

الگوی صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه

دکتر محمدتقی تقوی فرد*

دکتر محمدرضا تقوا**

دکتر مهدی فقیهی***

محمدجواد جمشیدی****

چکیده

مهمترین هدف این نوشتار ارائه‌ی الگوی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه است. این تحقیق توسعه‌دهنده‌ی مبانی نظری و مدل‌های دولت الکترونیک از بعد حقوقی-قانونی محسوب می‌شود. این پژوهش از نظر روش‌شناسی، کیفی بوده و در آن از روش‌های مطالعات اسنادی، تحلیل محتوا و مطالعه‌ی تطبیقی استفاده شده است. جامعه‌ی آماری تحقیق شامل تمامی کشورهای دارای قانون در حوزه‌ی حریم خصوصی اطلاعاتی، شامل ۵۸ کشور، است که با روش نمونه‌گیری قضاوتی، ۱۱ کشور انتخاب شده و مبنای مطالعه‌ی اسنادی قرار گرفته‌اند که عبارتند از: انگلستان، کانادا، فرانسه، آلمان، اسپانیا، ایتالیا، نروژ، سوئد، ایرلند، بلژیک، کره جنوبی. الگوی پیشنهادی این تحقیق دارای هفت بعد است: (۱) الزامات گردآوری داده‌های شخصی شهروندان؛ (۲) الزامات استفاده از داده‌های شخصی شهروندان؛ (۳) الزامات نگهداری داده‌های شخصی شهروندان؛ (۴) الزامات افشاء داده‌های شخصی شهروندان؛ (۵) حقوق شهروندان در زمینه‌ی حریم خصوصی اطلاعاتی؛ (۶) مسئولیت‌های کنترل‌گر داده‌های شخصی؛ و (۷) الزامات دسترسی شهروندان به داده‌های شخصی. از بین ۱۲۴ الزام شناسایی شده برای حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک به عنوان شاخص‌های این ابعاد، ۱۰۵ الزام دارای وزن بالای ۰/۵ بوده و می‌توانند به‌عنوان اصول استاندارد جهانی، الگویی برای کشورهای در حال توسعه جهت ضابطه‌مندساختن توسعه‌ی دولت الکترونیک در زمینه‌ی حفظ حریم خصوصی اطلاعاتی شهروندان محسوب شوند.

واژه‌های کلیدی: حریم خصوصی اطلاعاتی، دولت الکترونیک، پردازش داده‌های شخصی، حقوق شهروندی، کشورهای در حال توسعه

* نویسنده مسئول- دانشیار گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی،
taghavifard@atu.ac.ir

** دانشیار گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی.

*** استادیار و مدیر دفتر مطالعات فناوری‌های نوین مرکز پژوهش‌های مجلس شورای اسلامی.

**** دانشجوی دکترای مدیریت فناوری اطلاعات، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی (این مقاله مستخرج از رساله‌ی دکترای دانشجو می‌باشد).

مقدمه

در سالیان اخیر، پیشرفت های فناوری اطلاعات توانسته است قابلیت دولت ها را در گردآوری، نگهداری و انتقال اطلاعات شخصی شهروندان به طرز چشم‌گیری افزایش دهد (Anthony, Stablein & Carian, 2015). مسأله‌ی حفظ «حریم خصوصی اطلاعاتی شهروندان»^۱ در دولت الکترونیک دارای جنبه های ضد و نقیضی است. دولت‌ها از یک سو نیاز به جمع‌آوری حداکثری اطلاعات شهروندان دارند تا بتوانند بیشترین خدمات را به آنها ارائه دهند؛ و از سوی دیگر، این خیل عظیم اطلاعات جمع‌آوری‌شده، با یا بدون رضایت شهروندان، می‌تواند خود نقض کننده‌ی حقوق آنان باشد. مسائل حفظ حریم خصوصی اطلاعاتی شهروندان جزء مهمترین نگرانی‌هایی است که می‌تواند باعث محدودشدن رشد دولت الکترونیک گردد (Thibodeau, 2000).

هر چند آمار دقیقی از تعداد نقض اطلاعات حریم شخصی شهروندان در دنیا در دسترس نیست، اما تنها در آمریکا، سالانه حدوداً ۱۵ میلیون شهروند مورد سرقت اطلاعات شخصی قرار می‌گیرند که ضرر مالی ناشی از آن بیش از ۵۰ میلیارد دلار تخمین زده می‌شود (Douglas, 2016). علاوه بر این، نقض عامدانه‌ی حریم خصوصی آنها در دولت الکترونیک برخی کشورها منجمله آمریکا نگرانی‌های زیادی را بوجود آورده است. سازمان امنیت ملی آمریکا بطور منظم اقدام به گردآوری اطلاعات از شهروندان آمریکایی می‌کند (Landau, 2014).

در دولت الکترونیک، بنا به ماهیت آن، اطلاعات شهروندان و حتی نهادهای بخش خصوصی و مردم‌نهاد، در اختیار نهادهای دولتی قرار می‌گیرد. این موضوع باعث بوجود آمدن مسئولیت‌هایی برای بخش دولتی در حفاظت از اطلاعات افراد حقیقی و حقوقی می‌شود. نکته‌ی ظریفی که در اینجا وجود دارد، این است که هنگامی که مشتری با بخش‌های غیر دولتی ارتباط دارد، می‌تواند تصمیم بگیرد که به چه شرکتی، چه اطلاعاتی را بدهد. اما هنگام ارتباط دولت با شهروندان، دولت با قدرت قهریه می‌تواند شهروندان را مجبور به تسلیم هر نوع اطلاعاتی کرده و نیز بدون اطلاع شهروندان، اطلاعات آنها را در اختیار هر نهادی قرار دهد (BeVier, 1995: 457). همچنین، داده‌های بزرگ^۲ نیز مسأله‌ی حفظ حریم خصوصی شهروندان را پیچیده‌تر کرده است؛ داده‌های شخصی

1 -Citizens' Information Privacy

2 -Big Data

پراکنده‌ی شهروند که در اختیار نهادهای مختلف است، شاید به اندازه‌ی داده‌های بزرگ موجب نگرانی شهروندان نشود. مجموعه‌ی عظیم داده‌های شخصی شهروندان که بر روی رسانه‌های دیجیتالی قرار دارد، با تجمیع شدن در یک مکان (مثلاً یک پایگاه داده یا انبار داده)، نوعی داده بزرگ محسوب می‌شود که می‌تواند تصویر کاملی از یک شهروند را ارائه دهد (Stark, 2016).

ادراک شهروندان از این موضوع که دولت الکترونیک به نوعی نقض کننده‌ی حریم خصوصی آنان است، می‌تواند موجب عدم اعتماد آنها به دولت الکترونیک شود (Abu-Shanab, 2014). ایمنی و حفظ حریم خصوصی شهروندان از عوامل مهمی است که بر استقرار دولت الکترونیک اثرگذار است. سطح ایمنی و حفظ حریم خصوصی بر میزان اعتماد شهروندان به دولت الکترونیک اثر می‌گذارد و در صورتی که شهروندان به این نتیجه برسند که مبادلات الکترونیکی از ایمنی لازم برخوردار نیست یا اطلاعات خصوصی افراد توسط سایرین قابل دسترس است، اعتماد خود به دولت الکترونیک را از دست خواهند داد؛ از اینرو یکی از روش‌های تقویت اعتماد شهروندان، بالابردن سطح ایمنی و حفظ حریم خصوصی شهروندان است (یعقوبی، ۱۳۹۲: ۲۵۲). حریم خصوصی کاربر خدمات دولت الکترونیکی، نمایانگر شرایطی است که تحت آن، فرد مایل به سپهیم‌شدن اطلاعات فردی با دیگران است. حریم خصوصی زمانی نقض می‌شود که شرایط ضروری برای سپهیم‌شدن اطلاعات نقض شود (تقی پور، ۱۳۹۰: ۸۲).

