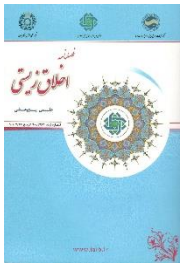

مجله اخلاق زیستی

دوره یازدهم، شماره سی‌وششم، ۱۴۰۰

https://doi.org/10.22037/bioeth.v11i36.35377

مقاله پژوهشی

چالش‌های راهکارهای پیشگیری وضعی از جرائم فضای مجازی با تأکید بر حریم خصوصی و آزادی بیان

سمیرا گلخندان[1]*، جواد گودرزی[2]، اکبر رجبی[3]

۱. استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکده علوم انسانی، واحد خمین، دانشگاه آزاد اسلامی، خمین، ایران.

۲. دانشجوی دکتری گروه حقوق کیفری و جرم‌شناسی، دانشکده علوم انسانی، واحد خمین، دانشگاه آزاد اسلامی، خمین، ایران.

۳. استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکده علوم انسانی، واحد خمین، دانشگاه آزاد اسلامی، خمین، ایران.

اطلاعات مقاله

تاریخ دریافت: ۱۴۰۰/۰۱/۲۳

تاریخ پذیرش: ۱۴۰۰/۰۵/۱۴

تاریخ انتشار: ۱۴۰۰/۱۰/۱۳

واژگان کلیدی:

پیشگیری از جرم

فضای مجازی

حق بر آزادی

حق بر حریم خصوصی

* نویسنده مسؤول: سمیرا گلخندان

آدرس پستی: ایران، خمین، دانشگاه آزاد اسلامی، دانشکده علوم انسانی، گروه حقوق کیفری و جرم‌شناسی.

کد پستی: ۳۸۸۱۶۱۳۴۸۵

پست الکترونیک:

S.golkhandan@gmail.com

چکیده

زمینه و هدف: در حوزه جرم‌شناسی، اولویت اصلی فعالیت دولت‌ها، پیشگیری از ارتکاب جرائم می‌باشد. پیشگیری وضعی یکی از روش‌های پیشگیری غیر کیفری است که با کاهش فرصت‌ها یا زمینه‌ها و موقعیت‌های جرم و از بین‌بردن این فرصت‌ها به کنترل و کاهش سطح جرائم ارتکابی از جمله در فضای مجازی کمک کند. هدف از پژوهش حاضر بررسی چالش‌های راهکارهای غیر کیفری پیشگیری از جرائم در فضای مجازی در ارتباط با حق بر حریم خصوصی و حق بر آزادی بیان می‌باشد.

مواد و روش‌ها: این تحقیق به روش توصیفی ـ تحلیلی انجام یافته است. روش جمع‌آوری اطلاعات به صورت کتابخانه‌ای است و ابزار آن، اسناد، کتب و مقالات موجود می‌باشد.

ملاحظات اخلاقی: در انجام پژوهش حاضر، ضمن پایبندی به اصالت متن، اصول اخلاقی صداقت و امانتداری رعایت شده است.

یافته‌ها: از یکسو، حق بر حریم خصوصی در سه فضای نظارت الکترونیک، نظارت مادی و شکل‌گیری جوامع نظارتی با چالش اساسی مواجه می‌شود و از سوی دیگر، حق بر آزادی بیان به واسطه پهنای باند پایین، موتورهای جستجوگر معین و محدود و همچنین نرم‌افزارهای پالایشگر، با محدودیت و نقض مواجه می‌شود.

نتیجه‌گیری: راهکارهای غیر کیفری پیشگیری از جرائم در فضای مجازی به واسطه نقض تعهدات حقوق بشری راجع به حق بر آزادی بیان و حق بر حریم خصوصی، عملاً برای دولت مسؤولیت‌زا خواهد بود. در ارتباط با نقض حق بر آزادی بیان، باید نظام مسؤولیت مشدد برای دولت در نظر گرفت، زیرا حق بر آزادی و مصادیق آن، جزئی از قواعد آمره حقوق بین‌الملل عام محسوب می‌شوند، اما در ارتباط با حق بر حریم خصوصی، اِعمال رژیم مسؤولیت عادی برای دولت، متناسب خواهد بود.

۱. مقدمه

در حوزه جرم‌شناسی عموماً تأکید بر فرآیند پیشگیری می‌باشد، لذا در این راستا باید نسبت به طراحی و اجرای راهکارهای پیشگیری از جرم، ظرافت و دقت فراوانی به کار برد، زیرا در عمل راهکارهای پیشگیری با برخی از سایر حقوق افراد در تعارض قرار می‌گیرد. فضای مجازی دارای ویژگی‌های خاصی، از جمله سرعت بالا، عدم امکان رهگیریِ جهت جریان اطلاعات، دسترسی عموم مردم و ارتباط نزدیک با افکار عمومی و... می‌باشد. فضای مجازی به واسطه ویژگی‌های خاص آن ارتباط نزدیکی با برخی از مصادیق حقوق بشر از جمله حق بر حریم خصوصی و حق بر آزادی بیان دارد. یکی از کارکردهای اصلی فضای مجازی دسترسی آزاد به جریان اطلاعات می‌باشد که در راستای اجرای حق بر آزادی بیان تعریف می‌شود. بر همین اساس در ماده ۲ قانون دسترسی و انتشار آزاد اطلاعات مشعر است که هر شخص ایرانی حق دسترسی به اطلاعات عمومی را دارد، مگر آنکه قانون منع کرده باشد. استفاده از اطلاعات عمومی یا انتشار آن‌ها تابع قوانین و مقررات مربوط خواهد بود. از طرفی دولت‌ها برای پیشگیری از وقوع جرائم مختلف در فضای مجازی از ابزارها و روش‌های پیشگیری مختلفی استفاده می‌کنند.

یکی از روش‌های پیشگیری از وقوع جرم، پیشگیری وضعی می‌باشد. در این روش، با تغییر وضعیت فرد یا شرایط محیطی مانند زمان و مکان، امکان ارتکاب جرم، کاهش یا از بین می‌رود. این روش در فضای مجازی کاربرد فراوانی دارد و دولت‌ها با وجود ابزارهای مختلفی از جمله فیلترینگ، به سادگی می‌توانند به اهداف خود در این زمینه نائل شوند. اعمال ابزارهای پیشگیری وضعی از جرائم در فضای مجازی، به صورت مستقیم بر مصادیق مختلف حقوق بشر از جمله جلوه خاص حق بر آزادی، یعنی آزادی بیان و حق بر حریم خصوصی تأثیر مستقیم می‌گذارد. پرسش اصلی که در پژوهش حاضر به دنبال پاسخ به آن هستیم، این است که راهکارهای غیر کیفری پیشگیری وضعی از جرائم در فضای مجازی چه چالش‌هایی برای حق بر حریم خصوصی و حق بر آزادی بیان ایجاد می‌کند؟

به عنوان تبیین پیشینه تحقیق، باید گفت که پیشگیری وضعی از جرائم در فضای مجازی مورد توجه برخی نویسندگان و پژوهشگران قرار گرفته است که در ادامه به نمونه‌هایی از این موارد اشاره خواهیم داشت:

در مقاله «پیشگیری وضعی در جرائم سایبری از منظر حقوق کیفری ایران و جهان» نوشته نصراله حیدری‌نژاد که در شماره ششم مجله قانون یار در سال ۱۳۹۷ به چاپ رسیده، آمده است: امروزه بحث فناوری اطلاعات و ارتباطات نوین که تجلی روشن آن فضای تبادل اطلاعات (فضای سایبری) است، مسأله جدیدی را به عنوان پاسخگویی به سوءاستفادهایی که از فضای تبادل اطلاعات به عمل می‌آید پیش روی دانشمندان علوم جنایی قرار داده است. یکی از پدیده‌های متفاوت و شگفت‌انگیز قرن بیست و یکم ظهور فضای سایبری و یا همان فضای مجازی است که سوءاستفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است، اما با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است. در این میان، پیشگیری وضعی یکی از اقدامات مهم و کاربردی محسوب می‌شود، ولی این پیشگیری با محدودیت‌هایی مواجه است که از جمله آن‌ها می‌توان به نقض موازین حقوق بشر اشاره کرد. ماهیت فضای سایبر به گونه‌ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است، اما تدابیر پیشگیرانه وضعی از جرائم سایبری، در بعضی موارد حقوق افراد را نقض می‌کند. در این مقاله سعی شده است ضمن تبیین انواع تدابیر پیشگیری وضعی از جرائم سایبری، به

تبیین چالش‌های حاکم بر این تدابیر با ملاحظه موازین حقوق بشری پرداخته شود.

در مقاله «راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی» نوشته غلامرضا شاه‌محمدی که در شماره نخست فصلنامه مطالعات راهبردی ناجا سال ۱۳۹۵ به چاپ رسیده است، از نظر نویسنده، فضای مجازی به دلیل ویژگی‌های خاصی مانند گمنامی و سهولت ارتباط، محملی برای انواع آسیب‌ها و جرائم است و با گذشت زمان بر حجم آسیب‌ها و جرائم این فضا افزوده می‌شود. فضای مجازی امکان آسیب‌رسانی به دیگران و آسیب‌دیدن را توأمان دارد. بنابراین پرداختن به مقوله پیشگیری از آسیب‌های مختلف این فضا که گستره تأثیر آن همه قشرهای جامعه را دربر می‌گیرد، امری ضروری و اجتناب‌ناپذیر است. بررسی تحقیقات انجام‌شده در حوزه پیشگیری از آسیب‌های فضای مجازی نشان می‌دهد که در این حوزه تحقیق زیادی انجام نشده است. هدف این تحقیق ارائه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی بوده است. در این تحقیق با مطالعات گسترده کتابخانه‌ای و تجارب محقق در حوزه فناوری اطلاعات، تدابیری در قالب راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی ارائه می‌شود. این تحقیق از نظر هدف از نوع کاربردی است و از نظر ماهیت به شیوه پیمایشی، انجام شده است.

