فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۵۰، شمارهٔ ۲، تابستان ۱۳۹۹: ۵۹۷-۶۱۶
DOI: 10.22059/jplsq.2018.261128.1778

کاربست قوانین و مقررات ارتباطی در صیانت از حریم خصوصی شهروندان در فضای سایبر

فلور قاسم‌زاده لیاسی[۱]، لیلا رییسی دزکی[۲*]

چکیده

با پیدایش و توسعهٔ فضای سایبر حمایت از حریم خصوصی شهروندان صرفاً با قواعد حقوق بشر سنتی امکان‌پذیر نیست. ازاین‌رو باید با توسعهٔ قوانین و مقررات داخلی همراستا با قواعد بین‌المللی و اقدامات فراملی، و نیز با در نظر گرفتن فناوری و شیوه های نوپدید ارتباطی و الزامات زیست در فضای سایبر و همچنین توصیه‌ها و قواعد تدوینی سازمان‌هایی مانند اتحادیهٔ بین‌المللی مخابرات و سازمان جهانی مالکیت فکری، از این حقوق مهم شهروندان صیانت کرد. در این پژوهش که به شیوهٔ توصیفی- تحلیلی است، به این مسئله پرداخته می‌شود که قوانین و مقررات ایران تا چه حد می‌تواند از حریم خصوصی شهروندان در فضای سایبر صیانت کند. بدیهی است وضع مقررات ملی بدون در نظر گرفتن گستردگی جهانی این فضا و بدون ملحوظ داشتن شرایط حاکم بر جامعهٔ جهانی و هنجارهای نوین، نه‌تنها از اثربخشی کافی بر خوردار نخواهد بود، بلکه بروز تناقضات و مشکلاتی را موجب خواهد شد.

کلیدواژگان

حریم خصوصی، حقوق شهروندی، حقوق بشر، فضای سایبر، مقررات ارتباطی.

---

۱. گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.
Email: Florence.titi2000@gmail.com
۲. گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران، دانشیار دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان) (نویسندهٔ مسئول.) Email: Raisi.leila@gmail.com
تاریخ دریافت: ۱۳۹۷/۰۴/۹، تاریخ پذیرش: ۱۳۹۷/۰۶/۱۹

مقدمه

فضای سایبر با توسعه و تسهیل شیوهٔ ارتباطی در میان اشخاص سرا سر ج هان زمی نه را برای دستیابی و آزادی‌های مختلف حقوق بشری فراهم ساخته و شاید در وه لهٔ اول گ مان رود که محدودیت‌های وارد بر این فضا با اصول و مبانی حقوق ب شری سازگار نبا شد و دو لت ها حق دخالت در این فضا را که فضایی مستقل و جهانی است ندارند، اما به‌ی قین ن می توان د یدگاه خودمراقبتی شهروندان و کاربران در فضای سایبر را که از نگاهی کاملاً آزادی‌خواهانه سرچشمه می‌گیرد، به‌طور مطلق پذیرفت، چراکه این دیدگاه نمی‌تواند تضمین‌کنندهٔ صیانت از حقوق بشر باشد، بلکه برای صیانت از حقوق بشر باید قواعد و مقرراتی وضع شود و ا گر قوانین و م قررات سایبری متناسب با تحولات فناوری اطلاعات گسترش نیابد، شاید بی شترین ا ثر من فی تو سعهٔ فناوری اطلاعات بر حریم خصوصی شهروندان نمود پیدا کند که با تهدیدهای شدیدتری موا جه می‌شوند و داده‌های شخصی راحت‌تر در دسترس همگان قرار می‌گیرد و این مسئله دولت ها را ملزم می‌سازد که برای صیانت از حقوق کاربران به وضع قوانین و مقرراتی اقدام کنند که حریم خصوصی شهروندان را مورد حمایت قرار دهد.

در این پژوهش قواعد بین‌المللی و قوانین و مقررات داخلی مرتبط با حریم خصو صی برر سی شده و به خلأهای موجود در نظام حقوقی ایران اشاره و به این موضوع پرداخته می‌شود که چگونه در فضای سایبر می‌توان صیانت از حریم خصوصی شهروندان را تضمین کرد؟ برای ارائهٔ این موضوع پس از ذکر این مقدمه، مفهوم حریم خصوصی و تأثیر فناوری اطلاعات بر آن، فضای سایبر و تزاحم ملزومات امنیت ملی با حریم خصوصی افراد، قواعد بین‌المللی مرتبط با حریم خصوصی، صیانت از حریم خصوصی شهروندان در نظام حقوقی ایران و نتیجه‌گیری تبیین می‌شود.

مفهوم حریم خصوصی و تأثیر فناوری اطلاعات بر آن

حریم خصوصی قلمرویی از زندگی فرد است که فرد نوعاً و عرفاً یا با اعلان قبلی از دی گران انت ظار دارد بدون رضایت وی به اطلاعات در مورد این قل مرو ما ند ارتبا طات خصو صی وارد ن شوند یا نظارت نکنند (انصاری، ۱۳۹۱: ۳۸-۱۱). در فضای سایبر حریم خصوصی اطلاعات و داده‌ها عبارت از اموری است که انسان تلاش می‌کند فاش نشوند، زیرا این حریم با شخصیت او در ارتباط ا ست. برخی معتقدند حق بر حریم خصوصی مختص اشخاص حقیقی است، ولی واقعیت ا ین ا ست که اشخاص حقوقی هم نوعی حریم خصو صی داده دار ند (جعفری و رهبری‌پور، ۱۳۹۶: ۴۷-۴۵). ازاین‌رو مفاهیم حریم خصوصی می‌تواند موارد متعددی را شامل شود که با ید از ن فوذ و ن ظارت دیگران مصون بماند، اگرچه این حق در شرایطی توسط دولت‌ها نادیده گرفته می‌شود.

حق حریم خصوصی در کنوانسیون‌ها و اسناد بین‌المللی و منطقه‌ای حقوق بشر پیش‌بی نی

شده است. البته علاوه‌بر اعتبار قراردادی از آنجا که این حق در زمرهٔ حقوق بشر است، به‌ع نوان یک عرف از الزام برخوردار بوده و رویهٔ مراجع بین‌المللی نیز بر ا ین م نوال ا ست (کدخـدایی، ۱۳۸۷). حق برخورداری از حریم خصوصی در مقولهٔ حقوق مدنی و سیا سی قرار می‌گ یرد و دولت نباید مانع اعمال این حق شود و در زمرهٔ تعهدات به نتیجه است، یعنی دولت باید رعا یت حقوق مذکور را تضمین کند و صرفاً تلاش و کوشش کفا یت ن می‌ک ند (ان صاری، ۱۳۹۱: ۵۳-۵۲)، بلکه صیانت از این حقوق از وظایف مسلم دولت است.

در کنار حریم خصوصی، در فضای سایبری داده‌ها نیز اهمیت بسیاری دارند. در سال ۱۸۹۰ سوءاستفادهٔ مأموران و مجریان قانون از اختیاراتشان به‌منظور مداخله در ا مور خصو صی سبب شد دو قاضی به نام‌های وارن[1] و براندیس[2] به دولت هشدار دهند که نباید به بهانهٔ اجرای قانون بدون اجازه به محیطی پا بگذارند که صاحبش حق دارد در آن خلوت ک ند. در ه مان ز مان در کشورهای اروپایی نیز حرکت‌های مشابهی صورت پذیرفت، اما به جای ب حث در مورد حریم خصوصی[3]، حمایت از داده‌ها[4] را مطرح کردند و قوانین آنها در این حوزه اغلب تحت این ع نوان به تصویب رسیده است (جلالی فرا هانی، ۱۳۸۴: ۱۲۰-۱۱۹). ا مروزه با تو جه به گ ستردگی فضای سایبر و پیوستگی این دو موضوع، این دو اصطلاح با یکدیگر اد غام شده‌ا ند و ح تی در اسناد لازم‌الاجرای منطقه‌ای یا بین‌المللی نیز به یک مفهوم و در کنار هم به‌کار می‌روند، البته با توجه به ماهیت امر و در بستر خدمات ارتباطی و فناوری اطلاعـات گرایش به سمت کاربرد عبارت «حمایت از داده‌ها» فزونی می‌یابد. از جمله در مقـررات حفا ظت از داده های عمـومی[5] سال ۲۰۱۸ که هدف خود را حمایت از حریم خصوصی هم گان در اتحاد یهٔ ارو پایی و منط قهٔ اقتصادی اروپا می‌داند. در مواد آن حمایت از داده‌ها به‌کار برده شده، لیکن در سند مر بوط به حفاظت از داده‌ها و حریم خصوصی اروپا در سال ۱۹۹۵ این دو اصطلاح در کنار هم ذ کر شده است (Directive 95/46/EC)، درحالی که حریم خصو صی و داده های شخ صی کاملاً برا بر نیستند. حریم، قلمرو است، حتی اگر تهی باشد و کافی است تعلق آن به شخص ثابت شود که می‌بایست مورد حمایت واقع شود، به همین دلیل دسترسی غیرم جاز به داده های ع مومی در حریم خصوصی جرم انگاشته شده است. مبنای ترسیم حریم، قانون، مقررات، قرارداد یا عرف است، اما داده، پیکره و مفهوم دارد و باید ارتباطش به شخص ثابت شود بسته به نوع اطلا عات عمومی، غیرعمومی یا انجمنی و خصوصی محسوب می‌شود و براساس تعریـف کمیسـیون اروپـا دادهٔ شخصی هر گونه اطلاعات مربوط به شخص مثل اطلاعات خانوادگی و دیدگاه‌های مـذهبی

