

دولت الکترونیک و حریم خصوصی افراد

زهرا صدر عرفانی^۱، ایوب طالب زاده^۲

^۱ کارشناس ارشد حقوق نفت و گاز از دانشگاه تهران.

^۲ کارشناس ارشد حقوق خصوصی از موسسه آموزش عالی ایرانیان.

نام نویسنده مسئول:

زهرا صدر عرفانی

چکیده

امروزه 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 غیردولتی قرار داده است. اهمیت مسئله‌ی نقض حریم خصوصی داده‌ها ناشی از توسعه‌ی فناوری است که در آن نقض حریم خصوصی خسارت‌بارتر از دیگر حوزه‌ها مطرح می‌گردد. مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها، نسبت به مسئولیت مدنی ناشی از نقض سایر انواع حریم خصوصی از پیچیدگی‌های بیشتری برخوردار است؛ زیرا در این نوع، بحث انتفاء موضوع و مرگ حریم خصوصی داده‌ها به میان می‌آید. از سوی دیگر حتی برخی معتقد به مالیت داشتن حریم خصوصی داده‌ها هستند. این دو مسئله، مسیر مباحث راجع به مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها را دگرگون می‌سازد. در این تحقیق قوانین حامی حریم خصوصی اطلاعاتی بررسی شده‌اند. روش‌شناسی این تحقیق، کیفی و شامل روش‌های مطالعات اسنادی، تحلیل محتوا و مطالعه تطبیقی است. در این تحقیق مسائلی همچون اصول گردآوری، استفاده، نگهداری و افشای داده‌های شخصی شهروندان، حقوق سوژه، مسئولیت‌های کنترلگر و اصول دسترسی سوژه به داده‌های شخصی مورد بررسی قرار گرفته است. نتایج تحقیق نشان می‌دهد، وضعیت حمایت از حریم خصوصی اطلاعاتی در ایران فاصله بسیار زیادی با کشورهای منتخب و استانداردهای جهانی دارد.

واژگان کلیدی: حریم خصوصی، امنیت، دولت الکترونیک، داده، مسئولیت.

مقدمه

دولت الکترونیک (E-government) مفهومی نسبتاً جدید در ادبیات حقوقی کشور ماست که در آن مهم ترین رسانه ارتباطی بین مردم و دولت، اینترنت است. دولت الکترونیک همواره در پی استفاده از ICT برای ارائه خدمات عمومی به شهروندان، کسب و کارها و دیگر دولت‌ها می‌باشد و هدف نهایی آن بهبود بخشیدن به عملکرد سازمان عمومی، فراهم سازی 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 به تدریج این مفهوم بر رابطه بین دولت و شهروندان تاثیر 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. اما به هر حال نمی‌توان گفت که این اطلاعات مشمول حریم خصوصی نیستند چون محرمانه نیستند؛ چرا که هنوز هم این اطلاعات، مبنای قضاوت‌ها و تصمیم‌گیری‌های مهم در مورد اشخاص، قرار می‌گیرند. امروزه در فضای دولت الکترونیکی، مفهوم سنتی حریم که مبتنی بر اصل محرمانگی است؛ دیگر پاسخگوی نگرانی‌های مردم در خصوص حفظ حریم خصوصی ایشان نخواهد بود.

در واقع در عصر اطلاعات، حریم خصوصی به معنای نبود اطلاعات مربوط به ما در ذهن دیگران نیست؛ بلکه کنترلی است که ما روی اطلاعات مان داریم. انسان از آن زمان که خود را شناخت جامعه و اجتماع را نیز شناخت و از همان زمان برای خود خلوتی را نیز قرار داد، این خلوت مرز زندگی اجتماعی و خصوصی بوده و هست. زندگی خصوصی دارا بودن حریمی شخصی را می‌طلب که در جهان امروز بدان حریم خصوصی، حق تنها بودن، حق خلوت و... می‌گویند؛ اما تاکنون تعریفی جامع از حریم خصوصی که مورد تایید همگان باشد، به دست داده نشده است. امروزه دخالت دولت به عنوان مظهر قدرت عمومی، در حریم خصوصی افراد در مقابل تعرض دیگران است؛ اما گاه دولت خود مجبور می‌شود وارد این حریم بشود. با اینکه اصل ورود دولت تحت شرایطی پذیرفته شده است، اما حدود این دخالت محل بحث و چالش می‌باشد. در این تحقیق در پی پاسخگویی به این سوالات خواهیم بود که الکترونیکی شدن دولت چه تاثیری بر حفظ یا نقض حریم خصوصی شهروندان خواهد داشت؟ تقابل بین حریم خصوصی و دولت الکترونیک، با تاکید بر مفهوم سنتی حریم خصوصی چه چالش‌هایی را ایجاد خواهد کرد؟ مفهوم و سطح امنیت اطلاعات در دولت الکترونیک با وجود دسترسی (محدود یا نامحدود) دولت بر اطلاعات مردم چیست؟

گفتار اول: مفهوم دولت الکترونیک

واژه‌های مختلفی در راستای کاربردی کردن ارتباطات و اطلاعات در دولت ابداع شده‌اند که از آن جمله دولت آنلاین، دولت دیجیتالی و دولت شبکه‌ای مطرح شده‌اند؛ که در حال حاضر واژه دولت الکترونیک مورد پذیرش عموم قرار گرفته است (مقیم، ۱۳۹۰: ۱۷۳). واژه دولت الکترونیک برای اولین بار در سال ۱۹۹۵ در ایالات متحده به کار گرفته شد (Heeks R, Bailur, 2007, 246).

تاکنون تعاریف گوناگونی برای دولت الکترونیک ارائه شده است که از جمله می‌توان به موارد زیر اشاره کرد:

– دولت الکترونیک عبارت است از استفاده از فناوری اطلاعات به طور کلی 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).

– دولت الکترونیک به معنی استفاده از اطلاعات و فناوری ارتباطات برای ایجاد تغییر در ساختارها و فرایندهای کاری سازمان‌های دولتی است (بینون و دیویس، ۲۰۰۵، ۳).

– دولت الکترونیک در واقع به مجموعه ارتباطات الکترونیکی میان دولت، شرکتها، شهروندان و کارکنان دولت گفته می‌شود که از طریق شبکه اینترنت برقرار می‌شود. دولت الکترونیک، کلیه شهروندان، شرکت‌های تجاری، سایر سازمان‌های دولتی و کارمندان دولت را قادر می‌سازد تا از طریق یک وبسایت در شبکه اینترنت و بدون محدودیتهای زمانی و مکانی به اطلاعات و خدمات دولتی دسترسی پیدا کنند (ربیع، ۱۳۸۳، ۱).

- دولت الکترونیک عبارتست از ارائه خدمات و اطلاعات دولتی از طریق اینترنت یا سایر رسانه‌های الکترونیکی که در این صورت سیستم‌های ارائه خدمات و اطلاعات مبتنی بر اینترنت برخلاف ساختارهای سنتی که سلسله مراتبی، خطی و یک طرفه‌اند، حالتی غیر سلسله مراتبی، غیر خطی و دو طرفه بخود گرفته‌اند. (یعقوبی، ۱۳۸۸، ص ۱۶).

- اتحادیه اروپا (کمیسیون مجامع اروپایی ۲۰۰۳) «دولت الکترونیک» را بشرح ذیل تعریف نموده است: استفاده از تکنولوژیهای اطلاعات و ارتباطات (ICT) در مدیریتهای عمومی در ترکیب با تغییر سازمانی و مهارتهای جدید به منظور بهبود خدمات عمومی و فرایندهای دموکراتیک و تقویت حمایت از خط مشی‌های عمومی.

رشد و تکوین دولت الکترونیک از نظر اجتماعی، فرهنگی، سیاسی و فنی موضوعی به غایت پیچیده است. کیفیت یک دولت الکترونیک وابسته به عوامل متعددی مانند سیاست و خط مشی اطلاعاتی دولت، تعداد کاربران، انگیزه و سطح تحصیلات آنان است. رواج فرهنگ بکارگیری IT در کل کشور و بدنه دولت، مردم را وادار ساخته است تا از رایانه به منظور نیل به جنبه‌های مختلف زندگی شان استفاده کنند (توحیدی، ۲۰۱۱، ۱۱۰۱). آمادگی پذیرش دولت الکترونیک در کشورهای مختلف به نحو قابل توجهی متفاوت است. میل به دولت الکترونیک ملی بستگی به عواملی مانند قابلیت دسترسی به منابع فناورانه، تمایل دولت به فهم و تأمین نیازهای مردم، زبان، اعتماد و محرمانه بودن دارد (خلیل، ۲۰۱۱، ۳۸۸).

