شناسهٔ دیجیتال (DOI): 10.22106/JLJ.2020.88629.2213

مقالهٔ پژوهشی، دورهٔ ۸۴، شمارهٔ ۱۱۰، تابستان ۱۳۹۹، صفحات ۱۱۹ الی ۱۴۲
تاریخ دریافت: ۱۳۹۷/۰۴/۰۳ - تاریخ پذیرش: ۱۳۹۸/۰۵/۱۲

چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر[1]

لیلا رییسی‌دزکی*، فلور قاسم‌زاده‌لیاسی**

چکیده

حریم خصوصی اشخاص تحت تأثیر توسعهٔ فناوری اطلاعات و کاربردهای مختلف فضای سایبر قرار گرفته است و به‌دلیل تسهیل جست‌وجو و تسریع دستیابی به داده‌ها، در صورت عدم ساماندهی صحیح فضای سایبر، حریم خصوصی و داده‌های شخصی افراد در این فضا در معرض تهدید قرار می‌گیرد. لذا این امر دولت‌ها را بر آن می‌دارد که با برپایی نظام حقوقی کارآمد، از طریق اصلاح قوانین و مقررات داخلی موجود و وضع شیوه‌های خاص، به ساماندهی وضعیت نوپدید اقدام کنند. پژوهش حاضر با روش توصیفی‌تحلیلی درصدد است تا با واکاوی قوانین و مقررات به این مسئله بپردازد که نظام حقوقی ایران در بازدارندگی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبر با چه مشکلاتی مواجه است. یافته‌های پژوهش حاضر حاکی از این است که سیاست‌گذاران تقنینی به صیانت از این حق شهروندان توجه داشته‌اند و نظام حقوقی ایران در این زمینه، شاهد دستاوردهای مثبتی بوده است؛ اما با معضلاتی هم در این زمینه روبه‌رو می‌باشد که رفع آن‌ها مستلزم

۱. این مقاله برگرفته از رسالهٔ دورهٔ دکتری تخصصی فلور قاسم‌زاده‌لیاسی تحت عنوان «نقش نهادهای ملی مقررات‌گذار ارتباطی و فناوری اطلاعات در صیانت از حقوق شهروندی در فضای سایبر از منظر حقوق بین‌المللی (مطالعهٔ موردی حقوق ایران)» با راهنمایی نویسندهٔ مسئول و مشاورهٔ آقایان دکتر هیبت‌الله نژندی‌منش و دکتر مسعود اخوان‌فرد در دانشگاه آزاد اسلامی واحد نجف‌آباد است.

* دانشیار گروه حقوق، دانشکدهٔ علوم انسانی، دانشگاه آزاد اسلامی (واحد اصفهان)، اصفهان، ایران (نویسندهٔ مسئول)
raisi.leila@gmail.com

** دانشجوی دکتری حقوق بین‌الملل عمومی، دانشکدهٔ حقوق، الهیات و معارف اسلامی، دانشگاه آزاد اسلامی (واحد نجف‌آباد)، نجف‌آباد، ایران Florence.titi2000@gmail.com

وضع قوانین و مقررات پیشینی و پسینی بهینه و مؤثر و متناسب با مقتضیات فضای سایبر است. بدون تردید این امر بدون تأثیرپذیری از قواعد بین‌المللی حقوق بشر و اقتباس از هنجارها و توصیه‌های اسناد بین‌المللی امکان‌پذیر نیست.

واژگان کلیدی: حریم خصوصی، فضای سایبر، داده‌های شخصی، حقوق بشر

مقدمه

تحولات اجتماعی و فناوری با حقوق شهروندی ارتباط نزدیکی داشته و دارد. فضای سایبری را می‌توان نتیجهٔ تحولات و پیشرفت‌های فناوری دانست که بستر جدیدی را برای زیست انسانی فراهم کرده است. افراد در این فضا، بسیاری از روابط خود را در حوزه‌های مختلف شکل و توسعه می‌دهند. ساده‌ترین فعالیت‌های انسانی، از گفت‌وگو گرفته تا تعاملات پیچیده مثل معاملات می‌توانند در این پهنه انجام شوند. همین امر باعث شده است تا این فضا از یک طرف مورد استقبال قرار گیرد و از طرفی دیگر نوعی نگرانی را در میان افراد ایجاد کند.

پیشرفت تکنولوژی و گسترش فضای مجازی در زندگی بشر با تغییر در نوع روابط، این امکان را فراهم ساخته است که با بهره‌مندی از قابلیت‌های فضای سایبر، اشخاص، هم‌زمان از دیدگاه یکدیگر مطلع گردند؛ لیکن پیدایش این فناوری‌ها با تسهیل دسترسی، زمینهٔ سوءاستفاده از این اطلاعات را در گسترهٔ وسیعی، فراهم آورده و بر نگرانی‌های مربوط به تهدید حریم خصوصی افراد در عصر ارتباطات دامن زده است. ازاین‌رو، بحث اطمینان از صیانت داده‌های شخصی در این فضا، از اهمیت خاصی برخوردار می‌باشد. این مسئله، دولت‌ها را ملزم می‌سازد که تدابیر و راهکارهای پیشینی و پسینی برای جلوگیری از نقض حریم خصوصی شهروندان، اتخاذ کنند. در این نوشتار، ضمن تبیین مفاهیم حریم خصوصی و داده‌های شخصی و قواعد بین‌المللی و قوانین و مقررات داخلی مربوط به حریم خصوصی و داده‌های شخصی، به معضلات موجود در نظام حقوقی ایران برای صیانت از این حق پرداخته و به این سؤال پاسخ داده می‌شود که چگونه می‌توان از شهروندانی که داده‌های شخصی و حریم خصوصی آنان در فضای سایبر نقض گردیده است، در برابر ناقضین این حقوق، حمایت به عمل آورد. برای ارائهٔ این موضوع، پس از ذکر این مقدمه، رابطهٔ حریم خصوصی و داده‌های شخصی در بخش اول، حمایت از حریم خصوصی و داده‌های شخصی در قواعد بین‌المللی و مقررات دیگر کشورها در بخش دوم و آسیب‌شناسی قوانین و مقررات حریم خصوصی و حمایت از داده‌ها در بازدارندگی از نقض این حریم در فضای سایبر در بخش سوم تبیین می‌گردد.

۱. رابطهٔ حریم خصوصی و داده‌های شخصی

برای تبین رابطهٔ بین حریم خصوصی و داده‌های شخصی، ابتدا به ذکر مفاهیم هریک از آن‌ها پرداخته می‌شود.

۱-۱. مفهوم حریم خصوصی

حریم، قلمرویی است که دارنده‌اش نمی‌خواهد دیگران بدون اجازه‌اش از آن آگاهی یابند یا با بهره‌برداری از آن آگاهی اقدامی کنند. حریم می‌تواند مکان، سند یا جسمی باشد که از دستیابی به اطلاعات و داده‌های درون آن به طرق ناروا باید جلوگیری شود، حتی اگر تهی باشد؛ چراکه حریم اشخاص، به‌نوعی با حیثیت و آبروی افراد در ارتباط است. اشخاص هم از طریق حریم و هم از طریق حرمت می‌توانند حق برحیثیت خود را استیفا کنند؛ لذا بعضی از امور در دایرهٔ حریم اشخاص، شاید مستقلاً حرمت شخص را مورد تعرض قرار ندهد؛ اما ممکن است زمینهٔ داوری‌هایی را فراهم آورند که به هتک حرمتش بینجامد. بنابراین حریم خصوصی، مفهوم گسترده‌ای دارد و امروزه از جمله آزادی اندیشه، داشتن خلوت، کنترل بر اطلاعات شخصی، حمایت از حیثیت خود و حمایت در برابر تفتیش‌ها و رهگیری‌ها را شامل می‌شود (انصاری، ۱۳۹۱: ۳۸-۱۱). از منظر این تعریف، ضابطهٔ معین برای ورود به آن حوزه و مطالبه از دولت برای شناسایی این حق و اجرای آن و مجازات‌کردن افرادی که بدون هیچ دلیلی این حریم را نقض می‌کنند، از مسائلی است که در حریم خصوصی، قلمرو و ماهیت آن نقش‌آفرینی می‌کنند. ازاین‌رو با توجه به نسبیت این مفهوم، مشکلات جدی در تعریف، ذات و قلمرو این حق وجود دارد. اما آنچه مسلم است آن است که حریم خصوصی، حق برخورداربودن از حوزه‌های خاص غیرقابل‌نقض، می‌باشد (راعی، ۱۳۸۹: ۱۱۷-۱۱۴). در واقع حریم خصوصی، تمایز بین حوزهٔ عمومی و خصوصی را بیان می‌کند. دامنهٔ حریم خصوصی مقامات و افراد مشهور نسبت به شهروندان عادی، محدودتر تلقی می‌گردد. کشورهای اروپایی از مادهٔ ۸ کنوانسیون اروپایی حقوق بشر استنباط می‌کنند که در اماکن عمومی، مثل کافه‌ها، مقامات و مشاهیر از حریم خصوصی برخوردارند؛ اما کشورهایی که قانون کامن‌لا در آن اعمال می‌گردد، کم‌وبیش با این امر مخالف هستند (Guinchard, 2010) و دایرهٔ حریم خصوصی را تنگ‌تر ترسیم می‌نمایند. برخی، حریم خصوصی اطلاعات را حوزه‌هایی از زندگی اشخاص می‌دانند که از سوی دیگران تسخیرناپذیر است. به نظر می‌رسد در تعریف این حق باید توجه داشت که قلمرو این حق، ناظر به مسائلی است که صرفاً در حیطهٔ موضوعات شخصی افراد بوده و ذی‌حق به‌هیچ‌وجه تمایلی به افشای آن نداشته باشد و نیز افشاشدن بخشی از اطلاعات خصوصی افراد و نقض حریم شخصی آن‌ها باعث نمی‌شود که افشای بقیهٔ اطلاعات یا انتشار مجدد بخش فاش‌شده را مجاز محسوب کرد. بحث

