پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران وجهان

(تاریخ دریافت۱۳۹۶/۱۲/۲۲ ، تاریخ تصویب ۱۳۹۷/۰۴/۰۸)

نصراله حیدری نژاد

پژوهشگر وکارشناس ارشد حقوق جزا و جرم شناسی

چکیده

امروز بحث فناوری اطلاعات وارتباطات نوین که تجلی روشن آن فضای تبادل اطلاعات (فضای سایبری) است.مسله جدیدی را به عنوان پاسخگویی به سوء استفادهایی که از فضای تبادل اطلاعات به عمل می آید پیش روی دانشمندان علوم جنایی قرار داده است.

یکی از پدیده های متفاوت وشگفت انگیز قرن بیست یکم ظهور فضای سایبری ویا همان فضای مجازی است .که سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری ار 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 وکاربردی محسوب می‌شود،ولی این پیشگیری با محدودیت هایی مواجه است که از جملهٔ آنها می توان 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 پیشگیرانهٔ وضعی از جرائم سایبری، در بعضی موارد حقوق افراد را نقص می کند.. در این مقاله سعی شده است ضمن تبیین انواع تدابیر پیشگیری وضعی از جرائم سایبری، به تبیین چالش های حاکم بر این تدابیر با موازین حقوق بشر بپردازد.

واژگان کلیدی: پیشگیری وضعی، جرایم سایبری ، حقوق بشر،آزادی بیان،حریم خصوصی، جریان آزادی اطلاعات

بخش اول: کلیات

انسان در طول حیات خود اعصار گوناگونی را پشت سر گذاشته است،وهر یک از آنها را با الهام از تحول عظیمی که در آن عصر پدید آمده وگامی از رشد وتکامل بشری را رقم زده نامگذاری کرده است ، مانند عصر آتش ،عصر آهن،عصر کشاورزی ،ودر حال حاضر عصر ارتباطات ،دوره‌های متفاوتی که با تغییر و تکامل مواجه بوده است. زمانی کشاورزی محوریت داشت، اما بشر پس از مدتی به این نتیجه رسید که با تحقق یک جامعهٔ صنعتی می‌تواند به آرزوهای خود دست یابد. لذا تمام همّ خود را در این راه نهاد و دورانی صنعتی را رقم زد که اوج آن را در سدهٔ نوزدهم میلادی شاهد هستیم. دو فناوری در عرصهٔ فناوری اطلاعات و ارتباطات نقش تعیین کننده‌ای به عهده داشته‌اند که عبارت‌اند از: رایانه و مخابرات هدف از اختراع رایانه، تسریع و تسهیل پردازش اطلاعات بود که به خوبی به ثمر نشست و مخابرات نیز به عنوان مهم‌ترین ابزار ارتباطی، در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است.

از حدود نیم‌قرن اخیر، به تدریج با کشف قابلیتهای شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصهٔ فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دههٔ نود میلادی به بعد، تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها که خود از بسیاری سیستم های رایانه‌ای متصل به یکدیگر تشکیل شده‌اند، به مدد فناوری های پیشرفتهٔ مخابراتی با یکدیگر ارتباط برقرار کرده و فضایی با ویژگی های کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند که عده‌ای آن را فضای مجازی نامیده‌اند و عده‌ای هم عنوان فضای سایبر را برای آن برگزیده‌اند.

اما ناگفته پیداست که فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیدهٔ بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به طور کلی، آنچه امروز تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند.

جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترس غیرمجاز به داده‌ها یا سیستم ها یا پخش برنامه‌های مخرب نظیر ویروسها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می‌شود .

همان‌گونه که ملاحظه می‌شود، به لحاظ امکان سوء استفادهٔ دوجانبه‌ای که از فضای سایبر وجود دارد، ضروری است برای آن چاره‌ای اندیشه شود. با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارت‌اند از: اقدامات کیفری و غیرکیفری. در زمینهٔ اقدامات کیفری سعی می‌شود از طریق جرم‌انگاری هنجارشکنی‌ها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفری گذشته، ارعاب‌انگیزی مؤثری دربارهٔ مجرمان بالقوه یا مکرر صورت گیرد تا به این ترتیب، از ارتکاب جرم بازداشته شوند. (نیازپور، ۱۳۸۲: ۱۲۴) اما رویکرد دوم که در بستر جرم‌شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی و .... پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. در این زمینه، تاکنون الگوهای مختلفی در عرصهٔ جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. بنابراین، آنچه در اینجا واجد اهمیت است اینکه میان این دو دغدغهٔ بزرگ گونه‌ای تعادل حقوقی واقع‌گرایانه و منصفانه برقرار شود که این خود نیازمند تجزیه و تحلیل مسائل گوناگونی است که سعی می‌شود در حد این مقاله به آنها پرداخته شود.