به رغم انجام برخی تحقیقات گذشته، ضرورتی که برای پرداختن به این پژوهش احساس می‌شود، خاصه از این زاویه مبرهن است که راهکارهای غیر کیفری پیشگیری از جرم عموماً از طرف رکن اجرایی دولت پیشنهاد و اجرا می‌شوند؛ و از طرف دیگر، قوه قانونگذاری و مقررات حقوق بشر بین‌المللی به تضمین حقوق بشر و مصادیق آن اهتمام دارند. اصولاً هماهنگی میان این دو فضا باید به نحوی باشد که تعارض و تزاحمی میان هنجارها و راهکارهای اجرایی ایجاد نشود. اهمیت این موضوع زمانی مشخص می‌شود که بدانیم حقوق مزبور در فضای نظام حقوق بشر بین‌المللی به عنوان مصداقی از حقوق بنیادین بشری محسوب می‌شوند و در رأس سلسله مراتب هنجاری نظام حقوق بشر بین‌المللی قرار دارند. به بیان ساده‌تر، نقض این حقوق تبعات سنگینی برای دولت‌ها در عرصه حقوق و روابط بین‌المللی ایجاد می‌کند.

۲. ملاحظات اخلاقی

در انجام پژوهش حاضر ضمن پایبندی به اصالت متن، اصول اخلاقیِ صداقت و امانتداری رعایت گردیده است.

۳. مواد و روش‌ها

تحقیق حاضر از حیث نوع، یک تحقیق نظری است و روش تحقیق به صورت توصیفی ـ تحلیلی می‌باشد. همچنین از لحاظ روش جمع‌آوری اطلاعات، این تحقیق به صورت کتابخانه‌ای و با مراجعه به اسناد، کتب و مقالات، انجام گرفته است.

۴. یافته‌ها

یافته‌های پژوهش حاضر حاکی از آن است که راهکارهای غیر کیفری پیشگیری از جرائم در فضای مجازی در عمل به گونه‌ای اجرا می‌شوند که حریم خصوصی شهروندان، به واسطه عوامل نظارت مادی و الکترونیکی و همچنین شکل‌گیری جوامع نظارتی، با چالش‌های مهمی مواجه می‌شود. از سوی دیگر، راهکارهایی مانند پهنای باند پایین، استفاده از موتورهای جستجوگر معین و محدود و همچنین نرم‌افزارهای پالایشگر در عمل، حق بر آزادی بیان و همچنین حق بر دسترسی به جریان آزاد اطلاعات را که از حقوق تبعیِ حق بر آزادی بیان می‌باشد، نقض می‌کند. در این خصوص، دولت در قبال نقض و تخطی از حقوق مزبور، مطابق نظام حقوق مسؤولیت بین‌المللی دارای مسؤولیت مشدد می‌باشد.

۵. بحث

راه حل‌های پیشگیری وضعی از جرائم در مقام اجرا با مسائل و موانعی مواجه هستند که اعمال این راهکارها را با مشکل رو به رو می‌کند. جهت پیشنهاد هر نوع راه‌حلی برای جلوگیری از جرائم فضای مجازی لازم است که ضمن شناخت این مسائل، راهکاری نیز برای رویارویی و عبور از آن‌ها ارائه داد.

۵-۱. حریم خصوصی مجازی: توسعه سریع تکنولوژی اطلاعات، پیشگیری از بزه‌کاری احتمالی را آسان می‌نماید و بسیاری از موانع و محدودیت‌های پیشگیری از جرائم مادی در فضای مجازی وجود ندارد، اما همانطور که این ابزار منجر به تسهیل پیشگیری می‌شود، زیر پاگذاردن برخی از حقوق بشری نیز افزایش می‌یابد. با استفاده از این ابزارها «به جهت طبیعت باز شبکه، راه برای نیروهای پلیس آنچنان هموار است که بدون داشتن حکم بازرسی می‌توانند افراد را تحت کنترل قرار دهد.» برخلاف اجماع ضمنی همگان بر اهمیت برخورداری از حق حریم خصوصی در جهات مختلف زندگی، هنوز، تعریف خاصی از این حق وجود ندارد. یکی از عوامل عدم اجماع، وجود زمینه‌های فرهنگی، اجتماعی و تاریخی متفاوت جوامع بشری است، زیرا آنچه که در یک جامعه به عنوان حریم خصوصی پذیرفته شده، ممکن است در جامعه دیگر جنبه عمومی داشته باشد و همگان مجاز به اطلاع از آن باشند. همچنین در بُعد تاریخی «در جوامع سنتی پیش از صنعت و غیر دموکراتیک، حریم خصوصی در مفهوم امروزی آن وجود نداشته و نهایتاً آنچه مد نظر بوده است، حریم خصوصی فیزیکی، جایی برای انزوا یا پنهان‌بودن و دور از نظاره عموم بوده است (۱).

لازمه مفهوم امروزی حریم خصوصی، تمایز واضح بین مفهوم حوزه خصوصی و عمومی است که در جوامع گذشته این تمایز آنچنان وجهه نظر نبوده است. بشر کنونی امکانات زیادی در اختیار دارد؛ تکنولوژی اطلاعات و ارتباطات دنیای جدید را پیش روی انسان قرار داده‌اند، لذا احتمال تعدی به حریم خصوصی بشر عصر فناوری اطلاعات و ارتباطات، بسیار بیشتر از نیاکانش بوده و وی نیازمند حمایت بیشتر در مقابل هرگونه تجاوز به این حق را دارد.

حریم خصوصی در فضای مجازی در ابعاد گوناگون مورد حمایت قرار می‌گیرد و راهکارهای پیشگیری وضعی از جرائم فضای مجازی نباید مخالف با این حمایت‌ها باشد.

ـ اصل محدودیت جمع‌آوری داده‌ها: برای جمع‌آوری داده‌های شخصی باید محدودیت وجود داشته باشد و این داده‌ها باید با استفاده از ابزارهای قانونی، منصفانه و مناسب به دست آیند و رضایت یا اطلاع موضوع داده نیز تحصیل شود (۲).

ـ اصل کیفیت داده‌ها: داده‌های جمع‌آوری‌شده برای اهدافی که برای آن جمع‌آوری شده‌اند، به میزان لازم مورد استفاده قرار گیرند. همچنین داده‌ها باید دقیق، صحیح و روزآمد باشد (۳).

ـ اصل تعیین هدف: هدفی که داده‌ها برای آن گردآوری می‌شوند، باید قبل از جمع‌آوری داده‌ها تعیین شود. هرگونه استفاده بعدی از این داده‌ها باید محدود به هدف مورد نظر باشد و تغییرات بعدی در هدف باید مشخص شوند (۴).

ـ اصل استفاده محدود: داده‌های شخصی نباید افشا شوند، در دسترسی قرار گیرند و یا برای هدف دیگری غیر از اهداف تعیین‌شده مطابق پاراگراف قبلی (اصل تعیین هدف) مورد استفاده قرار گیرند (۵).

ـ اصل تدابیر امنیتی: داده‌های شخصی باید از طریق اقدامات امنیتی معقول در برابر خطراتی از قبیل نابودی یا دسترسی غیر مجاز، تخریب، استفاده، اصلاح و یا افشا مورد حمایت قرار گیرند (۶).

ـ اصل شفافیت: رویه کلی شفافیت باید درباره پیشرفت‌ها و سیاست‌های راجع به داده‌های شخصی وجود داشته باشد. همواره باید ابزارهایی به منظور تصدیق وجود و ماهیت و همچنین اهداف اصلی داده‌ها و نیز هویت و محل اقامت کنترل‌کننده داده وجود داشته باشد (۷).

ـ اصل مشارکت فردی: بر اساس این اصل، هر فرد باید حق داشته باشد تا از کنترل‌کننده داده‌ها و با روشی دیگر، تأییدیه‌ای مبنی بر در اختیارداشتن و یا نداشتن داده‌هایش دریافت کند و درباره داده‌های او با وی در ارتباط باشند؛ تا بر این اساس، ۱ـ جمع‌آوری این داده‌ها در یک زمان معقولی صورت گیرد؛ ۲ـ به صورت یک تکلیف مورد توجه باشد؛ ۳ـ داده‌ها از شیوه معقولی جمع‌آوری شوند؛ ۴ـ برای صاحب داده‌ها قابل فهم باشد. همچنین باید این حق برای صاحب داده‌ها وجود داشته باشد که اگر در خواست وی رد شد، دلایل رد آن به وی ابلاغ شود و حق اعتراض به رد درخواست نیز برای وی به رسمیت شناخته شود. صاحبان داده باید حق اعتراض به داده‌های مربوط به خودشان را داشته باشند و در صورت تأیید اعتراض آن‌ها، داده‌ها حذف، تکمیل و یا اصلاح شوند (۸).

ـ اصل مسؤولیت: کنترل‌کننده داده‌ها برای انجام اقداماتی به منظور تأثیرگذاری بر اصول فوق، مسؤول می‌باشند.

با در نظرگرفتن اصول فوق، راه حل‌های پیشگیری وضعی از جرم، در برخی موارد نقض‌کننده حریم خصوصی هستند. برخی از چاره‌اندیشی‌های پیشگیرانه ماهیت نظارتی دارند و در صورت مراقبت از موقعیت‌های ارتکاب بزه قادر به پیشگیری از بزه احتمالی خواهند بود، اما در بعضی از شرایط این تدابیر از حریم خصوصی کاربران حفاظت نمی‌کند و از حدود قانونی تجاوز نموده و به عبارتی، حریم خصوصی کاربران را فدای پیشگیری از بزه احتمالی می‌نماید (۹).

