E-Government and Privacy (Challenges and Solutions)

Anas Abdolah Zadeh [1],Ali Hajipour Kandroud[2]
1. Master of Public Law, Urmia branch, Islamic Azad University, Urmia, Iran (corresponding author) anasabdollah@gmail.com
2. Assistant Professor, Department of Law, Urmia Branch, Islamic Azad University, Urmia, Iran. hajipour62@yahoo.com

Date Received 2021/09/08
Date of correction2022/1/7
Date of Release 2022/01/22

Abstract

E-government, with all its advantages in improving government processes, reducing costs, reducing bureaucracy, creating an e-community and facilitating communication with citizens, also has its weaknesses. The most important concern about the development and growth of e-government is the violation of citizens' rights in cyberspace. One of the most important citizenship rights in cyberspace is the right to information privacy. Information privacy is a right. The right that individuals have to control their information against misplaced searches, eavesdropping, spying, misappropriation and misuse of personal information. In this article, the concept and models of e-government are examined and the concept of citizens' information privacy and its relationship with e-government is stated. For citizens' information privacy in e-government, the challenge of information privacy and e-government maturity, the challenge of information privacy and public interest, the protection of information privacy and freedom of information and the challenge of granting citizens the right to access information in e-government are the most important challenges of this study. have been identified.

Key words: privacy, information privacy rights, citizen rights, e-government

[DOI: 10.52547/qjal.9.31.168]

فصلنامه حقوق اداری
سال نهم، تابستان ۱۴۰۱، شماره ۳۱
مقاله علمی پژوهشی

تحلیل چالش‌های دولت الکترونیک با حریم خصوصی اطلاعاتی شهروندان

انس عبداله‌زاده [۱] ؛ علی حاجی پور کندرود [۲]

تاریخ دریافت: ۱۴۰۰/۰۶/۱۷
تایخ پذیرش: ۱۴۰۰/۱۱/۰۲

چکیده

امروزه با پیشرفت‌های فناوری اطلاعات و ارتباطات علاوه بر مزایایی که در پی داشته، به‌طور فزاینده‌ای شهروندان را در معرض آسیب‌های ناشی از نقض حریم خصوصی اطلاعاتی‌شان توسط دیگران بالاخص سازمان‌های دولتی و غیر دولتی قرار داده است. دولت الکترونیک با تمامی مزایایی که در زمینه‌ی بهبود فرایندهای دولتی، کاهش هزینه‌ها، تقلیل بوروکراسی اداری، ایجاد جامعه‌ی الکترونیکی و تسهیل ارتباط با شهروندان دارد، دارای نقاط ضعفی نیز می‌باشد. مهم‌ترین نگرانی پیرامون توسعه و رشد دولت الکترونیک، همانا نقض حریم خصوصی شهروندان در فضای مجازی است. حقی که افراد برای کنترل اطلاعات خود در برابر جستجوهای نابجا، استراق سمع، تجسس، تصاحب و سوء استفاده‌هایی که ممکن است از اطلاعات شخصی‌شان شود، باید از آن برخوردار باشند. بر این اساس، در تحقیق پیش رو، مفهوم و مدل‌های دولت الکترونیک مورد بررسی قرار گرفته و مفهوم حریم خصوصی اطلاعاتی شهروندان و رابطه‌ی آن با دولت الکترونیک مورد تحلیل قرار گرفته است. باتوجه به تحقیقات بعمل آمده می‌توان چهار چالش ۱- چالش حفظ حریم خصوصی اطلاعاتی و تکامل دولت الکترونیک ۲- چالش حفظ حریم خصوصی اطلاعاتی و منافع عمومی ۳- حفظ حریم خصوصی اطلاعاتی و آزادی اطلاعات ۴- اعطای حق شهروند برای دسترسی به اطلاعات در دولت الکترونیک را به‌عنوان مهمترین چالش‌های حوزه‌ی حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک به شمار آورد و همچنین راهکارهایی برای رفع یا کم‌رنگ شدن آنها ارائه گردیده است و یافته‌های تحقیق حاضر که به صورت توصیفی، تحلیلی انجام شده است نشان از آن دارد. هدف از مقاله پیش رو ارائه راهکارهایی در ارتباط با چالش‌های دولت الکترونیک با حریم خصوصی اطلاعاتی شهروندان است.

واژگان کلیدی: امنیت، داده، دولت الکترونیک، حق حریم خصوصی اطلاعاتی، حقوق شهروندی، چالش‌ها.

۱. دانش آموخته کارشناسی ارشد حقوق عمومی، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران (نویسنده مسئول)
anasabdollah@gmail.com

۲. استادیار گروه حقوق, واحد ارومیه, دانشگاه آزاد اسلامی, ارومیه, ایران.
hajipour62@yahoo.com

[DOI: 10.52547/qjal.9.31.168]

مقدمه

دولت الکترونیک مفهومی نسبتاً جدید در ادبیات حقوقی کشور ماست که در آن مهم‌ترین رسانه ارتباطی بین مردم و دولت، اینترنت است. دولت الکترونیک همواره در پی استفاده از ICT برای ارائه خدمات عمومی به شهروندان، کسب وکارها و دیگر دولت‌ها می‌باشد و هدف نهایی آن بهبود بخشیدن به عملکرد سازمان عمومی، فراهم‌سازی و ارائه بهترین خدمات ممکن به ذینفعان (شامل شهروندان، کسب و کارها و دیگر دولت‌ها) می‌باشد، لذا افزایش بازدهی و تاثیرگذاری سازمان‌های عمومی، دو هدف اصلی دولت الکترونیک می‌باشد. گرچه در آغاز مفهوم الکترونیکی شدن به معنای اصلاح روابط و تعاملات درونی دولت بوده، اما با مرور زمان و به‌تدریج این مفهوم بر رابطه بین دولت و شهروندان تأثیر زیادی داشته و جایگزین روابط سنتی مابین دولت و مردم شده است. کارکردهای دولت الکترونیک را می‌توان در سه دسته کارکردهای خدماتی، اطلاعاتی و مشارکتی تقسیم کرد. ارائه خدمات الکترونیکی منجر بدان شده است که امروزه دولت‌ها جهت انجام امور خود به جمع‌آوری طیف وسیعی از اطلاعات شخصی و استفاده از آن‌ها بپردازند. در مقابل، این شبکه وسیع اطلاعات که در اختیار دولت‌ها قرار می‌گیرد، موجی از نگرانی‌ها را نسبت به حفظ حریم خصوصی در بین مردم ایجاد کرده است. چرا که این دسترسی امری یک سویه بوده و طرف مقابل (مردم) هیچ دخل و صرف و نقشی در آن ندارند. امروز اطلاعات شخصی تمام شهروندان در سیستم‌های اطلاعاتی بسیاری از نهادها و سازمان‌ها وجود دارد. جمع‌آوری داده در مورد افراد همیشه باعث مطرح شدن نگرانی‌هایی در زمینه‌ی حفظ حریم خصوصی آنها شده است. فناوری‌های آنلاین، نگرانی‌هایی را که از پیش پیرامون حفظ حریم خصوصی افراد وجود داشتند، دوچندان کرده‌اند؛ چرا که احتمالاً بدون اطلاع افراد، دسترسی سریع‌تر و ذخیره‌ی ساده‌تر مجموعه‌ی داده‌های بزرگتری را تسهیل می‌نمایند. هر چند، در تجارت الکترونیک، اغلب بنگاه‌های تجاری با مطرح نمودن مزایای ناشی از شخصی‌سازی و سفارشی سازی محصولات و خدمات، مشتری محور بودن و مزایای ناشی از آن برای مشتریان خود، مسائلی را که پیرامون حفظ حریم خصوصی اطلاعاتی مشتریان وجود دارد، به حاشیه می‌رانند، اما قدرتی که دولت در جمع‌آوری داده‌ها دارد، بسیار فراتر از سازمان های تجاری است و می‌تواند به خودی خود نوعی تجاوز به حریم خصوصی شهروندان تلقی گردد. آنچه حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک را با چالش مواجه می‌سازد، می‌تواند ناشی از قابلیت‌های دولت الکترونیک در جمع‌آوری و پردازش داده‌های شخصی شهروندان باشد. با توجه به اینکه برخورداری از حق حریم خصوصی اطلاعاتی یکی از مهمترین حقوق شهروندان در فضای مجازی محسوب می‌شود، سؤال اصلی و مساله مطروحه در پژوهش حاضر که بصورت توصیفی، تحلیلی انجام می‌شود این است که الکترونیکی شدن دولت چه تاثیری بر حفظ یا نقض حریم خصوصی شهروندان خواهد داشت و تقابل بین حریم خصوصی و دولت الکترونیک، چه چالش‌هایی را

[DOI: 10.52547/qjal.9.31.168]

ایجاد خواهد کرد؟ فرضیه نویسندگان آن است که دولت الکترونیک و مصادیق آن می‌تواند تا حدود زیادی حریم خصوصی شهروندان را خدشه‌دار نماید. اگر چه راه حل‌هایی نیز برای عبور از این چالش و یا کم رنگ کردن آن قابل ارائه می‌باشد. در این راستا در مقاله پیش رو پس از بیان مقدمات نظری بحث، مدل‌های دولت الکترونیک و چالش‌های آن با حریم خصوصی شهروندان مورد بحث و تحلیل قرار خواهد گرفت.

۱. مفاهیم

۱-۱. مفهوم دولت الکترونیک

"دولت الکترونیک" اصطلاحی است که در اواسط دهۀ ۱۹۹۰ مطرح شد و تاکنون تعاریف مختلفی از آن ارائه شده است. اما دو جنبه در تعاریف مختلف دولت الکترونیک مورد توجه بیشتر صاحب‌نظران قرار گرفته است: استفاده‌ی دولت از فناوری اطلاعات در راستای ارائه‌ی خدمات و اطلاعات بخش عمومی وکاهش شکاف میان مدیریت دولتی و شهروندان و افزایش سطح دسترسی شهروندان به خدمات دولتی (نمک‌دوست تهرانی، ۱۳۸۵: ۲۸). دولت الکترونیک عبارت است از استفاده از فناوری اطلاعات به طورکلی و تجارت الکترونیکی به طور خاص به منظور دسترسی آسان و مطمئن شهروندان و سازمان‌های اطلاعات و خدمات دولتی و ارائه خدمات دولتی به شهروندان، گروه‌های تجاری، تدارک‌کنندگان و کسانی که در بخش عمومی فعالیت می‌کنند (صرافی زاده،۱۳۸۳:۱۷۳).

