعی- فعال در پژوهشکده علوم شناختی
۲	IN-SP-02	زن - کارشناسی ارشد علوم سیاسی - تخصص در حوزه دولت الکترونیک
۳	IN-SP-03	زن - کارشناسی ارشد مهندسی نرم افزار
۴	IN-SP-04	مرد - کارشناسی IT - فعال در حوزه توان مدیریتی دولت
۵	IN-SP-05	مرد - دکترای آینده‌پژوهی - فعال در دانشکده عالی دفاع ملی
۶	IN-SP-06	مرد - کارشناسی ارشد هوش مصنوعی - فعال در حوزه توان مدیریتی دولت
۷	IN-SP-07	مرد - کارشناسی مهندسی نرم افزار - فعال در حوزه توان مدیریتی دولت
۸	IN-SP-08	زن - کارشناسی ارشد مهندسی نرم افزار - کارشناس سیستمی و متخصص هوش مصنوعی
۹	IN-SP-09	زن - کارشناسی ارشد IT - متخصص هوش مصنوعی
۱۰	IN-SP-10	مرد - دکترای جامعه‌شناسی - فعال در حوزه توان مدیریتی دولت
۱۱	IN-F-01	مرد - دکترای مهندسی کامپیوتر - استادیار مدرس در دانشگاه
۱۲	IN-F-02	مرد - دکترای علم کامپیوتر - استادیار مدرس در دانشگاه - مدرس IT
۱۳	IN-F-03	مرد - دکترای هوش مصنوعی - عضو اندیشکده سیاسی
۱۴	IN-B-01	مرد - کارشناسی مهندسی نرم افزار - دانشجوی دکتری فلسفه - فعال در حوزه توان نظارتی دولت
۱۵	IN-B-02	زن - کارشناسی مهندسی نرم افزار - کارشناسی ارشد علوم سیاسی - فعال در حوزه توان نظارتی دولت

یافته‌های پژوهش

به منظور دستیابی به پاسخ پرسش اصلی، مصاحبه‌ها در قالب چهار پرسش فرعی هدایت شد. در

ادامه این بخش، نظرات مصاحبه شونده‌گان به هر پرسش فرعی، در جدولی جداگانه ارائه می‌شود.^۱

۱. به منظور رعایت حجم مقاله از نظر تعداد صفحات، از ارائه توضیحات جداگانه بعد از هر جدول خودداری شده است. توضیحات لازم، ذیل بخش نتایج در پایان مقاله گنجانده شده است.

***پرسش اول: وضعیت کنونی دولت ایران، در استفاده از فناوری دیجیتال برای نظارت بر شهروندان را چگونه ارزیابی می‌کنید؟**

جدول ۲ - پاسخ مصاحبه‌شوندگان به پرسش اول

ردیف	کد مصاحبه شونده	کد گذاری باز	کد گذاری محوری	کد گذاری گزینشی
۱	IN-SP-01	در حوزه به‌کارگیری هوش مصنوعی در شبکه دوربین‌های مداربسته، اقدامات خوبی صورت گرفته است؛ اما کامل نیست. در حوزه جمع‌آوری داده شهروندان، حاکمیت بر فضای مجازی، به علت این که سرور شبکه‌های اجتماعی، در خارج از کشور هستند، عملاً غیرممکن است.	عملکرد خوب در به - کارگیری هوش مصنوعی، در شبکه دوربین‌های مداربسته و ضعف در جمع - آوری داده شهروندان، به علت وابستگی به سرورهای خارجی	پیشرفت قابل توجه در به - کارگیری هوش مصنوعی، اما رویارویی با چالش در اختیار نداشتن سرورهای خارجی.
۲	IN-SP-02	برنامه‌ریزی دولت (از اواخر دهه هشتاد)، در حوزه - هایی؛ مانند بخش‌های دفاعی، امنیتی، مرزبانی و پایش اطلاعاتی، تبادلات بانکی موفق بوده است؛ اما رویکرد سلبی در نظارت بر شهروندان، به علت مسدودسازی دسترسی و کاهش سرعت اینترنت، کمکی به توان دولت در نظارت و افزایش خدمات عمومی نخواهد کرد.	سرمایه‌گذاری موفقیت‌آمیز در عرصه توان نظارتی و دفاعی، امنیتی و بانکی، اما رویکرد سلبی در برخورد با فناوری‌های دیجیتال.	تعارض رویکرد دولت در سرمایه‌گذاری گسترده، برای نظارت بر شهروندان، با عملکرد سلبی و مسدودسازی و فیلترینگ
۳	IN-SP-03	بیشتر دستاوردهای دولت ایران، در استفاده از فناوری‌های دیجیتال در حوزه امنیتی است. در حوزه‌های اجتماعی، فرهنگی و اقتصادی که موثر بر زندگی مردم است، کمتر استفاده شده است.	تمرکز دولت در ایران، بر استفاده از فناوری‌های دیجیتال، در بُعد امنیتی است. کم‌رنگ بودن تأثیر فناوری در حوزه‌های اجتماعی، فرهنگی و اقتصادی.	تمرکز دولت در ایران، بر به - کارگیری فناوری دیجیتال در ابعاد امنیتی و غفلت از حوزه‌های فرهنگی و اقتصادی
۴	IN-SP-04	زیر نظر داشتن مردم، موجب آگاهی بهتر دولت از نیازهای مردم خواهد شد. همچنین بهبود خدمات - رسانی و شناخت بهتر دولت از جامعه را در پی دارد.	آگاهی بهتر دولت از جامعه و بهبود خدمات‌رسانی	شناخت بهتر دولت از جامعه و بهبود خدمت‌رسانی
۵	IN-SP-05	دولت در ایران، به‌طور فعالانه، داده شهروندان را جمع - آوری نمی‌کند. تحلیل هدفمندی در اطلاعات جمع‌آوری شده، صورت نمی‌گیرد و منتشر نمی‌شود. بیشترین استفاده از داده‌های جمع‌آوری شده، در عرصه امنیتی و شناسایی است.	بیشترین بهره‌گیری از فناوری دیجیتال، در عرصه امنیتی و شناسایی است؛ اما در عین حال، گردآوری و تحلیل داده‌ها نیز مستمر و هدفمند نیست.	تمرکز بر وجه امنیتی و شناسایی و غفلت از گردآوری مؤثر و تحلیل هدفمند داده‌ها، منتشر نشدن گزارش‌ها به‌صورت مستمر
۶	IN-SP-06	دسترسی به منابع داخلی که ارزیابی از وضعیت موجود ارائه دهند، ممکن نیست. سیستم نظارت دوربین‌های مداربسته در ایران، جای بسیار بیشتری برای هوشمندسازی و توسعه دارد. دانشگاه، در عرصه بهبود توان نظارتی دولت، ورود کرده است. در به - کارگیری هوش مصنوعی در بخش نظارت، اقدامات	کمبود گزارش از وضع موجود. پیشرفت خوب است؛ اما جای پیشرفت بسیاری وجود دارد. لزوم میدان دادن به دانشگاه، تمرکز	پیشرفت خوب در نظارت، با استفاده از هوش مصنوعی، نیاز به تلاش بیشتر در حوزه دوربین‌های نظارتی، محدودیت دسترسی به گزارش‌های ارزیابی داخلی،