در واقع حریم خصوصی آن قسمت از خصوصیات یا ویژگی‌های مربوط به فرد است که دیگران حق دخالت در آن را بدون رضایت شخص ندارند که به تعبیری دیگر آن را حق خلوت نیز می‌نامند (۱۰). قانون اساسی جمهوری اسلامی ایران در اصل ۲۳، تفتیش عقاید را ممنوع دانسته و اعلام نموده است هیچ کس را به صرف داشتن عقیده‌ای نمی‌توان مورد تعرض قرار داد.

۵-۱-۱. نقض حریم خصوصی در ارتباط با نظارت الکترونیک:

امروزه تدابیر نظارت الکترونیک از کارآمدترین تدابیر پیشگیرانه نظارتی می‌باشد که از بدو ورود این فناوری از آن برای رهگیری ارتباطات استفاده می‌شد، اما با توجه به ماهیت فضای مجازی، ابزارهای گذشته کارایی نداشته و امروزه از تدابیر جدید استفاده می‌شود. این تدابیر همان‌گونه که پیشگیری از جرائم فضای مجازی را آسان می‌نماید، به همان میزان نقض‌کننده حریم خصوصی کاربران نیز می‌باشند. در این زمینه، تهدید بالقوه‌ای برای حفاظت از این حق در جریان پیشگیری وجود دارد، زیرا برقراری تعادل بین رعایت این حق و اجرای تدابیر اتخاذشده، دشوار می‌باشد.

یکی از کارآمدترین روش‌های پیشگیری از بزه‌دیدگی کاربران، نظارت بر انتقال داده‌ها در فضای مجازی از طریق روش‌های هوش مصنوعی داده‌کاوی می‌باشد که این امر نیازمند در اختیارداشتن داده‌های کاربران در بانک‌های داده است (۱۱).

یکی از اصول مهم در این رابطه، تأمین داده‌ها در فرایند جمع‌آوری داده است. بر اساس این اصل با استفاده از ابزارهای قانونی، داده‌های کاربران جمع‌آوری می‌گردد. این اصل انعکاس قواعد مندرج در اسناد حقوق بشری برای حفاظت از حریم خصوصی است و وفق آن جمع‌آوری داده‌ها باید طبق قانون زیر نظر مقام قضایی صالح باشد و اگر قانون اجازه گردآوری داده‌های الکترونیک را نداده باشد، مقام قضایی اجازه صدور دستور گردآوری داده‌ها را نخواهد داشت. در همین خصوص ماده ۴ قانون انتشار و دسترسی آزاد به اطلاعات مشعر است بر اینکه «اجبار تهیه‌کنندگان و اشاعه‌دهندگان اطلاعات به افشای منابع اطلاعات خود ممنوع است، مگر به حکم مقام صالح قضایی و البته این امر نافی مسؤولیت تهیه‌کنندگان و اشاعه‌دهندگان اطلاعات نمی‌باشد.» استفاده از روش‌های پیشرفته نظارت الکترونیکی توسط نهادهای مذکور باعث نقض حریم خصوصی کاربران و ایجاد مسؤولیت برای آن‌ها نمی‌شود. آن دسته از بانک‌های داده که با اجازه مقام قضایی و

رعایت‌نمودن اصل گردآوری داده‌ها به صورت قانونی تأمین گردد، موجب نقض امنیت داده‌ها نخواهد شد. در این‌گونه موارد مأمورین پیشگیری از جرائم فضای مجازی در مورد استفاده از نرم‌افزارهای نظارت الکترونیکی مانند داده‌کاوی با مشکلی مواجه نمی‌گردند. در بیشتر موارد، برای پیشگیری مؤثر از جرائم فضای مجازی، باید داده‌های کاربران را در بانک‌های گسترده و در گروه‌های مختلف دسته‌بندی نمود، زیرا با التفات به سرعت انتقال داده‌ها در فضای مجازی، انسان در شناسایی شرایط جرم توانایی نداشته و شیوه‌های سنتی نظارت نیز پاسخگو نیستند (۱۲).

به هر تقدیر فضای مجازی با توجه به ویژگی‌های خاصی که دارد (از جمله عدم امکان کنترل گردش اطلاعات یا رهگیری جهت جریان اطلاعات)، حق بر حریم خصوصی را با چالش‌های مهمی مواجه کرده است. نکته جالب توجه این است که فعالیت‌های پیشگیرانه دولت‌ها، نظیر شنود ارتباطات الکترونیک، و فیلترینگ نیز به نوبه خود موانعی را برای اعمال و اجرای حقوق مزبور ایجاد نموده است. راهکاری که در این زمینه می‌توان ارائه نمود این است که قانون را فصل‌الخطاب بدانیم و شنود کنترل فضای الکترونیک در موارد ضروری و صرفاً با حکم قضایی امکان‌پذیر باشد.

بدین‌ترتیب با نظارت شدید فعالیت کاربران شبکه، می‌توان از بسیاری از موقعیت‌های احتمالی بزه‌دیدگی و بزه‌کاری جلوگیری نمود. نمونه بارز نقض حریم خصوصی بر خط به علت داده‌کاوی غیر قانونی فعالیت کاربران را می‌توان در ماه اوت سال ۲۰۱۳ در آمریکا رؤیت نمود. به دنبال جستجوی واژگان «کوله‌پشتی»، «زودپز» و «حادثه بمب‌گذاری آوریل سال ۲۰۱۳ بستون» توسط پدر، مادر و فرزند پسر خانواده در موتور جستجوگر شرکت گوگل، نیروهای ضد تروریستی آن‌ها را مظنون به عملیات تروریستی سال ۲۰۱۳، دانستند که در آن انفجارهای سه‌گانه‌ایی توسط دو برادر چچنی به نام‌های جوهر و تیمورلنگ تسارنایف صورت گرفت. آن‌ها از زودپز به عنوان کاور بمب استفاده نمودند. «زودپز در نزدیکی خط پایان مسابقه منفجر شد. در نتیجه این حمله سه نفر کشته و ۲۶۴ نفر مجروح شدند.» قضیه از این قرار بود که «مادر قصد داشت انواع زودپز را بشناسد، پدر می‌خواست بداند که چگونه می‌تواند کوله‌پشتی و چیزهای دیگر بخرد و پسر در مورد بمب‌گذاری که در آوریل سال ۲۰۱۳ در بستون اتفاق افتاده بود جستجو می‌کرد و همین عبارات کافی بود تا مقامات امنیتی، مظنون به طراحی حادثه‌ای مانند بمب‌گذاری سال ۲۰۱۳ بستون شدند.» نیروهای امنیتی روز بعد پس از محاصره منزل و دستگیری اعضای خانواده و بازرسی کتاب‌ها و آلبوم‌ها و بازجویی از آن‌ها اظهار داشتند که عبارات یافت‌شده موجب ظن آن‌ها به تهیه بمب خانگی و جاسازی آن در زودپز و وقوع حادثه‌ای چون بمب‌گذاری سال ۲۰۱۳ بستون شده‌اند؛ این واقع، نشانگر وجود نرم‌افزارهای داده‌کاوی پیشرفته است. نرم‌افزارهایی که بانک‌های داده آن‌ها حداقل از میزبان‌های شرکت گوگل تأمین می‌شوند و داده‌های جمع‌آوری‌شده متعلق به کاربران آمریکایی هستند و برای پیشگیری از جرائم احتمالی تروریستی تعریف شده‌اند. علاوه بر روش‌های «داده‌کاوی، دوربین‌های مداربسته نیز می‌توانند منجر به نقض حریم خصوصی کاربران شوند» (۱۳).

لذا چنانچه این دوربین‌ها در حدی که ناظران طبیعی مجاز هستند، مورد استفاده قرار گیرند، ایرادی بر کار آنان وارد نیست و استفاده از این دوربین‌ها در اماکن عمومی برای تأمین امنیت در قالب قانونی مجاز است و می‌توان از آن‌ها در اماکنی چون هتل‌ها، کافی‌نت‌ها و یا مدارس استفاده نمود. باید توجه داشت که استفاده از آن‌ها باید در راستای فعالیت‌های متعارف و قانونی مأموران این اماکن باشد و از این ابزار می‌توان برای نظارت بر فعالیت‌های خصوصی کاربران استفاده نمود. امروزه دوربین‌های مداربسته‌ای وجود دارند که صدا و تصویر را ضبط می‌کنند. بنابراین مراجعی که از فناوری انتقال صدا در بستر شبکه استفاده می‌کنند و تماس تلفنی یا گفتگوی ویدیویی

انجام می‌دهند، صحبت‌ها و تصویر طرف مقابل ضبط می‌گردد. همچنین با استفاده از خاصیت بزرگ‌نمایی این دوربین‌ها می‌توان حرکات مراجعین را زیر نظر داشت (۱۴).

از این رو ناظران می‌توانند بفهمند که کاربران چه مطالبی را مطالعه می‌کنند و از چه رمز عبوری استفاده و با چه کسی صحبت می‌کنند و به محض دریافت کوچک‌ترین نشانه‌های ارتکاب بزه، از ادامه فعالیت او جلوگیری می‌کنند. بنابراین از انتقادات وارده بر استفاده از این دوربین‌ها برای پیشگیری از بزه‌کاری احتمالی این است که این دوربین‌ها از روش سراسر بینیِ «Bentham» برای تحت نظرگرفتن فعالیت‌های کاربران استفاده می‌کنند، زیرا همانطور که زندانی در زندان پیشنهادی سراسر بینِ «Bentham» حق استفاده از حریم خصوصی را ندارد، این دوربین‌ها هم همان کاربرد را دارند و فعالیت‌های کاربر را ضبط می‌کنند و همان‌گونه که «Foucault» بیان می‌دارد «سراسر بین کاربرد چندگانه دارد.» بنابراین برای پیشگیری از بزه‌کاری جرائم فضای مجازی می‌توان از شیوه سراسربینی دوربین‌های مداربسته استفاده نمود و به منظور جلوگیری از مفاسد احتمالی ناشی از بکارگیری این دوربین‌ها باید مانند سایر حوزه‌های نظارتی قائل به این باشیم که دوربین‌های مراقبتی از همان محدودیت‌های پلیس برخوردار است یا خیر (۱۵).