در الگوی سنتی به کارگیری فناوری اطلاعات و ارتباطات در فعالیت‌های بخش عمومی، تأکید عمده بر خودکار کردن امور داخلی دولت بود، اما الگوی جدید به اموری فراتر از توجه صرف به اموراداخلی دولت می‌اندیشد (یعقوبی،۱۳۸۶:۲۵۴). براساس این الگو، سه کانون برای دولت الکترونیک در نظر گرفته می‌شود. ۱- بهبود فرایندها، اداره الکترونیکی ۲- برقراری ارتباط با شهروندان، شهروند الکترونیکی وخدمات الکترونیکی ۳- تعاملات بیرونی، جامعه الکترونیکی

الف) بهبود فرایندها (اداره‌ی الکترونیک): با بهره‌گیری از تجهیزات الکترونیکی و با هدف خودکارسازی فرایندها می‌توان به کاهش هزینه‌های فرایند، مدیریت عملکرد فرایند، برقراری روابط استراتژیک درون دولت و انتقال قدرت، اختیار و منابع از حالت فعلی فرایندها به حالت جدید آن دست یافت.

ب) ارتباط با شهروندان (شهروند الکترونیک و خدمات الکترونیک): دولت مشروعیت خود را از شهروندان کسب می‌کند. بنابراین باتواناسازی شهروندان و برقراری ارتباط با آنان به طرق الکترونیکی و حذف واسطه‌ها می‌تواند اطلاعات، فرم‌ها و خدمات را در اختیار آنها قرارداده و از پشتیبانی آنان برخوردار گردد.

[DOI: 10.52547/qjal.9.31.168]

ج) برقراری روابط بیرونی (جامعه‌ی الکترونیکی): با کمک فناوری اطلاعات و ارتباطات، خصوصاً اینترنت، دولت توانسته است در پاسخ به نیازهای شهروندان و سازمان‌ها در عصر دیجیتال، پاسخگوتر بوده، مردم‌سالارتر شده و درنهایت کاراتر گردد (یعقوبی،۱۳۸۶:۲۵۴).

تعامل میان دولت و شهروندان بدون مشارکت شهروندان معنایی ندارد؛ به عبارت دیگر، دولت الکترونیکی بدون مفهوم دموکراسی الکترونیکی مفهومی ناقص خواهد بود. بنا به تعریف سازمان همکاری و توسعه اقتصـــادی (OECD)، مشارکت الکترونیکی شهروندان، استفاده از فناوری‌های اطلاعاتی و ارتباطاتی برای پشتیبانی از تدارک اطلاعات برای شهروندان، مشورت با ایشان، و نیز مشارکت فعال آنان در تمامی مراحل چرخه سیاستگذاری شامل: خط مشی‌گذاری، تحلیل سیاست‌ها، ساختاردهی به سیاست‌ها، اجرای سیاست‌ها و نظارت و کنترل برنحوه‌ی اجرای سیاست‌ها می‌باشد (لوکیس و زنیاکیس، ۲۰۰۸:۳۱۳). از این تعریف می‌توان اینگونه استنباط کرد که مشارکت الکترونیکی می‌تواند سه بُعد داشته باشد: کسب اطلاعات، مشورت و مشارکت فعال که هریک می‌توانند پنج مرحله از سیاست‌گذاری را دربرگیرند. در اینجا مقصود از مشارکت فعال شهروندان فقط شرکت در رأی‌گیری‌های الکترونیکی نمی‌باشد، بلکه مقصـود شمول شهروندان در فرایندهای تصمیم‌گیری که از طریق آن سیاست‌های بخش عمومی بنا نهاده می‌شود. مشارکت، بنیادی‌ترین اصل دموکراسی اســت (براون و کیچر، ۲۰۰۴:۸۵) و یک دموکراسی موفق به‌وسیله‌ی شهروندان مشتاق و مطلع ساخته می‌شود. پشتیبانی عمومی از سیستم، سال‌ها به‌عنوان مشخصه‌ی کلیدی دموکراسی‌های موفق شناخته شده است (روزما و پاسکویسیوت، ۲۰۰۹:۲۵۴).

۲-۱. مدل‌های دولت الکترونیک

تاکنون چارچوب‌های مختلفی از دولت الکترونیکی مطرح شده است. سایموندز چهار فاز را برای دولت الکترونیک بر می‌شمارد: ارتباطات یک‌طرفه، ارتباطات دو طرفه، تبادل داده و اطلاعات و پورتال‌ها (ســایموندز، ۲۰۰۰:۱۲). واتســون و موندی (۲۰۰۱) مدلی را برای دولت الکترونیک پیشنهاد دادند که شـــامل سه بخش آغاز، انتشار و شخصی‌سازی می‌شد. این مدل‌های اولیه از دولت الکترونیکی بسیار ساده بوده و دربرگیرنده‌ی جنبه‌های پیچیده‌ی ارتباطی در دولت الکترونیک نمی‌شدند. یکی از اولین مدل‌های پیچیده‌ی دولت الکترونیک، مدل دفتر مدیریت و بودجه‌ی ایالات متحده‌ی آمریکا بود. این مدل چارچوب دولت الکترونیکی را مشتمل بر سه نوع رابطه می‌داند: ارتباط دولت با شهروندان (GC)، ارتباط دولت با کسب و کارها (GB) و ارتباط دولت با دولت (GG) (OMB۲۰۰). مدلی که در مقاله حاضر به‌عنوان چارچوب دولت الکترونیکی مطرح شده است، توسط تحقیقات چندی مورد تأیید قرار گرفته است (استیارت،۲۰۰۰؛ توماس و استریب، ۲۰۰۳؛ بلنگروهیلر، ۲۰۰۶) و مشتمل بر ۶ رابطه می‌باشد:

[DOI: 10.52547/qjal.9.31.168]

- مدل ارتباطی دولت با شهروندان- فرایند تحویل خدمات (۲GC یا GwIS): دراین مدل، دولت درصدد ایجاد روابط مستقیم با شهروندان با هدف تحویل خدمات تحت وب به آن‌ها می‌باشد. در این مدل ارتباطات به‌صورت تعاملی و دوطرفه بوده و شهروندان می‌توانند درخواست اطلاعات نموده و دولت به درخواست آنها پاسخ دهد.
- مدل ارتباطی دولت با شهروندان- فرایند سیاسی (GwIP): در این مدل مشارکت دادن شهروندان در فرایندهای سیاسی مدنظر است. در این مدل فرایندهای سیاسی همچون رأی‌گیری الکترونیکی تحت وب، ابراز عقاید و نظرات در فرم‌های وِبی یا بحث پیرامون سیاست‌های دولت از طریق ابزارهای اینترنتی همچون اتاق‌های گفتگوی مجازی، قرار می‌گیرند. این مدل را می‌توان به‌عنوان دموکراسی الکترونیکی درنظر گرفت.
- مدل ارتباطی دولت با کسب وکار به‌عنوان شهروند (GwBC): کسب وکارها اگرچه دقیقاً شهروند نمی‌باشند، اما می‌توانند از حقوق شهروندی همچون دسترسی به اطلاعات تجاری، آمارها و گزارشات دولتی، نرخ‌های تعرفه‌ی گمرکی و مواردی این‌چنینی برخوردار باشند. در این مدل همچنین امکان پرداخت مالیات به‌صورت تحت وب و نیز برخورداری از محیطی امن برای انجام تراکنش‌های مالی آنلاین برای کسب وکارها درنظر گرفته شده است.
- مدل ارتباطی دولت با کسب‌وکار در محیط بازار (GwBMKT): در این مدل، جدای از دریافت خدمات تحت وب که در مدل قبلی مطرح بود، تدارکات الکترونیکی توسط دولت برای کسب‌وکارها مطرح است.

در تدارکات الکترونیکی، کالاها و خدمات موردنیاز کسب‌وکارها توسط دولت الکترونیک فراهم می‌شود یا بالعکس.

مدل ارتباطی دولت با کارکنان (GwE): مصرف‌کننده‌ی بخش بزرگی از خدمات دولت الکترونیک، کارکنان دولت هستند. در این مدل، رابطه‌ی دولت با کارکنان در مدیریت منابع انسانی مطرح می‌شود. مدیریت منابع انسانی الکترونیکی همچون مسائل مربوط به حقوق و مزایای کارکنان، جبران خدمت و بازنشستگی، ارزشیابی عملکرد کارکنان، آموزش ضمن خدمت الکترونیکی، بخشنامه‌ها و دستورالعمل‌ها وغیره در این مدل مدنظر هستند.

مدل ارتباطی دولت با دولت (GwGor G2G): دراین مدل ارتباط میان دولت‌ها با سایر دولت‌ها و نهادهای بین‌المللی همچون سازمان ملل، سازمان بهداشت جهانی و غیره، به‌صورت الکترونیکی و مجازی مطرح می‌شود. تسریع در ارتباطات میان رؤسای‌جمهور، وزرای امور خارجه، دیپلمات‌ها، پارلمان‌ها و سایر نهادهای دولتی با یکدیگر در چارچوب سیاست‌های کلی هر دولت در این مدل ارتباطی از اهداف عمده می‌باشد. در این مدل همچنین ایجاد محیطی امن برای ارتباطات مجازی به

[DOI: 10.52547/qjal.9.31.168]

منظور جلوگیری از شـــنود اطلاعاتی مکالمات و ارتباطات بین طرفین از اهمیت زیادی برخوردار است.

