تحلیلی بر تأثیرات متقابل ویروس کرونا و هویت دیجیتال

دکتر هاتف رسولی [1]

چکیده

در این مقاله به بررسی تأثیرات شیوع ویروس کرونا (Covid-19) بر هویت دیجیتال و راهکارهای مبتنی بر هویت دیجیتال جهت کاهش شیوع این ویروس پرداخته می‌شود. هویت دیجیتال و ویروس کرونا تأثیر دوسویه بر هم داشته‌اند. از سویی مدیریت هویت دیجیتال به عنوان یک راهکار راهبردی و مهم در جهت کنترل این بیماری مورد استفاده قرار گرفته است و از سویی دیگر نوآوری‌ها، پیشرفت‌ها و چالش‌های قابل توجهی در حوزه هویت دیجیتال اتفاق افتاده که ناشی از این بیماری بوده است. در این مقاله به موضوعاتی نظیر حضور دیجیتال، فناوری‌های نوین، حاکمیت داده‌های هویتی، حریم خصوصی و چالش‌های مدیریت هویت و دسترسی در سازمان‌ها اشاره می‌شود که در این دوران بر هویت دیجیتال تأثیرگذاری بیشتری داشته‌اند. همچنین گوشه‌هایی از تجربیات کشورهای تایوان، کره جنوبی، سنگاپور و چین در کاهش شیوع این ویروس با استفاده از مدیریت هویت دیجیتال مورد توجه قرار گرفته است. امروز دنیا بیش از هر زمان دیگری به اهمیت و ضرورت هویت دیجیتال پی برده است. بحران رخ داده نشان داد که اگر کشورها از نظام هویت دیجیتال مناسبی برخوردار نباشند، در فضای مجازی و حتی در دنیای واقعی با مشکلات و ناکارآمدی‌های زیادی روبه‌رو خواهند شد. در مجموع می‌توان اذعان داشت این بیماری سرعت پیشرفت و بلوغ مدیریت هویت دیجیتال در فضای مجازی را بیش از پیش افزایش داده است.

کلیدواژه‌ها:

ویروس کرونا (Covid-19)، هویت دیجیتال، احراز هویت دیجیتال، مدیریت هویت دیجیتال، حاکمیت دیجیتال

[1] شرکت راهبران هویت مجازی آینده (برهان) - rasouli@borhanid.com

۱- مقدمه

ویروس کرونا بسیاری از عرصه‌های زندگی بشر را تحت تأثیر خود قرار داده و از حالت عادی خارج کرده است. تأثیرات آن در فضای دیجیتال نیز بسیار قابل توجه است. کاهش حضور در فضای فیزیکی باعث افزایش حضور در فضای دیجیتال (چه برای تأمین نیازمندی‌های کسب‌وکار و چه برای تفریح و سرگرمی) شده است. ویروس کرونا اهمیت تحول دیجیتال را بیش از پیش نشان داد و سرعت تحقق آن را در بسیاری از حوزه‌ها با افزایش چشم‌گیری همراه کرد. این تأثیرات چالش‌هایی نیز به همراه داشته است. بخش قابل توجهی از این چالش‌ها، موضوع هویت دیجیتال را متأثر ساخته و مدیریت هویت و دسترسی دیجیتال افراد در فضای دیجیتال را به چالش کشیده است. این مسئله موجب شد تا امروز دنیا بیش از هر زمان دیگری به اهمیت و ضرورت هویت دیجیتال پی ببرد و دولت‌ها را بر آن داشت تا از ظرفیت‌ها و زیرساخت‌های هویت دیجیتال به عنوان سرمایه‌ای با ارزش حداکثر بهره‌برداری را داشته باشند.

بحران رخ داده نشان داد که اگر کشورها از نظام هویت دیجیتال مناسبی برخوردار نباشند، در فضای مجازی با مسائل و مشکلات زیادی روبه‌رو خواهند شد؛ مسائلی همچون جعل هویت، سرقت هویت و سوءاستفاده‌هایی که اساساً ناشی از ناکارآمدی یا نبود یک نظام مدیریت هویت دیجیتال است. همه واقف‌اند که در موقع بحران فرصت‌ها برای تصمیم‌گیری اندک است و چابکی در سیاست‌گذاری و اجرای آن اهمیت سرنوشت‌سازی دارد. در این دوران حداکثر بهره‌گیری از امکانات موجود باید صورت بگیرد و در واقع هر آنچه در دوران قبلی «کاشت» شده الان باید با حداکثر توان «برداشت» شود. تجربه مقابله با ویروس کرونا نشان داد کشورهایی که از زیرساخت‌ها و برنامه‌ریزی مناسبی در حوزه هویت دیجیتال بهره‌مند بوده‌اند با قدرت بیشتری این بحران را مدیریت کرده‌اند و از شناسایی و احراز هویت شهروندان به عنوان پایه و اساس جلوگیری از شیوع و گسترش ویروس کرونا استفاده کردند. در این کشورها مدیریت هویت دیجیتال مبنای اعمال حاکمیت و مدیریت شهرها، استان‌ها و کل کشور قرار گرفته است. از سویی دیگر، در این شرایط بسیاری از فرآیندهای فیزیکی به صورت دیجیتالی درآمد؛ از خرده‌فروشی‌ها و کسب‌وکارهای کوچک گرفته تا فرآیندهای مهم دولتی نظیر دادرسی دیجیتال که در حال حاضر در دستور کار بسیاری از کشورها از جمله ایران قرار دارد. بدیهی است موضوع احراز هویت دیجیتال در این تحولات حائز اهمیت بسیار است.

هویت دیجیتال و ویروس کرونا تأثیر دوسویه بر یکدیگر داشته‌اند. از سویی مدیریت هویت دیجیتال به عنوان یک راهکار راهبردی و مهم در جهت کنترل این بیماری مورد استفاده قرار گرفته است و از سویی دیگر نوآوری‌ها، پیشرفت‌ها و چالش‌های قابل توجهی به دلیل مقابله با این بیماری در حوزه هویت دیجیتال اتفاق افتاده است. در این مقاله سعی می‌گردد تا به هر دو جنبه این موضوع پرداخته شود. از آنجایی که دنیا به تازگی چنین موضوعی را تجربه کرده است، صرفاً در وب سایت‌ها و برخی مقالات غیررسمی به بخش‌هایی از چالش‌های هویت دیجیتال ناشی از آن اشاره شده است. فلذا هنوز

مستندات قابل توجهی در این حوزه منتشر نشده است. آنچه بدیهی به نظر می‌رسد این است که دنیای هویت دیجیتال در دوران پسا کرونا صورت جدیدی به خود خواهد گرفت و این موضوع به شکل جدی‌تری توسط حاکمیت‌ها، دولت‌ها و برخی نهادهای خصوصی و مؤثر در این حوزه پیگیری خواهد شد. آنچه تا پیش از این به عنوان اهداف بلندمدت و کلان، طراحی مدل‌ها و معماری‌ها جهت مدیریت هویت دیجیتال در کشورها مطرح بود، در حال حاضر به صورت یک الزام و ضرورت مطرح شده است و لازم است تا در کوتاه‌ترین زمان ممکن عملیاتی شود. در مجموع می‌توان اذعان داشت، شیوع این بیماری سرعت پیشرفت و بلوغ مدیریت هویت دیجیتال در فضای مجازی را افزایش داده است.

۲- تحولات و چالش‌های هویت دیجیتال به واسطه شیوع ویروس کرونا

در این بخش به برخی از چالش‌های هویت دیجیتال پرداخته می‌شود که ناشی از شیوع ویروس کرونا بوده است.

۲-۱ حضور دیجیتال به جای حضور فیزیکی

ویروس کرونا باعث شده تا وارد «جهانی بدون تماس» شویم. بسیاری از خدمات حضوری، جای خود را به خدمات غیرحضوری داده‌اند. دسترسی به خدمات مدیریت هویت و دسترسی برای بسیاری از کسب‌وکارها خصوصاً خدمات دولت الکترونیک بسیار مهم شده است. برای نمونه وزارت آموزش و پرورش جهت ارائه خدمات آموزشی غیرحضوری به دانش آموزان اقدام به راه‌اندازی سامانه‌ای به نام «شاد[۱]» کرده است. احراز هویت دانش آموزان یکی از مؤلفه‌های مهم این سامانه است. همچنین دیگر کسب‌وکارها نظیر مؤسسات آموزشی که در این دوران به دنبال برگزاری آزمون به صورت آنلاین هستند، نیازمند احراز هویت دقیق کاربران خود می‌باشند. شیوع ویروس کرونا موجب شد تا شمار قابل توجهی از سازمان‌های بین‌المللی مردم را به دریافت خدمات دیجیتالی تشویق کنند. برای نمونه گروه ویژه اقدام مالی[۲] (FATF) در گزارشی به اهمیت هویت دیجیتال در دوران کرونا اشاره کرده و به دریافت خدمات مالی و بانکی به صورت غیرحضوری تأکید داشته است. همچنین متولیان طرح‌هایی مانند ID2020 که با هدف ایجاد هویت دیجیتال برای افراد فاقد هویت دیجیتال در دنیا مشغول به فعالیت بودند، طرح‌ها و پروژه‌های خود را با سرعت بیشتری پیگیری می‌کنند. این جریانات نشان می‌دهد تحولات قابل توجهی در هویت دیجیتال به وجود آمده است و جلوگیری از رویارویی با هویت‌های جعلی و جرایم هویتی و ایجاد امکان احراز هویت بلادرنگ اهمیت ویژه‌ای یافته است.