		خوبی صورت گرفته است.		
لزوم توجه به دانشگاه	دولت در ایران بر استفاده از فناوری های دیجیتال در بعد نظارت			
۷	IN-SP-07	در عرصه نظارت فعال بر شهروندان و جمع آوری داده آن ها اقدامات ویژه ای صورت نگرفته است. ضعف زیرساخت های نظارتی در کنار کمیود بودجه، مانع تقویت توان نظارتی کشور است. نسبت به امکانات موجود، اقدامات خوبی صورت گرفته است؛ اما جای پیشرفت بیشتری وجود دارد.	بیشترت های صورت گرفته است، اما جای پیشرفت بسیاری وجود دارد. عدم جمع آوری فعالانه داده، به علت ضعف زیرساخت ها و کمیود بودجه	به علت نبود زیرساخت ها و کمیود بودجه، نظارت بر شهروندان و گردآوری داده ها مطلوب نیست.
۸	IN-SP-08	در حال حاضر، دانش و تخصص لازم برای توسعه وجود دارد. در ساختار سیاسی ایران، علاقه و اراده بیشتری برای توسعه توان نظارتی وجود دارد. در ایران، به صورت محدود کارهایی انجام می شود؛ اما این کارها ساختاریافته نیستند. در برخی از حوزه ها، بنا به دلایلی، متخصصان به کار گرفته نشده اند.	دانش و تخصص در کشور، موجود است. اشتیاق بیشتری در تقویت توان نظارتی دولت وجود دارد. برنامه جامعی در این حوزه تعریف نشده است. لزوم به - کارگیری نیروهای متخصص	ساختارمند نبودن تلاش ها در این عرصه؛ مثلاً از متخصصان استفاده کافی نمی شود. تمرکز بیشتر ساختار سیاسی بر وجه امنیتی و نظارتی، ساختاریافته نبودن اقدامات انجام شده
۹	IN-SP-09	در حوزه نظارت، استفاده از هوش مصنوعی مهم است. در ایران، استفاده از هوش مصنوعی پیشرفت داشته است؛ اما سرعت آن اندک است. در ایران، بیشتر بر حوزه اعمال نظارتی تمرکز شده است.	در ایران، تمرکز بیشتر بر استفاده از هوش مصنوعی در حوزه نظارت است؛ اما سرعت پیشرفت، کم است.	تمرکز فناوری دیجیتال بر حوزه نظارت زیاد؛ اما پیشرفت آن کم است.
۱۰	IN-SP-10	با توجه به نبود رویکردی ثابت در دولت ها و عدم سرمایه گذاری در زیرساخت ها در این حوزه، نسبت به کشورهای منطقه عقب تر هستیم. اگر وضع فعلی در آینده ادامه یابد، وضعیت نگران کننده ای خواهیم داشت.	نیود رویکرد واحد میان دولت ها و نیود سرمایه گذاری، مهم ترین علل عقب ماندگی ما در منطقه است. ادامه این وضعیت سبب می شود، آینده نیز نگران کننده باشد.	وضعیت نامطلوب در حوزه نظارت، به علت نداشتن رویکرد واحد در دولت ها و نیود سرمایه گذاری. آینده نگران کننده در صورت ادامه این وضعیت.
۱۱	IN-F-01	فناوری دیجیتال در دو حوزه نرم افزار و سخت افزار، قابل بررسی است. در بخش سخت افزار در داخل کشور، تکیه بر واردات است. ضعف در بخش سخت افزاری، باعث ضعف در بخش نرم افزاری نیز شده است. با وجود این، در بخش نرم افزاری امنیتی، دستاوردهای مهمی در حوزه نظارت صورت گرفته است.	وابستگی در بخش سخت افزار، نظارت، سبب ضعف در بخش نرم افزار نیز شده است. با این وجود، دولت در بخش نرم افزار، دستاوردهای مهمی داشته است.	دستاوردهای مهم در بخش نرم افزار امنیتی نظارت، لزوم تلاش برای رفع موانع سخت افزاری (تحریم ها)
۱۲	IN-F-02	پیشرفت های خوبی در سال های اخیر صورت گرفته است. ایران در این عرصه از بسیاری از کشورهای منطقه جلوتر است. افزایش توان نظارتی دولت ایران	پیشرفت در سال های اخیر و جایگاه مطلوب ایران در حوزه نظارت در منطقه	پیشرفت خوب و لذا افزایش توان نظارتی دولت ایران در مقایسه با سایر کشورهای منطقه
۱۳	IN-F-03	دولت در ایران، به دلایل امنیتی، بیشتر بر حوزه نظارت دیجیتال تمرکز دارد. با وجود تمامی تلاش ها، ایران در حوزه نظارت، نسبت به کشورهای توسعه یافته و در حال توسعه، جای پیشرفت بسیاری دارد.	تمرکز بیشتر دولت در نظارت دیجیتال و در عین حال، عقب ماندن در مقایسه با کشورهای توسعه یافته	تمرکز بیشتر دولت در نظارت دیجیتال و در عین حال، عقب ماندن در مقایسه با کشورهای توسعه یافته

۱۴	IN-B-01	آن قدری که من اطلاع دارم، مقداری در این جهت پیشرفته‌ایم؛ اما در اول راه هستیم.	پیشرفت در سال‌های اخیر اما هنوز اول راه هستیم	پیشرفت اندک در حوزه نظارتی
۱۵	IN-B-02	اطلاعات موجود در رابطه با توان نظارتی ایران، اندک است. تقویت توان نظارتی دولت، مورد توجه حاکمیت است. تنها بخشی است که حاکمیت به فکر تقویت جدی آن است.	کمبود اطلاعات در رابطه با توان نظارت دولت، عزم جدی بیشتری در تقویت توان نظارتی دولت دیده می‌شود.	با وجود عزم جدی حاکمیت برای تقویت نظارت دیجیتال، اطلاعات در این خصوص کم است.

*پرسش دوم: دولت در ایران، در بهره‌برداری از فناوری دیجیتال برای نظارت، با چه چالش‌هایی مواجه است؟

جدول ۳ - پاسخ مصاحبه‌شوندگان به پرسش دوم

ردیف	کد مصاحبه‌شونده	کد گذاری باز	کد گذاری محوری	کد گذاری گزینشی
۱	IN-SP-01	سلطه فنی، اقتصادی و سیاسی قدرت‌های جهانی بر اینترنت و فناوری دیجیتال و نیز تحریم‌ها؛ تسلط حاکمیت بر بخش‌هایی از فناوری دیجیتال و منافع اقتصادی و سیاسی و مقاومت در برابر بهره‌برداری بیشتر؛ کیفیت بالای خدمات شرکت‌های خارجی تعارض عمیق دولت در این عرصه، به این دلیل که از یک سو به دنبال محدودسازی و مسدودسازی دسترسی شهروندان به فناوری-های دیجیتال، با استفاده از فیلترینگ و کاهش سرعت اینترنت است و از سوی دیگر، به دنبال افزایش توان نظارتی خود بر داده شهروندان در فضای دیجیتال است.	لزوم سرمایه‌گذاری در زیرساخت‌ها، تأثیر منفی تحریم‌ها مقاومت‌های داخلی بخش‌هایی از دولت کیفیت بالای خدمات خارجی چالش محدود و مسدودسازی، دسترسی شهروندان با افزایش توان نظارتی دولت بر شهروندان	تحریم و تبعات آن؛ مانند نبود زیرساخت‌ها، سلطه قدرت-های بزرگ فناوری دیجیتال، برخی مقاومت‌های داخلی تناقض دولت در فیلترینگ و مسدودسازی شهروندان با افزایش توان نظارتی دولت بر شهروندان در فضای دیجیتال
	IN-SP-02	به‌روز نبودن تجهیزات و لوازم مورد نیاز، خروج نخبگان از کشور، تنش در روابط با کشورهای خارجی، انفعال در تصمیم‌گیری‌های کلان سیاسی، نگاه بدبینانه برخی از مقامات، نسبت به افزایش استفاده از فناوری‌های دیجیتال، نگاه فرصت‌طلبانه برخی از مقامات، برای سوءاستفاده از این تکنولوژی‌ها، برای رصد و کنترل احزاب، اصناف و گروه‌ها، فرهنگ سنتی و رشد نیافته در مناطق محروم که مانع گسترش این فناوری‌ها می‌شود. اقتصاد بحران‌زده در ایران که به دلیل تحریم‌ها و فساد، رانت قادر به تأمین منابع مالی برای زیرساخت‌های فناوری دیجیتال نیست. بی-	به روز نبودن زیرساخت‌ها، خروج نخبگان، تنش در روابط خارجی، انفعال در تصمیم‌گیران سیاسی، نگاه بدبینانه و فرصت‌طلبانه مسئولان به فناوری، غلبه نگاه سنتی در مناطق محروم، بی-اعتمادی متقابل شهروندان	تحریم و تبعات آن؛ مانند و به‌روز نبودن زیرساخت‌ها و فساد و رانت، تنش در روابط خارجی و تعارض در نگاه مسئولان، غلبه فرهنگ سنتی در مناطق محروم و بی-اعتمادی متقابل مردم