گفتار دوم: مفهوم حریم خصوصی در ادبیات حقوقی

هرچند حریم خصوصی را مفهومی بسیار مبهم و تعریف آن را بسیار مشکل دانسته‌اند (محسنی، ۱۳۸۹، ۱۹) می‌توان گفت حریم خصوصی، قلمروی از زندگی اشخاص است که به‌هیچ‌وجه مایل نیستند دیگرانی بدون اجازه‌ی آن‌ها وارد این قلمرو شوند یا از آن آگاهی پیدا کنند. (هوسمن، ۱۳۷۰، ۴۲) مطابق بند ۱۱ ماده ۲۲ «لایحه حمایت از حریم خصوصی»، حریم خصوصی «قلمروی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند.» حریم خصوصی اطلاعات و داده‌ها عبارت از امور یا مسائلی است که انسان تلاش می‌کند فاش نشوند و سعی می‌کند آن را حفظ کند و با پوششی از حمایت آن را احاطه کند؛ زیرا این حریم با شخصیت او در ارتباط است. (الاهوانی، ۱۹۹۴، ۹)

برخی حریم خصوصی اطلاعات را حق پنهان کردن حقایق زندگی شخصی از دیگران دانسته‌اند. (Smartt, 2014, 35) بهتر است گفته شود حریم خصوصی مواردی از زندگی انسان است که از سوی دیگران غیرقابل تسخیر است؛ چنانچه برخی از آن به‌عنوان حق مصونیت و حق انسان نسبت به امور شخصی خود یاد کرده‌اند. (Louis and Samuel, 1890, 5)

به نظر می‌رسد در تعریف این حق بایستی مؤلفه‌های چندی را مدنظر قرار داد. نخست آن‌که قلمرو این حق ناظر به مسائلی است که صرفاً در حیطه‌ی موضوعات شخصی افراد بوده و ذی‌حق به‌هیچ‌وجه تمایلی به افشای آن ندارد. بنابراین با غیرشخصی شدن این موضوعات و وجود ارتباط بین آن‌ها و جامعه دیگر نمی‌توان از آن به‌عنوان یک حق اختصاصی یاد کرد. دوم آن‌که افشاء شدن بخشی از اطلاعات خصوصی افراد و نقض حریم شخصی آن‌ها نمی‌تواند موجهی برای افشای بقیه‌ی اطلاعات و یا توزیع و انتشار مجدد بخش فاش شده باشد. البته این احتمال نیز وجود دارد که آنچه افشاء شده دیگر از حیطه حریم خصوصی خارج شده و ممنوعیت انتشار مجدد از باب منع ایداء و اضرار است و ربطی به حریم خصوصی داده‌ها ندارد.

هر امری که خودبه‌خود آشکار نباشد و برای به دست آوردن آن تلاش شود یا از ابزار کشف استفاده گردد، داخل در حریم خصوصی داده فرد قرار می‌گیرد. هر آنچه از دید مستقیم و ظاهری افراد پنهان است و اشخاص برای آگاهی از آن مجبور به کوشش و تلاش در کشف و فهم آن گردند، در زمره‌ی حریم خصوصی داده خواهد بود. برخی معتقدند حق بر حریم خصوصی مختص اشخاص حقیقی است که هم در برابر اشخاص حقیقی و حقوقی حقوق خصوصی قابل طرح است و هم در برابر اشخاص حقوقی عمومی و حکومت. (انصاری، ۱۳۸۶، ۲۳۲) البته به نظر می‌رسد اشخاص حقوقی هم نوعی حریم خصوصی داده دارند، لکن انتظار متعارف از حریم در مورد آن‌ها متفاوت است و دایره‌ی مضیق‌تری را شامل می‌شود. برخی موضوعات مهم درحوزه‌ی حریم خصوصی مانند حریم خصوصی جنسی اصلاً در مورد اشخاص حقوقی صدق نمی‌کند. ولی بدیهی است که اشخاص حقوقی دارای حریم خصوصی اطلاعات مالی و تجاری هستند. (Weiming, 2006, 434)

گفتار سوم: مستندات قانونی دفاع از حریم خصوصی

حریم خصوصی در مقررات بین‌المللی و داخلی مورد اشاره و استناد قرار گرفته است که به برخی از مهمترین آنها اشاره می‌کنیم.

بند اول: در مقررات بین المللی

در کنوانسیون ها و قراردادهای متعدد بین المللی موضوع دفاع از حریم خصوصی با جدیت و تعصب فراوان پیگیری شده است. در برخی موارد نیز دولت ایران (قبل و بعد از انقلاب) به کنوانسیون های مذکور ملحق گردیده و با پیوستن به این کنوانسیون ها پایبندی خود را به دفاع از حریم خصوصی نشان داده است و در همین راستا انتظارات فراوان و بر حقی را در شهروندان ایجاد نموده است و به همین خاطر است که نقض حریم خصوصی به هر دلیل توسط شهروندان ایرانی تحمل نشده و گاه با واکنش و اعتراض شدید آنها همراه بوده است.

الف - ماده ۱۸ اعلامیه اسلامی حقوق بشر

ماده ۱۸ اعلامیه اسلامی حقوق بشر مصوب ۵ اوت ۱۹۹۰ یا ۱۵ مرداد ۱۳۶۹ اجلاس وزرای امور خارجه سازمان کنفرانس اسلامی

در قاهره می گوید:

- هر انسانی حق دارد که نسبت به جان و دین و خانواده و ناموس و مال خویش در آسودگی زندگی کند.
- هر انسانی حق دارد که در امور زندگی خصوصی خود (در مسکن و خانواده و مال و ارتباطات) استقلال داشته باشد و جاسوسی یا نظارت بر او یا مخدوش کردن حیثیت او جایز نیست و باید از او در مقابل هر گونه دخالت زور گویانه در این شئون حمایت شود.
- مسکن در هر حالی حرمت دارد و نباید بدون اجازه ساکنین آن یا به صورت غیر مشروع وارد آن شد و نباید آن را خراب یا مصادره کرد یا ساکنین اش را آواره نمود.

ب - ماده ۱۲ اعلامیه جهانی حقوق بشر

احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه، یا مکاتبات خود نباید مورد مداخله های خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد حمله قرار گیرد. هر کس حق دارد که در مقابل اینگونه مداخلات و حملات مورد حمایت قانون قرار گیرد. زندگی خصوصی دامنه وسیعی دارد و می توان هر آنچه را که به دیگران مربوط نمی باشد و با زندگی و امور دیگران ارتباط ندارد را جزو زندگی خصوصی دانست، که امور خانوادگی هم بخشی از زندگی خصوصی به حساب می آید. نحوه ارتباط با انسان های دیگر، آمدن، رفتن، لباس پوشیدن انتخاب های شخصی یا سیاسی، تجرد، تاهل، دارایی و اموال، علایق و گرایشهای شخصی و... از مصادیق زندگی خصوصی می باشند و جزو حریم خصوصی اشخاص به حساب می آیند و بموجب ماده ۱۲ اعلامیه جهانی حقوق بشر هیچکس حق دخالت در آنها را ندارد و هیچکس نمی تواند آنها را زیر سوال برده و یا تغییراتی را در آنها به صاحب آن حریم تحمیل نماید و احدی حق ندارد زندگی خصوصی دیگری را موضوع مداخله های خودسرانه خود قرار دهد؛ این امر دخالت در حریم خصوصی بوده و برابر ماده ۱۲ مذکور هر کس حق دارد در مقابل اینگونه مداخلات و حملات مورد حمایت قانونی قرار گیرد.

ماده ۱۲ اعلامیه جهانی حقوق بشر اقامتگاه را نیز در ردیف مصادیق حریم خصوصی اشخاص آورده و حکم ماده را شامل اقامتگاه افراد نیز می داند، اقامتگاه اشخاص برابر ماده ۱۲ قابل تحقیق و تفحص نمی باشد و شخص حق دارد آن را به هر کس که تمایل دارد اعلام نماید و تکلیفی در اعلام اقامتگاه خود به دیگران ندارد، مگر آن جا که برابر مقررات داخلی کشورها تعهد نموده است که تغییر در اقامتگاه خود را به اطلاع نهاد یا سازمان خاصی برساند یا توافق بر اعلام اقامتگاه نموده باشد. در غیر اینصورت اقامتگاه جزو حریم خصوصی شخصی محسوب شده و غیر قابل تعرض می باشد.

