

حریم خصوصی و جرایم اینترنتی



حسین ریحان، کارشناس ارشد حقوق جزا و جرم‌شناسی

چکیده

حریم خصوصی به قلمرو زندگی هر فردی اطلاق می‌شود که نوعاً یا عرفاً و یا با اعلان قبلی انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته، به آن قلمرو وارد نشوند یا نگاه و نظارت نکنند و به هر صورت دیگر، وی را در آن قلمرو مورد تعرض قرار ندهند.

بر این اساس، منازل و اماکن خصوصی، جسم افراد، اطلاعات شخصی و ارتباطات خصوصی از مهم‌ترین مصادیق حریم خصوصی هستند و همه افراد جامعه فارغ از نوع نگرش دینی و اعتقادی و حتی سیاسی و فرهنگی، باید به آن احترام بگذارند. حریم خصوصی از زمانی اهمیت پیدا می‌کند که فرد اهمیت دارد و بدون فرد، حریم او هم وجود نخواهد داشت. حال با توجه به این نکته که همین فرد، تأثیرگذارترین عنصر در فضای مجازی است و فرد است که به اینترنت به مثابه کاربر آن هویت می‌بخشد، بررسی حریم خصوصی و جرایم اینترنتی که منجر به نقض آن می‌شود و مجازات ناقضان این حریم اهمیت پیدا می‌کند.

واژگان کلیدی: حریم خصوصی، جرایم رایانه‌ای، فضای مجازی، نقض محرمانگی، مجازات



درآمد

حریم خصوصی محدوده معقولی است که فرد انتظار دارد از دسترس دیگران مصون بماند. این دیگری هم می تواند دولت باشد و هم می تواند سایر اشخاص حقیقی و حقوقی باشد. در فضای سایبر با توجه به تحولات و پیشرفت هایی که صورت گرفته و تبادل اطلاعاتی که در این عرصه صورت می گیرد، حریم خصوصی افراد با تهدیدات و فرصت هایی مواجه گردیده است. بستر فضای مجازی امکان ناشناخته ماندن، آنلاین بودن و انحصارطلبی در ارائه فضای مجازی را فراهم نموده و همین خود زمینه چالش هایی را برای نقض حریم خصوصی افراد در فضای مجازی فراهم می نماید. دولت ها می توانند به عنوان یک ناقض بزرگ حریم خصوصی در محیط فضای مجازی شناخته شوند. دلیل این موضوع در وقایعی نهفته است که دولت های مختلف به این نتیجه رسیدند که در دوگانه حریم خصوصی و امنیت باید جانب امنیت را بگیرند. آنها به انحای مختلف سعی در نظارت بر فضای مجازی دارند و با توجیه برقراری امنیت، حریم خصوصی سایبری افراد را نقض می نمایند. به علاوه افراد نیز در قالب شرکت های ارائه کننده خدمات و کسب درآمد و هکرها ممکن است به حریم خصوصی افراد در فضای سایبر دست اندازی کنند. تمامی این موارد و ویژگی ها و خصوصیات موجب تعیین محدوده و مشخصه مفهوم حریم خصوصی در فضای مجازی و تفاوت آن با فضای فیزیکی می شود.

۱- تاریخچه جرایم اینترنتی

۱-۱- ابداع اینترنت

اینترنت در سال ۱۹۶۴ توسط محققى به نام پائول باران در شرکت راند ابداع شد. وی به دنبال روشی برای مطمئن سازی

ارتباط پنتاگون (وزارت دفاع ایالت متحده آمریکا) با اعضای ارتش در هنگام حمله واقعی اتمی بود و یک شبکه ارتباطات رایانه ای غیرمتمرکز را پیشنهاد کرد که در آن رایانه مرکزی وجود نداشت.

در چنین شبکه ای که اینترنت شبکه آرپانت نام داشت، حتی در صورت انهدام و خرابی یک یا چند رایانه، همچنان امکان تبادل اطلاعات بین سایر رایانه های باقی مانده وجود خواهد داشت. در اوایل دهه ۷۰ میلادی محققان دریافتند که اینترنت علاوه بر روشی برای برقراری ارتباطات بین قسمت های مختلف ارتش، روش کم هزینه ای برای برقراری ارتباطات بین اشخاص و سازمان هاست. در واقع انگیزه بنیادین شکل گیری اینترنت حصول اطمینان از امکان برقراری ارتباطات پیوسته است. گفته می شود هدف اصلی از انجام پروژه آرپانت، افزایش امنیت اطلاعات محرمانه و نظامی این کشور (آمریکا) در مقابل مخاطرات ناشی از حملات هسته ای روسیه بود (باستانی، ۱۳۸۳: ۲۷).

۱-۲- اولین جرایم اینترنتی در جهان و ایران

تاریخچه مشخصی از پیدایش جرم اینترنتی و کامپیوتری وجود ندارد، ولی بهر حال این دسته از جرایم را باید زاینده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست.

بر اساس مطالعات صورت گرفته منشأ پیدایش جرم کامپیوتری و اینترنتی به قضیه رویس برمی گردد؛ او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی، به عنوان حسابدار آنها انتخاب می شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمت ها و تنظیم درآمد جنس، مبلغی از مرجع آن را کاهش و به جای خاص واریز می کند.

رویس با ظرافت خاصی قیمت ها را تغییر می داد، بعد از آن با نام ۱۷ شرکت محل و طرف قرارداد، چک های جعلی صادر و از آن حساب برداشت می کرد، به طوری که در کمتر از ۶ سال بیش از یک میلیون دلار به دست آورده است. اما به علت نداشتن مکانیزم برای توقف این روند، خودش را به محاکم قضایی معرفی می کند و به ۱۰ سال زندان محکوم می شود. بدین ترتیب زمینه پیدایش جرم رایانه ای شکل می گیرد و دادگاه را به تدوین قوانین مدون وامی دارد.

بر اساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آنها به عنوان جرم اینترنتی محسوب می شود.

بعد از این بود که گروه های هکر موسوم به گروه مش قاسم و ...، جرم های دیگری را مرتکب شدند، مواردی؛ چون جعل اسکناس، اسناد و بلیت های شرکت های اتوبوس رانی، جعل اسناد دولتی از قبیل گواهی نامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک های مسافرتی و عادی، بخشی از این جرایم اینترنتی هستند.

