

مقایسه تطبیقی قوانین حمایت از حریم خصوصی

اطلاعاتی در ایران و کشورهای منتخب

محمدتقی تقوی فرد،* محمدرضا تقوا،* مهدی فقیهی***

و محمدجواد جمشیدی****

تاریخ پذیرش ۱۳۹۵/۳/۱۸

تاریخ دریافت ۱۳۹۴/۱۲/۱۵

پیشرفت‌های فناوری اطلاعات و ارتباطات علاوه بر مزایایی که در پی داشته است، شهروندان را به‌طور فزاینده‌ای در معرض خطر نقض حریم خصوصی اطلاعاتی‌شان توسط سازمان‌های دولتی و غیردولتی قرار داده است. در این تحقیق قوانین حامی حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب به صورت تطبیقی با هم مقایسه شده‌اند و راهکارهایی برای کاهش فاصله ایران با استانداردهای جهانی در این زمینه پیشنهاد شده است. روش‌شناسی این تحقیق، کیفی و شامل روش‌های مطالعات اسنادی، تحلیل محتوا (با کدگذاری باز و محوری) و مطالعه تطبیقی است. جامعه آماری شامل ۵۸ کشور دارای قانون حمایت از حریم خصوصی اطلاعاتی است که با روش نمونه‌گیری قضاوتی، ۶ کشور (کره جنوبی، انگلستان، فرانسه، کانادا، ایتالیا و ایرلند) به‌عنوان کشورهای پیشرو انتخاب شده‌اند. چارچوب مقایسه تطبیقی حریم خصوصی اطلاعاتی دارای هفت بعد است: اصول گردآوری، استفاده، نگهداری و افشای داده‌های شخصی شهروندان، حقوق سوژه، مسئولیت‌های کنترلگر و اصول دسترسی سوژه به داده‌های شخصی. نتایج تحقیق نشان می‌دهد، وضعیت حمایت از حریم خصوصی اطلاعاتی در ایران فاصله بسیار زیادی با کشورهای منتخب و استانداردهای جهانی دارد.

کلیدواژه‌ها: حمایت از داده؛ حریم خصوصی اطلاعاتی؛ حقوق شهروند؛ مسئولیت‌های کنترلگر

* دانشیار گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی (نویسنده مسئول)؛

Email: dr.taghavifard@gmail.com

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

Email: taghva@gmail.com

Email: mail@mfaghihi.ir

*** استادیار مرکز پژوهش‌های مجلس شورای اسلامی؛

**** دانشجوی دکتری مدیریت فناوری اطلاعات، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی؛

Email: m_j_jamshidi@yahoo.com

مقدمه

فناوری اطلاعات و ارتباطات، همان قدر که زندگی انسان‌ها را راحت‌تر کرده است، آنها را در معرض خطراتی نیز قرار داده است. نقض حریم خصوصی اطلاعاتی شهروندان از جمله پیامدهای ناخوشایند دیجیتالی شدن زندگی امروزی است. در عصر حاضر، گویی انسان‌ها در خانه‌های شیشه‌ای می‌زیند و زندگی خصوصی آنها، جنبه‌ای عمومی یافته است. سازمان‌های مختلف می‌توانند به کوکی‌ها،^۱ گزارش‌ها،^۲ آدرس‌های آی. پی^۳ و حتی وبسایت‌های مورد دسترسی قرار گرفته توسط شهروندان دسترسی پیدا کنند (Belanger and Hiller, 2006: 54). یا با دسترسی به حجم عظیم داده‌های شهروندان که روی منابع پراکنده اطلاعاتی قرار گرفته است، از جنبه‌های پنهان و خصوصی زندگی افراد آگاه شوند (Margetts and Sutcliffe, 2013: 139).

حقوق شخصی انسان‌ها در دنیا مجموعه‌ای است از امتیازات که قوانین بین‌المللی آنها را برای افراد به رسمیت شناخته‌اند و دیگر افراد و نیز نهادهای خصوصی و دولتی موظف به رعایت و احترام به این حقوق هستند (هاشمی، ۱۳۸۴: ۳). بسیاری از کنوانسیون‌های بین‌المللی همچون «اعلامیه جهانی حقوق بشر (۱۹۴۸)»، «کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی (۱۹۵۰)»، «عهدنامه بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶)»، «اعلامیه تهران یا کنوانسیون بین‌المللی حقوق بشر (۱۹۶۸)»، «کنوانسیون آمریکایی حقوق بشر (۱۹۶۹)»، «کنفرانس حقوق دانان نروژ (۱۹۷۷)» و «اعلامیه اسلامی حقوق بشر (۱۹۹۰)»، دولت‌های کشورهای جهان را به حفاظت فعال از حقوق شهروندان‌شان در خصوص حریم خصوصی‌شان ملزم کرده‌اند. به‌عنوان مثال، در ماده (۱۲) اعلامیه جهانی حقوق بشر آمده است: «نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات هیچ‌کس مداخله‌های خودسرانه صورت گیرد یا به شرافت و آبرو و شهرت کسی حمله شود؛ در برابر چنین مداخله‌هایی برخورداری از حمایت قانون حق هر شخصی است» (Universal Declaration of Human Rights, 1948: 2-4). اما با وجود تأکید

1. Cookies
2. Logs
3. IP

قوانین فراملی و بین‌المللی بر لزوم حمایت از داده‌های شخصی شهروندان،^۱ متأسفانه بیشتر کشورهای دنیا از این نظر در وضعیت مناسبی به سر نمی‌برند. به طوری که یا قانونی در این زمینه به تصویب نرسانده‌اند یا قوانین بخشی و جزئی در آنها وجود دارد (DLA, 2016)؛ از نظر مؤسسه دی. ال. ای.^۲ ۱۳۸ کشور جهان (از جمله ایران) در وضعیت بسیار ضعیفی از نظر حمایت از حریم خصوصی اطلاعاتی شهروندان قرار گرفته‌اند.

هرچند در کشورهای پیشرفته، قانون حمایت از داده (یا حریم خصوصی اطلاعاتی) در همان سال‌های اولیه توسعه فناوری اطلاعات و اینترنت مورد توجه قرار گرفته است، اما در ایران متأسفانه توجه کمی به این موضوع شده است؛ ضرورت حمایت از «حریم خصوصی شهروندان» در برخی قوانین ایران مطرح شده است. به عنوان مثال می‌توان به قانون اساسی و قانون مسئولیت مدنی اشاره کرد. در قانون اساسی جمهوری اسلامی ایران، در اصول (۲، ۲۲، ۲۳، ۲۵، ۲۸، ۳۲، ۳۳ و ۳۹)، بر حفظ حریم خصوصی افراد و ممنوع بودن تجسس در اسرار دیگران تأکید شده است. همچنین در «ماده (۱)» قانون مسئولیت مدنی، مصوب ۱۳۳۹ آمده است: «هر کس بدون مجوز قانونی عمداً و یا در نتیجه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجاری یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه وارد نماید که موجب ضرر مادی یا معنوی دیگر شود، مسئول جبران خسارت ناشی از عمل خود می‌باشد». هرچند در قانون مسئولیت مدنی به صورت مستقیم به حریم خصوصی اشاره نشده است، اما می‌توان چنین برداشت کرد که اشاره به جان یا مال، آزادی، حیثیت و سایر حقوق شهروندان بی‌ارتباط با حریم خصوصی نباشد.

اما برخلاف اسناد بالادستی جمهوری اسلامی ایران به ویژه قانون اساسی، مقررات و قوانین حاکم ایران، حافظ حریم خصوصی شهروندان و داده‌های شخصی آنان نیست. با مطالعه قوانین حوزه سایبر در ایران به این موضوع می‌توان پی برد که اولاً، قانونی مجزا برای «حمایت از داده یا صیانت از حریم خصوصی اطلاعاتی» در ایران وجود ندارد. ثانیاً، قوانین موجود به صورت بسیار محدود به حمایت از داده‌های شخصی شهروندان پرداخته‌اند. در «قانون جرائم رایانه‌ای» مصوب ۱۳۸۸، مصادیق جرائم رایانه‌ای مشخص و برای ارتکاب

1. Data Protection

2. DLA

آنها تدابیر کیفی پیش‌بینی شده است؛ در این قانون، مسائلی همچون دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، جعل رایانه‌ای، سرقت و کلاهبرداری مرتبط با رایانه، جرائم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب همگی جرم محسوب شده و مرتکبان آنها به مجازات محکوم خواهند شد. به‌عنوان مثال، در ماده (۱) قانون جرائم رایانه‌ای آمده است: «هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد». همچنین در ماده (۲) این قانون آمده است: «هر کس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». در این قانون همچنین به مسائل مربوط به جمع‌آوری ادله الکترونیکی توسط نهادهای قضایی جهت کشف جرم پرداخته شده است؛ قوانین مربوط به کالبد شکافی رایانه‌ای^۱ که در آن، هدف، کشف ادله قابل استناد در دادگاه جهت اثبات وقوع جرم در محیط سایبر است. به‌عنوان مثال در ماده (۳۳) این قانون آمده است: «ارائه‌دهندگان خدمات میزبانی داخلی موظف‌اند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند». با توجه به محتوای قوانین حمایت از «حریم خصوصی اطلاعاتی» در کشورهای پیشرو، تنها قانونی که به‌عنوان مبنای مقایسه تطبیقی می‌توان به آن استناد کرد، قانون تجارت الکترونیک (بندهای «۵۸» تا «۶۱») است؛ چراکه در این قانون ابعاد حریم خصوصی اطلاعاتی (الزامات مربوط به گردآوری، نگهداری، استفاده، افشای داده‌های شخصی شهروندان، حقوق سوژه و مسئولیت‌های کنترل‌گر) تا حدی تحت پوشش قرار گرفته‌اند. این قانون مشتمل بر هشتاد و یک ماده و هفت تبصره بوده و در تاریخ ۱۷ دی ماه ۱۳۸۲ در مجلس شورای اسلامی تصویب و در ۲۴ دی ماه همان سال به تأیید شورای نگهبان رسیده است.

خلاً قانونی موجود در زمینه حریم خصوصی باعث شده است تا ضرورت حفاظت از حریم خصوصی اطلاعاتی شهروندان در ایران در تازه‌ترین سیاست‌های ابلاغی مقام معظم رهبری به شورای عالی فضای مجازی کشور در تاریخ ۴ شهریور ۱۳۹۴، به‌وضوح بیان شود (ششمین بند این سیاست‌ها عبارت است از: اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی کشور و نیز حفظ حریم خصوصی آحاد جامعه؛ و دهمین بند به این شرح است: تدوین و تصویب نظام‌های امنیتی، حقوقی، قضایی و انتظامی مورد نیاز در فضای مجازی). در ایران بنا به در حال رشد و توسعه بودن فناوری اطلاعات، دولت الکترونیک و تجارت الکترونیک و همچنین قابلیت‌های فزاینده سازمان‌ها در دسترسی هرچه بیشتر به داده‌های شخصی شهروندان، لازم است تا مسئله صیانت از داده‌های شخصی شهروندان به طریقی نظام‌مند مورد مذاقه قرار گیرد. بنابراین در این نوشتار سؤالات اصلی که به دنبال پاسخی برای آنها هستیم عبارت‌اند از: ایران در مقایسه با کشورهای منتخب از حیث وجود قوانین صیانت از حریم خصوصی شهروندان در چه وضعیتی قرار دارد؟ و چه اصولی را می‌توان به‌عنوان اصول استاندارد حمایت از حریم خصوصی اطلاعاتی، برای قانونگذاری در این حوزه به قانونگذار ایرانی پیشنهاد داد؟

۱. مبانی نظری

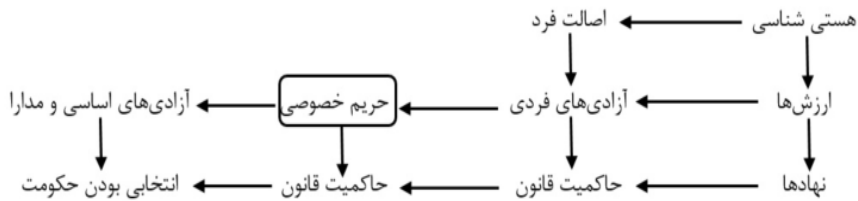
در ادامه مبانی نظری تحقیق شامل تعریف مفهوم حریم خصوصی و بیان مبانی هستی‌شناسی آن و نیز مبانی حریم خصوصی از منظر آیات، روایات و فقه اسلامی مورد بررسی قرار گرفته است. همچنین در این بخش، تعاریف، تاریخچه و اصول «حریم خصوصی اطلاعاتی» بیان شده است.