حریم خصوصی در فضای سایبر همان بحث حمایت از داده‌هاست و حق بر حریم خصوصی به اشخاص حقوقی نیز تسری می‌یابد؛ چراکه از حق بر داده‌ها برخوردارند (جعفری و رهبرپور، ۱۳۹۶: ۴۷-۴۵). از آنجا که حق بر حریم خصوصی از حقوقی است که به نوعی تضمین‌کنندهٔ امنیت، آزادی، آسایش و کرامت شهروندان است (ساریخانی و محترم‌قلاتی، ۱۳۹۸: ۱۶۴)، تدوین قوانین و مقررات شفاف و کارآمدی که بتواند از حریم خصوصی و داده‌های شخصی صیانت به عمل آورد و با ناقضین آن برخورد کند، از اهمیت ویژه‌ای برخوردار است؛ به‌نحوی که حتی دولت نیز نتواند جز در موارد مصرح قانونی، متعرض آن گردد.

۲-۱. مفهوم داده‌های شخصی

مطابق مادهٔ ۲ لایحهٔ صیانت و حفاظت از داده‌های شخصی، دادهٔ شخص عبارت است از داده‌ای که به‌تنهایی یا به‌همراه داده‌های دیگر، مستقیم یا غیرمستقیم، شخصِ موضوعِ داده را از طریق ارجاع به یک شناسه می‌شناساند. حریم زندگی افراد، هر لحظه با نوآوری‌های فناوری در تنگنای بیشتر قرار می‌گیرد و اطلاعات شخصی افراد در فضای سایبر همانند کالایی است که گردآوری و تبادل شده و به‌سهولت بازآفرینی می‌شود (نوری و نخجوانی، ۱۳۸۳: ۱۱) و از آنجا که آزادی بیان ارتباط تنگاتنگی با آزادی عقیده و مذهب و در نتیجه گردش آزاد اطلاعات پیدا می‌کند، حفاظت از اطلاعات شخصی و حق محرمانه‌بودن ارتباطات و مکاتبات در فضای سایبر، به‌طور خاص مورد توجه قرار می‌گیرد.

۳-۱. رابطهٔ حریم خصوصی و داده‌های شخصی

از اواسط دههٔ ۱۹۷۰ با توسعهٔ فناوری اطلاعات و فضای سایبر، حریم خصوصی افراد با تهدید جدی مواجه شد. حریم خصوصی اطلاعات که بعضی از نظام‌های حقوقی از آن به‌عنوان حمایت داده‌ها یاد می‌کنند، دربرگیرندهٔ قواعد حاکم بر پردازش داده‌ها و اطلاعات مربوط به اشخاص است. با این اوصاف، اگرچه اصل مباحث ذاتاً ارتباطی به فناوری‌های نوین ندارد، پیدایش این فناوری‌ها، زمینهٔ تسهیل و ترویج این قبیل اعمال را در گسترهٔ وسیعی فراهم آورده و بر نگرانی از سوءاستفادهٔ احتمالی از این اطلاعات دامن زده است.

نقض حریم خصوصی مستلزم سری و محرمانه‌بودن اطلاعات نیست؛ بلکه هرگونه اطلاعات مربوط به اشخاص را شامل می‌گردد (نوری و نخجوانی، ۱۳۸۳: ۲۹). لذا اتخاذ تدابیر پیشگیرانه از سوی دولت‌ها در طراحی سیستم‌های مطمئن بسیار حائز اهمیت است. دولت‌ها باید با جلوگیری از هرگونه نفوذ و سوءاستفاده، تمامیت و محرمانگی اطلاعات را تضمین کنند؛ چراکه سوءاستفادهٔ افراد از طریق شبکه یا محیط فیزیکی سیستم‌های اطلاعاتی ممکن است منجر به فاش‌شدن اطلاعات، تغییر یا حذف داده‌ها شود (عبدالهی و شهبازی‌نیا، ۱۳۸۸: ۱۲۷-۱۲۳)؛ در نتیجه چگونگی مدیریت

و ساماندهی مصونیت داده‌ها که از روابط مختلف بین افراد در حوزه‌های گوناگون، تولید و مبادله می‌گردد، برای حفظ کرامت انسانی آنان ضرورت دارد (Santanen, 2019: 5-14). بنابراین می‌توان گفت که حریم خصوصی در فضای سایبر، شامل مشخص‌نشدن هویت و پنهان‌ماندن اطلاعات است که می‌تواند مانع بروز زمینه‌های جرم و خشونت علیه کاربران گردد. ازاین‌رو، ضرورت احترام به حریم خصوصی در فضای سایبر همانند دنیای واقعی از مؤلفه‌های حقوق بشری و صیانت از آن، وظیفهٔ دولت‌هاست و باید توسط قوانین داخلی و معاهدات و قواعد بین‌المللی شناخته شود؛ به‌نحوی که شهروندان این اطمینان را داشته باشند که حریم خصوصی آنان، اعم از مشخصات فردی و پیام‌های ارسالی به دیگران، مصون از تعرض است.

۲. حمایت از حریم خصوصی و داده‌های شخصی در قواعد بین‌المللی و مقررات دیگر کشورها

قابلیت‌های فضای سایبر، این امکان را فراهم می‌سازد که کارفرمایان برای اخذ اطلاعات جهت استخدام یا اخراج کارکنان خود به جست‌وجو در اینترنت بپردازند و این امر، حریم خصوصی کاربران را با تهدید مواجه می‌سازد که علاوه بر وضع قوانین کارآمد، لزوم طراحی سیستم را به‌گونه‌ای که تنظیمات پیش‌فرض کاملاً خصوصی باشد، محرز می‌سازد. اگرچه بیشتر شبکه‌های اجتماعی بین حریم عمومی و خصوصی تفکیک قائل شده‌اند و تدابیری برای حفظ آنان در نظر گرفته‌اند، به‌دلیل تسهیل دسترسی و تبادل اطلاعات و نظارت نامرئی در فضای سایبر، انتظار آزادی در این فضا بیشتر است (فتحی و شاهمرادی، ۱۳۹۶: ۲۵۰-۲۴۹)؛ بنابراین رشد فزایندهٔ فناوری و جهانی‌شدنِ دسترسی به اطلاعات شخصی، امکان تخریب و تغییر سریع و آسان داده‌ها، گستردگی مشکلات ناشی از آن و روند سریع افزایش رقم بزهکاری در این فضا، مستلزم ساماندهی فضای سایبر برای کاهش معایب و آسیب‌هاست. ساماندهی بهینه با قوانین و مقرره‌هایی محقق می‌شود که متناسب با اصول بنیادین حقوق بشری و همکاری‌های بین‌المللی وضع گردد.

مادهٔ ۱۲ اعلامیهٔ جهانی حقوق بشر، به لزوم حمایت قانونی از حریم خصوصی در برابر تعرضات پرداخته و مادهٔ ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی و مادهٔ ۸ کنوانسیون اروپایی حقوق بشر نیز بر این حمایت قانونی تأکید گردیده است. در این اسناد، دو نوع تعهد برای دولت‌ها در نظر گرفته شده است: نخست اینکه دولت‌ها مکلف هستند در زمینهٔ حریم خصوصی، اقدامات ایجابی انجام دهند و دیگر اینکه ملزم شده‌اند که اقدامات سلبی لازم را در خصوص عدم مداخله در حریم خصوصی، ایجاد کنند (مقامی و عطاران، ۱۳۹۸: ۳۱۶-۳۱۵). از همان زمان، کشورها در این زمینه قوانینی را وضع کردند؛ لیکن ضوابطی که از سوی اعلامیه و میثاق در خصوص حفظ امنیت ملی، سلامت و اخلاق عمومی ذکر گردیده است، باعث شد برخی کشورها در تفسیر حدود و ثغور آن‌ها بی‌ملاحظگی‌هایی

به خرج دهند (فراهانی، ۱۳۸۴: ۱۲۰-۱۱۹). نکتهٔ شایان توجه این است که نگرانی‌های مربوط به حریم خصوصی حتی بر حق افراد مبنی بر داشتن سلامتی نیز تأثیر می‌گذارد؛ به‌خصوص در نوجوانان که خطرات و تهدیدهای حریم خصوصی، سلامتی آنان را به خطر می‌اندازد. اهمیت این موضوع، دولت‌ها را وادار به قاعده‌مندکردن این فضا برای بهره‌مندی بیشتر و آسیب کمتر کرده است.