		اعتمادی جامعه و عدم ارائه اطلاعات درست به دستگاه‌های دولتی، به دلیل نگرانی از افزایش مالیات و عوارض		
۳	IN-SP-03	بزرگ‌ترین چالش برای دولت ایران، چالش فرهنگی است که با حل آن، بقیه مشکلات حل خواهد شد. نظارت مخالف و متضاد در کنار رویکردهای متضاد دولت‌ها، باعث شده است تا تلاش‌ها برای تحقق اهداف مورد نظر به ثمر نرسد.	چالش فرهنگی، مهم‌ترین چالش دولت است. لزوم اتخاذ رویکرد واحد دولت‌ها در ایران، برای پیشبرد اهداف تعیین شده	لزوم حل چالش فرهنگی، ضرورت اتخاذ رویکرد واحد حاکمیتی در قبال این مسئله
۴	IN-SP-04	در وهله اول می‌بایست، فرهنگ‌سازی لازم برای کمک به مردم در این حوزه انجام شود. تاکید کردن بر مزیت‌های فناوری‌های دیجیتال برای مردم، نیاز به تأمین بودجه، همکاری لازم میان بخش‌های مختلف دولت، نیاز به تأمین نیروی انسانی متخصص	نیاز به فرهنگ‌سازی، تأمین بودجه، نبود هماهنگی در دولت، تأمین نیروی انسانی متخصص	چالش فرهنگی، سرمایه گذاری در زیرساخت‌ها، لزوم هماهنگی در دولت، تأمین نیروی انسانی متخصص
۵	IN-SP-05	برخی دولتمردان، از گسترش فناوری‌های دیجیتال احساس ناامنی می‌کنند؛ به دلیل این که ممکن است، امکان نظارت کامل را ندهد و نیز وابستگی به خارج را سبب شود. همچنین احتمال صدمه بخش اقتصاد سنتی ایران	نبود رویکرد واحد میان مسئولان، بی‌اعتمادی و بدبینی برخی مسئولان به‌خاطر احتمال وابسته شدن به خارج کشور، احتمال صدمه دیدن بخش‌هایی از اقتصاد سنتی در جامعه	بدبینی مسئولان به فناوری‌های دیجیتال خارجی، آسیب وارد آمدن به بخش اقتصاد سنتی ایران
۶	IN-SP-06	اینترنت فعلی در ایران، آمادگی تبادل اطلاعات در سطح بالا را ندارد. در بخش سخت‌افزار، وابستگی به خارج است که به دلیل تحریم‌ها، امکان نوسازی اندک است. دیدگاه منفی بخشی از جامعه به توسعه فناوری‌های اجتماعی، به دلیل برخی عواقب اجتماعی آن، اعتماد مردم و این که مایل به استفاده از پلتفرم‌های داخلی نیستند.	تحریم‌ها و تبعات آن؛ مانند نرم افزار و سخت‌افزار و نبود سرمایه‌گذاری در زیرساخت‌ها، بی‌اعتمادی مردم به پلتفرم‌های داخلی و نگرانی از عواقب آن	تحریم‌ها و تبعات آن؛ مانند نرم افزار و سخت‌افزار و نبود سرمایه‌گذاری در زیرساخت‌ها، بی‌اعتمادی مردم به پلتفرم‌های داخلی و عواقب آن
۷	IN-SP-07	اولین چالش چالش اقتصادی است. نبود بودجه لازم برای توسعه زیر ساخت‌ها، دوم چالش فنی است چراکه به دلیل تحریم‌ها امکان واردات تجهیزات و دانش به روز نیست. ضعف دانش داخلی نیز مانع به روز رسانی زیرساخت‌هاست.	کمبود بودجه لازم، چالش فنی به روز نبودن زیرساخت‌ها به علت تحریم‌ها، ضعف دانش داخلی	ضعف سرمایه‌گذاری در زیرساخت‌ها، چالش فنی به روز نبودن زیرساخت‌ها به علت تحریم‌ها
۸	IN-SP-08	مهم‌ترین چالش سیاسی است. در حال حاضر، در میان مسئولان عالی رتبه کشور، نسبت به توانایی‌های فناوری‌های دیجیتال، اتفاق نظری وجود ندارد.	چالش سیاسی؛ یعنی اختلاف نظر مسئولان در خصوص به کارگیری فناوری دیجیتال	چالش سیاسی و اختلاف نظر مسئولان در این باره
۹	IN-SP-09	بحث فنی و زیرساخت‌ها در ایران، اولویت بسیاری دارد. همچنین در حال حاضر، بودجه برای سرمایه‌گذاری در زیرساخت‌ها نیست. هر فناوری جدیدی، قبل از استفاده عمومی نیاز به فرهنگ‌سازی دارد.	ضعف فنی و زیرساخت‌ها، ضعف سرمایه‌گذاری و بودجه و نیاز به فرهنگ‌سازی برای فناوری‌های جدید	ضعف سرمایه‌گذاری در زیرساخت‌ها، مشکلات بودجه‌ای و نبود فرهنگ‌سازی لازم

<p>مسأله تحریم، نبود رویکرد حاکمیتی یکدست، بی اطلاعی مردم درباره فناوری‌های جدید و بی‌اشتیاقی آن‌ها</p>	<p>تحریم و پیامدهای آن: وارد نشدن فناوری و نبود سرمایه - گذاری. همچنین نبود اتفاق نظر بین مسئولان، در قبال فناوری دیجیتال. چالش فرهنگی؛ یعنی نبود فرهنگ استفاده صحیح در بین مردم</p>	<p>چالش تحریم که مانع ورود فناوری و هم مانع سرمایه‌گذاری در زیرساخت شده است. چالش بعدی، نبود اتفاق نظر بین مسئولان، درباره ضرورت به‌کارگیری فناوری‌های دیجیتال. چالش بزرگتر، البته فرهنگی است که مردم در قبال استفاده صحیح از فناوری دیجیتال، بی‌اطلاع هستند.</p>	<p>IN-SP-10</p>	<p>۱۰</p>
<p>نیود اعتماد از جانب مردم به برنامه‌های دولت در این خصوص</p>	<p>اعتماد نداشتن مردم به برنامه‌های دولت، در به‌کارگیری فناوری‌های دیجیتال؛ مانند پیام رسانه‌های داخلی</p>	<p>بزرگ‌ترین چالش دولت ایران، اعتمادسازی است. استقبال نکردن مردم از پیام‌رسان‌های داخلی، به دلیل نگرانی از سوءاستفاده اطلاعات آن‌ها است. مردم، پیام‌رسان‌های خارجی را که مطمئن هستند توسط آن‌ها رصد می‌شوند، به پیام‌رسان‌های داخلی ترجیح می‌دهند.</p>	<p>IN-F-01</p>	<p>۱۱</p>
<p>آشنا نبودن مردم با مزایا و معایب فناوری‌های جدید</p>	<p>فناوری برای دولت ایران، شمشیر دو لبه است. آشنا نبودن مردم با مزایا و معایب فناوری‌های جدید</p>	<p>فناوری‌های دیجیتال، مانند شمشیر دو لبه هستند. درباره استفاده از مزایا، نیاز به آموزش مردم داریم. در خصوص مدیریت معایب، نیاز به آموزش مردم داریم.</p>	<p>IN-F-02</p>	<p>۱۲</p>
<p>تأثیر منفی تحریم‌ها و چالش فنی ناشی از آن، چالش علمی در داخل، چالش فرهنگی داخلی، چالش مذهبی داخلی</p>	<p>چالش فنی در زیرساخت، چالش ضعف علمی داخلی، چالش فرهنگی و نگاه مردم، چالش مذهبی، تأثیر منفی تحریم‌ها</p>	<p>اولین چالش برای ایران، ضعف در زیرساخت‌ها است. دومین چالش، ضعف علمی در دانشگاه است. به دلیل تحریم‌ها، ارتباط علمی با جهان خارج قطع است. چالش فرهنگی و مذهبی در کشور، مهم‌ترین نقش را در جلوگیری از توسعه فناوری‌های دیجیتال دارند. بخشی از جامعه، نگران است؛ با فراگیری فناوری‌های دیجیتال، فرهنگ جامعه تضعیف شود.</p>	<p>IN-F-03</p>	<p>۱۳</p>
<p>چالش‌های امنیتی و سیاسی. چالش فرهنگی و چالش فنی (نیود زیرساخت‌ها)</p>	<p>وجود چالش‌های امنیتی و سیاسی. چالش فرهنگی، به دلیل تفاوت فرهنگ‌ها و نیز چالش فنی</p>	<p>ایران، در این عرصه با چالش‌های سیاسی و امنیتی مواجه است. در این خصوص، چالش فرهنگی هم داریم؛ چرا که خاستگاه تکنولوژی جدید، جای دیگری است؛ لاجرم چالش فرهنگی ایجاد می‌شود. چالش‌های فنی و مشکلاتی داشته‌ایم؛ اما تا حدودی در حوزه فنی، پیشرفت‌هایی داشته‌ایم.</p>	<p>IN-B-01</p>	<p>۱۴</p>
<p>چالش حاکمیتی - سیاسی سرمایه گذاری در زیرساخت‌ها چالش فرهنگی</p>	<p>نیاز به ایجاد درک صحیح مسئولان از فناوری‌های دیجیتال. چالش فنی در کشور؛ زیرساخت‌ها در کشور ضعیف‌اند. چالش فرهنگی در کشور</p>	<p>اولین چالش، حاکمیتی است. مسئولان باید درک کنند، نمی‌توان جلوی فناوری‌های دیجیتال ایستاد. دومین چالش، فنی است. سخت‌افزارها و دانش کافی برای استفاده از ظرفیت کامل فناوری‌های دیجیتال وجود ندارد. چالش دیگر، فرهنگی است. بخشی از جامعه معتقد است؛ فناوری‌های دیجیتال، اگر در جامعه فراگیر شوند، باعث تضعیف فرهنگ آن‌ها می‌شود.</p>	<p>IN-B-02</p>	<p>۱۵</p>

*پرسش سوم: اگر دولت در ایران بخواهد از فناوری دیجیتال برای نظارت بهره ببرد، نیازمند چه

