

<http://doi.org/10.22133/MTLJ.2024.407318.1226>

Legal Challenges of Privacy Protection in Smart Cities considering International and Iranian law

Aramesh Shahbazi^{1*}, Sanaz Shabani Kolahi²

¹Associate Prof. Department of International Law, Faculty of Law and Political Science, Allameh Tabatabai University, Tehran, Iran.

²MA. Student in Communication Technology Law, Luigi Bocconi University, Milan, Italy.

Article Info	Abstract
<p>Original Article</p> <hr/> <p>Received: 17-06-2023</p> <p>Accepted: 28-11-2023</p> <hr/> <p>Keywords: Privacy International Legal Documents Internal Technology Law Smart Cities</p> <hr/> <p>*Corresponding author e-mail: a.shahbazi@atu.ac.ir</p>	<p>With the formation and development of the Internet of Things, the smart city has been manifested as an emerging concept that monitors various aspects of human life and intelligent information processing and control systems. A smart city can monitor the physical world and provide smart services for citizens, transform services such as healthcare, transportation, entertainment and energy and make them available to the government in a new way. The technologies used in smart cities raise some concerns and challenges regarding the security and privacy of citizens because applications in smart cities provide a wide range of information related to citizens' privacy. They collect to meet the interests and benefits of the public, but they also have comprehensive control over the city, and naturally, the lives of citizens will be affected by serious supervision and restrictions. In this article, we identified the international and domestic laws and regulations by investigating books and articles and using the available sources. We examined the laws and regulations in international law and Iranian law regarding privacy in smart cities. The study's most important finding is identifying gaps related to this area in Iranian laws and the need for more speed of updating laws at both the international and Iranian levels with the speed of advancement of technologies used in smart cities.</p>
<p>How to Cite: Shahbazi, A., & Shabani Kolahi, S. (2024). Legal Challenges of Privacy Protection in Smart Cities considering International and Iranian laws. <i>Modern Technologies Law</i>, 5(9), 221-234.</p>	<p>Published by University of Science and Culture https://www.usc.ac.ir Online ISSN: 2783-3836</p>



حقوق فناوری‌های نوین

<http://doi.org/10.22133/MTLJ.2024.407318.1226>

چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران آرامش شهبازی^{۱*}، ساناز شبانی کلاهی^۲

^۱ دانشیار، گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران.

^۲ دانشجوی کارشناسی ارشد حقوق فناوری ارتباطات، دانشگاه لوییجی بوکونی، میلان، ایتالیا.

چکیده

اطلاعات مقاله

با شکل‌گیری و توسعه اینترنت اشیا، شهر هوشمند در قالب انگاره‌ای نوظهور تجلی یافته است که بر جنبه‌های مختلف زندگی انسان و سیستم‌های کنترل و پردازش اطلاعات هوشمند نظارت دارد. یک شهر هوشمند قادر است دنیای فیزیکی را تحت نظارت قرار دهد و سرویس‌های هوشمندی برای شهروندان ارائه کند، سرویس‌ها و خدماتی مانند بهداشت و درمان، حمل‌ونقل، سرگرمی و انرژی را متحول سازد و به شیوه‌ای نوین در دسترس دولت قرار دهد. فناوری‌های استفاده‌شده در شهرهای هوشمند برخی نگرانی‌ها و چالش‌ها در باب امنیت و حفظ حریم خصوصی شهروندان را مطرح می‌کنند؛ زیرا برنامه‌های کاربردی در شهر هوشمند نه فقط طیف گسترده‌ای از اطلاعات مربوط به حریم خصوصی شهروندان را در راستای رعایت منافع و مصالح عموم جمع‌آوری می‌کنند، بلکه کنترل همه‌جانبه‌ای بر شهر دارند و طبعاً زندگی شهروندان را تحت‌تأثیر نظارت‌ها و محدودیت‌های جدی قرار خواهد داد. در این مقاله، با مطالعه کتاب‌ها و مقالات و به‌کارگیری منابع دردسترس به بررسی قوانین و مقررات در حقوق بین‌الملل و حقوق ایران در رابطه با حریم خصوصی در شهرهای هوشمند پرداخته است که مهم‌ترین یافته آن خلأهای موجود در این حوزه در حقوق ایران و فقدان تناسب سرعت به‌روزشدن قوانین در هر دو سطح بین‌الملل و حقوق ایران با سرعت پیشرفت فناوری‌های استفاده‌شده در شهرهای هوشمند است.

مقاله پژوهشی

تاریخ دریافت:

۱۴۰۱/۰۴/۲۵

تاریخ پذیرش:

۱۴۰۲/۰۹/۰۷

واژگان کلیدی:

حریم خصوصی
اسناد حقوقی بین‌المللی
حقوق فناوری داخلی
شهرهای هوشمند

*نویسنده مسئول

رایانامه: a.shahbazi@atu.ac.ir

نحوه استناددهی:

شهبازی، آرامش، و شبانی کلاهی، ساناز (۱۴۰۳). چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران. حقوق فناوری‌های نوین، ۵(۹)، ۲۲۱-۲۳۴.

ناشر: دانشگاه علم و فرهنگ <https://www.usc.ac.ir>

شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

مقدمه

امروزه عناصر گوناگون زندگی شهری تأثیر بسزایی در ابعاد اجتماعی و اقتصادی جوامع و تأثیرات محیطی بنیادینی در نحوه فرایند زیست شهری دارند. این مسئله با توجه به این نکته که در قرن بیست و یکم درصد شایان توجهی از جمعیت جهان از شهرنشینان تشکیل شده است، اهمیت ویژه‌ای می‌یابد. شهرها از اساس با چالش‌های پیچیده و گسترده‌ای مواجه‌اند که فقط از طریق رویکردی نظام‌مند حل‌شدنی هستند. از آنجاکه بسیاری از این راه‌حل‌ها برپایه به‌کارگیری فناوری‌های جدید، از جمله فناوری اطلاعات و ارتباطات مبتنی است، شهرهایی را که براساس این رویکرد عمل می‌کنند شهر هوشمند می‌نامند؛ بنابراین روی آوردن به شهر هوشمند نه فقط به منزله رویکردی مدرن و فناوریانه، بلکه راهبردی جدی برای چیرگی بر تهدیدها و چالش‌هایی همچون فقر، اختلاف طبقاتی، بی‌کاری، معضلات اجتماعی و کمبود انرژی حائز اهمیت است (روستایی و همکاران، ۱۳۹۷، ص ۹۸).