بنابراین در این خصوص هرگونه بحث در مورد نقض حریم خصوصی کاربران در نتیجه استفاده از دوربین‌های مداربسته مستلزم بررسی دقیق نحوه استفاده از این ابزارها است، به گونه‌ای که فرضاً دوربین‌های مداربسته از نوع سراسربین نباشند؛ لذا، صرف استفاده از دوربین‌های مداربسته حریم خصوصی را نقض نمی‌کند. در واقع عواملی مانند نوع دوربین، مکان مورد استفاده، افراد تحت نظارت و مواردی از این دست عوامل مؤثر در احراز نقض حریم خصوصی هستند.

۵-۱-۲. نقض حریم خصوصی در ارتباط با نظارت مادی: یکی از راهکارهای جلوگیری از جرائم فضای مجازی، مراقبت از طریق مدیران محلی می‌باشد. به طور مثال سرپرستان اماکن عمومی ارائه‌دهنده خدمات دسترسی حضوری، یا مسؤولین مدارس در قلمرو این نوع از نظارت قرار می‌گیرند. یکی از تدابیر رایج در بعضی از کشورها، از جمله کشور ما، تشکیل پرونده کاربری برای کسانی است که به اماکن عمومی ارائه‌دهنده خدمات دسترسی مراجعه می‌کنند (۱۶).

متصدیان این اماکن مجبور به ثبت اطلاعات هویتی مراجعان و ذخیره‌کردن فعالیت آنان می‌باشند. مطابق بند ۸ بخش‌نامه پلیس فتا به کافی‌نت‌ها، مسؤولان این اماکن ملزم به ثبت اطلاعات هویتی و سایر اطلاعات می‌باشند، هرچند که استفاده از اطلاعات عمومی در بیشتر حوزه‌های خدمات‌رسانی مورد نیاز است و در اکثر نظام‌های حقوقی مشخصاتی مانند نام و نام خانوادگی در قلمرو حریم خصوصی محسوب نمی‌گردند، اما مسؤولین این اماکن با داشتن شماره شناسایی کاربران، نام و هویت آن‌ها در کنار سایر اطلاعات مانند صفحات ذخیره‌شده توسط دوربین‌های مداربسته، حافظه مرورگرهای اینترنتی، کلیدهای ورود به سیستم و مواردی از این قبیل، کوچک‌ترین فعالیت کاربران از دید این ناظران پنهان نمی‌ماند. با مطابقت مباحث ذکرشده و با راهکارهای وضعی نظارتی بیان‌شده در قسمت اول بحث، معین می‌گردد که صرفاً برای پیشگیری از جرم نمی‌توان وارد تمام قلمرو حریم خصوصی کاربران شد و در بیشتر موارد این سؤال طرح می‌شود که با توجه به فراوانی فضاهای موجود در دنیای مجازی چه معیاری برای به کار بردن تدابیر نظارتی ـ الکترونیکی و مادی وجود داشته، و به عبارتی چه فضاهایی خصوصی بوده و بدون اجازه مقام قضایی نمی‌توان به آن‌ها ورود نمود (۱۷). پاسخ به این سؤالات کمک فراوانی برای اجرای راهکارهای نظارتی پیشگیرانه مادی و مجازی می‌نماید، لذا بایسته است که به بررسی این موضوع و ارائه راه حل‌های درخور برای آن پرداخته شود.

لزوم حفاظت از حریم خصوصی کاربران و تعهد به اصول حمایت از داده‌ها، سازمان‌های مسؤول پیشگیری از جرم را از

نظارت مطلق بر داده‌های کاربران منع می‌کند؛ این نهادها فقط با اجازه قانونگذار و مقام قضایی می‌توانند به منظور پیشگیری از موقعیت‌های ارتکاب جرم از طراحی روش‌های نظارتی با بانک‌های اطلاعاتی اندک، استفاده نمایند.

به عنوان نمونه فرض نمایید مقامات امنیتی شهری متوجه شوند که در یکی از نامه‌های پست‌شده در ماه اخیر، طرح ترور یکی از مقامات عالی سیاسی یا نخبگان علمی کشور شرح داده شده است؛ یکی از راه حل‌های پیشگیری از این عملیات تروریستی این است که تمام نامه‌های دریافتی این شهر در فاصله زمانی ۳۰ روز گذشته توقیف شده و محتویات همه نامه‌ها دقیقاً بررسی شوند. از یکسو نامه‌های شهروندان جزء حریم خصوصی آن‌هاست و باید قانوناً محترم شمرده شوند و از سوی دیگر شاید بتوان نامه مذکور را که به این شهر ارسال شده است را از میان نامه‌های ارسالی پیدا نمود و با بازرسی تمام نامه‌ها و یافتن نامه مورد نظر از وقوع جرم احتمالی پیشگیری نمود. تفاوت این روش با نرم‌افزارهای داده‌کاوی این است که از هوش مصنوعی استفاده نشده و عامل انسانی مبادرت به تجزیه و تحلیل و پیش‌بینی می‌نماید، اما با این اقدام حریم خصوصی همه دریافت‌کنندگان نامه‌ها را باید نقض نمود (۱۸).

سؤالی که مطرح می‌شود، این است که آیا می‌توان برای پیشگیری از این خطر، حریم خصوصی کاربران را نقض نمود؟ برای نزدیک‌نمودن ذهن به این نظریه از مثال معروف «شکنجه و بمب ساعتی» کمک می‌گیریم که به طور خلاصه بیان می‌شود. به موجب این سناریو «پلیس، تروریست احتمالی را که مکان بمبی مهیب را می‌داند و ممکن است که تعداد بسیاری از افراد را به کشتن دهد، دستگیر نموده، حال آیا برای جلوگیری از این اتفاق و با هدف یافتن مکان بمب، می‌تواند وی را شکنجه نماید؟ و یا اینکه نباید وی را شکنجه کرد و با انفجار بمب احتمالی سبب مرگ افراد بی‌گناه شد؟» پاسخ ما به آن سؤال فرضی منفی است، زیرا طبق اصل برائت مجرم بودن فرد هنوز ثابت نشده است. همچنین اگر شکنجه را برای موارد استثنایی مجاز بدانیم، باید تشکیلاتی را برای این کار سازماندهی نمود و افرادی برای این منظور آموزش داد تا همیشه منتظر چنین حوادثی باشند و پس از مدتی شکنجه برای حالت اضطرار ـ با توجیح خطر برای منافع عمومی ـ امری عادی تلقی می‌گردد. تجاوز به حریم خصوصی برخط شهروندان در جهت جلوگیری از وقوع جرائم احتمالی مانند مثال قبلی است، هرچند ممکن است با در نظرنگرفتن حریم خصوصی کاربران از درصد بالایی از جرائم احتمالی جلوگیری کرد، اما در این صورت کاربران بهنجار فدای اقدامات خطرآمیز بزه‌کاران می‌شوند و به بهای جلوگیری از بزه احتمالی قلمرو حریم خصوصی خود را از دست می‌دهند. همچنین هیچ‌گونه تضمینی برای جلوگیری از جرم احتمالی بعد از نقض اولین حریم خصوصی وجود ندارد؛ به منظور پیدانمودن راهکاری برای ایجاد تعادل بین جلوگیری از جرم و حفاظت از حریم خصوصی کاربران باید حریم خصوصی را از جهت انسانی و جامعه‌شناختی مورد توجه قرار داد، زیرا با توجه به هر فرد و هر جامعه درمی‌یابیم توقع متفاوتی از حریم خصوصی وجود دارد. امری که امروزه از آن به عنوان انتظار معقولی از حریم خصوصی بیان می‌شود و حتی در برخی از قوانین ذکر شده است (۱۹).

هرچند با استناد به قانون، داده‌های کاربران را می‌توان برای مدت معینی ذخیره کرد، لیکن نهادهای نظارتی تحت هیچ شرایطی حق بررسی همه داده‌ها را نخواهند داشت. آن‌ها تنها زمانی می‌توانند محتویات ترافیک داده‌ها را بررسی کنند که دستور پرونده‌ای از مرجع قضایی داشته باشند و حتی نمی‌توانند ترافیکی را که طبق قانون دارند، وارد بانک‌های نرم‌افزاری داده‌کاوی کنند و یا الگوهای جدید متناسب با این داده‌ها طراحی کنند. آن‌ها باید اکثریت قریب به اتفاق فرصت‌های مجرمانه را نادیده بگیرند و از داده‌های کاربران عادی برای جلوگیری از جرم استفاده ننمایند.

از همین روی با تکیه بر این مفهوم تلاش در بازبینی قلمرو مجاز ورود مأموران فضای مجازی به حریم فعالیت کاربران خواهیم داشت. برخی از نویسندگان از جهت اختلاف اطلاعات خصوصی از اطلاعات عمومی برای توجیح این مفهوم بهره برده‌اند. به نظر آنان اطلاعات آن دسته از رفتارهایی که فرد منطقاً انتظار دارد که مورد نظارت قرار نگرفته یا ذخیره نشوند، در حوزه اطلاعات خصوصی جای دارند. بعضی دیگر عقیده دارند که «زمانی که فرد انتظار واقعی از حریم خصوصی دارد و جامعه آن انتظار را به عنوان انتظاری منطقی بپذیرد، انتظار معقول از حریم خصوصی وجود خواهد داشت.» به نظر می‌رسد که توقع عاقلانه از حریم خصوصی زمانی وجود دارد که عرف جامعه دموکراتیک، تعدی به آن را غیر مجاز محسوب می‌کند. علت ذکر قید دموکراتیک این است که به دلیل شرایط حاکم بر جوامع مختلف، توقع شهروندان جامعه‌ای غیر دموکراتیک از حقوقشان در مقایسه با شهروندان دموکراتیک کمتر است و نیز به علت «عادت‌کردن آن‌ها به تدابیر نظارتی، انتظار متعارف از حریم خصوصی نیز کاهش خواهد یافت» (۲۰).