۱-۱. مفهوم حریم خصوصی^۱

حریم خصوصی جزء مفاهیمی است که تاکنون بر آن معنای جامعی ارائه نشده است. «حریم خصوصی» از نظر لغوی به معنای جا، مکان و محدوده‌ای شخصی است که ورود و

مداخله در آن جایز نیست (آماده، ۱۳۹۲: ۱۸). اما از نظر کاربردی «حریم خصوصی را می‌توان فضایی دانست که نمی‌توان بدون اجازه شخصی به آن تجاوز یا تعرض کرد؛ در واقع دسترسی به آن فضا برای دیگران امکان‌پذیر نیست» (انصاری، ۱۳۸۰: ۲۷۰). به عبارت دیگر «حریم خصوصی عبارت است از حق اولیه افراد در مصون ماندن حوزه خصوصی ایشان از هرگونه مداخله یا تعرض فاقد مجوز قانونی و همچنین منع دیگران از وقوف بر اطلاعات این حوزه» (اصلانی، ۱۳۸۹: ۲۰). وین فیلد که یکی از قدیمی‌ترین مقالات را در زمینه حریم خصوصی نوشته است، حریم خصوصی را «محرمانه بودن خصوصیات شخص یا مال او از انظار عموم» معنا کرده است (هارلو، ۱۳۸۳: ۱۶۳). همان‌طور که در شکل ۱ آمده است، حریم خصوصی از نظر مبانی هستی‌شناسی ریشه در اصالت فرد داشته و از آزادی‌های فردی نشئت می‌گیرد.

شکل ۱. مبانی فلسفی حریم خصوصی



مأخذ: سروش، ۱۳۹۳: ۳۷.

۱-۲. حفظ حریم خصوصی از منظر آیات و روایات

هرچند در فرهنگ و دموکراسی غربی حفظ حریم خصوصی شهروندان دارای ریشه‌های زیادی است، اما نباید آن را غربی دانست. دین مبین اسلام در ۱۴۰۰ سال قبل بر لزوم رعایت و احترام به حریم خصوصی دیگران تأکید ورزیده و هرگونه تعرض به خلوت آنها را منع کرده است (آماده، ۱۳۹۲: ۳۳). انسان به‌عنوان اشرف مخلوقات^۱ و جانشین خداوند روی

۱. وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبُرِّ وَالْبَحْرِ وَرَزَقْنَاهُمْ مِنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِمَّنْ خَلَقْنَا تَفْضِيلًا (اسرا: ۷۰).

زمین^۱ در قرآن کریم دارای جایگاهی بسیار ویژه و عالی قدر است به طوری که خداوند متعال وی را شایسته سجده توسط فرشتگان دانسته و از دمیدن روح خود در وی خبر می‌دهد.^۲ در قرآن کریم مبحث جداگانه‌ای برای حریم خصوصی اختصاص نیافته است اما در برخی آیات به مسائل مرتبط با حفظ حریم خصوصی افراد پرداخته شده است: ۱. سوره مبارکه حجرات، آیه شریفه ۱۲ (ممنوعیت تجسس و تفتیش از افراد)؛ ۲. سوره مبارکه نساء، آیه شریفه ۲۹ (ممنوعیت استراق سمع و بصر، ممنوعیت تعرض به اموال شخصی افراد)؛ ۳. سوره مبارکه نور، آیات شریفه ۲۷ و ۲۸ و نیز سوره مبارکه بقره آیه شریفه ۱۸۹ (ممنوعیت ورود بدون اجازه به منازل افراد). پیامبر اکرم (ص) و ائمه اطهار (ع) در گفتار و کردار خود بر حفظ حریم خصوصی افراد و آبروی مؤمنان تأکید کرده‌اند. پیامبر اکرم (ص) حرمت مؤمن را از سه جهت تاقیامت محترم دانسته‌اند: خون، مال و آبروی مؤمن (الحرانی، ۱۳۶۳: ۳۱). از امام صادق (ع) نیز نقل شده است که احترام مؤمن از احترام کعبه بالاتر است.^۳

۳-۱. حفظ حریم خصوصی از منظر فقه اسلامی

از منظر فقه اسلامی، حفظ حریم خصوصی با عنوان «الناس مسلطون علی اموالهم» تعبیر شده و بر این اساس نیز حریم خصوصی با مالکیت خصوصی مترادف گردیده است (آماده، ۱۳۹۲: ۳۴). به تعبیر دیگر در فقه اسلامی هر فرد اختیار خود را دارد. محققان دو اصل فقهی را در حفظ حریم خصوصی شهروندان بر شمرده‌اند: ۱. اصل عدم ولایت؛ و ۲. اصل احتیاط (سروش، ۱۳۹۳: ۹۶). طبق اصل عدم ولایت هرگونه دخالت در شئون زندگی دیگران نیازمند آن است که شخص از «سلطه و اختیاری» نسبت به دیگری برخوردار باشد و تا وقتی که دلیلی برای این حق ارائه نشود، چنین سلطه‌ای مردود بوده و چنین دخالتی محکوم است. بنابراین اصل بر «عدم ولایت» است. فقهای همچون علامه حلی، فخر المحققین، فاضل هندی، سیدعلی طباطبائی، نراقی و شیخ انصاری به این اصل استناد

۱. إني جعل في الارض خليفة (بقره: ۳۰).

۲. نفخت في من روجي (حجر: ۲۹).

۳. الْمُؤْمِنُ أَكْبَرُ حُرْمَةً مِنَ الْكَعْبَةِ (طبرسی، بی تا: ۸۳).

کرده‌اند (همان: ۹۷). بنابراین اگر فردی بخواهد بدون اذن و اجازه شهروندان اطلاعاتی را از زندگی خصوصی شهروندان کسب کند، طبق اصل عدم ولایت و بنا به ادله عقلی موجب محرومیت شهروند از حقوقش شده و مجاز نیست. البته در مواردی که بنا به حکم قانون یا قاضی شرع اذن شهروند نیاز نباشد می‌تواند استثناء قرار گیرد. اصل دیگر «اصل احتیاط» است؛ این اصل لزوم احتیاط در تعرض به «عرض» و «جان» شهروندان را نشان می‌دهد، به طوری که در مواردی که احتمال می‌رود پای آبرو و جان شهروندان در میان باشد «احتیاط عقلی» حاکم است (یعنی نیازی نیست که در متون دینی دلیلی برای لزوم احتیاط پیدا شود بلکه عقل حکم می‌کند که باید حریم خصوصی شهروندان مورد صیانت قرار گیرد). برخی علما همچون امام خمینی (ره)، آیت‌... گلپایگانی، آخوند خراسانی، خوبی، عراقی و کریمی جهرمی به این اصل استناد کرده‌اند (همان: ۹۹-۱۰۰). بنابراین طبق فقه اسلامی نقض حریم خصوصی شهروندان همیشه نیازمند دلیل جواز است و تا وقتی وجود چنین دلیلی مورد تردید باشد، اصل بر ممنوعیت نقض است.

۱-۴. مفهوم حریم خصوصی اطلاعاتی^۱

برای حریم خصوصی ابعادی برشمرده‌اند: حریم خصوصی مکانی؛ حریم خصوصی جسمانی؛ حریم خصوصی شخصیت؛ حریم خصوصی خانواده؛ حریم لوازم شخصی؛ حریم خصوصی ارتباطاتی؛ و حریم خصوصی اطلاعاتی (همان: ۲۶-۱۶؛ انصاری، ۱۳۸۰: ۱۸۳-۱۵۹). با توجه به اینکه در این تحقیق بعد «حریم خصوصی اطلاعاتی» مدنظر قرار گرفته است، در ادامه به تعریف این مفهوم و بیان تاریخچه آن در قوانین ملی و بین‌المللی پرداخته شده است.

در عصر حاضر شاید مهم‌ترین جنبه حریم خصوصی، همان حریم خصوصی اطلاعاتی باشد چراکه سازمان‌های دولتی و غیردولتی به راحتی می‌توانند به حجم عظیمی از داده‌های شخصی شهروندان دسترسی پیدا کنند بدون اینکه حتی شهروندان از این موضوع مطلع شوند. آلن وستین^۲ (۱۹۶۷: ۷) «حریم خصوصی اطلاعاتی» را چنین تعریف کرده است: «حریم

1. Information Privacy

2. Alan Westin

خصوصی اطلاعاتی عبارت است از مطالبه‌ای که افراد، گروه‌ها، یا نهادها در زمینه تعیین چگونگی و حد انتقال اطلاعات در مورد آنها به سایرین دارند». بنابراین، حریم خصوصی اطلاعاتی یک حق است. حقی که افراد برای کنترل اطلاعات خود در برابر جست‌وجوهای نابجا، استراق سمع،^۱ تجسس،^۲ تصاحب^۳ و سوءاستفاده‌هایی که ممکن است از اطلاعات شخصی‌شان شود، دارند (Stanford Encyclopedia of Philosophy, 2016). فلوریدی^۴ (۱۹۹۹: ۵۲) حریم خصوصی اطلاعاتی را «آزادی از دخالت [های] معرفت‌شناختی»^۵ معنا می‌کند که هنگامی حاصل می‌شود که محدودیت‌هایی در مورد «حقایق»^۶ در مورد فردی که «ناشناخته»^۷ است، وجود داشته باشد. برخی محققان معتقدند حریم خصوصی اطلاعاتی شامل داده‌هایی در مورد فعالیت‌های روزانه یک فرد، زندگی شخصی وی، امور مالی او، تاریخچه سلامت وی و حتی موفقیت‌های دانشگاهی‌اش می‌شود. از آنجا که داده‌های شخصی افراد هم می‌تواند شامل داده‌هایی شود که مربوط به یک فرد بوده و در جایی ذخیره شده باشد یا داده‌هایی باشد که مربوط به ارتباطات فرد (مثل ایمیل، مکالمه‌های تلفنی، رسانه‌های ارتباطی بی‌سیم و ...)، تمایزی میان حریم خصوصی اطلاعاتی و حریم خصوصی ارتباطاتی^۸ به وجود آمده است (Tavani, 2008: 9; Johnson and Nissenbaum, 1995: 262-268). از این رو، آن دسته داده‌های مربوط به مکالمه‌های الکترونیکی با عنوان حریم خصوصی ارتباطاتی شناخته شده و خارج از حوزه این تحقیق تلقی می‌شود. با توجه به ضعف مبانی نظری تحقیق، به نظر می‌رسد درک مفهوم حریم خصوصی اطلاعاتی تنها با مراجعه به قوانین بین‌المللی و قوانین ملی کشورهای پیشرو ممکن باشد.

۵-۱. حریم خصوصی اطلاعاتی از منظر قوانین بین‌المللی و ملی

سازمان ملل متحد در دسامبر ۲۰۱۳ به اتفاق آراء، رأی به گنجاندن حق حفظ حریم

1. Eavesdropping
2. Surveillance
3. Appropriation
4. Floridi
5. Freedom from Epistemic Interference
6. Facts
7. Unknown
8. Communication Privacy

خصوصی اطلاعاتی افراد به عنوان یکی از بندهای حقوق بشر داده است تا انسان‌ها از این حقوق برخوردار باشند: الف) هرگونه ارتباطات برخط آنها مورد احترام قرار گرفته و حفاظت شود؛ ب) از تجاوز به حریم خصوصی آنها جلوگیری شده و قوانینی ملی کشورها با حق حفظ حریم خصوصی آنان سازگاری داشته باشد؛ ج) فرایندها، رویه‌ها و قوانین نظارت بر انتقال اطلاعات و جمع‌آوری داده‌های شخصی باید با حق حفظ حریم خصوصی اطلاعاتی افراد تطابق داشته باشد؛ و د) مکانیزم‌هایی برای اطمینان از شفافیت و مناسب بودن اقدامات دولت‌ها در نظارت بر انتقال و جمع‌آوری داده‌های شخصی افراد به وجود آید (1: Sharwood, 2013). با وجود این، تمامی کشورهای عضو سازمان ملل، به خصوص کشورهای در حال توسعه، قانونی برای صیانت از حریم خصوصی اطلاعاتی به تصویب نرسانده‌اند. در کشورهای پیشرفته قانونی به نام حمایت از داده^۱ یا صیانت از حریم خصوصی اطلاعاتی^۲ وجود دارد که همه سازمان‌های دولتی و غیردولتی را ملزم به رعایت مجموعه‌ای از الزامات کرده است.