۳-۱. مفهوم حریم خصوصی اطلاعاتی

حریم خصوصی جزء مفاهیمی است که تاکنون برای آن تعریفی جامع ارائه نشده است. وین فیلد که اولین مقالات را در حوزه‌ی حریم خصوصی تقریر کرده است، حریم خصوصی را «محرمانه بودن خصوصیات شخص یا مال او از انظار عموم» معنا کرده است (هارلو، ۱۳۸۳: ۱۶۳). محققان ابعادی را برای حریم خصوصی مطرح کرده‌اند: حریم خصوصی مکانی؛ حریم خصوصی جسمانی؛ حریم خصوصی شخصیت؛ حریم خصوصی خانواده؛ حریم ارتباطات شخصی؛ حریم لوازم شخصی؛ حریم خصوصی سازمانی. با توجه به ارتباط آخرین بعد حریم خصوصی با فناوری اطلاعات و دولت الکترونیک، در این نوشتار تنها حق حریم خصوصی مطرح است. (آلن وستین،۷:۱۹۶۷) «حریم خصوصی اطلاعاتی» را چنین تعریف کرده است: «حریم خصوصی اطلاعاتی عبارت است از مطالبه‌ای که افراد، گروه‌ها، یا نهادها در زمینه‌ی تعیین چگونگی و حد انتقال اطلاعات در مورد آنها به سایرین دارند». بنابراین، حریم خصوصی اطلاعاتی یک حق است. حقی که افراد برای کنترل اطلاعات خود در برابر جستجوهای نابجا، استراق سمع، تجسس، تصاحب و سوءاستفاده‌هایی که ممکن است از اطلاعات شخصی‌شان شود، دارند (فلوریدی، ۱۹۹۹: ۵۲) حریم خصوصی را «آزادی از دخالت‌های معرفت شناختی» معنا کرده است و هنگامی به‌دست می‌آید که محدودیت‌هایی درخصوص «حقایق» در مورد شخصی که «ناشناخته» است، وجود داشته باشد. برخی همانند تاوانی و جانسون معتقدند حریم خصوصی اطلاعاتی شامل داده‌هایی است درمورد فعالیت‌های روزانه، زندگی شخصی، امور مالی، تاریخچه‌ی سلامت و حتی موفقیت‌های دانشگاهی. از آنجایی که داده‌های شخصی افراد هم می‌تواند شامل داده‌هایی شود که مربوط به یک فرد بوده و در جایی ذخیره شده باشد و هم داده‌های مربوط به ارتباطات فرد (مثل ایمیل، مکالمات تلفنی، رسانه‌های ارتباطی بی‌سیم و...)، تمایزی میان حریم خصوصی اطلاعاتی و حریم خصوصی ارتباطاتی به‌وجود آمده است (تاوانی، ۲۰۰۸: ۹؛ جانسون ونیسنباوم، ۱۹۹۵: ۲۶۸-۲۶۲). از این رو، آن دسته داده‌های مربوط به مکالمات الکترونیکی با عنوان حریم خصوصی ارتباطاتی شناخته می‌شوند.

مفهوم حریم خصوصی اطلاعاتی با مفاهیم گردآوری و استفاده از داده‌های شخصی ارتباط نزدیکی دارد (رگان، ۱۹۹۵: ۶۹).

برخی محققان، درک مفهوم حریم خصوصی اطلاعاتی راوابسته به درک نحوه‌ی تغییر ماهیت حریم خصوصی اطلاعاتی در عصر دیجیتال و دوره‌ی ماقبل رایانه‌ها دانسته‌اند. تاوانی (۲۰۰۸: ۱۰) تأثیرگذاری عصر دیجیتال بر حریم خصوصی اطلاعاتی را در چهار جنبه معرفی کرده است:

[DOI: 10.52547/qjal.9.31.168]

(۱) حجم داده‌های شخصی در مورد یک شهروند که قابل گردآوری است: درعصر قبل از دیجیتال، حجم داده‌های شخصی که در مورد یک شهروند قابل گردآوری بود نیازمند صرف تلاش و هزینه‌ی زیادی بود؛ مثلافضای فیزیکی زیادی برای نگهداری داده‌های شخصی مورد نیاز بود و گردآوری آن‌ها نیازمند زمان زیادی بوده و مشکلات متعددی داشت. اما امروزه اطلاعات دیجیتالی که به صورت الکترونیکی در پایگاه‌های داده‌ی رایانه‌ای نگهداری می‌شوند، نه تنها فضای بسیار کمتری را می‌طلبند، بلکه گردآوری آنها مشکلات بسیار کمتری نسبت به عصر گذشته دارد.

(۲) سرعت انتقال داده‌های شخصی در مورد یک شهروند: سرعت انتقال داده‌های شخصی شهروندان، اشاره به سرعت انتقال داده‌های شخصی میان پایگاه‌های داده‌ی مختلف دارد. در عصر ماقبل دیجیتال، رکوردهای اطلاعاتی در مورد افراد باید بین ادارات مختلف یا مکان‌های نگهداری فایل‌ها، به صورت فیزیکی منتقل می‌شد؛ بنابراین سرعت انتقال و زمان مورد نیاز برای جا به جایی آنها بستگی به سیستم‌های حمل و نقل (هواپیما، قطار، کشتی، وسایل نقلیه موتوری و...) داشت. اما در عصر حاضر، رکوردهای اطلاعاتی شهروندان در کسری از ثانیه از طریق خطوط انتقالی سیمی یا بدون سیم و ماهواره‌ای، می‌توانند به پایگاه‌های داده‌ی مختلف منتقل شوند.

(۳) بازه‌ی زمانی که داده‌های شخصی شهروند قابل نگهداری است: درعصر ماقبل دیجیتال، مدت زمانی که افراد یا سازمان‌ها قادر به نگهداری داده‌های شخصی شهروندان بودند، بستگی به وجود فضای کافی برای نگهداری فایلها و آرشیوها داشت و بنا به مسائل فنی نمی‌شد، آنها را به صورت نامحدود نگهداری کرد. اما امروزه، نگهداری مقادیر ترابایتی از داده های شخصی شهروندان در فضای بسیار کم و برای مدت نامحدودی ممکن است.

(۴) نوع اطلاعاتی که درمورد یک شهروند می‌توان گردآوری کرد: درعصرماقبل دیجیتال، نوع اطلاعات شخصی که می‌شد از شهروندان گردآوری کرد بسیار محدود بود؛ چراکه بسیاری از فعالیت‌های روزمره زندگی افراد (مثل خریدهایی که انجام می‌دهند، سفرهایی که درطی یک سال می‌روند، عادات زندگی روزمره و...) عملاً برای سایرین مخفی بود. اما امروزه به راحتی می‌توان به عادات زندگی، خریدهای اینترنتی، سفرهای انجام شده، کوکی‌های اینترنتی و... درمورد یک شهروند پی برد.

حریم خصوصی مورد حمایت دولت الکترونیک است. اما این حمایت دارای اصول و استانداردهایی است که به‌صورت مختصر آنان را مورد بررسی قرار می‌دهیم.

۱-۳-۱. اصول مربوط به حقوق سوژه

الف ـ اصل شفافیت

براساس این اصل، موسسه مورد بحث باید اولاً در صورت تقاضا، امکان دسترسی اشخاص به محتوا، نوع، هدف گردآوری و سایر اطلاعات مربوط به داده‌های شخصی ایشان را فراهم آورده، ثانیاً باید

[DOI: 10.52547/qjal.9.31.168]

رویه خاصی برای حمایت از حریم خصوصی اطلاعاتی اشخاص داشته و آن را به نحو شفاف در دسترس کاربران قرار دهد. (رضایی زاده،۱۳۹۰:۱۵۰)

ب ـ اصل مشارکت

۱) حق دسترسی: به موجب این اصل موسسه دارنده داده‌ها می‌باید در صورت درخواست کاربری که داده‌های او تحصیل یا پردازش می‌شود (سوژه) امکان دستیابی او را به اطلاعات مربوط به نوع، ماهیت و روش گردآوری و احیاناً کیفیت داده‌های مزبور فراهم آورد.

۲) اصل امحاء: این اصل که از آثار اصل امنیت است، اقتضای آن را دارد که به محض برطرف شدن نیاز پردازشگر یا دارنده داده‌ها به آنها، نسبت به زائل نمودن و امحاء داده‌های مزبور اقدام نماید.

۳) اصل عدم انتقال: بر این اساس در بحث از حریم خصوصی اطلاعاتی یکی از اصول حاکم و بنیادین که در تمام مراحل، باید از سوی دارنده و پردازشگر داده‌ها رعایت شود، اصل ممنوعیت انتقال فرامرزی داده است. خصیصه فرامرزی و گیتی گستر بودن اینترنت و به‌طور کلی فناوری‌های اطلاعات و ارتباطات این امکان را فراهم آورده که اشخاص بتوانند از این ویژگی برای فرار از مقررات یک نظام حقوقی و یا تعقیب دستگاه‌های قضایی و امنیتی سوء استفاده کنند.

۲-۳-۱. اصول و استانداردهای حمایت از داده

تردیدی در لزوم حمایت از محرمانگی و امنیت داده‌های شخصی در فضای مجازی نیست. لیکن سؤال اساسی این است که ماهیت این حمایت چیست؟ و قواعد حقوقی مربوطه دقیقاً چه الزاماتی را به همراه دارند؟ برای پاسخ به این سؤال باید گفت که مجموعه الزامات و ضوابط حاکم بر مساله حمایت از داده (به‌ویژه در فضای مجازی) که صرف‌نظر از قوانین موجود در یک نظام حقوقی خاص قابل اعمال می‌باشند را اصول حاکم بر حمایت از داده می‌نامیم که در ذیل اشاره‌ای گذرا به هریک خواهیم داشت. این‌ها مبین اصول لازم‌الرعایه در عرصه حمایت از حریم خصوصی می‌باشند.

الف ـ اصول مربوط به جمع‌آوری داده

۱) اصل تحصیل قانونی و منصفانه: مطابق این اصل تحصیل داده‌های شخصی مربوط به دیگری می‌باید از طریق روش و ابزار قانونی و مشروع صورت گیرد. (رضایی زاده،۱۳۹۰:۱۲۱)

۲) اصل تحصیل محدود و مرتبط: به‌موجب این اصل اولاً تحصیل داده‌ها تنها برای هدف قانونی و مشروع مجاز است یا لااقل می‌توان گفت تحصیل داده‌ها برای هدف غیر قانونی یا نامشروع ممنوع است. ثانیاً نوع داده‌های گردآوری شده باید با هدف اولیه تحصیل داده‌ها منطبق باشد. ثالثاً گردآوری داده‌ها باید تنها به میزان مورد نیاز برای هدف اولیه و اعلام شده صورت گیرد و گردآوری داده‌های اضافه بر نیاز ممنوع است. (یعقوبی، ۱۹:۱۳۸۸)

[DOI: 10.52547/qjal.9.31.168]

۳) اصل انتخاب: اصل انتخاب بدان معناست که موسسه یا شخصی که قصد گردآوری داده‌ها در خصوص شخص سوژه را دارد، پیش از هر چیز می‌باید این امکان را برای کاربر فراهم آورد که صراحتاً نظر خود را مبنی بر اینکه آیا با گردآوری داده‌های شخصی خود موافقت دارد یا خیر؟ اعلام نماید.