اما در کنار مشکلات که به محیط فیزیکی شهرها مربوط می‌شود، مسائلی نیز درباره شهروندان وجود دارند که اگر نگوئیم از اهمیت بیشتر، بی‌شک از اهمیتی برابر با چالش‌های محیطی برخوردارند. درنهایت شهروندان هستند که در شهری هوشمند مشغول به زندگی‌اند و هر یک از فناوری‌های استفاده‌شده تأثیراتی در زندگی افراد خواهد داشت. نباید از یاد برد که این فناوری‌ها - چه هر یک به تنهایی و چه مجموع آن‌ها در قالب ساختارهای فناوریانه شهرهای هوشمند - می‌توانند تأثیراتی مخرب در زندگی شهروندان داشته باشند که این تأثیرات باید شناسایی شوند و راهکارهای قانونی مناسبی برای کنترلشان به‌کار گرفته شود تا تعادل زندگی شهروندان در کنار فناوری‌های استفاده‌شده حفظ شود. در این تحقیق نیز مسئله اصلی شناخت چالش‌های مرتبط با حریم خصوصی است و این‌که آیا مقررات موجود بین‌المللی و قوانین و مقررات نظام حقوقی ایران پاسخ‌های مناسبی برای شناسایی و کنترل این چالش‌ها به‌دست می‌دهد یا خیر؟

یکی از مهم‌ترین چالش‌های موجود در شهرهای هوشمند که از ابتدای مطرح‌شدن این ایده همواره ذهن محققان و سیاست‌گذاران را به خود مشغول داشته، مسئله حریم خصوصی در قلمرو شهرهای هوشمند است. چنان‌که می‌دانیم، فناوری‌های استفاده‌شده به‌صورت گسترده‌ای داده‌های جمع‌آوری‌شده از طریق اینترنت اشیا را به‌کار می‌گیرند. این داده‌ها از زندگی شخصی افراد نیز با اهداف گوناگونی جمع‌آوری و حفظ می‌شوند. در برخی از مقالات (نیسن‌بام، ۱۳۸۱) به مسئله حریم خصوصی درباره فناوری پرداخته شده است؛ برای مثال در مقاله معینی‌فر و وحیدزاده (۱۴۰۰) حریم خصوصی درباره اینترنت اشیا بررسی شده و با تبیین چالش‌های عملی و نظری، پیشنهادهایی برای صیانت از حریم خصوصی افراد ارائه شده است. در این مقاله، به‌دنبال رویکرد گسترده‌تر شناخت جایگاه حریم خصوصی افراد در کلیت شهرهای هوشمند با تمامی ویژگی‌های آن هستیم، نه فقط بخشی از فناوری‌های به‌کاررفته در آن و پس از شناخت جایگاه حریم خصوصی و اهمیت آن، کارآمدی قوانین و مقررات در تنظیم‌گری و وضع قواعد مناسب برای کنترل چالش‌های حریم خصوصی و حفاظت از آن در سطح بین‌المللی و داخلی حقوق ایران مدنظر قرار می‌گیرد.

در مقاله حاضر، نخست به تاریخچه، مؤلفه‌ها و اهداف شهرهای هوشمند پرداخته می‌شود و در ادامه، چالش‌های حمایت از حریم عمومی و حفاظت از حریم خصوصی در شهرهای هوشمند، با توجه به مقررات ملی و بین‌المللی موجود در این زمینه، بررسی و درنهایت نیز حریم خصوصی در حقوق ایران مطالعه می‌شود.

۱. تاریخچه، مفهوم و مؤلفه‌های شهرهای هوشمند

۱-۱. پیشینه و تعریف شهرهای هوشمند

اصطلاح شهر هوشمند در جنبش رشد هوشمند ریشه دارد، جنبشی که در اواخر دهه ۱۹۸۰ و اوایل ۱۹۹۰ به وجود آمد و از سیاست‌های جدید برنامه‌ریزی شهری حمایت کرد (Harrison & Donnelly, 2012, p. 2). براساس رهیافت رشد هوشمند، تصمیم‌های توسعه‌ای در همه ابعاد زندگی شخصی و همچنین زندگی جوامع و ملت‌ها تأثیرگذار است (پورا احمد و همکاران، ۱۳۹۷، ص ۹). به‌منظور غلبه بر عوامل جانبی توسعه،

راهبردهای رشد هوشمند می‌تواند به حفظ و توسعه محیط‌های شهری سالم، ایمن، مناسب و جذاب کمک کند (Karadag, 2013). در واقع اساس و بنیان شهر هوشمند استفاده از فناوری‌ها، به‌خصوص فناوری اطلاعات و ارتباطات، برای بهبود وضعیت جامعه و حرکت به سمت آینده‌ای پایدار به کمک تعامل مسالمت‌آمیز بین اقشار مختلف جامعه، کسب‌وکارها، فناوری‌های مختلف، زیرساخت‌ها، مصرف انرژی و منابع و محیط زندگی است (Harrison & Donnelly, 2012, p. 4).

باین حال، به دلیل گستردگی فناوری‌هایی که می‌توانند در یک شهر استفاده شوند تا آن شهر یک «شهر هوشمند» محسوب شود، تعریف مشخصی از شهر هوشمند وجود ندارد. مارک دیکن، یکی از دانشمندان پیش‌رو در حمایت از پیشرفت‌های نوظهور علم و فناوری، شهرهای هوشمند را شهری تعریف می‌کند که از فناوری ارتباطات و اطلاعات^۱ برای برآورده کردن نیازهای شهروندان استفاده می‌کنند و در راستای تحقق این هدف، همکاری کلیه اقشار جامعه در این فرایند لازم است. در شهرهای هوشمند، از برنامه‌های موبایل برای دسترسی سریع به اطلاعات، کانال‌های ارتباطی و غیره استفاده می‌شود تا مردم کلیه امور خود را مانند اجتناب از ترافیک تا یافتن محلی برای پارک ماشین و گزارش وجود دست‌انداز یا یک جوی آب به طریقی هوشمند انجام دهند.

۱-۲. مؤلفه‌های شهرهای هوشمند

پیش‌تر گفته شد که تعریف مشخصی از شهر هوشمند وجود ندارد و با وجود این که مدت زیادی نیست که ایده شهرهای هوشمند در جهان گسترده شده است و دولت‌ها به اعمال آن اقدام کرده‌اند؛ باین حال چهارچوب‌ها و مؤلفه‌هایی را می‌توان برای آن تعریف کرد که البته این مؤلفه‌ها همه در عنصر محوری استفاده از فناوری اشتراک دارند؛ برای مثال طبق تعریف دینکن و حسام‌الور (2011)، فاکتورهای تحقق شهر هوشمند عبارت‌اند از:

- ۱) استفاده از طیف گسترده‌ای از فناوری‌های دیجیتال و الکترونیکی در شهر و جوامع آن؛
- ۲) استفاده از فناوری ارتباطات و اطلاعات برای بهبود محل زندگی و محیط کار در منطقه؛
- ۳) درونی‌سازی این دست فناوری ارتباطات و اطلاعات در سامانه‌های حکومتی؛
- ۴) منطقه‌ای کردن اعمالی که مردم و فناوری ارتباطات و اطلاعات را به‌منظور پرورش نوآوری و ارتقای دانشی که ارائه می‌دهند گردهم می‌آورد.

طبق سند اتحادیه اروپا نیز شهر هوشمند محصول همسویی سرمایه‌های انسانی، سرمایه‌های اجتماعی و زیرساخت فناوری اطلاعات و ارتباطات به‌منظور دستیابی به زندگی با کیفیت بالا و اقتصاد پایدار است (Manville, 2014, p. 11). در این راستا، ابعاد شش‌گانه هوشمندسازی شهرها عبارت‌اند از: ۱. حکمرانی هوشمند؛ ۲. جابه‌جایی هوشمند؛ ۳. محیط‌زیست هوشمند؛ ۴. زندگی هوشمند؛ ۵. شهروند هوشمند؛ ۶. اقتصاد هوشمند (پوراحمد و همکاران، ۱۳۹۷، ص ۱۵).