طبق آمار موجود، از مجموع ۱۹۶ کشور جهان، ۱۳۸ کشور (شامل اغلب کشورهای آسیایی منجمله ایران، کشورهای آفریقایی و آمریکای لاتین) دارای وضعیت بسیارضعیفی از نظر حفاظت از حریم خصوصی اطلاعاتی هستند؛ و از ۵۸ کشور صنعتی باقیمانده (اغلب کشورهای اروپایی و آمریکای شمالی) نیز تنها ۱۱ کشور در وضعیت بسیار خوب از نظر حفاظت از حریم خصوصی اطلاعاتی شناخته شده‌اند (DLA, 2016). بنابراین هدف اصلی از انجام این تحقیق طراحی الگوی حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک برای کشورهای در حال توسعه، بر اساس قوانین کشورهای توسعه یافته است. بر این اساس، یکی از مهمترین ضرورت‌های انجام این تحقیق، وضعیت نابسامان اغلب کشورهای دنیا در حوزه‌ی صیانت از حریم خصوصی اطلاعاتی شهروندان است که علیرغم تأکید قوانین فراملی و کنوانسیون‌های بین‌المللی، اقدامی جدی توسط آنها در این زمینه به انجام نرسیده است. ضرورت دیگر انجام این تحقیق، ضعف در مبانی نظری دولت الکترونیک

و نبود چارچوبی جهانی برای صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک است. در بسیاری از مدل‌های دولت الکترونیک به اهمیت مسائل حقوقی-قانونی اشاره شده است، اما در هیچ‌یک، چارچوب حقوقی-قانونی جامعی برای حفاظت از حریم خصوصی اطلاعاتی شهروندان توسعه داده نشده است. بدین ترتیب، مهم‌ترین سؤال که در این تحقیق به دنبال پاسخ به آن هستیم، این است که الگوی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک چگونه است؟

مروری بر پیشینه‌ی تحقیق

پیشینه‌ی نظری

«حریم خصوصی اطلاعاتی عبارت است از مطالبه‌ای که افراد، گروه‌ها، یا نهادها در زمینه‌ی تعیین چگونگی و حد انتقال اطلاعات درمورد آنها به‌سایرین دارند» (Westin, 1967: 7). بنابراین، حریم خصوصی اطلاعاتی یک حق است؛ حقی که افراد برای کنترل داده‌های خود در برابر جستجوهای نابجا، استراق سمع، تجسس، تصاحب و سوءاستفاده‌هایی که ممکن است از داده‌های شخصی‌شان شود، دارند (Stanford Encyclopedia of Philosophy, 2016). سه نظریه را می‌توان به عنوان مبانی نظری حفاظت از حریم خصوصی اطلاعاتی شهروندان معرفی کرد: نظریه‌ی حقوق فطری، نظریه‌ی قرارداد اجتماعی و نظریه‌ی اخلاقی.

نظریه حقوق فطری

طبق نظریه‌ی حقوق فطری، تمامی انسان‌ها دارای حقوق بنیادی هستند که برتر از خواست و اراده‌ی دولت‌ها است (کاتوزیان، ۱۳۶۶: ۲۶). این حقوق از این جهت فطری نامیده شده‌اند که با تولد انسان‌ها، آنها را همراهی می‌کنند. حق حیات، حق آزادی بیان، حق دادخواهی و حق بهره‌مندی از زندگی خصوصی جزء حقوق فطری انسان‌ها هستند. حق بهره‌مندی از زندگی خصوصی که گاهی از آن به عنوان حق تنها ماندن نیز یاد می‌شود طبق نظریه‌ی حقوق فطری، شهروندان را مستحق این می‌داند که اولاً بتوانند از وقوف و آگاهی سایرین بر جوانب مختلف زندگی خصوصی خود جلوگیری نموده و به دیگران اجازه‌ی آگاهی و تفتیش در حوزه‌ی زندگی خصوصی خود را ندهد و ثانیاً در صورت تمایل بتوانند از مداخله‌ی سایرین در زندگی شخصی‌شان جلوگیری به عمل آورند (اصلانی، ۱۳۸۹: ۳۳). بر این اساس، هر گونه دخل و تصرف در شئون مختلف زندگی خصوصی شهروندان، منجمله

اطلاعات شخصی آنها بدون آگاهی یا رضایتشان به معنای نقض حقوق فطری آنها محسوب می‌شود.

نظریه قرارداد اجتماعی

بر اساس نظریه‌ی قرارداد اجتماعی-که قوانین اساسی را می‌توان مظهر و تجلی آن دانست- زندگی اجتماعی و مدنی انسان‌ها بر زندگی خصوصی آنها مرزهایی را می‌گستراند؛ میل به آزادی بی نهایت بشر و میل به زندگی جمعی با هم در تضادند؛ آنچه بین این دو آشتی برقرار می‌کند مجموعه قراردادهایی است که قدرتی فرافردی در اجتماع (مجموعه‌ی شهروندان) بوجود می‌آورد. این قرارداد، قرارداد اجتماعی نامیده می‌شود (روسو، ۱۳۶۶: ۱۸). طبق نظریه‌ی قرارداد اجتماعی، چنین می‌توان استدلال کرد که دخالت دولت‌ها در زندگی خصوصی افراد و اطلاع آنها از ابعاد پنهان زندگی شهروندان ممنوع است، مگر با استناد به قانون (عالم، ۱۳۸۰: ۱۸۰). بر این اساس، در نظریه‌ی قرارداد اجتماعی هم مثل نظریه‌ی حقوق فطری، بر حق صیانت از حریم خصوصی شهروندان صحه نهاده شده است. با این تفاوت که حد و مرز آن را قانون حاکم بر زندگی مدنی شهروندان مشخص می‌کند. به عبارت دیگر، دولت تنها هنگامی می‌تواند در حریم خصوصی اطلاعاتی شهروندان وارد شود که قانون اجازه‌ی این کار را به او داده باشد و در سایر موارد ورود بدون رضایت شهروندان ممنوع است.

نظریه اخلاقی

اخلاق مجموعه‌ای از قواعد رفتاری است که رعایت آن برای نیکوکاری و نیل به کمال ضروری بوده و مطبوع طبع نوع بشر می‌باشد (کاتوزیان، ۱۳۶۶: ۴۵۱). حقوق، مجموعه قواعدی است که بشر برای برقراری نظم و عدالت در اجتماع وضع نموده است و موضوع آن «رفتار انسان» است. حقوق، اخلاق را غایت و راهنمای خود در قاعده‌گذاری می‌داند؛ قاعده‌ی حقوقی که واجد صفت اخلاقی باشد، به دلیل اقناع درونی شهروندان با سهولت بیشتری مورد پذیرش قرار می‌گیرد. حمایت و صیانت از حریم خصوصی اطلاعاتی شهروندان مورد تأیید و تأکید اخلاق بوده و قانونگذار باید با وضع قواعد رفتاری منقح و روشن و همچنین ضمانت‌های اجرایی مادی (اعم از کیفری و غیرکیفری) بدان بپردازد (اصلانی، ۱۳۸۹: ۴۱). براین اساس، طبق نظریه‌ی اخلاقی نیز لزوم تدوین چارچوب‌های قانونی

مبتنی بر اخلاق برای صیانت از حریم خصوصی اطلاعاتی شهروندان و حفظ کرامت آنان امری مهم تلقی شده است که دولت‌ها را محدود به رعایت اصول اخلاقی در ورود به حریم خصوصی شهروندان می‌نماید.

بطور خلاصه چنین می‌توان استدلال کرد که سه نظریه‌ی حقوق فطری، قرارداد اجتماعی و اخلاقی همگی بر حق حفظ حریم خصوصی اطلاعاتی شهروندان تأکید کرده‌اند؛ هر چند تفاوت‌هایی در مبانی سه نظریه‌ی فوق وجود دارد، اما آنها مانعاًالجمع نبوده و می‌توان ترکیبی از این سه نظریه را به عنوان مبنای نظری برای حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک در نظر گرفت.