مکاتبات افراد نیز جزو حریم خصوصی معنوی اشخاص و مصادیقی از زندگی خصوصی آنهاست و نمی توان به اطلاع یا فاش نمودن یا علنی نمودن آنها اقدام کرد. مکاتبات افراد تا زمانی که از طرف صاحب آن ها اجازه داده نشود، خصوصی بوده و تلاش برای اطلاع از آنها نقض حریم خصوصی می باشد. البته باید این قید را اضافه نمود که برخی مکاتبات به واسطه اینکه حامل اطلاعات مهمی در مورد جرایم یا حقوق عمومی هستند، با دخالت مقامات صالحه قضایی و در جریان دادرسی قابل دسترسی و استفاده، آن هم فقط برای مقامات مذکور هستند.

ج - ماده ۱۷ میثاق بین المللی حقوق مدنی و سیاسی

۱. هیچکس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات، مورد مداخله خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیر قانونی واقع شود.

۲. و هر کسی حق دارد در مقابل اینگونه مداخلات یا تعرض ها از حمایت قانون برخوردار شود.

ماده ۱۷ میثاق تا حدودی همان پیام ماده ۱۲ اعلامیه جهانی حقوق بشر را دارد. با این تفاوت که در ماده ۱۷ پای قوانین را به میان کشیده و ورود به حریم خصوصی افراد را با مجوز قانون قبول نموده است. ماده ۱۷ میثاق مداخلاتی را که وفق قانون باشد نقض حریم خصوصی نمی داند و به نوعی قوای عمومی و قانونی را در ورود به حریم خصوصی افراد اعم از اقامتگاه، مکاتبات زندگی خصوصی و خانوادگی محق می داند. برابر ماده ۱۷ هر گاه قانون اجازه ورود به حریم خصوصی اشخاص را صادر نماید، شخص نمی تواند در مقابل آن

مقاومت کرده و به حراست از حریم خصوصی خود برخیزد؛ زیرا این امر با اراده و خواست قانون صورت گرفته است و قانون انعکاس و تجسم و بیان اراده عمومی است (ماده ۶ اعلامیه حقوق بشر و شهروند فرانسه) و نمی توان به بهانه دفاع از حریم خصوصی، مانع از اعمال اراده عمومی گردید؛ اما نحوه عمل اراده عمومی بایستی توسط قانون مشخص و مضیق گردد.

ماده ۱۷ میثاق با این مجوز به دفاع از حقوق عمومی در مقابل بخشی از حقوق خصوصی افراد پرداخته است. بند دو ماده ۱۷ به افراد حق می دهد که در مقابل تعرضات غیر قانونی به حریم خصوصی آنها اقدام نمایند، به شرطی که این تعرضات غیر قانونی باشند. بنابراین چنانچه تفتیش منازل به دستور قاضی و به موجب قانون باشد، حریمی برای شخصی باقی نخواهد ماند تا آن را خصوصی قلمداد کرده و به دفاع از آن برخیزد. در این حالت دفاع از حریم، مقاومت در مقابل قانون محسوب شده و حمایت نخواهد شد.

بند دوم - مقررات داخلی

در قوانین و مقررات داخلی 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 - 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 می رسد حقوق را مصداق حریم خصوصی معنوی و مسکن را مصداق حریم خصوصی مادی بیان نموده است. اما به نظر می رسد در مورد مسکن با توجه به مفهوم و معنای لغوی آن که افاده محل سکونت را می نماید و محل سکونت نیز عرفاً به جایی گفته می شود که صرفاً به منظور سکونت از آن بهره برداری می شود، نمی توان اماکنی که غیر از سکونت از آن استفاده دیگری می شود را داخل در موضوع اصل ۲۲ قرار داد و برای آنها قایل به حریم خصوصی شد. مثلاً نمی توان محل کسب و کار اشخاص را دارای در حریم خصوصی دانست، زیرا محل سکونت یا مسکن نیستند؛ در حالی که می بایست هر محدوده و مکانی را که شخص در آن دارای امور خصوصی می باشد دارای حریم دانست. در این صورت چنانچه مثلاً مکان کسب و تجارت را جزو حریم خصوصی ندانیم، مطابق اصل ۲۲ بدون تجویز قانون هم می توان به آن اماکن تعرض نمود! که بطور قطع این با هدف مقنن اساسی در تعارض بوده و به نوعی نقض غرض محسوب می گردد.

سوالی که در اینجا مطرح می شود اینکه، آیا برای نظارت یا کنترل و باز بینی ورود به اماکن غیر مسکونی، وجود نهادی مانند کمیته اماکن ضروری است و آیا وجود آن موافق با قانون اساسی می باشد یا خیر؟ به نظر می رسد با استفاده از همین ضعف قانون اساسی در این قسمت است که امکان ورود به حریم خصوصی اماکن غیر مسکونی به راحتی 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 می باشد.

ب - اصل ۲۵ قانون اساسی

«بازرسی و نرساندن نامه ها، 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 می باشد. 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 صاحب آن محترم و با ارزش است و چه بسا این حریم حاصل تفکرات یا احساسات یا هر گونه تمایلات و روحیات اشخاص باشد. می توان گفت در همین راستا اعمال شکنجه برای اعتراف به امری مصداق بارز نقض حریم حقوق معنوی اشخاص می باشد. آنچه اصل ۲۵ قانون اساسی بدان تصریح دارد، ضامن بخشی از امنیت اجتماعی شهروندان می باشد 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 می باشند، به طور مثال استراق سمع و افشای آن می تواند 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، امکان پذیر 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 به منظور نظارت و یا تحقیقات قضایی تصویب گردد، حریم خصوصی اشخاص شکسته شده و این اصل مهم قانون اساسی نادیده گرفته می شود. 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 می بایست قانونی وجود داشته باشد و فقط به موجب قانون می

توان 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 مامورین 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 آزادی های عمومی و حریم خصوصی اشخاص بوده و قابل رسیدگی در محاکم قضایی می باشد. (ربیعی، ۱۳۸۳، ۹).

ج - مواد ۵۸۰ و ۵۸۲ قانون مجازات اسلامی

هر یک از مستخدمین و مامورین قضایی یا غیر قضایی یا کسی که خدمت دولتی به او ارجاع شده باشد، بدون ترتیب قانونی بدون اجازه و رضای صاحب منزل داخل منزل کسی شود، به حبس از یک ماه تا یکسال محکوم خواهد شد؛ مگر ثابت نماید به امر یکی از روسای خود که صلاحیت حکم را داشته است مکره به اطاعت امر بوده و اقدام کرده است که در اینصورت مجازات مزبور در حق آمر اجرا خواهد شد و اگر مرتکب یا سبب وقوع جرم دیگری نیز باشد مجازات آن را نیز خواهد دید و چنانچه این عمل در شب واقع شود مرتکب یا آمر به حداکثر مجازات مقرر محکوم خواهد شد.

این ماده با دایره شمول محدودی که دارد اختصاصاً ورود به منزل اشخاص را توسط مستخدمین و مامورین قضایی یا غیر قضایی یا کسی که خدمت دولتی به او ارجاع شده، ممنوع اعلام می نماید و ورود افراد مذکور را منوط به اجازه و رضایت صاحب منزل دانسته است. اما نباید صاحب منزل را به مالک منزل تعبیر نماییم. هدف از ماده ۵۸۰ حفظ حریم خصوصی ساکنین منزل می باشد، نه مراعات حال مالک منزل که ممکن است در آن سکونت هم نداشته باشد؛ زیرا حریم خصوصی ساکنین منزل با سکونت آنها موجودیت یافته و این حریم مربوط به منزل است نه مالک آن. بنابراین چنانچه قبلاً نیز عنوان گردید حریم خصوصی مادی استلزامی با مالکیت ندارد. حریم خصوصی متصرف ملک (مثلاً مستاجر) در مقابل مالک قانونی آن محفوظ است و مالک اگر چه حق مالکیت بر ملک خود را دارد، اما حق ندارد حریم خصوصی متصرف آن را نادیده بگیرد.