تمهیداتی است؟

جدول ۴ - پاسخ مصاحبه شوندگان به پرسش سوم

ردیف	کد مصاحبه شونده	کد گذاری باز	کد گذاری محوری	کد گذاری گزینشی
۱	IN-SP-01	اعمال حاکمیت بر ابعاد مختلف فناوری دیجیتال، با تأکید بر اقدامات ایجابی تا سلبی توجه به آینده‌نگری و آینده‌نگاری، برای خروج از انفعال کنونی. فراهم کردن یک شبکه داخلی در کنار اینترنت جهانی و تهیه سرور و مراکز ذخیره داده فراهم کردن بستر رقابت برای شرکت‌های داخلی ترغیب شرکت‌های خارجی بر ارائه خدمات، بر بستر شبکه داخلی، با توجه به پهنای باند بیشتر و دعوت از آن‌ها به تبعیت از قوانین ایران	اتخاذ رویکرد ایجابی برای اعمال حاکمیت بر فناوری دیجیتال، لزوم برنامه - ریزی معطوف به آینده، فراهم کردن زیرساخت‌های شبکه داخلی، بسترسازی برای رقابت شرکت‌های داخلی با شرکت‌های خارجی، ترغیب شرکت‌های خارجی، برای ورود به کشور	لزوم اتخاذ رویکرد ایجابی بر حکمرانی فناوری‌های دیجیتال سرمایه‌گذاری در زیرساخت‌ها حمایت از شرکت‌های خصوصی داخلی بسترسازی برای حضور شرکت‌های فناور خارجی
۲	IN-SP-02	تنش‌زدایی در روابط با دول غربی و حرکت برای توسعه روابط در عرصه فناوری‌های دیجیتال، افزایش سرمایه‌گذاری در این عرصه، ایجاد رشته دانشگاهی جدید و دعوت از استادان برجسته، تلاش برای افزایش اعتماد شهروندان به دولت، با مشارکت دادن مردم در امور حاکمیتی و کلان، سرمایه‌گذاری در مناطق محروم و کمتر توسعه‌یافته برای افزایش سواد و رفاه عمومی، زمینه‌سازی وای آشنایی عموم با این فناوری‌ها	حل مسئله تحریم و توسعه روابط با غرب، سرمایه‌گذاری در زیرساخت‌های فناوری دیجیتال، استفاده از ظرفیت دانشگاه‌های داخل، اعتمادسازی در مردم نسبت به حاکمیت، آموزش به مردم	حل مسئله تحریم و توسعه روابط با غرب، سرمایه‌گذاری در زیرساخت‌ها، آموزش مردم، اعتمادسازی در مردم نسبت به حاکمیت
۳	IN-SP-03	مهم‌ترین چالش، تعریف ربط و نسبت دولت با فناوری‌های دیجیتال است؛ به نحوی که مردم نیز آن را بپذیرند. این رابطه، از جنس فرهنگی است.	برنامه داشتن دولت برای شیوه رویارویی با فناوری‌های دیجیتال، با در نظر گرفتن نگاه و نظر مردم. اعتمادسازی در مردم نسبت به حاکمیت فرهنگ‌سازی در مردم	تدوین و تعریف نسبت دولت در رویارویی با فناوری‌های دیجیتال اعتمادسازی در مردم نسبت به حاکمیت فرهنگ‌سازی در جامعه
۴	IN-SP-04	نخست؛ زیرساخت‌ها، اصلاح و به‌روز رسانی شوند. عقب‌افتادگی زیادی نسبت به برخی از کشورهای همسایه و آسیا داریم.	اصلاح و به‌روزرسانی زیرساخت‌ها و جبران عقب‌افتادگی	سرمایه‌گذاری در زیرساخت‌ها، جبران عقب‌ماندگی
۵	IN-SP-05	نیاز به زیرساخت‌های بومی، ایجاد بانک‌های اطلاعاتی، تولید نرم‌افزارهای ویژه پردازش زبان فارسی، تقویت توان تحلیل داده به زبان فارسی، تمرکز بر امنیت زیرساخت‌ها؛ به عنوان مثال حمله به مراکز سوخت، می‌تواند برای سایر بخش‌های دولت نیز اتفاق بیفتد.	تأمین زیرساخت‌های بومی در همه ابعاد تأمین امنیت زیرساخت‌ها	سرمایه‌گذاری در زیرساخت‌ها تأمین امنیت فناوری برای ممانعت از حملات
۶	IN-SP-06	استفاده از فناوری‌های دیجیتال در دولت، نیاز به تصمیم‌گیری حاکمیتی و فرادولتی دارد. نیاز به اقتناع بخش مخالف در دولت، برای پذیرش فناوری‌های دیجیتال، برخی دولت‌ها در کل مخالف اهداف دولت الکترونیک در ایرانند، ایجاد موانع قانونی برای جلوگیری از سوءاستفاده از داده‌های جمع‌آوری شده از شهروندان، لازم است توسعه بخش ابزار نظارت، توسط بخش خصوصی صورت گیرد. همچنین زیرساخت‌های فنی در کشور، به‌روزرسانی شود.	ضرورت عزم حاکمیتی، ایجاد ساختار قانونی برای ممانعت از سوءاستفاده از داده‌های شهروندان و جلوگیری از رانت، تأمین نظارت از سوی بخش خصوصی، سرمایه‌گذاری در زیرساخت‌ها	عزم حاکمیتی، اعتمادسازی در مردم، تدوین موانع قانونی برای ممانعت از سوءاستفاده از داده‌های شهروندان و جلوگیری از رانت، تقویت شرکت‌های خصوصی صاحب فناوری داخلی، سرمایه‌گذاری در زیرساخت‌ها
۷	IN-SP-	لازم است، بررسی شود؛ چنین سامانه‌ای در کشور، در اختیار کدام نهاد و یا سازمان قرار	تصمیم‌گیری در خصوص نهاد مدیریتی نظارت‌کننده، ممانعت از سوءاستفاده	عزم حاکمیتی، پیش‌بینی ممانعت از سوءاستفاده

		خواهد گرفت. در صورت بروز سودجویی، جلب دوباره اعتماد مردم، بسیار سخت خواهد بود.	07	
لزوم ایجاد عزم سیاسی حاکمیتی	نبود اراده سیاسی میان حاکمان	بیش از نیازهای تکنولوژیک و علمی، نیاز به اراده سیاسی در میان افراد رأس قدرت است.	IN-SP-08	۸
نبود جهت گیری های جناحی در مدیریت نظارت دیجیتال و بهره گیری از نگاه تخصصی غیر جناحی	اجتناب مدیران ارشد از نگرش های جناحی، سپردن مدیریت نظارت دیجیتال به افراد متخصص و غیر جناحی	مدیران ارشد در حوزه دیجیتال، باید از رویکرد حزبی دوری کنند. افراد متخصص، فارغ از جهت گیری سیاسی آن ها به کارگرفته شوند. افراد با سواد علمی و تکنیکی، به کار گرفته شوند و رانت در این حوزه حذف شوند.	IN-SP-09	۹
نیاز به سرمایه گذاری در زیرساخت ها، آموزش مردم و نیز فرهنگ سازی در جامعه	ضعف در زیرساخت ها، لزوم آموزش مردم و نیز فرهنگ سازی	زیرساخت ها و امکانات کشور ضعیف هستند و با وضعیت فعلی، نمی توان امید داشت که توانایی های نظارتی دولت، به نحو قابل توجهی بازده داشته باشند. به کارگیری فناوری های نظارتی در کشور، نیازمند آموزش به مردم است. مردم در جامعه نیاز دارند تا ضرورت تقویت نظارت دولتی را درک کنند.	IN-SP-10	۱۰
اعتماد سازی در مردم، تقویت شرکت های خصوصی صاحب فناوری داخلی، اتخاذ نگاه غیر انحصاری، تدوین سند جامع در این حوزه	اعتماد سازی در مردم، توجه به شرکت های دانش بنیان، اتخاذ رویکرد ضد انحصار، تدوین سند جامع در این حوزه	صداقت با مردم؛ سرمایه گذاری در شرکت های دانش بنیان؛ اتخاذ رویکرد ضد انحصار؛ تدوین سند جامع در حوزه نحوه برخورد و مدیریت با فناوری های دیجیتال	IN-F-01	۱۱
لزوم آموزش مردم، آسیب شناسی فناوری های دیجیتال و آگاه کردن مردم از آن، سرمایه گذاری در زیرساخت ها	لزوم آموزش شهروندان در حوزه فناوری های دیجیتال، آسیب شناسی توسعه فناوری های دیجیتال، آگاه کردن مردم از تأثیرات فناوری دیجیتال، بهبود زیرساخت ها	آموزش به شهروندان، به اندازه لازم، برای استفاده از امکانات جدید، آسیب شناسی تهدیدات رشد و توسعه فناوری های دیجیتال. همچنین بهبود زیرساخت ها، برای استفاده از فناوری های جدید	IN-F-02	۱۲
سرمایه گذاری در زیرساخت ها، میدان دادن به دانشگاه، رفع مسأله تحریم، فرهنگ سازی برای اطمینان جامعه	مشکلات اصلی در تامین بودجه، ضعف علمی و مسائل فرهنگی هستند. نیاز به سرمایه گذاری در زیرساخت ها، تقویت نقش دانشگاه ها، دعوت از متخصصان بین المللی، رفع مسأله تحریم ها، اطمینان دادن به گروه های مخالف (کار فرهنگی)	سه مشکل عمده ایران، کمبود بودجه، ضعف علمی و مشکلات فرهنگی است. در کنار هزینه برای زیرساخت ها، باید سرمایه گذاری علمی قابل توجهی در عرصه فناوری های دیجیتال نیز صورت گیرد. مطالب درسی در دانشگاه ها، باید مطابق با دانش روز باشد. از متخصصان و استادان خارج از کشور نیز دعوت به همکاری شود. واردات دانش جدید از خارج کشور، اهمیت زیادی در پیشرفت در حوزه فناوری های دیجیتال دارد. این موارد، همگی نیازمند رفع تحریم ها هستند. به گروه های فرهنگی در ایران اطمینان داده شود، نگرانی های آن ها مورد توجه خواهند بود.	IN-F-03	۱۳
ضرورت شناخت فناوری های دیجیتال از سوی دولت، میدان دادن به دانشگاه، ایجاد ساختار قانونی لازم	لزوم شناخت فناوری های نو، انجام مطالعات هدفمند دانشگاهی، فناوری باید در زندگی عموم مردم نمود پیدا کند. ایجاد ساختاری قانونی مناسب	دولت ایران نیاز دارد، ابتدا فناوری جدید را بشناسد؛ مطالعه و پژوهش دانشگاهی در حوزه فناوری های دیجیتال. گمان می کنیم، فناوری ها هر طور ما بخواهیم، صورت بندی می شوند و به هر جا بخواهیم، می روند؛ اما علم و تکنولوژی در اختیار آمال و امیال ما نیست. نیاز داریم، ابزارهایی توسعه بدهیم که توده زیادی از مردم از آن استفاده کنند و از خدمات آن بهره مند شوند. نیازمند ایجاد روال ها و قانون ها در جهت کنترل و تنظیم تکنولوژی هستیم.	IN-B-01	۱۴