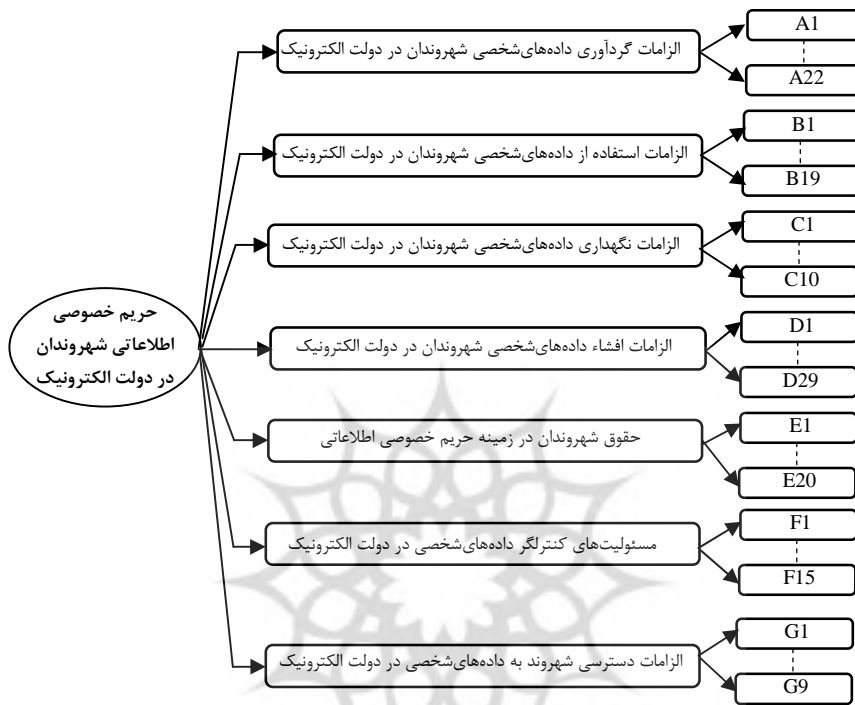
پیشینه‌ی تجربی

تا کنون تحقیقات اندکی در زمینه‌ی حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک انجام شده است. در پژوهشی، ارتباط میان وجود قوانین مربوط به حفظ حریم خصوصی اطلاعاتی افراد و میزان صیانت از حقوق شهروندان و مشتریان توسط دولت‌ها و کسب و کارها مورد بررسی قرار گرفته است (Gayton, 2006). طبق نتایج آن پژوهش، تمایل زیادی میان دولت‌ها وجود دارد تا با افزایش حوزه و میزان خدمات ارائه شده به شهروندان، داده‌های شخصی بیشتری را از آنان در مقادیر وسیع جمع‌آوری کنند. همچنین، دولت‌ها و کسب و کارها در مورد اطلاعاتی که از افراد جمع‌آوری می‌کنند، زیاد حساس نبوده و در مورد حفاظت از محرمانگی آنها اغلب غفلت می‌کنند. طبق نتیجه‌گیری محقق در تحقیق فوق، تنها در صورت وجود قوانین حفظ حریم خصوصی اطلاعاتی جامع است که می‌توان امید داشت تا داده‌های شخصی شهروندان مورد حفاظت قرارگیرد. در پژوهشی دیگر، معضلات پیرامون حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک در نیوزیلند و ژاپن مورد بررسی قرار گرفته است (Cullen, 2008). بر اساس آن تحقیق، ظهور دولت الکترونیک باعث شده است تا شهروندان به حفظ محرمانگی و امنیت اطلاعات خود چه بصورت آنلاین و چه بصورت آفلاین تردید داشته باشند. نتایج آن تحقیق حاکی از آن است که نگرانی شهروندان پیرامون محرمانگی اطلاعاتشان، تا حد زیادی وابسته به فرهنگ فردگرا یا جمع‌گراست. همچنین اقلیت‌ها و افرادی که از نظر مالی در سطوح پائین‌تری هستند، نسبت به محرمانگی اطلاعات خود حساسیت بیشتری نشان می‌دهند. با این وجود، تمامی گروه‌های مورد بررسی در هر دو کشور نسبت به حفظ

حریم خصوصی اطلاعاتی خود حساسیت نشان داده‌اند. همچنین اعتماد شهروندان نیوزیلندی بیشتر از اعتماد ژاپنی‌ها به دولت الکترونیک شناخته شده است. در پژوهشی دیگر، رابطه‌ی میان اعتماد شهروندان به دولت الکترونیک و حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک در نیوزیلند بررسی شده است؛ نتایج تحقیق حاکی از آن است که میان فرهنگ‌های مختلف، در میزان اعتماد به دولت الکترونیک، بر مبنای ادراک آنها از میزان حفظ حریم خصوصی اطلاعاتی شهروندان، تفاوت وجود دارد. به طوری که نیوزیلندی‌های با فرهنگ‌های مختلف دارای سطوح اعتماد متفاوتی به دولت الکترونیک شناخته شده‌اند (Cullen and Reilly, 2007).

چارچوب نظری تحقیق

به اعتقاد برخی محققان، میان حفاظت از حریم خصوصی اطلاعاتی شهروندان و پیاده‌سازی دولت الکترونیک رابطه وجود دارد (Belanger & Hiller, 2006). آنها حفظ حریم خصوصی اطلاعاتی شهروندان را به عنوان الزاماتی جهت کنترل پیاده‌سازی دولت الکترونیک معرفی می‌کنند. «الزامات سیاستگذاری و مقرراتی» به عنوان ابعاد نرم و «الزامات فنی و کاربری» به عنوان ابعاد سخت مدنظر قرار می‌گیرند. ابعاد نرم در سطحی بالاتر از ابعاد سخت قرار می‌گیرند و ناظر به شرایط حفظ حریم خصوصی اطلاعاتی شهروندان هستند که دولت‌ها را در نحوه‌ی استفاده از داده‌های شخصی شهروندان محدود ساخته و استفاده از اطلاعات به منظور خدمات رسانی را ضابطه‌مند می‌کند. الزامات فنی به معنای پروتکل‌های سخت افزاری و نرم افزاری جهت استفاده از داده‌ها و اطلاعات بوده و الزامات کاربری اشاره به میزان تمایل شهروندان در استفاده از خدمات دولت الکترونیک دارد. مبنای نظری این تحقیق بعد نرم مدل فوق به عنوان الزامات سطح بالای سیاستگذاری و مقرراتی است که نحوه‌ی استفاده از داده‌های شخصی شهروندان را ضابطه‌مند می‌کند. مدل مفهومی تحقیق در نمودار ۱ ترسیم شده است.



نمودار ۱: مدل مفهومی تحقیق

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

تعریف واژگان

در جدول شماره ۱ واژگان تحقیق تعریف شده‌اند.

جدول ۱. تعاریف واژگان تحقیق

واژه	تعریف
حریم خصوصی اطلاعاتی	مطالبه‌ای که افراد، گروهها، یا نهادها در زمینه‌ی تعیین چگونگی و حد انتقال اطلاعات در مورد آنها به سایرین دارند (Westin, 1967: 7).
سوژه	هر شهروند حقیقی که داده‌های شخصی به وی ارتباط پیدا می‌کند (Italian Personal Data Protection Code, 2003).
داده‌های شخصی	هر نوع اطلاعاتی که بصورت مستقیم یا غیر مستقیم به یک شهروند قابل شناسایی ارتباط داشته باشد (Italian Personal Data Protection Code, 2003).
داده‌های شخصی حساس	بخشی از داده‌های شخصی که شامل اطلاعات مربوط به قومیت و نژاد، نگرش‌های سیاسی، اعتقادات مذهبی، عضویت در اتحادیه‌ها، وضعیت سلامت جسمانی یا روانی یا زندگی جنسی و سوابق کیفری شهروند است (England Data Protection Act, 1998).
کنترل‌گردداده‌های شخصی	نهاد دولتی (یا سامانه دولت الکترونیکی) که داده‌های شخصی را (بصورت مستقیم یا غیر مستقیم) برای مقاصد دولتی مورد پردازش قرار می‌دهد. پردازش شامل موارد زیر می‌شود: <ul style="list-style-type: none"> گردآوری داده‌های شخصی (اخذ داده از سوژه یا نهاد ثالث)؛ استفاده از داده‌های شخصی (به کارگیری داده‌های شخصی در فرایندهای سازمانی)؛ نگهداری داده‌های شخصی (هر نوع ذخیره سازی داده در پایگاه‌های داده)؛ افشاء داده‌های شخصی (انتقال داده‌ها به فرد یا نهاد ثالث) (Korean Personal Information Protection Act, 2011).
پردازشگر	هر فرد یا نهادی که به جای کنترل‌گر (متولی) اقدام به پردازش داده‌های شخصی می‌کند (Korean Personal Information Protection Act, 2011).