۲. چالش‌های امنیتی مربوط به حریم خصوصی

۲-۱. مفهوم و قلمرو حریم خصوصی

امروزه حریم خصوصی، به‌منزله اصلی بنیادین و اخلاقی، از اهمیت و جایگاه ویژه‌ای برخوردار است. از جمله اسنادی که تاحدودی به این موضوع و حقوق مربوط به آن اشاره کرده‌اند ماده ۱۲ اعلامیه جهانی حقوق بشر^۱، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی^۲، بیانیه تهران (1968)، دستورالعمل اتحادیه اروپا در خصوص حمایت از داده‌ها (1995)، مقررات عمومی حفاظت از اطلاعات GDPR (2016) که جایگزین قانون اخیر شده و کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های بنیادین در این زمینه است (انصاری، ۱۳۹۰).

با وجود اهمیت این حق بشری، ارائه تعریفی جامع از آن با دشواری‌های بسیاری مواجه است و به‌طور کلی ارائه تعریفی جامع و مانع از حریم خصوصی امری نسبی است؛ زیرا حریم خصوصی با توجه به شرایط اقتصادی، اجتماعی، فرهنگی و مذهبی از زمانی به زمانی دیگر و همچنین از جامعه‌ای به جامعه‌ای دیگر متفاوت است. به این دلیل، به‌منظور ارائه تعریفی از این مفهوم نیز باید گستره آن را منعطف در نظر گرفت تا توان انطباق با تغییرات را داشته باشد.

با این حال درباره‌ی حریم خصوصی تعاریف متعددی در اسناد مختلف و دکتترین ارائه شده است؛ از جمله تعریفی که در قطعنامه کنفرانس استکهلم^۳ در سال ۱۹۶۷ بیان شده است با این مضمون که «حق هر فرد بشر است که همان‌طور که قصد دارد زندگی بکند، حمایت شود در مقابل:

الف) هرگونه مداخله در زندگی خصوصی خانوادگی و داخلی او؛

ب) هرگونه تعرض به سلامت جسمی یا روحی و به آزادی اخلاقی یا معنوی او؛

ج) هرگونه تعرض به شهرت و شرافت او؛

د) هرگونه تفسیر مضری که از گفته‌ها و اعمال او بشود؛

ه) افشای بی‌موقع امور ناراحت‌کننده مربوط به زندگی خصوصی او؛

و) استفاده از اسم، هویت و عکس او؛

ح) هرگونه فعالیت به‌منظور جاسوسی درباره او، درک‌نشدن، او را تحت نظر قراردادن و عرصه را بر او تنگ کردن؛

ط) توقیف مکاتبات او؛

ی) استفاده سوء از مخابرات کتبی یا شفاهی او؛

ک) افشای اطلاعاتی که او داده یا گرفته شده، برخلاف قاعده حفظ اسرار مربوط به شغل و حرفه.

از جمله تعاریفی که در دکتترین وجود دارد می‌توان به این تعریف اشاره کرد که «حریم خصوصی از جمله حقوق اساسی افراد است و تمام افراد بشری صرف‌نظر از تابعیت، سن، اهلیت مدنی، توانایی ذهنی یا مقام از حریم خصوصی برخوردار هستند. حتی اشخاص حقوقی نیز به اعتبار این‌که در جامعه مانند اشخاص حقیقی فعالیت دارند از حریم خصوصی برخوردار می‌شوند» (رحمدل، ۱۳۸۴، ص ۱۲۴).

۱. زندگی خصوصی یا امور خانوادگی یا محل سکونت یا مراسلات کسی نباید در معرض دخالت خودسرانه واقع شود. نیز به حیثیت و حسن شهرت هیچ‌کس نمی‌توان حمله کرد. هرکس حق دارد در این گونه دخالت‌ها یا این‌گونه تجاوزها، از پشتیبانی قانون برخوردار باشد.

۲. هیچ‌کس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود؛ (۲) هرکس حق دارد در مقابل این‌گونه مداخلات یا تعرض‌ها از حمایت قانون برخوردار شود.

۳. Nordic Conference On The Right To Privacy؛ برای مطالعه متن کامل قطعنامه مراجعه کنید به:

<https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf> (last visited at 2021/ 03/ 30 at 17: 15)

به‌طور کلی در راستای تحقیق پیش‌رو «حریم خصوصی را می‌توان قلمرو زندگی هر شخص دانست که تمایل ندارد افراد دیگر بدون اذن و رضایت وی وارد آن محدوده شوند یا آن حوزه تحت کنترل و نظارت دیگران قرار گیرد» (شهبازی، ۱۳۹۵، ص ۴۲۰).

علاوه بر حریم خصوصی می‌توان «حق بر حریم خصوصی»^۱ را این‌گونه تعریف کرد: «حق داشتن یک چارچوب محافظت‌شده، امن و خالی از اغیار که در این چهارچوب، فرد از یک نوع خودمختاری شخصی برخوردار است.» منظور از برخورداری «از خودمختاری شخصی» نیز اعمال حاکمیت فردی در حوزه زندگی خصوصی به دور از قیدوبند، کنترل، فشار و محدودیت‌های قانونی و عرفی است (موسی‌زاده و مصطفی‌زاده، ۱۳۹۱، ص ۵۷).

با توجه به تعاریف مطروحه، مهم‌ترین مشخصه‌های حق خلوت و حریم خصوصی شامل «دور از انظار عموم بودن»، «آزادی» و «مصونیت» است که تمامی این مؤلفه‌ها ضروری و هریک از این سه مشخصه، لازم و ملزوم یکدیگرند (موسی‌زاده و مصطفی‌زاده، ۱۳۹۱، ص ۵۶).

بحث مهمی که درباره حریم خصوصی وجود دارد قلمرو آن است و این‌که آیا باید این حق بدون هیچ قیدوشرطی شناسایی شود یا خیر. در این رابطه می‌توان ابراز داشت که حریم خصوصی و حق بر آن نیز مانند بسیاری از حقوق و آزادی‌های دیگر اساسی است، اما امری مطلق و غیرقابل تحدید نیست، بلکه امری نسبی است؛ به این معنا که می‌توان آن‌ها را مقید و محدود ساخت. البته چنین محدودیت‌هایی مستلزم وجود شرایط معقول، معین و مشخص اعمال آن‌هاست (Solove, 2023, p. 979). مهم‌ترین سند بین‌المللی که به مسئله تحدید حقوق اساسی بشر پرداخته است ماده ۴ میثاق حقوق مدنی و سیاسی مصوب ۱۹۶۶ است. همچنین اسناد دیگری نیز به پیروی این مسئله را مدنظر خود قرار داده‌اند؛ مانند ماده ۱۵ کنوانسیون اروپایی حقوق بشر مصوب ۱۹۵۰ و ماده ۲۷ کنوانسیون آمریکایی حقوق بشر مصوب ۱۹۶۹. به‌طور کلی در یک جامعه دموکراتیک، حقوق بشر باید محدود و مقید شود (مشهدی و محمدلو، ۱۳۹۵، ص ۱۲۹)، اما این محدودیت شروطی دارد که با توجه به اسناد نامبرده به شرح ذیل است:

۱. محدودیت‌ها باید منطبق با قانون باشند؛

۲. باید از هدفی مشروع برخوردار و متناسب باشند؛

۳. محدودیت‌ها باید به اطلاع جامعه بین‌المللی برسند؛

۴. نباید موجب ایجاد تبعیض شوند؛

۵. نباید موجب این شوند که دیگر تعهدات دولت نقض شود.