حکم ماده ۵۸۰ قانون مجازات اسلامی ناظر بر حکم آمر بر مامورین دولتی می باشد. در این ماده حریم خصوصی اشخاص در مقابل تهدیدات احتمالی مامورین دولتی حفظ گردیده است و ضمانت اجرای کیفری نیز برای آن در نظر گرفته شده است. شرط نقض حریم خصوصی منزل در ماده ۵۸۰ قانون مجازات آن است که اولاً ورود بدون ترتیب قانونی صورت گرفته باشد (ترتیب قانونی در اصول ۲۲ و ۲۵ قانون اساسی و مواد ۱۹۶ الی ۱۰۳ قانون آیین دادرسی کیفری بطور کلی بیان گردیده است). بنابراین مامورین دولتی باید در ورود به منزل افراد، مراعات ضوابط قانونی را نموده و صرفاً با مجوز و با رعایت ترتیبات قانونی اقدام به ورود نمایند. البته ماده ۵۸۰ این امر را نیز پیش بینی نموده که مأمور ممکن است در اجرای دستورات آمر قانونی خود مجبور به ورود غیر قانونی به منزل اشخاص شود که در اینصورت مسئولیت نقض حریم خصوصی منزل متوجه آمر خواهد بود و ضمانت اجرای ورود غیر قانونی نیز در حق آمر اجرا خواهد شد. (نقدی فر، ۱۳۸۲، ۸۸)

د - حریم خصوصی در قانون مدنی

در قانون مدنی نیز موضوع حریم خصوصی مورد غفلت قرار نگرفته و در چندین ماده به آن اشاره شده است. مانند ماده ۹۷ که بیان می دارد: "هر گاه کسی از قدیم درخانه یا ملک دیگری مجرای آب به ملک خود یا حق مرور داشته، صاحب خانه یا مالک نمی تواند مانع آب بردن یا عبور او از ملک خود شود و همچنین است سایر حقوق از قبیل حق داشتن در و شبکه و ناودان حق شرب و غیره" این ماده اجازه می دهد که شخصی که از قبل حق ورود به ملک دیگری را برای بردن آب یا عبور داشته، وارد حریم دیگری شده و صاحب ملک و درواقع صاحب حریم حق منع او را ندارد.

همچنین در قانون مدنی در ماده ۱۳۶ در مبحث املاک چنین آمده است: «حریم مقداری از اراضی اطراف ملک وقتان ونهرو امثال آن است که برای کمال انتفاع از آن ضرورت دارد». قانون مدنی در این تعریف صرفاً به حریم مادی آن هم ویژه املاک نظر دارد و توجهی به حریم مکان یا حریم معنوی ندارد. البته قانون مدنی مبحث حریم املاک را در فصل حق انتفاع نسبت به ملک غیر و در احکام و آثار املاک نسبت به املاک مجاور آورده است و در مواد بعدی نیز هر جا که به طریقی نظر به حریم داشته، صرفاً برای تعیین حدود املاک است؛ نه حفاظت از حریم اشخاص. بنابراین موضوع حریم در قانون مدنی املاک هستند و اشخاص صرفاً بعنوان صاحبان املاک و برای حفاظت از حریم املاک دارای حقوقی می باشند و در قانون مدنی از حریم خصوصی در معنایی که مورد نظر ماست، سخن روشنی به میان نیامده است و به واقع جای بیان تعریف و چاره جویی قانونی در مورد حفاظت از حریم خصوصی در قانون مدنی کاملاً خالی است. اگر چه در گذشته به مفهوم حریم خصوصی به عنوان یکی از مفاهیم حقوق بشری و یکی از شاخه های حقوق اشخاص بی توجهی شده است، اما جا دارد در حال حاضر با الحاقات و اضافاتی در قانون مدنی به طور جدی به این مقوله پرداخته شود؛ چرا که حریم خصوصی اشخاص ناشی از مدنیت زندگی اجتماعی بوده و چه عرصه ای شایسته تر از قانون مدنی که به این موضوع بپردازد؟

گفتار چهارم: حمایت از حریم خصوصی در فضای دولت الکترونیک

حریم خصوصی مورد حمایت دولت الکترونیک است. اما این حمایت دارای اصول و استانداردهایی است که در این گفتار مورد بررسی قرار می‌گیرد.

بند اول: اصول مربوط به حقوق سوژه

الف - 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 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 - اصل مشارکت

۱ - حق دسترسی

بموجب 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 آنرا 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 بطور 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. این ویژگی و خصیصه فاوا (فضای اطلاعات و امنیت) وقتی در کنار مشکل فقدان همگونی و هماهنگی تام میان مقررات نظامهای مختلف حقوقی قرار می‌گیرد، بویژه در بحث حمایت از داده‌ها، اهمیت مضاعف می‌یابد. فرض کنیم که پردازش و افشاء (و نه انتقال) داده‌های شخصی شهروندان در کشور الف ممنوع بوده، ولی در کشور ب حکم مشابهی وجود ندارد. در چنین وضعیتی اگر شخصی با تحصیل داده‌های شخص دیگر در کشور الف آنها را از طریق رایانامه (e-mail) برای دوست خود که در کشور ب سکونت دارد ارسال نماید و از او بخواهد که داده‌ها را از طریق یک وبلاگ یا سایت اختصاصی خود منتشر کند، در این مثال کسی تردیدی نخواهد داشت که نتیجه حاصل با فرضی که ارسال کننده داده‌ها خود اقدام به افشاء و انتشار آنها می‌نمود هیچ تفاوتی ندارد و در هر دو فرض، حریم خصوصی شخص سوژه به یک اندازه مورد تعدی و تجاوز قرار گرفته است.

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 (Transborder data flow) است. اهمیت این اصل تا بدانجاست که بدون آن در مقام حمایت از داده نقض غرض حاصل می‌شود. برخی کشورها (که عمدتاً در زمره کشورهای تولید کننده داده‌ها و اطلاعات می‌باشند نظیر کشورهای اروپایی) انتقال داده‌ها به کشورهای فاقد سطح کافی حمایت از داده را ممنوع نموده‌اند تا جایی که حتی ایالات متحده آمریکا برای پاسخ به نیاز موسسات این کشور (که از دید اروپائیان فاقد سطح کافی حمایت از داده است) به مبادله اطلاعات و داده‌ها با هم‌تایان اروپایی خود ناگزیر از تدوین موافقت نامه بندگاه امن (Safe Harbor Agreement) با اروپائیان شد. (اصلانی، ۱۳۸۹، ۸)

بند دوم: اصول و استانداردهای حمایت از داده

تردیدی در لزوم حمایت از محرمانگی و امنیت داده‌های شخصی در فضای مجازی نیست. لیکن سوال اساسی این است که ماهیت این حمایت چیست؟ و قواعد حقوقی مربوطه+ دقیقاً چه الزاماتی را به همراه دارند؟ برای پاسخ به این سوال باید گفت که مجموعه الزامات و ضوابط حاکم بر مساله حمایت از داده (بویژه 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 هر یک خواهیم داشت. این اصول مبین الزامات لازم‌الرعایه در عرصه حمایت از حریم خصوصی می‌باشند.

الف - 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، ۱۴۵)

۲- اصل تحصیل محدود و مرتبط

بموجب این اصل اولاً تحصیل داده ها تنها برای هدف قانونی و مشروع مجاز است (یا لاقلاً می توان گفت تحصیل داده ها برای هدف غیر قانونی یا نامشروع ممنوع است). ثانیاً نوع داده های گردآوری شده باید با هدف اولیه تحصیل داده ها منطبق باشد. ثالثاً گردآوری داده ها باید تنها به میزان مورد نیاز برای هدف اولیه و اعلام شده صورت گیرد و گردآوری داده های اضافه بر نیاز ممنوع است. (یعقوبی، ۱۳۸۸، ۱۹)

۲-۱- اصل انتخاب

اصل انتخاب بدان معناست که موسسه یا شخصی که قصد گردآوری داده ها در خصوص شخص سوژه را دارد، پیش از هر چیز می باید این امکان را برای کاربر فراهم آورد که صراحتاً نظر خود را مبنی بر اینکه آیا با گردآوری داده های شخصی خود موافقت دارد یا خیر؟ اعلام نماید.

۲-۲- اصل اطلاع

مفهوم اصل اطلاع آن است که گردآوری و پردازش داده های شخصی (حداقل در خصوص پردازش های تغییر دهنده داده) منوط به اعلام مراتب به شخص سوژه می باشد، مگر در مواردی که قانون بنا به پاره ای مصالح استثنایی و مصرح (همچون مسائل امنیتی) خلاف آن را مقرر دارد. (رضایی زاده، ۱۳۹۰، ۱۴۸)

ب- اصول مربوط به نگهداری و پردازش داده

۱- اصل پردازش مرتبط یا محدودیت استفاده

براساس این اصل گردآورنده و پردازشگر داده ها تنها اجازه پردازش داده ها 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 داده ها به اشخاص ثالث و به منظور نیل به یک هدف ثانوی، امری است که علی الاصول در چارچوب اجازه اولیه صادره از سوی سوژه یا قانونگذار نمی گنجد و لذا ممنوع است. این اصل در تمامی مراحل تحصیل پردازش و انتقال داده ها لازم الرعایه می باشد. (رضایی زاده، ۱۳۹۰، ۱۴۹)

برخی از صاحبان مشاغل به مناسبت شغل خود، بر اسرار و اطلاعات خصوصی دیگران مطلع می گردند که سوء استفاده از این اطلاعات و یا افشاء آن موجب نقض حریم خصوصی اشخاص می گردد. برخی از این مشاغل عمومی و دولتی هستند، برخی دیگر مشاغل عمومی غیردولتی هستند و برخی دیگر مشاغل بخش خصوصی می باشند. ماده ۶۴۸ قانون مجازات اسلامی طی حکم عامی دارندگان تمام این مشاغل را به حفظ اطلاعات مردم الزام کرده و مقرر می دارد: «اطباء و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می شوند، هرگاه در غیر از موارد قانونی اسرار مردم را افشاء کنند به ۳ ماه و یک روز تا یک سال و یا به یک میلیون و پانصد هزار ریال تا شش میلیون ریال جزای نقدی محکوم می شوند».