بر اساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرایم اینترنتی در کشور تشکیل شد که کشف جرایم آمار ۵۰ درصدی را نشان می دهد. با توجه به آمارهای سال ۸۴ میزان کشفیات مربوط به کلاهبرداری، جعل و سایر جرایم رایانه ای و اینترنتی ۱۱ درصد رشد را نشان می دهد (باستانی، ۱۳۸۳: ۲۷).

۱-۳- تاریخچه واکنش‌های قانون‌گذاری برای جرایم سایبری در ایران

اولین تلاش در خصوص قانون‌گذاری برای برخورد با جرایم رایانه‌ای در ایران به سال ۱۳۷۳ بازمی‌گردد. از آنجاکه در هیئت‌وزیران مطرح شده بود که در خصوص جرایم رایانه‌ای بررسی لازم انجام شود و در صورت لزوم یک سری مواد پیشنهادی جهت ضمیمه نمودن به لایحه جدید قانون تعزیرات ارائه گردد، دبیرخانه شورای عالی انفورماتیک و بانک مرکزی جمهوری اسلامی، هر کدام مواد پیشنهادی خود را جداگانه ارائه دادند و در نهایت یک ماده واحده به لایحه قانون تعزیرات افزوده شد؛ اما کمیسیون حقوقی و قضایی مجلس با این استدلال که جرایمی که از طریق رایانه ارتکاب می‌یابد تفاوتی با جرایم سنتی ندارند و فقط ابزار ارتکاب جرم متفاوت شده است و لذا قانون‌گذاری جدید نیاز ندارد، آن را نپذیرفت.

با الحاق تبصره ۳ ماده ۱ قانون مطبوعات در تاریخ ۱۳۷۹/۱/۳۰ با این مضمون که کلیه نشریات الکترونیکی مشمول مواد این قانون است، اولین واکنش قانونی نسبت به جرایم رایانه‌ای بروز پیدا کرد.

تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای در تاریخ ۱۳۷۹/۱۰/۴ را می‌توان به‌عنوان اولین واکنش قانونی در قالب یک قانون مستقل در قبال جرایم رایانه‌ای در ایران نام برد. همچنین در تاریخ ۱۳۸۲/۱۰/۰۹ قانون مجازات جرایم نیروهای مسلح، سوءاستفاده‌های مالی نظامیان را با استفاده از رایانه (کلاهبرداری و اختلاس) جرم انگاری نمود؛ و در نهایت قانون جرایم رایانه‌ای، مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی روز سه‌شنبه مورخ ۱۳۸۸/۳/۵

در مجلس شورای اسلامی تصویب و در تاریخ ۱۳۸۸/۳/۲۰ به تأیید شورای نگهبان رسید. در حال حاضر دادسرای رسیدگی به جرایم رایانه‌ای، مسئول رسیدگی به جرایم سایبری در ایران می‌باشد که با توجه به قوانین وضع شده به بررسی این جرایم و رسیدگی به شکایات افراد می‌پردازد (باستانی، ۱۳۸۳: ۲۷).

۲- حریم خصوصی ۱-۲- مفهوم حریم خصوصی در لغت و اصطلاح

حریم عبارت از اموری است که انسان از آن دفاع کرده، در مقام حمایت از آن برمی‌خیزد. همچنین حریم به معنای حرمت و آبروی مردم و... به کار رفته است. حریم از حرمت به معنای منع است به این دلیل تعرض دیگران به حق صاحب حریم، ممنوع است. البته واژه حریم برای غیر از انسان و در ارتباط با اموال نیز به کار رفته است. واژه «خصوصی» به معنای ویژه و اختصاصی در زبان عربی استعمال شده است.

در تعریفی جامع، حریم خصوصی قلمرو زندگی هر فرد دانسته شده است که نوعاً یا عرفاً و یا با اعلان قبلی، انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته باشند یا به آن قلمرو وارد نشوند یا به آن قلمرو نگاه یا نظارت نکنند یا به هر صورت دیگری وی را در آن قلمرو مورد تعرض قرار ندهند. آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، حریم خصوصی را قلمروی از زندگی شخصی فرد معرفی کرده است که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، وارد شدن، نظاره کردن، شنود و دسترسی به اطلاعات شخصی فرد

از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره شده خصوصی؛ نظیر هتل و کشتی؛ همچنین آنچه حسب قانون، فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات.

حقوق‌دانان نیز تعاریف متعددی از حریم خصوصی ارائه داده‌اند. برخی از این تعاریف عبارت‌اند از:

حق بر تنها ماندن، دسترسی محدود دیگران به انسان و توانایی ایجاد مانع در برابر دسترسی ناخواسته و ناخوانده به انسان، محرمانگی و پنهان ساختن برخی امور از دیگران، کنترل بر اطلاعات شخصی، حمایت از شخصیت و کرامت، حق بر عالم صمیمیت و کرامت انسان‌ها (انصاری، ۱۳۸۳: ۶ و ۷).

درواقع حریم خصوصی، حوزه زندگی هر فرد است که او با اعلان قبلی در چارچوب قانون انتظار دارد که دیگران بدون رضایت او به آن قلمرو وارد نشوند، یا نگاه و نظارت نکنند و به اطلاعات درباره آن دسترسی نداشته باشند و به آن تعرض نکنند. در این معنی جسم، البسه، اشیاء، تلفن همراه، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران جزء این قلمروهاست.

۲-۲- مفهوم حریم خصوصی در فقه امامیه

در فقه بحث «حریم خصوصی» تحت این عنوان مطرح نگردیده، ولی موضوعات و مسائل آن با مبانی متعدد و محکم مورد حمایت قرار گرفته است. می‌توان گفت که رعایت چنین حقی قبل از آنکه در حقوق مغرب زمین و کنوانسیون‌ها و اسناد بین‌المللی حقوق بشری پیش‌بینی گردد، در منابع فقهی و حقوقی اسلام مطرح



آزادی بیان افراد نیز ضعیف می‌شود و در درازمدت بی‌اعتمادی را در جامعه رواج می‌دهد و نگرانی از نقض حریم خصوصی موجب پناهندگی سایبری شهروندان می‌شود (Hyun Jin, 2018: 380-387)؛

بنابراین با توجه به تحولات گسترده جهانی ناشی از فناوری اطلاعات جا دارد که اجماع جهانی برای حریم خصوصی و ساماندهی حقوقی در فضای سایبر برای صیانت از این حق صورت پذیرد.