1. Samuel Warren
2. Louis Brandeis
3. Privacy
4. Data Protection
5. General Data Protection Regulation (GDPR)

را در برمی‌گیرد که باید مورد حمایت واقع شود، چراکه آگاهی اشخاص غیرمجاز از آنها می‌تواند به زیانشان تمام شود. با وجود این تفکیک مطلق این دو مفهوم از یکدیگر دشوار است و در مقدمهٔ لایحهٔ «صیانت و حفاظت از داده‌های شخصی»، عمل به فتوای رهبری بر حرام شرعی بودن نقض حریم خصوصی یکی از موارد تدوین آن دانسته شده و در قسمت پاسخگویی کنترل‌گران داده، تعهدات ناشی از خط‌مشی‌های حریم خصوصی را مدنظر قرار داده که بر پیوستگی این دو مفهوم اشاره دارد. حق بر داشتن حریم خصوصی و داده‌های شخصی دو هدف را دنبال می‌کند؛ یکی اینکه ضرری به شخص وارد نشود و دیگر اینکه موجب سوءاستفادهٔ دیگران از اطلاعات شخصی فرد نگردد. اما سبک زندگی در دنیای امروز و پذیرش و ضعیت نوپدید دسترسی دیگران به اطلاعات شخصی، اقتضا می‌کند که حق بر حریم و داده های شخصی را به‌گونه‌ای بازتعریف کرد که استیفای حق بنیادی زندگی در جهان فعلی و زیست در فضای سایبر امکان‌پذیر شود. با گستردگی فضای سایبر و ترویج حمایت از داده های شخصی، به‌نظر می‌رسد هر گونه دادهٔ ترافیکی که نمایانگر هویت یا شخصیت فرد باشد، باید شخصی انگاشته شود، ازاین‌رو در راستای اجرای قانون اساسی ضابطه‌مندسازی صیانت از حریم و اطلاعات غیرعمومی از یک سو و حمایت از بهره‌برداری‌های مشروع از سوی دیگر، به‌منظور هماهنگی و هم‌افزایی مصوبات قانونی و مقرراتی صیانت از حریم خصوصی و داده‌های شخصی از ضرورتی اجتناب‌ناپذیر برخوردار است.

از آنجا که امروزه مراودات و انتقال محتوا از طریق ارتباطات الکترونیکی در فضای سایبر صورت می‌پذیرد، بحث اطمینان از صیانت داده‌های شخصی در این فضا اهمیت خاصی دارد، چراکه داده‌های فضای سایبر از طریق فناوری‌های جدید قابل کنترل هستند و دولت‌ها با توسل به اصل حاکمیت اطلاعات و داده‌ها سعی می‌کنند بر داده‌های مختلف تسلط خود را اعمال کنند. مادهٔ ۳۷ قانون امنیت سایبری جمهوری خلق چین اشعار می‌دارد که می‌بایست ذخیره‌سازی داده‌های شخصی در قلمرو چین صورت پذیرد و در جایی که برای نیازهای تجاری و کسب‌وکار ضرورت به انتقال داده‌ها باشد، باید اقدام کارشناسانه توسط بخش امنیت شبکه صورت پذیرد(Fang, 2018: 359-362) که این موارد بیانگر نظارت و دسترسی بر داده‌های شخصی است که اگر ساماندهی نشود، حریم اشخاص مورد تعرض قرار خواهد گرفت.

در روسیه قانون حفاظت از اطلاعات شخصی، شرکت‌های جمع‌آوری‌کنندهٔ اطلاعات شهروندان مانند گوگل را ملزم به انتقال سرورهای ذخیره‌کننده به داخل روسیه کرده است(Fang, 2018: 362) . امروزه در قریب به اتفاق کشورها شرکت‌های خصوصی عهده‌دار ارائهٔ خدمات اینترنتی‌اند و این داده‌ها دیگر مستقیما در اختیار دولت‌ها نیست و دولت‌ها صرفا از این اطلاعات استفاده می‌کنند. فضای سایبر این امکان را می‌دهد که آنچه را که در گذشته به‌دلیل عدم پذیرش از طرف ناشر، امکان انتشارش وجود نداشت، منتشر شود (Guinchard, 2010: 3-

(10. حتی اشخاص عادی نیز با امکان دستر سی به ا ین ف ناوری ها، به ج مع‌آوری، ضبط و نگهداری حجم انبوهی از داده‌های مربوط به حریم خصوصی ا فراد ا قدام کن ند. تو سعهٔ سریع فناوری عملاً موجب تسهیل نقض حریم خصوصی داده‌ها شده است. اگر راه‌حلی قانونی نبا شد، سبب از بین رفتن آرامش و امنیت افراد جامعه می‌شود (جعفری و رهبری‌پور، ۱۳۹۶: ۴۴). اما نکتهٔ قابل تأمل این است که نظارت در فضای سایبر، نامرئی بوده و به‌دلیل تسهیل دسترسی و تبادل اطلاعات، انتظار آزادی در فضای سایبری بیشتر است (فتحی و شاهمرادی، ۱۳۹۶: الف ۲۵۰-۲۴۹)، ازاین‌رو تهدیدهای حریم خصوصی در فضای سایبر قابل درک نیست و حفظ حریم خصوصی افراد به‌دلیل سهولت دسترسی به داده‌های اشخاص مهم‌تر از گذشته است. جا دارد دولت تدابیر پیشگیرانه‌ای را در طراحی سیستم‌های ارتباطی مدنظر قرار دهد تا دستر سی به اطلاعات دیگر کاربران ممکن نباشد و تنها زمانی به داده‌های شخصی طرف برا ساس قوانین و مقررات دسترسی پیدا کرد که آن شخص نسبت به قوانین یا حقوق دیگران تعرض کرده باشد و ناهنجاری را در جامعه دامن زند. در این زمینه علاوه‌بر تصویب قوانین کارامد، آموزش‌های لازم نیز به کاربران ارائه شود. ازاین‌رو شهروندان باید اطمینان دا شته با شند که داده های آ نان در فضای سایبر مصون از تعرض است.

یکی دیگر از شرایط حریم خصوصی، از بین رفتن اطلاعات به مرور زمان است، درصورتی‌که در فضای سایبر اطلاعات دائمی درج می‌شوند و این خود نیز تهدید حریم خصوصی است. با پیشرفت فناوری اطلاعات و بالطبع دنیای داده‌های ع ظیم یـ کی از چالش های بزر گی که در آینده به‌طور جدی‌تر در برابر بشر نمایان خواهد شد، هتک بالقوهٔ حرمت‌هاست که داده های آن بسیار ساده‌تر از گذشته در اختیار هر کسی قرار می‌گیرد، ازاین‌رو صیانت از این حق شهروندان بسیار اهمیت می‌یابد و با حساسیت بیشتری باید مورد توجه قرار گ یرد، ازا ین‌رو همرا ستا با موازین بین‌المللی سیاستگذاران تقنینی- مقرراتی باید به آن تو جه کن ند و رسیدگی صیانتی خود نباید به زیان یا آسیب صیانتی بینجامد. همهٔ مراحل رسیدگی صیانتی باید با رعایت ضوابط و الزامات استنادپذیری ادله انجام گیرد و در تعیین و ترسیم حوزه‌های قضایی، اداری و مدنی، تا حد امکان شرایط زیان‌دیدگان صیانتی لحاظ شود.