بند اول: توضیح وتبیین پیشگیری وضعی

پیشگیری وضعی به عنوان یکی از روش‌های پیشگیری، به مجموعه‌ی تدابیری اطلاق می‌شود که کاهش و حذف موقعیت‌ها و فرصت‌های ارتکاب جرم را سرلوحه‌ی اقدامات خود قرار داده است. یکی از دلایل اقبال به این نوع پیشگیری، ناکارآمدی پیشگیری اجتماعی است. این

نوع پیشگیری، هرچند فرایند گذار از اندیشه به عمل را با مانع مواجه می‌کند، اما خود با موانع و محدودیت‌هایی همراه است که کارایی آن را کمرنگ می‌نماید. کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب یک جرم، سه عامل باید جمع شوند. مهم‌ترین آنها که قاعدهٔ مثلث جرم را هم تشکیل می‌دهد، انگیزهٔ مجرمانه است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه می‌شود. برای از بین بردن این عامل، ضروری است تدابیر پیشگیرانهٔ اجتماعی اتخاذ گردد. اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت و ابزار ارتکاب جرم جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد. زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند. هرچند در عین حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرائم نادیده گرفت.

پیوند و اتصال شبکه جهانی اینترنت به روشنی گویای این واقعیت است که ویرانگری و آسیب رسانی می تواند در یک لحظه سراسر جهان را فرا گیرد.سوء استفاده از فناوری های رایانه ای و اینترنتی می تواند امنیت ملی,آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تاثیرهای منفی بی شماری را بر زندگی افراد اجتماع تحمیل کند.با کمی دقت در این خصوص می توان به این نتیجه دست یافت که اغلب مرتکبان جرایم سایبری را جمعیت جوان تشکیل می دهند.این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می دهند.افرادی که در شرایط عادی زندگی ,هیچ گونه تصوری از سرقت یا تجاوز به اموال دیگران ندارند,در مواجه با فرصت ها و موقعیتهای ارزشمندی که رایانه و اینترنت برای آنها مهیا نکرده,حتی لحظه ای دچار تردید احساس گناه یا تزلزل در تصمیم گیری نخواهند شد.در بیشتر جرایم سایبری خشونت وجود ندارد ,بلکه طمع,غرور یا دیگر ضعفهای شخصیتی قربانی است که در ارتکاب این جرایم نقش اصلی را بازی می کنند.

فضای سایبر از تلفیق فناوریهای رایانه و مخابرات به وجود آمده است. شورای اروپا در یکی از جزوات آموزشی خود، مفهوم فضای سایبر را ترکیبی از رایانه، مودم و ابزار مخابراتی دانسته که از قابلیت شبیه‌سازی و مجازی‌سازی برخوردار باشد. اما نکتهٔ قابل توجه در اینجا این است: هنگامی که پیشینهٔ جرائم سایبر بررسی می‌گردد، ملاحظه می‌شود بیشتر بر روی جرائم مرتبط با رایانه بحث شده است. **نسل اول جرائم رایانه‌ای سایبری** به ابتدای ظهور سیستم های رایانه‌ای، به ویژه زمانی که برای اولین بار در سطح گسترده‌ای در دسترس عموم قرار گرفتند، مربوط می‌شود. اولین سیستم رایانه‌ای به مفهوم امروزی ENIAC نام داشت که سوئیچ آن در فوریهٔ ۱۹۴۶ چرخانیده شد. اما حدود سه دهه طول کشید که امکان تولید انبوه این سیستمها در قالب سیستمهای شخصی (Personal Computer) و رومیزی (Desktop)فراهم گشت و تعداد بیشتری از مردم توانستند آنها را بخرند و در امور مختلف از آنها استفاده کنند. بدیهی است سوء استفاده از این سیستمها از این زمان مورد توجه قرار گرفت و تلاشهایی جهت مقابله با آنها به عمل آمد.گفتنی است سوء استفاده‌هایی که در این دوره از سیستمهای رایانه‌ای می‌شد، از لحاظ نوع و حجم خسارات محدود بود که آن هم از قابلیت محدود این سیستمها نشأت می‌گرفت. در آن زمان، عمدهٔ اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستمها و به تبع آن دستکاری داده‌ها مربوط می‌شد. لذا تدابیری که جهت مقابله با آنها اتخاذ می‌گردید، بیشتر رویکردی امنیتی داشت.