بنابراین چنانچه مشاهده شد، در حقوق بین‌الملل بشر به مسئله حریم خصوصی به‌صورت گسترده پرداخته شده است که این مسئله نشان‌دهنده اهمیت آن در عرصه جهانی است. همین مسئله باعث می‌شود در مواجهه با پدیده‌های نوظهوری مانند شهر هوشمند بر خود واجب بدانیم که علاوه بر نگرانی‌ها و اقتضانات ملی و محلی، به مقررات و ملاحظات بین‌المللی نیز توجه کنیم؛ ازاین‌رو در بخش بعد به برخی از چالش‌های موجود در شهرهای هوشمند می‌پردازیم که در رابطه با حریم خصوصی وجود دارد.

۲-۲. تهدیدهای مربوط به حریم خصوصی در شهرهای هوشمند

فناوری‌های مدرن قلمرو نقض حریم خصوصی را گسترش داده و با چالش مواجه کرده است. این مسئله در شهرهای هوشمند، که از حجم وسیعی از فناوری‌های مدرن استفاده می‌کنند و عملکرد اصلی این‌گونه شهرها برپایه این فناوری‌هاست، بسیار حائز اهمیت است؛ به‌خصوص که این فناوری‌های استفاده‌شده در خدمات، شبکه‌ای گسترده را تشکیل می‌دهند و با یکدیگر ارتباط تنگاتنگی دارند.

شهبازی و شبانی کلاهی / چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران

معنی اجتماعی و متداول حریم خصوصی بیانگر مفهوم خصوصی بودن جنبه‌های محرمانه زندگی اشخاص، تحت کنترل بودن چهره اجتماعی توسط خود فرد و زندگی بدون دخالت اغیار است که با فضای مقتضی خود متناسب است و این امر به‌طور گسترده، چنانچه مشاهده شد، در بعد بین‌المللی نیز مورد توجه قرار گرفته است.

۲-۲-۱. حریم خصوصی در فضای سایبری

برای شناخت ویژگی‌ها و الزامات حریم خصوصی در شهرهای هوشمند باید ابتدا با مفهوم فضای سایبری (اینترنت) آشنا شد؛ زیرا فضای سایبری به‌صورت گسترده زیرساخت اصلی این شهرها را تشکیل می‌دهد و درحقیقت تصور شهر هوشمند بدون وجود فضای سایبری ناممکن است. فضای سایبری «محیطی است مجازی و غیر ملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به‌هم وصل می‌شوند) وجود دارد. در این محیط، تمامی اطلاعات مربوط به روابط افراد، ملت، فرهنگ‌ها و کشورها، به‌صورت ملموس و فیزیکی (به‌صورت نوشته، تصویر، اسناد و صوت) در یک فضای مجازی و به‌شکل دیجیتالی وجود دارد و در دسترس کاربران می‌باشد، کاربرانی که از طریق کامپیوتر و شبکه‌های بین‌المللی به هم مرتبط می‌باشند» (باستانی، ۱۳۸۶، ص ۳۶).

حریم خصوصی در فضای سایبری نیازمند تعریفی است که سنخیت بیشتری با خصوصیات و ویژگی‌های این فضا به‌طور عام و شهرهای هوشمند به‌طور خاص داشته باشد. از ویژگی‌های یک شهر هوشمند موفق این است که متناسب با ویژگی‌های هر فرد سرویس ارائه دهد. طبعاً ارائه این سرویس‌ها با استفاده از اینترنت است و همین مسئله باعث می‌شود که بتوانیم حریم خصوصی در فضای اینترنت را در ابعاد گسترده به شهرهای هوشمند مرتبط بدانیم؛ بنابراین لازمه شناسایی مفهوم حریم خصوصی در شهرهای هوشمند به‌دست آوردن درک درست از مفهوم حریم خصوصی در فضای سایبری است. حریم خصوصی در فضای سایبری را می‌توان این‌گونه شرح داد:

«وضعیتی که دسترسی غیرمجاز به یک کامپیوتر، شبکه و اطلاعات مربوطه، آگاهی، مداخله یا انتقال غیرمجاز اطلاعات و همچنین پردازش و آنالیز بدون مجوز آن‌ها را منع می‌کند. غیرمجاز بودن این اعمال می‌تواند به‌وسیله قانون، دستور قضایی یا اراده صاحب اطلاعات باشد» (Elmaghraby & Losavio, 2014, p. 493).

حریم خصوصی ناظر بر اطلاعاتی شخصی است که باید حفظ شود. در بند ۱ ماده ۴ مقررات عمومی حفاظت از اطلاعات (GDPR) اطلاعات شخصی افراد این‌گونه تعریف شده است: «اطلاعات شخصی به هر نوع اطلاعاتی که مربوط به یک شخص حقیقی شناخته‌شده یا شناخته‌نشده باشد گفته می‌شود. شخص حقیقی قابل شناسایی کسی است که می‌تواند به‌طور مستقیم یا غیرمستقیم به‌وسیله ارجاع به یک ممیزه مانند نام، شماره شناسایی، اطلاعات محلی، یک ممیز آنلاین یا یک یا بیشتر از یک فاکتور اختصاصی فیزیکی، روانی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی، که هویت آن شخص حقیقی است، شناخته شود.»

رعایت حریم خصوصی افراد در فضای سایبری به‌طور عام و به‌ویژه شهرهای هوشمند به‌دلیل ویژگی‌های آن و همچنین استفاده گسترده‌ای که از اینترنت و محیط‌های مجازی در آن می‌شود حق افراد شناخته می‌شود. حق رعایت حریم خصوصی، چنان‌که در بخش قبل گفته شد، در اسناد بین‌المللی بسیاری شناسایی شده است و اسناد محدودی نیز این حق را به‌طور ویژه در فضای سایبری شناسایی کرده‌اند؛ از جمله اصل پنجم «منشور حقوق بشر و اصول ناظر به اینترنت»^۱ که بیان می‌دارد:

«همه افراد حق برخورداری از حریم خصوصی آنلاین را دارند. این شامل عدم نظارت، حق رمزگذاری داده‌ها (اینکریپشن)^۲ و حق گمنامی آنلاین می‌شود. همچنین حق حفاظت از داده‌ها که شامل کنترل بر اطلاعات شخصی، نگه‌داری، پردازش، دفع و افشاست باید محترم شمرده شود.»

1. The Charter of Human Rights and Principles for The Internet
2. Encryption

۲-۲-۲. حریم خصوصی در شهرهای هوشمند

به‌طور کلی نگرانی‌های افراد درباره داده‌ها و حفظ حریم خصوصی ناظر به آن‌ها در شهرهای هوشمند شامل سه بعد اصلی می‌شود که عبارت‌اند از: «انواع اطلاعات جمع‌آوری‌شده»، «هدف از جمع‌آوری و استفاده از اطلاعات» و «انتقال داده‌ها» (Van Zoonen, 2016, p. 273).

الف) جمع‌آوری اطلاعات

همان‌طور که بیان شد، ارائه خدمات مستلزم دسترسی به اطلاعات شخصی افراد است که این مسئله چالش‌های بسیاری را درباره حریم خصوصی افراد در شهرهای هوشمند ایجاد می‌کند؛ زیرا این اطلاعات شخصی جامع از افراد می‌تواند تهدیدی علیه آن‌ها قلمداد شود. بسیاری از دوربین‌ها، سنسورها و دیگر دستگاه‌هایی که در این شهرها وجود دارند داده‌های مختلفی را جمع‌آوری می‌کنند و نظارت همه‌جانبه^۱ بر زندگی اشخاص بسیار گسترده بروز خواهد یافت؛ به‌همین منظور، باید در مرحله جمع‌آوری داده‌ها توجه کرد که چه شخصی برای چه مدتی و با چه هدفی از داده‌ها استفاده خواهد کرد.