فضای سایبر و تزاحم ملزومات امنیت ملی با حریم خصوصی افراد

به مدد پیشرفت فناوری، تروریسم بزرگ‌ترین تهدید برای امنیت ملی کشورهاست و امروز تروریست‌های اطلاعاتی می‌توانند با ورود به سیستم‌های رایانه‌ای امنیتی، آسیب‌های امنیتی جدی ایجاد کنند و موجب بحران‌های حاد شوند، ازاین‌رو علاوه‌بر اعمال مجازات، اتخاذ تدابیر پیشگیرانه برای تحقق امنیت ملی ضرورت پیدا می کند که این تدابیر در برخی مواقع در تقابل

با حریم خصوصی قرار می گیرد و امکان رهگیری ارتباطات در فضای سایبر توسط دولت را فراهم می‌سازد (فتحی و شاهمرادی، ۱۳۹۶: ب ۱۵-۱). اگرچه به دلایل امنیتی و مبارزه با تروریسم محدودیت‌های وارد بر حریم خصوصی و داده‌های شخصی قابل پذیرش است و اعلامیهٔ جهانی حقوق بشر و میثاق بین‌المللی حقوق مدنی و سیاسی نیز حفظ امنیت ملی را مجوزی برای تحدید حق بر حریم خصوصی دانسته است، اما در مواردی که تهدید امنیتی قریب‌الوقوع باشد و تدبیرهای پیشگیرانه، پیش‌دستانه یا واکنشی بدون نقض صیانت امکان‌پذیر نباشد یا زیان‌های مادی و معنوی ناشی از رعایت الزامات صیانتی به‌مراتب بیشتر یا جبران‌ناپذیر باشد، متناسب با نوع تهدید، صیانت از داده‌ها محدود یا متوقف می‌شود. امروزه در غرب به رهبری آمریکا کمپین «مبارزه با تروریسم» راه افتاده و به همین بهانه برای دسترسی به ایمیل‌ها و اطلاعات خصوصی افراد در سراسر جهان تلاش می‌کنند و تهدید حریم خصوصی از بزرگ‌ترین مشکلاتی است که با توسعهٔ فضای سایبر شهروندان را دچار مشکل ساخته است (Monshipouri, 2017: 129-133). در سال ۲۰۱۶ وزیر دفاع فرانسه نیز اعلام داشت که توسعهٔ فضای سایبر ابزارهای متعددی را برای حملهٔ سایبری فراهم ساخته و گستردگی و در دسترس بودن این سلاح‌ها چالش جدی برای امنیت فرانسه ایجاد می‌کند، اما دولت فرانسه باید برای مقابله با آن و تأمین امنیت کشور و شهروندان از پتانسیل‌های قانونی مطابق با تعهدات بین‌المللی استفاده کند (Géry, 2018: 307). با وجود این اصولا دولت‌ها ناقض بزرگ حریم خصوصی در فضای سایبر هستند و در دوگانهٔ حریم خصوصی و امنیت به بهانهٔ امنیت رد یابی و رصد کردن فعالیت افراد در فضای سایبری در دستور کار دولت‌ها قرار می‌گیرد. با این توجیه که آزادی‌های مدنی و سیاسی جزء حقوق قیدپذیر است و در تعارض میان دو مصلحت «حفظ حقوق امنیت ملی» و «حفظ حریم خصوصی» می‌بایست به نفع مصلحت گسترده‌تر حکم کرد، برای برقراری امنیت حریم خصوصی شهروندان را نقض می‌کنند (فتحی و شاهمرادی، ۱۳۹۶: الف ۲۳۹)، اما باید توجه داشت نقض حریم خصوصی در چالش با تهدیدهای امنیتی و تروریسم سایبری بدون رعایت قانون و ملحوظ قرار نگرفتن تناسب تحدید حریم خصوصی با اقدام صورت‌گرفتهٔ نقض حقوق شهروندی و خلاف قواعد حقوق بشری است و می‌تواند موجبات مسئولیت بین‌المللی دولت را فراهم سازد. بنابراین از یک طرف امنیت به‌عنوان یک مفهوم حاکمیتی نیازمند اتخاذ اقداماتی است که ممکن است به محدودیت یا تعلیق برخی از حقوق مرتبط با حریم خصوصی افراد منجر شود و از سوی دیگر، گاهی ممکن است اقدامات افراد در چارچوب حریم خصوصی‌شان تهدیدی برای امنیت ملی باشد. از همین‌رو، هنر باید در برقراری توازن بین این دو باشد. امنیت ملی نباید بهانه‌ای برای نقض حریم خصوصی و رعایت حریم خصوصی نباید بهانه‌ای برای اتخاذ اقدامات علیه امنیت ملی باشد. وجود قوانین و مقررات شفاف در این زمینه می‌تواند تا حدود زیادی به برقراری این توازن کمک کند.

قواعد بین‌المللی مرتبط با حریم خصوصی

مادۀ ۱۲ اعلامیۀ جهانی حقوق بشر اعلام می‌دارد زندگی خصو صی ا فراد نبا ید مورد مداخ لۀ خودسرانه قرار گیرد و افراد باید در برابر چ نین تعر ضاتی از حما یت قانون بر خوردار با شند. اگرچه سانسورهایی که با نظارت مقامات حکومتی در خصوص داده های ف ضای سایبر صورت می‌گیرد جنبۀ مثبت هم دارد، چرا که دستر سی به اطلا عات گذ شته در موارد بروز جرائم می‌تواند در کشف جرائم بسیار مؤثر باشد یا از انتقال اطلاعات نادرست به جام عه و پیا مدهای آن جلوگیری کند، اما با تهدید حریم خصوصی و نقض حقوق بشر حق آزادی ب یان ا فراد ن یز تضعیف می‌شود و در درازمدت بی‌اعتمادی را در جامعه رواج می‌دهد و نگرا نی از ن قض حریم خصوصی موجب پناهندگی سایبری شهروندان می‌شود (Hyun Jin, 2018: 380-387). ب نابراین با توجه به تحولات گستردۀ جهانی ناشی از فناوری اطلاعات جا دارد که اج ماع ج هانی برای حریم خصوصی و ساماندهی حقوقی در فضای سایبر برای صیانت از این حق صورت پذیرد.

در مادۀ ۱۷ میثاق بین‌المللی حقوق مدنی سیاسی درج شده که هیچ‌کس نباید خودسرانه در زندگی شخصی افراد مداخله کند و هر کسی در برابر چنین تعرضی حق دارد از حمایت‌های قانونی برخوردار باشد. ملاحظه می‌شود که این میثاق اجازۀ مداخله در حریم خصوصی را نمی‌دهد و حمایت‌های قانونی را در برابر این تعرض ضروری می‌داند. ا مروزه حریم خصو صی ارتباطات با ظهور اشکال جدید مراسلات همچون پست الکترونیکی با مسائل جدیدتری رو به‌رو شده است (نوری و نخجوانی، ۱۳۸۳: ۳۴) و گسترش فضای سایبر زمینه را برای تهد ید بی شتر حریم خصوصی فراهم آورد. یکی از اسناد مهم در این زمینه، کنوانسیون جرائم سایبر ا ست. از آنجا که این کنوانسیون جنبۀ الزام‌آور دارد، می‌توان امیدوار بود کشورهای عضو مجبورند تدابیر کیفری خود را که عملاً بخش مهمی از این اقدامات به حریم خصوصی ا فراد در ف ضای سایبر مربوط می‌شود، به‌نحوی تنظیم کن ند که به آن ها ت عرض ن شود. بدیهی ا ست با تو جه به مشابهت‌هایی که میان تدابیر نظارتی پیشگیرانه و تعق یب و پی گرد جرائم سایبر و جود دارد، می‌توان نتیجه گرفت که این کنوانسیون به طریق او لی ن سبت به تدابیر پی شگیرانه ن ظارتی صادق است (جلالی فراهانی، ۱۳۸۴: ۱۲۱-۱۱۹). مفاد این کنوانسیون بیانگر نگرانی دولت های عضو در لزوم صیانت از حریم خصوصی در فضای سایبر است و بی شک موفق یت ک شورها در تضمین این حق شهروندی با همکاری همدیگر برای و ضع قوا عد م شترک ساماندهی ف ضای سایبر و تو سعۀ قوانین و م قررات م لی مر بوط به حریم خصو صی شهروندان متنا سب با پیشرفت‌های حاصل از فناوری اطلاعات و تأثیر آن در سبک ز ندگی نوین و ح قوق اسا سی اشخاص است.

علاوه‌بر موافقت‌نامه‌های بین‌المللی و منطقه‌ای، آرای داد گاه های بین‌الملل ی و منط قه‌ای

به‌خصوص دادگاه اروپا که انعکاس‌دهندهٔ استانداردهای حقوق بشری است نیز می‌تواند مؤثر باشد که در ۶ اکتبر ۲۰۱۵ دادگاه اروپا[1] موافقتنامهٔ بین آمریکا و اتحادیهٔ اروپا را که در خصوص حفظ امنیت سایبر منعقد شده بود، به‌دلیل تهدید حریم خصوصی و حمایت از داده‌ها تعلیق کرد و معتقد بود تعهد انتقال داده‌های شهروندان اروپایی به برخی از شرکت‌های آمریکایی نقض حریم خصوصی است و اتحادیهٔ اروپا طبق دستورالعمل 95/46/EC ملزم به حفاظت از داده‌های شهروندان خود است و انتقال داده‌ها به کشور ثالث صرفاً در صورتی امکان‌پذیر است که از سطح حمایت تضمین‌شده برخوردار باشند، درحالی که ایالات متحده از این استاندارد برخوردار نبوده و واجد شرایط نیست، اگر چه حملات نوامبر ۲۰۱۵ در پاریس، موجب بروز انتقادهای مختلفی از مسئولان اروپایی شد، اما در نهایت، اروپایی‌ها استراتژی‌های انعطاف‌پذیری را برای امنیت فضای سایبر ارائه می‌دهند (Baihua, 2016: 282-283). یک عضو پارلمان اروپا بیان داشت که قانون نظارت بر شهروندان شرکت‌ها را مجاز به افشای داده‌های جمع‌آوری‌شده اشخاص بدون رضایت صریح آنان نمی‌داند و معاون کمیسیون اروپا نیز با توجه به اینکه داده‌ها امروز شاهرگ اقتصادند، اعلام می‌دارد که نباید با نقض حریم خصوصی بر داده‌ها نظارت کرد یا با محدودیت‌های غیرضرور در انتقال فرامرزی مانعی در کسب و کارنوین و فعالیت اقتصادی ایجاد کرد (Fang, 2018: 364). تمامی این موارد بیانگر دغدغه‌های صیانت از داده‌ها و حریم خصوصی است که به‌حدی ضرورت دارد که حتی به بهانه‌های افزایش موج حملات تروریستی و لزوم نظارت بر فعالیت‌های سایبری و داده‌ها برای مبارزه با تروریسم نیز نمی‌توان آن را نادیده انگاشت.