این ماده در خصوص مشاغل، کلی است؛ لذا شامل مشاغل دولتی و غیردولتی می گردد. بر همین اساس مأمورین دولتی که به مناسبت شغل خود بر پاره ای از اسرار افراد مطلع می گردند، حق ندارند اولاً خارج از محدوده ای که مرتبط با موضوع کاری و ضرورت های قانونی است کسب اطلاع نمایند و ثانیاً حق ندارند از مطالب به دست آمده خارج از محدوده لازم استفاده ای نمایند و یا آن اطلاعات را افشاء نمایند.

احکام خاصی نیز درباره حرفه های مشخصی وجود دارد که ذیلاً به بررسی آنها می پردازیم:

۲-۱- مسئولیت مشاغل عمومی در زمینه حفظ اسرار مردم

به علت اینکه دارندگان مشاغل و مناصب عمومی امکانات بیشتری برای دستیابی به اطلاعات خصوصی شهروندان دارند و همچنین اطلاعاتی که ایشان به دست می آورند از حساسیت بیشتری برخوردار است، مقنن در مورد این مشاغل حساسیت بیشتری به خرج داده است و این دست مشاغل را به حفظ حریم خصوصی اطلاعاتی شهروندان مکلف کرده است. به طور خلاصه این مشاغل عبارتند از:

۲-۱-۱- مسئولیت قضا و ضابطین در قبال اطلاعات ناشی از رسیدگی و محاکمه قضایی

قضات مکلفند دقت لازم برای جلوگیری از افشای مضمون و محتوای اسناد شخصی غیرمرتبط با اتهام را در طول تحقیقات به عمل آورند. همچنین بایستی در موارد لازم به ویژه در مورد اطفال محاکمه را غیرعلنی برگزار نمایند و در محاکمات علنی نیز بهتر است به اصحاب رسانه درباره ممنوعیت انتشار جریان محاکمه تا قبل از قطعی شدن حکم تذکرات لازم را ارائه دهند. براساس تبصره ۱ ماده ۱۸۸ قانون آ.د.ع.ا.د.ا.ک: «منظور از علنی بودن محاکمه، عدم ایجاد مانع جهت حضور افراد در دادگاه می باشد لکن انتشار آن در رسانه های گروهی قبل از قطعی شدن حکم مجاز نخواهد بود و متخلف از این تبصره به مجازات مفتری محکوم می شود».

همچنین ضابطین قضایی وفق ماده ۲۴ قانون آ.د.ع.د.ا.ک مکلفند برای تفتیش منازل، اجازه مقام قضایی را کسب کنند و براساس ماده ۸ «قانون احترام به آزادی های مشروع و حفظ حقوق شهروندی» مصوب ۱۳۸۲، در حین بازرسی و معاینات محلی نیز مجاز به تعرض نسبت به اسناد و مدارک و اشیایی که ارتباطی با جرم نداشته و یا به متهم تعلق ندارد و افشای مضمون نامه ها و نوشته ها و عکس های فامیلی و فیلم های خانوادگی و ضبط بی مورد آنها نمی باشند.

۲-۱-۲- مسئولیت مستخدمین و مأمورین دولتی در قبال مراسلات یا مخابرات یا مکالمات تلفنی

براساس ماده ۵۸۲ قانون مجازات اسلامی: «هر یک از مستخدمین و مأمورین دولتی، مراسلات یا مخابرات یا مکالمات تلفنی اشخاص را در غیر موارد که قانون اجازه داده حسب مورد مفتوح یا توقیف یا معدوم یا بازرسی یا استراق سمع نماید یا بدون اجازه صاحبان آنها مطالب آنها را افشاء نماید، به حبس از یک تا سه سال و یا جزای نقدی از شش تا هجده میلیون ریال محکوم خواهد شد». براساس این ماده مأمورین در مراسلات و مخابرات و مکالمات مکلفند دو شرط ذکر شده در قانون را رعایت نمایند؛ در غیر اینصورت فقط مقام قضایی می تواند در محدوده قانونی دستور مناسب صادر نماید. بر همین مبنا افشای اسرار اشخاصی که متهم باشند نیز ممنوع است. (باصری، ۱۳۹۱، ۱۳۰)

۳-۱-۲- مسئولیت مأمورین مالیاتی

ماده ۲۳۲ «قانون مالیات های مستقیم» مصوب ۱۳۶۶ نیز مأمورین مالیاتی را از افشاء اطلاعات مودیان مالیاتی منع نموده است. این ماده مقرر می دارد: «مأمورین تشخیص و سایر مراجع مالیاتی باید اطلاعاتی را که ضمن رسیدگی به امور مالیاتی مودی به دست می آورند، محرمانه تلقی و از افشای آن جز در امر تشخیص درآمد و مالیات نزد مراجع ذیربط در حد نیاز خودداری نمایند و در صورت افشاء طبق قانون مجازات اسلامی با آنان رفتار خواهد شد».

۴-۱-۲- محرمانه بودن اطلاعات در آمارگیری

ماده ۷ «قانون مرکز آمار ایران» مصوب ۱۳۵۴/۱۱/۱۰ مقرر می دارد: «هر شخص ساکن ایران همچنین اتباع ایرانی مقیم خارج از کشور مکلف اند به پرسش های مربوط به کلیه سرشماری ها و آمارگیری ها که توسط مرکز آمار ایران انجام می شود پاسخ صحیحی دهند. آمار و اطلاعاتی که ضمن آمارگیری های مختلف از افراد و مؤسسات جمع آوری می شود محرمانه خواهد بود و جز در تهیه آمارهای کلی و عمومی نباید مورد استفاده قرار گیرد. استفاده و مطالبه و استناد به اطلاعات جمع آوری شده از افراد و مؤسسات به هیچ وجه در مراجع قضایی و اداری و مالیاتی و نظائر آن مجاز نخواهد بود». این ماده اقدام به بیان اصل رازداری حرفه ای جهت ایجاد اطمینان به عدم افشاء این گونه اطلاعات نموده است.

۵-۱-۲- اطلاعات مربوط به پولشویی

براساس ماده ۶ لایحه مبارزه با پول شویی: «اطلاعات و اسناد گردآوری شده و اجرای این قانون، صرفاً در جهت اهداف تعیین شده در قانون مبارزه با پول شویی و جرائم منشاء آن مورد استفاده قرار خواهد گرفت. افشای اطلاعات یا استفاده از آن به نفع خود یا دیگری به طور مستقیم یا غیر مستقیم توسط مأموران دولتی یا سایر اشخاص مقرر در این قانون ممنوع بوده و متخلفین به مجازات مندرج در قانون مرتکبان افشای اسناد محرمانه و سری دولتی، محکوم خواهند شد».

۶-۱-۲- مسئولیت اشخاص دارای اطلاعات نهانی در بازار بورس

براساس قانون بازار اوراق بهادار (مصوب ۱۳۸۴)، دست اندرکاران اطلاعات بازار بورس در قبال اطلاعات نهانی این بازار دارای مسئولیت می باشند. براساس ماده ۴۶ این قانون: «اشخاص زیر به حبس تعزیری از سه ماه تا یک سال یا به جزای نقدی معادل دو تا پنج برابر سود به دست آمده یا زیان متحمل نشده یا هر دو مجازات محکوم خواهند شد».

۱. هر شخصی که اطلاعات نهانی مربوط به اوراق بهادار موضوع این قانون را که حسب وظیفه در اختیار وی قرار گرفته به نحوی از انحاء به ضرر دیگران یا به نفع خود یا به نفع اشخاصی که از طرف آنها به هر عنوان نمایندگی داشته؛ قبل از انتشار عمومی، مورد استفاده قرار دهد و یا موجبات افشاء و انتشار آنها را در غیر موارد مقدر فراهم نماید.
۲. هر شخصی که با استفاده از اطلاعات نهانی به معاملات اوراق بهادار مبادرت نماید».