پیشرفت فناوری سبب شد که انواع ارتباطاتی که از طریق تلفن و وسایل رادیویی صورت می‌گیرد، قابل‌شنود و رهگیری باشد. بنابراین موازینی در این خصوص باید وضع می‌گردید. اتحادیهٔ بین‌المللی مخابرات در مادهٔ ۳۷ اساسنامه به این امر توجه داشته است و اشعار می‌دارد: «اعضای اتحادیه موافقت می‌نمایند تا تدابیر لازم را جهت تضمین محرمانه‌ماندن مکالمات بین‌المللی اتخاذ کنند.» اما در بند ۲ این ماده به مقامات دولتی اجازه می‌دهد که نظارت قانونی خود را اعمال کنند (انصاری، ۱۳۹۱: ۳۰۲-۲۹۷). از آنجا که زمینه برای سوءاستفادهٔ دولت‌ها از طریق امکان نظارت بر مکالمات و داده‌های فضای سایبر وجود داشت، با بهره‌گیری از ظرفیت‌های قواعد بین‌المللی صیانت از حریم خصوصی، در سال ۱۹۸۸ کشورها در زمان صدور تفسیر عام[1] موضوع مادهٔ ۱۷ میثاق بین‌المللی، بر حریم خصوصی در فضای سایبر تأکید کردند و آلمان با بیان تأثیر نوآوری‌های تکنولوژی، خواهان اعمال اصول حقوق بشری حاکم بر صیانت از حریم خصوصی دنیای فیزیکی، بر فضای دیجیتال شد. در سال ۲۰۱۳ نیز رئیس‌جمهور برزیل خواهان تصویب معاهدهٔ الزام‌آوری مبنی بر طراحی مکانیسم چندجانبه برای تضمین اصول حقوق بشری، مثل حریم خصوصی و آزادی بیان در فضای سایبر گردید. شورای حقوق بشر و مجمع عمومی سازمان ملل در سال‌های ۲۰۱۲ تا ۲۰۱۶ قطعنامه‌هایی را در خصوص حریم خصوصی در عصر دیجیتال به تصویب رساندند و مقرر داشتند که قواعد مربوط به حقوق بشر در فضای فیزیکی برای فضای سایبر نیز اعمال گردد. قطعنامهٔ ۶۹/۱۶۶ با این هدف، کشورها را ملزم به اصلاح قوانین و مقررات خود در خصوص جمع‌آوری و نگهداری اطلاعات شخصی نمود و تأکید داشت که دولت‌ها به تعهدات خود تحت لوای قواعد بین‌المللی حقوق بشر عمل کنند. قطعنامهٔ ۲۸/۱۶ در سال ۲۰۱۵ نیز خواستار ارائهٔ یک روش مؤثر برای شناسایی اصول، استانداردها و شیوه‌های بهینهٔ حفاظت از حریم خصوصی شد (Wat, 2017) تا با تدوین قوانین و مقررات هم‌سو با موازین بین‌المللی حقوق بشر، دستاورد مطلوب در صیانت از حقوق شهروندی در فضای سایبر حاصل آید.

1. General Comment

در قانون اساسی ایالات متحدهٔ آمریکا نیز در خصوص نقض حریم خصوصی شهروندان، محدودیت‌های زیادی برای دولت در نظر گرفته شده است و قواعد مشابه مقررات حفاظت از داده‌های عمومی اروپا، به تصویب رسانده‌اند؛ هرچند ممکن است در قوانین ایالتی، این محدودیت‌ها کم‌رنگ‌تر باشد. در نشریهٔ حقوقی هاروارد، در سال ۱۸۹۰ با تأکید بر حفظ حریم خصوصی به‌عنوان حریم خلوت و تنهایی برای حق لذت‌بردن از زندگی که در واقع حق بنیادین زندگی است، انتشار هرگونه اطلاعات در خصوص افراد را خدشه به این حریم و نقض حقوق اساسی شخص دانسته است. دیوان عالی آمریکا نیز در آرای سال ۱۹۶۵[1] و ۱۹۷۳[2] مستفاد از اصول متعدد قانون اساسی، دولت را از مداخله در حریم خصوصی افراد منع می‌کند. اگرچه این آرا مربوط به حریم خصوصی در امور خانوادگی و ازدواج می‌شد، دامنهٔ شمول احترام به حریم خصوصی، به حریم خصوصی در فضای سایبر و حریم اطلاعات شخصی نیز تسری می‌یابد و دولت، نهادهای غیردولتی و اشخاص عادی از دخالت در حریم دیگران منع شده‌اند. با گسترش فناوری‌های جدید، بازبینی مفاهیم حریم خصوصی فیزیکی برای فضای سایبری با نظر به واقعیت‌های این فضا و تصویب قواعد متناسب با نیازهای آن ضروری است. از طرف دیگر، در دنیای جدید و فضای سایبر و تحولات ناشی از آن، از جمله حمایت از حقوق ناشی از کسب و کار اینترنتی که با امنیت فضای سایبر و صیانت از حریم خصوصی رابطهٔ مستقیم دارد، اصطلاح حمایت از داده‌های شخصی به جای حمایت از حریم خصوصی به‌نظر شفاف‌تر است (De George, 2018: 107-116). بنابراین در ساماندهی فضای سایبر باید به تمام قابلیت‌ها و واقعیت‌های این فضا توجه کرد تا از پیامدهای منفی آن کم شود.

به‌دلیل ماهیت حریم خصوصی و اهمیت داده‌های شخصی، برخی معتقد هستند بهتر است در این حوزه، قواعدی با قدرت و الزام قواعد عمومی وضع گردد؛ چراکه رضایت فرد برای استفاده از اطلاعات شخصی با علم به تمامی پیامدهای ناشی از نشر اطلاعات نبوده و ممکن است خطراتی را در پی داشته باشد. اگرچه کنترل افشا و انتشار اطلاعات شخصی توسط خود فرد و استفاده از آن اطلاعات در موارد تعیین‌شده، مؤثر در این زمینه است، رویکرد منفعت عمومی به حریم خصوصی، ممکن است بسیار مفید واقع گردد (Choi & others, 2019: 113-124). اتحادیهٔ اروپا در سال ۲۰۱۶ با بازنگری سند ۹۵/۴۶/EU سال ۱۹۹۵، حمایت افراد در برابر پردازش داده‌های شخصی و انتقال آن را مورد تأکید قرار داد و برابر این سند، حق استفاده و پردازش داده‌های شخصی، بدون کسب رضایت صریح شخص، غیرمجاز است و در صورت کسب اجازه هم صرفاً برای هدف مورد

1. Griswold v. Connecticut
2. Roe v. Wade

رضایت شخص، می‌تواند مورد بهره‌برداری قرار گیرد که مفاد این سند، با استقبال اکثر کشورهای جهان به‌استثنای کشورهای معدودی، از جمله آمریکا همراه شد و آن کشورها، قوانین و مقررات خود را در حمایت از داده‌های شخصی، مطابق با این سند تصویب یا اصلاح کردند. آمریکا معتقد است در مواردی که منافع اقتصادی شخص، هدف قرار می‌گیرد و با دستیابی به داده‌ها، به حقوق مالکیت تجاری و حق کسب‌وکار اشخاص خسارت وارد می‌گردد، بحث حمایت از حریم شخصی مطرح می‌شود. اما سرقت اطلاعات مربوط به هویت نیز علاوه بر اینکه ممکن است منجر به آسیب‌های جسمی، عاطفی و اجتماعی شخص گردد، بر روابط اشتغال، کار و کارگری و بیمه نیز تأثیرگذار است (De George, 2018: 116-119). بنابراین واقعیت دنیای امروز و فضای سایبر و اهمیت داده‌ها بر لزوم حفظ آن در برابر هرگونه تخریب و دستکاری حکایت می‌کند؛ حتی اگر پردازش و تغییر آن منجر به هیچ‌گونه ضرر مادی یا معنوی شخص نگردد.

مقررات حفاظت از داده‌های عمومی[1] با هدف تقویت حمایت از داده‌ها، از ماه می ۲۰۱۸ در تمامی کشورهای عضو اتحادیه، لازم‌الاجرا شده و جایگزین دستورالعمل ۲۰۱۶/۶۷۹ آن اتحادیه گردیده است. اجرای این مقررات برخلاف دستورالعمل سابق اتحادیه، موکول به تصویب قوانین ملی کشورهای عضو نشده است و بدون قانون‌گذاری مجدد، کشورهای عضو مکلف به رعایت قواعد مندرج در مصوبه شده‌اند. نکتهٔ دیگری که قانون‌گذاران اروپایی در حمایت از داده‌ها در موضوعات پژوهشی علمی و پزشکی به آن توجه داشته‌اند، بحث نگهداری داده‌ها برای مدت محدود و پردازش اطلاعاتی بوده است که مستقیماً به اهداف تحقیق آنان مرتبط می‌باشد (Grech, 2018: 44-45). از این منظر می‌توان حساسیت سیاست‌گذاران اروپایی در صیانت از داده‌ها و محرمانگی اطلاعات را در مقررات‌گذاری ملی مدنظر قرار داد تا با دستیابی غیرمجاز به داده‌های شخصی یا نگهداری طولانی‌مدت، علاوه بر امکان ورود خسارت مادی و معنوی، زمینهٔ احتمالی بروز جرایم ناشی از دستیابی آن اطلاعات فراهم نگردد و با وضع مجازات‌های بازدارندهٔ مؤثر، از نقض حق حریم خصوصی شهروندان در فضای سایبر جلوگیری به عمل آید.