دیوان اروپایی حقوق بشر، اصول بنیادینی را در رویهٔ خود در خصوص ذخیرهٔ داده‌ها معین کرده است. این اصول می‌توانند در موارد مقتضی اعمال شوند. از نظر دیوان اروپایی حقوق بشر دولت‌ها تعهدات ایجابی ذاتی در حمایت مؤثر از زندگی خصوصی افراد دارند (ECHR, 1979, para32) و دولت‌ها باید اقداماتی را اتخاذ کنند تا زندگی خصوصی افراد محترم شمرده شود، حتی در حوزهٔ روابط افراد بین خودشان مثلا کاربر اینترنت و کسانی که دسترسی به یک وب‌سایت مشخص را فراهم می‌سازند.[2] دیوان در پروندهٔ کی. یو. علیه فنلاند در سال ۲۰۰۸ این تعهد ایجابی دولت را برجسته‌تر کرده است. اصل دیگر در رویهٔ دیوان این است که دولت می‌تواند در خصوص طرف‌های ثالث که داده‌های افراد را ذخیره می‌کنند، مسئولیت داشته باشد.[3] سومین اصلی که می‌توان از رویهٔ دیوان استخراج کرد، این است که جایی که اطلاعات

1. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner [2015] EU:C:2015:650.
2. X and Y v. the Netherlands,6March 1985, §§ 23-24 and 27, Series A no. 91; August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003; and M.C. v. Bulgaria, no. 39272/98, § 150, ECHR 2003- XII
3. Leander v. Sweden, 26 March 1987, § 48, Series A no.116.

شخصی در راستای منافع امنیت ملی ذخیره می‌شود، باید تضمین‌های کافی مؤثر در مقابل سوءاستفادهٔ دولت وجود داشته باشد. اصل چهارم اینکه فعالیت‌های حرفه‌ای و تجاری از مفهوم زندگی خصوصی مستثنا نمی‌شوند.[1]

گسترهٔ فضای نوپدید در تمامی عرصه‌های زندگی و حجم عظیم داده‌ها تهدیدی برای حریم خصوصی اشخاص ایجاد کرده و بر چالش‌های عصر جدید افزوده است، اگرچه همزمان با رشد انتقال داده‌ها قواعدی نیز وضع شد، لیکن با وجود پیامدهای ناگوار نقض داده‌ها، قواعد وضع‌شده متناسب با اقتضائات و تهدیدهای نوین نبود و نمی‌توانست حمایت از حریم خصوصی و داده‌های اشخاص را به‌نحو بهینه تضمین کند تا اینکه اتحادیهٔ اروپا با تصویب مقررات حفاظت از داده‌های عمومی[2] که جایگزین قواعد قبلی شده و قوانین حفاظت از داده‌ها را در سراسر اتحادیهٔ اروپا هماهنگ می‌کند و از ۲۵ می ۲۰۱۸ لازم‌الاجرا شده، با در نظر گرفتن مجازات‌های سنگین برای ناقض داده تحولی را در حمایت از داده‌ها ایجاد کرد و مادهٔ ۴۸ در راستای حمایت از داده‌ها مقرر می‌دارد آرای محاکم و دستورهای اداری کشور ثالث به‌منظور انتقال یا افشای داده‌ها قابل اجرا نیست، مگر اینکه بین کشور درخواست‌کننده و اتحادیهٔ اروپا یا یکی از کشورهای عضو اتحادیه، موافقت‌نامهٔ همکاری منعقد شده باشد. بدیهی است فراگیر شدن فضای سایبر اقدامات هدفمند و منسجم در خصوص مدیریت داده‌ها را ایجاب می‌کند و حمایت از داده‌های شهروندان و حریم خصوصی مستلزم همکاری دولت‌ها برای بازتعریف مفاهیم و وضع قواعد و انعقاد موافقت‌نامه‌های بین‌المللی از طریق مجامع بین‌المللی و حقوق بشری و نیز الگوپذیری از مفاد آرای حقوق بشری است و بدون همکاری و درک مشترک نمی‌توان به الگوی مناسبی برای تنظیم فضای سایبری و حمایت از حریم خصوصی اشخاص دست یافت.

صیانت از حریم خصوصی شهروندان در نظام حقوقی ایران

اولین بار در قانون اساسی مشروطه مصوب ۱۲۸۵ به حریم خصوصی اشاره شد و این بیانگر پاسداشت حریم خصوصی شهروندان توسط قانونگذاران ایرانی حتی پیش از تصویب اعلامیهٔ جهانی حقوق بشر است. در قانون اساسی جمهوری اسلامی ایران نیز بسان قانون اساسی بسیاری از کشورهای دیگر اصول متعددی از آن به تبیین حریم خصوصی اختصاص داده شده است که می‌توان اصول ۲۲،۲۳ و ۲۵را برشمرد. در نظریهٔ مورخ ۰۶/۲۸/ ۱۳۶۰ شورای نگهبان مطابق اصل ۲۲ قانون اساسی افشای سوابق مربوط به تعرض به حیثیت اشخاص نیز جز با تجویز قانون ممنوع است و برابر اصل ۲۳ اعتقادات اشخاص چهرهٔ درونی دارد و جزئی از

1. Niemietz v. Germany , 16 December 1992, § 29, Series A no. 251-B; and Halford v. the United Kingdom , 25 June 1997, § 42, Reports of Judgments and Decisions 1997-III.
2. GDPR, 2018.

سرشت انسان است و تا زمانی‌که نمود بیرونی آن اختلال در نظم و امنیت ایجاد نکند، نبا ید آن شخص را مورد تعرض قرار داد و اصل ۲۵ که حریم خصوصی ارتبا طات را مورد حما یت قرار می‌دهد و در موارد ک شف جرم و تعق یب مجر مان ا ستثنایی بر آن وارد می شود (وک یل و عسکری، ۱۳۸۸: ۱۲۵-۱۲۲)، در ا صل ۳۹ ن یز با مم نوع دان ستن ه تک حر مت و حیث یت بازداشت‌شدگان و زندانیان و تعیین مجازات برای عاملان، به حریم خصوصی توجه شده ا ست. علاوه‌بر قانون اساسی، می‌توان به اسناد بین‌المل لی ماند مي ثاق بین‌المل لی ح قوق مدنی و سیاسی که ایران نیز به آن متعهد شده است، اشاره کرد و در اسناد بالادستی فضای سایبر و در بند ۶ آخرین حکم رهبری در انتصاب اعضای شورای عالی فضای مجازی در شهریور ۱۳۹۴ به حفظ حریم خصوصی توجه شده است.

بعضی معتقدند نتیجهٔ وضع قوانین دربارهٔ حریم خصوصی داده، کوچک‌تر شدن وسایل نقض حریم خصوصی داده، است، درحالی‌که هرچه نقض حریم در نتی جهٔ تو سعهٔ فـ ناوری ساده تر می‌شود، حمایت بیشتر از حریم خصوصی داده را می‌طلبد و می‌بایست میزان مسئولیت حقوقی نقض‌کنندهٔ این حریم افزایش یابد تا توازن و ن ظم ح قوقی ح فظ شود (جع فری و رهبر پور، ۱۳۹۶: ۴۹). در گذشته هیچ دولتی قادر به کنترل حریم خصوصی شهروندان خود نبود، ولی با بهره‌گیری از قابلیت‌های تکنولوژیکی که دریافت و ارسال همزمان داده‌ها را با یک وسیله ممکن می‌سازد، امکان نظارت تمام‌وقت یک شهروند میسر است و این تهدیدها حتی تو سط ا شخاص معمولی هم صورت می‌پذیرد (انصاری، ۱۳۸۳: ۳). بنابراین با توجه به تسهیل امکان نقض حریم خصوصی افراد در فضای سایبر ضروری است در قوانین ارتباطی ایران این م سئله مورد تو جه بیشتری واقع شود و هم نسبت به نظام‌مند ساختن نظارت دولت بر فضای سایبر و شفاف سازی حیطهٔ نظارت اقدام صورت پذیرد و هم اقدامات پیشینی و پسینی لازم در خصوص نقض حریم خصوصی شهروندان توسط دیگر اشخاص در نظر گرفته شود.