به‌علاوه میل شدید و روزافزون کاربران برای آنلاین‌بودن و انجام کارهای شخصی خود در محیط مجازی و انحصار خدمات‌رسانی در اینترنت نیز از دیگر عوامل درخور توجه در شهرهای هوشمندند (فتحی و شاهمرادی، ۱۳۹۶، صص ۲۳۶-۲۳۸)؛ زیرا در بسیاری از موارد، افراد در وهله اول داده‌ها را در اختیار اشخاص دولتی و خصوصی قرار می‌دهند، اما در مواردی به این مسئله برخورد می‌کنند که چه کسی مالک داده‌هاست و تصمیم‌گیری درباره این مسئله باید در مرحله جمع‌آوری داده‌ها انجام شود؛ برای مثال در کشور هنگ‌کنگ بنابر برنامه‌ریزی‌های انجام‌شده ساخت یک پلنفرم بزرگ تحلیل داده‌ها توسط مقامات بیمارستان‌ها در راستای تسهیل پژوهش‌های مرتبط با خدمات پزشکی و بهداشتی شروع و سیستم اشتراک‌گذاری سوابق پزشکی، که از برنامه‌های حمایت از خدمات پزشکی هستند، پیش‌بینی شده است. این برنامه مستقیماً با اطلاعات خصوصی افراد در ارتباط است و تضمینات قانونی متناسب با این فضا برای رعایت حداکثری حریم خصوصی افراد با تهیه دستورالعمل‌هایی برای استفاده‌کنندگان از داده‌ها^۲ و کاربرانی که داده‌ها را در اختیار پلنفرم قرار می‌دهند^۳ در نظر گرفته شده است.

اینترنت اشیا یکی از اصلی‌ترین فناوری‌های استفاده‌شده در شهرهای هوشمند است و از دو منظر می‌تواند امنیت و حریم خصوصی را با خطر مواجه کند. این خطرات می‌توانند ناشی از حملات داخلی یا خارجی باشند. ضعف فناوری‌های مبتنی بر اینترنت اشیا ناشی از این است که این فناوری‌ها در ارتباطات کلیدی خود با شبکه و اتصالات باسیم و بی‌سیم، داده‌ها را جمع‌آوری می‌کنند و دیتایی که بارگزاری، پردازش و ذخیره شده است می‌توانند در معرض حملاتی با مداخله انسانی یا حملات ناشی از عدم سرویس‌دهی قرار گیرند (Ismagilova, 2020, p. 6). بنابراین، یکی از مواردی که می‌تواند درصد بالاتری از حریم خصوصی افراد در شهرهای هوشمند را تضمین کند تقویت زیرساخت‌های شهر هوشمند است؛ به‌خصوص اینترنت اشیا^۴ که زیربنای شهرهای هوشمند است و رسیدن به خدماتی مانند خانه‌های هوشمند، حمل‌ونقل هوشمند، اقتصاد هوشمند، محیط زیست هوشمند مستقیماً با آن در ارتباط‌اند. افزایش امنیت در سیستم و کاربرد اینترنت اشیا^۵ می‌تواند به استفاده مؤثر کاربران با حفظ امنیت شخصی آن‌ها بینجامد که درنهایت، نگرانی‌ها درباره حریم خصوصی مربوط به ابعاد فنی و زیربنایی شهرهای هوشمند، می‌توانند تا حد زیادی تأمین شوند (Abosag, 2019, p. 3).

1. Surveillance

2. Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals), (2016), Office of Privacy Commissioner for Personal Data, Hong Kong

3. Electronic Health Record Sharing System and Your Personal Data Privacy, (2016), Office of Privacy Commissioner for Personal Data, Hong Kong

4. The Internet of Things (IOT)

5. اینترنت اشیا ساختار شبکه‌ای مسئول گردآوری و پردازش داده‌ها را از سنسورهای توزیع‌شده و ابزارهای هوشمند فراهم می‌کند.

شهبازی و شبانی کلاهی/ چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران

ب) اهداف جمع‌آوری داده‌ها

هدف از جمع‌آوری داده‌ها باید کاملاً مشخص و واضح باشد. با توجه به داده‌های بسیاری که در شهرهای هوشمند وجود دارند، هر نهادی با توجه به نیاز خود می‌تواند بخشی از این داده‌ها را استفاده کند، اما اعلام اهداف جمع‌آوری داده‌ها به‌وضوح به‌عموم برای دریافت داده‌ها با رضایت کاربر مهم است.

یکی از مهم‌ترین هدف‌های جمع‌آوری داده‌ها در شهرهای هوشمند، بهبود خدمات است. داده‌های اشخاص برای افزایش کیفیت خدمات شهری مثل حمل‌ونقل، مصرف انرژی و دیگر خدمات استفاده می‌شوند، اما نکته مهم در این مسئله استفاده ثانویه از داده‌هاست مانند بازاریابی شخصی‌سازی شده (Fabrègue & Bogoni, 2023, p. 591). بنابراین استفاده متعادل از داده‌ها برای تأمین اطمینان شهروندان و به‌خطر نینداختن حریم خصوصی آن‌ها باید مدنظر قرار گیرد.

همچنین جمع‌آوری داده‌ها نباید با اهداف غیرقانونی و حقوق بشری باشد؛ برای مثال در برخی موارد جمع‌آوری داده‌ها با هدف شناخت ابعاد مختلف افراد صورت می‌گیرد تا براساس آن‌ها تبعیض‌هایی در ارائه خدمات صورت گیرد.

ج) انتقال داده‌ها

نگرانی‌های موجود درباره داده‌ها در شهرهای هوشمند در مبحث انتقال داده‌ها دارای دو بعد است: بعد اول ناظر به این مسئله است که کارکرد خدمات شهرهای هوشمند به جریان انتقالی هماهنگ داده‌ها از یک سیستم و شبکه به سیستم و شبکه‌ای دیگر وابسته است و بعد دوم، که در مقابل بعد اول است، ناظر به اتصال این سیستم‌ها و شبکه‌ها و انتقال داده‌ها در میان آن‌هاست که می‌تواند حریم خصوصی و امنیت افراد را به‌خطر اندازد (Ismagilova, 2020, p. 2).

همچنین انتقال داده‌ها می‌تواند با ماهیت ناشناخته ماندن در فضای مجازی در تضاد باشد. ناشناخته ماندن در راستای حفظ حریم خصوصی در فضای مجازی، که با فضای فیزیکی متفاوت است (قبولی درافشان و همکاران، ۱۳۹۷، ص ۱۱۵)، باید در زیرساخت‌های فناوری‌های شهرهای هوشمند مدنظر قرار گیرد؛ زیرا انتقال داده‌ها از یک مخزن داده به مخزنی دیگر ممکن است باعث شناسایی یک شخص شود. ممکن است در یک مخزن داده، اطلاعات موجود از یک شخص باعث شناسایی او نشود و نتوان اطلاعات خاصی را به شخص حقیقی منتسب کرد، اما انتقال همان داده به مخزن داده دیگر می‌تواند باعث تجمیع این اطلاعات مکمل و شناسایی شخص شود.