۷-۱-۲- مسئولیت مشاغل عمومی غیردولتی در قبال اطلاعات شهروندان

برخی از مشاغل یک وظیفه و مأموریت عمومی انجام می دهند، در حالی که دارندگان این مشاغل مأموران دولتی محسوب نمی شوند. از این دسته مشاغل، در مورد سه حرفه، حکم صریح مبنی بر تکلیف به حفظ اطلاعات اشخاص وجود دارد. این افراد عبارتند از کارشناسان رسمی دادگستری، مترجمان رسمی و سردفتران و دفتریاران. ماده ۲۶ «قانون کنون کارشناسان رسمی دادگستری» مصوب ۱۳۸۱/۱/۱۸ یکی از موارد تخلف کارشناسان را که دارای مجازات انتظامی است افشای اسرار و اسناد محرمانه اشخاص دانسته است. ماده ۲۷

«آیین نامه مترجمان رسمی» مصوب ۱۳۷۴ مترجم را مکلف نموده تا اسراری که در اثر ترجمه به آنها واقف می شود را حفظ نماید و در نهایت ماده ۵۱ «قانون دفاتر اسناد رسمی» مصوب ۱۳۱۶ مقرر کرده که «سردفتران و دفتریاران و به طور کلی تمام کارکنان دفترخانه باید اسرار ارباب رجوع و متعاملین را که بر اثر تنظیم یا ثبت آن از آنها اطلاع حاصل کرده اند مکتوم دارند».

۲-۲- مسئولیت شاغلان بخش خصوصی

برخی از مشاغل بخش خصوصی به لحاظ ماهیت خود با اسرار بسیار مهم شهروندان سروکار دارند که برای حمایت از این اطلاعات، مقنن احکام خاصی را وضع کرده است. این مشاغل عبارتند از وکلا، پزشکان و اصحاب رسانه.

۱-۲-۲- مسئولیت وکلا در حفظ اسرار موکلین

اشخاص هنگام مراجعه به وکلا ممکن است به ناچار و به لحاظ ضرورت کار خود، مدارک و اطلاعاتی را مطرح نمایند که افشاء آنها، حیثیت ایشان را به مخاطره اندازد. به همین جهت ماده ۳۰ «قانون وکالت ایران» مصوب ۱۳۱۵ مقرر نموده: «وکیل باید اسراری را که به واسطه وکالت از طرف موکل مطلع شده و همچنین اسرار مربوطه به حیثیت و شرافت و اعتبارات موکل را حفظ نماید».

مسئلاً تخطی از این وظیفه و ورود خسارات ناشی از فعل یا ترک فعلی که براساس قانون مرتبط با شخص می باشد، موجب ایجاد مسئولیت قانونی (از جمله مسئولیت مدنی) خواهد شد.

۲-۲-۲- مسئولیت شاغلین حرفه پزشکی

چنانچه در ماده ۶۴۸ قانون مجازات اسلامی ملاحظه شد، دارندگان تمام مشاغلی که به اطلاعات خصوصی مردم دسترسی پیدا می کنند مکلف به حفظ اطلاعات ایشان شده‌اند که از آن جمله شاغلین در زمینه پزشکی هستند که به لحاظ اهمیت شغل و اطلاعات ناشی از آن، در این ماده صراحتاً از ایشان نام برده شده است. این ماده مقرر می دارد: «اطباء و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می شوند، هرگاه در غیر از موارد قانونی اسرار مردم را افشاء کنند؛ به سه ماه و یک روز تا یک سال و یا به یک میلیون و پانصد هزار ریال تا شش میلیون ریال جزای نقدی محکوم می شوند».

ماده ۴ آیین نامه انتظامی رسیدگی به تخلفات صنفی و حرفه‌ای شاغلان حرفه پزشکی نیز در این زمینه مقرر می کند: «شاغلان حرفه پزشکی موظفند اسرار و نوع بیماری بیمار را، مگر در موارد تصریح شده در قوانین حفظ کنند».

۳-۲-۲- مسئولیت اصحاب رسانه

براساس ماده ۳۱ قانون مطبوعات (اصلاحی ۱۳۷۹/۱/۳۰): «انتشار مطالبی که مشتمل بر تهدید به هتک شرف و یا حیثیت و یا افشای اسرار شخصی باشد ممنوع است و مدیر مسئول به محاکم قضایی معرفی و با وی طبق قانون تعزیرات رفتار خواهد شد».

این ماده می‌تواند تقییدی بر ماده ۶۹۷ ق.م.ا.ر.ج به افتراء محسوب شود و چون موخر بر آن و خاص از آن است، می‌تواند شرط اعمال مجازات در صورت عدم اثبات صحت اسناد را منقضي کند. به عبارتی صرف انتشار مطالبی که مشتمل بر تهدید به هتک شرف یا حیثیت و یا افشای اسرار شخصی باشد ممنوع است. البته این ماده قابلیت پوشش تمام مصادیق ماده ۶۹۷ را ندارد، مثلاً نمی‌تواند تقییدی بر نطق در مجامع محسوب شود.

لازم به ذکر است که وفق ماده (۱) قانون اصلاح قانون مطبوعات مصوب ۱۳۸۸/۹/۸، نشریه‌های الکترونیکی و نیز خبرگزاری های داخلی نیز مشمول قانون مطبوعات شد و تقریباً تمام اصحاب رسانه به تکلیف مقرر در ماده ۳۱ قانون مطبوعات ملزم هستند.

ج - اصول مربوط به کیفیت داده

۱ - اصل امنیت

اصل امنیت بدان معناست که کسی که داده ها را تحصیل نموده یا در اختیار دارد، می بایست تدابیر امنیتی لازم برای جلوگیری از دسترسی یا پردازش غیر مجاز داده ها توسط دیگران را بکار گیرد و عدم بکار گیری چنین تدابیری موجب مسئولیت اوست. (رضایی زاده، ۱۳۹۰، ۱۴۵)

۲ - اصل صحت و به روز بودن

این اصل که اصلی کیفی بوده و ناظر بر محتوای داده ها است، اقتضای آنرا دارد که موسسه یا شخصی که به گردآوری و پردازش داده ها می پردازد در تمام مراحل، نه تنها داده های صحیحی را گردآوری، پردازش و منتقل نماید؛ بلکه ترتیبات و تدابیر مقتضی را برای حصول اطمینان از صحیح، کامل بودن و روزآمد بودن داده ها نیز بکار گیرد.

گفتار پنجم: وضعیت حمایت از حریم خصوصی در کشورهای منتخب

اصولاً نظر به حساسیت و اهمیتی که ممکن است پردازش داده های شخصی یا ارتکاب سایر اعمال ممنوعه فوق الاشعار نسبت بدانها در پی داشته باشد، مقررات ویژه ای برای حمایت از آنها در حقوق خارجی در نظر گرفته شده است که ذیلاً اشاره ای گذرا به چگونگی حمایت از این داده ها و اعمال اصول فوق در چند نظام حقوقی پیشرو، می افکنیم.

بند اول: اتحادیه اروپایی

بند ۱ ماده ۸ دستورالعمل شماره EC۴۶/۹۵/اتحادیه اروپایی مقرر می دارد: «کشورهای عضو پردازش داده های شخصی مربوط به ریشه های قومی و نژادی، اعتقادات سیاسی، عقاید دینی و فلسفی، عضویت در اتحادیه های تجاری و پردازش داده های مربوط به سلامتی و زندگی جنسی را ممنوع خواهند نمود.» داده های موضوع این ماده که به «داده های شخصی حساس» معروفند، تقریباً در اغلب قوانین و متون قانونی مشابه مشمول حمایت هایی بیشتر از سایر داده ها قرار گرفته اند. همانگونه که ملاحظه می شود مطابق این ماده از دستورالعمل که در واقع راهنمای کشورهای عضو در امر قانون نویسی در عرصه حمایت از داده های شخصی می باشد، داده های مربوط به سلامتی اشخاص در زمره داده های مورد حمایت بوده و پردازش آنها جز در موارد مصرح مجاز نمی باشد. (خلیل، ۲۰۱۱، ۳۹۴)

همچنین ماده ۵ این سند تکلیف کشورهای عضو دائر بر لزوم تعیین دقیق موارد استثناء از حکم مزبور را پیش بینی نموده است. نکته ای که در اینجا ذکر آن ضروری است تعریف واژه «پردازش» بوده که در ماده ۸ فوق ممنوع شده است. مطابق بند b ماده ۲ این سند پردازش داده های شخصی یعنی عملیات یا مجموعه عملیاتی است که بر روی داده های شخصی انجام می شود، خواه از طریق ابزارهای خودکار و خواه توسط ابزارهای غیر خودکار از قبیل تحصیل، ضبط کردن، سازماندهی، ذخیره نمودن، هماهنگ نمودن یا جایگزین نمودن، بازیابی، استفاده، افشاء از طریق انتقال، انتشار یا در دسترس قرار دادن از طرق دیگر، دسته بندی یا ترکیب، انسداد، امحاء یا تخریب داده ها.