عدم حضور فیزیکی در محل کار یا محل دریافت خدمت، قواعد و رویه‌های هویتی و امنیتی را تا حد زیادی برهم زده است. همچنین رویه‌هایی مانند افزایش سقف برداشت پول از عابر بانک‌ها، افزایش سقف جابه‌جایی پول به صورت کارت به کارت نمونه‌ای از تغییرات جدید بوده‌اند. مشتریان در این دوران، تجربیات جدیدی داشته‌اند. از سویی دیگر با توجه به تغییر رفتار مشتریان و ردپای دیجیتال

---

[۱] شبکه آموزشی دانش‌آموزی

[2] Financial Action Task Force (FATF)

آن‌ها نظیر تنوع و گسترش فعالیت در شبکه‌های اجتماعی، الگوریتم‌های شناخت مشتریان بسیاری از کسب‌وکارها تغییر کرده است. گرچه برخی از این اتفاقات و تغییرات رخ داده احتمالاً موقتی است، اما باعث تغییر در انتظارات و رضایت مشتری شده است از این رو، بازگشت و رویگردانی از برخی از این تجربیات گاهی غیرممکن بوده و یا با هزینه‌های بسیار زیادی همراه خواهد بود. همواره بحث ایجاد تناسب و تعادل میان سهولت دسترسی به خدمات دیجیتال از یک سو و امنیت و حریم خصوصی کاربر از سوی دیگر مطرح بوده است. گاهی زیرساخت‌های مناسب و امن برقرار نیست و جهت ارائه خدمات در زمان محدود، فرصت کافی برای تأمین آن وجود ندارد. لذا ایجاد دسترسی به منابع اطلاعاتی و خدمات (تأمین سهولت)، بیشتر از امنیت و حریم خصوصی مورد توجه قرار می‌گیرد و این موضوع می‌تواند بسیار مسئله‌ساز و خطرناک باشد. لذا مدیریت هویت و دسترسی از زمان طراحی[1] اهمیت زیادی در طراحی کسب‌وکارها پیدا کرده است. در عین حال، با توجه به تغییر در ذائقه و تجربه مشتریان می‌توان اذعان داشت این تناسب در دوران بعد از کرونا دچار تغییرات قابل توجه خواهد شد.

۲-۲ حریم خصوصی و مدیریت داده‌های هویتی

با توجه به لزوم مدیریت ویروس کرونا، جمع‌آوری و تحلیل داده در کشورها اهمیت زیادی پیدا کرده است. تسلط بر این بیماری در کشورها وابستگی بسیاری به نحوه دسترسی و تحلیل داده‌های سلامت و دیگر داده‌های هویتی افراد دارد (مک‌دونالد، ۲۰۲۰). چه بسا اگر به اطلاعات مکانی و دیگر داده‌های هویتی افراد دسترسی وجود داشته باشد، کنترل تردد افراد، مسافرت‌ها و دیگر موضوعات ساده‌تر می‌تواند اجرا شود. برای نمونه در کشورهای اتریش و یا آلمان استفاده از داده‌های شبکه‌های مخابراتی به صورت بی نام به منظور ارزیابی شرایط و روند عمومی جامعه در مورد سرعت گسترش ویروس و نقاط بحرانی صورت گرفته است که داده‌های بی نام افراد را جهت بررسی در اختیار نهادهای مرجع قرار می‌دهند (آلیسون، ۲۰۲۰). همچنین در حال حاضر شرکت‌های بزرگی مثل آی‌بی‌ام[2] و اوراکل[3] به همراه سازمان بهداشت جهانی، از منابع داده باز استفاده می‌کنند تا از طریق فناوری‌هایی نظیر بلاک چین، تحلیل و راستی‌آزمایی داده‌های مرتبط با ویروس کرونا را انجام دهند. این کار گرچه در سطح کلان برای شناسایی روندها و نحوه شیوع بیماری در سطح دنیا انجام می‌شود، اما باید در نظر داشت هر چه اطلاعات مربوط به شهروندان و ساکنان شهرها دقیق‌تر و جامع‌تر باشد، مهار این ویروس امکان‌پذیرتر است. همچنین بخش عمده‌ای از این داده‌ها با توجه به اینکه مربوط به سلامت افراد هستند، از حساسیت بالایی برخوردارند. با این شرایط، موضوع حریم خصوصی داده‌ها اهمیت بسیار زیادی پیدا کرده است. به این معنی که نوع داده‌ها، هدف از گردآوری داده‌ها، محل نگهداری و نحوه امحاء آن محل بحث و چالش است. نبود نظارت کافی و استفاده از بسترهای ارتباطی نامناسب می‌تواند موجب سوء استفاده از این داده‌ها شود. برای نمونه افرادِ خاصی هستند که در مدیریت این بیماری اهمیت

[1] Identity and Access Management by Design

[2] IBM

[3] Oracle

بیشتری دارند؛ کسانی که دارای بیماری‌های زمینه‌ای مانند ناراحتی قلبی، دیابت و نظایر آن هستند از این جمله‌اند. با توجه به شرایط غیرعادی و بحرانی پیش آمده و حساسیت داده‌های هویتی این افراد، حفظ حریم خصوصی تبدیل به موضوعی حیاتی‌تر شده است.

۳-۲ مدیریت هویت و دسترسی در سازمان

بسیاری از کسب‌وکارها در دوران کرونا میزان حضور خود در فضای مجازی را افزایش داده‌اند. این موضوع برای سازمان‌ها مسائلی را به همراه داشته است که در این بخش به آن‌ها پرداخته می‌شود.

۱-۳-۲ چالش سطح بلوغ مدیریت هویت دیجیتال

برخی سازمان‌ها و کسب‌وکارها در دوران کرونا مجبور شدند فعالیت‌های خود را بر بستر آنلاین ارائه دهند. برای این اقدام، باید سطح بلوغ و آمادگی دیجیتال فرآیندهای کسب‌وکار آن‌ها متناسب‌سازی شود. برخی از کسب‌وکارها تجربه حضور آنلاین را داشته‌اند و از فرآیندهای مدیریت هویت دیجیتال بهره گرفته‌اند، اما عده‌ای دیگر از بلوغ کافی برای استفاده از هویت دیجیتال بهره‌مند نبوده‌اند و لذا برای این موضوع با چالش بیشتری مواجه شدند. از سویی دیگر بر اساس نوع خدمات دیجیتال ارائه شده، برخی از کسب‌وکارها نیاز به تأیید هویت توسط شخص ثالث نداشته و صرفاً از طریق ثبت‌نام مشتریان در یک وب‌سایت می‌توانند محصولات خود را به فروش برسانند اما برخی دیگر نیاز به تأیید و صحه‌گذاری بر هویت دیجیتال کاربران خود توسط یک نهاد شخص ثالث و قابل اعتماد داشته‌اند. بنابراین مدیریت ریسک خدمات و تعیین میزان ضمانت[1] لازم برای به کارگیری فرآیندها و ابزارهای مدیریت هویت و دسترسی اهمیت زیادی پیدا کرده است. نحوه یکپارچه‌سازی سیستم‌های مدیریت هویت و دسترسی با سیستم‌های فعلی سازمان در مدت زمان کم، تبدیل به یک مسئله مهم شده است. همچنین اغلب سازمان‌ها با این چالش مواجه‌اند که از کانال‌های دیجیتال و روش‌های مختلف بتوانند افراد و کاربران را شناسایی و احراز هویت کرده و با آن‌ها تعامل کنند.