۴) اصل اطلاع: مفهوم اصل اطلاع آن است که گردآوری و پردازش داده‌های شخصی حداقل در خصوص پردازش‌های تغییر دهنده داده منوط به اعلام مراتب به شخص سوژه می‌باشد، مگر در مواردی که قانون بنا به پاره‌ای مصالح استثنایی و مصرح همچون مسائل امنیتی خلاف آن را مقرر دارد. (رضایی زاده،۱۳۹۰:۱۲۳)

ب ـ اصول مربوط به نگهداری و پردازش داده

۱) اصل پردازش مرتبط یا محدودیت استفاده: براساس این اصل گردآورنده و پردازشگر داده‌ها، تنها اجازه پردازش داده‌ها را در حدود مورد توافق یا مورد اجازه قانونگذار دارد و باید از پردازش آنها برای اهداف غیر مرتبط و ثانویه خودداری کند.

۲) اصل ممنوعیت افشاء: براساس این اصل افشاء داده‌ها به اشخاص ثالث و به‌منظور نیل به یک هدف ثانوی، امری است که علی‌الاصول در چارچوب اجازه اولیه صادره از سوی سوژه یا قانونگذار نمی‌گنجد و لذا ممنوع است. این اصل در تمامی مراحل تحصیل پردازش و انتقال داده‌ها الزام‌الرعایه می‌باشد. (رضایی زاده،۱۳۹۰:۱۲۳).

۲. مخاطرات دولت الکترونیک درنقض حریم خصوصی شهروندان

چهار قابلیت دولت الکترونیک که ممکن است موجب خدشه‌دار شدن حریم خصوصی اطلاعاتی شهروندان شود، را می‌توان به شرح ذیل برشمرد:

۲-۱. گردآوری سریع‌تر و ساده‌تر داده‌ها: در دولت الکترونیک، امکان ثبت کوکی‌ها، گزارش‌ها، آدرس‌های آی پی یا وب‌سایتهای بازدید شده توسط شهروندان، به‌راحتی به‌وجود می‌آید و این امر می‌تواند حریم خصوصی اطلاعاتی شهروندان را خدشه‌دار سازد (بلنگر و هیلر، ۲۰۰۶: ۵۴).

۲-۲. گردآوری داده‌های بزرگ: یکی از مهم‌ترین مسائلی که می‌تواند موجب خدشه‌دار شدن حریم خصوصی اطلاعاتی شهروندان شود، چالش "داده‌های بزرگ" است (ماگرت و سوتکلیف ۲۰۱۲: ۱۳۹). حجم عظیم داده‌هایی که شهروندان به طور خودخواسته برروی وبلاگ‌ها، سایت‌ها و شبکه‌های اجتماعی قرار می‌دهند، به صورت مقادیر ترابایتی درآمده که امکان مطالعه‌ی نگرش‌ها، رفتارها و سبک‌های زندگیشان را به دولت‌ها که به‌راحتی به این حجم داده‌ها دسترسی دارند می‌دهد. همچنین، مطالعه‌ی نحوه‌ی رشد و گسترش جریان‌های سیاسی با استفاده از داده‌کاوی چنین داده‌های بزرگی، به‌راحتی ممکن می‌گردد. نمونه‌ای از چنین نقض آشکار حریم خصوصی افراد، می‌تواند تحلیل نحوه‌ی پیوستن جوانان در کشورهای عرب‌زبان به جریان "بهار عربی" در سالیان

[DOI: 10.52547/qjal.9.31.168]

اخیر باشد، که منجر به دستگیری‌های گسترده آنان توسط دولت‌های خودکامه برخی کشورهای عربی شد (لیندگرن، ۲۰۱۳: ۲۰۷).

۳-۲. ادغام داده‌ها: ادغام یا تجمیع داده‌ها به این موضوع اشاره دارد که سازمان‌های دولتی، با وجود اینکه به ظاهر جدا از هم هستند، اما به راحتی می‌توانند به تلفیق داده‌های شهروندان پرداخته و پایگاه‌های داده‌ای به‌وجود آورند که تمامی اطلاعات ثبت شده‌ی شـهروندان در پایگاه‌های داده پراکنده، در سـازمان‌های دولتی مختلف را در خود جای دهد. به عنوان مثال، سازمان امور مالیاتی می‌تواند به داده‌های سازمان ثبت احوال، بانک‌ها، سازمان ثبت اسناد، شهرداری و غیره دسترسی پیدا کرده و با کد یکتایی همچون کدملی شهروندان، پایگاه داده یا انبار داده‌ای به‌وجود آورد که به اصطلاح داده‌های آنها را در خود تلفیق کرده است. تصور اینکه داده‌های پراکنده و ناقص شهروندان توسط یک سازمان دولتی از پایگاه‌های داده متفاوت گردآوری شده و به‌یک‌باره دریک انبار داده‌ی واحد قرار گیرد، نگرانی‌های بسیاری در مورد حفظ حریم خصوصی اطلاعاتی شهروندان به‌وجود می‌آورد (بلنگروهیلر، ۲۰۰۶: ۵۵).

٤-۲. جمع‌آوری مخفیانه‌ی داده‌ها: پس از سـال ۲۰۱۳ و افشـاگری‌های ادوارد اسـنودن، کارمند سـابق آژانس امنیت ملی امریکا، مشخص شد که برخی دولت‌های غربی، خصوصاً ایالات متحده آمریکا، سال‌هاست که به‌صورت مخفیانه اقدام به جمع‌آوری داده‌های شخصی شهروندان یا استراق سمع تلفنی و اینترنتی از شهروندان کرده‌اند. وی اسنادی را منتشر کرد که نشان‌دهنده جزئیات تلاش گسترده‌ی آژانس امنیت ملی آمریکا برای جاسوسی اینترنتی از شهروندان آمریکا و سایر کشورهاست (گرینوالد، ۲۰۱۴:۲۱۵). همچنین جولیان آسانژ در سایت ویکی لیکس نیز اسناد زیادی را در زمینه‌ی تلاش سازمان‌های جاسوسی همچون سی. آی. ای. آمریکا و برخی دولت‌ها، خصوصاً در کشورهای غربی، برای دسترسی به اطلاعات شخصی شهروندان، منتشر کرده است (پویتراس، روزنباخ و استارک،۲۰۱۳).

۳. چالش‌های حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک

در این تحقیق، چهار چالش عمده برای حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک شناسایی و معرفی شده است: (الف) چالش حفظ حریم خصوصی اطلاعاتی شهروندان و تکامل دولت الکترونیک؛ (ب) چالش حفظ حریم خصوصی اطلاعاتی و منافع عمومی؛ (ج) حفظ حریم خصوصی اطلاعاتی و آزادی اطلاعات؛ و (د) چالش حق شهروند برای دسترسی به اطلاعات در دولت الکترونیک.

[DOI: 10.52547/qjal.9.31.168]

۱-۳. چالش حفظ حریم خصوصی اطلاعاتی شهروندان و تکامل دولت الکترونیک

با نگاهی به ادبیات نظری دولت الکترونیک چنین به‌نظر می‌رسد که تاکنون مدلی نسبتاً جامع از دولت الکترونیک که مورد قبول جامعه‌ی علمی و نهادهای بین‌المللی تحقیقاتی باشد، توسعه پیدا نکرده است. نکته‌ی مهم دیگر این است که در هیچ یک از مدل‌های توسعه‌ی دولت الکترونیک، جایی برای حفظ حریم خصوصی اطلاعاتی شهروندان درنظر گرفته نشده است (تقوی فرد و دیگران ۱۳۹۵). شاید یکی از دلایل این امر این باشد که نگاه محققان به جنبه‌های اصلی توسعه‌ی دولت الکترونیک بوده و با توجه به نوظهور بودن مفهوم دولت الکترونیک، مسائل تحقیقاتی که در دولت الکترونیک به آنها پرداخته نشده است باز باقی مانده و تحقیقات بیشتری در آن زمینه‌ها موردنیاز است. توسعه‌ی دولت الکترونیک مزایای زیادی برای دولت و برای سایر ذینفعان (همچون شهروندان، بنگاه‌های تجاری و...) در پی دارد.

از مهمترین منافع توسعه‌ی دولت الکترونیک برای دولت می‌توان به کاهش هزینه‌ها، کاهش کاغذبازی‌های زائد، افزایش اثربخشی و بهره‌وری و نیز افزایش سرعت انجام فرایندها اشاره کرد. مهم‌ترین منافع توسعه‌ی دولت الکترونیک برای شهروندان عبارتند از: دریافت سریع‌تر خدمات دولتی با هزینه‌ی کمتر و به‌صورت شفاف‌تر، دسترسی سریع و آسان به اطلاعات و خدمات مورد نیاز، کاهش پیچیدگی‌های بوروکراتیک اداری و توانایی اثرگذاری بیشتر برفرایندهای حکمرانی و سیاسی و داشتن جامعه‌ای مردم‌سالارتر با استفاده از ابزارهای الکترونیکی. تمامی این مزایا می‌تواند توجیه‌کننده‌ی توسعه‌ی هرچه بیشتر دولت الکترونیک باشد. اما توسعه‌ی بدون ضابطه‌ی دولت الکترونیک می‌تواند موجب نگرانی شهروندان در خصوص حفظ حریم خصوصی اطلاعاتی آنها باشد؛ چراکه با توسعه ی دولت الکترونیک، مرزهای میان سازمان‌های دولتی که قبلاً مجزا بوده و اطلاعات شخصی شهروندان را در اختیار دارند، کمرنگ‌تر شده و امکان دسترسی سازمان‌های دولتی دیگر به اطلاعات شخصی شهروندان بیشتر می‌شود؛ و این موضوع به معنای افزایش احتمال نقض حریم خصوصی اطلاعاتی شهروندان است (جمشیدی، ۱۳۹۶).