علاوه‌بر قوانین عام مانند قانون مسئولیت مدنی مصوب ۱۳۳۹ و قانون احترام به آزادی های مشروع و حفظ حقوق شهروندی مصوب ۱۳۸۳ که بر رعایت حریم خصوصی تأکید دارند و این حریم فضای سایبر را هم در برمی‌گیرد، در قوانین و مقررات مختلف دیگر به حق حریم خصوصی در فضای سایبر و حمایت از داده توجه و تمهیداتی برای صیانت از این حق لحاظ شده است. قانون انتشار و دسترسی آزاد ضمن تعریف اطلاعات شخصی در بند دوم قانون، با عنوان «حمایت از حریم خصوصی» مواد ۱۴ و ۱۵[1] را به این امر اخت صاص داده ا ست. در این

---

۱. مادهٔ ۱۴ـ چنانچه اطلاعات درخواست‌شده مربوط به حریم خصوصی اشخاص باشد یا در زمرهٔ اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود.
مادهٔ ۱۵ـ مؤسسات مشمول این قانون درصورتی‌که پذیرش درخواست متقاضی متضمن افشای غیرقانونی اطلاعات شخصی دربارهٔ یک شخص حقیقی ثالث باشد باید از در اختیار قرار دادن اطلاعات درخواست‌شده

قانون هر دو وجه حریم خصوصی و حمایت از داده‌های اشخاص مورد توجه قانونگذار قرار گرفته و دسترسی اشخاص غیرمجاز به اطلاعات فردی منع شده است. ضمن اینکه حریم خصوصی اشخاص و همچنین جلوه‌هایی از اطلاعات متضمن آنها، مانند اطلاعات مربوط به سلامت اشخاص مورد تصریح قانونگذار قرار گرفته، لیکن حمایت شایستهٔ مورد انتظار به‌عمل نیامده است و در مواقعی که اطلاعات غیرواقعی در مورد شخص منتشر شود، صرفا حق پیگیری از طریق قواعد عمومی مسئولیت مدنی برای وی شناخته شده است، درحالی‌که باید امکان جبران فوری ناهنجاری صیانتی با کمترین هزینه و آسیب شناخته شود.

در بند ۴ مصوبهٔ شورای عالی فضای مجازی، به حفظ حریم خصوصی کاربران تأکید شده و در ضوابط فنی اجرایی توسعهٔ دولت الکترونیکی مصوب ۱۳۹۳ دبیرخانهٔ شورای عالی فناوری اطلاعات را ملزم به تأسیس کارگروه با همکاری سازمان های ذی‌ربط برای اصلاح قوانین و مقررات موجود یا تصویب قوانین و مقرره‌های جدید برای صیانت از حریم خصوصی و حمایت از داده‌ها و پایگاه‌های اطلاعات دولت الکترونیکی کرده است. در قانون آیین دادرسی کیفری مصوب ۱۳۹۴ نیز در بخش دادرسی الکترونیکی، قوهٔ قضاییه موظف به فراهم سازی تمهیدات فنی و قانونی لازم برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان شده و برای ناقضان آنان مجازات تعیین شده است و در اینجا هم قانون‌گذاران حریم خصوصی و داده‌های شخصی را در کنار هم به‌کار برده‌اند.

مادهٔ ۳ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات در راستای صیانت از حریم خصوصی شهروندان در فضای سایبر، حفاظت و حراست از انواع مراسلات، مکالمات و اطلاعات اشخاص را از وظایف این وزارتخانه برمی‌شمارد و در واقع مسئولیت صیانت از حریم خصوصی ارتباطات و اطلاعات در مورد آنها به این وزارتخانه واگذار شده که با عنایت به اختیارات سیاستگذاری اجرایی خود می‌تواند مستقلا یا حسب مورد از طریق کمیسیون تنظیم مقررات ارتباطات و سازمان تنظیم مقررات و ارتباطات رادیویی ضوابطی را وضع و ابلاغ کند. در مصوبه‌های کمیسیون تنظیم مقررات ارتباطات و پروانه‌های صادره توسط سازمان تنظیم مقررات و ارتباطات رادیویی نیز به این مهم توجه شده است که در اجرای وظیفهٔ خود مبنی بر صدور مجوز ارتباطی و فناوری اطلاعات و نظارت بر فعالان بخش ارتباطات و فناوری اطلاعات کشور مانند اپراتورهای مخابراتی و دارندگان پروانه‌های ایجاد و بهره‌برداری از شبکهٔ ارتباطات

خودداری کنند، مگر آن‌که:

الف) شخص ثالث به‌نحو صریح و مکتوب به افشاء اطلاعات راجع به خود رضایت داده باشد.

ب) شخص متقاضی، ولی یا قیم یا وکیل شخص ثالث، در حدود اختیارات خود باشد.

ج) متقاضی یکی از مؤسسات عمومی باشد و اطلاعات درخواست‌شده در چهارچوب قانون مستقیما به وظایف آن به‌عنوان یک مؤسسهٔ عمومی مرتبط باشد.

ثابت[1] و خدمات ارتباطی ثابت[2] ضوابطی را به‌منظور صیانت از حریم خصوصی اطلاعات شخصی و ارتباطی کاربران و مشترکان وضع و ابلاغ کرده است. اگرچه با عدم اتخاذ راهکارهای اجرایی دقیق و عدم نظارت صحیح عملا آن‌طور که باید و شاید از این حریم صیانت به‌عمل نیامده، چراکه حمایت مناسب و شایسته حمایتی است که قابل سنجش باشد. به‌عبارت دیگر، به‌صورت عینی بتوان آن را ارزیابی کرد تا در صورت ادعای نقض از سوی شهروند مرجع صلاحیتدار، مثلا دادگاه، بتواند بر مبنای معیارهای عینی آن را ارزیابی کند. از طرف دیگر، می‌بایست مرجع مقررات‌گذار الزامات و شرایط حاکم بر سازوکارها و ابزارهای نظارتی را وضع کند و از اختیار تعیین ضمانت اجراهای تخلفات صیانتی برخوردار باشد تا حریم شخصی اشخاص نقض نشود، آن‌گونه که امروزه در پیام‌های مختلف دریافتی اعم از مراکز آموزشی و غیره دسترسی آنان به اطلاعات شخصی و نقض این حریم محرز است.

منشور حقوق شهروندی جمهوری اسلامی ایران مصوب ۱۳۹۵ در مادهٔ ۳۵ به حریم خصوصی شهروندان در فضای سایبر توجه داشته و در مواد ۳۶ تا ۴۲ نیز بر رعایت حریم خصوصی تأکید کرده است، اگر چه از لحاظ حقوقی این منشور الزام‌آور نیست و ضمانت اجراهای مشخصی برای نادیده گرفتن تعهدات منشور و نقض حریم خصوصی شهروندان ذکر نشده است، لیکن جنبهٔ ترویجی منشور حقوق شهروندی در نهادینه شدن و مطالبه‌گر کردن شهروندان بسیار مؤثر است و مبنای مناسبی برای پیگیری بسیاری از مطالبات و انتظارات مشروع شهروندان و الزام به پاسخگویی دستگاه‌های اجرایی در برابر آنهاست. همچنین درصدد جبران کاستی‌های قانونی ـ مقرراتی برآمده و اصلاح سازوکارهای نظام اداری را فراهم آورده است و در مادهٔ ۱۹ منشور حقوق شهروندی در نظام اداری نقض مندرجات منشور اخیرالتصویب از مصادیق تخلفات اداری مندرج در مادهٔ ۸ قانون رسیدگی به تخلفات اداری محسوب می‌شود.

مادهٔ ۱ قانون حمایت از پدیدآورندگان نرم‌افزار های رایانه‌ای مصوب ۱۳۷۹ نیز متضمن احترام به حریم خصوصی و مالکیت داده‌هاست. مادهٔ ۳۱ قانون مطبوعات افشای اسرار شخصی و هتک حرمت را ممنوع اعلام داشته و در تبصرهٔ ۳ مادهٔ ۱ این قانون (اصلاحی ۱۳۷۹) با مشمول قرار دادن نشریات الکترونیکی، در واقع صیانت از حریم خصوصی در فضای سایبر را لحاظ داشته است.

مادهٔ ۵ قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌کنند مصوب ۱۳۷۹ (اصلاحی ۱۳۸۷)، نیز برخی مصادیق نقض حریم خصوصی اطلاعات و داده‌ها را تعیین و مجازات در نظر گرفته است. لیکن برای تحقق بند «ج» مادهٔ ۵ یعنی تهیهٔ مخفیانهٔ فیلم یا عکس مبتذل از مراسم خانوادگی و تکثیر آن، اولاً، باید تهیهٔ فیلم یا عکس مخفیانه باشد؛ ثانیاً