بخش دوم: انواع تدابیر پیشگیری وضعی از جرائم سایبر

به طور کلی، تدابیر پیشگیرانهٔ وضعی از جرائم سایبر را می‌توان در چهار گروه بررسی کرد.

بند اول: تدابیر محدودکننده یا سلب‌کنندهٔ دسترس

این تدابیر، در زمرهٔ مهم‌ترین تدابیر پیشگیرانهٔ وضعی از جرائم سایبر قرار دارند که نمونه‌های اولیهٔ آن برای جلوگیری از جرائم نسل اول نیز به کار می‌رفت. در اینجا سعی می‌شود با نصب سیستمها یا برنامه‌های خاص بر روی گرههای (Nodes) دسترس به شبکه، یعنی کامپیوترهای شخصی، مسیریابها(Routers) ، سیستمهای ارائه‌دهندگان خدمات شبکه‌ای و از همه مهم‌تر ایجادکنندگان نقطهٔ تماس بین‌المللی، از ورود یا ارسال برخی داده‌های غیرمجاز

یا غیرقانونی جلوگیری شود. این سیستم‌ها و برنامه‌ها عمدتاً در سه قالب دیوارهای آتشین (Firewall)، فیلترها (Filtering) و پراکسیها (Proxy) هستند. این ابزارها حاوی فهرستی از موضوعات مجاز (White List) یا غیرمجاز (Black List) هستند و بر اساس فرایند انطباق عمل می‌کنند (Thornburgh, ۲۰۰۴ : ۵۱) بعضی از آنها مانند فیلترها و دیوارهای آتشین یک سویه عمل می‌کنند، یعنی فقط از ورودیهای غیرمجاز جلوگیری می‌کنند، اما بعضی دیگر دوسویه عمل می‌کنند و علاوه بر ورودیها، از خروجیها هم مراقبت می‌نمایند(Shinder, ۲۰۰۲ :۳۴۹).

بنددوم: تدابیر نظارتی

نظارت شبکه‌ای شاید بیش از آنکه یک اقدام پیشگیرانه (Preventive) باشد، از لحاظ بازدارندگی (Deterrence) مورد توجه قرار می‌گیرد. این اقدام به دو شکل فنی و انسانی قابل اجراست. در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیهٔ فعالیتهای شبکه‌ای اشخاص، حتی ضرباتی که بر روی صفحه کلیدشان زده‌اند یا نقاطی را که به وسیلهٔ ماوس بر روی آنها کلیک کرده‌اند ضبط می‌کنند. سپس مأمور مورد نظر می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد. شایان ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر بداند فعالیت هایش تحت نظارت قرار دارد، زیرا همان‌طور که می‌دانیم، نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد. اکنون بسیاری از محیطهای گپ شبکه‌ای (Chat Rooms)، به ویژه آنها که مورد اقبال قشر جوان و نوجوان است، تحت نظارت فنی یا زنده قرار دارند. اما مهم‌ترین مزیت این اقدام نسبت به اقدامات محدودکننده یا سلب‌کنندهٔ دسترس این است که در عین اثرگذاری بازدارنده که پیشگیرانه نیز تلقی می‌شود، در فعالیت کاربران خللی ایجاد نمی‌کند و از این لحاظ اشکالی به وجود نمی‌آورد، اما خود آن با ایرادات مهم حقوقی مواجه است که در جای خود به آن خواهیم پرداخت.