بر این اساس ملاحظه می شود که مجموعه اعمال ممنوعی که مطابق این تعریف، با ملحوظ داشتن حکم ماده ۸ پیش گفته، بایستی در خصوص داده های شخصی مربوط به سلامتی مورد رعایت قرار گیرد؛ طیف وسیعی از اعمال را در برمی گیرد. همچنین در دستورالعمل فوق مطابق بند ۲ همان ماده؛ پردازش این قبیل داده ها در پنج مورد مجاز شمرده شده است، که در واقع استثنای اصل فوق می باشند. لازم به توضیح است که هرچند در این دستورالعمل و برخی متون قانونی مشابه عبارت داده های مربوط به ریشه های قومی و نژادی مستقل از داده های مربوط به سلامتی و خصوصیات وراثتی بکار رفته است، لیکن به اعتقاد ما با کمی مسامحه می توان این گونه داده ها را در زمره داده های وراثتی مورد بررسی قرار داد. (خلیل، ۲۰۱۱، ۳۹۸)

بند دوم: انگلستان

قانون حمایت از داده انگلستان مصوب (۱۹۹۸) نیز در ماده ۲، داده های شخصی حساس را در ۸ بند برشمرده که بند پنجم آن به داده های مربوط به سلامتی و شرایط جسمانی یا روانی شخص سوژه اختصاص دارد و در جدول شماره ۳ ضمیمه، مقررات نسبتاً مفصلی مربوط به پردازش داده ها از جمله داده های شخصی حساس را مقرر نموده است. این مقررات که نوعاً تحت تاثیر دستورالعمل فوق اشاره تنظیم شده است تا حدود زیادی از حیث محتوا با احکام دستورالعمل مزبور انطباق دارد.

بند سوم: ایالات متحده امریکا

(Health Insurance Portability and Accountability Act)

عبارت فوق عنوان قانون مصوب امریکا در سال ۱۹۹۶ است که یک قانون فدرال می باشد. همچنین سازمانی با همین نام متکفل قاعده مند نمودن نحوه تحصیل و پردازش داده های مربوط به سلامتی اشخاص می باشند. اهم مفاد و اصول مندرج در این قانون عبارتند از:

- حداقل استانداردهای ملی لازم الرعایه
- اعلام رویه مورد عمل در حمایت از حریم خصوصی بیمار، به او
- حق دسترسی بیمار به فایل های حاوی داده های او
- حق اصلاح داده های نادرست
- اعلام موارد افشاء داده های بیمار در موارد مجاز افشاء، به او
- وظایف بیمارستانها و نهادهای مشابه در جهت آموزش و بکارگیری رویه های فنی و اداری متناسب، انتصاب کارکنان و مرجع پاسخگویی
- منع افشاء داده ها به کارفرمایان
- منع افشاء داده های مربوط به سلامت روانی
- حق منع بیمارستان از درج نام بیمار در سیاهه بیماران بیمارستان

– موارد استثناء قانونی

– رسیدگی به شکایات

بند چهارم: وضعیت حمایت از حریم خصوصی در حقوق ایران

در باب وضعیت حقوق ایران در این زمینه باید گفت که حمایت قانونگذار ایرانی از داده های شخصی افراد پیش از تصویب قانون تجارت الکترونیکی، تنها در گستره ای بسیار محدود مسبوق به سابقه می باشد و هرگز قانونگذار ایرانی به فکر حمایت همه جانبه از این داده ها نبوده است.

بعنوان نمونه در قوانین پیشین (قبل از تصویب قانون تجارت الکترونیکی) ماده ۶۴۸ قانون مجازات اسلامی مقرر می دارد: « اطباء و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می شوند؛ هرگاه در غیراز موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می شوند. » اگرچه حکم این ماده نسبت به مانحن فیه خاص بوده و تنها شامل کسانی می شود که به مناسبت شغل خود محرم اسرار مردم می شوند و مطلق دارندگان داده های مربوط به سلامتی را تحت پوشش قرار نمی دهد، لیکن پذیرش این حکم از جانب قانونگذار بویژه با لحاظ تحولات ناشی از پیدایش و گسترش فناوری اطلاعات و ارتباطات مبین آن است که قانونگذار ایران آمادگی و زمینه مناسب برای تهیه قوانین حمایت کننده از داده های مورد بحث را داراست.

در باب وضعیت بحث در پرتو فناوری اطلاعات و ارتباطات در حقوق داخلی نیز باید خاطر نشان نمود که قانونگذار ایران در ماده ۵۸ قانون تجارت الکترونیکی سال ۱۳۸۲ – به عنوان تنها قانونی که به این امر پرداخته است – مقرر می دارد: « ذخیره، پردازش و یا توزیع «داده پیام» های شخصی مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده پیام» های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است.»

همچنین مطابق ماده ۶۰ همان قانون: « ذخیره، پردازش و یا توزیع «داده پیام» های مربوط به سوابق پزشکی و بهداشتی تابع آیین نامه ای است که در ماده (۷۹) این قانون خواهد آمد. » البته این آئین نامه تاکنون به تصویب نرسیده و لذا خلاء قانونی در این خصوص مشهود است. همچنین به موجب ماده ۷۱ قانون فوق الذکر: « هرکس در بستر مبادلات الکترونیکی شرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید، مجرم محسوب شده و به یک تا سه سال حبس محکوم می شود. »

گذشته از ایرادات متعدد نگارشی و قانون نویسی موجود در متن مواد مذکور، باید گفت که مطابق این نصوص قانونی:

اولاً؛ قانونگذار علی الاصول مطلق داده های شخصی را مورد حمایت قرار نداده است، بلکه مصادیق داده های مورد حمایت احصاء شده در ماده ۵۸ فوق مبین آن است که تنها داده های شخصی حساس (از جمله داده های مربوط به سوابق پزشکی و بهداشتی) مورد حمایت قانونگذار می باشد.

ثانیاً؛ مطابق ماده ۵۹ همان قانون که مقرر می دارد: « در صورت رضایت شخص موضوع «داده پیام» نیز به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد؛ ذخیره، پردازش و توزیع «داده پیام» های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

- ۱) اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.
- ۲) «داده پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع آوری برای شخص موضوع «داده پیام» شرح داده شده جمع آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.
- ۳) «داده پیام» باید صحیح و روزآمد باشد.
- ۴) شخص موضوع «داده پیام» باید به پرونده های رایانه ای حاوی «داده پیام» های شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام» های ناقص و یا نادرست را محو یا اصلاح کند.
- ۵) شخص موضوع «داده پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه، درخواست محو کامل پرونده رایانه ای «داده پیام» های شخصی مربوط به خود را بنماید. «

همچنین قید مذکور در ذیل ماده ۵۸ (بدون رضایت صریح آنها) تنها موردی است که در نظر قانونگذار ایرانی به عنوان استثنایی بر اصل ممنوعیت پردازش این گونه داده ها مقرر گردیده است. اخذ رضایت سوژه، البته با رعایت شرایط مقرر در این مواد می باشد و قانونگذار با آنکه در مقام بیان بوده است؛ از موارد خاص و استثنایی که بنا به دلایل امنیتی و مصالح عمومی و امثال ذلک بتوان دست به پردازش این داده ها زد، سخنی به میان نیاورده که این سکوت در مقام بیان موید این نتیجه نه چندان معقول و منطقی است که حتی در چنین شرایط خاصی نیز حاکمیت نباید اقدام به پردازش داده ها کند که البته این امر نیز با رویکرد قانون مزبور که مبتنی بر حداقل حمایت و اصولاً محدودنگر است، چندان انطباقی ندارد.