برای جلوگیری از وقوع جرائم احتمالی و شناخت شرایط تهدیدآمیز بر اساس این میزان که در چه محیط‌هایی توقع عاقلانه از حریم خصوصی وجود دارد و ورود به آن‌ها نیاز به مجوز به قضایی دارد؟ و بالعکس چه محیط‌هایی عمومی محسوب می‌شوند و امکان ورود به آن‌ها وجود دارد؟ باید گفت همان‌گونه که در دنیای واقعی توقع افراد از حریم خصوصی با توجه به جامعه‌ای که در آن قرار دارند، متفاوت است، این انتظار در فضای مجازی نیز وجود دارد. به همین جهت به عنوان یک اصل کلی نمی‌توان اظهار نمود که در محیط عمومی، حریم خصوصی وجود ندارد، بلکه در این محیط‌ها نیز حریم خصوصی محترم شمرده می‌شود، اما نمی‌توان به اندازه محیط شخصی انتظار مراعات حداکثری آن را داشت. بنابراین به قول یکی از نویسندگان «اشخاصی که در اماکن عمومی به سر می‌برند، باید قبول کنند که تابع و تسلیم حوادث و اتفاقات عادی و طبیعی در زندگی اجتماعی روزمره هستند» (۲۱).

زمانی که برای ورود به فضایی باید اجازه گرفت و افراد عادی نمی‌توانند بدون اجازه وارد آن شوند، حریم خصوصی افراد نیز در سطح بالاتری قرار داشته و نمی‌توان برای جلوگیری از وقوع جرم و یا هر منظور دیگری بدون اجازه کاربران و یا حکم قضایی وارد آن فضا شد، زیرا مانند آن است که نیروی پلیس برای پیشگیری از جرم احتمالی در جمع افرادی که در پارک با هم گفتگو می‌کنند حضور یابد (۲۲).

چنانچه مأموران نظارتی داده‌های مورد نظر را در بازرسی‌های فضای مجازی مورد بررسی قرار دهند یا اینکه آن‌ها را در بانک‌های داده نرم‌افزارهای داده‌کاوی قرار دهند، نمی‌توان به دلیل نقض حریم خصوصی بر آن‌ها ایرادی وارد نمود. برای نمونه چنانچه کاربری در صفحه رسمی خود نرم‌افزارهای ضد پاکسازی قرار دهد، متصدیان ناظر وظیفه دارند اقدام به بستن صفحه وی نمایند، اما چنانچه آن کاربر با پست الکترونیکی شخصی خود این نرم‌افزارها را برای کاربر دیگر بفرستد، نمی‌توانند اقدامی انجام دهند، زیرا اصل بر این است که مأموران نظارت حق بررسی فعالیت کاربران را در قلمرو شخصی بدون اجازه مقام قضایی ندارد. همان‌گونه که سازمان‌های نظارتی در دنیای واقعی در محیط عمومی اقدام به بازرسی و شناسایی فرصت‌های مجرمانه می‌کنند، همین امر در فضای مجازی نیز اجرا می‌گردد. نهادهای نظار برای بررسی صفحات عمومی، شناخت خلأها و کاهش نفوذپذیری می‌توانند از نیروی انسانی استفاده کنند. نهادهای ناظر می‌توانند برای دسترسی به داده‌های موجود از نرم‌افزارهای داده‌کاوی در فضای مجازی استفاده کنند و نمی‌توان بر آن‌ها خورده گرفت، زیرا هر کس به این فضاها دسترسی دارد و روش دسترسی به این فضاها برای آن‌ها مانند دیگران است، ولی نمی‌توانند نامه‌های الکترونیکی، عبارات مورد جستجو، تاریخچه فعالیت کاربران و مواردی مانند آن را بدون اجازه مقام قضایی مورد

بازبینی قرار دهند. اهمیت موضوع زمانی روشن می‌گردد که به توانایی‌های زیادی که فضای مجازی در اختیار بزه‌کاران قرار می‌دهد، توجه کنیم. از جمله مواردی که ارتکاب جرم را در فضای مجازی آسان می‌کند، پولشویی الکترونیکی، تصاویر هرزه‌نگاری، دعوت به همکاری با گروه‌های تروریستی و انتقال محتویات مجرمانه می‌باشند (۲۳).

بنابراین نگارنده معتقد است هر چیزی که نیاز به زندگی اجتماعی دارد، بخشی از حریم خصوصی در خارج نخواهد بود، لیکن همانطور که مرکز حفظ حریم خصوصی اطلاعات الکترونیکی می‌گوید، تا زمانی که مردم در یک محیط عمومی حرکات غیر عادی انجام ندهند، نمی‌توانند انتظار حفظ حریم خصوصی را داشته باشند. تشخیص حریم خصوصی فرد به رفتار او در محیط عمومی بستگی دارد. فرضاً وقتی چند نفر از دوستان در یک پارک با صدای نسبتاً آهسته صحبت می‌کنند، انتظار دارند که سیستم شنوایی وجود نداشته باشد و مکالمات آن‌ها ضبط نشود و رهگذران در حالی که در جمع هستند، از مکالمات آن‌ها مطلع نشوند، لذا در همان محیط عمومی آن‌ها انتظار دارند که حریم خصوصی آن‌ها حفظ گردد، در نتیجه چانچه شخصی بخواهد از مکالمات آن‌ها مطلع شود، باید اجازه بگیرد و سپس وارد حریم خصوصی آنان شود، در غیر این صورت هرگونه اقدامی در جهت شنیدن مکالمات آن‌ها، شنود غیر مجاز تلقی می‌شود. در این فرض وقتی فردی از طریق بلندگو صحبت می‌کند، نمی‌تواند انتظار داشته باشد که حریم ارتباطی او حفظ شود. این اصل در فضای مجازی هم وجود دارد.

۵-۱-۳. نقض حریم خصوصی در ارتباط با شکل‌گیری جوامع نظارتی: اگرچه حاکمیت‌ها از چاره‌اندیشی‌های وضعی نظارتی برای تأمین امنیت حداکثری کاربران استفاده می‌نمایند، بنا به تجربه درمی‌یابیم که کاربران این‌گونه حاکمیت‌ها کمتر در معرض بزه‌دیدگی و ضررهای جبران‌ناپذیر ناشی از آن قرار می‌گیرند، اما این پرسش باقی مانده که تأمین این امنیت به چه بهایی صورت می‌گیرد؟ آیا این حق زمانی ارزش دارد که کرامت انسانی آن‌ها مورد تعرض قرار نگیرد و یا در مقابل محافظت از بزه‌دیدگی، ارزش‌های بنیادین آن‌ها کنار گذاشته و یا محدود گردد؟ آنچه که موجب انتقادات بیشتر از به کارگرفتن همه‌جانبه تدابیر وضعی نظارتی می‌گردد، این است که اگرچه تدابیر مورد نظر با مراقبت دائم موجب کاهش بزه‌دیدگی می‌گردند و شرایط ارتکاب جرائم احتمالی را از بین می‌برند، لیکن همین مراقبت گسترده موجب تشکیل جوامع نظارتی می‌شوند. جوامعی که در بسیاری از ابعاد آن، تعهد به صیانت از حریم خصوصی به کمترین حد خود رسیده است و کرامت انسانی کاربران قربانی ایجاد نظم و امنیت عمومی خواهد شد و این امر به فراموشی سپرده شده است که «حریم خصوصی ایشان نیز چهره‌ای از همان امنیتی است که دولت متکفل تأمین آن است»، اگرچه با به کارگیری تدابیر امنیتی مانند استفاده از نرم‌افزارهای فوق پیشرفته داده‌کاوی، نصب دوربین‌های مداربسته در اماکن ارائه‌دهنده خدمات دسترسی، تشکیل پرونده برای مراجعین و مواردی مانند آن می‌توان از بسیاری از جرائم فضای مجازی جلوگیری نمود، اما این پرسش همچنان باقی است که به چه بهایی از خطر بزه‌دیدگی کاربران کم می‌شود؟ (۲۴).

در بعضی از قوانین حوزه فناوری اطلاعات کشورمان کمبودهای فراوانی رؤیت می‌شود که در عمل مجوز تشکیل بانک‌های داده‌کاوی نیرومند را به مقامات ناظر می‌دهند. مورد اول مربوط به «آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا» می‌باشد. قبل از بررسی موارد نقض‌کننده حریم خصوصی کاربران در این آیین‌نامه، لازم است که به طور مختصر به بررسی این آیین‌نامه که جزء مصوبات جلسات ۴۸۲ تا ۴۸۶ و همچنین جلسه ۴۸۸ شورای عالی انقلاب فرهنگی است، بپردازیم.

ابتدا باید به این سؤال پاسخ داد که آیا شورای عالی انقلاب فرهنگی شایستگی ورود به این حوزه و تصویب آیین‌نامه را

دارد یا نه؟ به نظر می‌رسد که این نهاد شایستگی ورود در این زمینه را داشته باشد، چراکه اگر آیین‌نامه مذکور به منظور اجرایی‌نمودن قانونی خاص در این حوزه اجرا می‌شد، اشکالی متوجه آن نمی‌بود و صرفاً قواعد اجرایی را معین می‌نمود. این آیین‌نامه بر اساس جلسات ۴۸۲ تا ۴۸۶ و همچنین جلسه ۴۸۸ شورای انقلاب فرهنگی تصویب شده است که البته در این راستا مقررات ناظر بر شورای عالی فضای مجازی و قوانین مربوط به دسترسی و انتشار اطلاعات نیز حائز اهمیت‌اند و همچنین دولت، وزارت ارتباطات و فناوری اطلاعات، وزارت فرهنگ و ارشاد اسلامی، بنیاد ملی بازی‌های رایانه‌ای، قوه قضاییه، صدا و سیما، نیز آیین‌نامه‌ها و مصوباتی داشته‌اند که هر کدام با نظارت خود به عنوان نهادی نظارتی با تصویب مصوبه‌ها و آیین‌نامه‌های مختلف به نوعی اسباب نقض حریم خصوصی را فراهم ساخته‌اند.