بند سوم: تدابیر صدور مجوز

در اینجا تلاش می‌شود بر اساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری شود. نمونهٔ سادهٔ این اقدام، به کارگیری گذرواژه (Password) است که در

گذشته و اکنون جایگاه خود را حفظ کرده است. به این ترتیب، تنها کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار لازم، گذرواژهٔ مربوط را دریافت کنند. ممکن است این مجوز بر اساس سن، جنس، ملیت، مذهب یا گرایشهای خاص فکری داده شود. امروزه در این حوزه پیشرفتهای بسیاری صورت گرفته است. به عنوان مثال، برای ارتقای هرچه بیشتر امنیت، چندی است از شیوه‌های بیومتریک نیز استفاده می‌شود. به عنوان مثال، به جای یا علاوه بر گذرواژه، از اسکن عنبیه یا شبکیهٔ چشم یا اثر انگشت نیز برای شناسایی فرد استفاده می‌شود تا ضریب خطا به حداقل برسد.

به نظر می‌رسد تدابیر این حوزه نسبت به دو حوزهٔ دیگر ایرادات اساسی ندارد، اما خالی از اشکال هم نیست و حداقل به دو نقص مهم آن می‌توان اشاره کرد:

۱. نسبت به تمامی حوزه‌های فضای سایبر قابل اجرا نیست و موارد استفادهٔ آن بسیار محدود است. ۲. این ایراد که البته راجع به دیگر ابزارهای پیشگیرانه نیز صادق است، به پیشرفت لحظه‌شمار فناوریهای موجود در فضای سایبر مربوط می‌شود. ممکن است یک سیستم اکنون با بهره‌گیری از ابزارهای صدور مجوز، از ایمنی قابل قبولی برخوردار باشد، اما به نظر نمی‌رسد هیچ متخصصی بتواند این ایمنی را تا مدت مشخصی تضمین نماید، زیرا این فناوری در معرض آزمون و خطای هزاران نفر از سراسر جهان قرار دارد و به زودی نقاط ضعف آن کشف می‌شود.

بند چهارم: ابزارهای ناشناس‌کننده و رمزگذاری

این دو اقدام تا حدی از لحاظ کارکرد با یکدیگر تفاوت دارند، اما از آنجا که یک هدف را دنبال می‌کنند، در اینجا با هم بررسی می‌شوند. همان گونه که از این اصطلاحات پیداست، این ابزارها ماهیت اصلی یک مفهوم را پنهان یا غیرقابل درک می‌کنند تا غیرقابل شناسایی و تشخیص گردد. ناشناس‌کننده‌ها هویت اشخاص را در فضای سایبر پنهان می‌کنند و از این طریق به آنها امکان می‌دهند با ایجاد حریم بیشتر به فعالیت شبکه‌ای بپردازند. این اقدام به ویژه برای زنان و کودکان یا به طور کلی اشخاصی که به هر دلیل آسیب‌پذیرند سودمند است، زیرا بی‌آنکه فرصت شناسایی خود را به مجرمان سایبر بدهند، می‌توانند به فعالیتهای شبکه‌ای

بپردازند (Thornburgh, ۲۰۰۱ :۶۶). اما از ابزارهای رمزنگاری بیشتر برای محتوای ارتباطات استفاده می‌شود. در اینجا بر اساس کدهای خاصی متن اصلی به رمزنوشته (Cipher Text)تبدیل می‌شود و گیرنده در مقصد به وسیلهٔ کلیدی که در اختیار دارد، آن را رمزگشایی (Decryption) می‌کند. متأسفانه ابزارهای متنوع و بسیاری در فضای سایبر برای شنود و دستیابی به ارتباطات افراد وجود دارد که بهره‌گیری از برنامه‌های رمزنگاری می‌تواند خطر این گونه تعرضات را کاهش دهد (Shinder, ۲۰۰۲ : ۳۷۸) . با این حال، نباید از یاد برد که امکان استفاده از این ابزارها برای مجرمان نیز وجود دارد. آنها با پنهان کردن هویت یا رمزنگاری محتوای مجرمانهٔ ارتباطاتشان، امکان شناسایی خود را کاهش می‌دهند. لذا این گزینه نسبت به سه تدبیر پیشگیرانهٔ قبل از این ضعف برخوردار است که در کنار از بین بردن برخی از فرصتهای ارتکاب جرم، زمینهٔ ارتکاب ایمن برخی دیگر از جرائم را هم فراهم می‌آورد.