در ماده 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 اجازه مداخله در حریم خصوصی را نمی‌دهد و حمایت‌های قانونی را در برابر این تعرض ضروری می‌داند. امروزه حریم خصوصی ارتباطات با ظهور اشکال جدید مراسلات همچون پست الکترونیکی با مسائل جدیدتری روبه‌رو شده است (نوری و نخجوانی، ۱۳۸۳: ۳۴) و گسترش فضای سایبر زمینه را برای تهدید بیشتر حریم خصوصی فراهم آورده است. یکی از اسناد مهم در این زمینه، کنوانسیون جرایم سایبر است. از آنجاکه این کنوانسیون جنبه الزام‌آور دارد، می‌توان امیدوار بود کشورهای عضو مجبورند تدابیر کیفری خود را که عملاً بخش مهمی از این اقدامات به حریم خصوصی افراد در فضای سایبر مربوط می‌شود، به نحوی تنظیم کنند که به آنها تعرض نشود. بدیهی است با توجه به مشابهت‌هایی که میان تدابیر نظارتی پیشگیرانه و تعقیب و پیگرد جرایم سایبر وجود دارد، می‌توان نتیجه گرفت که این کنوانسیون به طریق اولی نسبت به تدابیر پیشگیرانه نظارتی

سمره بن جندب که قاعده فقهی لا ضرر از آن استخراج گردیده به گونه‌ای دلالت بر این معنی دارد (انصاری، ۱۳۸۳: ۱۳-۱۲).



آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، حریم خصوصی را قلمرویی از زندگی شخصی فرد معرفی کرده است که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، وارد شدن، نظاره کردن، شنود و دسترسی به اطلاعات شخصی فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره شده خصوصی؛ نظیر هتل و کشتی؛ همچنین آنچه حسب قانون، فعالیت حرفه‌ای خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات.



۳- قواعد بین‌المللی مرتبط با حریم خصوصی

ماده ۱۲ اعلامیه جهانی حقوق بشر اعلام می‌دارد زندگی خصوصی افراد نباید مورد مداخله خودسرانه قرار گیرد و افراد باید در برابر چنین تعرضاتی از حمایت قانون برخوردار باشند؛ اگرچه سانسورهایی که با نظارت مقامات حکومتی در خصوص داده‌های فضای سایبر صورت می‌گیرد جنبه مثبت هم دارد، چراکه دسترسی به اطلاعات گذشته در موارد بروز جرایم می‌تواند در کشف جرایم بسیار مؤثر باشد یا از انتقال اطلاعات نادرست به جامعه و پیامدهای آن جلوگیری کند، اما با تهدید حریم خصوصی و نقض حقوق بشر حق

بوده است. آیات متعدد قرآن و سنت پیامبر (صلی‌الله‌علیه‌وآله‌وسلم) و ائمه (علیهم‌السلام) دلالت بر ضرورت و وجوب رعایت حریم شخصی دیگران و حرمت نقض آن و در نتیجه ضمانت اجرای دنیوی و اخروی آن دارد.

احکام مرتبط با حریم خصوصی نیز از اصول و قواعد و احکام مختلف اسلام قابل استنباط است؛ از جمله ممنوعیت تجسس، ورود به منازل بدون استیذان، استراق بصر، استراق سمع، سوءظن، نیمه و غیبت، سب و هجو و قذف، اشاعه فحشا و هتک ستر، خیانت در امانت و نظایر آن که به نوعی بر حقوق و آزادی‌های فردی و حق حریم خصوصی دلالت می‌نمایند. همان‌طور که اشاره گردید این موارد مستقیماً تحت عنوان و یا به منظور حمایت از حریم خصوصی وضع و مطرح نشده‌اند، ولی مفهوم و مقررات مربوط به حریم خصوصی از آن استنباط می‌گردد. به همین ترتیب تقسیم‌بندی‌های مطرح شده در زمینه حریم خصوصی نیز مستقیماً در آنها منظور نگردیده ولی از فحوای قاعده یا حکم می‌توان حق حریم خصوصی در زمینه‌های مختلف؛ از جمله اطلاعات را استنباط نمود؛ مثلاً حرمت ورود به منزل دیگران بدون اذن آنها، در بادی امر خود حریم خصوصی منازل و اماکن محسوب می‌گردد، ولی در حقیقت این مداخله در ملک دیگری اگر در معنای صرفاً فیزیکی‌اش معنی شود تحت عناوین غصب و تصرف عدوانی قابل بررسی است. ولی شاید از عمده دلایل ناخوشایندی افراد در اشراف غیر نسبت به منزل ایشان (حتی هنگامی که در منزل حضور ندارند) کسب اطلاع و دستیابی به امور محرمانه و اسرار ایشان باشد. ماجرایی حدیث معروف «لا ضرر و لا ضرار فی الاسلام» در مورد

صادق است (جلالی فراهانی، ۱۳۸۴: ۱۲۱-۱۱۹). مفاد این کنوانسیون بیانگر نگرانی دولت‌های عضو در لزوم صیانت از حریم خصوصی در فضای سایبر است و بی‌شک موفقیت کشورها در تضمین این حق شهروندی با همکاری همدیگر برای وضع قواعد مشترک ساماندهی فضای سایبر و توسعه قوانین و مقررات ملی مربوط به حریم خصوصی شهروندان متناسب با پیشرفت‌های حاصل از فناوری اطلاعات و تأثیر آن در سبک زندگی نوین و حقوق اساسی اشخاص است.

علاوه بر موافقت‌نامه‌های بین‌المللی و منطقه‌ای، آرای دادگاه‌های بین‌المللی و منطقه‌ای به خصوص دادگاه اروپا که انعکاس دهنده استانداردهای حقوق بشری است نیز می‌تواند مؤثر باشد که در ۶ اکتبر ۲۰۱۵ دادگاه اروپا موافقت‌نامه بین آمریکا و اتحادیه اروپا را که در خصوص حفظ امنیت سایبر منعقد شده بود، به دلیل 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 اتحادیه اروپا طبق دستورالعمل EC/95/46 ملزم به حفاظت از داده‌های شهروندان خود است و انتقال داده‌ها به کشور ثالث صرفاً در صورتی امکان‌پذیر است که از سطح حمایت تضمین شده برخوردار باشند، درحالی‌که ایالات متحده از این استاندارد برخوردار نبوده و واجد شرایط نیست، اگرچه 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 جمع‌آوری شده 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 غیرضروری در انتقال فرامرزی، مانعی در کسب و کار نوین و فعالیت اقتصادی ایجاد کرد. تمامی این موارد بیانگر دغدغه‌های صیانت از داده‌ها و حریم خصوصی است که به حدی 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 (Fang.2018: 364).