سؤالات پژوهش

با توجه به مدل مفهومی تحقیق (نمودار ۱) سؤالات تحقیق عبارتند از:

سؤال اصلی. الگوی صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک چگونه است؟

سؤال فرعی ۱. الزامات گردآوری داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟

سؤال فرعی ۲. الزامات استفاده از داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟

سؤال فرعی ۳. الزامات نگهداری داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟

سؤال فرعی ۴. الزامات افشاء داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟

سؤال فرعی ۵. حقوق شهروندان در زمینه حریم خصوصی اطلاعاتی در دولت الکترونیک کدامند؟

سؤال فرعی ۶. مسئولیت‌های کنترل‌گر داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟

سؤال فرعی ۷. اصول دسترسی شهروند به داده‌های شخصی در دولت الکترونیک کدامند؟

روش پژوهش

این تحقیق از نظر روش‌شناسی جزء تحقیقات کیفی دسته بندی می‌شود و شامل روش‌های تحلیل محتوا، مطالعات اسنادی و تطبیقی می‌شود. همچنین نظر به اینکه نتایج این تحقیق قابلیت کاربرد در دولت الکترونیک در کشورهای در حال توسعه را داراست، می‌توان گفت که این پژوهش از نظر هدف در حیطه پژوهش‌های کاربردی است. علاوه بر این، تحقیق حاضر از نظر ماهیت یک تحقیق اکتشافی است که به توسعه مبانی نظری حریم خصوصی اطلاعاتی در دولت الکترونیک کمک می‌کند و بر اساس روش گردآوری داده‌ها، یک پژوهش توصیفی محسوب می‌شود.

ابزار گردآوری داده‌ها

در این پژوهش از روش‌های مطالعه کتابخانه ای و اسنادی برای گردآوری داده‌ها استفاده شده است.

فنون تجزیه و تحلیل اطلاعات

تحلیل داده‌ها با روش‌های عینی (کدگذاری) و آماری (شمارش فراوانی و میانگین وزنی تکرار شاخص‌ها) با نرم افزار Excel 2013 انجام شده است. بدین منظور، با کدگذاری باز، تمامی قوانین حفاظت از حریم خصوصی اطلاعاتی در کشورهای منتخب که به سازمان های دولتی اختصاص داشتند، کدگذاری شدند؛ سپس با کدگذاری محوری، شاخص‌های استخراج شده از مرحله اول، در سطحی بالاتر، ابعاد حفاظت از حریم خصوصی اطلاعاتی در دولت الکترونیک را شکل دادند. در گام بعد، میزان تکرار هر یک از شاخص ها در تمامی کشورهای منتخب بدست آمده و وزن‌دهی به شاخص ها بر اساس میانگین تکرار آنها در ۱۱ کشور منتخب محاسبه شده است.

جامعه‌ی آماری، حجم نمونه و روش نمونه‌گیری

جامعه‌ی آماری این تحقیق، شامل تمامی کشورهای دارای قانون حمایت از حریم خصوصی اطلاعاتی است که طبق آمار مؤسسه DLA از ۱۹۶ کشور، ۵۸ کشور دارای قوانین مرتبطی در این زمینه هستند. حجم نمونه برابر ۱۱ کشور (انگلستان، کانادا، فرانسه، آلمان، اسپانیا، ایتالیا، نروژ، سوئد، ایرلند، بلژیک، کره جنوبی) است که با استفاده از روش نمونه‌گیری معیار به‌عنوان کشورهای منتخب مورد مطالعه قرار گرفته‌اند. معیار انتخاب این کشورها داشتن وضعیت خیلی خوب از نظر حفظ حریم خصوصی اطلاعاتی شهروندان طبق آمار مؤسسه DLA بوده است.

یافته‌های پژوهش

سؤال اصلی تحقیق عبارت است از: الگوی صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک به چه شکل است؟ بر اساس این تحقیق، الگوی حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک دارای ۷ بعد است که مجموعاً شامل ۱۰۵ شاخص (الزام) می‌شود (جدول‌های ۲ تا ۷). بر این اساس، الزاماتی که در بیش از نصف کشورهای منتخب آمده باشند (دارای وزن بالای ۰/۵ باشند) به عنوان الزامات پیشنهادی برای حفظ حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک معرفی شده‌اند. وزن هر یک از شاخص‌ها بر اساس فرمول شماره ۱ محاسبه شده است:

$$W = \frac{\sum_{i=1}^{11} X_i}{11} \quad (\text{فرمول ۱})$$

{W: وزن هر شاخص | Xi: وجود یا عدم وجود الزام در یک کشور (وجود=۱ و عدم وجود=۰)}

الف- الزامات گردآوری داده‌های شخصی شهروندان در دولت الکترونیک در جدول شماره ۲ الزامات گردآوری داده‌های شخصی شهروندان در دولت الکترونیک به همراه وزن هر یک از الزامات آمده است.

جدول ۲: الزامات مربوط به گردآوری داده‌های شخصی شهروندان در دولت الکترونیک

وزن (W)	الزامات مربوط به گردآوری داده‌های شخصی شهروندان در دولت الکترونیک (کد A)
۱	A1. لزوم گردآوری داده‌های شخصی برای اهداف مشخص و قانونی
۱	A2. لزوم ارائه اطلاعات کافی به سوژه در زمان گردآوری داده‌های شخصی در صورت عدم وجود منع قانونی
۱	A3. لزوم ارائه اطلاعات کافی به سازمان افشاء‌کننده در زمان گردآوری داده‌های شخصی از منبعی غیر از سوژه در صورت عدم وجود منع قانونی
۱	A4. مجازبودن گردآوری داده‌های شخصی از سوژه پس از جلب رضایت سوژه
۰/۹	A5. لزوم گردآوری داده‌های شخصی تا حد کفایت برای اهداف اعلام شده
۰/۹	A6. مجازبودن گردآوری بدون جلب رضایت سوژه در صورت وجود الزام قانونی
۰/۹	A7. مجازبودن گردآوری بدون جلب رضایت سوژه در صورت ضروری بودن برای حفاظت از جان سوژه
۰/۹	A8. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن برای مقاصد تحقیقاتی با شرط بیشتر بودن منافع عمومی از منافع خصوصی و ناشناخته ماندن هویت سوژه
۰/۸۱	A9. غیرمجازبودن گردآوری داده‌های حساس شخصی بدون جلب رضایت سوژه
۰/۸۱	A10. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن گردآوری برای انجام وظایف قانونی متولی داده‌های شخصی
۰/۸۱	A11. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت اجتناب ناپذیر بودن گردآوری بنا به قرارداد منعقد شده میان متولی و سوژه
۰/۸۱	A12. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن گردآوری برای حفاظت از اموال و دارائی‌های سوژه
۰/۸۱	A13. مجازبودن گردآوری داده‌های شخصی سوژه که به حالت عمومی درآمده اند بدون جلب رضایت سوژه
۰/۷۲	A14. لزوم ارائه اطلاعات کافی به سوژه‌ها بلافاصله پس از گردآوری داده‌های شخصی از منبعی غیر از سوژه در صورت عدم وجود منع قانونی
۰/۶۳	A15. مجازبودن گردآوری داده‌های حساس شخصی بدون جلب رضایت سوژه در صورت وجود الزام قانونی
۰/۵۴	A16. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف اجرای احکام قضائی
۰/۵۴	A17. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف انجام وظیفه در جهت منافع عمومی
۰/۵۴	A18. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای حفاظت از منافع مشروع متولی با شرط پایمال نشدن منافع سوژه
۰/۴۵	A19. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف حفاظت از امنیت ملی
۰/۳۶	A20. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای پیگرد قضائی مجرمان
۰/۲۷	A21. ممنوع بودن گمراه کردن سوژه‌ها در هنگام گردآوری داده‌های شخصی با روش‌های فریبنده
۰/۲۷	A22. مجازبودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای تحقیق پیرامون نقض قانون

سؤال فرعی اول تحقیق عبارت است از: الزامات گردآوری داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟ طبق جدول ۲، از بین ۲۲ الزام شناسایی شده برای گردآوری داده‌های شخصی شهروندان در دولت الکترونیک ۱۸ مورد دارای وزن بالای ۰/۵ بوده و در

الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۱ عبارت است از کدهای A1 تا A18.