۳. مواجهه حقوق بین‌الملل با شهرهای هوشمند

با نگاهی به حقوق بین‌الملل در می‌یابیم که با وجود تلاش‌های نهادهای مختلف برای تنظیم مقررات مربوط به فناوری، همچنان در زمینه قواعد و استانداردهای ناظر بر ابعاد مختلف فناوری به‌صورت کلی و به‌صورت خاص در رابطه با امنیت و حریم خصوصی فناوری‌های نوین مانند اینترنت اشیا با کمبود و خلأ حقوقی مواجه است. در واقع حقوق بین‌الملل در جهانی که در آن فناوری با سرعتی چشمگیر در حال رشد است و این رشد و فراگیری تأثیرات مستقیم و غیرمستقیمی در ابعاد مختلف آن داشته نتوانسته است به‌صورت پویا و فعال همگام با رشد فناوری به شناخت و نظام‌مند کردن بخش‌های مختلف آن پردازد و فقط در بخش‌هایی از این حوزه اقداماتی به چشم می‌خورد.

درباره حق حریم خصوصی اسنادی موجود است که به حفاظت از این حق می‌پردازد و الزاماتی را بر دوش دولت‌ها و شرکت‌های خصوصی می‌گذارد از جمله ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷ میثاق جهانی حقوق مدنی و سیاسی، ماده ۸ کنواسیون اروپایی حقوق بشر، ماده ۱۶ منشور آفریقایی حقوق بشر و ماده ۸ منشور عربی حقوق بشر. مهم‌ترین اصلی که برای حفاظت حریم خصوصی افراد در این اسناد بیان شده اصل تناسب است؛ به این معنی که دولت‌ها باید در اعمال هر نوع محدودیتی که حریم خصوصی افراد را در معرض خطر قرار می‌دهد اصل

تناسب را مدنظر داشته باشند (Serwin, 2008, p. 876)؛ زیرا دولت‌ها ابزار اصلی سیاست‌گذاری بالادستی هستند و باید تناسب بین حفظ حریم خصوصی و دیگر حقوق بشری را براساس اصول پذیرفته شده همواره مدنظر داشته باشند.

سلسله قطعنامه‌های مرتبط با فناوری‌های ارتباطی و اطلاعاتی، که مجمع عمومی سازمان ملل متحد از سال ۱۹۸۱ تا ۲۰۱۹ دائم به تصویب رسانده‌اند، از جمله اقداماتی است که نهادی بین‌المللی برای بیان دغدغه‌ها، تحولات و چشم‌اندازهای مدنظر جامعه جهانی تهیه کرده است. در این قطعنامه‌ها، به اهمیت تأثیرات فناوری‌های اطلاعاتی و ارتباطی در تمامی دولت‌ها و لزوم توجه و همکاری دولت‌ها برای استفاده صحیح از این فناوری‌ها با توجه به امکان استفاده دوگانه از آن‌ها پرداخته شده است.

علاوه بر قطعنامه‌های مذکور، مجمع عمومی سازمان ملل متحد دو قطعنامه^۳ نیز درباره «حق بر حریم خصوصی در عصر دیجیتال» دارد که به ابعاد مختلف این حق و احترام به آن توسط نهادهای دولتی و خصوصی درون قلمرو دولت‌ها پرداخته است. همچنین شورای حقوق بشر به مسئله حقوق بشر در ارتباط با فناوری پرداخته است که ماحصل آن در دو قطعنامه پیوسته به نام «توسعه، حمایت و برخورداری از حقوق بشر در اینترنت»^۴ مکتوب و مستند شده است.

از معدود مواردی که آثار فناوری در سطح بین‌المللی برای کنترل و شناسایی مقررات مربوط به آن توسط یک سند سخت مورد توجه قرار گرفته است در حوزه حقوق بین‌الملل کیفری است. «کنوانسیون جرایم سایبری بوداپست»^۵، که درباره مقررات امنیتی مرتبط با فناوری است، یکی از اسناد تهیه شده در این حوزه است. همان‌طور که از نام آن نیز مشخص است، این کنوانسیون فقط درباره تقویت اجرای قانون جهانی برای موارد کیفری است، نه به‌صورت کلی درباره تمامی استانداردهای مورد نیاز این حوزه.

با توجه به مباحث پیش‌گفته در راستای فراگیری استفاده از فناوری در بخش‌های مختلف، جامعه بین‌المللی نیز ضرورت تنظیم روابط و وضع مقررات برای مواجهه صحیح و کنترل تأثیرات فناوری را دریافته و به‌خصوص برای صیانت از نظم بین‌المللی و حفظ صلح قدم‌هایی را در این عرصه برداشته است؛ هرچند نیازمند سرعت‌بخشیدن به این اقدامات و روزآمد کردن این مقررات است.

۴. نگاه قوانین ایران به حریم خصوصی در شهرهای هوشمند

در قوانین ایران نیز تاحدودی به مسئله حریم خصوصی پرداخته شده است؛ هرچند این بررسی به‌هیچ‌وجه با سطح پیشرفت فناوری متناسب نیست و همچنان بخش‌های ناشناخته بسیاری برای قانون‌گذار باقی مانده است. گفتنی است مهم‌ترین مسئله‌ای که از ساختار شهرهای هوشمند مورد توجه قانون‌گذار ایران قرار گرفته مربوط به جمع‌آوری داده‌هاست که البته این قوانین و مقررات به‌صورت عمومی درباره استفاده از فناوری ذکر شده و احکام اختصاصی مربوط به حریم خصوصی در شهرهای هوشمند نیستند.

اگر بخواهیم مبنایی اصولی برای حق افراد بر حریم خصوصی خود در حقوق ایران برشماریم، قاعده تسلیط گویاترین قاعده است. مطابق این قاعده، هر شخصی بر اموال خود مالکیت دارد و هیچ‌کس حق تصرف در اموال او را ندارد. براساس این قاعده، می‌توان این‌گونه نتیجه‌گیری کرد که وقتی انسانی بر اموال خویش - که با آن رابطه اعتباری دارد - اختیار و تسلط کامل دارد، به طریقی اولی بر نفس خویش، که تعلق آن امری حقیقی است، مسلط است (ابطحی و همکاران، ۱۴۰۱، ص ۸) سوای مبنای مشخص شده برای حفاظت از حریم خصوصی، در مواردی نیز قانون‌گذار مقرراتی را برای حمایت از داده‌های اشخاص پیش‌بینی کرده است.

1. A/RES/53/70
2. A/RES/74/29
3. A/RES/68/167 & A/RES/69/166
4. A/67/53 و A/69/53

۵. برای مطالعه متن کامل کنوانسیون مراجعه کنید به:

<https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> (last visited: 2021/03/30 at 16: 24)

شهبازی و شبانی کلاهی/ چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران

اصطلاح «اطلاعات» در ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات به صورت ضمنی به دو دسته عمومی و شخصی تقسیم می‌شوند. اطلاعات شخصی در بند ب ماده ۱ این قانون با عنوان اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور تعریف شده است. همچنین در بند ب ماده ۱ آیین‌نامه اجرایی این ماده نیز اطلاعات شخصی با مصادیق بیشتری به نسبت خود قانون تعریف شده‌اند.^۱

اما تعریف مهم‌تری که در این آیین‌نامه بیان شده تعریف «حریم خصوصی» است. حریم خصوصی در بند پ این‌گونه تعریف شده است: «قلمروی از زندگی شخصی فرد که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، واردشدن، نظاره‌کردن، شنود و دسترسی اطلاعات فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره‌شده خصوصی نظیر هتل و کشتی، همچنین آنچه که حسب قانون فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات.» در این تعریف، اصلی‌ترین معیاری که برای شناسایی حریم خصوصی افراد تعیین شده است اعلام و رضایت شخصی افراد است. در واقع اشخاص براساس وضعیت خود تعیین می‌کنند که می‌خواهند چه میزان اطلاعات و داده‌ها را در اختیار دیگران بگذارند و این امر را به طرق مختلف اعلان می‌کنند.