علاوه بر این، یکی از مشکلات مهمی که برخی سازمان‌ها در این دوران با آن مواجه شدند معماری نادرست سیستم‌های مدیریت هویت دیجیتال است، به نحوی که برخی از آن‌ها از مقیاس‌پذیری (افقی و عمودی) مناسبی بهره‌مند نبوده‌اند. گرچه این اتفاق و چنین افزایش تقاضایی برای استفاده از این سیستم‌ها پیش‌بینی نمی‌شد، اما اگر در طراحی این سیستم‌ها، مقیاس‌پذیری مورد توجه قرار می‌گرفت، با مشکلات عدم امکان خدمات‌رسانی به کاربران خود مواجه نمی‌شدند (مکینتوشن، ۲۰۲۰).

۲-۳-۲ دورکاری نیروی انسانی

دورکاری پرسنل یکی از سیاست‌های مهمی بود که اغلب سازمان‌ها اعم از بزرگ، متوسط و کوچک در سراسر دنیا در پیش گرفتند که به دلیل رعایت بهداشت و سلامت افراد از آن‌ها خواسته می‌شد که بدون حضور در محل کار به انجام وظایف محوله در منزل بپردازند. علی‌رغم اینکه این تصمیم به جلوگیری

[1] Level of Assurance (LoA)

از شیوع این ویروس کمک شایانی کرد اما مشکلات و چالش‌هایی را در حوزه امنیت، دسترسی به منابع و هویت دیجیتال ایجاد کرده است. برخی از این چالش‌ها به شرح زیر است:

- مدیریت هویت و دسترسی به منابع اطلاعاتی نظیر اسناد، گزارش‌ها و دیگر مستنداتی که صرفاً در بستر داخلی سازمان‌ها[1] قابل دسترس بود به دلیل دورکاری و پراکندگی حضور کارکنان باید به صورت ابری[2] در اختیار آن‌ها قرار بگیرد و لذا استفاده بیشتر از بسترهای ابری مدیریت هویت و دسترسی (نظیر مدیریت هویت و دسترسی به عنوان خدمت[3]) یکی از اتفاقاتی است که رقم خورده است. بدیهی است این مهاجرت نیازمند تصمیم‌گیری‌های مهم در مورد منابع اطلاعاتی و خدمات و نحوه دسترسی به آنها است.
- در دورکاری کارکنان، استفاده از احراز هویت قوی[4] به دلیل عدم تعامل حضوری بسیار مهم است. یعنی جهت احراز هویت، صرفاً رمز عبور کفایت نمی‌کند و احراز هویت کارکنان باید با استفاده از روش‌های چند گانه، متنوع و قابل اتکا نظیر زیست‌سنجی به درستی انجام شود. همچنین احراز هویت مستمر[5] و حصول اطمینان از اینکه یک کارمند در طول زمان کاری همانی است که باید در دسترس باشد پراهمیت شده است.
- در اغلب موارد به کاربران اجازه داده می‌شود تا از طریق دستگاهی که در اختیار دارند، به شبکه متصل شوند. در اینجا احراز هویت دستگاه‌ها[6] و برقراری ارتباط امن با تبلت، گوشی هوشمند و لپ‌تاپ کاربران اهمیت دارد. همچنین نوع دستگاه، سیستم عامل، تنظیمات اجازه دسترسی و نرم‌افزارهای کاربردی نصب شده روی آن باید مورد توجه قرار بگیرد. استفاده از نرم‌افزارهای ضد ویروس و به‌روز و حصول اطمینان از داده‌هایی که جمع‌آوری شده یا مورد استفاده قرار می‌گیرد بسیار اهمیت دارد (بیل، ۲۰۲۰). به علاوه باید در نظر داشت هر فرد می‌تواند ریسک[7] منحصربه‌فرد خود را در استفاده از هر یک از این دستگاه‌ها داشته باشد. علاوه بر اینکه هر دستگاه نیز به خودی خود دارای ریسک امنیتی خاص است.
- امن بودن بستر ذخیره‌سازی داده‌ها (مرتبط با کاربر و داده‌هایی که در طول دورکاری تولید می‌کند) و حفظ حریم خصوصی داده‌ها حائز اهمیت است.

---

[1] On-Premise
[2] Cloud
[3] Identity and Access Management as a Service
[4] Strong Authentication
[5] Continuous Authentication
[6] Bring your own Device (BYOD)
[7] Bring your own Risk (BYOR)

۳- استفاده از فناوری‌های نوظهور برای مدیریت هویت دیجیتال به واسطه شیوع ویروس کرونا

به کارگیری فناوری‌های نوظهور در حوزه هویت دیجیتال در دوران ویروس کرونا جالب توجه بوده است. استفاده از اینترنت چیزها و پوشیدنی‌ها برای جمع‌آوری و رصد داده‌های سلامتی افراد، تقویت ارتباط ماشین به ماشین[1] و استفاده از هوش مصنوعی برای ارزیابی و تأیید هویت در سیستم‌های هویت دیجیتال مصداق‌هایی از این موضوع هستند. یکی از دلایل مهم به کارگیری فناوری‌های نوظهور در حوزه هویت دیجیتال را می‌توان نیاز به احراز هویت سریع افراد و کاربران در سیستم‌های مختلف نسبت داد. برای نمونه در حال حاضر شناسایی و احراز هویت سریع بیمار برای پزشک و کادر پزشکی بیمارستان‌ها اهمیت زیادی یافته است (لوماس، ۲۰۲۰). همچنین تمایل زیاد به استفاده از خدمات پراهمیت نظیر خدمات بانکی و مالی به صورت برخط دلیل دیگری برای این موضوع است. آمارها نشان می‌دهد در شرایط شیوع کرونا حدود ۲۰ درصد از افراد، متقاضی دسترسی به خدمات مالی به صورت برخط و برای اولین بار هستند (هووات، ۲۰۲۰؛ گلوبال‌آی‌دی، ۲۰۲۰). بسیاری از تأمین‌کنندگان نرم‌افزار در دنیا از این فرصت استفاده کرده‌اند و محصولات و خدمات خود را معرفی کرده‌اند و از آن به عنوان فرصتی برای بازارسازی استفاده کرده‌اند. در ادامه مثال‌هایی از کاربرد فناوری‌های نوظهور در حوزه هویت دیجیتال مورد بررسی قرار می‌گیرد.

۳-۱ زیست‌سنجی و هوش مصنوعی

کاهش تمایل به استفاده از گذرواژه و جایگزینی آن با زیست‌سنجی یک روند جهانی است، اما در این دوران قوت زیادتری گرفته است. در واقع در دوران کرونا نیاز به توسعه فناوری‌های پیشرفته‌تر در حوزه احراز هویت خصوصاً در زمینه زیست‌سنجی بیش از پیش نمایان شده است (آکوونت، ۲۰۲۰). بسیاری از استارتاپ‌ها[2] در این حوزه فعال شده‌اند و نوآوری‌های قابل توجهی از خود نشان داده‌اند که اغلب آن‌ها از تلفیق روش‌های زیست‌سنجی با قابلیت‌های هوش مصنوعی ممکن شده است. در ادامه به مثال‌هایی در این زمینه اشاره می‌شود:

- در کشور چین، سنسورهایی روی صندلی‌های اتوبوس نصب می‌شود که درجه حرارت بدن مسافران را ضبط می‌کند و دوربین‌هایی وجود دارد که از چهره آن‌ها عکس می‌گیرد. در صورت مثبت بودن تست کرونای مسافر، از این عکس‌ها برای ردیابی تماس‌های برقرار شده مسافر با دیگر شهروندان استفاده می‌شود.
- شرکت آمریکایی آتنا سکوریتی[3]، سیستم شناسایی تحت عنوان «غربالگری تب کویید ۱۹» را ارائه داده است. در این سیستم، «دوربین‌های حرارتی مبتنی بر هوش مصنوعی» برای سنجش تب و هشدار به افراد در مورد حضور احتمالی اشخاص ناقل ویروس کرونا

[1] Machine to Machine Communication

[2] Startup

[3] Athena Security

مورد استفاده قرار می‌گیرد. این شرکت محصول خود را برای استفاده در فروشگاه‌های مواد غذایی، بیمارستان‌ها و مکان‌های رای‌گیری عرضه کرده است و هم اکنون در حال استقرار آن در سازمان‌های دولتی، فرودگاه‌ها و شرکت‌ها معتبر است.