ب- الزامات استفاده از داده‌های شخصی شهروندان در دولت الکترونیک

در جدول شماره ۳ الزامات استفاده از داده‌های شخصی شهروندان در دولت الکترونیک به همراه وزن هر کدام از آنها لیست شده است.

جدول ۳: الزامات مربوط به استفاده از داده‌های شخصی شهروندان در دولت الکترونیک

وزن (W)	الزامات مربوط به استفاده از داده‌های شخصی شهروندان در دولت الکترونیک (کد B)
۱	B1. غیرمجاز بودن استفاده از داده‌های شخصی در صورت غیرمجاز شمرده شدن گردآوری آنها
۰/۹	B2. مجاز بودن استفاده از داده‌های شخصی پس از جلب رضایت سوژه در صورت گردآوری از سازمان ثالث
۰/۹	B3. لزوم سازگار بودن استفاده از داده‌های شخصی با اهداف اعلام شده در هنگام گردآوری
۰/۹	B4. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از جان سوژه
۰/۹	B5. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از اموال سوژه
۰/۸۱	B6. غیرمجاز بودن استفاده از داده‌های حساس شخصی بدون جلب رضایت سوژه
۰/۸۱	B7. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت وجود الزام قانونی برای استفاده
۰/۸۱	B8. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در زمان گردآوری در صورت ضروری بودن استفاده از آنها بنا به قرارداد منعقد شده با سوژه
۰/۸۱	B9. لزوم تعلیق استفاده از داده‌های شخصی سوژه در صورت موجه بودن درخواست سوژه مبنی بر تعلیق استفاده و ممکن بودن انجام وظایف متولی پس از تعلیق
۰/۸۱	B10. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن برای انجام تحقیقات با شرط بیشتر بودن منافع عمومی از منافع خصوصی سوژه و ناشناخته ماندن هویت سوژه
۰/۶۳	B11. لزوم استفاده از داده‌های شخصی بصورت منصفانه (در صورتی که قبلاً اهداف استفاده اعلام شده باشد)
۰/۶۳	B12. لزوم استفاده از داده‌های شخصی بصورت قانونی (متناسب بودن استفاده با وظایف قانونی متولی)
۰/۵۴	B13. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای انجام وظایف قانونی متولی
۰/۵۴	B14. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای دعوی حقوقی
۰/۵۴	B15. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از منافع مشروع متولی با شرط پایمال نشدن منافع سوژه
۰/۵۴	B16. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده با هدف انجام وظیفه در جهت منافع عمومی
۰/۴۵	B17. مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از امنیت ملی
۰/۳۶	B18. مجاز بودن استفاده از داده‌ها فراتر از اهداف اعلام شده برای پیگرد قانونی مجرمان
۰/۲۷	B19. مجاز بودن استفاده از داده‌ها فراتر از اهداف اعلام شده برای انجام تحقیقات جنائی

سؤال فرعی دوم تحقیق عبارت است از: الزامات استفاده از داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟ طبق جدول ۳، از بین ۱۹ الزام شناسایی شده برای استفاده از داده‌های شخصی شهروندان در دولت الکترونیک، ۱۶ الزام در حداقل نیمی از کشورها تکرار شده‌اند (دارای وزن بالای ۰/۵ هستند) و در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۲ عبارت است از کدهای B1 تا B16.

ج- الزامات نگهداری داده‌های شخصی شهروندان در دولت الکترونیک

در جدول شماره ۴ الزامات نگهداری داده‌های شخصی شهروندان در دولت الکترونیک به همراه وزن هر یک آمده است.

جدول ۴: الزامات مربوط به نگهداری داده‌های شخصی شهروندان در دولت الکترونیک

وزن (W)	الزامات مربوط به نگهداری داده‌های شخصی شهروندان در دولت الکترونیک (کد C)
۱	C1. غیرمجاز بودن نگهداری داده‌های شخصی در صورت غیرمجاز شمرده شدن گردآوری آنها
۱	C2. لزوم اطمینان از صحت داده‌ها پیش از اقدام به نگهداری آنها (نگهداری داده‌های صحیح)
۰/۹	C3. لزوم نابودسازی داده‌های شخصی در صورت منقضی شدن زمان نگهداری آنها
۰/۹	C4. لزوم نابودسازی داده‌های شخصی در صورت تقاضای سوژه و ناتوانی متولی در اثبات مشروعیت نگهداری آنها
۰/۸۱	C5. لزوم به روز رسانی داده‌های شخصی در هنگام ضرورت
۰/۸۱	C6. مجاز بودن نگهداری داده‌های شخصی بیش از زمان مورد نیاز جهت رسیدن به اهداف اولیه گردآوری برای مقاصد تحقیقاتی با شرط بیشتر بودن منافع عمومی از منافع خصوصی سوژه و ناشناخته ماندن هویت سوژه
۰/۸۱	C7. مجاز بودن نگهداری داده‌های شخصی بیش از زمان مورد نیاز جهت رسیدن به اهداف اولیه گردآوری در صورت وجود الزام قانونی برای نگهداری آنها
۰/۷۲	C8. مجاز بودن نگهداری داده‌های شخصی تا زمان مورد نیاز جهت رسیدن به اهداف اولیه گردآوری
۰/۷۲	C9. لزوم اطمینان از کامل بودن داده‌های شخصی در جهت اهداف اولیه گردآوری پیش از اقدام به نگهداری آنها
۰/۳۶	C10. لزوم حذف داده‌های شخصی غیر دقیق (ناقص یا غیر صحیح) در صورت عدم امکان اصلاح

سؤال فرعی سوم تحقیق عبارت است از: الزامات نگهداری داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟ بر اساس جدول ۴، از بین ۱۰ الزامی که برای نگهداری داده‌های شخصی شهروندان در دولت الکترونیک در کشورهای منتخب آمده است، ۹ مورد دارای وزن بالاتر از ۰/۵ بوده و در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۳ عبارت است از کدهای C1 تا C9.

د- الزامات افشاء داده‌های شخصی شهروندان در دولت الکترونیک

در جدول شماره ۵ الزامات افشاء داده‌های شخصی شهروندان در دولت الکترونیک به همراه وزن مربوط به هر یک، لیست شده است.