از اولین تلاش‌های شهروندان برای حفظ حریم خصوصی اطلاعاتی خود در برابر دولت می‌توان به تلاش‌های سیاهان آمریکا در دهه ۱۹۵۰ اشاره کرد. در آن زمان دولت آمریکا مخالفان سیاه‌پوست را بنا به اظهارنظر درباره مسائل مختلف جامعه آن زمان، شناسایی و تحت پیگرد قرار می‌داد. دولت محلی آلاباما، برای ارباب‌انجمن ملی پیشرفت مردم رنگین‌پوست «تلاش کرد تا انجمن را مجبور به افشای اطلاعات مربوط به اعضای انجمن کند. اما دیوان عالی آمریکا طرف انجمن را گرفت و حق «عدم تعیین هویت» و مخفی ماندن اطلاعات افراد (همچون نام آنها) زیر دست‌نوشته‌ها و اعلامیه‌ها را به رسمیت شناخت. قانون حفظ حریم خصوصی در سال ۱۹۷۴ از اولین قوانینی بود که - با توجه به تقدم آمریکا در توسعه اینترنت - در این کشور به منظور حفظ حریم خصوصی اطلاعاتی شهروندان به تصویب رسید. این قانون ملزم کرد هر نهادی را که اطلاعات قابل شناسایی افراد (همچون کدملی، تلفن، اطلاعات DNA، اثر انگشت، اطلاعات کارت‌های بانکی و ...) را نگهداری می‌کند علاوه بر اینکه در مورد نحوه استفاده از اطلاعات،

1. Data Protection Act

2. Information Privacy Act

اطلاع‌رسانی کند، بلکه آن اطلاعات را قابل دسترس کرده، از صحت آنها مطمئن شده، امکان بازرسی از آنها را فراهم آورده و همچنین اجازه به اشتراک‌گذاری‌شان را فراهم آورد (Bevier, 1995: 456-457). پس از ایالات متحده، بسیاری از کشورها نیز درصدد ارائه راهکاری برای موضوع حفظ حریم خصوصی شهروندان شدند. در اتحادیه اروپا نیز در سال ۱۹۹۵ دستورالعملی به‌عنوان «رهنمود حمایت از داده»^۱ کشورهای عضو آن اتحادیه را ملزم به تصویب قوانین حمایت از داده جهت صیانت از حقوق حریم خصوصی اطلاعاتی شهروندان در آن کشورها کرد. برخی کشورهای آسیایی مثل کره جنوبی و ژاپن نیز پس از کشورهای غربی اقدام به تصویب قوانین مشابه کردند. ژاپن، قانون حفاظت از اطلاعات شخصی را در سال ۲۰۰۳ به تصویب رساند. قانونی که متوجه نهادهای دولتی مرکزی، محلی و منطقه‌ای و نیز کسب‌وکارها و سایر نهادهای خاص می‌شد. در این قانون، حفاظت از اطلاعات شخصی افراد، از جمله نام، تاریخ تولد، آدرس پستی یا ایمیل، عنوان شغلی، اطلاعات استخدامی و ... برای سازمان‌های مشمول ضروری شده بود (Japan Personal Information Protection Act, 2003). کره جنوبی نیز در سال ۲۰۱۱ قانون حفظ حریم خصوصی اطلاعاتی را به تصویب رسانده که در آن اصول زیادی برای ضابطه‌مندسازی پردازش داده‌های شخصی شهروندان گنجانده است (Korean Personal Information Protection Act, 2011). متأسفانه تاکنون قانونی جامع برای حفظ حریم خصوصی اطلاعاتی شهروندان در ایران مصوب نشده است. با این وجود، در برخی قوانین همچون قانون تجارت الکترونیکی در بخش‌هایی به این مهم پرداخته است.

۶-۱. اصول حفظ حریم خصوصی اطلاعاتی

یکی از شناخته‌شده‌ترین دسته‌بندی‌های اصول حفظ حریم خصوصی اطلاعاتی می‌توان به اصول مطرح شده توسط سازمان همکاری و توسعه اقتصادی^۲ اشاره کرد. این اصول برای کشورهای عضو این سازمان به‌عنوان راهنمایی برای تدوین قوانین درون‌مرزی برای حفاظت از حریم خصوصی اطلاعاتی شهروندان پیشنهاد شده‌اند. این اصول عبارت‌اند از:

1. Data Protection Directive

2. Organization for Economic Cooperation and Development (OECD)

۱. اصل محدودیت جمع آوری: ^۱ باید محدودیت‌هایی در جمع آوری داده‌های شخصی وجود داشته باشد. همچنین همه داده‌های شخصی تنها باید از سوی ابزارهای قانونی و منصفانه و با اطلاع و رضایت افراد به دست آیند. ۲. اصل کیفیت اطلاعات: ^۲ داده‌های شخصی باید مربوط به اهدافی باشند که در آن زمینه مورد استفاده واقع می‌شوند؛ همچنین تا حدی که برای این اهداف مورد نیاز است، باید دقیق، کامل و به روز باشند. ۳. اصل مشخص بودن هدف: ^۳ اهدافی که در جهت آنها داده‌های شخصی جمع آوری می‌شوند، باید درست هنگام جمع آوری داده‌ها مشخص شوند و نیز استفاده‌های بعدی نیز باید محدود به برآورده کردن همان اهداف، یا اهدافی سازگار با اهداف اولیه باشند. ۴. اصل محدودیت استفاده: ^۴ داده‌های شخصی نباید در جهت اهدافی غیر از اهداف مشخص شده، آشکار شده، در دسترس قرار گرفته، یا مورد استفاده قرار گیرند، مگر در شرایطی با رضایت صاحب داده‌ها یا نهاد قانونی صاحب اختیار. ۵. اصل تدابیر حفاظتی امنیتی: ^۵ تدابیر حفاظتی ایمنی معقولی باید برای حفاظت از داده‌های شخصی در مقابل ریسک‌هایی چون از دست دادن یا دسترسی، تخریب، استفاده، اصلاح، یا افشای غیرمجاز داده‌ها به کار گرفته شوند. ۶. اصل گشودگی ^۶ (یا شفافیت): باید سیاستی کلی برای گشودگی (صراحت) در مورد توسعه، روش‌ها و سیاست‌های مربوط به داده‌های شخصی وجود داشته باشد. ابزارهای استقرار وجود و ماهیت داده‌های شخصی و اهداف اصلی استفاده از آنها باید در دسترس عموم قرار گرفته و نیز باید هویت نهاد کنترل‌کننده و در اختیار دارنده داده‌ها به‌طور شفاف بیان شود. ۷. اصل مشارکت فردی: ^۷ هر فرد باید این حق را داشته باشد که: تصدیقی از کنترل‌کننده داده‌ها به دست آورد که کنترل‌کننده داده‌های مربوط به وی را در اختیار دارد یا خیر؛ همچنین باید بتواند داده‌های مربوطه را (به‌صورت قانونی) به چالش کشیده و اگر پیگرد قانونی موفقیت‌آمیز بود، بتواند داده‌ها را اصلاح یا کامل کرده و تغییر

-
1. Collection Limitation Principle
 2. Data Quality Principle
 3. Purpose Specification Principle
 4. Use Limitation Principle
 5. Security Safeguards Principle
 6. Openness Principle
 7. Individual Participation Principle

دهد یا حذف کند. ۸. اصل پاسخگویی: ^۱ یک کنترل کننده داده باید پاسخگویی تطابق با سنجها (معیارها)یی باشد که اصول فوق‌الذکر را عملی می‌سازند (OECD, 2013).

سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه، ^۲ نیز همچون اصول سازمان همکاری و توسعه اقتصادی اصولی را برای حفاظت از داده‌های شخصی شهروندان کشورهای عضو پیشنهاد داده است. این اصول در سال ۲۰۰۳ مطرح شد و در سال ۲۰۰۵ توسط کشورهای عضو لازم‌الاجرا تلقی شد. برخلاف اصول سازمان همکاری و توسعه اقتصادی که به‌عنوان به‌اصطلاح کف شناخته می‌شوند و کشورهای عضو می‌توانند با تدوین قوانین ضرورت جداگانه، این اصول را ارتقا دهند، در اصول سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه، در هیچ کجا بیان نشده است که کشورهای عضو می‌توانند با تصویب قوانین تقویتی، این اصول استاندارد را ارتقا دهند. بنابراین به نظر می‌رسد در چارچوب پیشنهادی سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه برای حفاظت از حریم خصوصی اطلاعاتی سقف تعیین شده است (Greenleaf, 2009). اصول ^۳ نه‌گانه سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه به این شرح است: ۱. اصل پیشگیری از ضرر: اصول حفاظت از حریم خصوصی اطلاعاتی باید بر مبنای جلوگیری از ضرر افراد طراحی شوند؛ ۲. اصل اطلاع‌رسانی: افراد باید در مواقع لزوم از اطلاعاتی همچون: اهداف گردآوری، احتمال افشای داده‌های شخصی، جزئیات مربوط به مشخصات کنترل‌گر داده‌های شخصی، روش‌هایی که یک فرد می‌تواند استفاده از داده‌های شخصی خود را محدود کند، راه‌های اصلاح داده‌های شخصی و روش‌های دسترسی به آن داده‌ها توسط فرد آگاه شوند؛ ۳. اصل محدودیت گردآوری: داده‌های شخصی باید مرتبط با اهداف گردآوری باشند و باید حداقل اطلاعات در مورد افراد گردآوری شود. ۴. اصل (محدودیت) استفاده از داده‌های شخصی: استفاده از داده‌های شخصی افراد باید سازگار با اهداف مرتبط با گردآوری بوده و همراه با جلب رضایت فرد انجام گیرد. ۵. اصل انتخاب: افراد باید بتوانند در خصوص گردآوری، استفاده و افشای داده‌های شخصی خود از حق انتخاب برخوردار

1. Accountability Principle

2. Asia-Pacific Economic Cooperation (APEC)

3. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ccsg_privacyframewk.ashx

باشند. ۶. اصل یکپارچگی اطلاعات شخصی: اطلاعات شخصی افراد باید تا حد مورد نیاز برای اهداف استفاده، دقیق، کامل و به روز باشند. ۷. اصل تدابیر حفاظتی امنیتی: کنترلگرهای داده باید تدابیر حفاظتی امنیتی کافی را برای جلوگیری از ریسک‌های داده‌های شخصی متناسب با شدت ریسک و حساسیت اطلاعات به کار گیرند. ۸. اصل دسترسی و اصلاح: افراد باید بتوانند به داده‌های شخصی خود دسترسی داشته باشند و در صورت غیرصحیح بودن، بتوانند آنها را اصلاح کنند. و ۹. اصل مسئولیت‌پذیری: کنترلگر داده‌های شخصی مسئولیت تطابق با اصول مطرح‌شده فوق را دارد و در صورت انتقال داده‌های شخصی به شخص یا کشور ثالث باید از قبل رضایت فرد را جلب کرده باشد.

به نظر می‌رسد قوانین ملی کشورهای پیشرو عموماً مبتنی بر یکی از دسته‌بندی‌های پیش‌گفته است. هرچند تفاوت‌هایی نیز میان آنها دیده می‌شود که نشان از استثنائاتی برای ورود به حریم خصوصی شهروندان است. با توجه به اینکه با بررسی ادبیات تحقیق به نظر می‌رسد که نه تنها تعریف جامعی برای حریم خصوصی اطلاعاتی، صاحب‌نظران ارائه نداده‌اند، بلکه ابعاد حریم خصوصی اطلاعاتی نیز نامشخص است. بنابراین تنها گزینه ممکن برای درک مفهوم حریم خصوصی اطلاعاتی، بررسی همه‌جانبه قوانین کشورهای پیشرفته در این زمینه و استخراج ابعاد و شاخص‌های مربوط به هر بعد است که در این مقاله چارچوبی نسبتاً جامع برای آن پیشنهاد شده است. با وجود اینکه سابقه حریم خصوصی اطلاعاتی در قوانین بین‌المللی و ملی تقریباً به دو دهه پیش بازمی‌گردد، اما تعداد تحقیقات انجام شده در دنیا در این حوزه چندان زیاد نیست. در ادامه پیشینه پژوهش مورد بررسی قرار گرفته است.

۲. پیشینه پژوهش

گیتون، در تحقیقی به بررسی ارتباط میان وجود قوانین مربوط به حفظ حریم خصوصی اطلاعاتی و میزان صیانت از حقوق محرمانگی شهروندان توسط دولت‌ها و کسب‌وکارها پرداخته است. وی ادعا کرده است که دولت‌ها و کسب‌وکارها در مورد اطلاعاتی که از افراد (شهروندان/مشتریان) جمع‌آوری می‌کنند زیاد حساس نبوده و در مورد حفاظت از محرمانگی آنها اغلب غفلت می‌کنند. نتیجه‌گیری وی نشان می‌دهد که تنها در صورت وجود قوانین حفظ

حریم خصوصی، اطلاعاتی جامع است که می‌توان امید داشت تا داده‌های شخصی شهروندان مورد حفاظت قرار گیرد (Gayton, 2006). در پژوهشی دیگر کولن به بررسی معضلات پیرامون حفظ حریم خصوصی اطلاعاتی شهروندان در نیوزیلند و ژاپن پرداخته است. نتایج تحقیق وی 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 پایین‌تری هستند، نسبت به محرمانگی اطلاعات خود حساسیت بیشتری نشان می‌دهند. با وجود این طبق نتایج این تحقیق، همه گروه‌های مورد بررسی در هر دو کشور نسبت به حفظ حریم خصوصی اطلاعاتی خود حساسیت نشان داده‌اند (Cullen, 2009).