دیوان اروپایی حقوق بشر، اصول بنیادینی را در رویه خود در خصوص ذخیره 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 حوزه روابط افراد بین خودشان مثلاً کاربر اینترنت و کسانی که دسترسی به یک وبسایت مشخص را فراهم می‌سازند. دیوان در پرونده کی. یو. علیه فنلاند در سال ۲۰۰۸ این تعهد ایجابی دولت را برجسته‌تر کرده است. اصل دیگر در رویه دیوان این است که دولت می‌تواند در خصوص طرف‌های ثالث که داده‌های افراد را ذخیره می‌کنند، مسئولیت داشته باشد. سومین اصلی که می‌توان از رویه دیوان استخراج کرد، این است که جایی که اطلاعات شخصی در راستای منافع امنیت ملی ذخیره می‌شود، باید تضمین‌های

کافی مؤثر در مقابل سوءاستفاده دولت وجود داشته باشد. اصل چهارم اینکه فعالیت‌های حرفه‌ای و تجاری از مفهوم زندگی خصوصی مستثنا نمی‌شوند. گستره 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 وضع شده متناسب با اقتضائات و تهدیدهای نوین نبود و نمی‌توانست حمایت از حریم خصوصی و داده‌های اشخاص را به نحو بهینه تضمین کند تا اینکه اتحادیه اروپا با تصویب مقررات حفاظت از داده‌های عمومی که جایگزین قواعد قبلی شده و قوانین حفاظت از داده‌ها را در سراسر اتحادیه 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 ماده 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 اتحادیه اروپا یا یکی از کشورهای عضو اتحادیه، موافقت‌نامه 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



نباشیم به دنبال مجرم بگردیم؛ هرچند که این مطلب هیچ‌گاه به معنای توجیه عملکرد بزهکار سایبری نیست؛ یعنی اگر افراد در محافظت از اطلاعات شخصی و یا حریم خصوصی خود کوتاهی نمایند دلیل بر آن نیست که ما خود را مجاز به تعرض به حریم خصوصی افراد بدانیم.

۵- صیانت از حریم خصوصی شهروندان در نظام حقوقی ایران

اولین بار در قانون اساسی مشروطه مصوب ۱۲۸۵ به حریم خصوصی اشاره شد و این امر بیانگر پاسداشت حریم خصوصی شهروندان توسط قانون‌گذاران ایرانی حتی پیش از تصویب اعلامیه جهانی حقوق بشر است. در قانون اساسی جمهوری اسلامی ایران نیز به‌سان قانون اساسی بسیاری از کشورهای دیگر اصول متعددی از آن به تبیین حریم خصوصی اختصاص داده شده است که می‌توان اصول ۲۲، ۲۳ و ۲۵ را برشمرد. در نظریه مورخ ۱۳۶۰/۰۶/۲۸ شورای نگهبان مطابق اصل ۲۲ ق، افشای سوابق مربوط به تعرض به حیثیت اشخاص نیز جز با تجویز قانون ممنوع است و برابر اصل ۲۳ اعتقادات اشخاص چهره درونی دارد و جزئی از سرشت انسان است و تا زمانی که نمود بیرونی آن اختلال در نظم و امنیت ایجاد نکند، نباید آن شخص را مورد تعرض قرار داد و اصل ۲۵ که حریم خصوصی ارتباطات را مورد حمایت قرار می‌دهد و در موارد کشف جرم و تعقیب مجرمین استثنایی بر آن وارد می‌شود (وکیل و عسکری، ۱۳۸۸: ۱۲۵-۱۲۲). در اصل ۳۹ نیز با ممنوع دانستن هتک حرمت و حیثیت‌بازداشت شدگان و زندانیان و تعیین مجازات برای عاملان، به حریم خصوصی توجه شده است. علاوه بر قانون اساسی، می‌توان به اسناد بین‌المللی؛ مانند میثاق بین‌المللی حقوق مدنی و سیاسی که ایران نیز به آن

که از دو منظر قابل بررسی است: یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضین حریم خصوصی در فضای مجازی. بزه دیدگان در فضای مجازی نقش مهمی را در بروز جرایم نقض حریم خصوصی ایفا می‌کنند و در عین حال می‌توانند در اقدامات پیشگیرانه علیه جرایم سایبری یا همان cyber prevention نقش‌آفرین باشند. بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می‌شود، استعداد قابل توجهی برای قربانی شدن (immolate) بروز می‌دهند و به راحتی طعمه بزهکاران سایبری می‌شوند. برخی کلاهبرداری‌های اینترنتی ناشی از کسب اطلاعات به روش‌های بسیار ساده و سوءاستفاده از عکس‌ها و اسرار شخصی نمونه‌هایی از این موضوع می‌باشد. ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و ... مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می‌کند. در صدر عرایض بیان گردید که افراد بایستی نسبت به صیانت از حریم خصوصی خود همت نمایند. بسیاری افراد بدون رعایت مسائل امنیتی، خصوصی‌ترین اطلاعات خود را بر روی سیستم رایانه‌ای و یا حامل‌های داده نظیر فلش و کارت‌های حافظه و تلفن همراه و سی دی و ... ذخیره می‌نمایند و به‌نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و این چنین استعداد قربانی شدن در فضای مجازی را از خود نشان می‌دهند. با الهام از این ضرب‌المثل که «مالت را حفظ کن، همسایه‌ات را دزد نکن» می‌توان گفت: در فضای مجازی از اطلاعات شخصی و حریم خصوصی خود محافظت نماییم تا مجبور

الگوی مناسبی برای تنظیم فضای سایبری و حمایت از حریم خصوصی اشخاص دست یافت.