آرای دادگاه‌های بین‌المللی، طبق اصول دادرسی، صرفاً برای طرفین اختلاف و برای همان موضوع مجری می‌باشد و این امر در مادهٔ ۵۹ اساسنامهٔ دیوان بین‌المللی دادگستری، تأکید شده است؛ اما دیوان بین‌المللی در آرای متعدد خود به رویه‌های گذشته استناد کرده است و از این منظر آرای صادره از دادگاه‌های بین‌المللی می‌تواند زمینه‌ساز اصول حقوق بشری و عرف‌های بین‌المللی و

1. General Data Protection Regulation “GDPR”

منطقه‌ای‌گردد. بنابراین اصول حقوق بشری مندرج در آرای دیوان اروپایی حقوق بشر (این دیوان متشکل از قضات برجستهٔ علمی و با دغدغه‌های حقوق بشری، فارغ از تمایلات منفعت‌طلبانه و مصلحت‌اندیشی است)، می‌تواند در توسعهٔ حقوق بشر مثمرثمر باشد. هرچند در آرای صادره به آرای گذشته به‌عنوان اصول و قواعد حقوقی اشاره نشده باشد، به‌دلیل استناد به مبانی دقیق حقوقی نه‌تنها به‌عنوان اصول حقوقی و تفسیری از کنوانسیون حقوق بشر اروپایی در کشورهای عضو لازم‌الاجرا می‌گردد، بلکه کشورهای دیگر نظیر ترکیه و روسیه نیز از آرای دیوان تبعیت نموده و خود را ملزم به رعایت مفاد و اصول مقرر در آن آرا می‌دانند و قوانین خود را مطابق با احکام صادره، تصویب می‌کنند. در دعوای اس و مارپر علیه بریتانیا[1] دیوان اروپایی حقوق بشر در سال ۲۰۰۸ با تکیه بر حریم خصوصی و تحت مادهٔ ۳۴ کنوانسیون اروپایی حقوق بشر و آزادی‌های اساسی به موضوع رسیدگی کرد. در این پرونده که شاکیان با استناد به مادهٔ ۸ کنوانسیون، به حق حریم خصوصی خود استناد کرده و اعلام داشتند که نگهداری هویت و داده‌های مربوط به شناسایی متهمین، پس از تبرئه، موجب خدشه‌دارشدن حیثیت آنان شده و تجاوز به حریم آنان محسوب می‌گردد. دیوان با استناد به قوانین و مقررات مختلف، از جمله مقررات عمومی حفظ داده‌های اروپا ۱۹۹۵ و قواعد کیفری، نگهداری اطلاعات شخصی متهمین را حتی با هدف پیشگیری از جرم، صحیح ندانست و ضمن تأکید بر اینکه احترام به حریم خصوصی مجرمین نیز اقتضا می‌کند که مدت نگهداری اطلاعات هویتی، ژنتیکی و تمام داده‌های مربوط به آن محدود و صرفاً برای هدف مشخص قانونی، پردازش و استفاده شود، اعلام کرد نگهداری اطلاعات متهمین تبرئه‌شده با افراد عادی تفاوتی نداشته و بدون رضایت آنان، حتی اگر مورد استفاده نیز قرار نگرفته باشد، نقض مادهٔ ۸ کنوانسیون است و بریتانیا ملزم به پرداخت خسارت تعیین‌شده، گردید.[2] در دیوان عالی کانادا نیز با تأکید بر اینکه نگهداری و استفاده از اطلاعات اشخاص جز در مواردی که منافع ملی اقتضا می‌کند، نقض جدی حریم خصوصی و داده‌های شخصی است، آرای مشابه‌ای صادر شده است.[3] بنابراین آرای صادره از دادگاه‌های بین‌المللی و کشورهای پیشرو و موفق در صیانت از حقوق بشری و به‌خصوص آرای دیوان اروپایی حقوق بشر، که اصولاً مبتنی بر قواعد و استدلال‌های حقوق بشر است، می‌تواند به‌عنوان یک الگوی مقرره‌گذاری ملی در حمایت از حقوق شهروندی مدنظر قرار گیرد.

1. S. and Marper v. the United Kingdom
2. R. v. R.C(2005), R. v. Plant (1993)
3. REPORTS OF JUDGMENTS AND DECISIONS,2008-V, EUROPEAN COURT OF HUMAN RIGHTS.pp.174-212

فضای یکپارچهٔ سایبر، لزوم وضع قواعد هماهنگی را که بتواند بر قوانین ملی دولت‌ها حاکم باشد، ایجاب می‌نمود و کنوانسیون جرایم سایبری با هدف ساماندهی فضای سایبر، هماهنگی قوانین ملی در راستای جلوگیری از جرم، توسط شورای اروپا به تصویب رسید و رویکردی جامع در هماهنگ‌سازی کشورها علیه جرایم سایبر، از جمله نقض حریم خصوصی ارائه می‌دهد که از سال ۲۰۰۴ به اجرا درآمد و علاوه بر کشورهای عضو اتحادیه، کشورهای دیگر نظیر ایالات متحدهٔ آمریکا، ژاپن و آفریقای جنوبی نیز در مناظرات آن شرکت داشتند و نقش ایالات متحدهٔ آمریکا به‌دلیل تجارب بیشتر در مسائل سایبری، در نحوهٔ تدوین کنوانسیون بسیار تأثیرگذار بود. یکی از جنبه‌های مهم این کنوانسیون که عملاً در اجرا مغفول مانده، این است که کنوانسیون صرفاً محدود به جرایم سایبری نیست بلکه به تمام جرایمی که آثار و شواهدش می‌تواند به‌طور الکترونیکی جمع‌آوری گردد، تسری می‌یابد. این کنوانسیون، شامل سه بخش می‌باشد که بخش سوم آن مربوط به مکانسیم‌های تقویت همکاری‌دولت‌ها برای پیشگیری و مقابله با جرایم سایبری است و حائز اهمیت است. مطابق با این کنوانسیون، کشورهای عضو ملزم به تصویب قوانین ملی، برابر تعهدات مندرج در آن می‌باشند. دسترسی غیرمجاز به داده‌های شخصی الکترونیکی، تخریب، دستکاری و انتقال داده‌ها، تولید، فروش برنامه‌هایی که با هدف تخریب و ازکارافتادن سیستم‌های الکترونیکی یا دسترسی یا استفاده از اطلاعات آن طراحی شده، از جرایم مهم سایبری ذکر گردیده است. آنچه مرتبط با حریم خصوصی در این کنوانسیون قابل‌تأمل است، علاوه بر مواردی که به‌عنوان جرم شناخته شده، بحث دسترسی یک‌طرفه به داده‌های ذخیره‌شده در کشور دیگر در مواقع بروز جرم است که با مشکل جدی مواجه گردید و عده‌ای معتقد بودند که باید محدود به رضایت مالک داده‌ها و صرفاً برای دسترسی به داده‌های باز شود. و نهایتاً در کنوانسیون، دسترسی یک‌طرفه، نه مطلقاً مجاز و نه به‌طور مطلق ممنوع گردید (Vatis, 2010: 207-217). بنابراین لزوم شفاف‌سازی در این زمینه می‌تواند بسیار مؤثر واقع شود. برای صیانت بهتر از حریم خصوصی و داده‌های شخصی، جا دارد دسترسی یک‌طرفه به داده‌های ذخیره‌شده توسط دولت دیگر، محدود به موارد خاص و مصرح گردد.

۳. آسیب‌شناسی نظام حقوقی ایران در بازدارندگی از نقض حریم خصوصی در فضای‌سایبر

آنچه در این مبحث به آن پرداخته می‌شود، جایگاه حریم خصوصی در ایران و صیانت از این حق شهروندان در فضای سایبر است. حق حریم شخصی که در قوانین بین‌المللی حقوق بشر و قوانین دیگر کشورها بر آن تأکید ورزیده شده است، در قانون اساسی ایران نیز در اصول متعددی از جمله اصل بیست‌ودوم، بیست‌وسوم و بیست‌وپنجم بدان اختصاص یافت و اصل سی‌ونهم نیز با

ممنوع‌دانستن هتک حرمت زندانیان و تعیین مجازات برای عاملین این اقدام غیرقانونی، تجاوز به حریم خصوصی را ممنوع کرده است.