جدول ۵: الزامات مربوط به افشاء داده‌های شخصی شهروندان در دولت الکترونیک

وزن (W)	الزامات مربوط به افشاء داده‌های شخصی شهروندان در دولت الکترونیک (کد D)
۱	D1. غیرمجاز بودن افشاء داده‌های شخصی در صورت قرارنگرفتن افشاء جزء اهداف اعلام شده
۱	D2. غیرمجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده بدون جلب رضایت سوژه
۰/۹	D3. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده به سوژه در زمان گردآوری در صورت ضروری بودن افشاء برای انجام وظایف قانونی متولی (یا سازمان دریافت کننده)
۰/۸۱	D4. لزوم ارائه اطلاعات کافی به سوژه‌ها پیش از افشاء داده‌های شخصی در صورت عدم وجود منع قانونی
۰/۸۱	D5. غیرمجاز بودن افشاء داده‌های حساس شخصی بدون جلب رضایت سوژه
۰/۸۱	D6. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده در صورت وجود الزام قانونی
۰/۸۱	D7. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن برای حفاظت از جان سوژه
۰/۸۱	D8. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن افشاء برای مقاصد تحقیقاتی با شرط بیشتر بودن منافع عمومی از منافع خصوصی و ناشناخته ماندن هویت سوژه
۰/۸۱	D9. مجاز بودن افشاء داده‌های شخصی بدون جلب رضایت سوژه در صورت اجتناب ناپذیر بودن افشاء بنا به قرارداد منعقد شده میان متولی و سوژه
۰/۸۱	D10. لزوم درخواست از دریافت کنندگان داده‌های شخصی برای تعلیق استفاده از داده‌های شخصی و لزوم تعلیق استفاده از آنها توسط دریافت کنندگان طبق درخواست متولی در صورت موجه بودن درخواست سوژه
۰/۷۲	D11. غیرمجاز بودن افشاء داده‌های شخصی در صورت منقضی شدن زمان نگهداری آنها
۰/۷۲	D12. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از اموال سوژه
۰/۷۲	D13. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده در زمان گردآوری در صورت ضروری بودن افشاء برای پیشبرد پرونده‌های قضائی توسط سازمان‌های ذی صلاح
۰/۷۲	D14. لزوم درخواست از دریافت کنندگان داده‌های شخصی برای اصلاح داده‌های شخصی و لزوم اصلاح آنها توسط دریافت کنندگان طبق درخواست متولی (در صورت افشاء قبلی و آگاهی متولی از غیردقیق بودن-عدم صحت، ناقص بودن یا به روز نبودن- داده‌ها)
۰/۷۲	D15. لزوم درخواست از دریافت کنندگان داده‌های شخصی برای حذف داده‌های شخصی و لزوم حذف آنها توسط دریافت کنندگان طبق درخواست متولی (در صورت افشاء قبلی و درخواست سوژه برای حذف داده‌ها)
۰/۶۳	D16. مجاز بودن افشاء داده‌های حساس شخصی در صورت وجود الزام قانونی برای افشاء آنها
۰/۶۳	D17. مجاز بودن افشاء داده‌های حساس شخصی به نهادهای پزشکی حرفه‌ای برای مقاصد درمانی
۰/۶۳	D18. غیرمجاز بودن انتقال داده‌های شخصی به کشورهای خارجی در صورت عدم وجود سطوح کافی امنیت در آنها
۰/۵۴	D19. مجاز بودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده با هدف انجام وظیفه در جهت منافع عمومی
۰/۵۴	D20. مجاز بودن افشاء داده‌های شخصی بدون جلب رضایت سوژه با هدف قادر ساختن سازمان دریافت کننده به حفاظت از منافع مشروع متولی با شرط پامال نشدن منافع سوژه

۰/۵۴	D21. مجازبودن انتقال داده‌های شخصی به کشورهای دارای سطح پایین امنیت در صورت اعلام رضایت سوژه
۰/۵۴	D22. مجازبودن انتقال داده‌های شخصی به کشورهای دارای سطح پایین امنیت برای حفاظت از جان سوژه
۰/۵۴	D23. مجازبودن انتقال داده‌های شخصی به کشورهای دارای سطح پایین امنیت برای حفاظت از اموال سوژه
۰/۵۴	D24. مجازبودن انتقال داده‌های شخصی به کشورهای دارای سطح پایین امنیت برای پیشبرد پرونده‌های قضائی
۰/۴۵	D25. مجازبودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از امنیت ملی
۰/۴۵	D26. مجازبودن انتقال داده‌های شخصی به کشورهای خارجی دارای سطح پایین امنیت برای انجام قرارداد با سوژه
۰/۳۶	D27. مجازبودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده به متولی در زمان گردآوری در صورت ضروری بودن افشاء برای وظایف قانونی سازمان دریافت کننده
۰/۳۶	D28. مجازبودن افشاء داده‌های شخصی فراتر از اهداف اعلام شده در زمان گردآوری در صورت ضروری بودن افشاء برای تحقیقات مربوط به ارتکاب جرایم توسط سازمان‌های ذی صلاح
۰/۳۶	D29. لزوم رمزگذاری داده‌های شخصی با جدیدترین روش‌های رمزنگاری هنگام انتقال آنها

سؤال فرعی چهارم تحقیق عبارت است از: الزامات افشاء داده های شخصی شهروندان در دولت الکترونیک کدامند؟ بر اساس جدول ۵، از بین ۲۹ الزامی که برای افشاء داده‌های شخصی شهروندان در دولت در کشورهای منتخب آمده است، ۲۴ مورد دارای وزن بیشتر از ۰/۵ بوده و در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۴ عبارت است از کدهای D1 تا D24.

ه- حقوق شهروندان در زمینه‌ی حریم خصوصی اطلاعاتی

در جدول شماره ۶ الزامات حقوق شهروندان (سوژه‌ها) در زمینه‌ی حریم خصوصی اطلاعاتی در دولت الکترونیک به همراه وزن هر یک، آمده است.

جدول ۶: حقوق شهروند در زمینه‌ی حریم خصوصی اطلاعاتی در دولت الکترونیک

وزن (W)	حقوق شهروند در خصوص حریم خصوصی اطلاعاتی در دولت الکترونیک (کد E)
۱	E1. حق آگاهی از اهداف گردآوری داده‌های شخصی توسط یک سازمان
۱	E2. حق آگاهی از وجود(یا عدم وجود) داده‌های شخصی نزد یک سازمان
۱	E3. حق آگاهی از افشاء داده‌های شخصی به نهاد ثالث در گذشته یا احتمال افشاء در آینده
۱	E4. حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های شخصی
۱	E5. حق آگاهی از هویت متولی داده‌های شخصی (کنترلگر) و راههای تماس با وی
۱	E6. حق دسترسی به داده‌های شخصی
۱	E7. حق اصلاح داده‌های شخصی غیر دقیق (غیر صحیح یا ناقص)
۰/۹	E8. حق حذف داده‌های شخصی در صورت داشتن توجیه‌مشروع مبنی بر غیرمجازبودن گردآوری آنها توسط کنترلگر
۰/۸۱	E9. حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های حساس شخصی

۰/۸۱	E10. حق درخواست تعلیق استفاده داده‌های شخصی در صورت داشتن توجیه قانونی مبنی بر اینکه استفاده داده‌های شخصی موجب ضرر برای سوژه یا ناراحتی برای سایرین می‌شود
۰/۷۲	E11. حق آگاهی از منطق تصمیم‌گیری مبتنی بر پردازش تمام خودکار داده‌ها
۰/۷۲	E12. حق آگاهی از منبع گردآوری داده‌ها
۰/۶۳	E13. حق آگاهی از پیامدهای اعلام عدم رضایت نسبت به پردازش داده‌های شخصی
۰/۶۳	E14. حق پیگرد قانونی خسارت ناشی از پردازش داده‌های شخصی در فرآیندی منصفانه
۰/۶۳	E15. حق منع استفاده از داده‌های شخصی برای فعالیت‌های بازاریابی مستقیم
۰/۶۳	E16. حق آگاهی از حقوقی که سوژه در خصوص حریم خصوصی اطلاعاتی از آنها برخوردار است
۰/۶۳	E17. حق آگاهی از هویت متولی داده‌های شخصی و راههای تماس با وی
۰/۵۴	E18. حق پیگرد قانونی عدم پاسخگویی متولی به درخواست سوژه در برخورداری از حقوق خود
۰/۵۴	E19. حق تقاضای پردازش غیرخودکار (توسط انسان) داده‌های شخصی در صورت قرارگیری در معرض تصمیم‌گیری مبتنی بر پردازش تمام خودکار داده‌های شخصی
۰/۳۶	E20. حق آگاهی از مدت زمان نگهداری داده‌های شخصی توسط متولی

سؤال فرعی پنجم تحقیق عبارت است از: حقوق شهروندان در زمینه‌ی حریم خصوصی اطلاعاتی در دولت الکترونیک کدامند؟ بر اساس جدول ۶، از بین ۲۰ حقی که برای شهروندان در دولت الکترونیک در کشورهای منتخب در نظر گرفته شده است، ۱۹ مورد دارای وزن بیشتر از ۰/۵ بوده و در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۵ عبارت است از کدهای E1 تا E19.