بند پنجم: انعکاس موازین حقوق بشر در فضای سایبر

پس از آشنایی با ماهیت جرائم سایبر و نیز پیشگیری وضعی و انواع تدابیر آن در زمینهٔ جرائم مزبور، اینک نوبت بررسی چالشهای تدابیر پیشگیری وضعی با موازین حقوق بشر است. اما لازم است ابتدا ببینیم اتخاذ تدابیر پیشگیری وضعی ممکن است به رعایت نشدن کدام موازین حقوق بشری بینجامد. پیش از هر چیز، در خور ذکر است منظور از موازین حقوق بشر، اصول و هنجارهایی است که در اعلامیهٔ جهانی حقوق بشر (۱۹۴۸) و میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) منعکس شده‌اند. سه اصل از اصول این اسناد به طور قابل توجهی تحت تأثیر فضای سایبر قرار گرفته‌اند که در اینجا به آنها پرداخته می‌شود.

الف)تأثیر فضای سایبر بر آزادی عقیده و بیان:یکی از اصول مهمی که در اعلامیهٔ حقوق بشر و شهروند فرانسه مصوب ۲۶ اوت ۱۷۹۶ مورد تأکید تدوین‌کنندگان آن قرار گرفته است، آزادی عقیده و بیان است. همان‌طور که می‌دانیم، یکی از اهداف انقلاب کبیر فرانسه، برپایی یک جامعهٔ مردم‌سالار بود؛ یعنی جامعه‌ای عاری از استبداد و خودکامگی تا هر کس بتواند با ابراز عقاید و دیدگاههای خویش، در سرنوشت مملکتش سهیم باشد. بی‌تردید تحقق این مهم

منوط به آزادی انجام چنین کاری بود و به همین دلیل به صراحت از سوی انقلابیون در این منشور مورد تأکید قرار گرفت و پس از آن در اعلامیهٔ جهانی حقوق بشر و دیگر اسناد مربوط به رسمیت شناخته شد. (بسته‌نگار، ۱۳۸۰: ۵۱) . در این زمینه، مادّهٔ ۱۹ اعلامیه اشعار می‌دارد:

هرکس حق آزادی عقیده و بیان دارد و این حق مستلزم آن است که از داشتن عقیده بیم نداشته باشد و در دریافت و انتشار اطلاعات و افکار، به تمام وسایل ممکن، بدون ملاحظات مرزی، آزاد باشد. این مادّه چنان صراحت و جامعیتی دارد که به نظر می‌رسد نیازی به تفسیر و روزآمد کردن آن نیست و به حتم در هر زمان و در تمامی شرایط و اوضاع و احوال صادق است. از آنجا که این اعلامیه جنبهٔ الزام‌آور نداشت و از طرف دیگر، ضرورت ایجاب می‌کرد این اصول از سوی کشورها رعایت گردد، در سال ۱۹۶۶ سند بین‌المللی دیگری به نام میثاق بین‌المللی حقوق مدنی و سیاسی به تصویب رسید و در ۲۳ مارس ۱۹۷۶ لازم‌الاجرا شد. اما از آنجا که برخی از الزامات به کشورها تحمیل شده بود، تمامی اصول و هنجارهای مورد بحث از آن قالب مطلق خود که اعلامیهٔ حقوق بشر بر آن تأکید داشت خارج شدند و به کشورها اجازه داده شد در برخی موارد مهم محدودیتهایی را اعمال کنند. به عنوان مثال، در بند یک مادّهٔ ۱۸ میثاق آمده: "۱. هرکس حق آزادی فکر، وجدان و مذهب دارد. ... ." اما در بند ۳ آن نیز قید شده است.