تحقیقات بومی اغلب در حوزه حمایت از داده‌های پزشکی صورت گرفته‌اند. به عنوان مثال فقیهی، معمارزاده و رفوگر آستانه (۱۳۸۹) به بررسی وضعیت محرمانگی اطلاعات در سلامت الکترونیک در ایران پرداخته‌اند. طبق این تحقیق، متأسفانه برخلاف کشورهای چوچون آلمان، انگلیس و کانادا، وضعیت محرمانگی اطلاعات پزشکی در ایران با وضعیت مقبول فاصله زیادی دارد. آنها پیشنهاد داده‌اند که برای حفاظت از محرمانگی اطلاعات بیماران، نیاز است تا قانونگذاران دسترسی به این اطلاعات را برای مجریان در چارچوب قانون، ضابطه‌مند سازند. همچنین صدوقی، خوشگام و بهنام (۱۳۸۶)، در تحقیقی به بررسی وضعیت سطوح دسترسی و محرمانگی مدارک پزشکی در چهار کشور کانادا، استرالیا، آمریکا و انگلستان پرداخته‌اند و وضعیت این کشورها را با ایران مقایسه کرده‌اند. طبق نتایج تحقیق آنها، در ایران سازمان‌دهی منسجمی برای مدیریت محرمانگی اطلاعات پزشکی وجود ندارد و وضعیت محرمانگی اطلاعات پزشکی در ایران با استانداردهای جهانی فاصله زیادی دارد. برخی تحقیقات داخلی نیز با تکیه بر «قانون مجازات اسلامی» در باب ضرورت حفظ اسرار بیمار، به بررسی رازداری و حدود آن در حرفه پزشکی پرداخته‌اند. در ایران براساس قانون مجازات عمومی، مصوب ۱۳۰۴، افشای اسرار بیماران جرم شناخته شده و با تغییراتی که در طول سال‌ها داشته اصل مصوبه به حال خود باقی مانده و آخرین اصلاحیه در خرداد ۱۳۷۵ انجام شده است. براساس ماده (۶۴۸) قانون مجازات اسلامی، «اطباء و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل و حرفه خود

محرم اسرار می‌شوند، هرگاه در غیر موارد قانونی اسرار مردم را افشاء 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 می‌شوند» (جهانگیر، ۱۳۸۶: ۱۷۹).

مهدوی‌نژاد (۱۳۸۷) در پژوهشی چنین نتیجه‌گیری کرده است که پزشکان در ایران در مورد حفظ اسرار بیماران دچار شک و سرگردانی شده‌اند؛ آنها با دو حکم الزامی «وجوب» و «حرمت» مواجه‌اند: از یک سو با حرمت افشای اسرار بیمار، که قانون مجازات اسلامی نیز بر آن تأکید کرده است، و از سوی دیگر، با وجوب جلوگیری از مفاسد و حفظ منافع جامعه از طریق افشای اسرار بیمار. وی معتقد است با توجه به اینکه بین آن دو حکم «تزام» است، انجام هر دو مقدور نیست و مکلف وظیفه دارد هر کدام را که دارای مصلحت بیشتر و ملاکی قوی‌تر باشند مقدم دارد. در صورتی که قوت ملاک با دلیل عقلی یا شرعی، یا دلیل دیگری که از نگاه علمی دارای اعتبار است ثابت نشد، باید به مقتضای «اصل اولی» از افشای آن راز خودداری کند. در تحقیقی مشابه، جوادی‌پور، طبیبی جبلی و راعی (۱۳۸۹) به بررسی رازداری پزشکی در فقه و حقوق ایران پرداخته‌اند. ایشان معتقدند پزشکان، هم بنا به وظیفه اخلاقی و سوگندی که یاد کرده‌اند، و هم به استناد ماده (۶۴۸) قانون مجازات اسلامی، موظف به حفظ اسرار بیماران هستند. اما بنا به نتایج تحقیق آنها، ممکن است شرایطی پیش آید که پزشک ناگزیر به نقض رازداری شده، ولی باید از ناحیه این آشکارسازی کمترین ضرر متوجه بیمار شود. مصلحت عام (مواردی همچون: جلوگیری از شیوع بیماری مهلک در جامعه، پیشگیری از وقوع قتل یا ضرر به شخص ثالث و ...) و مصلحت خاص (مواردی همچون: ابراز رضایت بیمار نسبت به افشای رازش، دفاع پزشک از خود در دادگاه و ...) از موارد استثنایی هستند که در آنها ممکن است پزشک رازداری را نقض کند.

۳. روش تحقیق

این تحقیق از نظر روش‌شناسی جزء تحقیقات کیفی دسته‌بندی می‌شود. روش‌شناسی کیفی شامل روش‌های مطالعات اسنادی، تحلیل محتوا و مطالعات تطبیقی می‌شود. همچنین نظر به اینکه نتایج این تحقیق قابلیت کاربرد در قانونگذاری بخش عمومی در سطح ملی را داراست،

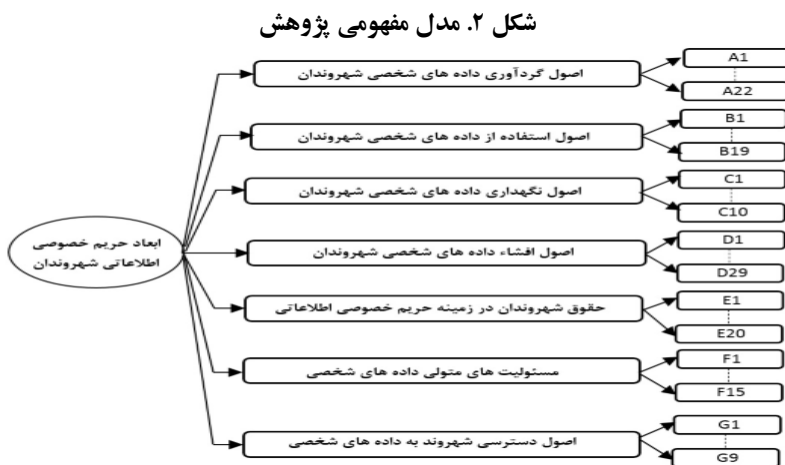
می‌توان گفت که این پژوهش از نظر هدف در حیطه پژوهش‌های کاربردی قرار دارد. همچنین پژوهش حاضر براساس ماهیت و روش گردآوری داده‌ها، یک پژوهش توصیفی محسوب می‌شود. در این پژوهش از روش‌های مطالعه کتابخانه‌ای و اسنادی برای گردآوری داده‌ها استفاده شده است؛ تحلیل داده‌ها به صورت دستی و نیز با استفاده از نرم‌افزارهایی همچون صفحه‌گسترده Excel 2013 انجام شده است. تحلیل داده‌های مطالعات اسنادی از طریق کدگذاری براساس محتوا و مطالعات تطبیقی صورت گرفته است. در تحلیل محتوای قوانین حفظ حریم خصوصی اطلاعاتی در کشورهای منتخب، ابتدا تمامی مفاد قوانین مورد کدگذاری باز قرار گرفتند، سپس با کدگذاری محوری هفت بعد به‌عنوان ابعاد مقایسه تطبیقی کشورها از حیث حفظ حریم خصوصی اطلاعاتی شناسایی شدند. در نهایت الزامات حریم خصوصی اطلاعاتی در کشورها، در هر یک از ابعاد به صورت تطبیقی مقایسه شدند. همچنین جامعه آماری این تحقیق شامل کشورهای دارای قانون حمایت از حریم خصوصی اطلاعاتی است که طبق آمار مؤسسه دی.ال.ای از ۱۹۶ کشور ۵۸ کشور دارای قوانین مرتبطی در این زمینه هستند. در مجموع ۶ کشور (کره جنوبی، فرانسه، انگلستان، کانادا، ایرلند و ایتالیا) 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 دی.ال.ای. بوده است.

۴. مدل مفهومی تحقیق

با توجه به اینکه تاکنون مدلی برای حریم خصوصی اطلاعاتی در ادبیات تحقیق مطرح نشده است، در این تحقیق برای مقایسه تطبیقی کشورهای منتخب با ایران از نظر حمایت از داده‌های شخصی^۱ شهروندان، پس از انجام کدگذاری باز، چارچوب مقایسه تطبیقی با

۱. داده‌های شخصی عبارت‌اند از هر نوع اطلاعاتی که به‌صورت مستقیم یا غیرمستقیم به یک شهروند قابل شناسایی ارتباط داشته باشد (Italian Personal Data Protection Code, 2003). و داده‌های شخصی حساس عبارت‌اند از: 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 (UK Data Protection Act, 1998).

استفاده از روش کدگذاری محوری طراحی شده است (شکل ۲). بر این اساس حفظ حریم خصوصی اطلاعاتی در هفت بعد مورد مقایسه قرار گرفته است: ۱. الزامات گردآوری داده‌های شخصی (اخذ داده از سوژه یا نهاد ثالث)؛ ۲. الزامات استفاده از داده‌های شخصی (به کارگیری داده‌های شخصی در فرایندهای سازمانی)؛ ۳. الزامات نگهداری داده‌های شخصی (هزینه ذخیره‌سازی داده در پایگاه‌های داده)؛ ۴. الزامات افشای داده‌های شخصی (انتقال داده‌ها به فرد یا نهاد ثالث)؛ ۵. حقوق سوژه^۱ در زمینه حریم خصوصی اطلاعاتی؛ ۶. مسئولیت‌های کنترل‌گر داده‌های شخصی؛ ۷. الزامات دسترسی سوژه به داده‌های شخصی.



۵. تجزیه و تحلیل داده‌ها

به‌رغم اینکه در کشورهای منتخب، قانونی جداگانه برای حفاظت از حریم خصوصی اطلاعاتی شهروندان وجود دارد، متأسفانه در ایران شاهد وجود چنین قانونی نیستیم. تنها قانونی که می‌تواند برای حفاظت از حریم خصوصی اطلاعاتی شهروندان در ایران مورد استناد قرار گیرد مواد (۵۸ تا ۶۱) قانون تجارت الکترونیک است و در این تحقیق مبنای

۱. سوژه: هر شهروند حقیقی که داده‌های شخصی به وی ارتباط پیدا می‌کند (Italian Personal Data Protection Code, 2003).

مقایسه تطبیقی با قوانین سایر کشورها قرار گرفته است. الزامات مربوط به هریک از ابعاد هفت گانه حفظ حریم خصوصی اطلاعاتی شهروندان به این شرح هستند: ۱. الزامات مربوط به گردآوری داده‌های شخصی شهروندان؛ ۲. الزامات مربوط به استفاده از داده‌های شخصی شهروندان؛ ۳. الزامات مربوط به نگهداری داده‌های شخصی شهروندان؛ ۴. الزامات مربوط به افشای داده‌های شخصی شهروندان؛ ۵. حقوق شهروند (سوژه) در زمینه حریم خصوصی اطلاعاتی؛ ۶. مسئولیت‌های متولی داده‌های شخصی (کنترل‌گر) در خصوص حفاظت از حریم خصوصی اطلاعاتی شهروندان؛ و ۷. الزامات دسترسی شهروندان (سوژه‌ها) به داده‌های شخصی.

۱-۵. الزامات مربوط به گردآوری داده‌های شخصی شهروندان

در جدول ۱ الزامات گردآوری داده‌های شخصی شهروندان در کشورهای منتخب و ایران با هم مقایسه شده است.

جدول ۱. الزامات مربوط به گردآوری داده‌های شخصی شهروندان

| ردیف | الزامات مربوط به گردآوری داده‌های شخصی شهروندان (کد) | فرانسه | کانادا | ایرلند | ایتالیا | ایران |
|------|---|--------|--------|--------|---------|-------|
| A1 | لزوم گردآوری داده‌های شخصی برای اهداف مشخص و قانونی | ✓ | ✓ | ✓ | ✓ | ✓ |
| A2 | لزوم ارائه اطلاعات کافی به سوژه‌ها در زمان گردآوری داده‌های شخصی از سوژه در صورت عدم وجود منع قانونی | ✓ | ✓ | ✓ | ✓ | - |
| A3 | لزوم ارائه اطلاعات کافی به سازمان افشاءکننده در زمان گردآوری داده‌های شخصی از منبعی غیر از سوژه در صورت عدم وجود منع قانونی | ✓ | ✓ | ✓ | ✓ | - |
| A4 | مجاز بودن گردآوری داده‌های شخصی از سوژه پس از جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A5 | لزوم گردآوری داده‌های شخصی تا حد کفایت برای اهداف اعلام شده | ✓ | ✓ | ✓ | ✓ | - |
| A6 | مجاز بودن گردآوری بدون جلب رضایت سوژه در صورت وجود الزام قانونی | ✓ | ✓ | ✓ | ✓ | - |
| A7 | مجاز بودن گردآوری بدون جلب رضایت سوژه در صورت ضروری بودن برای حفاظت از جان سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A8 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن برای مقاصد تحقیقاتی (علمی، آماری، تاریخی) یا شرط بیشتر بودن منافع عمومی از منافع خصوصی و ناشناخته مآخذ هویت سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A9 | غیرمجاز بودن گردآوری داده‌های شخصی حساس بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ |
| A10 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن گردآوری برای انجام وظایف قانونی متولی | ✓ | ✓ | ✓ | ✓ | - |
| A11 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت اجتناب‌ناپذیر بودن بنا به قرارداد متولی یا سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A12 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه در صورت ضروری بودن گردآوری برای حفاظت از اموال و دارایی‌های سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A13 | مجاز بودن گردآوری داده‌های شخصی سوژه که به حالت عمومی درآمده‌اند بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A14 | لزوم ارائه اطلاعات کافی به سوژه‌ها بلافاصله پس از گردآوری داده‌های شخصی از منبعی غیر از سوژه در صورت عدم وجود منع قانونی | ✓ | ✓ | ✓ | ✓ | - |
| A15 | مجاز بودن گردآوری داده‌های شخصی حساس بدون جلب رضایت سوژه در صورت وجود الزام قانونی برای گردآوری آنها | ✓ | ✓ | ✓ | ✓ | - |
| A16 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف اجرای احکام قضایی | ✓ | ✓ | ✓ | ✓ | - |
| A17 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف انجام وظایف در جهت منافع عمومی | ✓ | ✓ | ✓ | ✓ | - |
| A18 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای حفاظت از منافع مشروع متولی یا شرط پایمال نشدن منافع سوژه | ✓ | ✓ | ✓ | ✓ | - |
| A19 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه با هدف حفاظت از امنیت ملی | ✓ | ✓ | ✓ | ✓ | - |
| A20 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای پیگرد قضایی مجرمان | ✓ | ✓ | ✓ | ✓ | - |
| A21 | منوع بودن گمراه کردن سوژه‌ها در هنگام گردآوری داده‌های شخصی با روش‌های فریبنده | - | - | ✓ | ✓ | - |
| A22 | مجاز بودن گردآوری داده‌های شخصی بدون جلب رضایت سوژه برای تحقیق پیرامون نقض قانون | - | - | ✓ | ✓ | - |