و- مسئولیت‌های کنترل‌گر داده‌های شخصی در دولت الکترونیک

در جدول شماره ۷ الزامات مربوط به مسئولیت‌های کنترل‌گر (متولی) داده‌های شخصی در دولت الکترونیک با وزن مربوط به هر یک، لیست شده است.

جدول ۷: مسئولیت‌های کنترل‌گر داده‌های شخصی در دولت الکترونیک

وزن (W)	الزامات مربوط به مسئولیت‌های کنترل‌گر داده‌های شخصی در دولت الکترونیک (کد F)
۰/۹	F1. تدارک تمهیدات امنیتی سازمانی (مدیریتی) جهت حفاظت از داده‌های شخصی
۰/۸۱	F2. تدارک تمهیدات امنیتی فنی (نرم افزاری) جهت حفاظت از داده‌های شخصی
۰/۸۱	F3. پاسخگویی به تمامی درخواست‌های سوژه برای برخورداری از حقوق خود
۰/۸۱	F4. شفافیت در صورت رد درخواست‌های سوژه با ارائه‌ی توجیحات قانونی کافی به وی
۰/۸۱	F5. عقد قرارداد مکتوب با پردازشگر و تدوین نیازمندی‌های امنیتی برای حفاظت از امنیت داده‌های شخصی و نظارت منظم بر اجرای دستورالعمل‌های تعیین شده در قرارداد
۰/۶۳	F6. تدارک تمهیدات امنیتی فیزیکی (سخت افزاری) جهت حفاظت از داده‌های شخصی
۰/۶۳	F7. جبران خسارت‌های ناشی از نقض حریم خصوصی اطلاعاتی سوژه‌ها در صورت مقصربودن متولی طبق تشخیص نهاد دیده بان حریم خصوصی اطلاعاتی
۰/۵۴	F8. نصب مأمور حفظ حریم خصوصی اطلاعاتی (Information Privacy Officer) با دانش تخصصی کافی در حوزه حفاظت از حریم خصوصی اطلاعاتی و پشتیبانی از وی در جهت انجام وظایفش
۰/۵۴	F9. تدوین و انتشار آنلاین سیاست حریم خصوصی (Privacy Policy)
۰/۵۴	F10. آگاه‌سازی کارکنان در خصوص اهمیت حفظ محرمانگی داده‌های شخصی
۰/۳۶	F11. حفاظت از امنیت داده‌های شخصی بر اساس سطح حساسیت آنها و تخمین ریسک‌های نشت آنها
۰/۲۷	F12. تدوین و در دسترس قرار دادن سند امنیتی برای کارکنان
۰/۲۷	F13. انتخاب شایسته‌ترین پردازشگر از نظر تجربه و قابلیت اعتماد در صورت تصمیم به برون‌سپاری عملیات پردازش
۰/۲۷	F14. تعریف حوزه دسترسی کارکنان به داده‌های شخصی و به روز رسانی منظم آن
۰/۲۷	F15. استقرار سیستم احراز هویت نرم افزاری برای کنترل دسترسی کارکنان به داده‌های شخصی

سؤال فرعی ششم تحقیق عبارت است از: مسئولیت‌های کنترل‌گر داده‌های شخصی شهروندان در دولت الکترونیک کدامند؟ همانطوری که در جدول ۷ مشخص شده است، از بین ۱۵ مسئولیتی که برای متولیان (کنترل‌گرهای) داده‌های شخصی شهروندان در دولت الکترونیک مطرح شده است، ۱۰ مورد دارای وزن بالای ۰/۵ هستند. این مسئولیت‌ها اغلب برای ملزم کردن کنترل‌گرهای داده‌های شخصی به رعایت اصول امنیت اطلاعات و شفافیت در خصوص سیاست‌های حریم خصوصی هستند. نکته‌ی مهم دیگر این است که برون‌سپاری عملیات پردازش در اغلب کشورهای منتخب پیش‌بینی شده و در صورت تصمیم کنترل‌گرها به برون‌سپاری، آنها ملزم به عقد قرارداد مکتوب با پیمانکار (پردازشگر) و تدوین نیازمندی‌های امنیتی در آن قرارداد و نظارت بر اجرای دستورالعمل‌های تعیین شده در قرارداد توسط پردازشگر هستند. این الزامات دهگانه به عنوان مسئولیت‌های متولی

داده‌های شخصی در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۶ عبارت است از کدهای F1 تا F10.

ی- شرایط دسترسی شهروند به داده‌های شخصی

در جدول شماره ۸ الزامات دسترسی شهروند به داده‌های شخصی در دولت الکترونیک به همراه وزن هر یک آمده است.

جدول ۸: الزامات دسترسی شهروند به داده‌های شخصی خود

وزن (W)	الزامات مربوط به دسترسی شهروند به داده‌های شخصی (کد G)
۱	G1. لزوم فراهم کردن امکان دسترسی سوژه به داده‌های شخصی خود، در صورت درخواست سوژه
۱	G2. لزوم ارائه تمامی داده‌های مربوط به شهروند به او در صورت مجازبودن درخواست دسترسی به داده‌های شخصی (منجمله تمامی داده‌های ایجاد شده پس از پردازش داده‌های وی)
۱	G3. لزوم ارائه اطلاعات کافی (شامل اهداف پردازش و...) به سوژه هنگام دسترسی سوژه در صورت نداشتن منع قانونی
۱	G4. لزوم استفاده از روش‌های ایمن برای فراهم کردن دسترسی سوژه به داده‌های شخصی وی
۱	G5. لزوم فراهم کردن امکان دسترسی سوژه به داده‌های شخصی خود با قابلیت ویرایش و ذخیره سازی مجدد در صورت درخواست سوژه برای اصلاح آنها
۰/۸۱	G6. ممنوعیت دریافت وجه از سوژه بابت فراهم کردن دسترسی سوژه به داده‌های شخصی وی
۰/۶۳	G7. مجازبودن رد درخواست سوژه برای دسترسی به داده‌های شخصی خود در مسائل مرتبط با امنیت ملی
۰/۵۴	G8. لزوم ارائه داده‌های شخصی در قالبی قابل درک (خوانا) و بدون نیاز به نرم افزار غیر معمول در صورت قبول درخواست سوژه برای دسترسی به داده‌های شخصی خود
۰/۵۴	G9. مجازبودن رد درخواست سوژه برای دسترسی به داده‌های شخصی خود در صورت وجود منع قانونی

سؤال فرعی هفتم تحقیق عبارت است از: الزامات دسترسی شهروند به داده‌های شخصی در دولت الکترونیک کدامند؟ براساس جدول ۸، از بین ۹ الزامی که برای دسترسی شهروند به داده‌های شخصی در دولت الکترونیک در کشورهای منتخب مطرح شده است، تمامی آنها دارای وزنی بالاتر از ۰/۵ بوده و به عنوان اصول دسترسی شهروند به داده‌های شخصی در الگوی نهایی حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک قرار می‌گیرند. بنابراین پاسخ سؤال فرعی ۷ عبارت است از کدهای G1 تا G9.