به موجب قواعد مستنبط از قانون اساسی، سیاست‌های کلی نظام و رویه و رویکردهای حاکم کنونی و مطالعات تطبیقی در ارتباط با حریم خصوصی و داده‌های شخصی، می‌توان خلأها و چالش‌های موجود در این حوزه را شناسایی کرد. به‌ویژه به‌دلیل ماهیت این فضا که بعضاً در آن، اقداماتی با اثرات فرامرزی صورت می‌پذیرد، مقررات شکلی فضای سایبر بیشتر از مقررات ماهوی متأثر گردیده است و خلأهای بیشتری در این زمینه وجود دارد که با توجه به شرایط خاص حاکم بر سازکارهای فضای سایبر، تدابیر کلاسیک حقوقی بعضاً نمی‌تواند پاسخگو باشد و حتی تطبیق معیارهای سنتی، ممکن است باعث مشکلات فراوانی شود (طهماسبی و شاهمرادی،۱۳۹۷: ۹۸-۹۷). بنابراین یکی از اقدامات لازم برای رفع مشکل و صیانت از حقوق کاربران، علاوه بر مقرره‌گذاری متناسب با وقایع و نیازمندی‌های دنیای نوین، مدیریت قوانین و مقررات موجود می‌باشد تا تورم قوانین و مقررات در کشور، عملاً حقوق‌دانان، نهادهای اجرایی و حتی مقامات قضایی را در پاسداشت حقوق شهروندان و ذی‌نفعان با مشکل مواجه نسازد. این امر با تدوین و تنقیح صحیح قوانین و مقررات محقق می‌گردد و از طرف دیگر شهروندان نیز با رجوع به چنین مجموعه‌ای از حقوق و تکالیف خود آگاه می‌شوند (آقایی طوق، ۱۳۹۸: ۱۳-۱). راهکار دیگر در مواجهه با این چالش‌ها، نهادسازی صحیح فضای سایبری است که نبود یا کاستی نهادهای ذی‌صلاح، معضلاتی را هم برای حاکمیت و هم شهروندان، پدید می‌آورد. همان گونه که نقش کمیتهٔ ملی کنترل موانع امنیتی در فرانسه می‌تواند در ایجاد تعادل بین صیانت از حریم خصوصی و تأمین امنیت ملی مؤثر باشد، در ایران نیز مرکز ملی فضای مجازی می‌تواند بسیار مؤثر باشد. در هر صورت لزوم احترام به حریم خصوصی و صیانت از آن ایجاب می‌کند که حتی به هنگام ضرورت دسترسی به اطلاعات اشخاص، به‌منظور حفظ امنیت ملی، از شیوه‌های غیرقانونی و اهداف غیرقانونی استفاده نگردد؛ مثل دسترسی به حساب‌های مالی و اسرار تجاری و کسب سود تجاری از این مسیر که این امر درآمریکا نیز با تأکید رئیس‌جمهور وقت در سال ۲۰۱۳ همراه شده است (Laurent, 2015: 5-17) و توجه به این حق و دیگر حقوق شهروندان باید در شرح وظایف نهادهای مرتبط با فضای سایبر مورد توجه واقع گردد.

بر پایهٔ نظام‌های حقوقی ترسیم‌شدهٔ ارتباطی و فناوری اطلاعات، ضمانت‌اجرای‌های موجود و کاستی‌ها و نارسایی‌های نظام حقوقی ایران برای درک ضرورت قاعده‌مندسازی حمایت از حریم خصوصی کاربران اینترنتی، شناسایی و برشمرده شده است تا با امکان‌سنجی مقرراتی و قانونی، در راستای برقراری نظام حقوقی کارآمدتر و اثربخش‌تر گام برداشته شود.

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
قانون مسئولیت مدنی	مادهٔ ۱: کسی که به هرحق دیگری لطمه وارد آورد مسئول جبران خسارت وارده می‌باشد. مادهٔ ۸: کسی که با تصدیق یا انتشار به حیثیت دیگری زیان وارد کند، مسئول جبران آن می‌باشد. مادهٔ ۱۰: حق تقاضای جبران برای متضرر شناخته و دادگاه می‌تواند در صورت اثبات تقصیر علاوه بر صدور حکم به خسارت مالی، به رفع زیان از طریق دیگر از قبیل الزام به عذرخواهی و درج حکم در جراید حکم دهد.	جبران خسارت‌های مادی و معنوی ناشی از نقض حریم خصوصی در فضای فیزیکی و سایبر	شایسته است در خصوص نقض داده‌های شخصی که دامنه خساراتش گسترده‌تر و احتمال نقض آن نیز بیشتر و سهل‌تر، در صورت تبرئه متهمین و اشخاصی که حریم داده‌های آنان، توسط مقامات ذی‌صلاح، به موجب ظن قوی و دستیابی به ادله جرم، نقض گردیده، جبران صیانتی در نظر گرفته شود و اعاده حیثیت با رعایت مصالح زیان‌دیده صورت پذیرد.
قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب سال ۱۳۸۳	بندهای ۶: ایذای افراد در جریان دستگیری، بازجویی و تحقیق ممنوع است. ۸ بازرسی بدون مزاحمت بوده و از تعرض به متعلقات آنان که ارتباطی به جرم نداشته خودداری کنند و افشای مضمون نامه‌ها، عکس‌های خانوادگی ممنوع شده است. ۱۱ پرسش مرتبط با اتهام باشد و ازکنجکاوی در اسرار شخصی احتراز گردد.		قانون‌گذار به حریم خصوصی شهروندان و احترام به شخصیت و روابط شخصی توجه داشته لیکن برای اجرای بهینه قانون، ضمانت‌اجراهای بازدارنده از نقض حریم خصوصی توسط ضابطین و مامورین، ضرورت دارد که در قوانین ایران این امر کم‌رنگ بوده و در رویه قضایی به ندرت برخورد با ناقضین این حریم مشاهده شده است. شایسته است مجازات مقامات، مامورین و ضابطین ناقض این حریم خصوصاً در خصوص داده‌های شخصی الکترونیکی، علنی باشد
قانون مطبوعات ۱۳۶۴ و اصلاحی ۱۳۷۹	ماده ۳۱ - انتشار مطالبی مشتمل بر تهدید به هتک شرف و یا حیثیت و یا افشای اسرار شخصی، ممنوع است.	توقف انتشار و برخورد با ناقضین حریم خصوصی و مدیران نشریات متخلف (رسانه‌های فیزیکی و الکترونیکی با توجه به تسری این قانون به نشریات الکترونیکی)	
قانون تجارت	ماده ۵- هر گونه تغییر در تولید، ارسال، دریافت ذخیره و یا پردازش داده پیام با توافق و قرارداد خاص طرفین معتبر است.	. برای ناقضین این حق مجازات از جمله	از حریم داده‌های شخصی اشخاص حمایت به عمل آمده و بسیاری از جنبه‌ها از جمله مشخص بودن هدف در شرایط

	مفاد قانون یا مقرره	ضمانت‌اجرا	چالش‌های موجود و راهکار
الکترونیکی مصوب سال ۱۳۸۲	ماده ۵۸- ذخیره، پردازش و یا توزیع داده‌های شخصی داده بدون رضایت صریح آن‌ها غیر قانونی است. ماده ۵۹- در صورت رضایت،دسترسی تحت شرایط زیر باشد: - اهداف آن به طور واضح شرح داده شده باشند. - داده پیام به اندازه ضرورت و برای اهداف تعیین شده مورد استفاده قرار گیرد. د- شخص موضوع داده پیام به پرونده‌های رایانه‌ای خود دسترسی داشته و بتواند داده پیام‌های ناقص یا نادرست را محو یا اصلاح کند. ه- شخص موضوع داده پیام بتواند درهر زمان درخواست محو کامل پرونده رایانه‌ای خود را بنماید. ماده ۶۵- به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیر قانونی اسرار تجاری جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید	حبس تعیین نموده است.	دسترسی ذکر گردیده و شناسایی داده‌ها به‌عنوان مال در ماده ۶۵ و در صورت لزوم بهره‌مندی از قانون مدنی برای حمایت از مالک داده، امکانپذیر می‌باشد لیکن در زمان اجرا، به دلیل ابهام در تقسیم‌بندی، به‌عنوان مال منقول یا غیرمنقول، عملاً نهادهای اجرایی و قضایی را با چالش مواجه ساخته و باعث می‌شود امکان حمایت مؤثر از داده‌های شخصی، میسر نگردد.
قانون مجازات اسلامی	**ماده۷۲۹ـ (۹۵۲)** دسترسی غیرمجاز به داده‌ها یا سامانه‌ها که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۵/۰۰۰/۰۰۰ ریال تا ۲۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات محکوم خواهدشد. **ماده۷۳۰ـ (۹۵۳)** شنود غیرمجاز ارتباطات غیرعمومی مستوجب حبس از شش ماه تا دو سال یا جزای نقدی از ۱۰/۰۰۰/۰۰۰ ریال تا ۴۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات خواهدبود. **ماده۷۴۰ (۹۶۳)ـ** ربودن غیرمجاز داده‌های متعلق به دیگری، چنانچه عین دادها در اختیار صاحب آن باشد مستوجب	دسترسی غیرمجاز به اطلاعات خصوصی اشخاص جرم محسوب و مشمول مجازات می‌شود.	۱. مجازات‌های مقرر در این قانون نمی‌تواند جنبه بازدارندگی مؤثر داشته باشد چون مجازات نقدی مبلغ قابل توجهی نیست و اصولاً مجازات حبس نیز اعمال نمی‌گردد. مضاف بر اینکه مجازات‌های جایگزین حبس مؤثرتر می‌باشد. جا داشت مبالغ جزای نقدی نوعی و ثابت نبوده و شخصی و بنا به شرایط وکارشناسانه در نظر گرفته می‌شد. ۲. طبق مواد (۹۸۶) تا (۹۸۹) قانون مجازات اسلامی، دسترسی به داده‌های ترافیک و اطلاعات کاربران خدمات دسترسی و بهره‌برداری از داده‌ها تنها توسط ضابطان و با اجازه مقام قضایی