با مقایسه الزامات مربوط به گردآوری داده‌های شخصی شهروندان در ایران و کشورهای منتخب چنین برمی‌آید که از ۱۹ الزامی که حداقل در ۴ کشور از ۶ کشور منتخب وجود دارند (مثل کدهای A1 تا A19)، ایران تنها در دو الزام با سایر کشورها مشترک است (کدهای A1 و A9). اولی «لزوم گردآوری داده‌های شخصی برای اهداف مشخص و قانونی» که در بند «الف» از ماده (۵۹) و دومی «غیرمجاز بودن گردآوری داده‌های شخصی حساس بدون جلب رضایت سوژه» که در ماده (۵۸) از فصل سوم قانون تجارت الکترونیک ایران آمده است. بنابراین چنین برداشت می‌شود که در ایران تنها از داده‌های شخصی حساس (عقیدتی، سیاسی، مذهبی، سلامت جسمی یا روانی و ...) حمایت به عمل آمده است و از داده‌های شخصی عام شهروندان حمایتی به عمل نمی‌آید. همچنین، متولی (کنترل‌گر^۱) برای گردآوری داده‌های شخصی مجبور به ارائه اطلاعات (مثلاً هویت متولی و راه‌های تماس با او، حقوقی که سوژه از آنها برخوردار است، مدت زمان نگهداری، امکان افشای داده‌های شخصی یا هویت دریافت کنندگان احتمالی و ...) به شهروندان نیست. اما در همه کشورهای منتخب، ارائه اطلاعات در موارد ذکر شده الزامی بوده و در صورت عدم ارائه اطلاعات، گردآوری غیرمجاز تلقی می‌شود. بنابراین، در بعد الزامات گردآوری داده‌های شخصی شهروندان، ایران فاصله زیادی با کشورهای منتخب دارد.

۲-۵. الزامات مربوط به استفاده از داده‌های شخصی شهروندان

در جدول ۲ الزامات استفاده از داده‌های شخصی شهروندان در کشورهای منتخب و ایران با هم مقایسه شده است.

طبق جدول ۲، ۱۴ الزام برای استفاده از داده‌های شخصی شهروندان در حداقل ۴ کشور از ۶ کشور منتخب وجود دارند (کدهای B1 تا B14). از این تعداد تنها دو الزام B5 (غیرمجاز بودن استفاده از داده‌های شخصی حساس بدون جلب رضایت سوژه) طبق ماده (۵۸) و B6 (لزوم سازگار بودن استفاده از داده‌های شخصی با اهداف اعلام شده به سوژه یا سازمان افشاء کننده در هنگام گردآوری) طبق بند «ب» از ماده (۵۹) قانون تجارت الکترونیک، میان

ایران و کشورهای منتخب مشترک است. بنابراین در ایران استفاده از داده‌های شخصی به صورت عام مورد حمایت قرار نگرفته است، بلکه تنها داده‌های شخصی حساس (عقیدتی، سیاسی، مذهبی، سلامت جسمی یا روانی و ...) مورد حمایت قانونگذار قرار گرفته‌اند. سکوت قانونگذار در سایر موارد امکان نقض حریم خصوصی اطلاعاتی شهروندان را بالا برده است. در کشورهای منتخب، استفاده از داده‌های شخصی در صورتی که گردآوری آنها غیرمجاز بوده باشد یا رضایت سوژه در هنگام گردآوری جلب نشده باشد، غیرمجاز تلقی می‌شود. البته در صورتی که هدف استفاده، حفاظت از جان یا مال سوژه بوده باشد استفاده بدون رضایت مجاز شمرده شده است. همچنین در تمامی کشورها به جز فرانسه، متولی (کنترلگر) ملزم است در صورت موجه بودن درخواست سوژه برای تعلیق استفاده از داده‌های شخصی اش، استفاده از آنها را به حالت تعلیق درآورد. استفاده از داده‌های شخصی برای مقاصد تحقیقاتی (علمی، آماری یا تاریخی) فراتر از اهداف اعلام شده، تنها با شرط بیشتر بودن منافع عمومی از منافع خصوصی سوژه و ناشناس ماندن هویت سوژه مجاز شمرده شده است. با توجه به جدول ۲ به نظر می‌رسد وضعیت حفاظت از حریم خصوصی اطلاعاتی شهروندان در ایران از بعد استفاده از داده‌های شخصی شهروندان با کشورهای منتخب فاصله زیادی دارد.

جدول ۲. الزامات مربوط به استفاده از داده‌های شخصی شهروندان

| ردیف | الزامات مربوط به استفاده از داده‌های شخصی شهروندان (کد B) | ترکیبی | فرانسه | انگلس | کانادا | ایرلند | ایتالیا | ایران |
|------|---|--------|--------|-------|--------|--------|---------|-------|
| B1 | غیرمجاز بودن استفاده از داده‌های شخصی در صورت غیرمجاز شمرده شدن گردآوری آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B2 | مجاز بودن استفاده از داده‌های شخصی پس از جلب رضایت سوژه در صورت گردآوری از سازمان ثالث | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B3 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن استفاده از آنها برای حفاظت از جان سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B4 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن استفاده از آنها برای حفاظت از اموال سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B5 | غیرمجاز بودن استفاده از داده‌های شخصی حساس بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| B6 | لزوم سازگاری بودن استفاده از داده‌های شخصی با اهداف اعلام شده به سوژه یا سازمان افشاکننده در هنگام گردآوری | ✓ | ✓ | - | ✓ | ✓ | ✓ | ✓ |
| B7 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن استفاده از آنها به نفع قرارداد یا سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B8 | لزوم تعلیق استفاده از داده‌های شخصی در صورت موجه بودن درخواست سوژه و ممکن بودن انجام وظایف متولی پس از تعلیق | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B9 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن داده‌های شخصی برای انجام تحقیقات (علمی، آماری، تاریخی) بشرط بیشتر بودن منافع عمومی از منافع خصوصی و ناشناس ماندن هویت سوژه | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| B10 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده هنگام گردآوری در صورت وجود الزام قانونی | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| B11 | لزوم استفاده از داده‌های شخصی به صورت متناسب (در صورتی که اهداف استفاده به سوژه یا سازمان افشاکننده اعلام شده باشد) | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B12 | لزوم استفاده از داده‌های شخصی به صورت قانونی (متناسب بودن استفاده از داده‌های شخصی با وظایف قانونی متولی) | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B13 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن داده‌ها برای حفاظت از امنیت ملی | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B14 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن داده‌های شخصی برای دعای حقوقی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B15 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای حفاظت از منافع مشروع متولی بشرط پامال شدن منافع سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B16 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده در صورت ضروری بودن استفاده برای انجام وظایف قانونی متولی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B17 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده با هدف انجام وظایف در جهت منافع عمومی | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B18 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای پیگرد قانونی مجرمان | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| B19 | مجاز بودن استفاده از داده‌های شخصی فراتر از اهداف اعلام شده برای انجام تحقیقات جنایی | - | ✓ | ✓ | ✓ | ✓ | ✓ | - |

۳-۵. الزامات مربوط به نگهداری داده‌های شخصی شهروندان

در جدول ۳ الزامات مربوط به نگهداری داده‌های شخصی شهروندان در کشورهای منتخب و ایران باهم مقایسه شده است.

جدول ۳. الزامات مربوط به نگهداری داده‌های شخصی شهروندان

| ردیف | الزامات مربوط به نگهداری داده‌های شخصی شهروندان (کد) | کره جنوبی | فرانسه | انگلستان | کانادا | ایرلند | ایتالیا | ایران |
|------|--|-----------|--------|----------|--------|--------|---------|-------|
| C1 | غیرمجاز بودن نگهداری داده‌های شخصی در صورت غیرمجاز شمرده شدن گردآوری آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| C2 | لزوم اطمینان از صحت داده‌ها پیش از اقدام به نگهداری آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| C3 | مجاز بودن نگهداری داده‌های شخصی تا زمان مورد نیاز جهت رسیدن به اهداف اولیه گردآوری | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| C4 | لزوم به‌روزرسانی داده‌های شخصی در هنگام ضرورت | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| C5 | لزوم نابودسازی داده‌های شخصی در صورت منقضی شدن زمان نگهداری آنها | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| C6 | لزوم نابودسازی داده‌های شخصی در صورت تقاضای سوژه مبنی بر حذف آنها و ناتوانی متولی در اثبات مشروعیت نگهداری آنها | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| C7 | مجاز بودن نگهداری داده‌های شخصی بیش از زمان مورد نیاز جهت رسیدن به اهداف اولیه گردآوری برای مقاصد تحقیقاتی (علمی، آماری، تاریخی) با شرط بیشتر بودن منافع عمومی از منافع خصوصی و ناشناخته شدن هویت سوژه | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| C8 | مجاز بودن نگهداری داده‌های شخصی بیش از زمان مورد نیاز جهت رسیدن به اهداف گردآوری در صورت وجود الزام قانونی | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| C9 | لزوم اطمینان از کامل بودن داده‌های شخصی در جهت اهداف اولیه گردآوری پیش از اقدام به نگهداری آنها | ✓ | ✓ | - | ✓ | ✓ | ✓ | - |
| C10 | لزوم حذف داده‌های شخصی غیردقیق (ناقص یا غیرصحيح) در صورت عدم امکان اصلاح | - | ✓ | - | - | - | - | - |

طبق جدول ۳، ۹ الزام (C1 تا C9) در حداقل ۴ کشور از ۶ کشور مطرح شده‌اند. از این تعداد ایران تنها یک الزام را با کشورهای منتخب اشتراک دارد (کد C4) که طبق بند «ج» از ماده (۵۹) قانون تجارت الکترونیک، بر لزوم به‌روزرسانی داده‌های شخصی در هنگام ضرورت تأکید کرده است. در کشورهای منتخب نگهداری داده‌های شخصی که گردآوری آنها غیرمجاز بوده باشد، غیرمجاز بوده و متولی باید برای جلوگیری از ضایع شدن حق شهروندان قبل از اقدام به نگهداری داده‌های شخصی، از صحت داده‌ها اطمینان حاصل کند. همچنین طبق اصل کفایت زمانی نگهداری، نگهداری داده‌های شخصی تا حدی مجاز است که متولی به اهداف اولیه گردآوری برسد. در تمامی کشورهای منتخب جز انگلستان، متولی در دو صورت باید داده‌های شخصی شهروندان را نابود کند (منظور از نابودسازی حذف آنها بدون قابلیت بازیابی داده‌هاست): ۱. منقضی شدن زمان نگهداری داده‌ها؛ و ۲. تقاضای سوژه مبنی بر حذف آنها و ناتوانی متولی در اثبات مشروعیت نگهداری آنها. در اکثر کشورهای منتخب، نگهداری داده‌های شخصی برای مقاصد تحقیقاتی (علمی، آماری یا تاریخی) فراتر از اهداف اعلام شده، تنها با شرط بیشتر بودن منافع عمومی از منافع خصوصی سوژه و

ناشناس ماندن هویت سوژه مجاز شمرده شده است. همچنین در صورتی که الزام قانونی برای نگهداری داده‌های شخصی وجود داشته باشد، متولی مجاز به نگهداری داده‌های شخصی بیش از مدت زمان لازم برای رسیدن به اهداف اولیه گردآوری است. با توجه به جدول ۳ نیز به نظر می‌رسد وضعیت حفاظت از حریم خصوصی اطلاعاتی شهروندان در ایران از بعد نگهداری داده‌های شخصی شهروندان با کشورهای منتخب فاصله زیادی دارد.