اما آنچه که سبب ایجاد بانک‌های ترافیک داده‌های کاربران و شکستن حریم خصوصی آنان و در عین حال روش حداکثری برای جلوگیری وضعی از جرائم احتمالی فضای مجازی می‌شود، مقرری شماره پنج از قسمت سوم بند پنج آیین‌نامه صدر الاشاره است که بر اساس آن «هر رسا (ISP) موظف است اطلاعات کلی کاربران و IPهای مربوط را ثبت و یک نسخه از آن را به وزارت پست و تلفن اعلام نماید». خورده‌گیری‌های موجود در بند فوق که موجبات نقض حریم خصوصی بر خط کاربران را فراهم نموده‌اند، عبارتند از: اولاً مقنن از «اطلاعات» نام برده و ذکر ننموده که هدف وی از این واژه چه بوده است، بلکه با اضافه‌نمودن وصف «کلی» دستیابی متصدیان نظارتی را به بسیاری از اطلاعات شخصی کاربران آسان نموده است؛ ثانیاً شرایط و قواعدی را که رساها بر اساس آن‌ها اقدام به ضبط اطلاعات کاربران نمایند را معین نکرده است و راه برای به دست‌آوردن غیر مجاز اطلاعات هموار است؛ ثالثاً در مواردی که جمع‌آوری اطلاعات محتاج طی‌نمودن جریان قضایی می‌باشد را به حساب نیاورده است؛ در صورتی که باید گرفتن دستور مرجع قضایی خاص برای صدور مجوز دسترسی به اطلاعات شخصی کاربران را ضروری می‌شمرد و تعهدات قانونی برای محترم‌شمردن حق حریم خصوصی کاربران را پیش‌بینی می‌کرد. بنابراین احتمالاً یکی از اهداف مهم قراردادن این بند، اتخاذ پیش‌بینی‌های لازم برای پیشگیری از وقوع جرائم از طریق نظارت مداوم بر فعالیت‌های کاربران و شناسایی موقعیت‌های ارتکاب جرم بوده است، اما در عین حال موفق به ضمانت‌نمودن یکی از اساسی‌ترین حقوق افراد، یعنی حریم خصوصی بر خط نشده است.

مورد دوم، «قانون جرائم رایانه‌ای» است؛ یکی دیگر از موارد نقض حریم خصوصی بر خط کاربران در حین پیشگیری از جرائم و کشف و دنبال‌نمودن مجرمین فضای مجازی، مواد ۳۲ و ۳۳ قانون جرائم رایانه‌ای است. به موجب ماده ۳۲ این قانون: «ارائه‌دهندگان خدمات دسترسی موظف‌اند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.»

اگرچه قانونگذار تلاش نموده تا اشتباه آیین‌نامه سابق‌الذکر را در مورد ارائه تعاریف مبهم تکرار نکند، اما در نیل به این هدف موفق نبوده است و همچنان اختیارات بسیاری به منظور اخذ اطلاعات کاربران به مقامات ذی‌صلاح داده است. تبصره ۲ ماده ۳۲ سعی در تعریف «اطلاعات کاربر» نموده است تا رساها مطلقاً مجبور به دادن این موارد به مقامات ذی‌ربط باشند، لیکن با به کاربردن الفاظ کلی و نامشخص و تشبیه‌کردن مفاهیم، قلمروی را معین ننموده است، لذا متصدیان نظارت می‌توانند با استناد به تبصره مبنی بر اهمیت دسترسی به اطلاعات برای اهداف مهمی مانند امنیت ملی، پیشگیری از جرم، مبارزه با تروریسم فضای مجازی و مواردی از این قبیل، تقاضای دریافت اطلاعات بیشتری در مورد کاربران داشته باشند.

ایراد مهم دیگری که به تبصره فوق وارد است، عبارت «سایر مشخصات فرد» است. این عبارت موجب افزایش اختیارات

ناظران شده و کمک بسیاری به نقض حریم خصوصی کاربران نموده است، زیرا سایر مشخصات فردی از نظر مقامات نظارت که به دنبال کشف جرم و یا پیشگیری از جرم می‌باشد، می‌تواند اطلاعات شخصی مهم از قبیل عقیده، نژاد، سابقه پزشکی و بسیاری از موارد دیگر باشد، در صورتی که از نظر مقام ناظر سهل‌گیر شامل این موارد نمی‌شود. همچنین در هر ۲ ماه «حداقل مدت نگهداری تعیین شده است، در حالی که لازمه ایجاد توازن میان منافع فردی یا منافع عمومی تعیین حداکثر مدت نگهداری نیز می‌باشد» (۲۵).

سومین ایراد مواد ذکر شده این است که تعهداتی یک‌طرفه برای رساها به منظور عرضه اطلاعات به مقامات ذی‌صلاح ایجاد نموده و هیچ ضمانتی برای حفاظت از حریم خصوصی برخط کاربران پیش‌بینی نشده است. یکی از نمونه‌های آشکار نقض حداکثری حریم خصوصی شهروندان به منظور پیشگیری وضعی از جرائم در قانون میهن‌پرستی ایالات متحده آمریکا رؤیت می‌گردد. طی مدت ۴۵ روز بعد از حادثه حمله به برج‌های دوقلو در تاریخ ۱۱ سپتامبر سال ۲۰۰۱، مجلس سنا اقدام به تصویب قانون میهن‌پرستی نمود. این قانون به منظور حفظ امنیت ملی و تضعیف مجرمین، حریم خصوصی برخط کاربران را نقض کرده است. بر اساس قسمت ۲۱۰ این قانون، مأموران پلیس با گرفتن اخطاریه اداری می‌توانند به اطلاعات مربوط به کارت اعتباری، شماره حساب، نشانی اینترنت و... کاربران که در حین ارتباطات الکترونیکی، استفاده شده است، دست پیدا کنند؛ درحالی که دستیابی به این اطلاعات مهم با گرفتن اخطاریه‌ای اداری، احتمال سوءاستفاده از اطلاعات را افزون می‌کند. از این رو لازم بود برای حفظ حریم خصوصی کاربران، تعهدات بیشتری برای دست‌یافتن به این اطلاعات در نظر گرفته می‌شد و صرف اخطاریه کفایت نمی‌کرد، بلکه نیاز به مجوز مرجع قضایی و صدور «قرار» می‌بود. همچنین برای تأیید درستی درخواست پلیس و به منظور حفاظت از حریم خصوصی کاربران و جلوگیری از درخواست‌های غیر ضروری، حداقل از میان سازمان پلیس، افرادی ناظر به عنوان نهاد تشخیص موارد درخواست‌شده معین می‌گردید؛ ثالثاً برخی از اطلاعاتی که پلیس فقط با اخطاریه‌ای، مایل به دسترسی به آن است اطلاعات بسیار مهمی است و جزء حریم خصوصی افراد تلقی می‌شود. مواردی مانند اطلاع از حساب بانکی کاربران خطرناک بوده و اجازه اطلاع مأموران را از منشأ نقل و انتقالات و موارد هزینه و... می‌دهد (۲۶).

یکی از دلایلی که برای درج این ماده و گستره وسیع آن بیان می‌گردد، مفیدبودن این اطلاعات است، زیرا تروریست‌ها و بزه‌کاران از اسامی جعلی برای ورود به اینترنت و یا استفاده از خطوط تلفن، بهره می‌گیرند و همین امر سبب ایجاد مشکلاتی برای شناسایی مظنونین حملات احتمالی تروریستی و یا کمک‌های انجام‌شده به آنان می‌شود. به همین دلیل دریافت مدت زمان اینترنت و حساب‌های بانکی در کنار سایر اطلاعات برای شناسایی مظنونین کمک می‌نماید. یکی دیگر از مشکلات مواد قانون میهن‌پرستی، قسمت ۲۱۶ آن است که وفق آن نهادهای نظارتی حکومتی قادرند با بهره‌بردن از اختیارات مندرج در این ماده از ابزارها و نرم‌افزارهای ردیابی اطلاعات الکترونیکی استفاده نمایند. ظاهراً این بخش از قانون برای مطابقت با نیاز نهادهای امنیتی وضع شده است، زیرا مقررات پیش از این قانون نیز اجازه ردیابی مکالمات تلفنی، ارتباطات فکس و ارتباطاتی از این قبیل را می‌دادند. با تصویب این ماده مأمورین امنیتی مجوز استفاده از نرم‌افزارهای ردیابی الکترونیکی اینترنتی را خواهند یافت. بر اساس این ماده بررسی موضوعات کلی ارتباطات الکترونیکی نیاز به تأیید مقام قضایی ندارد و زمانی که نیروهای پلیس خواهان دسترسی به محتویات ارتباطات باشند، درخواست آنان باید به تأیید مقام قضایی برسد. بررسی موضوعات ارتباطات الکترونیکی حاوی نشانی مکان‌یاب یکنواخت منبع وب، نشانی پروتکل اینترنت، موضوعات مندرج در پوشه‌های ارسالی و مواردی از این دست است. به عنوان نمونه زمانی که کاربر «الف» برای کاربر «ب»

ایمیل ارسال می‌نماید، نشانی مکان‌یاب یکنواخت منبع وب او ذخیره خواهد شد و به همین ترتیب معین می‌گردد که ایمیل از طرف چه کسی و برای چه شخصی در کدام نقطه دنیا ارسال می‌شود (۲۷).