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
	جزای نقدی از ۱/۰۰۰/۰۰۰ ریال تا ۲۰/۰۰۰/۰۰۰ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۵/۰۰۰/۰۰۰ریال تا ۲۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات خواهد شد. **ماده۷۴۱ (۹۶۴)ـ** هرکس به طور غیرمجاز از سامانه با ارتکاب اعمالی از قبیل وارد کردن، تغییر داده‌ها یا مختل کردن سامانه، هر منفعت یا امتیازات مالی تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از (۲۰/۰۰۰/۰۰۰) ریال تا (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. **ماده۷۴۴ـ** (۹۶۷)هرکس به وسیله فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از (۵/۰۰۰/۰۰۰) ریال تا (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. **تبصره ـ** چنانچه تغییر یا تحریف مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد. **ماده۷۴۵ـ (۹۶۸)** هر کس به وسیله سامانه صوت یا تصویر یا فیلم خصوصی یا اسرار دیگری را بدون رضایت منتشر کند یا دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از (۵/۰۰۰/۰۰۰) ریال تا			امکان‌پذیر است. که برابر مادهٔ ۶۹۸ قانون آیین دادرسی کیفری مصوب ۱۳۹۳ صریحاً نسخ گردیده و تحت قانون اخیرالذکر ساماندهی شده است. هرچند از لحاظ مفاد تغییری نداشته و شایسته است قانون‌گذاران نسبت به اصلاح شیوه دسترسی، تفتیش و توقیف مبادرت نمایند.

	مفاد قانون یا مقرره	ضمانت‌اجرا	چالش‌های موجود و راهکار
	(۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد. **ماده۷۴۶ (۹۶۹)ـ** هر کس به قصد اضرار به غیر به وسیله سامانه نشر اکاذیب نماید یا با همان مقاصد اعمالی را بر خلاف حقیقت، به شخص دیگری نسبت دهد، افزون بر اعاده حیثیت (در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از (۵/۰۰۰/۰۰۰) ریال تا (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.		
قانون آیین دادرسی کیفری مصوب ۱۳۹۲ و اصلاحی ۱۳۹۴	ماده۶۵۸ـ تمهیدات فنی و قانونی لازم برای حفظ حریم خصوصی و امنیت داده‌های شخصی فراهم آید. ماده۶۶۰ـ اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد را فراهم به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از دو تا ده سال محکوم خواهند شد. ماده ۶۶۱- اشخاصی که مسئول نگهداری اطلاعات موضوع این بخش هستند موجبات ارتکاب جرائم رایانه‌ای به‌وسیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از شش ماه تا دو سال یا انفصال ازخدمت تا پنج سال یا جزای‌نقدی از ده تا صدمیلیون ریال محکوم خواهند شد. ماده ۶۷۱ ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد.	در مواد ۶۶۰ و ۶۶۱ ضمانت‌اجرا برای جبران نقض صیانت از داده‌ها حبس یا جریمه نقدی و انفصال از خدمت درنظر گرفته شده	۱. در مواد ۶۶۰ و ۶۶۱از آنجا که پیامدهای نقض بسته به مورد متفاوت است می‌بایست متناسب با شرایط بزه‌دیده یا بزه‌دیدگان، فرایند جبران مشخص گردد و همه جنبه‌های مادی و معنوی را دربرگیرد. و ضرر ناشی از همه ناهنجاری‌های صیانتی جبران‌پذیر باشد که این مهم خصوصاً با تدقیق در مفاد مادۀ ۶۶۱ نمی‌تواند جنبه بازدارندگی مؤثر داشته و تامین کننده عدالت و جبران کننده حقوق تضییع شده اشخاص باشد و می‌بایست مجازات انفصال خدمت همراه جریمه نقدی در نظر گرفته شود. و در صورت رضایت شخص بزه‌دیده جبران تنبیهی متناسب پیش‌بینی شود ۲. اعاده حیثیت با رعایت مصالح زیان‌دیده اعمال شود. ۳. با توجه به اهمیت حریم خصوصی در فضای سایبر در مواقعی که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم از طریق دسترسی به داده‌ها، وجود دارد پرونده به شعبه‌های خاص استانی و به هیات قضایی متشکل از قضات با تجربه ارجاع گردد. و افرادی هم که اجازه

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
	ماده ۶۷۲ ـ تفتیش و توقیف داده‌ها یا سامانه ها در حضور متصرفان قانونی انجام می‌شود. درغیر این‌صورت چنانچه تفتیش یا توقیف ضرورت داشته قاضی با ذکر دلایل دستور تفتیش و توقیف را صادر می‌کند. ماده ۶۷۵ ـ در توقیف داده‌ها، با رعایت تناسب نقش آن‌ها در ارتکاب جرم، به روشهایی از قبیل چاپ داده‌ها از تمام یا بخشی از داده‌ها، با روشهایی از قبیل تغییرگذرواژه عمل می‌شود.		دسترسی،جستجو و پایش اطلاعات دارند، محدود گردند. ۴. از آنجا که اصولاً نقض حریم خصوصی توسط مقامات دولتی یا اشخاص تحت نظارت آن‌ها راحت‌تر صورت می‌پذیرد، اتخاذ تدابیر پیشگیرانه امنیتی و آموزش به شهروندان و نیز اعمال مجازات سنگین‌تر می‌تواند مؤثر واقع شود. و از بروز مشکلات که عملاً در کشور در خصوص نقض حریم خصوصی و دسترسی به داده‌ها، وجود دارد جلوگیری شود. همانگونه که ارسال پیامک به رانندگان اسنپ مبنی بر حذف نرم افزار مسیریاب ویز[1] شبهه دسترسی شرکت حمل و نقل اسنپ را در جامعه ایجاد کرد. حتی اگر اذن دسترسی، پایش و جستجو این شرکت به دستور دادستانی کل کشور صورت گرفته باشد نیز خلاف قانون می‌باشد زیرا مرجع قضایی حق صدور احکام کلی را نداشته است. نقض و محدودیت با صدور احکام کلی توسط مقام ذیصلاح قضایی شاید صرفاً در مواردی که خطر جدی و قریب‌الوقوع امنیتی باشد قابل توجیه به‌نظر برسد. لذا اذن دسترسی به حریم خصوصی یک استثناست که باید در موارد محدود و شفاف صورت پذیرد، آن‌هم توسط عده محدود، و مجاز به نظر نمی‌رسد، به خاطر نصب یک نرم‌افزار ممنوع، یک شرکت خصوصی امکان دسترسی به داده‌های گوشی همراه رانندگان و مسافران خود را داشته باشد.

1. waze

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
			۵. الزام قانونی برای حضور مقام قضایی در زمان دسترسی و تفتیش داده‌ها، در نظر گرفته شود چرا که نقض حریم خصوصی، نقض یک حق بنیادی است که هم ممکن است زمینه‌ساز جرایمی نظیر قتل کلاهبرداری گردد و هم زندگی خصوصی و خانوادگی که حفظ ارکان خانواده و تقویت آن از سیاست‌های کلان نظام می‌باشد، مورد تهدید قرار گیرد. با حضور مقام قضایی نظیر دادیار احتمال بهره‌برداری ناروا کمتر و تضمین حریم و حیثیت کاربران بیشتر می‌شود
قانون انتشار و دسترسی آزاد به اطلاعات	**ماده ٦** -درخواست دسترسی به اطلاعات شخصی تنها از خود اشخاص یا نماینده قانونی آنان پذیرفته می‌شود. **ماده ١٤**- چنانچه اطلاعات درخواست شده مربوط به حریم خصوصی اشخاص باشد و یا در زمره اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود. **ماده ١٥**- موسسات مشمول این قانون در صورتی که پذیرش درخواست متقاضی متضمن افشای غیرقانونی اطلاعات شخصی درباره یک شخص حقیقی باشد باید از در اختیار قرار دادن اطلاعات درخواست شده خودداری کنند، مگر آنکه: **الف**- شخص ثالث به نحو صریح و مکتوب به افشای اطلاعات خود رضایت داده باشد. **ب**- شخص متقاضی، ولی یا قیّم یا وکیل شخص ثالث، در حدود اختیارات خود باشد. **ج**- متقاضی یکی از موسسات عمومی باشد و اطلاعات درخواست شده در	۱. تدابیر پیشینی برای سواستفاده از دسترسی به اطلاعات و نقض حریم خصوصی در نظر گرفته شده است و منوط به رضایت پیشینی شخص، شده است. ۲. برابر این قانون، رضایت باید صریح و استنادپذیر باشد و در صورت ادعا بتوان پاسخ معتبر و مستدلی ارائه کرد. ۳. در ماده ١٤ دسترسی به اطلاعات راجع به حریم خصوصی اشخاص منوط به رضایت آنهاست	۱. جا داشت امکان نظارت رایگان ذی‌نفع یا ذی‌نفعان نیز در قانون مدنظر قرار می‌گرفت تا میزان دسترسی به داده‌ها طور دقیق و شفاف تعیین می‌شد و امکان پیشگیری از نقض حریم داده‌ها با کمترین هزینه و آسیب فراهم باشد. ۲. برابر این قانون رضایت باید صریح باشد به این معنا که ضمنی یا همراه با سایر موضوعات دریافت نگردد و استنادپذیر باشدو در صورت ادعا بتوان پاسخ معتبر و مستدلی ارائه کرد. ۳. برای رفع ابهام و بروز مشکلات احتمالی درج رضایت باید آگاهانه باشد می‌توانست اثربخشی قانون در احترام به داده‌های شخصی را ارتقا دهد. به این معنا که مالک داده‌ها درباره همه جنبه‌های موضوع صیانت، آگاهی مشخص و متمایزی داشته باشد.برای رفع ابهام و به این معنا، که مالک داده‌ها، درباره همه جنبه‌های موضوع صیانت، آگاهی مشخص و متمایزی داشته باشد. ۴. دسترسی به اطلاعات راجع به حریم خصوصی اشخاص منوط به رضایت