ارتباط میان توسعه‌ی دولت الکترونیک (یا تکامل آن) و حفظ حریم خصوصی اطلاعاتی شهروندان معکوس بوده و هرچه سطح بلوغ دولت الکترونیک بالاتر رود، احتمال نقض حریم خصوصی اطلاعاتی شهروندان بیشتر می‌شود. به عنوان مثال، در مراحل ابتدایی توسعه‌ی دولت الکترونیک، دولت الکترونیک کمترین تعامل را با شهروندان داشته و ارتباط دولت با شهروند بیشتر یک طرفه است؛ به‌طوری که برخی اطلاعات بر روی سامانه‌های دولت الکترونیک به صورت ایستا در اختیار شهروندان قرار می‌گیرد. در این مراحل به این دلیل که حجم داده‌های شخصی گردآوری شده‌ی شهروندان توسط دولت ناچیز یا بسیار اندک است، کمترین امکان نقض حریم خصوصی اطلاعاتی شهروندان به‌وجود می‌آید؛ در مرحله‌ی سوم استقرار دولت الکترونیک (مرحله‌ی تعاملی)،

[DOI: 10.52547/qjal.9.31.168]

امکان گردآوری داده‌های شخصی شهروندان به صورت برخط به‌وجود می‌آید. در این مرحله گردآوری داده‌های شخصی از خود شهروند انجام می‌گیرد و شهروند با مراجعه به سامانه‌ی دولت الکترونیک داده‌های شخصی را در فرم‌های الکترونیکی ثبت می‌کند. بنابراین امکان نقض حریم خصوصی اطلاعاتی شهروندان از سه نظر به وجود می‌آید: گردآوری، استفاده و نگهداری غیرمجاز آنها. به‌عنوان مثال، درصورتی که در هنگام گردآوری داده‌های شخصی به شهروندان اطلاعات کافی در خصوص اهداف گردآوری ارائه نشده باشد، یا استفاده از داده‌های شخصی توسط سازمان مربوطه با اهداف اولیه متناسب نباشد یا حتی نگهداری داده‌های شخصی بیش از مدت زمان مورد نیاز برای اهداف گردآوری انجام شده باشد، احتمال نقض حریم خصوصی اطلاعاتی شهروندان می‌رود. مرحله‌ی چهارم استقرار دولت الکترونیک (تراکنش)، بسیار به مرحله‌ی سوم شباهت دارد، با این تفاوت که در این مرحله تراکنش‌های مالی شهروندان به انجام می‌رسد؛ بنابراین در این مرحله هم امکان نقض حریم خصوصی اطلاعاتی شهروندان به خاطر گردآوری، استفاده یا نگهداری غیرمجاز یاغیرقانونی وجود دارد. علاوه بر این موارد، امکان نقض حریم خصوصی اطلاعاتی شهروندان به خاطر افشای غیرمجاز یا ناخواسته آن‌ها بنا به دلایلی ناشی از مسائل مرتبط با امنیت اطلاعات (همچون سرقت اطلاعات حساس مالی در حین تراکنش مالی اینترنتی یا هک‌شدن سامانه‌های دولت الکترونیکی و سرقت هویت شهروندان) به‌وجود می‌آید. در مرحله‌ی آخر استقرار دولت الکترونیک (یکپارچگی)، بیشترین امکان نقض حریم خصوصی اطلاعاتی شهروندان به وجود می‌آید؛ چرا که مرزهای موجود میان سازمان‌های دولتی کمرنگ شده و سازمان‌های دولتی به راحتی قادر به دسترسی به داده‌های شخصی شهروندان که در اختیار سایر سازمان‌های دولتی قرار دارد، هستند. بنابراین علاوه بر مسایل ناشی از سطوح بلوغ قبلی (مثل گردآوری داده‌های شخصی از شهروند، استفاده یا نگهداری غیرمجاز یا افشای داده‌های حساس مالی ناشی از مسائل امنیتی)، گردآوری غیرمجاز داده‌های شخصی بدون آگاهی شهروند از سازمان دولتی دیگر و افشای داده‌های شخصی به سازمان‌های دولتی یا غیردولتی فراتر از اهداف اولیه‌ی گردآوری مسئله‌ساز است. به مثال عنوان، یک سازمان می‌تواند بدون آگاهی شهروند داده‌های شخصی وی را که بر روی پایگاه‌های داده‌ی سازمان دولتی دیگری ذخیره شده است، گردآوری کند. همچنین داده‌های شخصی شهروندان می‌توانند به سازمان‌های متعدد داخلی یا خارجی افشا شوند (جمشیدی، ۱۳۹۶).

چالش مطرح شده موجب تار شدن اعتماد شهروندان به دولت الکترونیک شده است؛ بنابراین راهکاری که برای این چالش پیشنهاد می‌شود این است که قانونگذاری و سیاستگذاری حقوق شهروندی در دولت الکترونیک پیش از اقدام به اجرایی‌سازی و استقرار دولت الکترونیک صورت گیرد.

[DOI: 10.52547/qjal.9.31.168]

برای حفظ حریم خصوصی اطلاعاتی شهروندان اصولی پیشنهاد شده است. برخی از این اصول عبارت‌اند از اصول (HEW)[1]، اصول (APEC)[2]، اصول (OECD)[3]، اصول بندرگاه ایمن و غیره. تفاوت‌ها و هم‌پوشانی‌هایی میان اصول پیش گفته وجود دارد. آن‌ها که اغلب شامل ۱۰ اصل می‌شوند، به‌عنوان اصول زیربنایی حفظ حریم خصوصی و تصویب قوانین حفاظت از حریم خصوصی اطلاعاتی در کشورهای پیشرفته شناخته می‌شوند.

۲-۳. حریم خصوصی اطلاعاتی و منافع عمومی

حریم خصوصی اطلاعاتی شهروندان، ماهیتی شخصی داشته و در حوزه‌ی آزادی‌های فردی قرار می‌گیرد، اما شهروندان آزادی‌های دیگری نیز دارند و با توجه به اینکه در یک محیط اجتماعی زندگی می‌کنند، دارای منافع جمعی یا عمومی نیز هستند. گاهی اوقات آزادی‌های فردی در تعارض با منافع عمومی هستند؛ به عنوان مثال، آزادی‌های فردی یک مجرم یا کلاهبردار مالی با منافع عمومی جامعه در تضاد است و منافع عمومی را در معرض خطر قرار می‌دهد. مدافعان حریم خصوصی شهروندان با این موضوع موافقند که حریم خصوصی شهروندان جزء منافع مهم افراد محسوب می‌شود اما باید میان این منفعت و سایر منافع شهروندان یک موازنه برقرار کرد. نظریه‌پردازان حریم خصوصی معتقدند حمایت از حریم خصوصی یک شهروند ممکن است مانع آزادی‌های شهروند دیگر شده یا برای وی ضرر یا خطری را در پی داشته باشد (نیسنباوم، ۲۷:۱۹۹۸). حریم خصوصی علاوه بر آزادی اطلاعات با منافع عمومی دیگری نیز در تعارض قرار می‌گیرد، همچون امنیت ملی، سلامت عمومی، بهداشت جمعی، اطلاعات لازم برای دعاوی حقوقی، پیشگیری و تعقیب جرائم کیفری، تحقیقات علمی، آماری یا تاریخی (رجبی، ۱۳۹۳: ۴۳).

حفظ حریم خصوصی اطلاعاتی شهروندان هنگام ایجاد موازنه با منافع عمومی ممکن است بنا به ضعف در حوزه‌ی قانونگذاری، به خطر بیافتد؛ چرا که در صورت نبود قوانین حامی حریم خصوصی، کفه ترازو به سمت منافع عمومی سنگینی می‌کند. ریمان (۱۹۷۶) معتقد است حفظ حریم خصوصی عملاً در ایجاد موازنه میان منافع خصوصی و منافع عمومی ناممکن است. هنگامی که اطلاعات خصوصی پایش به حوزه‌ی عمومی می‌رسد، تنها درصورتی می‌تواند مورد حمایت قرار گیرد که فرد آن را عامداً عمومی نکرده باشد؛ پارنت (۱۹۸۳) ایده‌ی حریم خصوصی به مثابه «جزیره‌ای ازخودمختاری‌های فردی» را مورد انتقاد قرار می‌دهد. وی معتقد است اطلاعات شخصی هنگامی تحت پوشش حق حریم خصوصی قرار می‌گیرند که تنها در جاهای خاصی مستند شده باشند (مثلاً

1. Health, Education and Welfare
2. Asia-Pacific Economic Cooperation
3. Organization for Economic Cooperation and Development

[DOI: 10.52547/qjal.9.31.168]

در پایگاه‌های داده یک سازمان دولتی)؛ اما همین که داده‌های پراکنده‌ی شهروندان در یک پایگاه داده یا انبار داده‌ی مرکزی قرار می‌گیرد، نگرانی‌های زیادی برای شهروندان به‌وجود می‌آید.

نمونه‌ی بارزی از تعارض حریم خصوصی اطلاعاتی با منافع عمومی در مورد داده‌های پزشکی شهروندان است که در اختیار نهادهای پزشکی حرفه‌ای قرار دارد (یانگ،۲۰۱۵:۳۸۹). دولت ممکن است به بهانه‌ی حمایت از بهداشت عمومی یا تحقیقات پزشکی و علمی، اقدام به دسترسی به داده‌های شخصی بیماران کند. نمونه‌ای دیگر از این دست تعارضات میان منافع خصوصی و عمومی، همانا دسترسی دولت و سازمان‌های دولتی به رکوردهای مربوط به سـوابق کیفری شهروندان است. دولت می‌تواند با بهانه‌های مختلفی مثل مبارزه با کلاهبرداری یا شناسایی مجرمان به چنین داده‌هایی دسترسی پیدا کند. نمونه‌ی دیگری از تعارض میان حریم خصوصی اطلاعاتی با منافع عمومی در مورد داده‌های مالی و بانکی شهروندان است که در اختیار بانک‌ها و مؤسسات مالی است و دولت به بهانه‌ی جمع‌آوری مالیات و محاسبه‌ی میزان درآمدهای شهروندان می‌تواند به آنها دسترسی داشته باشد (اسلمورد، ۱۲:۲۰۰۶). با توجه به اینکه حمایت مطلق از حریم خصوصی اطلاعاتی عقلاً و عملاً ناممکن می‌نماید، برای ممانعت از بازگشت تاریخ به نفع اختیارات مقامات عمومی برای دست‌اندازی به حقوق فردی، باید موارد منافع جمعی مهم که نسبت به حریم خصوصی به طور استثنایی اولویت دارد، به صراحت مشخص شود (رجبی، ۱۳۹۳: ۴۵ به نقل از محسنی، ۱۳۸۸)؛ چنین استثنائاتی در قوانین حمایت از داده، در کشورهای پیشرفته پیش‌بینی شده‌اند. مشخص کردن استثنائات در قانون برای ایجاد توازن میان حفظ حریم خصوصی اطلاعاتی و منافع عمومی، بدین معناست که نقض حریم خصوصی فقط و فقط در همان استثنائات مجاز بوده و در سایر موارد غیرمجاز تلقی می‌شود؛ اما مشخص نکردن موارد استثناء (آن گونه که در قوانین بسیاری از کشورهای در حال توسعه یا توتالیتر) دیده می‌شود، به معنای باز بودن درهای ورود به حریم خصوصی اطلاعاتی شهروندان و عدم حمایت از آن است.