۴- نقض حریم خصوصی در فضای مجازی

توسعه فضای مجازی مانند همه پیشرفت‌های دیگر در زندگی بشر با پیامدهای منفی و مثبت همراه بوده است. یکی از بدترین پیامدها در این فضا، به خطر انداختن حریم خصوصی افراد است. حق حریم خصوصی حقی است سیال، متداخل و مرتبط با حقوق دیگری؛ همچون حق تصرف انحصاری در مال ملوک، حق داشتن تمامیت جسمانی و روانی، حق خلوت در فضای خصوصی، حق برخورداری از آبرو و حیثیت. به دلیل اهمیت و حساسیت این موضوع است که این حق علاوه بر پشتیبانی کافی در متون دینی، اعم از فقهی و اخلاقی، از حمایت حقوقی و کیفری نیز برخوردار است.

گاهی نقض حریم مجازی حیثیت ماهوی ندارد، بلکه به قصد دستیابی به حریم واقعی غیر ایجاد می‌شود. در این صورت فضای مورد بحث حالت مجازی واقعی ماهوی پیدا می‌کند و نوع نقض نیز جنبه ابزاری برای شکستن حریم واقعی می‌یابد؛ برای مثال ورود به میل باکس دیگری برای دستیابی به مکاتبات و عکس‌ها و تصاویر وی، یا برای مثال رؤیت خلوت او از طریق وب کم متصل به رایانه شخصی مستقر در منزل کاربر، یا ورود به صفحه خصوصی وی برای ملاحظه گفت‌وگوهای کاربر. این موارد کاملاً به استراق سمع از طریق تلفن یا دستگاه شنود و دید زدن داخل منزل دیگری از طریق دوربین شباهت دارد و بعد ابزاری فناوری به کاررفته ملحوظ است.

نقض حریم خصوصی در فضای مجازی یکی از مهم‌ترین مسائل روز جامعه ماست



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. علاوه بر قوانین عام؛ مانند قانون مسئولیت مدنی مصوب ۱۳۳۹ و قانون احترام به آزادی‌های 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 را به این امر اختصاص داده است. در این 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 شایسته مورد انتظار به عمل نیامده است و در مواقعی که اطلاعات غیرواقعی در مورد شخص منتشر شود، صرفاً 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 چهار مصوبه شورای عالی فضای مجازی، به حفظ حریم خصوصی کاربران تأکید شده و در ضوابط فنی اجرایی توسعه دولت الکترونیکی مصوب ۱۳۹۳ دبیرخانه

شورای عالی فناوری اطلاعات ملزم به تأسیس کارگروه با همکاری سازمان‌های 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 شده است. در قانون آیین دادرسی کیفری مصوب ۱۳۹۴ نیز در بخش دادرسی الکترونیکی، قوه قضاییه موظف به فراهم‌سازی 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 به کار برده‌اند.

ماده 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 درواقع 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 مستقلاً 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 وظیفه 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 شبکه ارتباطات ثابت و خدمات ارتباطی ثابت، به منظور صیانت از حریم خصوصی اطلاعات شخصی و ارتباطی کاربران و مشترکان ضوابطی وضع و ابلاغ شده است.

منشور حقوق شهروندی جمهوری اسلامی ایران مصوب ۱۳۹۵ در ماده ۳۵ به حریم خصوصی شهروندان در فضای سایبر توجه داشته و در مواد ۳۶ تا ۴۲ نیز بر رعایت حریم خصوصی تأکید کرده است، اگرچه 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 جنبه 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 - مقرراتی برآمده و اصلاح سازوکارهای نظام اداری را فراهم آورده است و در ماده ۱۹ منشور حقوق شهروندی در نظام اداری نقض مندرجات منشور اخیرالتصویب از مصادیق تخلفات اداری مندرج در ماده ۸ قانون رسیدگی به تخلفات اداری محسوب می‌شود.

ماده ۱ قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹ نیز متضمن احترام به حریم خصوصی و مالکیت داده‌هاست. ماده ۳۱ قانون مطبوعات ۱۳۶۴ افشای اسرار شخصی و هتک حرمت را ممنوع اعلام داشته و در تبصره ۳ ماده ۱ این قانون اصلاحی ۱۳۷۹ با مشمول قرار دادن نشریات الکترونیکی، در واقع صیانت از حریم خصوصی در فضای سایبر را لحاظ داشته است.



ماده 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» ماده ۵؛ یعنی تهیه مخفیانه فیلم یا عکس مبتذل از مراسم خانوادگی و تکثیر آن، اولاً، باید تهیه فیلم یا عکس مخفیانه باشد؛ ثانیاً، فیلم‌ها و عکس‌های تهیه شده مبتذل باشد. اشکال وارد مقید کردن فیلم یا عکس به قید مبتذل است، درحالی‌که افراد دوست ندارند که از اماکن اختصاصی آنها هیچ‌گونه عکس یا فیلمی بدون رضایت آنان گرفته شود. شایسته بود مقنن، از حریم خصوصی اطلاعات و داده‌های افراد در مقابل چنین تعدیاتی به طور مطلق حمایت می‌کرد. اشکال دیگر این ماده در مقید کردن تهیه 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 به صورت راحت و بدون پوشش کامل زندگی می‌کنند که تهیه عکس یا فیلم در حالت‌های عادی نیز، به ویژه از بانوان، ناقض حریم خصوصی است که باید مقنن از آن حمایت کند؛ اما نکته مثبت این ماده در بند «ب» مشاهده می‌شود که درباره تهیه فیلم یا عکس از محل‌های اختصاصی بانوان است. برخلاف تصور اولیه، حریم خصوصی در اماکن عمومی نیز به رسمیت شناخته شده و از آن حمایت می‌شود و استخرها، سالن‌های ورزشی و این‌گونه محل‌ها در زمان‌های خاصی که به بانوان اختصاص داده شده، در عین حفظ ویژگی عمومیت، از این نظر حریم خصوصی آنها محسوب شود. دادگاه اروپایی حقوق بشر نیز در دعوای پک علیه دولت انگلستان در

سال ۲۰۰۳ میلادی چنین حکم داد که حوزه‌هایی از تعامل فرد با دیگران حتی در یک مکان عمومی وجود دارد که در چارچوب زندگی خصوصی قرار می‌گیرد و با بهره‌مندی از این وصف، شایسته است قانون‌گذاران ما به وضع قوانین جدید، مبادرت ورزند که در آن به‌صراحت، مطالب و تصاویری که در فضای سایبر، پروفایل‌های شخصی شبکه‌های اجتماعی و گروه‌ها منتشر شده، حریم خصوصی افراد شناخته شود و با ناقضان این حریم برخورد شود.