همچنین ماده ۵ قانون حمایت از آمران به معروف و ناهیان از منکر و تبصره آن نیز می‌تواند مبنایی برای شناخت حریم خصوصی در قوانین ایران قرار گیرند. در ماده ۵ ذکر شده است که اقدامات اجرایی امر به معروف و نهی از منکر نمی‌تواند باعث تعرض به حریم خصوصی افراد شود. در راستای مشخص کردن حدود حریم خصوصی در تبصره این ماده، قانون‌گذار بیان می‌کند: «اماکنی که بدون تجسس در معرض دید عموم قرار می‌گیرند، مانند قسمت‌های مشترک آپارتمان‌ها، هتل‌ها، بیمارستان‌ها و نیز وسایل نقلیه مشمول حریم خصوصی نیست.» از مفهوم مخالف تبصره مذکور می‌توان این‌گونه برداشت کرد که هر مکانی که نیازمند تجسس است و به راحتی در معرض دید عموم قرار ندارد مشمول حریم خصوصی می‌شود و بدین ترتیب، می‌توان مرزهای حریم خصوصی افراد را در محدوده فیزیکی شهرها تبیین کرد.

قوانین ذکرشده مهم‌ترین مواردی است که می‌توان در آن‌ها تعاریفی از حریم خصوصی را یافت و علاوه بر دو مورد مذکور، هرچند که در قوانین دیگر نیز مواردی درباره حریم خصوصی افراد ذکر شده، اما هیچ‌یک از قوانین موجود متضمن تعریف دقیقی از حریم خصوصی در فضای مجازی نیست.

معیار رضایت فرد برای جمع‌آوری اطلاعات خصوصی وی در منشور حقوق شهروندی نیز بیان شده است. در این منشور، ضمن این که محترم شمرده شدن حریم خصوصی حق هر شهروند شناخته شده، مصونیت تفتیش و بازرسی اماکن و وسایل شخصی افراد و همچنین ممنوعیت گردآوری، پردازش، به‌کارگیری و افشای اطلاعات و مراسلات افراد به صراحت بیان شده است و بر رضایت آگاهانه شخص برای استفاده از اطلاعات خصوصی وی تأکید شده است. هرچند منشور حقوق شهروندی مصادیق بسیاری از حریم خصوصی افراد را تعریف و مقرراتی برای حفاظت و حراست از آن پیش‌بینی کرده است، اما استثنایی که در این منشور برای نقض حریم خصوصی و اطلاعات شخصی بیان شده بسیار کلی است؛ این استثنا حکم قانون است. درحقیقت قانون‌گذار بدون هیچ شرایطی حق استفاده از اطلاعات خصوصی افراد را فقط با وضع قانون برای خود محفوظ نگه داشته است. این بیان کلی حکم قانون، با توجه به این که نوع قانون ذکر نشده و شرایط و مراتبی برای استفاده از آن در این منشور بالادستی مقرر نشده است، ممکن است خطراتی را برای حریم خصوصی افراد به همراه داشته باشد.

در قوانین دیگر، به صورت غیرمستقیم به حقوق افراد برای داشتن حریم خصوصی اشاره شده است و همچنین مسئولیت‌هایی برای پاسداشت این حق بر برخی از افراد تحمیل شده است؛ برای مثال اصل ۲۵ قانون اساسی که هرگونه تجسس در ارتباطات خصوصی افراد را

۱. اطلاعات مربوط به هویت، احوال شخصی، وضعیت فردی، عقاید و باورها، پست الکترونیکی، عکس و فیلم و صوت و تصویر و عادت‌های رفتاری و فردی از قبیل نام و نام خانوادگی، محل و تاریخ تولد، ازدواج، طلاق، مشخصات همسر، والدین و فرزندان، نسبت خانوادگی، ناراحتی‌های جسمی و روحی، شماره حساب بانکی و رمز عبور، محل کار و سکونت و همچنین اطلاعات شخصی مربوط به انجام امور تجاری، شغلی، تحصیلی، مالی، آموزشی، اداری، پزشکی و حقوقی.

ممنوع می‌داند. از جمله مسئولیت‌های پیش‌بینی شده برای نهادهای ارائه‌دهنده اطلاعات در ماده ۱۴ قانون انتشار و دسترسی آزاد به اطلاعات این است که چنانچه اطلاعات درخواستی مربوط به حریم خصوصی اشخاص باشد یا جزو اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود، اما در ماده ۱۵ استثنائاتی بر این اصل وارد شده است. استثنای مذکور در بند ج این ماده، درخواست اطلاعات توسط یک مؤسسه عمومی متقاضی با ارتباط مستقیم در چهارچوب وظایف قانونی وی را مجاز می‌شمارد. می‌توان به مورد اخیر این انتقاد را وارد کرد که مجوز افشای داده‌های شخصی بسیاری از افراد را به نهادهای مختلف داده است که نتیجه آن نقض حریم خصوصی افراد است و در نهایت، هدف اصلی حفظ حریم خصوصی به دست نمی‌آید.

نتیجه‌گیری

مسئله حریم خصوصی به دلیل وابستگی بسیار شهرهای هوشمند به داده‌های اشخاص در راستای بهبود کیفیت زندگی، چالش‌برانگیز است. اسناد بین‌المللی عام و خاصی مسئله حریم خصوصی را بررسی کرده‌اند، اما اقدامات قانونی و عملی در سطح بین‌المللی و چه بسا ملی تا به حال به دقت طرح مسئله صیانت از حریم خصوصی افراد را در شهرهای هوشمند تنظیم نکرده‌اند. منشور حقوق بشر و اصول ناظر به اینترنت و GDPR به مسئله امنیت داده‌های افراد پرداخته است که می‌توان اصول و قواعد آن را در بستر شهرهای هوشمند اجرا کرد تا به نگرانی‌هایی که عمدتاً ناشی از «انواع اطلاعات جمع‌آوری شده»، «هدف از جمع‌آوری و استفاده از اطلاعات» و «افراد دخیل در جمع‌آوری اطلاعات» است، پاسخ‌های شایسته‌ای داده شود و راهکارهایی به کار بسته شود تا با استفاده از بسترسازی حقوقی و فنی مناسب، به فضای اینترنتی امن‌تر و در نتیجه شهرهای هوشمند امن‌تری دست پیدا کرد و بتوانند از حقوق اساسی افراد، که حریم خصوصی مصداق مهم آن در شهرهای هوشمند است، حفاظت کنند. در سطح قوانین موجود در ایران، تا به حال به طور خاص قانونی درباره حریم خصوصی افراد در شهرهای هوشمند به تصویب نرسیده است؛ هر چند تلاش‌های اندکی صورت گرفته است که براساس آن‌ها تفکیکی بین اطلاعات شخصی افراد و دیگر اطلاعات انجام و روش‌های مراقبتی برای آن‌ها پیش‌بینی شده است؛ مانند مقررات قانون انتشار و دسترسی آزاد به اطلاعات یا منشور حقوقی شهروندی. همچنین مقرراتی وجود دارند که هر چند به طور خاص درباره حریم خصوصی افراد نیستند، اما می‌توان با استفاده از آن‌ها در مواردی به حفاظت از حریم خصوصی افراد اقدام کرد؛ مانند قانون اساسی.