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
	چارچوب قانون مستقیما به وظایف آن به‌عنوان یک موسسه عمومی مرتبط باشد.		آنهاست. و اشخاص می‌توانند مدیریت بهتری بر روی جنبه‌های حیثیتی و مالکیتی زندگی خود، داشته باشند و این یک فرصت به‌شمار می‌رود. اما از طرف دیگر کثرت مالکان داده‌ها، به ویژه در سطح کلان‌داده‌ها، می‌تواند مشکلات جدی پدید آورد. ۵. امکان بهره‌برداری موسسات عمومی از داده‌های شخصی دیگران تا جاییکه به وظایف آنان مربوط بوده، اگر درست سامان‌دهی نشود و منحصر به موارد خاص و با حکم مراجع ذیصلاح نگردد با توجه به حساسیت داده‌های شخصی، حریم و حیثیت اشخاص در معرض تهدید جدی قرار می‌گیرد. البته شیوه نامه شماره ۲۴۵۴۱۷ تاریخ ۱۳۹۸/۰۹/۱۰ موضوع مواد ۱۴ و ۱۵ قانون انتشار و دسترسی آزاد به اطلاعات با تعیین مصادیق مختبف حریم خصوصی و داده‌های شخصی از جمله مشمول حریم خصوصی دانستن اطلاعاتی که از طریق دوربین‌های منصوبه در اماکن عمومی به دست می‌آید از اقدامات مثبت دولت بوده است.
قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات	**ماده ۳.** **ف-** حفاظت و حراست از مراسلات، مکالمات و داده‌های اشخاص بر عهده وزارت ارتباطات و فناوری اطلاعات می‌باشد.		ابزارهای اجرایی و نظارتی لازم برای حفظ و صیانت از حریم خصوصی، وجود ندارد
قانون حمایت از حقوق پدید آورندگان	ماده ۱ - حق نشر، عرضه، اجرا و حق بهره برداری مادی و معنوی نرم افزار رایانه‌ای متعلق به پدید آورنده آن است. نحوه تدوین و ارائه داده‌ها درمحیط قابل پردازش	با حمایت از مالکیت معنوی، حریم داده‌ها، مورد صیانت واقع می‌شود و منافع آن	

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
نرم افزارهای رایانه ای	رایانه‌ای نیز مشمول احکام نرم‌افزار خواهد بود.	صرفاً مورد بهره برداری مالک داده‌ها قرار می‌گیرد.	
قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌کنند" مصوب ۱۳۷۹	ماده ۵- مرتکبان جرائم زیر به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم می‌شوند: الف- وسیله تهدید قراردادن آثار مستهجن ب - تهیه فیلم یا عکس از محلهایی که اختصاصی بانوان ج- تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران	حمایت از حریم خصوصی محدود به شرایطی گردیده از جمله ایتکه وسیله اخاذی واقع شود. و در مادۀ ۴ این قانون نیز در واقع حیثیت و حریم خصوصی مورد توجه قرار گرفته که مقرر می‌دارد، اگر به بهانه انتشار عکس فرد را وادار به زنا کند به مجازات زنای به عنف و اگر عمل ارتکابی غیر از زنا و مشمول تعزیر باشد به حداکثر مجازات محکوم می‌گردد.	اگرچه در این قانون تهیه فیلم یا عکس از محل‌های اختصاصی بانوان و یا عکس مبتذل از مراسم خانوادگی را مشمول مجازات دانسته اما با مصادیق تعیین شده حریم شخصی و داده‌های شخصی در مصوبه شماره ۴۵۴۱۷ تاریخ ۱۳۹۸/۰۹/۱۰ و داده شخصی خواندن عکس افراد و فیلمی که بدون اذن و اجازه آنان تهیه شده باشد به طور مطلق، کمک مؤثری به افراد در پیگیری حقوق آنان تحت عنوان انتشار داده‌های شخصی ونقض حریم خصوصی می‌باشد.
آیین نامه جمع اوری و استناد پذیری ادله الکترونیکی مصوب ۱۳۹۳ قوه قضاییه	ماده ۲۴- ضابطان قضایی باید کلیه اطلاعات ضرورت تفتیش و توقیف را در درخواست خود اعلام نمایند. ماده ۲۷ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود. ماده ۳۴ـ صرفاً مجاز به تفتیش و توقیف داده‌ها و سامانه‌هایی هستند که به طور صریح در دستور قضایی ذکر گردیده. ماده ۳۷ـ هنگام تفتیش رعایت موارد زیر ضروری است: الف ـ هیچ گونه تغییردر داده‌های ایجاد نشود	به حریم صیانت از داده‌ها برابر قانون توجه شده و در ماده ۳۶ آن نیز به لزوم داشتن تخصص و توانایی ضابطین، اشاره گردیده است.	در مواقع تفتیش و توقیف داده‌های شخصی، از آنجا که پیامدهای دسترسی از لحاظ روحی و معنوی، می‌تواند بسیار سنگین و غیرقابل جبران باشد، لازم است: ۱. شرایط ایجابی و سلبی اشخاصی که به تفتیش و توقیف داده‌ها، مبادرت می‌کنند، در مصوبه اعلام گردد. ۲. ضابطین خاص و مشخص برای این امر، انتخاب گردند و داشتن گواهی جداگانه و مختص تفتیش و توقیف داده‌ها الزامی‌باشد. ۳. توان ایفای تعهدات و جبران مسولیت‌های ناشی از نقض غیرضرور

مفاد قانون یا مقرره		ضمانت‌اجرا	چالش‌های موجود و راهکار
	ب ـ صرفاً در محدوده دستور قضایی انجام پذیرد. ج ـ کلیه فرایندهای انجام شده بر روی داده‌های با استفاده از روش‌های قابل تشخیص، ثبت و محافظت شود.		حریم خصوصی و داده‌ها و دسترسی نابجا و یا فاش شدن را داشته باشند. ۴. اخذ تضامین مؤثر، نیز می‌تواند در بازدارندگی از نقض حریم خصوصی ضابطین مؤثر باشد. ۵. با حضور مقام قضایی صورت پذیرد.
دستورالعمل اجرایی ارایه خدمات عمومی اجباری ارتباطات و فناوری اطلاعات مصوب کمیسون تنظیم مقررات ارتباطات	بند ۱۳ماده ۱۵ رازداری و عدم افشای اطلاعات محرمانه، بی‌طرفی در خدمات موضوع قرارداد و عدم اعمال تبعیض در مورد مشتریان و مشترکین.	این تعهدات در پروانه‌های اپراتورها، درج و توسط سازمان تنظیم مقررات که مطابق قانون نهاد حاکمیتی نظارتی بخش ارتباطی و فناوری اطلاعات می‌باشد، رصد شده و در صورت نقض این حریم، برابر مقررات برخورد خواهد شد. همانگونه که در اسفند سال ۹۶، عدم رعایت ضوابط فنی- امنیتی توسط دو اپراتور و سوء استفاده شرکت‌های طرف قرارداد آن‌ها از شماره‌های مشترکین و ارسال پیام‌های تبلیغاتی، موجب جریمه ۴۰ میلیارد ریالی آنان شد.[1]	به دلیل ضعف قانونی- مقرراتی و عدم پیش‌بینی راهکارهای نظارتی دقیق و شفاف، عملاً حریم خصوصی و داده‌های اشخاص، مورد بهره‌برداری ارگان‌ها و شرکت‌های مختلف واقع می‌گردد.