راهکاری که برای این چالش نیز پیشنهاد می‌شود این است که پیش از توسعه‌ی دولت الکترونیک، باید قوانین حمایت از حریم خصوصی اطلاعاتی توسط مجالس قانونگذاری کشورها (خصوصاً در کشورهای در حال توسعه) جهت ضابطه‌مندسازی توسعه‌ی دولت الکترونیک و جلوگیری از نقض حریم خصوصی اطلاعاتی شهروندان تصویب و اجرایی شوند.

کشورهای دنیا در زمینه‌ی حفظ حریم خصوصی اطلاعاتی شهروندان سه رویکرد را در پیش گرفته‌اند: (عدم تصویب قانون، تصویب قوانین بخشی و تصویب قانون جامع). آمریکا و ژاپن تصویب قوانین بخشی، کانادا، انگلستان و ۱۱ کشور دیگر قانون جامع حفظ حریم خصوصی اطلاعاتی را به تصویب رسانده‌اند. (تقوی فرد و دیگران، ۱۳۹۵)

[DOI: 10.52547/qjal.9.31.168]

در قوانین بین‌المللی ماده ۱۸ اعلامیه اسلامی حقوق بشر، ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، حق حریم خصوصی شهروندان محترم شمرده شده است، در قوانین و مقررات جمهوری اسلامی ایران نیز به عناوین مختلف حریم خصوصی افراد مورد توجه قرار گرفته و الزام افراد و دولت به حراست از حریم خصوصی و احترام بدان گوشزد شده است. مهم‌ترین مستندات حفاظت از حریم خصوصی در مقررات داخلی عبارتند از:

الف ـ اصل ۲۲ قانون اساسی جمهوری اسلامی ایران «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند». اصل ۲۲ قانون اساسی هم حریم خصوصی و هم حریم مادی را مدنظر قرار داده است و به نظر می‌رسد حقوق را مصداق حریم خصوصی معنوی و مسکن را مصداق حریم خصوصی مادی بیان نموده است. اما به نظر می‌رسد در مورد مسکن با توجه به مفهوم و معنای لغوی آن که افاده محل سکونت را می‌نماید و محل سکونت نیز عرفاً به جایی گفته می‌شود که صرفاً به‌منظور سکونت از آن بهره‌برداری می‌شود، نمی‌توان اماکنی که غیر از سکونت از آن استفاده دیگری می‌شود را داخل در موضوع اصل ۲۲ قرار داد و برای آن‌ها قائل به حریم خصوصی شد. مثال نمی‌توان محل کسب و کار اشخاص را دارای در حریم خصوصی دانست، زیرا محل سکونت یا مسکن نیستند؛ در حالی که می‌بایست هر محدوده و مکانی را که شخص در آن دارای امور خصوصی می‌باشد دارای حریم دانست. در این صورت چنانچه مثلاً مکان کسب و تجارت را جزو حریم خصوصی ندانیم، مطابق اصل ۲۲ بدون تجویز قانون هم می‌توان به آن اماکن تعرض نمود! که به‌طور قطع این با هدف مقنن اساسی در تعارض بوده و به نوعی نقض غرض محسوب می‌گردد. سوالی که در اینجا مطرح می‌شود اینکه، آیا برای نظارت یا کنترل و بازبینی ورود به اماکن غیر مسکونی، وجود نهادی مانند کمیته اماکن ضروری است و آیا وجود آن موافق با قانون اساسی می‌باشد یا خیر؟ به‌نظر می‌رسد با استفاده از همین ضعف قانون اساسی در این قسمت است که امکان ورود به حریم خصوصی اماکن غیر مسکونی به‌راحتی فراهم گردیده است، در حالی که اماکن غیر مسکونی اعم از تجاری و حتی اداری نیز دارای حریم خصوصی بوده و ورود به آن بدون مجوز قانونی تعرض محسوب شده و ورود به آنها آشکارا نقض حریم خصوص اشخاص می‌باشد.

ب ـ اصل ۲۵ قانون اساسی «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس و سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هر گونه تجسس ممنوع است، مگر به حکم قانون». اصل ۲۵ قانون اساسی به طور اختصاصی مدافع حریم خصوصی معنوی اشخاص می‌باشد. هر شخص برای خود دارای خلوتی است که دیگران را به آن راه نیست و این حریم و خلوت ممکن است در یک نامه خصوصی یا مکالمه تلفنی یا پیام کوتاه باشد. ممکن است این حریم برای دیگران هیچ ارزشی نداشته باشد یا فاقد هرگونه جذابیتی باشد، اما برای

[DOI: 10.52547/qjal.9.31.168]

صاحب آن محترم و با ارزش است و چه بسا این حریم حاصل تفکرات یا احساسات یا هر گونه تمایلات و روحیات اشخاص باشد. می‌توان گفت در همین راستا اعمال شکنجه برای اعتراف به امری مصداق بارز نقض حریم حقوق معنوی اشخاص می‌باشد. آنچه اصل ۲۵ قانون اساسی بدان تصریح دارد، ضامن بخشی از امنیت اجتماعی شهروندان می‌باشد که در صورت نقض آن موجبات از بین رفتن بخشی از امنیت اجتماعی نیز فراهم خواهد شد، تاجایی که شاید هر شخص مجبور شود برای حراست از حریم معنوی خویش به هر وسیله ممکن متوسل شود. مخاطبین اصل ۲۵ قانون اساسی هم شهروندان و هم دولت هر دو می‌باشند، به‌طور مثال استراق سمع و افشای آن می‌تواند توسط شهروندان نیز صورت گیرد. اما سایر موارد مذکور در اصل ۲۵ جزو اموری است که اصولاً نقض آنها فقط توسط دولت، با امکاناتی که در اختیار دارد، امکان‌پذیر است. اصل ۲۵ قانون اساسی یکی از اصول مهم جهت حفظ حریم خصوصی معنوی اشخاص در جهت تثبیت امنیت اجتماعی است که هر آن ممکن است توسط دولت نقض گردد که متاسفانه به جای آنکه قوانین و مقرراتی به‌منظور نظارت و یا تحقیقات قضایی تصویب گردد، حریم خصوصی اشخاص شکسته شده و این اصل مهم قانون اساسی نادیده گرفته می‌شود. اصل ۲۵ قانون اساسی بازرسی و افشای مکاتبات و مخابرات و فاش کردن مکالمات تلفنی و سانسور و استراق سمع و هر گونه تجسس را به حکم قانون مجاز دانسته است. آنچه که واضح است برای تجویز هر کدام از موارد اصل ۲۵ می‌بایست قانونی وجود داشته باشد و فقط به موجب قانون می‌توان مثلاً به افشای مکالمات تلفنی مبادرت یا آنها را ضبط و فاش نمود. نتیجه آنکه در جریان تحقیقات قضایی و پلیسی، امکان استراق سمع یا ضبط مکالمات قانوناً وجود ندارد و قاضی و مأمورین پلیس حق صدور دستور استراق سمع یا ضبط مکالمات بازرسی و نرساندن نامه را ندارند، مگر به موجب که صراحت در این مورد دارد و اجازه چنین اقدامی را داده است، توسل جویند و اگر چنین قانونی وجود ندارد اقدام آنها خلاف قانون اساسی و آزادی‌های عمومی و حریم خصوصی اشخاص بوده و قابل رسیدگی در محاکم قضایی می‌باشد. (ربیعی، ۹:۱۳۸۳).

۳-۳. حریم خصوصی اطلاعاتی و آزادی اطلاعات

آزادی اطلاعات به معنای «آزادی افراد و حق بنیادی آنان در دسترسی به اطلاعات عمومی» است (رابرتز، ۸۹:۲۰۰۱). به نظر سزکلی (۲۰۰۹: ۲۹۵-۲۹۴) در یک جامعه‌ی دموکراتیک، حریم خصوصی اطلاعاتی و آزادی اطلاعات هر دو مؤلفه‌های اساسی استقلال اطلاعاتی شهروندان هستند و به عنوان مکمل‌های همدیگر شناخته می‌شوند. از یک سو چنین فرض می‌شود که کارکردهای حفاظت از داده یا حمایت از حریم خصوصی اطلاعاتی به شـهروندان کمک می‌کنند تا بتوانند تعیین کنند کی، چگونه و تا چه حد از اطلاعاتشان توسط دیگران قابل دستیابی باشد و از طرف دیگر، به عنوان مؤلفه‌ی دیگری از استقلال اطلاعاتی، شهروندان باید قادر باشند به آن حد از اطلاعات مورد نیازشان

[DOI: 10.52547/qjal.9.31.168]

در فضای عمومی که می‌خواهند دسترسی پیدا کرده یا حتی جلوی سرازیر شدن آن اطلاعاتی که به نظر آنها خوشایند نیست (مثل پیام‌های تبلیغاتی یا بازاریابی) به سمت خودشان را بگیرند. باید توجه داشت که حق آزادی اطلاعات، مربوط به حق شهروندان در دسترسی به فایل‌ها و اسناد دولتی است و نباید چنین برداشت کرد که شهروندان حق دارند به داده‌های شخصی سایر شهروندان دسترسی داشته باشند (مالونی، ۱۹۸۴: ۲۵۶). زندگی خصوصی و دریافت خدمات عمومی نیازمند بوجود آمدن توازنی میان حفظ حریم خصوصی اطلاعاتی شهروندان و حق آزادی اطلاعات آنان است. اگر شهروندان بخواهند یک دولت شفاف از نظر اطلاعاتی داشته باشند، و هر زمان که خواستند به اطلاعات دولتی که می‌خواهند دسترسی داشته باشند، باید خطر نقض حریم خصوصی اطلاعاتی خود را در نظر بگیرند.

آنچه مسلم است این است که تنها در صورت وجود قوانین حامی حریم خصوصی اطلاعاتی است که می‌توان با ضابطه‌مندسازی میزان دسترس‌پذیر بودن داده‌های شخصی شهروندان، دسترسی سایرین (سایر شهروندان و نهادهای دولتی و خصوصی) به داده‌های شخصی شهروندان را کنترل کرد (مالونی، ۱۹۸۴: ۲۵۵).