1. Fixed Communication Provider(Fcp)
2. Servco

فیلم‌ها و عکس‌های تهیه‌شده مبتذل باشد. اشکال وارد این است که مقید کردن فیلم یا ع کس به قید «مبتذل» است، درحالی‌که افراد دوست ندارند که از ا ماکن اختصا صی آن ها هیچ‌گو نه عکس یا فیلمی بدون رضایت آنان گرفته شود، شایسته بود مقنن، از حریم خصوصی اطلاعات و داده‌های افراد در مقابل چنین تعدیاتی به‌طور مطلق حمایت می‌کرد. اشکال دیگر ا ین ماده در مقید کردن تهیهٔ عکس یا فیلم مبتذل از «مراسم» خانوادگی و اختصاصی است که دلیلی برای چنین قیدی وجود ندارد؛ چه اینکه در غیر از «مراسم» نیز افراد در مسکن خود به‌صورت راحت و بدون پوشش کامل زندگی می‌کنند که تهیهٔ عکس یا فیلم در حالت‌های عادی نیز، به‌و یژه از بانوان، ناقض حریم خصوصی است که باید مقنن از آن حمایت کند. اما نکتهٔ مثبت این ماده در بند «ب» مشاهده می‌شود، که دربارهٔ تهیهٔ فیلم یا عکس از محل‌های اختصا صی بانوان ا ست. برخلاف تصور اولیه، حریم خصوصی در اماکن عمومی ن یز به ر سمیت شناخته شده و از آن حمایت می‌شود و استخرها، سالن‌های ورزشی و این‌گونه محل‌ها در ز مان های خا صی که به بانوان اختصاص داده شده، در عین حفظ ویژگی عموم یت، از ا ین ن ظر حریم خصو صی آن ها محسوب شود. دادگاه اروپایی حقوق بشر نیز در د عوای پک[1] عل یه دو لت انگل ستان در سال ۲۰۰۳ میلادی چنین حکم داد که: «حوزه‌هایی از تعامل فرد با دی گران ح تی در یک م کان عمومی وجود دارد که در چارچوب زندگی خصوصی قرار می‌گیرد» (جعفری و رهبر پور، ۱۳۹۶: ۶۳-۵۶) و با بهره‌مندی از این وصف، شایسته است قانونگذاران ما به وضع قوانین جدید مبادرت ورزند که در آن به‌صراحت، مطا لب و ت صاویری که در ف ضای سایبر، پروفا یل های شخ صی شبکه‌های اجتماعی و گروه‌ها منتشر شده، حریم خصوصی افراد شناخته شود و با ناق ضان ا ین حریم برخورد شود.

قانون مجازات اسلامی علاوه‌بر اینکه به حریم خصوصی در مواد متعدد[2] تو جه کرده، مواد زیادی را به حریم خصوصی در فضای سایبر و ارتباطی اختصاص داده است. در قانون مجازات اسلامی در بخش جرائم رایانه‌ای و در قسمت جرائم علیه محرمانگی داده‌ها و مواد متعدد در بحث شنود غیرمجاز و دسترسی غیرمجاز، و در فصل دوم مبحث جعل رایانه‌ای، فصل سوم سرقت و کلاه‌برداری و فصل پنجم هتک حیثیت و نشر اکاذیب نیز به‌نوعی حق حریم خصوصی شهروندی لحاظ شده و محترم دانسته شده است و برای متعرضین به این حقوق مجازات در نظر گرفته است. در مادهٔ ۹۶۸ (۷۴۵) قانون مجازات هم در حمایت از حریم خصو صی، پ خش فیلم و تصاویر افراد به‌وسیلهٔ سامانه‌های رایانه‌ای و مخابراتی به‌نحوی که به ضرر یا عرفاً مو جب هتک حیثیت منجر شود، جرم محسوب شده و برای آن مجازات در ن ظر گرف ته شده ا ست و نسبت به قوانین قبلی، پخش فیلم در فضای سایبر به‌صراحت مورد توجه وا قع شده و از ن کات

1. Peck

۲. مانند مواد ۸۰۱(۵۷۰)-(۵۷۳)۸۰۴-(۵۷۸)۸۰۹- (۵۸۰) ۸۱۱.

مثبت است. لیکن از آنجا که صرف عدم رضایت فرد شرط کافی نیست و مقید به عرف و ورود ضرر شده، شاید در بعضی مواقع به نقض حریم خصوصی ا فراد و نار ضایتی آ نان من جر شود، بدون اینکه امکان پیگیری قانونی وجود داشته باشد.

قانون مجازات اسلامی همچنین در مواد ۸۱۳ (۵۸۲) و ۸۶۷ (۶۴۱) با تعیین مجازات برای مأموران و مستخدمان دولتی که غیرقانونی، مراسلات یا مخابرات اشخاص را مفتوح، توق یف یا بازرسی یا استراق سمع می‌کنند و مزاحمان که از وسایل ارتباطی استفاده می‌کن ند، علاوه بر قانون شرکت مخابرات ایران و غیرحصری دانستن وسایل مذکور و تعمیم آن، در واقع حمایت از حریم خصوصی اشخاص در فضای سایبر را ت حت پو شش قرار می‌د هد و برای ناق ضان آن مجازات تعیین می‌کند. در این قانون جرم شنود محتوای ارتباطات در حال انتقال غیرعمومی پیش‌بینی شده که به حریم خصوصی دلالت دارد و در بخش جرائم علیه عفت و اخلاق عمومی نیز انتشار اطلاعات شخصی و اسرار اشخاص جرم‌انگاری شده که مبین حمایت از داده‌های شخصی اشخاص است. از طرف دیگر، در این قانون برای اشخاصی که مسئولیت نگهداری از داده‌های ترافیک و اطلاعات کاربران را به‌عهده دارند، یعنی ارائه‌دهندگان خدمات دسترسی و میزبانی، الزاماتی در نظر گرفته شده که عدم رعایت آن از ضمانت اجرای کیفری برخوردار است و این اشخاص حق ارائه و افشای این اطلاعات را جز برای مقام صلاحیتدار قضایی ندارند. علاوه‌بر این، حفظ فوری داده‌های رایانه‌ای که جز در موارد اضطراری تنها با دستور مقام قضایی به‌عمل می‌آید، به‌منزلهٔ افشای اطلاعات سامانه‌های محافظت‌شده نیست و دیگر اینکه در تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی براساس قانون به‌منظور صیانت از حریم و حرمت اشخاص از دسترسی مجریان قانون به داده‌ها و اطلاعات غیرضرور ممانعت به‌عمل آمده و تصریح شده است که باید بر پایهٔ ظن متعارف مشخص کنند که به کدام داده‌ها یا سامانه‌ها برای پیگیری کیفری خود نیاز دارند و اعمال سازوکارهای کنترل ارتباطات اشخاص نیز مشمول ضوابط سخت‌گیرانه‌ای شده و از هر گونه اعمال سلیقه از سوی مجریان قانون جلوگیری شده است.

ممنوعیت مطلق افشای اطلاعات و داده‌های جمع‌آوری‌شده و ممنوعیت مطلق ب هره برداری از آنها توسط مراجع قضایی، مالیاتی مندرج در مادهٔ ۷ قانون مر کز آ مار ا یران، م بین ا صل «ناشناسی داده‌ها» و به معنای عدم افشای هویت موضوع داده‌هاست. بنابراین استنباط می شود که وارد کردن داده‌های مربوط در پایگاه‌های اطلاعاتی دولت الکترو نیک و غ یره مم نوع ا ست (محسنی، ۱۳۸۸: ۴۸۸- ۴۸۷) و این خود بیانگر حساسیت قانونگذاران در دهه‌های گذ شته در صیانت از حریم خصوصی شهروندان ا ست که ح تی دستر سی مقا مات ق ضایی و دول تی به اطلاعات شخصی را نیز غیرممکن ساخته است.

قانون تجارت الکترونیکی هم در مواد ۵، ۵۸ و ۵۹ به حریم خصو صی و حما یت از داده ها

توجه داشته و در مادۀ ۷۱ این قانون نیز برای ناقضان ا ین حق، م جازات حبس تع یین شده است. مطابق این قانون برای حفظ حریم خصوصی و امنیت شهروندان ضروری ا ست ابزار های الکترونی کی و شیوه های حفا ظت از سی ستم پو یا با شد و روش های حفا ظت از سی ستم به‌روزرسانی شود و این شرایط با توجه به اوضاع و احوال مبادلۀ پیام ارزیابی می‌شود. ا یراد وارد بر آن این است که مدعی مطمئن بودن سیستم باید ادعای خود را اثبات کند و شرایط م ندرج در این ماده برای دادگاه احراز شود، و دادگاه برای احراز شرایط، موضوع را به کار شناس ار جاع می‌دهد که مستلزم صرف هزینه و زمان زیادی است و بعضاً مم کن ا ست مدعی توان اث بات نداشته باشد، ازاین‌رو شای سته ا ست بر خی روش های ف نی مو جود که از شرایط اطمی نان برخوردارند، به‌عنوان امارات اطمینان دلیل معرفی شوند که پیش‌نویس این قانون در مادۀ ۱۲۷ راهکاری را در این خصوص مدنظر داشت و کمیته‌ای با عنوان کمیتۀ فناوری و استاندارد سازی سیستم‌های اطلاعاتی پیش‌بینی کرده بود تا بهترین روش‌های مو جود را با تو جه به آ خرین دستاوردهای علمی به‌عنوان راهنمای عمل منتشر کنند که روش‌های ف نی معر فی شده بدون نیاز به اثبات می‌توانستند در دادگاه مورد قبول قرار گیرند که این بند در تن ظیم ن هایی حذف شد. ازاین‌رو باید با استفاده از نسخه‌های استاندارد و رویه‌های متحدال شکل از بار اث بات د عوا کاست (عبدالهی و شهبازی‌نیا، ۱۳۸۸: ۱۲۹-۱۲۳) و صرفاً با همکاری دولت‌ها در سطح ج هانی و وضع قواعد متناسب با تنوع کاربری فناوری ارتباطی و فناوری اطلاعات سازوکارهای نظارتی و سیاست‌های پیشینی و پسینی شرایط فضای سایبر می‌توان از حریم خصوصی کاربران صیانت به‌عمل آورد.