1. www.cra.ir, ۲۳ اسفند ۱۳۹۶

نتیجه

تکنولوژی ارتباطی و فناوری اطلاعات، بسان تکنولوژی‌های دیگر که با انگیزهٔ خدمت و رفاه بشری پدید آمده است و گسترش می‌یابد، اثر دوگانه دارد: هم می‌تواند مطلوب جامعهٔ بشری واقع گردد و هم می‌تواند دارای جنبه‌های منفی و تهدیدکنندهٔ حقوق بشری باشد که حقوق افراد جامعه را تحت تأثیر قرار می‌دهد. از آنجا که دامنهٔ استفاده از فضای سایبر محدود به جغرافیای خاصی نیست، در صورت عدم ساماندهی و استفادهٔ ناصحیح از آن ممکن است بر حقوق شهروندان جامعهٔ جهانی از جنبه‌های مختلف اثر گذارد و موجب نقض حقوق شهروندی آنان به‌خصوص حق بر حریم خصوصی شود که شدیداً متأثر از تکنولوژی است. لذا ساماندهی این فضا، نیازمند سازکارهای تقنینی و مقرراتی صحیح متناسب با مقتضیات آن فضا خواهد بود. حتی آن دسته از قوانینی که برای صیانت از حقوق بنیادی بشری وضع گردیده و لازم‌الاجرا شده‌اند نیز شاید نیازمند بازنگری و بازآفرینی برپایهٔ اندیشه‌های نوآورانه و سازگار با دنیای نوین باشند و دولت باید با پیش‌بینی مکانیزم‌های کارآمد از حقوق اساسی شهروندان خود در برابر تهدیدها و آسیب‌های ناشی از بسط و توسعهٔ تکنولوژی صیانت به عمل آورد. اگرچه نمی‌توان انکار کرد که وقوع برخی جرایم از جمله جرایم امنیتی ممکن است موجبات نقض حریم خصوصی اشخاص را فراهم نماید، نقض این حریم یا اعمال محدودیت توسط دولت باید موجه و مبتنی بر قانون باشد. مسئلهٔ دیگری نیز که در وهلهٔ اول با حریم داده‌های شخصی در تضاد است، تجارت آزاد، کسب‌وکارهای آنلاین و استفادهٔ شرکت‌های بزرگ از برخی داده‌های اشخاص و حق بر دسترسی می‌باشد که واقعیت دنیای اقتصادی امروز، آن را اجتناب‌ناپذیر می‌سازد و بازنگری در اصول حاکم بر حریم و داده‌های شخصی را ایجاب می‌کند. به‌جای اینکه پیش‌فرض، ممنوعیت و محدودیت دیگران و حاکمیت محض دارندهٔ حریم و داده‌های شخصی قرار گیرد، باید قاعدهٔ «بهره‌برداری منصفانه»را بنیان نهاد. ازاین منظر، ایجاد توازن و تعادل میان حفظ داده‌های شخصی و بهره‌برداری اصولی از آن، تأمین‌کنندهٔ منافع دو یا چندجانبه خواهد بود و دیگر تحکیم و تحکم یک‌سویه وجود ندارد. شایسته است نهادهای سیاست‌گذار، اجرایی و نظارتی برای کاهش آسیب‌ها و بزه‌دیدگی در برقراری توازن منطقی در این فضا تلاش کنند. وضع قوانین و قواعد دقیق در صیانت از این حق بشر، مؤثر می‌باشد؛ چراکه بی‌توجهی به این امر با امکان سهولت دسترسی به داده‌ها و تخریب آنان، سایر حقوق شهروندان، نظیر حق بر کار را نیز متأثر می‌سازد.

در قوانین ایران حمایت از حریم خصوصی تحت حمایت از اشخاص در برابر هتک حرمت، حیثیت و مال و... به کار رفته است اما هنوز چالش‌های زیادی در صیانت از حریم خصوصی و داده‌های شخصی وجود دارد که به منظور رفع و کاهش تهدیدهای این حوزه پیشنهاد می‌گردد:

۱. ساز و کارهای مؤثر قانونی برای بازدارندگی از نقض حریم خصوصی در فضای سایبر پیش بینی گردد و تمهیدات لازم برای صیانت از کاربران فضای سایبر وضع و لازم‌الاجرا کرد.

۲. کمیته صیانت از حریم خصوصی شهروندان در فضای سایبر متشکل از حقوقدانان زبده (نمایندگان قوه قضاییه)، کارشناسان فنی و حقوقی (نمایندگان سازمان تنظیم مقررات و ارتباطات رادیویی)، نماینده شورای عالی امنیت ملی، نماینده شورای عالی فضای مجازی و نماینده اپراتورها تشکیل گردد.

۳. موارد دسترسی به اطلاعات و داده‌های شخصی، به طور شفاف در قوانین تبیین شده و مجازات نقض کنندگان آن، در هر منصب و مقامی نیز مشخص و بدون تبعیض باشد. تا امکان دو گانگی در اجرا، میسر نگردد از طرف دیگرف اشخاصی که حق دسترسی به این اطلاعات و داده‌ها را دارند، محدود و مشخص باشند.

۴. تشریفات غیرضرور اداری و قضایی در پرونده‌های مرتبط به نقض حریم خصوصی، با هدف کاهش پیامدهای ناشی از نقض این حریم هم از جنبه معنوی وهم تحت تاثیر قراردادن سایر حقوق و زمینه ساز شدن وقوع جرایم دیگر، برچیده شده و این پرونده‌ها خارج از نوبت رسیدگی شوند.

۵. الزام قانونی برای ارجاع پرونده‌های نقض حریم خصوصی در فضای سایبر، به کارشناسان فنی، لحاظ گردد.

منابع

فارسی

- آقایی طوق، مسلم (۱۳۹۸)، «تدوین شکلی؛ حلقه مفقوده نظام تدوین و تنقیح قوانین و مقررات کشور»، **مجله حقوقی دادگستری**، شماره ۱۰۶.
- انصاری، باقر (۱۳۹۱)، **حقوق حریم خصوصی**، تهران: سازمان مطالعه و تدوین کتب علوم انسانی (سمت).
- جعفری، علی و محمدرضا رهبرپور (۱۳۹۶)،«مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه»، **فصلنامه پژوهش حقوق خصوصی**، شماره ۱۸.
- جلالی فراهانی،امیرحسین (۱۳۸۴)، **پیشگیری از جرایم رایانه‌ای**، پایان نامه برای دریافت درجه کارشناسی ارشد، تهران: گروه حقوق جزا و جرم‌شناسی دانشگاه امام صادق.
- راعی، مسعود (۱۳۸۹)، «حریم خصوصی و امر به معروف و نهی از منکر»، **نشریه حکومت اسلامی**، شماره ۲.
- ساریخانی، عادل و ایمان محترم قلاتی (۱۳۹۸)، «تعامل ضابطان دادگستری با حریم خصوصی خودروها»، **مجله حقوقی دادگستری**، شماره ۱۰۵.
- طهماسبی، جواد و خیراله شاهمرادی (۱۳۹۷)، «چالش‌ها و خلاهای موجود در رسیدگی به جرایم سایبری»، **مجله حقوقی دادگستری**، شماره ۱۰۴.
- عبدالهی، محبوبه و مرتضی شهبازی نیا (۱۳۸۸)، «سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی»، **مجله پژوهش‌های حقوقی**، شماره ۱۶.
- فتحی، یونس و خیراله شاهمرادی (۱۳۹۶)، «گستره و قلمرو حریم خصوصی در فضای مجازی»، **مجله حقوقی دادگستری**، شماره ۹۹.
- مقامی، امیر و نادیا عطاران (۱۳۹۸)، «موازنه افشای حریم خصوصی خانوادگی چهره‌های مشهور در رسانه‌ها و آزادی بیان در رویه نهادهای قضایی»، **فصلنامه مطالعات حقوق عمومی**، شماره ۲.
- نوری، محمدعلی و رضا نخجوانی (۱۳۸۳)، **حقوق حمایت داده‌ها**، تهران: کتابخانه گنج دانش.

غیرفارسی

- Baihua, Wen (2016), "An Assessment of the Strategic Situation in Cyberspace", **International Strategic Relations and China's National Security**, vol.2.
- Choi, Jay Pil &others (2019), "Privacy and personal data collection with information externalities", **Journal of Public Economics**, vol.173.
- De George, Richard T (2018), privacy, "Public Space and Personal Information", **The Philosophical Foundations of Law and Justice**, vol.8.
- Grech, Victor, Hugo Agius-Muscat (2018), "WASP (Write a Scientific Paper): **Data protection", a guide for health researchers**,vol,124.
- Guinchard, Audrey (2010), **Human Rights in Cyberspace**, Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694483> (last visited on 21/10/ 2010).
- Hyun Jin, Chang (2018), "Self-Concepts in Cyber Censorship Awareness and Privacy Risk Perceptions: What Do Cyber Asylum-Seekers have?", Computers in Human Behavior,volume 80.

- Laurent, Sébastien-Yves (2015), "Liberté et sécurité dans un monde anomique de données", **Commission nationale de contrôle des interceptions (CNCIS) de rapport d'activité** 2013-2014 – 22e rapport.
- Monshipouri, Mahmood (2017), " Human Rights in the Digital Age: Opportunities and Constraints", **Public Integrity** ,Volume 19, 2017 - Issue 2: Symposium on the Social Practices of Human Rights.
- Santanen, Eric (2019), "The Value of protecting privacy", **Business Horizons**, Volume 62, Issue 1.
- Vatis, Michael A (2010), "The Council of Europe Convention on Cybercrime", Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy.
- Wat, Eliza (2017), **The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance**, Available at: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2006%20The%20Role%20of%20International%20Human%20Rights%20Law%20in%20the%20Protection%20of%20Online%20Privacy%20in%20the%20Age%20of%20Surveillance.pdf>
- REPORTS OF JUDGMENTS AND DECISIONS (2008)-V, **EUROPEAN COURT OF HUMAN RIGHTS**.