۴-۵. الزامات مربوط به افشای داده‌های شخصی شهروندان

در جدول ۴ الزامات مربوط به افشای داده‌های شخصی شهروندان در کشورهای منتخب و ایران با هم مقایسه شده است.

براساس جدول ۴، از بین ۱۷ الزام از ۲۹ الزام (کدهای D1 تا D17) در حداقل ۴ کشور از ۶ کشور منتخب برای افشای داده‌های شخصی شهروندان ذکر شده‌اند. از بین آنها تنها یک الزام (D4)، در ایران وجود دارد که طبق ماده (۵۸) قانون تجارت الکترونیک، به غیرمجاز بودن افشای داده‌های شخصی حساس بدون جلب رضایت شهروند (سوژه) پرداخته است. در تمامی کشورهای منتخب در صورتی که افشاء قبلاً جزء اهداف اعلام شده به سوژه نبوده باشد، غیرمجاز تلقی می‌شود، مگر در صورتی که رضایت سوژه جلب شده باشد یا اینکه افشاء به نهادهای قضایی و با هدف پیشبرد پرونده‌های قضایی صورت گرفته باشد. علاوه‌براین موارد، استثنائاتی همچون حفاظت از جان یا اموال سوژه، ضرورت افشاء برای انجام وظایف متولی یا سازمان دریافت‌کننده، حفاظت از امنیت ملی، مقاصد درمانی و موارد این‌چنینی برای افشاء فراتر از اهداف گردآوری در اغلب کشورهای منتخب ذکر شده است. همچنین در کشورهای انگلستان، ایرلند و ایتالیا محدودیت‌هایی برای انتقال داده‌های شخصی به کشورهای خارجی مطرح شده است؛ به این صورت که افشا تنها با حصول اطمینان از وجود امنیت اطلاعات کافی در آن کشورها برای حفاظت از داده‌های شخصی شهروندان مجاز است. البته استثنائاتی همچون اعلام رضایت سوژه، مسائل مرتبط با امنیت ملی، حفاظت از جان یا مال سوژه، یا لزوم انتقال بین‌المللی داده‌های شخصی بنا به قرارداد منعقد شده با سوژه در کشورهای ایتالیا و ایرلند برای انتقال داده‌های شخصی به کشورهای دارای سطوح ناکافی

امنیت اطلاعات مطرح شده‌اند. حتی با در نظر گرفتن برخی اختلافات میان کشورهای منتخب چنین برداشت می‌شود که در ایران وضعیت حفاظت از داده‌های شخصی شهروندان از بعد افشاء، وضعیت قابل قبولی نداشته و از کشورهای منتخب فاصله زیادی دارد.

جدول ۴. الزامات مربوط به افشای داده‌های شخصی شهروندان

| ردیف | الزامات مربوط به افشای داده‌های شخصی شهروندان (کد D) | آسیب | تعمیر | تعمیر | تعمیر | تعمیر | تعمیر | تعمیر |
|------|---|------|-------|-------|-------|-------|-------|-------|
| D1 | غیرمجاز بودن افشای داده‌های شخصی در صورتی که افشای جزء اهداف اعلام‌شده در هنگام گردآوری نبوده باشد | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D2 | غیرمجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D3 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن افشای برای پیشبرد پرونده‌های قضایی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D4 | غیرمجاز بودن افشای داده‌های شخصی حساس بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D5 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن برای وظایف قانونی متولی (با درنظرگرفتن) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D6 | لزوم ارائه اطلاعات کافی به سوژه‌ها پیش از افشای داده‌های شخصی در صورت عدم وجود منع قانونی برای اطلاع رسانی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D7 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت وجود الزام قانونی برای افشای آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D8 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن افشای برای حفاظت از جان سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D9 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن افشای برای مقاصد تحقیقاتی (علمی، آماری، تاریخی) با شرط پیش‌بینی منافع عمومی از منافع خصوصی و نشان‌دهنده مآخذ هویت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D10 | مجاز بودن افشای داده‌های شخصی بدون جلب رضایت سوژه در صورت اجتناب‌ناپذیری بودن افشای بنابه قرارداد میان متولی و سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D11 | لزوم درخواست از دریافت‌کنندگان داده‌های شخصی برای تعلیق استفاده از داده‌های شخصی و لزوم تعلیق استفاده از آنها توسط دریافت‌کنندگان طبق درخواست متولی در صورت افشای قبلی و موجود بودن درخواست سوژه برای تعلیق استفاده | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D12 | غیرمجاز بودن افشای داده‌های شخصی در صورت منقشی شدن زمان نگهداری آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D13 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن افشای برای حفاظت از اموال سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D14 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده در صورت ضروری بودن افشای برای انجام تحقیقات مربوطه جرایم | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D15 | مجاز بودن افشای داده‌های شخصی حساس در صورت وجود الزام قانونی برای افشای آنها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D16 | مجاز بودن افشای داده‌های شخصی حساس به نهادهای پزشکی حرفه‌ای برای مقاصد درمانی (همچون: تحقیقات پزشکی) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D17 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده برای حفاظت از امنیت ملی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D18 | لزوم درخواست از دریافت‌کنندگان داده‌های شخصی برای اصلاح داده‌های شخصی و لزوم اصلاح آنها توسط دریافت‌کنندگان | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D19 | طبق درخواست متولی در صورت افشای قبلی و آگاهی متولی از عدم صحت، ناقص بودن یا به‌روزرسانی داده‌ها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D20 | لزوم درخواست از دریافت‌کنندگان داده‌های شخصی برای حذف داده‌های شخصی و لزوم حذف آنها توسط دریافت‌کنندگان | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D21 | طبق درخواست متولی در صورت افشای قبلی و موجه بودن درخواست سوژه برای حذف داده‌های شخصی وی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D22 | غیرمجاز بودن انتقال داده‌های شخصی به کشورهای خارجی در صورت عدم وجود سطوح کافی امنیت اطلاعات در آن کشورها | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D23 | مجاز بودن افشای داده‌های شخصی فراتر از اهداف اعلام‌شده با هدف انجام وظایف‌های درجهت منافع عمومی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D24 | مجاز بودن افشای داده‌های شخصی بدون جلب رضایت سوژه با هدف نادر ساختن سازمان دریافت‌کننده به حفاظت از منافع مشروع متولی یا شرط پایداری نهادن منافع سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D25 | مجاز بودن انتقال داده‌های شخصی به کشورهای خارجی دارای سطح پایین امنیت در صورت اعلام رضایت سوژه برای انتقال | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D26 | مجاز بودن انتقال داده‌های شخصی به کشورهای خارجی دارای سطح پایین امنیت برای پیشبرد پرونده‌های قضایی | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D27 | مجاز بودن انتقال داده‌های شخصی به کشورهای خارجی دارای سطح پایین امنیت برای انجام قرارداد با سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D28 | لزوم رمزنگاری داده‌های شخصی با استفاده از جدیدترین روش‌های رمزنگاری هنگام انتقال داده‌ها به سازمان ثالث | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D29 | مجاز بودن افشای داده‌های شخصی سوژه که توسط سوژه به حالت عمومی درآمده‌اند بدون جلب رضایت سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| D29 | لزوم گزارش هرگونه افشای داده‌های شخصی به سازمان دیدبان حریم خصوصی شهروندان | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

۵-۵. حقوق شهروند در زمینه حریم خصوصی اطلاعاتی

در جدول ۵ حقوق شهروند در زمینه حریم خصوصی اطلاعاتی در کشورهای منتخب و ایران با هم مقایسه شده است. طبق جدول ۵ از میان ۱۱ حقی که در حداقل ۴ کشور از ۶ کشور به‌عنوان حقوقی که شهروند در زمینه حریم خصوصی اطلاعاتی خود از آنها برخوردار است (کدهای E1 تا E11)، در ایران تنها ۵ حق به شهروند داده شده است:

۱. کد E3: حق اعلام رضایت نسبت به پردازش داده‌های شخصی حساس (طبق ماده (۵۸) قانون تجارت الکترونیک)؛ ۲. کد E6: حق آگاهی از اهداف گردآوری داده‌های شخصی توسط یک سازمان (طبق بند «الف» ماده (۵۹) قانون تجارت الکترونیک)؛ ۳. کد E7: حق دسترسی به داده‌های شخصی (طبق بند «د» ماده (۵۹) قانون تجارت الکترونیک)؛ ۴. کد E8: حق اصلاح داده‌های شخصی (طبق بند «د» ماده (۵۹) قانون تجارت الکترونیک)؛ ۵. حق درخواست حذف داده‌های شخصی (طبق بند «ه» ماده (۵۹) قانون تجارت الکترونیک)؛ اما برای شهروندان هیچ‌گونه حقی در خصوص آگاهی از وجود (یا عدم وجود) داده‌های شخصی نزد یک سازمان، اعلام رضایت یا عدم رضایت برای پردازش داده‌های شخصی به صورت عام، آگاهی از افشای داده‌های شخصی به نهاد ثالث در گذشته یا احتمال افشا در آینده، آگاهی از هویت متولی داده‌های شخصی (کنترل‌گر) و راه‌های تماس با وی یا درخواست تعلیق استفاده از داده‌های شخص، در نظر گرفته نشده است. با توجه به اینکه در ایران حقوق شهروندان در زمینه حریم خصوصی اطلاعاتی تنها مختص به داده‌های شخصی حساس است نه داده‌های شخصی به صورت عام، بنابراین در مقایسه با کشورهای پیشرو، نمی‌توان قوانین ایران در این زمینه را حامی حریم خصوصی اطلاعاتی شهروندان دانست.

جدول ۵. حقوق شهروند (سوژه) در زمینه حریم خصوصی اطلاعاتی

| ردیف | حقوق شهروند در زمینه‌ی حریم خصوصی اطلاعاتی (کد E) | گروه ۱ | فرانسه | انگلیس | آلمان | ایران |
|------|--|--------|--------|--------|-------|-------|
| E1 | حق آگاهی از وجود (یا عدم وجود) داده‌های شخصی نزد یک سازمان | ✓ | ✓ | ✓ | ✓ | - |
| E2 | حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های شخصی | ✓ | ✓ | ✓ | ✓ | ✓ |
| E3 | حق اعلام رضایت یا عدم رضایت برای پردازش داده‌های شخصی حساس | ✓ | ✓ | ✓ | ✓ | ✓ |
| E4 | حق آگاهی از افشای داده‌های شخصی به نهاد ثالث در گذشته یا احتمال افشای آینده | ✓ | ✓ | ✓ | ✓ | - |
| E5 | حق آگاهی از هویت متولی داده‌های شخصی (کنترل‌گر) و راه‌های تماس با وی | ✓ | ✓ | ✓ | ✓ | - |
| E6 | حق آگاهی از اهداف گردآوری داده‌های شخصی توسط یک سازمان | ✓ | ✓ | ✓ | ✓ | ✓ |
| E7 | حق دسترسی به داده‌های شخصی | ✓ | ✓ | ✓ | ✓ | ✓ |
| E8 | حق اصلاح داده‌های شخصی غیر دقیق (غیر صحیح یا ناقص) | ✓ | ✓ | ✓ | ✓ | ✓ |
| E9 | حق حذف داده‌های شخصی در صورت داشتن توجیه مشروع مبنی بر غیرمجاز بودن گردآوری آنها توسط کنترل‌گر | ✓ | ✓ | ✓ | ✓ | ✓ |
| E10 | حق درخواست تعلیق استفاده از داده‌های شخصی در صورت داشتن توجیه قانونی مبنی بر ضرر داشتن استفاده برای سوژه یا ایجاد نراحتی برای سایرین | - | ✓ | ✓ | ✓ | - |
| E11 | حق آگاهی از منطبق تصمیم‌گیری مبتنی بر پردازش تمام‌خودکار داده‌ها | - | ✓ | ✓ | ✓ | - |
| E12 | حق آگاهی از منبع گردآوری داده‌ها | - | ✓ | ✓ | ✓ | - |
| E13 | حق آگاهی از پیامدهای اعلام عدم رضایت نسبت به پردازش داده‌های شخصی | - | ✓ | ✓ | ✓ | - |
| E14 | حق پیگرد قانونی هرگونه خسارت ناشی از پردازش داده‌های شخصی در فرآیندی منصفانه (حق دادخواهی) | - | ✓ | ✓ | ✓ | - |
| E15 | حق منع استفاده از داده‌های شخصی برای فعالیت‌های بازاریابی مستقیم | - | ✓ | ✓ | ✓ | - |
| E16 | حق آگاهی از حقوقی که سوژه در زمینه‌ی حریم خصوصی اطلاعاتی از آنها برخوردار است | - | ✓ | ✓ | ✓ | - |
| E17 | حق آگاهی از هویت متولی داده‌های شخصی و راه‌های تماس با وی | - | ✓ | ✓ | ✓ | - |
| E18 | حق پیگرد قانونی عدم پاسخگویی متولی به درخواست‌های سوژه در برخورداری از حقوق حریم خصوصی اطلاعاتی خود | - | ✓ | ✓ | ✓ | - |
| E19 | حق تقاضای پردازش غیرخودکار توسط انسان داده‌های شخصی در صورت قرارگیری در معرض تصمیم‌گیری مبتنی بر پردازش تمام‌خودکار داده‌های شخصی | - | ✓ | ✓ | ✓ | - |
| E20 | حق آگاهی از مدت زمان نگهداری داده‌های شخصی توسط متولی | ✓ | - | - | - | - |