توسعه فضای مجازی مانند همه پیشرفت‌های دیگر در زندگی بشر با پیامدهای منفی و مثبت همراه بوده است. یکی از بدترین پیامدها در این فضا، به خطر انداختن حریم خصوصی افراد است. حق حریم خصوصی حقی است سیال، متداخل و مرتبط با حقوق دیگری؛ به دلیل اهمیت و حساسیت این موضوع است که این حق علاوه بر پشتیبانی کافی در متون دینی، اعم از فقهی و اخلاقی، از حمایت حقوقی و کیفری نیز برخوردار است.



قانون مجازات اسلامی علاوه بر اینکه به حریم خصوصی در مواد متعدد توجه کرده، مواد زیادی را به حریم خصوصی در فضای سایبر و ارتباطی اختصاص داده است. در قانون مجازات اسلامی در بخش جرایم رایانه‌ای و در قسمت جرایم 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 به نوعی حق حریم خصوصی شهروندی لحاظ و محترم دانسته شده است و برای متعرضین به این حقوق مجازات در نظر گرفته شده است. در ماده ۷۴۵ قانون مجازات هم در حمایت از حریم خصوصی پخش فیلم و تصاویر افراد به وسیله سامانه‌های رایانه‌ای و مخابراتی به نحوی که به ضرر یا عرفاً موجب هتک حیثیت شود، جرم محسوب و برای آن مجازات در نظر گرفته شده است و نسبت به قوانین قبلی، پخش فیلم در فضای سایبر به‌صراحت مورد توجه واقع شده و از نکات 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 افراد و نارضایتی آنان منجر شود، بدون اینکه امکان پیگیری قانونی وجود داشته باشد. قانون مجازات اسلامی همچنین در مواد ۵۸۲ و ۶۴۱ با تعیین مجازات برای مأموران و مستخدمان دولتی که غیرقانونی، مراسلات یا مخابرات اشخاص را مفتوح، توقیف یا بازرسی یا استراق سمع می‌کنند و مزاحمان که از وسایل ارتباطی استفاده می‌کنند، 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 تحت پوشش قرار می‌دهد و برای ناقضان 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 جرایم علیه عفت و اخلاق عمومی نیز انتشار اطلاعات شخصی و اسرار اشخاص جرم انگاری 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 به عهده 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. علاوه بر این، حفظ فوری داده‌های رایانه‌ای که جز در موارد اضطراری تنها با دستور مقام قضایی به عمل می‌آید، به منزله افشای اطلاعات سامانه‌های محافظت شده نیست و دیگر اینکه در تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی بر اساس قانون، به‌منظور صیانت از حریم و حرمت اشخاص از دسترسی مجریان قانون به داده‌ها و اطلاعات غیرضروری ممانعت به عمل آمده و تصریح شده است که باید بر پایه ظن متعارف مشخص کنند که به کدام داده‌ها یا سامانه‌ها برای پیگیری کیفری خود نیاز دارند و اعمال ساز و کارهای کنترل ارتباطات اشخاص نیز مشمول ضوابط سخت‌گیرانه‌ای شده و از هرگونه اعمال سلیقه از سوی مجریان قانون جلوگیری شده است.

ممنوعیت مطلق افشای اطلاعات و داده‌های جمع‌آوری شده و ممنوعیت مطلق بهره‌برداری از آنها توسط مراجع قضایی، مالیاتی مندرج در ماده ۷ قانون مرکز آمار ایران، مبین اصل (ناشناسی داده‌ها) و به معنای عدم افشای هویت موضوع داده‌هاست؛ بنابراین استنباط می‌شود که وارد کردن داده‌های مربوط در پایگاه‌های اطلاعاتی دولت الکترونیک و غیره ممنوع است (محسنی، ۱۳۸۸: ۴۸۷-۴۸۸) و این خود بیانگر حساسیت قانون‌گذاران در دهه‌های گذشته در

صیانت از حریم خصوصی شهروندان است که حتی دسترسی مقامات قضایی و دولتی به اطلاعات شخصی را نیز غیرممکن ساخته است.

قانون تجارت الکترونیکی هم در مواد ۵، ۵۸ و ۵۹ به حریم خصوصی و حمایت از داده‌ها توجه داشته و در ماده ۷۱ این قانون نیز برای ناقضان این حق، مجازات حبس تعیین شده است. مطابق این قانون برای حفظ حریم خصوصی و امنیت شهروندان ضروری است ابزارهای الکترونیکی و شیوه‌های حفاظت از سیستم پویا باشد و روش‌های حفاظت از سیستم به‌روزرسانی شود و این شرایط با توجه به اوضاع و احوال مبادله پیام ارزیابی می‌شود. ایراد وارد بر آن این است که مدعی مطمئن بودن سیستم باید ادعای خود را اثبات کند و شرایط مندرج در این ماده برای دادگاه احراز شود و دادگاه برای احراز شرایط، موضوع را به کارشناس ارجاع می‌دهد که مستلزم صرف هزینه و زمان زیادی است و بعضاً ممکن است مدعی توان اثبات نداشته باشد. از این‌رو شایسته است برخی روش‌های فنی موجود که از شرایط اطمینان برخوردارند، به‌عنوان امارات اطمینان دلیل معرفی شوند که پیش‌نویس این قانون در ماده ۱۲۷ راهکاری را در این خصوص مدنظر داشت و کمیته‌ای با عنوان کمیته فناوری و استانداردسازی سیستم‌های اطلاعاتی پیش‌بینی کرده بود تا بهترین روش‌های موجود را با توجه به آخرین دستاوردهای علمی به‌عنوان راهنمای عمل منتشر کنند که روش‌های فنی معرفی شده بدون نیاز به اثبات می‌توانستند در دادگاه مورد قبول قرار گیرند که این بند در تنظیم نهایی حذف شد. از این‌رو باید با استفاده از نسخه‌های استاندارد و رویه‌های متحدالشکل از بار اثبات دعوا کاست (عبدالمهی و شهبازی نیا،

۱۳۸۸: ۱۲۹-۱۲۳) و صرفاً با همکاری دولت‌ها در سطح جهانی 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 به عمل آورد.