<p>اتخاذ رویکرد حکمی، حل مساله تحریم، نوسازی زیرساخت‌ها، ایجاد ساختارهای قانونی، آموزش مردم</p>	<p>ایجاد حس نیاز میان مسئولان کشور، حل مسئله تحریم‌ها به منظور ارتباط با قطب‌های تکنولوژیک، نوسازی زیرساخت‌ها، تدوین ساختارهای قانونی، به منظور رفع نگرانی شهروندان، لزوم استفاده از ظرفیت شرکت‌های خصوصی، آموزش مردم با هدف صحیح، از قابلیت‌های فناوری‌های دیجیتال و رفع نگرانی‌های ایشان</p>	<p>مهم‌ترین مسئله، ایجاد حس ضرورت در میان مسئولان رده‌بالا در کشور است. هم‌اکنون به علت تحریم، دانش و تکنولوژی‌های جدید، به کندی وارد کشور می‌شود. زیرساخت‌ها در کشور باید نوسازی شوند و این امر، مستلزم برقراری روابط با کشورهای صاحب تکنولوژی در شرق و غرب است. قانون جامعی در حوزه توان نظارتی دولت وضع شود تا حد و حدود اختیارات دولت در این حوزه، مشخص شود. نگرانی و بی‌اعتمادی مردم، به دلیل نبود ساختارهای قانونی در کشور است. برای پیشرفت در حوزه فناوری‌های دیجیتال، لازم است؛ دولت به شرکت‌های خصوصی میدان دهد. لازم است، مردم در جامعه برای استفاده صحیح از فناوری‌های دیجیتال، آموزش داده شوند.</p>	<p>IN-B-02</p>	<p>۱۵</p>
---	--	---	----------------	-----------

*پرسش چهارم: آینده رشد و توسعه فناوری دیجیتال و رابطه آن با قدرت دولت، در حوزه توان

نظارتی بر شهروندان را چگونه ارزیابی می‌کنید؟

جدول ۵- پاسخ مصاحبه‌شوندگان به پرسش چهارم

کد گذاری گزینشی	کد گذاری محوری	کد گذاری باز	کد مصاحبه شونده	ردیف
<p>افزایش روزافزون موفقیت دولت در نظارت هوشمند بر افراد، با استفاده از فناوری دیجیتال. احتمال بهره‌گیری از علوم شناختی</p>	<p>- اتکای فزاینده دولت به کلان داده‌ها و هوش مصنوعی - موفقیت سریع دولت در گسترش نظارت هوشمند بر رفتار شهروندان</p>	<p>سامانه‌های نظارتی حوزه فناوری دیجیتال، متکی به تحلیل کلان داده و هوش مصنوعی هستند و این دو توان نظارتی دولت را به کلی متحول کرده‌اند. استفاده از علوم شناختی در نظارت و کنترل افراد نیز ضروری است.</p>	<p>IN-SP-01</p>	<p>۱</p>
<p>افزایش توان نظارتی دولت بر شهروندان و مدیریت بهتر امور و خدمات اجتماعی، به علت افزایش به کارگیری فناوری دیجیتال</p>	<p>-رابطه رشد و توسعه فناوری دیجیتال، با افزایش توان نظارتی دولت‌ها -استفاده از داده‌های شهروندان، برای ارائه خدمات عمومی و اجتماعی بهتر با اهداف متفاوت</p>	<p>تداوم رشد و توسعه فناوری‌های دیجیتال در آینده، موجب افزایش توان نظارتی دولت‌ها بر شهروندان خواهد شد. دولت در صدد استفاد از این فناوری‌ها برای کسب اطلاعات در خصوص شهروندان، برای مدیریت بهتر امور عمومی و ارائه خدمات اجتماعی استفاده کند.</p>	<p>IN-SP-02</p>	<p>۲</p>
<p>نبود رابطه مستقیم بین استفاده از فناوری دیجیتال و افزایش قدرت نظارتی دولت؛ مثلا رمز ارزها</p>	<p>-نبود رابطه مستقیم میان رشد و توسعه فناوری دیجیتال و قدرت نظارتی دولت‌ها. رمز ارزها، نمونه‌ای از کاهش قدرت نظارتی دولت با افزایش فناوری‌های دیجیتال است.</p>	<p>نمی‌توان رابطه مستقیمی میان رشد و توسعه فناوری دیجیتال و قدرت نظارت دولت تعریف کرد. امکان دارد، رشد و توسعه فناوری دیجیتال، تأثیر منفی بر قدرت نظارتی دولت داشته باشد. فراگیری رمز ارزها، نمونه‌ای واضح از کاهش توان نظارتی دولت است.</p>	<p>IN-SP-03</p>	<p>۳</p>

۴	IN-SP-04	دولت، با افزایش توان نظارتی خود می‌تواند درک بهتری از نیازهای مردم داشته باشد.	-افزایش توان نظارتی دولت، عملکرد دولت را بهبود می‌بخشد.	بهبود عملکرد دولت، با افزایش توان نظارتی آن در قبال نیازهای مردم
۵	IN-SP-05	دولت و بخش بروکراتیک آن، با هوش مصنوعی و داده‌های آن تقویت می‌شود. هوش مصنوعی، توان بسیاری به توان نظارتی دولت می‌بخشد.	هوش مصنوعی، سبب تقویت بروکراسی دولت و افزایش توان نظارتی آن خواهد شد.	تأثیر مثبت هوش مصنوعی، بر توان نظارتی و بروکراتیک دولت
۶	IN-SP-06	به دو عامل اصلی بستگی دارد: اول قوانین کشور و ذهنیت مردم کشور. در چین، جمع‌آوری داده در سطح بسیار بالایی اتفاق می‌افتد؛ اما حساسیت مردم نسبت به این امر اندک است. در آمریکا، جمع‌آوری داده در سطح بالا وجود دارد؛ اما حساسیت مردم نسبت به این امر بسیار شدیدتر است.	قانون اساسی کشور، بر بعد نظارت تأثیر دارد. حساسیت مردم بر بعد نظارت تأثیر دارد.	موقعیت دولت در نظارت دیجیتال، به دو عامل قانون‌گذاری و حساسیت مردم بستگی دارد.
۷	IN-SP-07	رشد و توسعه توان نظارتی دولت، تاجایی ادامه خواهد داشت که کنترل کامل دولت را بر شهروندان اعمال کند. افزایش توان نظارتی دولت، اراده انسان را از او سلب خواهد کرد.	افزایش توان نظارتی دولت، سلب اراده افراد	افزایش توان نظارتی دولت تا حد نظارت کامل و سلب اراده انسان
۸	IN-SP-08	رشد و توسعه جهانی برای مدتی طولانی وجود داشته است و کشورهای توسعه‌یافته، همچنان به دنبال افزایش توان خود در عرصه فناوری‌های دیجیتال هستند. پیشرفت، با سرعت بالا در سطح جهانی در حال رخ دادن است.	رشد و توسعه، با سرعت بالایی در حال حاضر وجود دارد.	سرعت بالای دولت‌ها، در به-کارگیری فناوری دیجیتال
۹	IN-SP-09	در آینده، این حوزه به دلیل پیشرفت هوش مصنوعی، بسیار توانمند خواهد شد. هوش مصنوعی می‌تواند در حوزه نظارتی، مانع جرم و جنایت شود. هوش مصنوعی، به‌طور خاص در حوزه کلان‌داده، توان نظارتی دولت‌ها را به‌طور قابل ملاحظه‌ای افزایش می‌دهد.	تأثیر مثبت هوش مصنوعی در حوزه کلان‌داده‌ها، بر توان نظارتی دولت‌ها و جلوگیری از جرم و جنایت	افزایش قابل ملاحظه توان نظارتی دولت با بهره‌گیری از هوش مصنوعی
۱۰	IN-SP-10	رشد و توسعه فناوری، در هر کجا که باشد، همراه با موجی از موافقت‌ها و مخالفت‌ها است. فناوری‌های دیجیتال، به دلیل جهان‌شمولی بودن، در هر کجا که وارد شوند، توسعه پیدا می‌کنند. به-کارگیری فناوری‌های دیجیتال در حوزه نظارت، امری طبیعی است. امکان دارد، حریم خصوصی افراد مورد دست‌درازی قرار گیرد. شاید با	فناوری‌های دیجیتال، جهان‌شمول و عامل توسعه‌اند. به-کارگیری فناوری‌های دیجیتال در حوزه نظارت، امری طبیعی است. نظارت دولتی، افزون بر تسهیل کارهای دولت، می‌تواند حریم خصوصی را به‌خطر اندازد؛ لذا نیاز به وضع قوانین است.	به‌کارگیری فناوری دیجیتال، در نظارت دولت امری طبیعی است و سبب توسعه نظارت می‌گردد؛ اما ممکن است، حریم خصوصی را تقض کند؛ لذا نیاز به وضع قوانین است.