نتیجه گیری

در این تحقیق الگویی برای حفاظت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک پیشنهاد شد که توسعه‌دهنده‌ی مبانی نظری دولت الکترونیک است. این الگو می‌تواند به عنوان مکملی برای توسعه‌ی دولت الکترونیک در کشورهای در حال توسعه محسوب شود. الگوی پیشنهادی هفت بعد دارد: (۱) الزامات گردآوری داده‌های شخصی شهروندان؛ (۲) الزامات استفاده از داده‌های شخصی شهروندان؛ (۳) الزامات نگهداری داده‌های شخصی شهروندان؛ (۴) الزامات افشاء داده‌های شخصی شهروندان؛ (۵) حقوق شهروند؛ (۶) مسئولیت‌های کنترل‌گر؛ و (۷) الزامات دسترسی شهروند به داده‌های شخصی. بر اساس نتایج این تحقیق، از میان ۱۲۴ الزام شناسایی شده از مطالعات اسنادی قوانین کشورهای منتخب، ۱۰۵ الزام در حداقل نیمی از کشورهای منتخب تکرار شده‌اند که به عنوان الزامات پیشنهادی در ابعاد هفت‌گانه‌ی الگوی مطرح شده معرفی شدند. با توجه به اینکه در تمامی کشورهای مورد مطالعه، برای تضمین اجرای قوانین حریم خصوصی اطلاعاتی، سازمان‌هایی مستقل به عنوان دیده‌بان حریم خصوصی اطلاعاتی وجود دارند و بر نحوه‌ی پیروی سازمانها از قوانین حفاظت از حریم خصوصی نظارت فعال دارند، بنابراین لازم است تا در کنار تدوین الگوی مطرح شده در این تحقیق، ساختارهای اجرایی برای نظارت بر حسن اجرای قوانین حریم خصوصی اطلاعاتی شهروندان نیز بوجود آید؛ در صورت عدم وجود چنین نهادهای ناظر مستقلی، ضمانت اجرایی برای الگوی پیشنهادی وجود نخواهد داشت. به عنوان مثال در کره جنوبی «کمیسیون حفاظت از اطلاعات شخصی»، در فرانسه «کمیسیون حفاظت از اطلاعات شخصی و آزادی»، در انگستان «دفتر کمیسیونر اطلاعات»، در کانادا «دفتر کمیسیونر حریم خصوصی»، در بلژیک «هیأت حریم خصوصی»، در اسپانیا «آژانس حفاظت از داده»، در ایتالیا «سازمان حافظ داده‌های شخصی»، در آلمان «نهاد حفاظت از داده»، در نروژ «نهاد حفاظت از داده»، در سوئد «کمیسیون حفاظت از امنیت و تمامیت» و در ایرلند «دفتر کمیسیونر حافظ داده‌های شخصی» به عنوان سازمان‌های مستقلی شناخته می‌شوند که بر اجرای قوانین حریم خصوصی اطلاعاتی نظارت داشته و مستقیماً به مجالس قانونگذاری (پارلمان) این کشورها گزارش می‌دهند. همچنین، پیگرد شکایات شهروندان در مورد حریم خصوصی اطلاعاتی و پیشنهاد اصلاحات مورد نیاز در قوانین حریم خصوصی جزء وظایف آنهاست.

مهمترین پیشنهادات این تحقیق جهت صیانت از حریم خصوصی اطلاعاتی شهروندان در دولت الکترونیک در کشورهای در حال توسعه عبارتند از: (۱) تدوین قانونی مجزا توسط نهادهای قانونگذار برای حفاظت از حریم خصوصی اطلاعاتی شهروندان با در نظر گرفتن الزامات شناسایی شده در این تحقیق؛ (۲) ایجاد نهادی مستقل از دولت تحت عنوان «دیده‌بان حریم خصوصی اطلاعاتی» به منظور نظارت بر حسن اجرای قوانین حریم خصوصی اطلاعاتی، دریافت و رسیدگی به شکایات شهروندان و نیز شناسایی نارسایی‌های قانونی و پیشنهاد اصلاحات مورد نیاز در قوانین موجود جهت ارتقای وضعیت حریم خصوصی اطلاعاتی شهروندان.



منابع و مأخذ

- ۱- اصلانی، حمیدرضا، (۱۳۸۹)، حقوق فناوری اطلاعات (چاپ دوم)، تهران، میزان.
- ۲- تقی پور، عبدا...، (۱۳۹۰)، دولت الکترونیکی (چاپ اول)، تهران، مبنای خرد.
- ۳- روسو، ژان ژاک، (۱۳۶۶)، قرارداد اجتماعی یا اصول حقوق سیاسی (چاپ اول)، (منوچهرکیا)، تهران، گنجینه.
- ۴- عالم، عبدالرحمن، (۱۳۸۰)، بنیادهای علم سیاست (چاپ اول)، تهران، نشر نی.
- ۵- کاتوزیان، ناصر، (۱۳۶۶)، فلسفه حقوق، جلد اول (چاپ اول)، تهران، انتشارات بهنشر.
- ۶- یعقوبی، نورمحمد، (۱۳۹۲)، دولت الکترونیک: رویکرد مدیریتی (چاپ سوم)، تهران، افکار.
- 7- Abu-Shanab, E., (2014), Antecedents of trust in e-government services: an empirical test in Jordan. *Transforming Government: People, Process and Policy*, 8(4), 480-499.
- 8- Anthony, D., Stablein, T., & Carian, E. K., (2015), Big Brother in the information age: Concerns about government information gathering over time, *IEEE Security & Privacy*, (4), 12-19.
- 9- Belanger, F., & Hiller, J. S., (2006), A framework for e-government: privacy implications, *Business Process Management Journal*, 12(1), 48-60.
- 10- BeVier, L. R., (1995), Information about individuals in the hands of government: some reflections on mechanisms for privacy protection, *William and Mary Bill of Rights Journal*, 4(2), 455-506.
- 11- Canadian Personal Information Protection Act, [2015], [online], Personal Information Protection & Electronic Documents Act of 2015 (PIPEDA), <<https://www.priv.gc.ca>>[17/08/2015].
- 12- Cullen, R., (2009), THEME ARTICLE Culture, identity and information privacy in the age of digital government, *Online Information Review*, 33(3), 405-421.
- 13- Cullen, R., & Reilly, P., (2007), Information privacy and trust in government: a citizen-based perspective from New Zealand, *Journal of Information Technology and Politics*, 4(3), 61-80.
- 14- DLA, [2016], [online], Piper's Data Protection. Privacy and Security group, <<http://www.dlapiperdataprotection.com>>[02/01/2016].
- 15- Douglas, R., [2016], [online], Identity Theft Victim Statistics, <www.identitytheft.info/about.aspx>[13/01/2016].
- 16- England Data Protection Act, [1998], [online], Data Protection Act of 1998 (DPA), <<https://ico.org.uk>>[17/08/2015].

- 17-French Data Protection Act, [1978], [online], Data Protection Act. <<http://www.legifrance.gouv.fr/Traductions/en-English>> [17/08/2015].
- 18-Ireland Data Protection Act, [2003], [online], Data Protection Act of 2003(DPA), <<https://www.dataprotection.ie>> [17/08/2015].
- 19-Gayton, C. M., (2006), Beyond terrorism: data collection and responsibility for privacy, The journal of information and knowledge management systems, 36(4), 377-394.
- 20-Germany Federal Data Protection Act, [2014], [online], Federal Data Protection Act of 2014(FDPA), <www.bfdi.bund.de> [17/08/2015].
- 21-Italian Personal Data Protection Code, [2003], [online], Personal Data Protection Code, <www.privacy.it/privacocode-en.htm>[17/08/2015].
- 22-James, G., (2000), Empowering bureaucrats, MC Technology Marketing Intelligence , 20(12), 62-68.
- 23-Korean Personal Information Protection Act, [2011], [online], Personal Information Protection Act of 2011(PIPA),<www.law.go.kr>[17/08/2015].
- 24-Landau, S., (2014), Making Sense of Snowden Part II: What's Significant in the NSA Surveillance Revelations. IEEE Security and Privacy, 12(1), 62-64.
- 25-Norway Personal Data Act, [2000], [online], Personal Data Act(PDA), <<https://www.datatilsynet.no/English>>[17/08/2015].
- 26-Spanish Data Protection Act, [2008], [online], Data Protection Act, <www.agpd.es>[17/08/2015].
- 27-Swedish Personal Data Act, [2006], [online], The Personal Data Act, <www.datainspektionen.se>[17/08/2015].
- 28-Stanford Encyclopedia of Philosophy, [2016], [online], Information Privacy Definition, <<http://plato.stanford.edu>>[12/01/2016].
- 29-Stark, L., (2016), The emotional context of information privacy, The Information Society, 32(1), 14-27.
- 30-Thibodeau, P., (2000), E-government spending to soar through. Computerworld , 34 (17), 12-13.
- 31-Westin, A., (1967), Privacy and Freedom, New York, Atheneum.