در قانون تجارت الکترونیکی دیل قسمت جرایم و مجازات‌ها، در مادتین ۶۷ و ۶۸ نیز کلاه‌برداری و جعل از طریق فضای سایبری مشمول مجازات شده است. در اینجا بحث حریم خصوصی فعالیت‌های تجاری الکترونیکی مدنظر قرار گرفته و می‌بایست تلاش‌های معقولانه‌ای برای حفظ و نگهداری محرمانۀ اسناد تجاری صورت گرفته باشد و اگر به حریم خصوصی تجاوز شده باشد، برای حمایت از اسرار تجاری برخلاف کلاه‌برداری کلاسیک مانور متقلبانه، رکن وقوع جرم نیست. لیکن با وجود تخصیص مبحثی به حمایت از داده پیام و ذکر مصادیق اطلاعات شخصی و پیش‌بینی ضمانت اجرا برای متخلفان در این قانون با گذشت بیش از یک دهه آیین‌نامۀ مربوط تصویب نشده است.

مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب ۱۳۸۰ شورای عالی انقلاب فرهنگی (جل سات ۴۸۲-۴۸۸) اگر چه در ب ند ۵-۳-۱۰ ق سمت «ب» با ع نوان آ یین‌نا مۀ وا حدهای ارائه‌کنندۀ خدمات اطلاع‌رسانی و اینترنت ر سا، شرکت ها یا مؤس سات ارا ئه‌کن ندۀ خدمات اطلاع‌رسانی و اینترنتی، رسا (ISP)[1] را موظف به در نظر گرفتن تمهیدات برای حفظ حقوق

1. Internet Service Provider

کاربران و جلوگیری از حمله به کامپیوترهای آنان کرده و در بند ۵-۳-۱۲ نیز آنان را مکلف ساخته که اطلاعات مربوط به نحوهٔ حفاظت از حریم خصوصی اطلاعات و ارتباطات افراد در شبکهٔ خود را در اختیار کاربران قرار دهد و این بندها و نیز بندهای ۵-۳-۱۵، ۶-۱۳، ۶-۱۷ و ۶-۱۹ به‌نوعی توجه به حریم خصوصی و پیشگیری از دسترسی به داده‌های شخصی است، لیکن در شق «ج» بند ۶ قسمت الف با عنوان آیین‌نامهٔ نحوهٔ اخذ مجوز و ضوابط فنی نقطهٔ تماس بین‌المللی، دایرکنندهٔ نقطهٔ تماس بین‌المللی را موظف کرده تا بانک فعالیت‌های اینترنتی کاربران خود را در اختیار وزارت ارتباطات قرار دهد، و حسب درخواست وزارت اطلاعات با حکم قاضی این اطلاعات در اختیار آنان قرار گیرد. ازاین‌رو نمی‌توان این مصوبه را کاملاً همسو با حفظ حریم خصوصی شهروندان و صیانت از حریم آنان توسط دولت دانست، چرا که اولاً به ذخیرهٔ کلیهٔ داده‌ها و دسترسی وزارت ارتباطات به آن منجر می‌شود، از طرف دیگر مدت نگهداری داده ها مشخص نشده و نباید مدت نامحدود باشد. همچنین در اختیار قرار دادن داده‌های ذخیره شده باید به مبدأ و مقصد ارتباط محدود باشد و جمع‌آوری و افشای اطلاعات بیشتر با حکم قاضی نمی‌تواند ضامن حفظ حریم خصوصی شهروندان شود و در اختیار قرار دادن اطلاعات بیشتر باید صرفاً به موارد اقدام علیه امنیت ملی و با حکم مرجع ذی‌صلاح صورت پذیرد.

دستورالعمل ضوابط و شرایط تأسیس، فعالیت و انحلال دفتر خدمات الکترونیک قضایی، ابلاغی رئیس قوهٔ قضاییه سال ۱۳۹۲ و آیین‌نامهٔ نحوهٔ استفاده از سامانه‌های رایانه‌ای و مخابراتی، ابلاغی رئیس قوهٔ قضاییه در سال ۱۳۹۵ هم به رعایت حریم خصوصی تأکید ورزیده است و مادهٔ ۶ اصول حاکم بر صدور پروانهٔ دفاتر پیشخوان دولت و بخش عمومی غیردولتی مصوب کمیسیون تنظیم مقررات ارتباطات در جلسهٔ شمارهٔ ۲۶۱ مورخ ۱۳۹۶/۰۵/۱۵ به استناد تبصرهٔ ۲ مادهٔ ۲۶ قانون اساسنامهٔ شرکت ملی پست جمهوری اسلامی ایران مصوب ۱۳۹۵/۰۵/۱۸ و بند «پ» مادهٔ ۶۷ قانون برنامهٔ ششم توسعهٔ کشور، تحت عنوان آیین‌نامهٔ صدور مجوز تأسیس و راه‌اندازی، تعهدات و وظایف دارندهٔ پروانه، شرایط مکان و تجهیزات دفتر، تمدید، تغییر نام و مکان دفتر و لغو پروانه، در بند ۱۲ مادهٔ ۲ که وظایف و اختیارات دارندهٔ پروانه را بیان می‌کند، حفظ و حراست از اسناد، مدارک و اطلاعاتی که در اختیار وی قرار می‌گیرد در زمرهٔ وظایف دارندهٔ پروانه است که توجه نهاد مقررات‌گذار ارتباطی به حفظ حریم خصوصی شهروندان است.

در مادهٔ ۱۵ «دستورالعمل اجرایی ارائهٔ خدمات عمومی اجباری ارتباطات و فناوری اطلاعات» مصوب کمیسیون تنظیم مقررات ارتباطات، تعهدات اپراتور مبنی بر رعایت محرمانگی و رازداری، رعایت مفاد قراردادهای سطح سرویس و قراردادهای مشترکان و لزوم پاسخگویی در این موارد ذکر شده است. با تمام این اوصاف باید گفت که کشور ما هنوز از قانون مستقلی برای حمایت از حریم خصوصی و اطلاعات شخصی شهروندان و اشخاص تحت

حاکمیتش برخوردار نیست و تاکنون هیچ‌یک از پیشنهادهای قانونی سرانجام نیافته‌اند. به‌نظر می‌رسد مهم‌ترین مانعی که تاکنون سبب شده این حوزهٔ بنیادی در بخش‌های تقنینی و بالطبع تنظیمی از زیرساخت قانونی جامع‌الشمولی برخوردار نشود، این است که این حق بنیادی بشری به‌ویژه در بستر ارتباطات و فناوری اطلاعات نوین خواسته یا ناخواسته در برابر دو حوزهٔ نظم و امنیت عمومی از یک سو و فعالیت‌های اقتصادی سایبری از سوی دیگر قرار گرفته است. گروه نخست، با چالش بسیار جدی دشواری شناسایی تهدیدها و تهدیدآفرینان در فضای بیکران سایبری روبه‌روست و چنانچه به‌هنگام و به اندازه، اطلاعات مورد نیازش فراهم نیاید، نمی‌تواند به وظیفهٔ حیاتی‌اش عمل کند و فعالان اقتصادی نوین، به‌ویژه آنهایی که کسب‌وکار خود را در فضای سایبر و مبتنی بر داشته‌های آن بنیان نهاده‌اند، مانند کلان‌داده‌ها، به اطلاعات فزایندهٔ این فضا نیاز دارند، ازاین‌رو ضروری است در تدوین مصوبات حاکم بر این حوزه، دربارهٔ این موضوعات نیز تصمیم منصفانه و منطقی اتخاذ شود.

نتیجه‌گیری

با توجه به پدیدهٔ جهانی شدن و فضای فراگیر سایبری و عدم تعین مرز جغرافیای فیزیکی برای کاربران فضای سایبر، مباحث حقوق بشری مانند حفظ حریم خصوصی متفاوت از دنیای سنتی و محیط فیزیکی است که قواعد وضع‌شده توسط یک کشور بر افراد کشور دیگر تأثیرگذار ا ست و از این منظر نمی‌توان معیارهای سنتی را در این فضا اعمال کرد. دگرگون‌سازی شیوه‌های تجاری زمینهٔ رقابت اقتصادی سالم در عرصهٔ ملی و بین‌المللی را فراهم می‌سازد، از طرف دیگر توسعهٔ جریان آزاد اطلاعات بین تب عهٔ ک شورهای مخت لف، تناق ضات قانونی در حوزهٔ ح قوق اساسی افراد بیشتر شده و در این بین حقوق شهروندان تضییع می‌شود و ممکن است با تسهیل نقض حریم خصوصی تأثیر منفی بر این امر و سایر جنبه‌های زندگی افراد داشته باشد و بر نگرانی‌های شهروندان افزوده شود. برای رفع نگرانی‌های شهروندان مقررات سایبری متناسب با دغدغه‌های آنان می‌تواند مؤثر باشد. بدیهی است که قواعد سنتی بین‌المللی و حتی تحولات صورت‌گرفته در این قواعد بین‌المللی با سرعت و پیشرفت فناوری اطلاعات هماهنگ نیست و نمی‌تواند از حقوق بنیادین بشر پاسداری کند و تنها با تعاملات بیشتر برای و ضع قوا عد حاکم در این عرصه و هماهنگ‌سازی قوانین اسا سی ک شورها م طابق با ا صول م شترک در ح قوق اساسی بشر و ایجاد نظام حقوقی کارامد است که می توان از ح قوق شهروندان از جم له حق حریم خصوصی صیانت به‌عمل آورد.