- شرکت دمالوگ[1]، یک شرکت مطرح در حوزه زیست‌سنجی است که قابلیت تعیین درجه حرارت بدن را به محصولات خود اضافه کرد و آن را به عنوان یک ویژگی امنیتی جدید در نظر گرفته است. دولت تایلند در حال حاضر از محصول این شرکت به عنوان بخشی از سیستم کنترل مرزی خود استفاده می‌کند.
- شرکت تلپو[2] سیستم‌های سنجش دما را به عنوان بخشی از فناوری تشخیص چهره خود راه اندازی کرده است. این سیستم حتی اگر افراد ماسک بپوشند نیز عملکرد درستی از خود نشان می‌دهد.
- شرکت چینی وایزسافت[3] یک سیستم تشخیص چهره سه بُعدی توسعه داده است که می‌تواند افرادی که ماسک پوشیده‌اند را با دقت ۹۸٪ شناسایی کرده و دمای بدن آن‌ها را اندازه‌گیری کند. چندین دانشگاه و بیمارستان در چین تاکنون محصولات این شرکت را جهت بهره‌برداری مستقر کرده‌اند. به طور مشابه، یکی دیگر از شرکت‌های چینی به نام هان‌ون[4] نیز فناوری را توسعه داده است که می‌تواند چهره‌ها را از طریق ماسک‌ها تشخیص دهد و همچنین دمای بدن را اندازه‌گیری کند (بروم‌فیلد، ۲۰۲۰).

۲-۳ بلاک‌چین[5]

با شیوع ویروس کرونا جهان نیاز به شبکه گسترده‌تری از اعتماد برای مدیریت هویت افراد دارد. فناوری بلاک‌چین یکی از فناوری‌های راهبردی جهت ایجاد شبکه اعتماد در فضای مجازی به شمار می‌رود. همچنین خودکارسازی و هوشمندسازی فرآیندها و ایجاد قراردادهای هوشمند از دیگر مزایای آن است. از طریق این فناوری اطمینان حاصل می‌شود که داده‌های شخصی افراد برای اهداف سودجویانه مورد استفاده قرار نمی‌گیرد و حریم خصوصی داده‌های هویتی حفظ می‌شود (سونمز، ۲۰۲۰). طرح فاصله‌گذاری اجتماعی فرصتی فراهم آورد تا برخی استارتاپ‌هایی که در حوزه بلاک‌چین فعال هستند راه‌حل‌های خود را بیش از پیش به سمت کاربردی شدن پیش ببرند. برای مثال در کشورهایی مثل آلمان برخی شرکت‌ها، محصولات خود را جهت خرید آنلاین دارو از داروخانه‌ها از طریق بلاک‌چین ارائه کرده‌اند. در برخی از این راه‌حل‌ها، امکان اتصال کیف پول الکترونیکی به صندوق داروخانه‌ها برای انجام پرداخت الکترونیک فراهم شده است (آلیسون، ۲۰۲۰). همچنین برخی دیگر از شرکت‌های ارائه دهنده

---

[1] Dermalog
[2] Telpo
[3] Wisesoft
[4] Hanvon
[5] Blockchain

بلاک‌چین و سیستم‌های هویت دیجیتال غیرمتمرکز در حوزه‌هایی مانند پرونده الکترونیک سلامت و ایجاد ارتباط امن بین پزشک و بیمار از راه دور در برخی از کشورها راه‌حل‌های ارزشمندی ارائه داده‌اند (گودبل، ۲۰۲۰).

بلاک‌چین در سطح ملی و دولت الکترونیک کشورها نیز تأثیر داشته است. برای مثال وزارت بازرگانی امارات متحده عربی برای ارائه خدمات دولتی بر کانال‌های دیجیتال تمرکز بیشتری کرده و برای احراز هویت از سیستم احراز هویت مبتنی بر بلاک‌چین بهره گرفته است. همچنین این کشور برای جمع‌آوری داده‌های بهداشت و درمان و احراز هویت اسناد از بلاک‌چین بهره گرفته است (رودگرز، ۲۰۲۰). در کشورهایی مثل استونی، طرح‌های اقامت دیجیتال قوت بیشتری پیدا کرده است چرا که امکان افتتاح حساب بانکی، ثبت شرکت، تبادلات مالی و غیره حتی بدون حضور فیزیکی در این کشور از طریق این طرح میسر شده است.

۴- سیاست‌گذاری کشورها به منظور مقابله با ویروس کرونا با استفاده از مدیریت هویت دیجیتال

کشورهای مختلف به منظور جلوگیری از شیوع و گسترش ویروس کرونا، راهکارها و تمهیدات متعدد و متفاوتی را مورد استفاده قرار داده‌اند. در این بخش به بررسی برخی از این تجربیات پرداخته می‌شود. در حال حاضر «قرنطینه هوشمند» در بسیاری از این کشورها مورد استفاده قرار می‌گیرد. برای مثال در شکل ۱، دستبند هوشمند قرنطینه جهت ردیابی افراد در هنگ‌کنگ را نشان می‌دهد که برای رصد همه مسافران تازه وارد به این شهر مورد استفاده قرار می‌گیرد. این دستبند از طریق اتصال به یک برنامه کاربردی نصب شده روی تلفن همراه هوشمند، محل زندگی شخص قرنطینه شده را کنترل کرده و تخلفات رخ داده را به پلیس و دیگر مقامات گزارش می‌دهد.

شکل ۱- دست‌بند هوشمند قرنطینه

اما در مقابل نیز در بعضی از کشورها استفاده از راه‌حل‌های جدید فناوری پرهزینه و دشوار بوده است. به همین دلیل در این کشورها از گزینه‌های ارزان‌تر برای ردیابی افراد استفاده می‌شود. برای نمونه در کشور هند از مُهر جوهری برای قرنطینه خانگی شهروندان استفاده می‌شود که زمان انقضای قرنطینه هم روی آن درج می‌شود (شکل ۲) (استریلکوفسکی، ۲۰۲۰).

شکل ۲- مُهر جوهری برای قرنطینه خانگی افراد در کشور هند

تمرکز این مقاله بیشتر بر روش‌های دیجیتالی استفاده شده توسط کشورها جهت جلوگیری از شیوع ویروس کرونا است. در این روش‌ها، تمرکز بر داده‌های هویتی افراد است. در واقع کشورهایی که از روش‌های دیجیتالی برای رصد و کنترل بیماری استفاده می‌کنند از مدیریت هویت دیجیتال افراد بهره می‌گیرند. در ادامه به تشریح تجربیات برخی کشورها در این حوزه پرداخته می‌شود.

۱-۴ کشور تایوان

تایوان دارای سیستم گسترده دوربین‌های مدار بسته است و بسیاری از شرکت‌های تولید کننده تجهیزات CCTV در این کشور قرار دارند. فعالیت‌های زیرساختی قابل توجهی در حوزه شهر هوشمند در تایوان انجام شده است و سیاست‌گذاری‌ها در این کشور اغلب به صورت داده محور انجام می‌شود. به عنوان مثال می‌توان به پایگاه داده ملی بیمه درمانی این کشور اشاره کرد که با کارت‌های هوشمند جهت مدیریت هویت بیمار و تاریخچه پزشکی او در ارتباط است. استفاده گسترده از ردیابی تلفن همراه مبتنی بر اپراتورهای تلفن همراه نیز یکی از راهکارهای این کشور در راستای اجرای رویه‌های مرتبط با قرنطینه می‌باشد. به همین منظور، این کشور از پیوند میان پایگاه داده‌های ملی حداکثر استفاده را داشته است. یکی از اهداف صریح کشور تایوان، بهبود مدیریت اطلاعات و ایجاد یک سیستم اطلاعاتی قدرتمند جهت اجرای فرآیند قرنطینه است. همچنین تلاش تایوان برای حفظ حریم خصوصی به ایجاد اعتماد بالای عمومی کمک کرده است.

تایوان در پی اپیدمی سارس[1] ساختارهای ویژه‌ای جهت پاسخگویی به نیازمندی‌های مرتبط با رفع شیوع این بیماری در سال ۲۰۰۳ ایجاد کرده است. این کشور ضمن استفاده از تجربیات قبلی خود، هماهنگی وزارت‌خانه‌های بهداشت و رفاه، حمل و نقل، اقتصاد، کار و آموزش و حفاظت از محیط زیست و ادغام پایگاه داده‌های مرتبط با آن‌ها (با تأکید بر داده‌های بانک اطلاعات ملی بیمه سلامت، مهاجرت و گمرک) را جهت پاسخگویی به نیازمندی‌های بیماری کرونا در دستور کار خود قرار داده است. هدف از این کار، ترسیم نقشه اطلاعات پروازهای ورودی به کشور به منظور غربالگری افراد بوده است. در این راستا اطلاع‌رسانی به افراد از طریق ارسال پیامک و یا استفاده از کدهای QR جهت تعیین گزارش تاریخچه سفر و تاریخچه سلامت افراد برای ۱۴ روز الی ۳۰ گذشته انجام می‌شود.