		وضع قوانین، بتوان جلوی برخی مشکلات را گرفت.		
افزایش نفوذ شرکت‌های خصوصی صاحب تکنولوژی در حوزه نظارت، تأثیر مثبت و منفی فناوری‌های دیجیتال در حوزه نظارت	سلطه شرکت‌های صاحب فناوری بر عرصه نظارت و وابستگی دولت‌ها به بخشی از این داده‌ها، داده‌های جمع - آوری شده، مصرف دوگانه دارند؛ هم در عرصه امنیتی هم در عرصه بهبود خدمات‌رسانی	در کشورهای غربی، تعداد دوربین‌های مداربسته را افزایش داده و الگوریتم‌های پیشرفته‌تری برای جمع‌آوری داده، ابداع می‌کنند. دولت‌ها ناگزیرند تا بخشی از داده‌ها را از شرکت‌های خصوصی صاحب تکنولوژی تهیه کنند. این داده‌ها، در حال حاضر جمع‌آوری شده و مورد استفاده قرار می‌گیرد؛ هم برای مصارف امنیتی و هم برای مصارف غیرامنیتی مانند ارزیابی‌های اقتصادی و اجتماعی.	IN-F-01	۱۱
به‌کارگیری فناوری دیجیتال از سوی دولت، اجتناب‌ناپذیر است. تأثیرگذاری مثبت و منفی فناوری‌های دیجیتال در حوزه نظارت	توسعه اجتناب‌ناپذیر فناوری‌های دیجیتال، به نفع مردم و جامعه است؛ اما در عین حال، نتایج منفی مانند رمز ارزها را در پی دارد.	پیشرفت و توسعه فناوری دیجیتال، اجتناب‌ناپذیر است. ادعا همیشه این بوده است که پیشرفت فناوری‌های دیجیتال، به نفع مردم و جامعه است. پیشرفت فناوری دیجیتال، به‌همراه خود چالش‌های بسیاری نیز به وجود آورده است. برای مثال؛ رمز ارزها امروزه بیشتر در دارک وب و فعالیت‌های غیرقانونی مصرف می‌شوند.	IN-F-02	۱۲
فناوری دیجیتال، سبب تقویت نظارت دولت‌ها می‌شود. دولت‌ها، بروز مخالفت‌ها را با ایجاد دوگانگی امنیتی یا آزادی توجیه می‌کنند.	هوش مصنوعی، سبب تقویت نظارت شده است. دولت‌ها در موارد بروز چالش، با ایجاد دوگانگی امنیتی یا آزادی، نظارت را توجیه می‌کنند.	هوش مصنوعی، کمک بسیاری به تقویت توان نظارتی دولت‌ها کرده است. نظارت بر شهروندان، امری جهانی است؛ اما در صورت بروز مخالفت، دولت‌ها از طریق دوگانگی، امنیتی یا آزادی را برای شهروندان توجیه می‌کنند. تمامی دولت‌ها، سطحی از نظارت را بر شهروندان خود اعمال می‌کنند.	IN-F-03	۱۳
افزایش توان نظارتی دولت و نیز احتمال این که فناوری در برنامه - ریزی و مدیریت و ایجاد تغییر، رقیب دولت بشود.	فناوری‌ها، سبب تقویت توان نظارتی دولت می‌شود. در عین حال ممکن است، به‌عنوان رقیب دولت در برنامه - ریزی، مدیریت و تغییر عمل کند.	تکنولوژی، ابزاری است در دست دولت و به او می‌تواند کمک کند. جزیی‌ترین رفتار شهروندان را نظارت کند، تکنولوژی‌های جدید را می‌توان به‌عنوان نهادی در عرض دولت در نظر گرفت که قدرت تغییر، برنامه‌ریزی و مقابله دارد.	IN-B-01	۱۴
تأثیر مثبت هوش مصنوعی و کلان‌داده‌ها بر افزایش توان نظارتی دولت‌ها، لزوم قوانین تنظیم‌کننده حوزه و توان نظارتی دولت‌ها	هوش مصنوعی و کلان داده‌ها، توان دولت برای نظارت شهروندان را تقویت کرده است. همچنین با توجه به احتمال نظارت دولت‌ها بر تمام زندگی افراد، تدوین قوانین در این زمینه ضروری است.	فناوری‌های دیجیتال، با سرعت بی‌سابقه‌ای در عرصه نظارت، در حال پیشرفت هستند. کلان‌داده و هوش مصنوعی، توان نظارتی دولت‌ها را متحول کرده‌اند. به‌زودی شاهد وضعیتی خواهیم بود که تمامی امور زندگی انسان تحت نظارت دولت‌ها قرار خواهد داشت.	IN-B-02	۱۵

		<p>نکته مهم در این میان، اعمال قوانینی است که مطابق آن، دولت با کدام بخش از داده‌هایی که در دست دارد، بتواند شهروندان را تحت تعقیب قرار دهد.</p>
--	--	--

مفاهیم کلی و جزئی برگرفته از نظرات مصاحبه شونده‌گان

جدول ۶- جدول مفهومی براساس نظرات مصاحبه شونده‌گان

مفاهیم کلی	مفاهیم جزئی	کدهای محور
وضعیت مطلوب در کنار تحریم و امنیتی شدن	۱. وضع مطلوب نظارت دولت	۱. وضع قابل قبول بهره‌گیری دولت از فناوری دیجیتال برای نظارت بر مردم
	۱. تبعات تحریم ۲. تمرکز بر وجه امنیتی نظارت	۱. تبعات ناشی از تحریم‌ها ۲. وابستگی به سرورهای خارجی ۳. نبود زیرساخت و کمبود بودجه ۴. تمرکز بر وجه امنیتی نظارت و غفلت از سایر ابعاد ۵. تعارض در به‌کارگیری فناوری دیجیتال با امر فیلترینگ ۶. تعارض در رویکرد دولت‌های مختلف
تحریم، ضعف فنی و چالش‌های علمی و فرهنگی	بیرونی؛ ۱. تحریم‌ها و تبعات آن ۲. تنش در روابط خارجی	۱. مسئله تحریم‌ها و تبعات آن (وارد نشدن دانش روز، فساد و رانت) ۲. تنش در روابط خارجی ۳. کاهش بودجه برای سرمایه‌گذاری در زیرساخت‌ها
	داخلی؛ ۱. تناقض مواضع دولت با جامع ۲. بی‌اعتمادی جامعه به فناوری- های نو ۳. ضعف علمی داخلی ۴. تهدیدات امنیتی ۵. موانع فرهنگی	۱. تناقض مواضع دولت‌ها در فیلترینگ با تلاش برای افزایش نظارت دیجیتال ۲. غلبه نگاه سنتی بر بخشی از مسئولان و نیز مردم ۳. بی‌اعتمادی مردم به فناوری‌های نو و نیز پلتفرم‌های داخلی ۴. ضعف علمی دانشگاه‌ها ۵. امکان تهدیدات امنیتی ۶. نگرانی‌های فرهنگی و مذهبی در جامعه
توان داخلی و فرهنگ سازی رفع تحریم، بهره‌گیری از	بیرونی؛ ۱. مسئله تحریم ۲. تنش در روابط خارجی	۱. تلاش برای حل مسئله تحریم ۲. تنش‌زدایی در روابط خارجی ۳. تسهیل امکان سرمایه‌گذاری در زیرساخت‌ها
	داخلی؛ ۱. تحول نگرش حاکمیت به فناوری ۲. حمایت از افراد و شرکت‌های فناور داخلی ۳. تدوین قانون جامع ۴. تسهیل حضور مردم در فضای مجازی ۵. فرهنگ‌سازی ۶. ایمن‌سازی زیرساخت‌ها در برابر حملات	۱. تغییر نگاه حاکمیت به فناوری ۲. عزم حاکمیت و ضرورت یکدستی در تصمیمات حاکمیتی ۳. اتخاذ نگاه غیرانحصاری و حمایت از شرکت‌های فناور داخلی ۴. به‌کارگیری نیروهای متخصص غیرچنانچی ۵. تدوین قانون و سند جامع در این حوزه ۶. ایجاد اعتماد بین مردم، نسبت به عملکرد دولت و نیز فناوری‌های دیجیتال ۷. تسهیل حضور مردم در فضای مجازی آموزش مردم ۸. تأمین امنیت فناوری برای جلوگیری از حملات

<p>امیدبخشی‌ها</p> <p>۱. دولت، در آینده با به‌کارگیری فناوری دیجیتال و البته علوم شناختی، شاهد افزایش توان نظارتی بر شهروندان و نیز ارتقای مدیریت امور اجتماعی خواهد بود.</p> <p>۲. همراهی و اعتماد جامعه</p> <p>۳. دغدغه‌ها؛</p> <p>۴. احتمال سلب اراده از افراد</p> <p>۵. تهدید حریم خصوصی افراد</p> <p>۶. نبود ساختار قانونی برای ممانعت از سوءاستفاده</p> <p>۷. احتمال افزایش نفوذ شرکت‌های فناوری در برابر دولت؛ مثلا در حوزه رمز ارزها</p>	<p>۱. گسترش روزافزون توان نظارتی دولت</p> <p>۲. احتمال سلب حریم خصوصی افراد</p> <p>۳. احتمال سوءاستفاده از داده‌ها</p> <p>۴. احتمال قدرت‌نمایی شرکت‌های فناوری در برابر دولت</p>	<p>نظارت بر شهروندان</p>
--	--	--------------------------

نتیجه گیری

بر اساس جدول مفهومی شماره (۶)، از کل داده‌های مصاحبه شوندگان، ۲۹ مقوله به دست آمد. این مقوله‌ها، در فرآیند انتزاع نهایی، ذیل چهار مفهوم کلی دسته‌بندی شدند (ستون اول از راست)؛ هریک از این مفاهیم کلی، بیانگر تأثیرات مثبت و منفی فناوری دیجیتال، بر عملکرد نظارتی دولت است که در چهار وضعیت، به شرح ذیل دسته‌بندی می‌شوند.