در قانون تجارت الکترونیکی، ذیل قسمت جرایم و مجازات‌ها، در ماده‌های 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 محرمانه 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 داده‌پیام و ذکر مصادیق اطلاعات شخصی و پیش‌بینی ضمانت اجرا برای متخلفان در این قانون با گذشت بیش از یک دهه آیین‌نامه مربوط تصویب نشده است.

مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب ۱۳۸۰ شورای عالی انقلاب فرهنگی (جلسات ۴۸۲-۴۸۸) اگرچه در بند ۵-۳-۱۰ قسمت «ب» با عنوان آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا، شرکت‌ها یا مؤسسات ارائه‌کننده خدمات اطلاع‌رسانی و اینترنتی، رسا (ISP) را موظف به در نظر گرفتن تمهیدات برای حفظ حقوق کاربران و جلوگیری از حمله به کامپیوترهای آنان کرده و در بند ۵-۳-۱۲ نیز آنان را مکلف ساخته که اطلاعات مربوط به نحوه حفاظت از حریم خصوصی اطلاعات



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. به نظر می‌رسد مهم‌ترین مانعی که تاکنون سبب شده این حوزه بنیادی در بخش‌های تقنینی و بالطبع تنظیمی از زیرساخت قانونی جامع‌الشمولی برخوردار نشود، این است که این حق بنیادی بشری به ویژه در بستر ارتباطات و فناوری اطلاعات نوین خواسته یا ناخواسته در برابر دو حوزه نظم و امنیت عمومی از یک‌سو و فعالیت‌های اقتصادی سایبری از سوی دیگر قرار گرفته است. گروه نخست، با چالش بسیار جدی دشواری شناسایی تهدیدها و تهدید آفرینان در فضای بیکران سایبری روبه‌روست و چنانچه به هنگام و به اندازه، اطلاعات مورد نیازش فراهم نیاید، نمی‌تواند به وظیفه حیاتی‌اش عمل کند و فعالان اقتصادی نوین، به‌ویژه آنهایی که کسب‌وکار خود را در فضای سایبر و مبتنی بر داشته‌های آن بنیان نهاده‌اند، مانند کلان داده‌ها، به اطلاعات فزاینده این فضا نیاز دارند. از این‌رو ضروری است در تدوین مصوبات حاکم بر این حوزه، درباره این موضوعات نیز تصمیم منصفانه و منطقی اتخاذ شود.

قضایی، ابلاغی رئیس قوه قضاییه در سال ۱۳۹۲ و آیین‌نامه نحوه استفاده از سامانه‌های رایانه‌ای و مخابراتی، ابلاغی رئیس قوه قضاییه در سال ۱۳۹۵ هم به رعایت حریم خصوصی تأکید ورزیده است. بر اساس ماده ۶ اصول حاکم بر صدور پروانه دفاتر پیشخوان دولت و بخش عمومی غیردولتی مصوب کمیسیون تنظیم مقررات ارتباطات در جلسه شماره ۲۶۱ مورخ ۱۳۹۶/۵/۱۵ به استناد تبصره ۲ ماده ۲۶ قانون اساسنامه شرکت ملی پست جمهوری اسلامی ایران مصوب ۱۳۹۵/۵/۱۸ و بند «پ» ماده ۶۷ قانون برنامه ششم توسعه کشور، تحت عنوان آیین‌نامه صدور مجوز تأسیس و راه‌اندازی، تعهدات و وظایف دارنده پروانه، شرایط مکان و تجهیزات دفتر، تمدید، تغییر نام و مکان دفتر و لغو پروانه، در بند ۱۲ ماده ۲ که وظایف و اختیارات دارنده پروانه را بیان می‌کند، حفظ و حراست از اسناد، مدارک و اطلاعاتی که در اختیار وی قرار می‌گیرد، در زمره وظایف دارنده پروانه است که بیانگر توجه نهاد مقررات‌گذار به حفظ حریم خصوصی شهروندان است. در ماده ۱۵ دستورالعمل اجرایی ارائه 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

و ارتباطات افراد در شبکه خود را در اختیار کاربران قرار دهد و این بندها و نیز بندهای ۵-۳-۱۵، ۶-۱۳، ۶-۱۷ و ۶-۱۹ به نوعی توجه به حریم خصوصی و پیشگیری از دسترسی به داده‌های شخصی است، لیکن در شق «ج» بند ۶ قسمت «الف» با عنوان آیین‌نامه نحوه اخذ مجوز و ضوابط فنی نقطه تماس بین‌المللی، دایرکننده نقطه 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. از این‌رو نمی‌توان این مصوبه را کاملاً همسو با حفظ حریم خصوصی شهروندان و صیانت از حریم آنان توسط دولت دانست؛ چراکه اولاً به ذخیره کلیه داده‌ها و دسترسی وزارت ارتباطات به آن منجر می‌شود؛ از طرف دیگر مدت نگهداری داده‌ها 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

برآمد

نقض حریم خصوصی در فضای واقعی به طور معمول با نوعی حضور و تقرب مکانی همراه است. تحقق این عمل مجرمانه بدون آگاهی و اطلاع قربانی دشوار است. چون مرزهای حریم واقعی در اختیار و کنترل انسان است و همین آگاهی امکان دفاع و مقابله را تا حد زیادی برای وی فراهم می‌سازد؛ اما یک کاربر ماهر می‌تواند مرزهای فضای خصوصی قربانی در محیط سایبر را درنوردد، بدون اینکه کمترین اطلاعی از این امر پیدا کند و قدرت مقابله یا لاقط پیش‌بینی عواقب مسئله برای او ممکن باشد. همه این ویژگی‌ها موجب تشدید آثار مخرب نقض حریم در فضای مجازی می‌شود. شدت، سرعت، سهولت و گستردگی آسیب‌های ناشی از این نوع نقض، در صورت تسری به فضای واقعی، طبیعتاً اتخاذ تدابیر پیشگیرانه با درجه بازدارندگی بالا، توسط قانون‌گذار را اقتضا می‌کند. در این شرایط، ضمانت اخلاقی بی‌شک کفایت نمی‌کند. حتی مسئولیت مدنی نیز بازدارندگی کافی ندارد؛ بنابراین باید متناسب با ابعاد وسیع جرم و آسیب‌های فردی و اجتماعی ناشی از آن، مجازات کیفری