نظام حقوقی هر جامعه باید توانایی آن را داشته باشد که همگام با فناوری حرکت کند. یکی از چالش‌های مشترک در حوزه بین‌المللی و همچنین حقوق داخلی ایران، عدم تناسب سرعت قانون‌گذار با پیشرفت فناوری است؛ بنابراین درباره نگرانی‌های مربوط به حریم خصوصی در شهرهای هوشمند باید ابزارهایی مانند قانون‌گذاری کارآمد را به کار بست تا افراد در عین بهره‌مندی از مزایای زندگی در شهرهای هوشمند و استفاده از فضای سایبر و محیط دیجیتال، از آثار زیان‌بار آن تا حد ممکن در امان باشند.

در راستای تحقیقات انجام‌شده، پیشنهادت زیر برای پرکردن خلأهای قانونی در نظام حقوقی ایران و متناسب‌سازی سرعت قانون‌گذار با پیشرفت فناوری با هدف ارائه خدمات به‌روز در راستای شهر هوشمند به ذهن نگارنده می‌رسد:

۱. ارائه سازوکار مناسب برای دریافت داده از کاربران براساس رضایت افراد و آگاه‌کردن اشخاص از حقوق خود در راستای حفاظت از حریم خصوصی در هنگام استفاده از خدمات؛
۲. تهیه دستورالعمل برای شرکت‌های ارائه‌دهنده خدمات در شهرهای هوشمند در راستای حفظ حریم خصوصی افراد؛
۳. تهیه استانداردهای فنی به منظور ارائه خدمات مطمئن با سطح امنیت بالا در برنامه‌های کاربردی؛
۴. الزام بخش خصوصی و دولتی به ارزیابی تأثیرات اقداماتشان بر حریم خصوصی در مراحل پیش از عملیاتی.

منابع

- ابراهیمی، مازیار و معرف، مریم (۱۳۹۷). توسعه پایدار شهری بر مبنای رشد هوشمند شهری تحلیلی بر مؤلفه‌ها، ویژگی‌ها و مزایای شهر هوشمند. نشریه علمی تخصصی شباک، ۴(۳۵)، ۳۹-۴۹.
- ابطحی، فاطمه، ابوطالب کوشا، مهدی منتظر قائم و میرشکاری، عباس (۱۴۰۱). حریم خصوصی در اماکن عمومی با تکیه بر حق تصویربرداری. مطالعات حقوق تطبیقی، ۱۳(۱)، ۱-۲۲.
- انصاری، باقر (۱۳۹۰). حقوق حریم خصوصی. تهران: سمت.
- باستانی، برومند (۱۳۸۶). جرایم کامپیوتری و اینترنتی، جلوه‌های نوین از بزهکاری. تهران: انتشارات بهنامی.
- پوراحمد، احمد، کرامت‌الله زیاری، حسین حاتمی‌نژاد و پشاه‌آبادی، شهرام پارسا (۱۳۹۷). تبیین مفهوم و ویژگی‌های شهر هوشمند. فصل‌نامه باغ نظر، ۱۵(۵۸)، ۵-۲۶.
- رحمدل، منصور (۱۳۸۴). حق انسان بر حریم خصوصی. مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران. ۷۰(۷)، ۱۱۹-۱۴۵. https://jflps.ut.ac.ir/article_12688.html
- روستایی، شهریور، پورمحمدی، محمدرضا و قنبری، حکیمه (۱۳۹۷). تئوری شهر هوشمند و ارزیابی مؤلفه‌های زیرساختی آن در مدیریت شهری موردشناسی: شهرداری تبریز. فصل‌نامه جغرافیا و آمایش شهری، ۸(۲۶)، ۱۹۷-۲۱۶.
- شهبازی، آرامش (۱۳۹۵). «لزوم رعایت حریم خصوصی - درمانی قربانیان کاربرد سلاح‌های شیمیایی جنگ عراق علیه ایران». فصل‌نامه مطالعات حقوق عمومی دانشگاه تهران، ۴۶(۲)، ۴۱۷-۴۴۰.
- فتحی، یونس و شاهمدرادی، خیراله (۱۳۹۶). گستره و قلمرو حریم خصوصی در فضای مجازی. مجله حقوقی دادگستری، ۸۱(۹۹)، ۲۵۲-۲۲۹.
- قبولی درافشان، سیدمحمد هادی، بختیاروند، مصطفی و آقامحمدی، اکرم (۱۳۹۷). حق فراموش شدن در ترازو: نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان؟. پژوهش حقوق عمومی، ۱۹(۵۸)، ۱۱۳-۱۳۵. <https://sid.ir/paper/225300/fa.۱۳۵-۱۱۳>
- مشهدی، علی و محمدلو، سجاد (۱۳۹۵). مطالعه تطبیقی مفهوم و معیار حق حریم خصوصی؛ رویکرد عرفی و فرهنگی. پژوهش‌های حقوق، ۲۰(۲)، ۱۲۵-۱۶۶.
- معینی‌فر، محدثه و وحیدزاده، دلارام (۱۴۰۰). الزامات استیفای حق بر حریم خصوصی در بستر اینترنت اشیا از منظر حقوق ایران. حقوق فناوری‌های نوین، ۳(۶)، ۶۱-۷۵. <https://doi.org/10.22133/MTLJ.2022.361434.1123>
- موسی‌زاده، ابراهیم و مصطفی‌زاده، فهیم (۱۳۹۱). نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی. فصل‌نامه بررسی‌های حقوق عمومی، ۱(۲)، ۴۵-۶۷.
- نیسن‌بام، هلن (۱۳۸۱). حمایت از حق خلوت آدمیان در عصر اطلاعات. ترجمه و تلخیص عباس ایمانی، پژوهش‌های حقوقی، ۱(۲)، ۱۷۱-۲۰۱.
- Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491-497.

- Fabrègue, B. F., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. *Smart Cities*, 6(1), 586-613. <https://doi.org/10.3390/smartcities6010027>
- Harrison, C., & Donnelly, I. A. (2011, September). A theory of smart cities. In *Proceedings of the 55th Annual Meeting of the ISSS-2011, Hull, UK*. <https://journals.iss.org/index.php/proceedings55th/article/view/1703>
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22. <https://doi.org/10.1007/s10796-020-10044-1>
- Karadag, T. (2013). *An Evaluation of the Smart City Approach*. (Master thesis, Middle East Technical University).
- Manville, C. (2014). Mapping Smart Cities in the EU. https://unece.org/fileadmin/DAM/hlm/prgm/urbandevt/Measuring_Progress__Achieving_Smarter_Cities_/Presentations/Catriona_Manville.pdf
- Serwin, A. B. (2008). Privacy 3.0-the principle of proportionality. *U. Mich. JL Reform*, 42, 869. Available at: <https://repository.law.umich.edu/mjlr/vol42/iss4/5>
- Solove, D. J. (2022). The Limitations of Privacy Rights. *Notre Dame L. Rev.*, 98, 975.
- Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472-480.