۱- توصیف وضعیت موجود

۲- چالش‌ها

۳- تمهیدات و الزامات

۴- چشم‌انداز

در ادامه به توصیف هریک از این وضعیت‌ها، بر اساس پاسخ‌های مصاحبه شوندگان می‌پردازیم.

۱- وضعیت موجود: در این بخش، برآیند داده‌ها، از نگاه مصاحبه‌شوندگان، بیانگر تأثیر مطلوب فناوری بر عملکرد نظارت دولت و وضعیت قابل قبول تحول در آن است. در عین حال، از نگاه مصاحبه شوندگان، وضعیت موجود تحت تأثیر دو عامل مهم؛ یعنی تحریم‌ها به لحاظ بیرونی و امنیتی شدن نظارت دولت به لحاظ داخلی قرار دارد.

در توصیف این یافته‌ها می‌توان افزود؛ از نگاه نخبگان، با وجود ارزیابی مطلوب وضعیت کنونی، توقف در این مرحله، پاسخ‌گوی نیازهای آینده کشور نیست و ضرورت دارد، بسترهای پیشرفت بیش از پیش تسهیل گردد. از نگاه نخبگان مصاحبه شونده، تصمیم‌گیران کشور بدون توجه به دو چالش تحریم و امنیتی شدن نظارت و ضرورت تلاش برای رفع آن‌ها قادر نخواهند بود، عملکرد

نظارتی دولت را به وضعیت ایده آل برسانند؛ لذا از نگاه راهبردی، اولویت نخست، از یک سو رفع تحریم بیرونی و از سوی دیگر، اتخاذ نگرشی جامع؛ نه صرفاً امنیتی، به مسئله نظارت به لحاظ درونی است.

۲- چالش‌ها؛ برآیند پاسخ مصاحبه شوندگان در بخش دوم؛ یعنی چالش‌های پیش روی دیجیتال شدن نظارت دولت بر شهروندان، در بردارنده چهار نوع چالش عمده است: اول؛ ضعف فنی ناشی از وابستگی به فناوری دیجیتال، از نظر بیرونی که البته ریشه در تحریم‌ها دارد. دوم؛ چالش‌های سیاسی؛ شامل تناقض مواضع دولت‌ها در این خصوص با یکدیگر و نیز با جامعه. سوم؛ چالش فرهنگی؛ شامل بی‌اعتمادی مردم به فناوری‌های نو و چهارم؛ چالش علمی، یعنی ضعف دانش بومی است.

توصیف این بخش از یافته‌ها از نگاه نخبگان، بیانگر این است که نبود عزم جدی برای رفع تحریم‌ها در این حوزه، منجر به تداوم وابستگی به فناوری دیجیتال در حوزه نظارت و لذا استمرار ضعف فنی دولت در این حوزه خواهد بود. بدیهی است، چنین وضعیتی پیامدهای اعلام نشده بعدی را در همین حوزه در پی خواهد داشت. از سویی، آنچه در بالا در خصوص چالش داخلی اشاره شد، در این بخش به خوبی تبیین شده است. از نگاه نخبگان ضروری است، دولت‌ها به منظور دستیابی به گفتمان و درکی یکسان در این حوزه، اقدامات عاجلی را صورت دهند. رفع بدفهمی‌ها و تناقضات، اتخاذ نگاه جامع در حوزه نظارت دیجیتال، نزدیک‌تر ساختن ادراک خود به فهم و انتظارات جامعه، به حداقل رساندن موانع فرهنگی و رفع بی‌اعتمادی مردم به فناوری‌های نو و توجه جدی و برنامه‌ریزی برای فعال ساختن نهادهای علمی داخلی. رفع این چالش‌ها و نگرانی‌ها، از نگاه مصاحبه شوندگان غیرقابل اغماض است. نخبگان مصاحبه شونده، ضمن آسیب‌شناختی این حوزه، بر ضرورت رفع سریع این چالش‌ها نیز تأکید دارند.

۳- تمهیدات و الزامات: از نگاه مصاحبه شوندگان، مهم‌ترین الزام در حل چالش‌های ذکر شده، رفع تحریم‌ها و نیز توسعه روابط خارجی است. بهره‌گیری از توان داخلی؛ شامل حمایت از افراد و شرکت‌های فناوری و نیز فرهنگ‌سازی؛ شامل آموزش مردم و رفع نگرانی‌های امنیتی و دغدغه‌های مذهبی جامعه، اولویت‌های بعدی در بخش داخلی است. در بخش مبانی نظری، با مقوله‌هایی؛

همچون دیجیتالی شدن، شبکه‌ای شدن، اطمینان بخشی امنیت فضای دیجیتالی و مغایرت نداشتن آن با باورهای مذهبی اشاره شد؛ اولویت‌هایی که می‌بایست، برای رفع نگرانی از آن‌ها برنامه‌ریزی صورت گیرد.

تفسیر این بخش از پاسخ‌ها، بیانگر راهکارهای عملیاتی است. از نگاه نخبگان، تلاش برای توسعه روابط خارجی به شکل جامع و بدون نگاه مضیق، اصلی‌ترین اولویت عملیاتی در حل مسئله تحریم است. بدیهی است؛ در این فرایند، توسعه مناسبات با کشورهای برخوردار، از چنین فناوری‌هایی فوریت دارد. از سویی، گام‌های عملیاتی در داخل نیز مجموعه‌ای از اقدامات و برنامه‌های حمایتی را شامل می‌شود؛ نظیر حمایت از ظرفیت داخلی، افراد و شرکت‌های فناور این حوزه و برنامه‌ریزی برای فرهنگ‌سازی و آموزش مردم. در بین پاسخ‌ها، به‌ویژه تأکید و توجه نخبگان به دغدغه‌های مذهبی مردم، قابل توجه است که مستلزم برنامه‌ریزی هوشمندانه و تدریجی است.

۴- چشم‌انداز: برآیند پاسخ مصاحبه شونده‌گان در این بخش، برگرفته از وضعیت موجود (شماره ۱) است. در نگاه ایشان، مهم‌ترین چشم‌انداز پیش رو در این بخش، گسترش کمی و ارتقای کیفی نظارت دیجیتالی دولت بر شهروندان است؛ اما در عین حال، همین چشم‌انداز با دغدغه‌هایی همراه است. مصاحبه شونده‌گان درباره‌ی بروز مواردی؛ همچون تهدید حریم خصوصی افراد، احتمال سوءاستفاده از داده‌های شهروندان و نیز احتمال تبدیل شدن شرکت‌های صاحب فناوری داخلی به رقیبانی برای دولت هشدار داده‌اند.

به نظر می‌رسد، نخبگان مصاحبه شونده، ضمن ترسیم تصویری روشن و امیدبخش از این فرایند، در خصوص آینده‌ی نظارت دیجیتالی دولت، بر دو ملاحظه کمی و کیفی تأکید دارند. در آینده‌ی نظارت دیجیتالی، هم به لحاظ گستره و هم به لحاظ کیفیت و عمق، گسترش خواهد یافت. این یعنی حرکت به سمت تحقق کامل نظارت دیجیتالی در ایران. بدیهی است، سایر بخش‌های جامعه هم خود را برای همراهی با این فرایند آماده کنند؛ اما در این فرایند، تهدید و تحدید حریم خصوصی شهروندان، دغدغه‌ای جدی است که باید در برنامه‌های سیاستی مسئولان لحاظ شود. در بخش مبانی نظری اشاره شد که تحقق نظارت کامل، دست دولت را برای محدود کردن و مقابله دیجیتالی با مخالفان نیز بازمی‌گذارد.

چالش جدی دیگر در این میان، شکل‌گیری رقبای جدید در این حوزه برای دولت؛ یعنی شرکت‌های فناوری است که در بخش مبانی نظری، به برخی مصادیق آن اشاره شد. این چالش، در نگاه نخبگان به این معناست که از این پس، در حوزه نظارت دیجیتال، دولت تنها بازیگر نخواهد بود و بازیگری آن نیز با ملاحظه حضور دیگر رقبیان، معنا خواهد یافت. با توجه به یافته‌های پژوهش، به نظر می‌رسد دولت جمهوری اسلامی ناگزیر است، خود را هم برای مواجهه با وضعیت نوین و هم هم‌زیستی در چنین زیست‌بومی مهیا سازد.

پیشنهادها

براساس آنچه از داده‌های پژوهش به دست آمد، بهره‌گیری از فناوری دیجیتال برای نظارت دولت بر شهروندان در ایران، تاکنون تأثیری قابل قبول داشته است و البته چشم‌انداز بهتری نیز از نظر دایرة شمول و کیفیت نظارت در پیش روی دارد. اشاره شد که دولت جمهوری اسلامی، برای تحقق اهداف خود در این حوزه ضروری است، تدابیری راهبردی اجرا کند. برای این منظور، پیشنهادهایی برگرفته از همین یافته‌ها، به ترتیب اولویت ارائه می‌شود:

- تلاش دولت برای رفع تحریم‌ها و به حداقل رساندن آثار و تبعات آن، به منظور تسهیل دسترسی به فناوری و دانش روز در این حوزه (به‌ویژه هوش مصنوعی و علوم شناختی).