۵-۶. مسئولیت‌های متولی داده‌های شخصی (کنترلگر)

در جدول ۶ مسئولیت‌های متولی داده‌های شخصی (کنترلگر) در خصوص حفاظت از حریم خصوصی اطلاعاتی شهروندان در کشورهای منتخب و ایران با هم مقایسه شده است. همان‌طوری که در جدول ۶ نیز آمده، در قوانین ایران هیچ‌گونه مسئولیتی برای حفاظت از حریم خصوصی اطلاعاتی شهروندان برای متولیان داده‌های شخصی (کنترلگرها) مشخص نشده است. از بین ۱۴ مسئولیتی که در کشورهای منتخب برای کنترلگرها مشخص شده است، ۷ مورد (کدهای F1 تا F7) در حداقل ۴ کشور به صورت مشترک تکرار شده است. کنترلگرها برای حفاظت از حریم خصوصی اطلاعاتی شهروندان باید تمهیدات امنیتی سازمانی (مدیریتی)، تمهیدات امنیتی فنی (نرم‌افزاری) و تمهیدات امنیتی فیزیکی (سخت‌افزاری) را جهت حفاظت از داده‌های شخصی در مقابل دسترسی غیرمجاز، نشر پیدا کردن، نابودی، مورد سرقت واقع شدن و ... تدارک بینند. همچنین پاسخگویی به همه درخواست‌های سوژه برای برخورداری از حقوق خود و شفافیت در صورت رد درخواست‌ها با ارائه توجیحات قانونی کافی از دیگر وظایف کنترلگرهاست. علاوه بر این موارد، برون‌سپاری عملیات پردازش داده‌های شخصی در قوانین اغلب کشورهای منتخب پیش‌بینی شده است، به نحوی که کنترلگر در صورت تصمیم به برون‌سپاری عملیات پردازش داده‌های شخصی ملزم به عقد قرارداد مکتوب با پردازشگر^۱ (پیمان‌کار) و تدوین نیازمندی‌های امنیتی (فنی، سازمانی و فیزیکی) برای حفاظت از امنیت داده‌های شخصی و نظارت منظم بر اجرای دستورالعمل‌های تعیین شده در قرارداد با پردازشگر شده است. همچنین متولی باید تمهیداتی را برای حفاظت از داده‌های شخصی براساس سطح حساسیت آنها در نظر گیرد. بر این اساس کشورهای منتخب از تصویب قوانینی برای برخورداری شهروندان از حقوق خود در زمینه حریم خصوصی اطلاعاتی فراتر رفته و برای کنترلگرها نیز مسئولیت‌هایی در نظر گرفته‌اند.

۱. پردازشگر: هر فرد یا نهادی که به جای کنترلگر (متولی) اقدام به پردازش داده‌های شخصی می‌کند (Korean

جدول ۶. مسئولیت‌های کنترل‌گر در خصوص حفاظت از حریم خصوصی اطلاعاتی شهروندان

| ردیف | الزامات مربوط به مسئولیت‌های کنترل‌گر داده‌های شخصی (کد F) | | | | | | |
|------|--|---------|--------|--------|---------|--------|---|
| | ایران | ایتالیا | ایرلند | کانادا | نگلستان | فرانسه | |
| F1 | - | ✓ | ✓ | ✓ | ✓ | ✓ | تدارک تمهیدات امنیتی سازمانی (مدیریتی) جهت حفاظت از داده‌های شخصی (در مقابل دسترسی غیرمجاز، نشر پیدا کردن، نفوذی، مورد سرقت واقع شدن و...) |
| F2 | - | ✓ | ✓ | ✓ | ✓ | ✓ | تدارک تمهیدات امنیتی فنی (رم‌افزایی) جهت حفاظت از داده‌های شخصی (در مقابل دسترسی غیرمجاز، نشر پیدا کردن، نفوذی، مورد سرقت واقع شدن و...) |
| F3 | - | ✓ | ✓ | ✓ | ✓ | ✓ | پاسخگویی به تمامی درخواست‌های سوژه برای برخورداری از حقوق خود |
| F4 | - | ✓ | ✓ | ✓ | ✓ | ✓ | شفافیت در صورت رد درخواست‌های سوژه با ارائه توضیحات قانونی کافی به وی |
| F5 | - | ✓ | ✓ | - | ✓ | ✓ | ازوم عقد قرارداد مکتوب با پردازشگر (پیمانکار) و تدوین نیازمندی‌های امنیتی (فنی، سازمانی و فیزیکی) برای حفاظت از امنیت داده‌های شخصی و نظارت منظم بر اجرای دستورالعمل‌های تعیین شده در قرارداد |
| F6 | - | ✓ | ✓ | ✓ | - | ✓ | تدارک تمهیدات امنیتی فیزیکی (سخت‌افزاری) جهت حفاظت از داده‌های شخصی (در مقابل دسترسی غیرمجاز، نشر پیدا کردن، نفوذی، مورد سرقت واقع شدن و...) |
| F7 | - | - | ✓ | ✓ | ✓ | ✓ | ازوم حفاظت از امنیت داده‌های شخصی بر اساس سطح حساسیت آنها و تخمین ریسک‌های ناشی از آنها |
| F8 | - | ✓ | - | ✓ | - | ✓ | چیران خسارت‌های ناشی از نقض حریم خصوصی اطلاعاتی در صورت مقصودن طبق تشخیص نهاد دیدبان حریم خصوصی |
| P9 | - | ✓ | - | ✓ | - | ✓ | نصب مأمور حفظ حریم خصوصی اطلاعاتی ^۱ با دانش تخصصی کافی در حریم خصوصی اطلاعاتی و پشتیبانی از وی در انجام وظایفش |
| F10 | - | ✓ | - | ✓ | - | ✓ | تدوین و انتشار آئین سیاست حریم خصوصی ^۲ |
| F11 | - | ✓ | ✓ | ✓ | - | - | ازوم آگاسازی کارکنان در خصوص اهمیت حفظ محرمانگی داده‌های شخصی |
| F12 | - | ✓ | - | - | - | - | تدوین و در دسترس قراردادن سند امنیتی برای کارکنان |
| F13 | - | ✓ | - | - | ✓ | - | ازوم انتخاب شایسته‌ترین پردازشگر از نظر تجربه و قابلیت اعتماد در صورت تصمیم به برون‌سپاری عملیات پردازش داده‌ها |
| F14 | - | ✓ | - | - | - | - | تعریف حوزه دسترسی کارکنان به داده‌های شخصی و به‌روزرسانی منظم آن |
| F15 | - | ✓ | - | - | - | - | استقرار سیستم اجراز هویت نرم‌افزاری برای کنترل دسترسی کارکنان به داده‌های شخصی |

۷-۵. الزامات دسترسی شهروند (سوژه) به داده‌های شخصی

در جدول ۷ الزامات دسترسی شهروندان (سوژه‌ها) به داده‌های شخصی در کشورهای منتخب و ایران با هم مقایسه شده است. بر اساس جدول ۷، از بین ۸ الزام مطرح شده برای دسترسی شهروندان به داده‌های شخصی، شش الزام در حداقل ۴ کشور از ۶ کشور منتخب تکرار شده است (کدهای G1 تا G7). ایران در کدهای G1 و G5 با کشورهای منتخب مشترک است. بنابراین شهروند در ایران، طبق بند «د» ماده (۵۹) قانون تجارت الکترونیک، در صورت تقاضا، باید بتواند به داده‌های شخصی خود که در اختیار کنترل‌گر است دسترسی داشته باشد و آنها را اصلاح کند. اما در صورت درخواست دسترسی شهروند، کنترل‌گر ملزم به فراهم کردن دسترسی شهروند به تمامی داده‌های شخصی وی که در اختیار کنترل‌گر هستند (همچون داده‌های ناشی از پردازش یا نتایج پردازش داده‌های شخصی)، نشده است. همچنین در کشورهای منتخب کنترل‌گرها ملزم به ارائه اطلاعات تکمیلی (همچون اهداف نگهداری داده‌های شخصی، افشا در گذشته یا احتمال افشا در آینده و...) به شهروندان در هنگام

دسترسی آنها به داده‌های شخصی وی هستند. علاوه بر این، کنترل‌گرها برای فراهم کردن دسترسی شهروندان به داده‌های شخصی خود، ملزم به استفاده از روش‌هایی شده‌اند که ایمن بوده و امکان نقض حریم خصوصی اطلاعاتی آنها و دسترسی غیرمجاز اشخاص ثالث را حداقل کند. ممنوع بودن دریافت وجه از شهروندان در ازای فراهم کردن دسترسی آنان به داده‌های شخصی شان و نیز مجاز بودن رد درخواست دسترسی آنها بنا به مسائل امنیت ملی در اغلب کشورهای منتخب مطرح شده است. با توجه به الزامات پیش گفته، به نظر می‌رسد دسترسی به داده‌های شخصی توسط شهروندان در ایران با کشورهای منتخب فاصله داشته و از شفافیت کافی برخوردار نیست.

جدول ۷. الزامات دسترسی شهروندان (سوژه‌ها) به داده‌های شخصی

| ردیف | الزامات مربوط به دسترسی شهروند به داده‌های شخصی (کد G) | اردن | فرانسه | کانادا | ایرلند | ایتالیا | ایران |
|------|---|------|--------|--------|--------|---------|-------|
| G1 | لزوم فراهم کردن امکان دسترسی-سوژه به داده‌های شخصی خود توسط کنترل‌گر در صورت درخواست سوژه | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| G2 | لزوم ارائه تملی داده‌های مربوط به شهروند به او در صورت مجاز بودن درخواست دسترسی به داده‌های شخصی (مجموعه تملی داده‌های ایجاد شده پس از پردازش داده‌های شخصی وی) | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| G3 | لزوم ارائه اطلاعات کلی به سوژه هنگام فراهم کردن دسترسی وی به داده‌های شخصی در صورت نداشتن منع قانونی برای اطلاع‌رسانی | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| G4 | لزوم استفاده از روش‌های ایمن برای فراهم کردن دسترسی سوژه به داده‌های شخصی | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| G5 | لزوم فراهم کردن امکان دسترسی سوژه به داده‌های شخصی با قابلیت ویرایش و ذخیره‌سازی در صورت درخواست سوژه برای اصلاح | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| G6 | ممنوعیت دریافت وجه از سوژه بابت فراهم کردن دسترسی سوژه به داده‌های شخصی خود | ✓ | - | ✓ | ✓ | - | - |
| G7 | مجاز بودن رد درخواست سوژه برای دسترسی به داده‌های شخصی خود در مسائل مرتبط با امنیت ملی | - | ✓ | - | ✓ | ✓ | - |
| G8 | لزوم ارائه داده‌های شخصی در قالبی قابل درک و بدون نیاز به نرم‌افزار غیرمعمول در صورت قبول درخواست سوژه برای دسترسی به داده‌های شخصی خود | - | ✓ | - | ✓ | - | - |
| G9 | مجاز بودن رد درخواست سوژه برای دسترسی به داده‌های شخصی خود در صورت وجود منع قانونی | ✓ | - | - | ✓ | ✓ | - |

۶. جمع‌بندی، نتیجه‌گیری و پیشنهادها

به‌طور خلاصه می‌توان چنین نتیجه‌گیری کرد که ایران از نظر حفاظت از حریم خصوصی اطلاعاتی شهروندان فاصله زیادی با کشورهای منتخب و پیش‌تاز دارد. طبق تحقیق حاضر وجود دو عامل اصلی باعث به‌وجود آمدن فاصله با استاندارد جهانی در این زمینه شده‌اند: ۱. شکاف قانونی؛ ۲. شکاف نظارتی. در مورد شکاف قانونی باید گفت که در ایران، برخلاف کشورهای مورد مطالعه، اولاً قانون مستقل و جامعی برای حفاظت از حریم خصوصی اطلاعاتی شهروندان وجود نداشته و قوانین قابل استناد موجود بسیار محدودند.