بنابراین این وظیفه‌ی سازمان‌های دولتی است که تمایزی میان اطلاعات حوزه‌ی عمومی و داده‌های شخصی شهروندان ایجاد کنند و اجازه‌ی دسترسی را تنها به اطلاعات عمومی محدود کنند. با این وجود، این حق برای سازمان‌های دولتی وجود دارد که برخی از اطلاعات را سری و محرمانه تلقی کرده و آنها را از دسترسی عموم محفوظ دارند. به عنوان مثال، اطلاعات و اسناد مربوط به مسائل امنیت ملی، برنامه‌های تسلیحاتی موشکی، مبارزه با تروریسم و غیره توسط بسیاری از دولت‌ها سری تلقی شده و امکان دسترسی عمومی به آنها وجود ندارد. اما این موضوع می‌تواند بهانه‌ای برای دولت‌ها برای عدم شفافیت باشد. به عنوان مثال دولت‌ها می‌توانند حق آزادی اطلاعات شهروندان را در خصوص دسترسی به سیاست‌ها، برنامه‌ها، میزان پیشرفت پروژه‌های عمرانی یا حتی دانستن میزان واقعی نرخ تورم و بیکاری زیر پا بگذارند. هرچند یکی از کارکردهای دولت الکترونیک ایجاد شفافیت است (کارلو برتوت، جاگر و گریمز، ۸۶:۲۰۰۱)، اما بدون وجود قوانین حامی حریم خصوصی اطلاعاتی، این شفافیت مبتنی بر آزادی اطلاعات ممکن است باعث نقض حریم خصوصی اطلاعاتی شهروندان شود.

برای چالش حریم خصوصی اطلاعاتی و آزادی اطلاعات راهکاری که پیشنهاد می‌شود این است که در استانداردهای دولت الکترونیک و چارچوب‌های معماری فناوری اطلاعات دولت الکترونیک (همچون سند ملی چارچوب تعامل‌پذیری دولت جمهوری اسلامی ایران یا (IGIF) باید الزامات حفظ حریم خصوصی و امنیت اطلاعات برای صیانت از حقوق شهروندان لحاظ شده باشد.

[DOI: 10.52547/qjal.9.31.168]

٤-۳. چالش حق شهروند برای دسترسی به اطلاعات در دولت الکترونیک

حق دسترسی به اطلاعاتی که توسط نهادهای دولتی ثبت و ضبط می‌شود (RTI) عبارت است از حقی که افراد یا شهروندان یک مملکت دارند تا به اطلاعاتی که در اختیار نهادهای دولتی است دسترسی داشته باشند (بانیسار، ۲۰۱۱: ۵). اعتقاد بر این است که حق دسترسی به اطلاعات (RTI) یکی از نیازمندی‌های یک دموکراسی است. به ترتیبی که شهروندان با دسترسی به اطلاعاتی که در اختیار دولت قرار دارد (همچون اطلاع از فعالیت‌های دولتی، تصمیم‌گیری‌ها، سیاست‌های خرد و کلان و...) قادر خواهند بود مشارکت فعالی در دولت الکترونیک داشته باشند. علاوه بر نقشی که حق دسترسی به اطلاعات (RTI) در دموکراسی الکترونیکی دارد، می‌تواند مانعی باشد برای فساد؛ یا به عبارت دیگر، باعث افزایش سلامت اداری در دولت الکترونیک شود. امروزه بیش از ۹۰ کشور در دنیا حق دسترسی به اطلاعات (RTI) را در مجموعه قوانین خود گنجانده‌اند؛ می‌توان مفاد اصلی حق دسترسی به اطلاعات (RTI) که عمومی‌ترین و پذیرفته‌ترین در میان کشورهای جهان هستند را به شرح زیر دانست (بانیسار، ۲۰۱۱: ۵):

- حق افراد حقیقی، افراد حقوقی و سازمان‌ها برای درخواست اطلاعات از نهادهای دولتی بدون اینکه مجبور به نشان دادن حکمی قانونی برای آن اطلاعات باشند.
- وظیفه‌ی هر نهاد برای پاسخگوی و فراهم نمودن اطلاعات: شامل مکانیزم‌هایی برای مدیریت درخواست‌ها و محدوده‌های زمانی برای پاسخگویی به درخواست‌ها.
- معافیت‌هایی برای اجازه به منع گروه‌های خاص اطلاعاتی. این معافیت‌ها شامل حفاظت از اطلاعات امنیت ملی و روابط بین‌المللی، محرمانگی شخصی، محرمانگی تبلیغاتی (بازرگانی)، الزامات قانونی، اطلاعات محرمانه دریافت شده و مذاکرات بین‌المللی است.
- مکانیزم های داخلی درخواست برای تقاضاکنندگان اطلاعات به‌منظور به چالش کشیدن منع اطلاعات (درخواست شده).
- مکانیزم‌هایی برای بازبینی خارجی منع اطلاعات. این مورد شامل برپاکردن نهادی خارجی مثل سازمان بازرسی می‌باشد.
- الزام نهادهای دولتی برای انتشار ایجابی برخی انواع اطلاعات در مورد ساختارها، قوانین، و فعالیت‌هایشان. این امر اغلب از طریق استفاده از فناوری اطلاعات و ارتباطات امکان‌پذیر می‌گردد.

در حق دسترسی شهروند به اطلاعات، منظور شفاف‌سازی فرایندهای دولتی و ارتقای مردم‌سالاری است تا شهروندان بتوانند به اطلاعاتی که در زندگی آنان اهمیت دارد (اطلاع از تصمیمات دولتی، فرایندهای سازمانی و مالی، مفاد قوانین، فرصت های استخدامی، اخبار و وقایع روزمره، اطلاعات مورد نیاز برای مسائل علمی و ژورنالیستی و ...) دسترسی پیدا کنند. به‌طوری که سازمان‌های دولتی

[DOI: 10.52547/qjal.9.31.168]

به‌صورت شفاف این اطلاعات را در اختیار شهروندان بگذارند و آنها را از دسترسی به اطلاعاتی که آگاهی شهروندان از آنها منع قانونی ندارد (همچون اطلاعات خصوصی سایر شهروندان، اطلاعات محرمانه و سری دولتی) منع نکنند و این از پیش نیازهای دولت‌های مردم‌سالار محسوب می‌شود.

با توجه به اینکه توسعه‌ی دولت الکترونیک بدون جلب اعتماد و مشارکت شهروندان عملاً ناممکن است، مهمترین راهکار و پیشنهادی که برای آخرین چالش مطرح می‌شود این است که مجموعه‌ای از الزامات برای محرمانگی اطلاعات شهروندان در سند ملی چارچوب تعامل‌پذیری دولت جمهوری اسلامی ایران قرار بگیرد و حقوق زیر به عنوان حقوق شهروندان در زمینه حریم خصوصی اطلاعاتی در دولت الکترونیک مورد توجه قرار گیرد.

۱- حق آگاهی از اهداف گردآوری داده‌های شخصی توسط یک سازمان
۲- حق آگاهی از وجود (یا عدم وجود) داده‌های شخصی نزد یک سازمان
۳- حق آگاهی از افشای داده‌های شخصی به نهاد ثالث درگذشته یا احتمال افشاء در آینده
۴- حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های شخصی
۵- حق آگاهی از هویت متولی داده‌های شخصی (کنترل‌گر) و راه‌های تماس با وی
۶- حق دسترسی به داده‌های شخصی
۷- حق اصلاح داده‌های شخصی غیردقیق (غیر صحیح یا ناقص)
۸- حق حذف داده‌های شخصی در صورت داشتن توجیه مشروع مبنی بر اینکه گردآوری داده‌های شخصی غیرمجاز بوده باشد
۹- حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های حساس شخصی
۱۰- حق درخواست تعلیق استفاده داده‌های شخصی در صورت داشتن توجیه قانونی مبنی بر اینکه استفاده داده‌های شخصی موجب ضرر برای شهروند یا ناراحتی برای سایرین می‌شود
۱۱- حق آگاهی از تصمیم‌گیری منطقی مبتنی بر پردازش تمام خودکار داده‌ها
۱۲- حق آگاهی از منبع گردآوری داده‌ها
۱۳- حق آگاهی از پیامدهای اعلام عدم رضایت نسبت به پردازش داده‌های شخصی
۱۴- حق پیگردی قانون هرگونه خسارت ناشی از پردازش داده‌های شخصی در فرآیندی منصفانه (حق دادخواهی)
۱۵- حق منع استفاده از داده‌های شخصی برای فعالیت‌های بازاریابی مستقیم
۱۶- حق آگاهی از حقوقی که شهروند در خصوص حریم خصوصی اطلاعاتی از آنها برخوردار است
۱۷- حق آگاهی از هویت پردازشگر (پیمانکار) داده‌های شخصی و راه‌های تماس با وی

[DOI: 10.52547/qjal.9.31.168]

۱۸- حق پیگرد قانونی عدم پاسخگویی متولی به درخواست‌های شهروندی در برخورداری از حقوق خود در خصوص حریم خصوصی اطلاعاتی
۱۹- حق تقاضای پردازش غیر خودکار (توسط انسان) داده‌های شخصی در صورت قرارگیری در معرض تصمیم‌گیری مبتنی بر پردازش تمام خودکار داده‌های شخصی
۲۰- حق آگاهی از مدت زمان نگهداری داده‌های شخصی توسط متولی
۲۱- حق درخواست ادغام داده‌های شخصی از متولی. (جمشیدی،۱۳۹۶)