اقدامات قرنطینه ١٤ روزه در تایوان برای کلیه افرادی که از مناطق پرخطر وارد کشور می‌شوند الزامی است. کلیه افراد در معرض خطر، موظف هستند تا به صورت الکترونیکی فرم اخطار قرنطینه را امضا کنند. مواردی که مربوط به افراد با ریسک بالاتر باشد از طریق ردیابی تلفن همراه برای آن‌ها یک «حصار الکترونیکی» در نظر گرفته می‌شود. در صورت خارج شدن آن‌ها از محیط تعیین شده به صورت پیامک به آن‌ها هشدار داده می‌شود. اگر فرد تحت قرنطینه در حال حرکت دیده شود، با وی تماس گرفته شده و به او اخطار داده می‌شود. اگر تلفن همراه فرد خاموش باشد پلیس به محل اقامت او مراجعه می‌کند. برای عده‌ای دیگر که پرخطر بوده و تلفن همراه قابل اطمینانی ندارند، سیم کارتی از طرف دولت جهت نظارت دیجیتالی بر آن‌ها در نظر گرفته می‌شود. پلیس و دیگر مقامات دو بار در روز با افراد تماس ویدیویی برقرار می‌کنند تا اطمینان حاصل کنند که افراد با قراردادن تلفن‌های خود در خانه از ردیابی جلوگیری نمی‌کنند.

همچنین تأمین ماسک بهداشتی از طریق کارت ملی بیمه سلامت فرد و به صورت سفارش آنلاین انجام می‌شود. ارائه ماسک به افراد تبعه خارجی که فاقد این کارت هستند، از طریق کد QR ارائه شده توسط خدمات مهاجرتی این کشور امکان‌پذیر است (میرتل، کلیمبورگ و ورهاگن، ۲۰۲۰).

۲-۴ کشور کره جنوبی

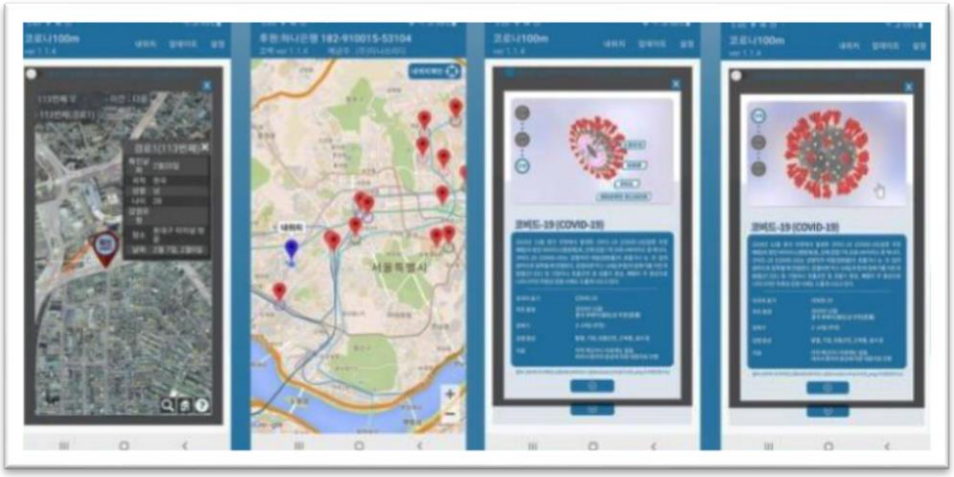
کره جنوبی سابقه‌ای طولانی در زمینه نظارت و رصد شهروندان دارد که ناشی از دیکتاتوری‌های نظامی بومی و گذشته این کشور است. کره جنوبی تأکید زیادی بر ردیابی افراد به کمک سیستم جب‌پی‌اس[2] دارد و در این زمینه از همکاری بین شرکت‌های مخابراتی و آژانس‌های حقوقی و قانون‌گذاری بهره زیادی گرفته است. یکی از این برنامه‌ها «کرونا ۱۰۰ متر[3]» است (شکل ۳) که از داده‌های ارائه شده توسط اپراتورهای مخابرات استفاده می‌کند. نحوه کارکرد این برنامه‌ها به گونه‌ای است که اگر افراد در فاصله ۱۰۰ متری از مکانی که شخص مبتلا شده به کرونا در آن حضور داشته است قرار بگیرد، به او هشدار داده می‌شود.

---

[1] SARS

[2] GPS

[3] Corona 100m



شکل ۳- نرم‌افزار کاربردی کرونا ۱۰۰ متر

علاوه بر این، دولت کره جنوبی یک برنامه مبتنی بر جی‌پی‌اس ایجاد کرده است که اگر بیماران از قرنطینه خارج شوند به آن‌ها اخطار و هشدار می‌دهد. در حالت کلی دولت کره جنوبی به داده‌های قابل توجهی از افراد دسترسی دارد. این کشور بین داده‌های خصوصی و «داده‌های شناسایی نشده[۱]» تمایز قائل شده است. داده‌های شناسایی نشده به عنوان داده شخصی محسوب نمی‌شود و لذا دولت می‌تواند بدون رضایت سوژه‌های مورد نظر هر گونه بهره‌برداری و تحلیل داده‌های بزرگ را انجام دهد. این داده‌ها حتی می‌تواند در اختیار اشخاص ثالث قرار گیرد.

بخش دیگری از تحلیل داده‌های کلان به این شکل انجام می‌شود که مناطق پر ریسک شهرها به صورت خوشه‌ای مشخص شده و ردیابی و رصد افراد بر اساس احتمال انتقال بیماری در این خوشه‌ها انجام می‌شود. هر کسی که به عنوان ناقل ویروس در نظر گرفته شود به صورت اجباری قرنطینه می‌شود و از طریق حصار مبتنی بر مکان[۲] به صورت رسمی از طریق تماس تلفنی و اپلیکشین‌های موبایلی[۳] رصد و مانیتور می‌شود. همچنین در مواردی، جهت تکمیل رویه رصد، مصاحبه با بیمار، تأیید صحت فیلم‌های دوربین مدار بسته، سوابق کارت اعتباری و داده‌های جی‌پی‌اس تلفن همراه وی نیز انجام می‌شود. دولت با انتشار داده‌های مرتبط با نقاط انتشار بیماری از طریق پیام متنی (پیامک) و وب‌سایت‌های تحت مدیریت دولت نقشه نقاط آلوده را جهت دسترسی عموم ترسیم و به‌روزرسانی می‌کند.

۳-۴ کشور سنگاپور

سنگاپور یکی از قوی‌ترین و دقیق‌ترین سیستم‌های نظارت را در جهان دارد. این کشور از مجموعه پایگاه داده‌های کاملاً یکپارچه استفاده می‌کند و از تحلیل داده‌ها در تصمیم‌گیری‌های سیاسی خود استفاده

---

[۱] De-identified data

[2] Geo-fencing

[3] Mobile Application

گسترده‌ای کرده است. علاوه بر این، سنگاپور از نظر بهره‌برداری از دوربین‌های مدار بسته سومین کشور پیشرفته بعد از کشور چین است و از نرم‌افزار تشخیص چهره با استفاده از هوش مصنوعی نیز استفاده می‌کند. رویکرد کشور سنگاپور، ردیابی مخاطبین و همچنین استفاده از کدهای QR و تهیه نقشه نقاط آلوده احتمالی جهت ارائه برای عموم است. به علاوه، این کشور قرنطینه خانگی را بر اساس سطوح مختلف ریسک در شهرهای مختلف در نظر می‌گیرد.

سنگاپور ردیابی اطلاعات افراد و مسافران با استفاده از تلفن همراه و همچنین تشخیص چهره با استفاده از دوربین مدار بسته را در دستور کار خود قرار داده است. در موارد به اصطلاح «تماس نزدیک» یا موارد خاص ممکن است از فرد خواسته شود تا به صورت داوطلبانه تلفن همراه خود را در اختیار مراجع ذی‌صلاح قرار دهد تا داده‌های مربوط به حرکت جی‌پی‌اس مرتبط به او استخراج شده و مورد تحلیل قرار بگیرد. سنگاپور نقشه سلامت در سطح کشور را در قالب تصویری از شبکه‌های اجتماعی ترسیم می‌کند که دائماً در حال به‌روزرسانی است (شکل ٤).