در پایان لازم به ذکر است که معیار ارائه‌شده برای نظارت بر ارتباطات الکترونیکی معیار مناسبی نیست و موجب آگاهی ماموران از محتویات ارتباطات الکترونیکی می‌گردد. به عنوان نمونه زمانی که کاربران برای ایمیل‌های خود عنوانی را می‌نویسند عنوان، جزء محتوای نامه به حساب نیامده و مورد بررسی قرار نمی‌گیرد، در حالی که معمولاً عناوین انتخابی بیانگر محتویات مندرج در متن نامه هستند. برای حل این مشکل به نظر می‌رسد باید تأیید مقام قضایی در مورد این نظارت در هر صورت و تحت هر شرایطی وجود داشته باشد، زیرا اهمیت حفظ حریم خصوصی در فضای مجازی مهم‌تر از جنبه پیشگیری وضعی آن است.

۵-۲. حق بر آزادی بیان: امروزه از تدابیر سلب‌کننده یا محدودکننده دسترسی به عنوان تدابیر وضعی مؤثر برای پیشگیری تعداد زیادی از جرائم فضای مجازی استفاده می‌شود و در عمل بسیاری از این تدابیر، کم و بیش موجب تأمین امنیت این فضا می‌شوند، اما هر یک از این موارد، قابلیت نقض نسبی و یا مطلق آزادی بیان و جریان آزاد اطلاعات برخط را دارند. «ماهیت فناورانه برخی از تدابیر موقعیت مدار سایبری می‌تواند منجر به نقض حق آزادی جریان اطلاعات کاربران از طریق سلب و یا محدودیت آنان در دریافت، انتقال و یا اشتراک محتویات مورد نظرشان شود.» آزادی بیان از گذشته تاکنون اهمیت بسیار داشته و انسان همواره در پی ابراز افکار خود و تعامل با دیگران بوده است. انسان برای به دست‌آوردن این حق سختی‌های فراوانی را تحمل نموده، حکاکی بر روی سنگ‌ها، روزنامه‌ها، مجلات، تلگراف، نامه‌های الکترونیکی و شبکه‌های اجتماعی مواردی از سیر تحول ابزارهای ارتباطی و توسعه ارتباطات می‌باشند.

«جریان فلسفه سیاسی آزادی‌گرای غربی که تا اواخر قرن ۱۸ در حال گسترش بود، زیربنای مستحکمی برای آزادی بیان و مطبوعات فراهم ساخت. در آن عصر، جریان مذکور به صورت‌های گوناگون جلوه‌گری داشت. کسانی که آزادی بیان را ابزار ضروریِ مبارزه بر ضد قدرت استبداد تلقی می‌کردند و همچنین افرادی که مطبوعات را وسیله اعمال قدرت می‌شناختند، در مسیرهای مختلف این جریان که با مکتب خردگرای Rene Descartes (۱۵۹۶-۱۶۵۰ م.) مکتب حقوق طبیعی John Locke (۱۶۳۲-۱۷۰۴ م.) و مکتب برابری‌جویی Jean-Jacq Rousseau (۱۷۱۲-۷۸ م.) مشخص می‌شدند، گام برمی‌داشتند. عقاید اقتصادی فیزیوکرات‌ها که از لغو محدودیت‌های اقتصادی و صنفی و از یک استبداد قانونی محدود، به ویژه از طریق آزادی مطبوعات طرفداری می‌کردند، نیز فلسفه آزادی‌گرایی را تقویت می‌نمودند» (۲۸).

در حقوق اسلام آزادی بیان از جایگاه والایی برخوردار است. خداوند در قرآن کریم مکرر انسان را به تفکر در نشانه‌های خلقت، امر به معروف و نهی از منکر، مشورت با دیگران و گزینش بهترین نظر و جدال نیکو سفارش نموده است.

قانون اساسی جمهوری اسلامی ایران نیز به پیروی از شرع حق آزادی بیان را به رسمیت می‌شناسد، اما فصل خاصی را به آن اختصاص نداده است و در قالب اصول مختلف و در ذیل مباحث گوناگون به مواردی از این حق اشاره نموده است. به عنوان نمونه اصل ۲۴ قانون اساسی حق آزادی بیان را برای نشریات و مطبوعات به رسمیت شناخته است. به موجب این اصل «نشریات و مطبوعات در بیان مطالب آزادند، مگر آنکه مخل به مبانی اسلام و یا حقوق عمومی باشد؛ تفصیل آن را قانون معین می‌کند.»

اصل ۱۵۷ نیز آزادی بیان را از طریق صدا و سیما مورد تأکید قرار داده است. به موجب این اصل «در صدا و سیمای جمهوری اسلامی ایران، آزادی بیان و نشر افکار با رعایت

موازین اسلامی و مصالح کشور باید تعیین گردد.» «حق آزادی اندیشه و بیان» به عنوان ششمین بند از منشور حقوق شهروندی است که در سال ۱۳۹۵ ابلاغ گردید، در این خصوص می‌توان به مواد ۲۶ تا ۲۹ منشور حقوق شهروندی نیز استناد نمود. علاوه با موارد فوق اعلامیه حقوق بشر اسلامی ـ مصوب دسامبر ۱۹۸۹ میلادی ـ با پیروی از قاعده مذکور، برای اعمال محدودیت بر آزادی بیان مطلق، به بحث آزادی بیان و محدودیت‌های آن نگاه ویژه‌ای دارد و بند «الف» ماده ۲۲ اعلامیه اسلامی حقوق بشر برخورداری از حق آزادی بیان را برای همه انسان‌ها به رسمیت می‌شناسد. در میان تمامی محدودیت‌های آزادی بیان، اخلاق، تنها محدودیتی است که در تمامی اسناد بین‌المللی و منطقه‌ایِ حقوق بشر ذکر شده است. ماده ۱۹ اعلامیه جهانی حقوق بشر، بند ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۱۰ کنوانسیون اروپایی حقوق بشر و ماده ۱۳ کنوانسیون آمریکایی حقوق بشر، اخلاق را به عنوان خط قرمزی برای آزادی بیان پذیرفته‌اند. در ایران نیز صدا و سیما به موجب ماده ۱۹ قانون خط مشی کلی و اصول برنامه‌های صدا و سیما، مکلف به رعایت مسائل اخلاقی است.

منشور ملل متحد در برخی از موادِ خود وظایف کشورها در حمایت از حقوق بشر و آزادی‌ها و اعمال آن‌ها را مورد تصریح قرار داده است. بند «ج» ماده ۷۳ منشور، بند «ب» ماده ۱۳ منشور، بند ۳ ماده ۱ منشور، همینطور مواد ۵۵ و ۵۳ منشور نیز، احترام جهانی و رعایت حقوق بشر و آزادی‌های اساسی، را کانون توجه قرار داده‌اند. همچنین حق آزادی بیان در ماده ۱۹ اعلامیه جهانی حقوق بشر که مهم‌ترین سند بین‌المللی و اولین دستاورد کمیسیون حقوق بشر سازمان ملل متحد به شمار می‌رود، مورد تصریح قرار گرفته است. علاوه بر این وفق بند ۲ از ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، «هر کس حق آزادی بیان دارد. این حق شامل آزادی تفحص و تحصیل و اشاعه اطلاعات و افکار از هر قبیل بدون توجه به سر حدات خواه شفاهاً یا به صورت نوشته یا چاپ یا به صورت هنری یا به هر وسیله دیگر به انتخاب خود می‌باشد.»

اما سؤالی که مطرح می‌شود، این است که آیا آزادی بیان حق مطلقی بوده و انسان‌ها حق ابراز و دسترسی به هرگونه افکار و اندیشه‌های دیگران را دارند و یا این حق مانند سایر حقوق مدنی و سیاسی محدودیت دارد؟ با توجه به احتمال نتایج سوء آزادی بیان بدون قید و شرط می‌توان گفت، چنانچه انسان حق دسترسی به هرگونه عقاید و اطلاعاتی را به نحو مطلق داشته باشد، نظم عمومی و حقوق شخصی دیگران ضایع می‌گردد. با مطالعه اسناد حقوق بشر درمی‌یابیم که آزادی بیان حقی مطلق نیست و محدودیت‌هایی بر آن مقرر گشته است. از جمله بند ۳ از ماده ۱۹ میثاق اشاره دارد به اینکه اعمال حقوق مذکور در بند ۲، مستلزم حقوق و مسؤولیت‌های خاص است و لذا ممکن است تابع محدودیت‌های معینی بشود که در قانون تصریح شده و برای احترام حقوق یا حیثیت دیگران و حفظ امنیت ملی یا نظم عمومی یا سلامت یا اخلاق عمومی ضرورت داشته باشد.

در بحث حاضر نیز برخی از تدابیر پیشگیرانه وضعی گرچه کم و بیش منتهی به تأمین امنیت شبکه می‌شوند، لیکن قابلیت نقض نسبی و یا مطلق حق آزادی بیان را خواهند داشت. دسته‌ای از این تدابیر زمانی می‌توانند از بزه‌دیدگی احتمالی کاربران پیشگیری کنند که اجازه دسترسی آزاد آن‌ها را به شبکه ندهند و بدین طریق از ایجاد موقعیت‌های احتمالی بزه‌دیدگی جلوگیری نمایند. گروه دیگری از تدابیر پیشگیرانه، بزه‌کاران را هدف قرار داده و سعی در افزایش هزینه‌های ارتکاب بزه دارند، ولی به دلیل به کار بردن این تدابیر در سطح وسیع امکان نقض حق آزادی بیان کاربران را نیز فراهم می‌آورند و بعضاً آنان از دسترسی به شبکه منع خواهند شد.

۶. نتیجه‌گیری

اعمال راهکارهای غیر کیفری پیشگیری از جرائم در فضای مجازی به واسطه نقض تعهدات حقوق بشری راجع به حق بر آزادی بیان و حق بر حریم خصوصی، عملاً برای دولت مسؤولیت‌زا خواهد بود. نکته‌ای که در اینجا باید به آن دقت داشت، این است که در ارتباط با نقض حق بر آزادی بیان، باید مسؤولیت مشدد برای دولت در نظر گرفت، زیرا همانطور که مشاهده شد، حق بر آزادی و مصادیق آن، جزئی از قواعد آمره حقوق بین‌الملل عام محسوب می‌شود و در نتیجه نقض آن موجب اعمال رژیم مسؤولیت مشدد برای دولت خواهد شد، اما در ارتباط با حق بر حریم خصوصی باید رژیم مسؤولیت عادی برای دولت در نظر گرفت.