نتیجه گیری

با توجه به آنچه در این تحقیق بیان کردیم تحقق دولت الکترونیک مستلزم ایجاد پیش زمینه ها و تمهیداتی است که داشتن فناوری های پیشرفته اطلاعاتی و ارتباطی اساس آن بشمار می رود. هر کشوری که بخواهد سهم قابل توجهی از اقتصاد جهانی را داشته باشد، باید بتواند خود را مجهز به مجموعه ای از زیرساخت های مخابراتی پیشرفته کرده و از حداکثر فناوری ها استفاده کند. دولت الکترونیک یک شکل جدید از حکومت داری است برای حصول اطمینان از اینکه همه شهروندان به گونه ای یکسان از فرصت مشارکت در تصمیماتی برخوردارند که به نوعی بر وضعیت و کیفیت زندگی آنها تاثیر می گذارد. این شیوه، شهروندان را از مصرف کنندگان منفعل خدمات دولتی به بازیگران فعال تبدیل می کند که می توانند درباره نوع خدماتی که به آن نیاز دارند اظهار نظر کنند. همچنین دولت الکترونیک با به کارگیری فناوری های جدید ارتباطی و اطلاعاتی به بهبود فرآیندهای ارائه خدمات در بخش عمومی، تسریع ارائه خدمات به شهروندان، پاسخگوشدن ماموران دولتی، شفاف شدن اطلاعات، کاهش فاصله میان مردم و دولتمردان، افزایش مشارکت اثربخش شهروندان و اعضای جامعه مدنی در فرآیند تصمیم گیری عمومی، گسترش عدالت اجتماعی از طریق فرصت های برابر افراد برای دسترسی به اطلاعات و... کمک شایانی می کند و امروزه حکومتی که بخواهد در مسیر تحقق حکومت داری به نحو ایده آل حرکت کند، باید به ابزار نیرومندی همچون دولت الکترونیک مسلح باشد.

دولت الکترونیک می تواند به حکومت ها در بهبود ارتباطات و تامین رضایت مردم کمک کرده، همچنین ایجاد ارتباط دو سویه بین مردم و مسئولان از راه های مختلف را میسر سازد. اطلاع رسانی و آگاه کردن مردم از مصوبات، مقررات و مجموعه وظایف و اختیارات دولت و نیز مشارکت دادن مردم در تصمیم سازی از طریق نظرسنجی الکترونیکی و ایجاد صندوق شکایات از طریق پست الکترونیکی، پاسخگویی سریع به خواسته ها و شکایات مردم و نظایر آن، شیوه هایی است که دامنه ارتباطات مردمی را بیش از پیش گسترده و بهینه می کند. همچنین عرضه خدمات عمومی به صورت الکترونیک مانند پرداخت هزینه های آب، برق، تلفن، قبض جریمه، رزرو بلیت و صدور گذرنامه مزایایی از جمله صرفه جویی در وقت و نیروی انسانی، کاهش تردهای درون شهری و بین شهری و کاهش بار ترافیک را در پی دارد. این امور می توانند در روش زندگی مردم و تامین رفاه و رضایت آنان تاثیر بسزایی داشته باشد و در نهایت می تواند موجبات توسعه و رشد اقتصادی، اجتماعی، فرهنگی و سیاسی را در کشور فراهم سازد.

نگاه به حقوق کشورهای پیشرو در این زمینه، مبین اتخاذ رویکرد منطقی و متوازن این نظام های حقوقی در حمایت از داده ها است؛ رویکردی که مبتنی بر اصل اولیه حمایت و امکان ترتیب استثنای قانونی بر این اصل اولیه می باشد. برخلاف نظام های حقوقی مزبور، قانونگذار ایران در این زمینه رویکردی دوگانه اتخاذ نموده است. از یک سو مطلق این گونه داده را مورد حمایت قرار نداده و تنها صور خاصی از آن را، آن هم در صورتی که در قالب داده پیام باشد، مورد حمایت تلقی نموده است و از سوی دیگر هیچ گونه استثنایی را جز اخذ رضایت شخص سوژه در این مسیر به رسمیت نشناخته است. بنابراین روشن نیست که در برخورد با مواردی که گردآوری و پردازش این داده ها برای تامین سلامت عمومی یا امنیت و مصالح عمومی ضروری می باشد، همچنین در خصوص مواردی که استفاده تنها جنبه آماری یا علمی تحقیقاتی دارد، چه رویکردی را اتخاذ نموده است؟

در کشور ما بررسی عملکرد دولتهای مختلف در به اجرا در آوردن طرح دولت الکترونیک نشانگر آن است که مشکل اصلی ایجاد و توسعه دولت الکترونیک تکنولوژی نیست. با توجه به اینکه فرهنگ جامعه ایران ترکیبی از دو فرهنگ ملی و دینی (ارزشی) است، الکترونیکی بودن در صورتی که با تمام جنبه های فرهنگ جامعه ایران سازگار باشد، ضروری به نظر می رسد. لذا بایستی از یک سری جنبه های زائد الکترونیکی شدن چشم پوشی کرد و در کنار آن برخی جنبه های فرهنگی جامعه را تعدیل نمود تا بتوان دولت الکترونیک و مجازی را بکار گرفت (مبحث بومی سازی). با توجه توضیحات فوق مشکل اصلی، نبود زیر ساخت های فرهنگی است و اینکه آیا فرهنگ جامعه آمادگی پذیرش تغییرات بسیار گسترده ای که ایجاد خواهد شد را دارد یا خیر؟ همچنین می بایست به این موضوع نیز توجه نمود که در کنار عوامل فرهنگی، مهارتهای تخصصی نیروی انسانی نیز از اهمیت بسزایی برخوردار است که هم راستا با عوامل فرهنگی باید مورد مذاقه قرار گیرد. با عنایت به موارد مطروحه فوق می توان اذعان داشت، توجه به عوامل سازمانی (که خود نیز ریشه در عوامل فرهنگی دارد) به نوبه خود می تواند در جهت استقرار دولت الکترونیک مفید واقع شود.

منابع و مراجع

- [۱] اصلانی، حمیدرضا، حقوق فناوری اطلاعات، تهران، میزان، ۱۳۸۹.
- [۲] انصاری، باقر، حقوق حریم خصوصی، تهران: انتشارات سمت، ۱۳۸۶، ص ۲۳۲.
- [۳] الاهوانی، حسام‌الدین کامل، (۱۹۷۸) الحق فی احترام الحیاة الخاصة، قاهره، دار النهضة العربیة.
- [۴] باصری، حمید؛ نصری راد، محسن، تأثیرپذیری فرهنگی واجتماعی استقرار دولت الکترونیک و چالش‌های فرارو، نشریه علمی- تخصصی مهندسی فرهنگی، شماره ۶۳، ۱۳۹۱.
- [۵] ربیعی، حمیدرضا، دولت الکترونیکی تجربه دولت آلمان، با حمایت شورای عالی اطلاع رسانی مرکز مخابرات معاونت پشتیبانی وزارت کار و امور اجتماعی، دانشگاه صنعتی شریف، ۱۳۸۳.
- [۶] رضایی زاده، محمد جواد؛ زرشکیان، سهرورد، مدخلی بر خدمات عمومی الکترونیک در نظام حقوقی ایران، مجله حقوق خصوصی، پاییز و زمستان ۱۳۹۰، شماره ۱۹.
- [۷] صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، تهران: نشر میزان، ۱۳۸۸.
- [۸] صرافی زاده، اصغر، فناوری اطلاعات در سازمان، تهران: انتشارات میر، ۱۳۸۳.
- [۹] محسنی، فرید، حریم خصوصی اطلاعات، تهران: انتشارات دانشگاه امام صادق (ع)، ۱۳۸۹.
- [۱۰] مقیمی، سید محمد؛ اعلائی اردکانی، مصطفی، سنجش شاخص‌های حکمرانی خوب و نقش دولت الکترونیک در ارتقای آن، مجله مدیریت فناوری اطلاعات، دوره ۳، شماره ۸، پاییز ۱۳۹۰، صص ۱۷۱ تا ۱۸۸.
- [۱۱] نقدی فرد هاشمیان، محسن، مفاهیم دولت الکترونیکی، مجمع تکفا، ۷ و ۸، ۱۳۸۲.
- [۱۲] یعقوبی، نورمحمد، دولت الکترونیک الگوی انتقالی، فصلنامه مطالعات مدیریت، شماره ۵۰، ۱۳۸۸.
- [13] Brandeis, Louis D. and Samuel D. Warren, (1890) The Right To Privacy, Harvard Law Review, V. IV, No.5.
- [14] Betnon- Davies, P., Constructing electronic government: the case of the UK inland revenue. International Journal of Management ۲۵(۱) , ۲۰۰۵.
- [15] Heeks R, Bailur S. Analyzing E-Government Research: Perspectives, Philosophies, Theories, Methods and Practice. Government Information Quarterly ۲۰۰۷; ۲۴: ۲۴۳-۲۶۵.
- [16] Khalil, Omar E.M. (۲۰۱۱). E-Government readiness: Does national culture matter?, Government Information Quarterly, ۲۸, ۳۸۸-۳۹۹.
- [17] Smartt, Ursula, (2014) Media & Entertainment Law, London: Routledge. P35.
- [18] Tohidi, Hamid. (۲۰۱۱). E-government and its different dimensions: Iran, Procedia Computer Science, ۳, ۱۱۰۱-۱۱۰۵.
- [19] Weiming, Shen, "Applications of agent-based systems in intelligent manufacturing", Advanced Engineering Informatics, 20, 2006, 415-431.