شکل ۴ – نقشه سلامت در قالب شبکه اجتماعی در کشور سنگاپور

سنگاپور در کلیه ساختمان‌های عمومی و اکثر نقاط حمل و نقل (از جمله تاکسی) از کدهای QR استفاده گسترده‌ای کرده است تا در صورت نیاز ردیابی مخاطب را تسهیل کند. این کشور تأکید بسیاری بر دریافت اطلاعات به صورت داوطلبانه از افراد دارد و حفظ حریم خصوصی در این کشور بسیار مهم است. سنگاپور برنامه کاربردی تحت حمایت دولت با عنوان «تریس‌توگدر[1]» را تبلیغ کرده است. در این برنامه از فناوری بلوتوث و پروتکل توسعه‌یافته «بلوتریس[2]» برای شناسایی فاصله کاربر استفاده می‌شود. با استفاده از این نرم‌افزار، اگر سوژه‌ای به مدت حداقل ۳۰ دقیقه و در فاصله ۲ متری در مجاورت شخصی

[1] TraceTogether

[2] BlueTrace

قرار بگیرد که به لحاظ ریسک انتقال ویروس در سطح بالایی است، شناسایی شده و به او اطلاع داده می‌شود. البته عنوان شده که این برنامه فقط ۲۱ روز اطلاعات افراد پرخطر را ذخیره می‌کند. همچنین به منظور ایجاد شفافیت، دولت سنگاپور تصمیم گرفته است تا کد منبع این برنامه را به صورت رایگان در اختیار عموم مردم قرار دهد. افرادی که به واسطه قرنطینه خانگی باید به مدت ۱٤ روز در خانه بمانند از چند روش کنترل می‌شوند. یکی از این راه‌ها، تماس تلفنی دو بار در روز و ارسال تصاویر زنده از طریق تلفن همراه از محیط اطراف فرد است. همچنین در مواقع لازم از برچسب‌های آراف‌آی‌دی[۱] نیز استفاده می‌شود. علاوه بر این‌ها افرادِ در قرنطینه خانگی، برای ارسال موقعیت فعلی خود باید از لینکی استفاده کنند که در مواقع تصادفی به آن‌ها پیامک می‌شود. این کشور همچنین از نرم‌افزاری با عنوان گاوتک[۲] به منظور مقابله با خبرها و پیام‌های اشتباه و غلط بهره می‌گیرد. در این راستا از ابزارهای هوش‌مصنوعی برای ترجمه سریع مطالب از انگلیسی به زبان‌های رسمی استفاده می‌شود تا با مقابله با شایعه‌پراکنی، ترس و اضطراب را در جامعه به حداقل برساند. سنگاپور اطلاعیه‌های روزانه در مورد آلودگی‌های افراد تحت عنوان «موارد جدید» و همچنین احتمال بروز عفونت در مکان‌های مختلف را در یک وب سایت دولتی اعلام می‌کند.

۴-۴ کشور چین

کشور چین به دلیل استفاده از سیستم‌های گسترده هوش مصنوعی، دوربین‌های مدار بسته و فناوری تشخیص چهره، نظارت بر ارتباطات از راه دور (از طریق اینترنت و ردیابی موقعیت مکانی تلفن همراه) و استفاده از داده‌های جامع زیست‌سنجی یکی از دقیق‌ترین ظرفیت‌های نظارت ملی در جهان را دارد. برای مقابله با ویروس کرونا، این کشور با استفاده از ترکیبی از اطلاعات یاد شده، برنامه‌ای تحت عنوان «سپر طلایی[۳]» طراحی و پیاده‌سازی کرده است که در ادامه به جزئیات آن پرداخته می‌شود.

---

[۱] RFID

[۲] GovTech

[۳] Golden Shield

از مهم‌ترین سیاست‌های قرنطینه در چین، استفاده از «کد سلامتی[1]» مرتبط با نرم‌افزارهای وی‌چت[2] و علی‌پی[3] است که از سیستم‌های دارای کد QR رنگی برای ردیابی مخاطب استفاده می‌کند (شکل ۵) و ارائه آن برای ورود به هر محیطی کاملاً اجباری است. کدQR سبز به معنای شرایط عادی (سالم) برای فرد است. رنگ‌های زرد و قرمز به این معنی است که فرد با یک فرد آلوده به ویروس کرونا، تماس قطعی یا احتمالی داشته است. رنگ زرد یعنی فرد باید به مدت ۱ هفته در قرنطینه بماند و رنگ قرمز یعنی ۲ هفته قرنطینه برای فرد لازم است (داویدسون، ۲۰۲۰).

شکل ۵- کد سلامتی مورد استفاده به صورت QR در کشور چین

این برنامه کاربردی دائماً با سرورها و پایگاه‌های داده دولتی در ارتباط است، بر اساس تحلیل ریسکی که انجام می‌شود، رنگ کد یا «رنگ سلامتی» دائم تغییر می‌کند. این تغییر بر اساس مسافرت‌های شهری و بین شهری که شهروندان داشته‌اند، میزان حضور آن‌ها در کانون‌های شیوع بیماری و در نهایت میزان ریسک آن‌ها برای انتقال آلودگی صورت می‌گیرد. این برنامه در بیش از ۲۰۰ شهر چین عملیاتی شده است. برای استفاده از وسایل حمل‌ونقل عمومی، ورود به سوپر مارکت‌ها یا استفاده از خدمات عمومی، دارا بودن کد QR سبز ضروری است. همچنین داده‌های این کد با دیگر داده‌ها از جمله تاریخچه مسافرت و داده‌های تلفن همراه افراد یکپارچه است. در این برنامه از ابزارهای هوش مصنوعی و چت بات‌ها[4] و تماس‌های خودکار برای بررسی تاریخ سفر و دریافت اطلاعات لازم به منظور شناسایی نقاط مهم شیوع ویروس کرونا استفاده می‌شود. همچنین این کد برای تردد در شهرهای دیگر مورد استفاده قرار می‌گیرد. هر استان، سیستم کد سلامت مربوط به خود را دارد. برای افرادی که بین چند استان تردد اجباری دارند، استان‌های مختلف با هم برای یکسان‌سازی و تعامل‌پذیری کدها همکاری می‌کنند. امکان به اشتراک‌گذاری داده‌های این نرم‌افزار با پلیس نیز وجود دارد.

---

[1] Health Code
[2] WeChat
[3] Alipay
[4] chatbots

شکل ۶- نرم‌افزار کاربردی نشان‌دهنده «کد سلامتی»

یکی از چالش‌های مهم استفاده از این برنامه کاربردی، عدم رعایت حریم خصوصی شهروندان چینی است. اغلب مردم چین این سؤال را دارند که این نرم‌افزار کاربردی چگونه کار می‌کند و از این طریق چه داده‌هایی از آن‌ها جمع‌آوری شده و مورد استفاده قرار می‌گیرد؛ چرا که اگر کد قرمز رنگ به کسی اختصاص داده شد، فرد نمی‌تواند آن را تغییر دهد و مجبور است از مقررات سفت و سخت قرنطینه تبعیت کند (موزور و زانگ، ۲۰۲۰).

برنامه‌های کاربردی دیگری نیز برای مدیریت شیوع ویروس کرونا در کشور چین به کار می‌رود که البته اجباری نیستند. برای مثال برنامه کاربردی با عنوان «فوکوسما[1]» توسط شرکت تنسِنت[2] تولید شده است که دانش آموزان را ترغیب می‌کند تا با ورود داده‌های زیست‌سنجی خود (مانند درجه حرارت بدن)، مجموعه داده‌های مرتبط با ریسک ابتلاء به این بیماری را تکمیل کنند. همچنین از طریق این نرم‌افزار می‌توان مناطق «شیوع» عمومی را شناسایی کرد (شکل ۷). این برنامه کاربران را ترغیب می‌کند تا از ورود به یک منطقه خاص و پرخطر خودداری کنند. همچنین این برنامه به افراد امکان می‌دهد تا از ریسک ابتلاء به ویروس در مکان‌های مختلف آگاهی پیدا کنند و بتوانند میزان خطر افراد دیگر را ارزیابی کنند. این ارزیابی بر اساس متغیرهایی مانند حضور در کلاس‌های مشترک، مسافرت‌ها و نظایر آن صورت می‌گیرد. این برنامه به پایگاه داده‌های وزارت بهداشت، وزارت حمل‌ونقل، راه آهن و اداره هواپیمایی کشوری چین متصل است.

[1] Fuxuema
[2] Tencent

شکل ۷- نقشه سلامتی مرتبط با نرم‌افزار تنسِنت

دیگر نرم‌افزارهایی که برای مدیریت شیوع کرونا در چین مورد استفاده قرار می‌گیرند از طریق روش‌های ردیابی موقعیت مکانی، افراد را رصد می‌کنند و یا از آن برای ارسال اخبار و هشدارهای شخصی‌سازی شده برای هر شهروند استفاده می‌شود.

۵- جمع‌بندی و نتیجه‌گیری

ویروس کرونا و هویت دیجیتال تأثیرات متقابلی بر روی یکدیگر داشته‌اند. با توجه به آنچه از تأثیرات متقابل ویروس کرونا و هویت دیجیتال در این مقاله سخن به میان آمد، در این بخش به جمع‌بندی و نتیجه‌گیری موضوعات پرداخته می‌شود.