در خور اندیشیده شود. بی گمان مسئولیت مدنی و کیفری ناظر به وقوع جرم در فضای واقعی، در زمینه مسئله فضای مجازی کارایی و بازدارندگی کافی را ندارد. اکنون در بعضی کشورهای جهان مجازات‌های بسیار سنگینی علیه متجاوزان به این حریم اعمال می‌شود. در فضای مجازی ما با حقوق دیگری نیز مواجه می‌باشیم که موجب تعارض می‌شود. برخی از این تعارض‌ها در عرصه حقوق فردی و بعضی دیگر در عرصه عمومی مطرح می‌شود. در عرصه عمومی، دولت به عنوان حافظ نظم و امنیت در عرصه‌های مختلف، واجد حقوق و تکالیفی است. حق فردی حریم که آن را از حقوق منفی شمرده‌اند، به این معنا که دولت مکلف به تکلیف منفی (عدم‌مداخله) است، گاهی با حقوق تأمین دولت تعارض دارد. حقوق و تکالیف تأمین دولت؛ مانند تأمین جزایی، حقوقی، اقتصادی و اجتماعی، بی‌شک به این نهاد حق نقض حریم خصوصی را، چه در فضای واقعی و چه در محیط مجازی، می‌دهد. در این زمینه دو معیار و ضابطه، یکی خفیف‌تر و دیگری سخت‌گیرانه‌تر، مطرح شده است. کمیته حقوق بشر میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۷)، معقول بودن مداخله دولت را معیار قرار داده، ولی کنوانسیون اروپایی برای حمایت از حقوق بشر و آزادی‌های بنیادین (ماده ۸)، ضروری بودن مداخله را به‌عنوان ضابطه کلی وضع کرده است. 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 مجازات اسلامی ضمانت اجرای نسبی برای نقض این حق پیش‌بینی شده است. لیکن خلأهای زیادی چه از لحاظ ساختار سازمانی نهادهای تقنینی - مقررات‌گذاری و چه در مفاد قواعد وضع شده وجود دارد. الگوبرداری از ادبیات حقوقی، قانونی و مقرراتی کشورهای پیشرو و موفق و تطابق قواعد داخلی با مصوبات بین‌المللی و منطقه‌ای و بومی‌سازی آن‌ها با شرایط و اقتضائات داخلی در راستای وضع قوانین و مقررات ارتباطی و فناوری اطلاعات روزآمد و کارآمد ضرورتی انکارناپذیر است، در غیر این صورت استفاده صرف از ادبیات حقوقی و قوانین کشورهای موفق به دلیل ناهمگونی در اجرا با چالش‌هایی مواجه خواهد شد.

ناآشنایی کاربران و کنشگران عرصه سایبری با قواعد و مقررات حقوق شهروندی و الزامات حقوق بشری و نیز تهدیدهای این فضا از جمله نقض حریم خصوصی و عدم درک لزوم نظام‌مند ساختن فضای سایبر توسط آنان، از جمله مشکلاتی است که در آن ضرورت قاعده‌مند کردن فضای سایبر درک نشده است. از این رو آموزش شهروندان و مدیران مسئول با قواعد بین‌المللی، منطقه‌ای و قوانین و مقررات کشورهای موفق می‌تواند هم‌نیاز به وضع این قواعد و مقررات را به یک مطالبه جدی ملی مبدل کند و هم دستگاه‌های اجرایی با تهیه و تدوین پیش‌نویس قوانین و مقررات حوزه صیانت از حقوق شهروندی در فضای سایبر خلأهای موجود را پر خواهند کرد.

برای حفظ حریم خصوصی و حمایت از داده‌ها، در راستای محدودیت میزان دسترسی نمایندگی‌های اپراتور به اطلاعات مشترکان و ممنوعیت دسترسی آنان به داده‌ها دستورالعملی تدوین شود و نظارت صحیح و آنلاین توسط رگولاتور صورت پذیرد.

فهرست منابع

- ۱- انصاری، باقر، حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی و ایران، مجله دانشکده حقوق و علوم سیاسی، شماره ۶۶، ۱۳۸۳
- ۲- انصاری، باقر، حقوق حریم خصوصی، تهران، سازمان مطالعه و تدوین کتب علوم انسانی، ۱۳۹۱
- ۳- باستانی، پرومند، جرایم کامپیوتری و اینترنتی، چاپ بهنامی، سال ۱۳۸۳
- ۴- پروجیدی، مهدخت، حریم خصوصی در جامعه اطلاعاتی، تهران، انتشارات دادگستر، ۱۳۸۲
- ۵- بهمنی قاجار، محمدعلی، دادرسی عادلانه بر پایه قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی، مجله اطلاعات سیاسی - اقتصادی، شماره ۲۳۹، ۱۳۸۶
- ۶- پور قهرمانی، بابک؛ و علی صابرزاد، حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، تهران، انتشارات مجد، چاپ ۱، ۱۳۹۴
- ۷- رحمدل، منصور، حق انسان بر حریم خصوصی، مجله دانشکده حقوق و علوم سیاسی، دوره ۷۰، شماره ۱۰، ۱۳۸۴
- ۸- صاعی، پرویز، حقوق و اجتماع، جلد ۱، تهران، انتشارات طرح نو، چاپ ۱، ۱۳۸۹
- ۹- عالیپور، حسن، حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، تهران،
- انتشارات خرسندی، ۱۳۹۰
- ۱۰- محسنی، فرید؛ و فریدون قاسم‌زاده، حریم شخصی در فضای مجازی با تکیه بر حقوق ایران، فصلنامه علمی و پژوهشی شریف، شماره ۳۴، ۱۳۸۵
- ۱۱- نوری، محمدعلی؛ نخجوانی، رضا، حقوق حمایت داده‌ها، تهران: کتابخانه گنج دانش، ۱۳۸۳
- ۱۲- وکیل، امیرساعت؛ عسکری، پوریا، قانون اساسی در نظم حقوق کنونی، تهران: مجد، ۱۳۸۸
- 13- Fang, Binxing, **Cyberspace Sovereignty**, Singapore, Springer, 2018
- 14- Hyun Jin, Chang, **"Self-Concepts in Cyber Censorship Awareness and Privacy Risk Perceptions: What Do Cyber Asylum-Seekers have,"** Computers in Human Behavior, 2018
- 15- Baihua, Wen, **"An Assessment of the Strategic Situation in Cyberspace"**, International Strategic Relations and China's National Security, 2016
- 16- Airey v. Ireland, 9 October, 32, Series A no. 32. 1979