ممکن است دولت، در توجیه مسؤولیت خود به این اصل استناد کند که رفتارش در جهت پیشگیری وضعی از جرم بوده است، در نتیجه نباید برای او مسؤولیتی در نظر گرفت، اما باید دقت داشت که حق بر آزادی و مصادیق مختلف آن به موجب مفاد میثاق حقوق مدنی و سیاسی در رأس سلسله مراتب هنجاری حقوق بشر بین‌المللی قرار دارد، زیرا حق مزبور به عنوان یکی از مصادیق مسلم حقوق بنیادین بشری محسوب می‌شود. از طرفی حق بر حریم خصوصی در فضای حقوق بین‌الملل موضوعه جزئی از مصادیق حقوق بنیادین بشری محسوب نمی‌شود، بلکه جزء مصادیق حقوق بشر غیر آمره در نظر گرفته می‌شود، لذا همانطور که گفته شد، در موارد نقض قواعد آمره، رژیم مسؤولیت مشدد برای دولت‌ها منظور می‌شود. باید خاطرنشان کرد که در رژیم مسؤولیت مشدد، دولت نمی‌تواند به علل و عوامل موجهه مسؤولیت مانند ضرورت و اضطرار استناد کند. این استدلال شاید در ارتباط با حق بر حریم خصوصی که در حقوق بین‌الملل موضوعه مصداقی از قواعد آمره محسوب نمی‌شود، در جهت خفیف‌کردن مسؤولیت دولت قابل پذیرش باشد، اما استدلال مزبور در ارتباط با نقض حق بر آزادی بیان قابل قبول نیست. از طرفی نباید از نظر دور داشت که نقض حق بر آزادی بیان و حریم خصوصی در فضای مجازی با تصویب قوانین و مقررات داخلی و به صورت برنامه ریزی‌شده صورت می‌گیرد، در نتیجه از نظر نظام حقوق بشر بین‌المللی، نقض مزبور، یک نقض سیستماتیک یا به تعبیری نقض فاحش حقوق بشری قلمداد می‌شود.

۷. تقدیر و تشکر

از تمامی عزیزانی که با مشاوره و راهنمایی خود در تألیف این مقاله مساعدت نمودند، تقدیر و تشکر می‌شود.

۸. سهم نویسندگان

در این مقاله جواد گودرزی، مسؤولیت جمع‌آوری مطالب و نگارش مقاله را به عهده داشته است. سمیرا گلخندان و اکبر رجبی، ضمن راهنمایی و مشاوره در نگارش تحقیق، بر انجام آن نظارت داشته‌اند.

۹. تضاد منافع

در این مقاله هیچ‌گونه تضاد منافعی وجود ندارد.

References

1. Abolhassan F. Security: The Real Challenges for Digitalization. In: Abolhassan F. Cyber Security. Simply. Make it Happen.: Leveraging Digitization Through IT Security. London: Springer International Publishing; 2017. p.1-12. [Persian]

2. Grafenstein M. The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles and Private Standards as Elements for Regulating Innovation. Washington: Nomos; 2018. p.11-19.

3. Talburt J, Yeoh W, Zhou Y. Information Quality and Governance for Business Intelligence. London: IGI Global; 2013. p.400-401.

4. Pennings F, Besselink L, Prechal S. The Eclipse of the Legality Principle in the European Union. London: Kluwer Law International; 2011. p.279-281.

5. Mooradian NA. Ethics for Records and Information Management. Washington: American Library Association; 2018. p.127-128.

6. Gollmann D. Computer Security. London: Wiley; 2009. p.346-349.

7. Waldemarson Y. Openness and Elite Oral History: The Case of Sweden. In: Marklund C, Götz N. The Paradox of Openness: Transparency and Participation in Nordic Cultures of Consensus. London: Brill; 2014. p.173-196.

8. Bekkers V. Emerging Electronic Highways: New Challenges for Politics and Law. London: Springer; 2008. p.115-116.

9. Shalhoub Z, Qasimi L. Cyber Law and Cyber Security in Developing and Emerging Economies. London: Edward Elgar; 2010. p.138-139.

10. Bakhshayeshi Bayghoot M, Heidari M. Privacy in Iranian Law and International Documents. *Journal of International Police Studies.* 2018; 7(29): 207-232. [Persian]

11. Ransome J, Rittinghouse J. Voice over Internet Protocol (VoIP) Security. London: Elsevier Science; 2005. p.306-308.

12. Dudley A, Vincenti G, Braman J. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices. London: Information Science Reference; 2012. p.189-190.

13. Gercke M. Red Teaming and Wargaming: How Can Management and Supervisory Board Members Become More Involved in Cybersecurity? In: Cyber Security. Simply. Make it Happen. London: Springer International Publishing; 2017. p.27-36.

14. Abolhassan F. Cyber Security. Simply. Make it Happen.: Leveraging Digitization Through IT Security. London: Springer International Publishing; 2017. p.27-36. [Persian]

15. Marcella A, Menendez D. Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes. Washington: CRC Press; 2010. p.232-235.

16. Kirichenko A, Christen M, Grunow F, Herrmann D. Best Practices and Recommendations for Cybersecurity Service Providers. In: Gordijn B, Christen M, Loi M. The Ethics of Cybersecurity. London: Springer International Publishing; 2020. p.299-316.

17. Chander H. Cyber laws and IT Protection. London: PHI Learning; 2012. p.186-188.

18. Easttom C. CCFP Certified Cyber Forensics Professional All-in-One Exam Guide. New York: McGraw-Hill Education; 2014. p.25-29.

19. Singh Y. Cyber Laws. New York: Universal Law Publishing Company; 2010. p.182-185.

20. Watt E. State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. London: Edward Elgar Publishing; 2021. p.109-110.

21. Khosrowpour DB, editor. Encyclopedia of Criminal Activities and the Deep Web. London: IGI Global; 2020. p.417-420.

22. Hagen J, Lysne O. Protecting the digitized society: The challenge of balancing surveillance and privacy. *The Cyber Defense Review*. 2015; 1(1): 75-90.

23. Keshavarz M, Ansari A, Sheshgol H. Ontology of computer crimes according to the law of computer crimes. *Azad Comparative Law Researches Quarterly.* 2020; 13(47): 149-168. [Persian]

24. Kosseff J. Cybersecurity Law. London: Wiley; 2017. p.285-287.

25. Reveron D, Lindsay J, Cheung T. China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain. Oxford: Oxford University Press; 2015. p.319-321.

26. Dougherty T. Freedom of Expression and the Internet. Greenhaven Publishing LLC; 2010. p.6-10.

27. Rand D. Roots of the Arab Spring: Contested Authority and Political Change in the Middle East. Pennsylvania: University of Pennsylvania Press; 2013. p.129-130.

28. Gupta S, Gupta G. Information Security & Cyber Laws. London: Khanna Book Publishing Company; 2013. p.54-57.

Majale "Akhlāq-i zīstī" (i.e., Bioethics Journal)
2021; 11(36): e28
https://doi.org/10.22037/bioeth.v11i36.35377

ORIGINAL RESEARCH

Challenges of Cybercrime Situational Prevention Strategies with Emphasis on Privacy and Freedom of Expression

Samira Golkhandan[1]*, Javad Goodarzy[2], Akbar Rajabi[3]

1. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Humanities, Khomein Branch, Islamic Azad University, Khomein, Iran.

2. Ph.D. Student, Department of Criminal Law and Criminology, Faculty of Humanities, Khomein Branch, Islamic Azad University, Khomein, Iran.

3. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Humanities, Khomein Branch, Islamic Azad University, Khomein, Iran.

ARTICLE INFORMATION

Article history:

Received: *12 April 2021*

Accepted: *05 August 2021*

Published online: *03 January 2022*

Keywords:

Crime Prevention

Cyberspace

Right to Freedom

Right to Privacy

* **Corresponding Author:** Samira Golkhandan

Address: Department of Criminal Law and Criminology, Faculty of Humanities, Khomein Branch, Islamic Azad University, Khomein, Iran.

Postal Box: 3881613485

Email: S.golkhandan@gmail.com

ABSTRACT

Background and Aim: In the field of criminal law, the main priority of government activities is crime prevention. Situational prevention as a non-criminal prevention method helps to control and reduce the level of crimes committed, including in cyberspace, by reducing and eliminating the opportunities or grounds and situations of crime. The purpose of this study is to examine the challenges of non-criminal cybercrime prevention strategies in relation to the right to privacy and the right to freedom of expression.

Materials and Methods: This research has been done by descriptive-analytical method. The method of collecting information is library and its tools are documents, books and articles.

Ethical Considerations: In order to organize this research, originality of the text and the ethical principles of honesty and fidelity have been observed.

Findings: On the one hand, the right to privacy in the three areas of electronic surveillance, material surveillance and the formation of regulatory communities is facing a fundamental challenge and on the other hand, the right to freedom of expression is restricted and violated due to low bandwidth, certain and limited search engines as well as refining software.

Conclusion: Non-criminal cybercrime prevention strategies will effectively hold the government responsible for violating human rights obligations regarding the right to freedom of expression and the right to privacy. In connection with the right to freedom of expression, the system of aggravated responsibility for the government should be considered, because the right to freedom and its instances are part of the rules of public international law, but in relation to the right to privacy, current responsibility system seems to be consistent.

Cite this article as: Golkhandan S, Goodarzy J, Rajabi A. Challenges of Cybercrime Situational Prevention Strategies with Emphasis on Privacy and Freedom of Expression. *Majale "Akhlāq-i zīstī" (i.e., Bioethics Journal).* 2021; 11(36): e28.