- ایجاد، تقویت و توسعه زیرساخت‌های هویت دیجیتال در سطح ملی بیش از پیش مورد توجه کشورها قرار گرفته است. علاوه بر موضوعات فنی و تکنولوژیکی، بحث‌های حقوقی، سیاسی، بین‌المللی، اجتماعی و فرهنگی هم نمود بهتری پیدا کرد و تأثیرات این ابعاد از هویت دیجیتال در مدیریت این بیماری بیش از پیش به چشم آمد.
- مدیریت هویت دیجیتال در کنار مدیریت دسترسی دیجیتال قرار گرفت و هر دو در کنار هم معنای حقیقی یافتند. لذا مدیریت هویت و دسترسی به عنوان یک موضوع جدی حاکمیتی مطرح گردید.
- بین هویت فیزیکی و هویت دیجیتال افراد پیوند عمیق‌تری برقرار شد و شکاف بین آن‌ها کمرنگ‌تر گردید. این موضوع به شکل‌گیری و بلوغ هر چه بیشتر دیجیتال توین[1] (قُل دیجیتال) افراد در فضای مجازی کمک خواهد کرد.
- تلاش کشورها در استفاده حداکثری از کلیه منابع اطلاعاتی و پایگاه‌های داده و تجمیع آن‌ها به منظور فراهم کردن اطلاعات دقیق و جامع از شهروندان و نیز اتباع خارجی در کشور خود

[1] Digital twin

بوده است. برای مثال در حال حاضر اتحادیه اروپا درصدد امکان‌سنجی بهره‌برداری از نسخه دوم سیستم اطلاعاتی شینگن[۱] جهت ردیابی مسافرت‌ها و جابجایی افراد است و تا کنون هم از بخشی از این اطلاعات استفاده کرده است.

- تسلط روی داده‌های هویتی و شخصی افراد برای کشورها در این دوران اهمیت زیادی داشته است. شاید بتوان ادعا کرد کشورهایی که تسلط بیشتری بر داده‌های افراد داشته‌اند، رصد آن‌ها را بهتر انجام داده و بر مدیریت این بیماری تسلط بیشتری داشته‌اند. اما باید در نظر داشت این موضوع ارتباط مستقیم و تنگاتنگی با موضوع حریم خصوصی دارد. طبق آنچه بررسی شد، حریم خصوصی در برخی دولت‌ها رعایت می‌شود اما برخی دیگر از کشورها به منظور حفظ نظم اجتماعی و محافظت از منافع ملی و امنیت ملی این موضوع را به طور جدی مد نظر قرار ندارند. برای مثال جهت قرنطینه دیجیتالی افراد، برخی کشورها مانند سنگاپور از رویه‌های داوطلبانه استفاده کرده‌اند. در حالی که در کشوری مثل چین، استفاده از رویه‌های تعیین شده و ارسال اطلاعات شخصی اجباری است. در بعضی کشورها حتی جمع‌آوری اطلاعات بدون آگاهی و دخالت مردم انجام می‌شود. به نظر می‌رسد رعایت حریم خصوصی در دستور کار این دولت‌ها قرار ندارد. علاوه بر جهت‌گیری کشورها نسبت به حریم خصوصی، لازم است که رویکرد این کشورها نسبت به مدیریت بحران و موضوع ویروس کرونا هم مد نظر قرار گیرد، چرا که این موضوع باعث شده است تا برخی کشورها جهت مواجهه با موضوع حریم خصوصی متناقض عمل کنند. برای نمونه در اتحادیه اروپا رعایت الزامات قوانین حریم خصوصی مانند جی‌دی‌پی‌آر[۲] برای همه کشورها الزامی است. برای مثال در کشور اتریش از اپلیکیشن‌های موبایلی برای ردیابی تماس افراد استفاده می‌شود که اولاً استفاده از آن اجباری نیست و در ثانی اطلاعات کاربر با اجازه مستقیم آن‌ها برای مراجع ذی‌ربط ارسال می‌گردد. اما در مقابل در کشور لهستان برای اجرای برنامه‌های قرنطینه خانگی، استفاده از اپلیکیشن‌های موبایلی و ارسال اطلاعات شخصی افراد اجباری است. علی‌رغم وجود بحران در دنیا و ضرورت جمع‌آوری اطلاعات از افراد جامعه می‌توان اذعان داشت قوانین و مقررات فعلی در حوزه حریم خصوصی پاسخگوی این شرایط نیست. عده‌ای معتقدند حریم خصوصی در بُعد حاکمیتی و خصوصاً در زمان بحران بی معنا است. حتی بسیاری از کشورهایی که برای حریم خصوصی قوانین و رگولاتوری تدوین کرده‌اند (خصوصاً کشورهای اروپایی) در برخی موارد از خطوط قرمز پا را فراتر گذاشته‌اند. لذا قوانینی مانند جی‌دی‌پی‌آر آن‌چنان خاصیت بازدارنگی نداشته است. شاید بتوان بیان کرد که حریم خصوصی در دوران بحران یک نیازمندی جدید است که قوانین و رگولاتوری خاص خود را می‌طلبد. لذا نباید به دلیل شرایط خاص، قوانین حریم خصوصی به کلی نقض شوند، بلکه

---

[۱] Schengen Information System (SIS)

[2] General Data Protection Regulation (GDPR)

بسته به شرایط لازم است تا در قوانین موجود تغییراتی اعمال گردد یا الزامات قانونی جدیدی در نظر گرفته شود. رویکرد حریم خصوصی باید ارائه‌دهنده راه‌حل‌های چندذی‌نفعی باشد، به نحوی که جایگاه شهروندان، دولت‌ها و حاکمیت‌ها باید به صورت همزمان و متناسب در قوانین مد نظر قرار گیرد.

- مدیریت ارتباطات هویت[۱] در این دوران اهمیت بسیار پیدا کرد. هویت افراد از پایگاه‌های داده مختلف و از طریق دستگاه‌های متنوع گردآوری شد و ارتباط دقیق بین داده‌های هویتی افراد برقرار گردید و بدین ترتیب «نقشه داده‌های هویتی» افراد به صورت به‌روز شده و بلادرنگ شکل گرفت که این حجم از داده‌ها و ایجاد یکپارچگی میان آن‌ها بسیار جالب توجه است.
- غربالگری و اعتبارسنجی هویت دیجیتال اهمیت در موارد متعددی مورد استفاده قرار گرفته است. صحت‌سنجی هویت افراد پس از جمع‌آوری از منابع مختلف انجام شده و جهت بهره‌برداری مورد ارزیابی، غربال و تأیید قرار می‌گیرد. همچنین میزان دقت سیستم‌های احراز هویت بسیار تقویت شده است و با به کارگیری فناوری‌های نوین نظیر زیست‌سنجی احتمال بروز خطا کاهش چشم‌گیری داشته است.
- اطلاعات مکانی جزو دقیق‌ترین و حساس‌ترین اطلاعات هویتی افراد به حساب می‌آید که به عنوان حاکمیتی‌ترین منبع اطلاعاتی برای کنترل این بیماری توسط دولت‌ها در کنار داده‌های سلامتی و تردد افراد مورد استفاده قرار گرفته است. تا جایی که شاید بتوان به واسطه اطلاعات هویتی افراد یک شهر، سطح اطمینان یا اعتماد را برای مکان فیزیکی (به عنوان یک موجودیت مستقل) در نظر گرفت و ارزیابی‌ها و تحلیل‌های مربوط به آن را انجام داد.
- با توجه به داده‌های ارزشمند و حساسی که از شهروندان گردآوری می‌گردد، مدیریت دسترسی ممتاز[۲] برای مقامات دولتی و حاکمیتی بسیار مهم است؛ اینکه چه فرد یا افرادی به داده‌های خاص و حساس مردم دسترسی دارند و برای چه منظوری از این داده‌ها استفاده می‌کنند بسیار مهم است. عدم رعایت این موضوع می‌تواند تبدیل به یک فاجعه امنیتی و ملی شود.
- تلفن همراه هوشمند به عنوان مهم‌ترین اعتبارنامه[۳] جهت مدیریت هویت دیجیتال افراد توسط دولت‌ها در این دوران مورد استفاده قرار گرفته است. شاید یکی از مهمترین دلایل آن، امکان دسترسی به اطلاعات هویتی افراد به صورت سریع و بلادرنگ از طریق تلفن همراه باشد؛ بنابراین به نظر می‌رسد فناوری‌هایی نظیر کارت هوشمند، علی رغم اهمیت آن‌ها در زیست‌بوم هویت دیجیتال کشورها، نقش جدی و قابل توجهی در رصد و مدیریت هویت دیجیتال افراد ایفا نکرده است.