در قوانین و مقررات عمومی و سایبری حقوق ایران به موازین و موضوعات مربوط به حریم خصوصی توجه شده و در برخی قوانین عادی مثل قانون م جازات ا سلامی ضمانت اجرا های

نسبی برای نقض این حق پیش‌بینی شده است. لـیکن خلأهـای زیـادی چـه از لحـاظ سـاختار سازمانی نهادهای تقنینی– مقررات‌گذاری و چه در مفاد قواعد وضـع‌شـده وجـود دارد. ازایـن‌رو برای ایفای شایستهٔ وظیفهٔ صیانت از داده‌های شخصی پیشنهاد می‌شود:

۱. نیازهای نهادی، ماهوی و شکلی شناخته شـده و در سـطوح تقنینـی و مقـررات‌گـذاری احکام موردنیاز پیش‌بینی شود؛

۲. قوانین و مقررات کاربردی براساس قوانین بنیادی وضع و در صورت خلأ قوانین بنیـادی نسبت به تدوین آن اقدام شود، در غیر این صورت قوانین و مقررات کـاربردی بـه‌دلیـل نبود قوانین بنیادی قابلیت اجرا ندارند؛

۳. الگوبرداری از ادبیات حقوقی، قانونی و مقرراتی کشورهای پیشرو و موفق و تطابق قواعد داخلی با مصوبات بین‌المللی و منطقه‌ای و بومی‌سازی آن الگوها بـا شـرایط و اقتضـائات داخلی در راستای وضع قوانین و مقررات ارتباطی و فناوری اطلاعات روزامـد و کارامـد، در غیر این صورت استفادهٔ صرف از ادبیات حقوقی و قوانین کشورهای موفـق بـه‌دلیـل ناهمگونی در اجرا با چالش‌هایی مواجه خواهد شد؛

۴. ناآگاهی بیشتر قانونگذاران، مقررات‌گذاران و مدیران دستگاه‌های حـاکمیتی اجرایـی بـا موضوعات و مباحث ارتباطی و فناوری اطلاعات و نیازهای حقوقی این حـوزه، ناآشـنایی کاربران و کنشگران عرصهٔ سایبری با قواعد و مقررات حقوق شهروندی و الزامات حقوق بشری و نیز تهدیدهای ایـن فضـا از جملـه نقـض حـریم خصوصـی و عـدم درک لـزوم نظام‌مند ساختن فضـای سـایبر توسـط آنـان، از جملـه مشـکلاتی اسـت کـه ضـرورت قاعده‌مند کردن فضای سایبر درک نشده است، ازایـن‌رو آمـوزش شـهروندان و مـدیران مسئول با قواعد بین‌المللی، منطقه‌ای و قوانین و مقررات کشورهای موفق می‌توانـد هـم نیاز به وضع این قواعـد و مقـررات را بـه یـک مطالبـهٔ جـدی ملـی مبـدل کنـد و هـم دستگاه‌های اجرایی با تهیه و تدوین پیش‌نویس قوانین و مقررات حوزهٔ صیانت از حقوق شهروندی در فضای سایبر خلأهای موجود را پر خواهند کرد؛

۵. برای حفظ حریم خصوصی و حمایـت از داده‌هـا، دسـتورالعمل در راسـتای محـدودیت میزان دسترسی نمایندگی‌های اپراتور به اطلاعات مشترکان و ممنوعیت دسترسی آنـان به داده‌ها تدوین شود و نظارت صحیح و آنلاین توسط رگولاتور صورت پذیرد؛

۶. به‌منظور توازن بین حق صـیانت از داده‌هـای شخصـی و بهـره‌بـرداری از کـلان داده‌ای، قوانین ناظر بر حریم داده‌های شخصی اصلاح شود؛

۷. قواعد و ضوابط حاکم بر چگونگی صیانت و استنادپذیری ادله در زمینهٔ تخلفات صـیانتی را تدوین و انواع تمهیدات تأمینی و شرایط اعمال آنها نسبت به متخلفان تدوین شود.

منابع

۱. فارسی

الف) کتاب‌ها

۱. انصاری، باقر (۱۳۹۱)، *حقوق حریم خصوصی*، تهران، سازمان مطالعه و تدوین کتب علوم انسانی (سمت).

۲. وکیل؛ امیرساعد؛ عسکری، پوریا (۱۳۸۸)، *قانون اساسی در نظم حقوق کنونی*، تهران: مجد.

۳. نوری، محمدعلی؛ نخجوانی، رضا (۱۳۸۳)، *حقوق حمایت داده‌ها*، تهران: کتابخانهٔ گنج دانش.

ب) مقالات

۴. انصاری، باقر (۱۳۸۳)، «حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی و ایران»، *مجلهٔ دانشکدهٔ حقوق و علوم سیاسی*، ش ۶۶، صص ۱-۵۳.

۵. جعفری، علی؛ رهبرپور، محمدرضا (۱۳۹۶)، «مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه»، *فصلنامهٔ پژوهش حقوق خصوصی*، ش ۱۸، صص ۴۳-۷۴.

۶. عبدالهی، محبوبه؛ شهبازی، مرتضی (۱۳۸۸)، «سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی»، *مجلهٔ پژوهش‌های حقوقی*، ش ۱۶، صص ۱۲۳-۱۳۱.

۷. فتحی، یونس؛ شاهمرادی، خیراله (۱۳۹۶الف)، «گستره و قلمرو حریم خصوصی در فضای مجازی»، *مجلهٔ حقوقی دادگستری*، ش ۹۹، صص ۲۲۹-۲۵۲.

۸.---------- (۱۳۹۶ب)، «تقابل حریم خصوصی اشخاص و امنیت ملی در مقابله با تروریسم سایبری»، *فصلنامهٔ قضاوت*، ش۹۱، صص ۱-۲۸.

۹. کدخدایی، عباس (۱۳۸۷)، «شبکه‌های اطلاعاتی جهانی و نقض حقوق بشر با تأکید بر حق حریم خصوصی»، *مرکز پژوهش‌های ارتباطات*، آخرین به‌روزرسانی ۲۰۱۶، قابل دسترس در: http://vista.ir/article/313123

۱۰. قوانین و مصوبات مختلف مرتبط بین‌المللی و ملی.

ج) پایان‌نامه‌ها

۱۱. جلالی فراهانی، امیرحسین (۱۳۸۴)، «پیشگیری از جرایم رایانه‌ای»، پایان‌نامهٔ کارشناسی ارشد، استاد راهنما، علی‌حسین نجفی ابرندآبادی، *دانشگاه امام صادق (ع)*، گروه حقوق جزا و جرم‌شناسی.

۱۲. محسنی، فرید (۱۳۸۸)، «حمایت کیفری از حریم خصوصی در زمینهٔ اطلاعات»، رسالهٔ دکتری، *دانشگاه امام صادق (ع)*، گروه حقوق خصوصی.

۲. انگلیسی

A) Book

13. Fang, Binxing (2018), *Cyberspace Sovereignty*, Singapore, Springer.

B) Articles

14. Baihua, Wen (2016), "An Assessment of the Strategic Situation in Cyberspace", *International Strategic Relations and China's National Security*, .vol.2, pp. 281-307, Available from: http://www.worldscientific.com/doi/abs/10.1142/9789813144941_0014
15. Géry, Aude (2018), "La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense", *Les Champs de Mars*, No.30, 2018/1.PP.307-316,25/5/2018 from:https://www.cairn.info/revue-les-champs-de-mars-2018-1-p-307.htm.
16. Guinchard, Audrey (2010), "Human Rights in Cyberspace", Keynote paper at *the Cyberlaw section 2010 Society of Legal Scholars Conference*,Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694483.
17. Hyun Jin, Chang (2018), "Self-Concepts in Cyber Censorship Awareness and Privacy Risk Perceptions: What Do Cyber Asylum-Seekers have?," *Computers in Human Behavior*,Vol. 80, pp.379-389, Available from: https://www.sciencedirect.com/science/article/pii/S0747563217306660
18. Monshipouri, Mahmood (2017), "Human Rights in the Digital Age: Opportunities and Constraints" ,*Public Integrity* ,Vol. 19, 2017 - Issue 2: Symposium on the Social Practices of Human Rights, 24/3/2017 from: http://www.tandfonline.com/doi/abs/10.1080/10999922.2016.1230690?tab=permissions&scroll=top

C) Cases

19. Airey v. Ireland, 9 October 1979, § 32, Series A no. 32.
20. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner [2015] EU:C:2015:650.

D) Documents

21. Directive 95/46/EC
22. EU General Data Protection Regulation ("GDPR") – FAQSExternal Version – 16 March 2018