نتیجه گیری

هرچند دولت الکترونیک مزایای بی‌شماری را برای شهروندان، کسب و کارها و حتی کارکنان دولت به ارمغان آورده و هزینه‌ها و زمان انجام فرایندهای دولتی را بسیار کاهش می‌دهد، اما امکان نقض گسترده‌ی حقوق حریم خصوصی اطلاعاتی شهروندان باعث سلب اعتماد آنان شده و بر مشارکت الکترونیکی آنان در فرایندهای سیاسی و دموکراسی الکترونیکی تأثیر منفی می‌گذارد. دولت الکترونیک با به کارگیری فناوری‌های جدید ارتباطی و اطلاعاتی به بهبود فرآیندهای ارائه خدمات در بخش عمومی، تسریع ارائه خدمات به شهروندان، پاسخگو شدن ماموران دولتی، شفاف‌شدن اطلاعات، کاهش فاصله میان مردم و دولتمردان، افزایش مشارکت اثربخش شهروندان و اعضای جامعه مدنی در فرآیند تصمیم‌گیری عمومی، گسترش عدالت اجتماعی از طریق فرصت‌های برابر افراد برای دسترسی به اطلاعات و.... کمک شایانی می‌کند و امروزه حکومتی که بخواهد در مسیر تحقق حکومت‌داری به نحو ایده‌آل حرکت کند، باید به ابزار نیرومندی همچون دولت الکترونیک مسلح باشد. دولت الکترونیک می‌تواند به حکومت‌ها در بهبود ارتباطات و تأمین رضایت مردم کمک کرده، همچنین ایجاد ارتباط دو سویه بین مردم و مسئولان از راه‌های مختلف را میسر سازد. اطلاع‌رسانی و آگاه کردن مردم از مصوبات، مقررات و مجموعه وظایف و اختیارات دولت و نیز مشارکت دادن مردم در تصمیم‌سازی از طریق نظرسنجی الکترونیکی و ایجاد صندوق شکایات از طریق پست الکترونیکی، پاسخگویی سریع به خواسته‌ها و شکایات مردم و نظایر آن، شیوه‌هایی است که دامنه ارتباطات مردمی را بیش از پیش گسترده و بهینه می‌کند. همچنین عرضه خدمات عمومی به صورت الکترونیک مانند پرداخت هزینه‌های آب، برق، تلفن، قبض جریمه، رزرو بلیت و صدور گذرنامه مزایایی از جمله صرفه‌جویی در وقت و نیروی انسانی، کاهش ترددهای درون شهری و بین شهری و کاهش بار ترافیک را در پی دارد. این امور می‌تواند در روش زندگی مردم و تأمین رفاه و رضایت آنان تأثیر بسزایی داشته باشد و در نهایت می‌تواند موجبات توسعه و رشد اقتصادی، اجتماعی، فرهنگی و سیاسی را در کشور فراهم سازد. حق داشتن حریم خصوصی اطلاعاتی یکی از مهمترین حقوق شهروندان در فضای مجازی است. در این مقاله حداقل چهار قابلیت دولت الکترونیک که ممکن است موجب خدشه‌دار شدن حریم خصوصی اطلاعاتی شهروندان شود، بدین شرح معرفی

[DOI: 10.52547/qjal.9.31.168]

شدند: جمع‌آوری سریع‌تر و ساده‌تر داده‌ها، گردآوری داده‌های بزرگ، ادغام داده‌ها و جمع‌آوری مخفیانه‌ی داده‌ها. این قابلیت‌های دولت الکترونیک می‌تواند موجب نقض وسیع حقوق شهروندی در زمینه‌ی حفاظت از حریم خصوصی شهروندان شود. در این مقاله، چهار چالش عمده برای حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک شناسایی و معرفی شـــد، که عبارتند از: (الف) چالش حفظ حریم خصوصی اطلاعاتی شـــهروندان و توسعه‌ی دولت الکترونیک؛ (ب) چالش حفظ حریم خصوصی اطلاعاتی و منافع عمومی؛ (ج) حفظ حریم خصوصی اطلاعاتی و آزادی اطلاعات؛ و (د) چالش حق شهروند برای دسترسی به اطلاعات در دولت الکترونیک. توسعه‌ی دولت الکترونیک و افزایش سطوح بلوغ آن اولین چالشی است که می‌تواند حق حریم خصوصی اطلاعاتی شهروندان را خدشه‌دار سازد. هر چه سطوح بلوغ دولت الکترونیک بالاتر رود، امکان تجمیع اطلاعات شخصی شهروندان که در پایگاه‌های اطلاعاتی پراکنده ذخیره شده‌اند (مثل: ثبت احوال، ثبت اسناد و املاک، بانک‌ها و ...) در یک پایگاه داده بیشتر می‌شود. همچنین، در دولت الکترونیک همیشه میان مصلحت عمومی و خصوصی تعارض وجود داشته است. به‌عنوان مثال آیا دولت این حق را دارد که به بهانه‌هایی همچون مبارزه با تروریسم یا ارتقای رفاه و بهداشت جامعه به حریم خصوصی اطلاعاتی افراد ورود پیدا کند؟ چالش دیگر، ایجاد حفظ حریم خصوصی اطلاعاتی افراد و آزادی اطلاعات است. زندگی خصوصی و دریافت خدمات عمومی نیازمند بوجود آمدن توازنی میان حق حریم خصوصی اطلاعاتی شهروندان و حق آزادی اطلاعات آنان است. اگر شهروندان بخواهند یک دولت شفاف از نظر اطلاعاتی داشته باشند، و هر زمان که خواستند به اطلاعات دولتی که می‌خواهند دسترسی داشـــته باشند، باید خطر نقض حریم خصوصی اطلاعاتی خود را در نظر بگیرند. چالش آخر هم چالش اعطای حق شهروند در زمینه‌ی دسترسی به اطلاعات در دولت الکترونیک است. در حق دسترسی به اطلاعات، شهروندان باید بتوانند به اطلاعات مورد نیاز خود دسترسی داشته باشند؛ همچنین هر وقت بخواهند باید بتوانند به اطلاعات شخصی خود که در اختیار سازمان‌های دولتی است دسترسی داشته باشند، آن‌ها را اصلاح کرده و در صورت داشتن مجوز قانونی حذفشان نمایند.

[DOI: 10.52547/qjal.9.31.168]

فهرست منابع

۱. فارسی

الف) کتاب‌ها

آماده، مهدی (۱۳۹۲)، حمایت از حریم خصوصی، تهران: دادگستر.
اصلانی، حمیدرضا (۱۳۸۹)، حقوق فناوری اطلاعات، تهران: میزان .
تقوی فرد، محمدتقی و جمشیدی، محمدجواد (۱۳۹۶)، اصول و مبانی حریم خصوصی اطلاعاتی، تهران: چراغ دانش.
رجبی، اکرم (۱۳۹۳)، نقض حریم خصوصی در فضای سایبر، تهران: آرمان رشد.
سروش، محمد (۱۳۹۳)، حریم مبانی خصوصی بر اساس منابع اسلام، تهران: سمت.
هارلو، کارل؛ (۱۳۸۳)، شبه جرم، کامبیر سیدی (مترجم)، تهران: میزان.
یعقوبی، نور محمد (۱۳۹۲)، دولت الکترونیک: رویکرد مدیریتی، تهران: افکار.

ب) مقالات

انصاری، باقر (۱۳۹۱)، «مطالعه تطبیقی مسؤولیت مدنی ناشی از نقض حقوق مربوط به شخصیت در رسانه‌ها»، مجله علمی پژوهشی حقوق خصوصی، دوره ۹، شماره ۲، صص ۱۰۰-۶۷
تقوی فرد، محمدتقی، تقوا، محمدرضا، فقیهی، مهدی و جمشیدی، محمدجواد (۱۳۹۵)، «الگوی صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه»، پژوهش‌های مدیریت عمومی، ۳۱، صص ۹۹-۱۲۱.
تقوی فرد، محمدتقی، تقوا، محمدرضا، فقیهی، مهدی و جمشیدی، محمدجواد (۱۳۹۵)، «مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب»، مجله مجلس و راهبرد، دوره ۲۴، شماره ۸۹، صص ۳۰۱-۳۳۳.
ربیعی، حمیدرضا (۱۳۸۳)، «دولت الکترونیکی تجربه دولت آلمان»، دانشگاه صنعتی شریف،
رضایی زاده، محمدجواد (۱۳۹۰)، «مدخلی بر خدمات عمومی الکترونیک در نظام حقوقی ایران»، مجله حقوق خصوصی، شماره ۱۹.
نمک دوست تهرانی، حسن (۱۳۸۵)، «اخلاق حرفه‌ای، حریم خصوصی و حق دسترسی به اطلاعات»، رسانه، شماره ۶۶، صص ۱۹۷-۲۳۲.
یعقوبی، نور محمد (۱۳۸۸)، «دولت الکترونیک الگوی انتقالی»، فصلنامه مطالعات مدیریت، شماره ۵۰ .

ج) پایان نامه

جمشیدی، محمدجواد (۱۳۹۶)، «الگوی حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک ایران»، دانشگاه علامه طباطبایی.

۲. انگلیسی

A) Books

Johnson, Deborah. and Nissenbaum, Helen. (1995). *Privacy and databases. Computers, Ethics and Social Values*. Prentice Hall, Englewood Cliffs, NJ.

[DOI: 10.52547/qjal.9.31.168]

Regan, Patrick. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill, NC

B) Aticels

Belanger, France., & Hiller, Janet. (2006). "A framework for e-government: privacy implications". *Business Process Management Journal*, 12(1), 48-60.

Carlo-Bertot, John., Jaeger, Paul., & Grimes, J. M. (2012)." Promoting transparency and accountability through ICTs, social media, and collaborative e-government". *Transforming Government: People, Process and Policy*, 6(1), 78-91.

Floridi, Luciano. (1999). "Information ethics: on the philosophical foundations of computer ethics". *Ethics and Information Technology*, 1(1), 37–56.

Maloney, Maureen. (1984). "Freedom of Information and Privacy. In Protection of Human Research Subjects*"Springer US*, (pp. 255-310).

Moor, James. (1997). "Towards a theory of privacy in the information age". Computers and Society, 27(3), 27–32.

Reiman, Jeffrey. (1976)."Privacy, intimacy, and personhood". *Philosophy & Public Affairs*, 26-44.

Roberts, Alasdair. (2001). "Structural pluralism and the right to information". *The University of Toronto Law Journal*, 51(3), 243-271.

Slemrod, Joel. (2006)." Taxation and Big Brother: Information, Personalisation and Privacy in 21st Century Tax Policy". *Fiscal Studies*, 27(1), 1-15.

Steyaert, Jo, 2000, "Local government online and the role of the resident-government shop versus electronic community", *Social Science Computer Review*, vol 18, no 1, pp 3-16.

Symonds, Mallon., 2000, "Government and the internet: no gain without pain", *The Economist*, vol 355, pp S9-S14.

Szekely, Istvan. (2009). "Freedom of Information Versus Privacy: Friends or Foes?. In Reinventing Data Protection?" *Springer Netherlands*, (pp. 293-316).

15- Thomas, John. and Streib, Gregory., 2003, "The new face of government: citizen-initiated contacts in the era of e-government", *Journal of Public Administration Research and Theory*, vol 13, no 1, pp 82-102.

[DOI: 10.52547/qjal.9.31.168]