---

[۱] Identity Relationship Management (IRM)

[2] Privileged Access Management

[3] Credential

- استفاده از قابلیت‌های شبکه‌های اجتماعی جهت به‌روزرسانی آنی وضعیت سلامت کشور با توجه به تماس‌های فیزیکی افراد اقدام بسیار ارزشمندی است که امروزه از آن استفاده می‌شود. همچنین استفاده از نرم‌افزارهای شبکه اجتماعی موبایلی با توجه به توانمندی‌ها و ضریب نفوذ بالای آن در بسیاری از کشورها (مثل چین) قدرت زیادی را در اختیار حاکمیت‌ها جهت اعمال قدرت قرار داده است.
- سیاست‌گذاری‌ها و تصمیمات به سمت داده-محور شدن پیش رفته است و تصمیم‌گیری‌ها به واسطه تحلیل‌های پیش‌گیرانه و پیش‌گویانه بر همین مبنا به صورت بلادرنگ درآمده است. به واسطه این موضوع، شاید «حاکمیت چابک» یا «حاکمیت بلادرنگ» عبارت جدیدی برای حاکمیت باشد که در آن تصمیم‌گیری‌ها به سرعت قابل انجام است و دستخوش فوت وقت نمی‌شود. از این رو می‌توان گفت حاکمیت دیجیتال در فضای مجازی با استفاده از هویت دیجیتال وارد فاز نوینی شده و سمت و سوی جدیدی یافته است. این موضوع باعث می‌شود حاکمیت بر فضای فیزیکی از طریق فضای دیجیتال با قدرت بیشتری صورت پذیرد. از سویی دیگر باید در نظر داشت که دلیل این تحول، دسترسی گسترده به منابع اطلاعاتی و ایجاد یکپارچگی میان آنها است. لذا شکل‌گیری زیست‌بوم داده (خصوصاً داده‌های هویتی) و بلوغ آن، در افزایش دامنه حاکمیتی دولت‌ها نقش سازنده‌ای دارد. بنابراین بخش قابل توجهی از حاکمیت چابک را حاکمیت داده[1] شکل می‌دهد. حاکمیت داده و مدیریت هویت و دسترسی لازم و ملزوم یکدیگرند. چرا که بخش عمده‌ای از دلایل موفقیت حاکمیت داده منوط به ایجاد سازوکارهای حاکمیت داده‌های هویتی از طریق مدیریت هویت و دسترسی است. در واقع قلب حاکمیت داده و اطلاعات، نظام مدیریت هویت و دسترسی است.
- مدیریت هوشمند شهری به واسطه مدیریت هویت دیجیتال شهروندان (مدیریت ترددها، خودروها، ترسیم نقشه بیماری مبتنی بر ریسک) بیش از پیش به صورت بلادرنگ ممکن شده است. علاوه بر این، استفاده از ارزیابی و مدیریت ریسک در سطح ملی و در برخی موارد در سطح بین‌المللی اهمیت زیادی پیدا کرده است. بدیهی است پایه و اساس ارزیابی ریسک، داده‌های هویتی افراد است.
- در دوران ویروس کرونا، سرعت پیشرفت و بلوغ فناوری‌های نوین مرتبط با هویت دیجیتال مخصوصاً در حوزه هوش مصنوعی و بلاک‌چین افزایش چشم‌گیری پیدا کرده است. البته به نظر می‌رسد هوش مصنوعی کاربردهای قابل توجهی در بخش‌های حاکمیتی داشته باشد که احتمالاً نمی‌توان به صورت دقیق به اطلاعات مرتبط با نحوه و چگونگی کارکرد هوش مصنوعی در این بخش‌ها دست یافت.

[1] Data Governance

ظهور ویروس کرونا در کنار همه آفت‌هایی که داشته است، فرصتی برای محک زدن قدرت و توانمندی کشورها در استفاده از ابزار راهبردی مدیریت هویت و دسترسی به جهت اعمال حاکمیت و مهار این بیماری بود. شاید اگر این اتفاق نمی‌افتاد، آشکار شدن نیازهای پنهان در حوزه مدیریت هویت و دسترسی، ماه‌ها و شاید سال‌ها به طول می‌انجامید. بدیهی است در دوران پسا کرونا، پیشرفت و بلوغ مدیریت هویت دیجیتال در فضای مجازی با سرعت و شتاب بیشتری ادامه خواهد یافت. دوران پسا کرونا ما را وارد دنیای جدیدی خواهد کرد که باید به هویت دیجیتال با رویکرد جدید و از زاویه جدی‌تری نگریسته شود.

دوران کرونا، شاید بهترین زمانی باشد که جوامع بیش از پیش به اهمیت هویت دیجیتال و مدیریت هویت و دسترسی پی برده باشند. در چنین بحران‌هایی باید بتوان به صورت چابک و در کمترین زمان ممکن به اطلاعات هویتی دسترسی پیدا کرد و بر آن اساس، ضمن احراز هویت، مشخص کرد کدام موجودیت (اعم از انسان و غیرانسان) در چه شرایط و موقعیتی به چه منابع اطلاعاتی و خدماتی دسترسی دارد و این کار با چه هدفی و برای چه مدتی انجام می‌دهد. بدیهی است این موضوع نیازمند رگولاتوری و قانون‌گذاری سریع و چابک است. این موضوع چابکی را در مرکز مفهوم مدیریت هویت و دسترسی قرار می‌دهد. بنابراین می‌توان موضوع مدیریت هویت و دسترسی چابک[1] را به عنوان یک موضوع نوین و در عین حال حیاتی در شرایط بحران (حتی شرایط دیگری که لزوماً بحرانی نیست) تعریف کرد و ابعاد و مؤلفه‌های آن را به ادبیات هویت دیجیتال افزود. مدیریت هویت و دسترسی چابک در عین حال نیازمند هوشمندی بیشتر و قابلیت تطبیق‌پذیری بالا در شرایط و موقعیت‌های گوناگون است.

۶- مراجع

Acuant. (2020). *Transacting with Trust During COVID-19 & Beyond: Online/Mobile Identity Verification*. Retrieved from Acuant: https://www.acuant.com/

Allison, I. (2020). *German Startup Pitches Decentralized ID for Prescription Pickup During COVID-19*. Retrieved from Coindesk: https://www.coindesk.com/

Beal, S. (2020). *The Role of Digital Identity in COVID-19*. Retrieved from OneWorldidentity: https://oneworldidentity.com/

Brumfield, C .(2020) .*New Coronavirus era surveillance and biometric systems pose logistical privacy problems*. CSOonline: https://www.csoonline.com/

[1] Agile Identity and Access Management

Davidson, H .(2020) .*China's coronavirus health code apps raise concerns over privacy*. TheGuardian: https://www.theguardian.com/

GlobaliD. (2020). *Why demand for digital identity is surging in the wake of COVID-19*. Retrieved from Medium - GlobaliD: https://medium.com/

Godbole, O. (2020). *Online Black Markets' Bitcoin Revenues Take a Hit Amid Pandemic*. Retrieved from Coindesk: https://www.coindesk.com/

Howat, E. (2020). *Jumio's free AI Verification Services for COVID-19 Relief*. Retrieved from Medium: https://medium.com/

Klimburg, A., Verhagen, P & ,.Mirtl, P. (2020) .*Pandemic Mitigation in the Digital Age Digital Epidemiological Measures to Combat the Coronavirus Pandemic. Austrian Institute for European and Security Policy* .Austrian Institute for European and Security Policy.

Lomas, N. (2020). *Online ID verification is seeing a spike in demand driven by COVID-19*. Retrieved from TechCrunch: https://techcrunch.com/

Mackintoshn , N. (2020) .*Are Your IAM Systems Up to the Challenge of COVID-19?* SecurityBoulevard: https://securityboulevard.com/

McDonald, S. (2020). *The Digital Response to the Outbreak of COVID-19*. Retrieved from Cigionline: https://www.cigionline.org/

Mozur, P & ,.Zhong, R .(2020) .*In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*. Nytimes: https://www.nytimes.com/

Rodgers, W. (2020). *UAE adopts digital identity and blockchain to fight COVID-19*. Retrieved from Shuftipro: https://shuftipro.com/

Sönmez, M. (2020). *How personal data could help contribute to a COVID-19 solution*. Retrieved from WEF: https://www.weforum.org/

Strielkowski, W. (2020) .*International Tourism and COVID-19: Recovery Strategies for Tourism Organizations* .Preprints.