در همه کشورهای منتخب، قانونی مستقل با عنوان «قانون حمایت از داده» یا «قانون صیانت از حریم خصوصی اطلاعاتی» وجود دارد که الزامات حفظ حریم خصوصی اطلاعاتی شهروندان آن کشورها را برای سازمان‌های مختلف مشخص کرده است. از میان ۱۲۴ الزامی که در کشورهای منتخب برای حفاظت از حریم خصوصی اطلاعاتی شناسایی شده است، ۸۱ الزام در بیش از ۴ کشور تکرار شده‌اند؛ اما از این تعداد تنها ۱۳ مورد در قوانین ایران وجود دارد. ثانیاً، قوانین محدود موجود، تنها از داده‌های شخصی حساس (عقیدتی، سیاسی، پزشکی و ...) حمایت به عمل آورده‌اند و برخلاف کشورهای منتخب داده‌های شخصی عام را مورد حمایت قرار نداده‌اند. از آنجا که حساس بودن داده‌های شخصی ادراکی بوده و ممکن است برای شهروندی داده‌های پزشکی حساس تلقی شود و برای شهروندی دیگر داده‌های سابقه تحصیلی حساس شناخته شود، بنابراین نامیدن برخی داده‌های شخصی به عنوان حساس و حمایت صرف از آنها نمی‌تواند حریم خصوصی اطلاعاتی را به‌طور کامل مورد صیانت قرار دهد. به عنوان شاهدی دیگر، در دولت الکترونیک، بنا به ماهیت آن که داده‌های شخصی شهروندان برای ارائه خدمات باید از نهادهای مختلفی گردآوری یا به اصطلاح از پایگاه‌های داده مختلفی تلفیق شوند؛ تکه‌های پراکنده اطلاعات که در اختیار سازمان‌های مختلف هستند، پس از تلفیق، تصویری کامل از شهروند را شکل می‌دهند؛ بنابراین چگونه می‌توان داده‌های شخصی حساس را از داده‌های شخصی عام تمیز داد و از آنها حمایت به عمل آورد؟ بنابراین، حمایت صرف از داده‌های شخصی حساس عملاً ناممکن بوده و تنها با حمایت از تمامی داده‌های شخصی شهروندان است که می‌توان به صیانت از حریم خصوصی اطلاعاتی آنان امید داشت.

در مورد شکاف نظارتی باید گفت که برخلاف ایران، در تمامی کشورهای منتخب، سازمانی به عنوان دیده‌بان حریم خصوصی اطلاعاتی بر نحوه پیروی تمامی سازمان‌های دولتی و غیردولتی از قوانین حمایت از داده (یا قوانین حفاظت از حریم خصوصی اطلاعاتی) نظارت فعال داشته و شهروندان می‌توانند شکایات خود درباره نقض حریم خصوصی اطلاعاتی‌شان را به این سازمان تسلیم کنند و پیگیر خسارات ناشی از نقض حریم خصوصی اطلاعاتی خود باشند. به عنوان مثال، در کره جنوبی «کمیسیون حفاظت از

اطلاعات شخصی»،^۱ در فرانسه «کمیسیون حفاظت از اطلاعات شخصی و آزادی»،^۲ در انگلستان «دفتر کمیسیونر اطلاعات»،^۳ در کانادا «دفتر کمیسیونر حریم خصوصی»،^۴ در ایتالیا «سازمان حافظ داده‌های شخصی»،^۵ و در ایرلند «دفتر کمیسیونر حافظ داده‌های شخصی»^۶ به‌عنوان سازمان‌های مستقلی شناخته می‌شوند که بر اجرای قوانین حریم خصوصی اطلاعاتی نظارت داشته و مستقیماً به پارلمان این کشورها گزارش می‌دهند. علاوه بر این وظیفه، رسیدگی به شکایات شهروندان در مورد حریم خصوصی اطلاعاتی و پیشنهاد اصلاحات مورد نیاز در قوانین حریم خصوصی جزء وظایف آنهاست.

بر این اساس مهم‌ترین پیشنهادهای این تحقیق عبارت‌اند از: ۱. تدوین قانونی مجزا برای حفاظت از حریم خصوصی اطلاعاتی شهروندان با در نظر گرفتن الزامات شناسایی شده در جدول‌های ۱ تا ۷ در این تحقیق؛ به‌طوری که در آن، هر دو دسته داده‌های شخصی حساس و داده‌های شخصی عام، مدنظر قانونگذار قرار گیرند. ۲. ایجاد نهادی مستقل از دولت و تحت نظر مجلس شورای اسلامی یا قوه قضائیه تحت عنوان «دیده‌بان حریم خصوصی اطلاعاتی» به‌منظور نظارت بر حسن اجرای قوانین حریم خصوصی اطلاعاتی، دریافت و رسیدگی به شکایات شهروندان پیرامون مسائل مرتبط با حریم خصوصی اطلاعاتی آنان، شناسایی نارسایی‌های قانونی و همچنین پیشنهاد اصلاحات مورد نیاز در قوانین موجود جهت ارتقای وضعیت حریم خصوصی اطلاعاتی شهروندان.

1. Personal Information Protection Commission
 2. Commission Nationale de l'Informatique et des Libertés (CNIL)
 3. Information Commissioner's Office (ICO)
 4. Office of the Privacy Commissioner of Canada
 5. Data Protection Authority (Italian: Garante per la Protezione dei dati Personali) (DPA)
 6. Data Protection Commissioner (Irish: An Coimisinéir Cosanta Sonraí)

منابع و مآخذ

- قرآن کریم، ترجمه محمدمهدی فولادوند، قم، دفتر مطالعات تاریخ و معارف اسلامی.
- آماده، مهدی (۱۳۹۲). *حمایت از حریم خصوصی*، تهران، دادگستر.
- اصلانی، حمیدرضا (۱۳۸۹). *حقوق فناوری اطلاعات*، تهران، میزان.
- الحرانی، ابن شعبه (۱۳۶۳). *تحف العقول*، ترجمه علی اکبر غفاری، قم، مؤسسه نشر اسلامی.
- انصاری، ولی‌اله (۱۳۸۰). *حقوق تحقیقات جنایی (مطالعه تطبیقی)*، تهران، سمت.
- بابی، ارل (۱۳۹۰). *روش‌شناسی کاربردی تحقیق در علوم انسانی*، ترجمه کامران فیضی و سیدحسین رضوی، تهران، انتشارات سازمان مدیریت صنعتی.
- جهانگیر، منصور (۱۳۸۶). *قانون مجازات اسلامی*، چاپ چهل و نهم، تهران، نشر دیدار.
- جوادیپور، مریم، مرتضی طیبی جلی و مسعود راعی (۱۳۸۹). «بررسی رازداری پزشکی در فقه و حقوق»، فصلنامه حقوق پزشکی، سال ۱۴، ش ۱۳.
- داوسون، کترین (۱۳۹۲). *راهنمای عملی روش تحقیق: راهنمای آسان کسب مهارت در تکنیک‌های پژوهش و انجام پروژه‌های تحقیقاتی*، ترجمه زهره دهدشتی، شاهرخ و امید مهدیه، تهران، ترمه.
- روسو، ژان ژاک (۱۳۶۶). *قرارداد اجتماعی یا اصول حقوق سیاسی*، ترجمه منوچهر کیا، تهران، گنجینه.
- سرمد، زهره، عباس بازرگان و الهه حجازی (۱۳۷۸). *روش‌های تحقیق در علوم رفتاری*، تهران، انتشارات آگاه.
- سروش، محمد (۱۳۹۳). *مبانی حریم خصوصی (براساس منابع اسلامی)*، تهران، سمت.
- صدوقی، فرحناز، معصومه خوشگام و سروش بهنام (۱۳۸۶). «مقایسه سطوح دسترسی و محرمانگی مدارک پزشکی در کشورهای منتخب و ایران»، *مجله علمی پژوهشی مدیریت سلامت*، دوره ۱۰، ش ۲۸.
- عالم، عبدالرحمن (۱۳۸۰). *بنیادهای علم سیاست*، تهران، نشر نی.
- فقیهی، مهدی، غلامرضا معمارزاده و حسین رفوگر آستانه (۱۳۸۹). «حفظ حریم خصوصی بیماران، پیش‌نیاز توسعه سلامت الکترونیک»، *فصلنامه اخلاق پزشکی*، دوره ۴، ش ۱۲.
- کاتوزیان، ناصر (۱۳۶۶). *فلسفه حقوق*، جلد اول، تهران، انتشارات بهنشر.
- کرپیندورف، کلوس (۱۳۷۸). *تحلیل محتوا*، ترجمه هوشنگ نایب، تهران، انتشارات روش.
- طبرسی، علی بن حسن (بی‌تا). *مشکاة الأنوار فی غرر الأخبار*، نجف اشرف، المكتبة الحیدریه.
- مهدوی‌نژاد، غلامحسین (۱۳۸۷). «رازداری و حدود آن در حرفه پزشکی»، *مجله ایرانی اخلاق و تاریخ*

پزشکی، دوره اول، ش ۴.

هارلو، کارل (۱۳۸۳). شبه جرم، ترجمه کامبیز سیدی، تهران، میزان.

هاشمی، سیدمحمد (۱۳۸۴). حقوق بشر و آزادی‌های اساسی، تهران، میزان.

_____ (۱۳۹۴). حکم انتصاب اعضای شورای عالی فضای مجازی، آدرس: <http://farsi.khamenei.ir/message-content?id=30658>

_____ (۱۳۵۸). *قانون اساسی جمهوری اسلامی ایران*، آدرس: http://rc.majlis.ir/fa/content/iran_constitution

_____ (۱۳۸۲). *قانون تجارت الکترونیکی ایران*، آدرس: <http://rc.majlis.ir/fa/law/show>

_____ (۱۳۳۹). *قانون مسئولیت مدنی*، آدرس اینترنتی: <http://legal.umsu.ac.ir/uploads/12.pdf>

Belanger, F. and J. S. Hiller (2006). "A Framework for E-government: Privacy Implications", *Business Process Management Journal*, 12(1).

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).

Bretschneider, S. (2003). "Information Technology, E-government and Institutional Change", *Public Administration Review*, 63(6).

Canadian Personal Information Protection Act (2015). Personal Information Protection and Electronic Documents Act of 2015 (PIPEDA), Available at: <https://www.priv.gc.ca>.

Cullen, R. (2009). "Theme Article Culture, Identity and Information Privacy in the Age of Digital Government", *Online Information Review*, 33(3).

Cullen, R. and P. Reilly (2007). "Information Privacy and Trust in Government: a Citizen-based perspective from New Zealand", *Journal of Information Technology and Politics*, 4(3).

DLA. (2016). Piper's Data Protection, Privacy and Security Group, Available: <http://www.dlapiperdataprotection.com>.

Floridi, L. (1999). "Information Ethics: on the Philosophical Foundations of Computer Ethics", *Ethics and Information Technology*, 1(1).

Freil, B. (2002). "Government Benefits", *Government Executive*, 34(15), 38.

Gayton, C. M. (2006). "Beyond Terrorism: Data Collection and Responsibility for Privacy", *The Journal of Information and Knowledge Management Systems*, 36(4).

Germany Federal Data Protection Act (2014). Federal Data Protection Act of 2014 (FDPA). Available at: www.bfdi.bund.de.

Greenleaf, G. (2009). "Five Years of the APEC Privacy Framework: Failure or Promise?", *Computer Law and Security Review*, 25(1).

- Ireland Data Protection Act (2003). Data Protection Act of 2003 (DPA). Available at: <https://www.dataprotection.ie>.
- Italian Personal Data Protection Code (2003). Personal Data Protection Code of 2003 (PDPC). Available at: www.privacy.it/privacycode-en.htm.
- James, G. (2000). "Empowering Bureaucrats", *MC Technology Marketing Intelligence*, 20(12).
- Japan-Personal-Information-Protection-Act (2003). Personal Information Protection Act. Japan Government, Available at: <http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf>.
- Johnson, D. G. and H. Nissenbaum (1995). *Privacy and Databases. Computers, Ethics and Social Values*, Prentice Hall, Englewood Cliffs, NJ.
- Korean Personal Information Protection Act (2011). Personal Information Protection Act of 2011(PIPA), Available at: www.law.go.kr.
- Margetts, H. and D. Sutcliffe (2013). "Addressing the Policy Challenges and Opportunities of "Big data", *Policy and Internet*, 5(2).
- OECD (2013). OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data. Available at: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2>.
- Sharwood, S. (2013). "United Nations Signs Off on 'right to Privacy in the Digital age", *The Register*. Available at: www.theregister.co.uk/2013/12/19/united_nations_signs_off_on_right_to_privacy.
- Solove, D. J. and C. J. Hoofnagle (2006). A Model Regime of Privacy Protection (Version 3.0), *University of Illinois Law Review* (2).
- Stanford Encyclopedia of Philosophy (2016). *Information Privacy Definition*, Available at: <http://plato.stanford.edu>.
- Tavani, H. T. (2008). "Informational Privacy: Concepts, Theories and Controversies", *The Handbook of Information and Computer Ethics*.
- Thibodeau, P. (2000). "E-government Spending to Soar Through", *Computerworld*, 34 (17).
- UK Data Protection Act (1998). Data Protection Act of 1998 (DPA), Available at: <https://ico.org.uk>.
- Universal Declaration of Human Rights (1948). *Office of the United Nations High Commissioner for Human Rights*, Available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.
- Westin, A. (1967). *Privacy and Freedom*, New York, Atheneum.