- تلاش برای توسعه مناسبات با کشورهایی که در این حوزه از ظرفیت حمایت و تقویت دولت ایران برخوردارند.

- شکل‌گیری عزم جدی حاکمیتی در این حوزه، به دور از تأثیرپذیری دولت‌ها و نیز جهت‌گیری‌های سیاسی

- سرمایه‌گذاری و تقویت زیرساخت‌های لازم

- شناسایی افراد و شرکت‌های فناور و تدوین برنامه‌های حمایتی از ایشان، توأم با بهره‌گیری از توان دانشگاه‌های داخلی

- تدوین ساختار قانونی جامع، به‌مثابه بستری تسهیل‌گر و هم‌زمان ممانعت‌کننده از سوءاستفاده‌های احتمالی

- تلاش برای اصلاح نگرش منفی مسئولان به فناوری‌های نو
- فرهنگ‌سازی و آموزش عمومی مردم با هدف رفع نگرانی‌های امنیتی و مذهبی

منابع و مآخذ

- خبرگزاری جمهوری اسلامی (۱۳۹۷). جرایم سایبری در کشور ۹۰۰ درصد افزایش یافت. [/https://www.ima.ir/news/82900640](https://www.ima.ir/news/82900640) از ۱۴۰۰ دی ۱
- خبرگزاری تجارت نیوز (۱۳۹۹). چرا تلگرام فیلتر شد؟ [/https://tejaratnews.com/startup](https://tejaratnews.com/startup) از ۱۴۰۰ ماه ۱ دی
- بی‌بی‌سی فارسی فارسی (۱۳۹۲) درخواست دولت‌ها از فیس‌بوک، درباره اطلاعات ده‌ها هزار کاربر، https://www.bbc.com/persian/world/2013/08/130827_u08_facebook_user_data از ۱۳۹۲ شهریور ۶
- شبستین، ویکتور (۱۴۰۰). انقلاب‌های ۱۹۸۹، سقوط امپراتوری شوروی در اروپا. ترجمه بیژن اشتري. تهران: نشر ثالث.
- صفری، حسین؛ غلامرضا خوش‌سیما؛ ایوب محمدیان؛ عادل مصلحی؛ محمدکاظم حاکی، عماد فرازمنند و علیرضا تمیزی (۱۳۸۲).
- مدل بلوغ دولت الکترونیک. وزارت بازرگانی ایران. ماهنامه دانش مدیریت، شماره ۶۳، ۵۳-۷۸.
- عجم اوغلو، دارون و جیمز رایبسون (۱۳۹۳). چرا ملت‌ها شکست می‌خورند؟ ترجمه محسن میردامادی و محمدحسین نعیمی‌پور. تهران: نشر روزنه.
- فرانکوین، پیت (۱۳۹۹). راه‌های ایریشم، تاریخ جهان از دیدگاهی نو. ترجمه: حسین افشار، تهران: نشر مرکز.
- کیسنجر، هنری، اریک اشمیت و دانیل هوتنلوچر (۲۰۱۴). عصر هوش مصنوعی و آینده ما انسان‌ها. تهران: بنگاه ترجمه و نشر کتاب پارسه.
- ماجرای فیلترینگ سیگنال در ایران چیست؟ (۱۳۹۹) وب سایت باشگاه خبرنگاران جوان. بازیابی در ۸ آبان ۱۴۰۰ <https://www.yjc.news/fa/news/7643585>
- محمدپور، احمد. (۱۳۸۹). ضد روش: زمینه‌های فلسفی و رویه‌های عملی در روش‌شناسی کیفی. قم: نشر لوگوس.

معمارزاده طهران، غلامرضا؛ محمد مبینی و مهدی ققیهی (۱۳۹۷). دولت الکترونیک. تهران: نشر اندیشه‌های گوهربار.

تلگرام اطلاعات کاربران ایرانی را به آمریکا و اسرائیل فروخت (۱۳۹۶). وب سایت خبرگزاری تابناک. بازبایی در ۸ آبان ۱۴۰۰ از <http://www.tabnak Yazd.ir/fa/news/559546/>

References

- Ajamoglu, Daron and James Robinson (2013). Why nations fail? Translated by Mohsen Mirdamadi and Mohammad Hossein Naimipour. Tehran; Rozaneh publications. (In Persian)
- Andrews, Evan. (2019). Who Were the Luddites? HISTORY. Retrieved 2021, Jan 5, from <https://www.history.com/news/who-were-the-luddites>
- BBC Persian (2012). governments request from Facebook about the information of tens of thousands of users, Retrieved on September 6, 2012, from https://www.bbc.com/persian/world/2013/08/130827_u08_facebook_user_data
- Bellaby, Ross. (2012, February). What's The Harm? The Ethics of Intelligence Collection. *Intelligence and National Security*, 27(1), 93-177.
- Chin, Josh & Lin, Liza. (2017). China's All-Seeing Surveillance State Is Reading Its Citizens' Faces. *The Wall Street Journal*. Retrieved 2020, August 14 From https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020?mod=article_re
- Castells, Manuel (2009). *Communication Power*. Oxford University Press.
- Delfanti, Alessandro and Adam Arvidsson (2019). *Introduction to Digital Media*. John Wiley & Sons, Inc.
- Frankopen, Peter (2019). *Silk roads, world history from a new perspective*. Translated by Hossein Afshar, Tehran: Markaz Publishing. (In Persian)
- Haggerty, Kevin D & Samatas, Minas. (2010). *Surveillance and Democracy*. New York: Routledge.
- Holmes, Aaron. (2021). 533 million Facebook users' phone numbers and personal data have been leaked online. *Insider*, Retrieved 2021, Jan 22 From <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T>
- IRNA (2017). - Cyber-crimes in the country increased by 900%. Retrieved 22 December 2022, from Islamic Republic News Agency website. (In Persian)
- Kissinger, Henry, Eric Schmidt and Daniel Huttenlocher (2021). *The Age of AI and Our Human Future*. Tehran: Parse Book Publishing. (In Persian)
- Lennon, Hailey. (2021). The False Narrative of Bitcoin's Role in Illicit Activity. *Forbes*. Retrieved 2021, Jan 22 from <https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/>
- Mazzetti, Mark. Perloth, Nicole & Bergman, Ronen. (2019). It Seemed Like a Popular Chat App. It's Secretly a Spy Tool. *The New York Times*. Retrieved

- 2020, Aug 14 from <https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html>
- McIver, William J & Elmagarmid, Ahmed K. (2020). *ADVANCES IN DIGITAL GOVERNMENT Technology, Human Factors, and Policy*. Boston: KLUWER ACADEMIC PUBLISHERS.
- Memarzadeh Tehran, Gholamreza; Mohammad Mobini and Mehdi Faqih (2017). *E-government*. Tehran: Andishehay Goharbar Publications. (In Persian)
- Ransom, Harry Howe. (2014). *The Intelligence Establishment*. Cambridge: Harvard University Press.
- Safari, Hossein; Gholamreza Khosh Sima; Ayub Mohammadian; Adel Moslehi; Mohammad Kazem haki, Emad Farazmand and Alireza Tamizi (2012). *E-Government Maturity Model*. Ministry of Commerce of Iran. *Management Knowledge Monthly*, No. 63, 53-78. (In Persian)
- Mohammadpour, Ahmed (2015). *Anti-Method: Philosophical Backgrounds and Practical Procedures in Qualitative Methodology*. Qom: Logos Publishing. (In Persian)
- Schneier, Bruce. (2015). *Data and Goliath the Hidden Battles to Collect Your Data and Control Your World*. New York: Norton & Company.
- Schroeder, Ralph (2018). *Social Theory after the Internet Media, Technology and Globalization*. UCL press university college London.
- Sebestyen, Victor (2022). *The revolutions of 1989, the fall of the Soviet empire in Europe*. Translated by Bijan Ashtari. Tehran: Saless publication (In Persian)
- Simeon, J. Yates & Ronad, E. Rice. (2020). *The oxford Handbook of digital technology and Society*. New York: Oxford University Press.
- Snowden, Edward. (2019, september 17). *Edward Snowden On Trump, Privacy, And Threats to Democracy*. [Video File]. Retrieved 2021, 20 August from <https://www.youtube.com/watch?v=e9yK1QndJSM> .
- Tabnak news agency website (2016). *Telegram sold the information of Iranian users to America and Israel*. Retrieved on November 8, 2022 from <http://www.tabnak Yazd.ir/fa/news/559546/> (In Persian)
- Tejarat News Agency (2019). *Why was Telegram filtered?* Retrieved on 22 December 2022 <https://tejaratnews.com/startup/> . (In Persian)
- Thomsen, Frej.k, (2019, October). *The Concepts of Surveillance and sousveillance: a critical analysis*. *Social Science Information*, 53(4), 701-703.
- Van Dijck, José; Thomas Poel, and Martijn de Waal (2018). *The Platform Society; PUBLIC VALUES IN A CONNECTIVE WORLD*. Oxford University Press.
- Van loon, Joost (2008). *Media Technology; Critical Perspectives, issues in Cultural and Media Studies*. McGrow hill Open University press.
- Young Journalists Club website (2019). *What is the story of signal filtering in Iran?* Retrieved on November 8, from <https://www.yjc.news/fa/news//۷۶۴۳۵۸۵>. (In Persian)