آزادی ابراز مذهب یا معتقدات را نمی‌توان تابع محدودیتهایی نمود، مگر آنچه منحصراً به موجب قانون برای حمایت از امنیت، نظم، سلامت یا اخلاق عمومی یا حقوق و آزادیهای اساسی دیگران ضرورت داشته باشد. همان گونه که ملاحظه می‌شود، در اینجا به استثنائات کلی و مهمی اشاره شده که هر دولتی می‌تواند برای توجیه اقدامات خود به آنها تمسک جوید. (ساندرا کولیور، ۱۳۷۹: ۱۷۷) با اینکه در این سند قید شده کلیهٔ اقدامات باید به موجب قانون و با توجه به سایر الزامات حقوق بین‌الملل باشد، به نظر می‌رسد ابزار بازدارندهٔ مهمی تلقی نشود. لذا برای اینکه این اقدامات تحت ضوابط دقیق‌تری اجرا شود، در اول اکتبر ۱۹۹۵، گروهی از متخصصان حقوق بین‌الملل، امنیت ملی و حقوق بشر، بیانیهٔ ژوهانسبورگ را درباره نحوهٔ تعامل امنیت ملی با آزادی بیان و دسترس به اطلاعات منتشر کردند. (نمک‌دوست تهرانی، ۱۳۸۴) این

بیانیه که مشتمل بر ۲۵ اصل است، تلاش کرده حدود و ثغور اصول حقوق بشر راجع به آزادی بیان و دسترس به اطلاعات را در تقابل با ضرورت حفظ امنیت و مصلحت ملی مشخص کند. اصل اول این بیانیه، همانند اصول پیش‌بینی شده در اعلامیهٔ حقوق بشر و میثاق، آزادی عقیده، بیان و اطلاعات را به رسمیت می‌شناسد. بی‌تردید این فضا با گسترهٔ نامحدود و قابلیتهای بی‌شمار خود، مؤثرترین کمک را به تحقق هرچه کامل‌تر این اصل کرده است. زیرا اگر در گذشته‌ای نه چندان دور شخصی می‌خواست عقیدهٔ خود را به اطلاع دیگران برساند، یا باید به اطرافیان خود اکتفا می‌کرد یا با صرف هزینه و وقت بسیار، به تدریج به گوش دیگران می‌رساند. اما اکنون این امکان فراهم آمده که کلام خود را از پشت سیستم رایانه‌ای در منزل خود، آن هم به شکل دوسویه، به اطلاع تمامی جهانیان برساند، یعنی به طور همزمان از نظرها و دیدگاههای مخاطبان خود نیز بهره‌مند شود. این ویژگی مزیت بزرگی است که دیگر رسانه‌های ارتباط جمعی از آن بی‌بهره‌اند. از سوی دیگر، این فضا با چالش هایی در خصوص سوء استفاده‌های بسیار متنوع مواجه است که ضروریاز سوی دیگر، این فضا با چالشهایی در خصوص سوء استفاده‌های بسیار متنوع مواجه است که ضروری است با آنها مقابله شود تا امنیت، نظم، سلامت یا اخلاق عمومی یا حقوق و آزادیهای دیگران حفظ شود. حال باید دید تا چه اندازه می‌توان این دو دغدغهٔ به ظاهر یا واقعاً متناقض را با یکدیگر جمع کرد. گفتار بعد به بررسی این موضوع اختصاص دارد.

ب) تأثیر فضای سایبر بر جریان آزاد اطلاعات: یکی از اصولی که همواره در اسناد بین‌المللی حقوق بشر در کنار و هم‌ارز آزادی عقیده و بیان به آن تأکید شده، جریان آزاد اطلاعات است. بی‌تردید آزادی عقیده و بیان زمانی در معنای واقعی خود تحقق خواهد یافت که بتوان اطلاعات را بی‌هیچ محدودیتی در جامعه منتشر کرد. همان‌گونه که اشاره شد، ماهیت آزادی بیان به گونه‌ای است که باید دیدگاهها و عقاید افراد بدون محدودیت در اختیار همگان قرار گیرد. این مبنا کاملاً با آنچه فضای سایبر فراهم می‌آورد منطبق است و حتی زمینه‌های شکوفایی آن به مراتب فراتر از آنچه تصور می‌رفت به وجود آمده است. از سوی دیگر، تدابیر محدودکننده یا سلب‌کننده دسترس، به ویژه فیلترینگ، مانع بزرگی در تحقق این اصل

محسوب می‌شوند، زیرا از جریان آزاد اطلاعات جلوگیری می‌کنند. دلایل مختلفی باعث ایجاد محدودیت از سوی این ابزارها می‌شود که در اینجا به دو عامل مهم اشاره می‌شود:

بند ششم: مراجع تدوین‌کننده فهرست ها

معمولاً کسانی مبادرت به تدوین فهرست فیلترها می‌کنند که درباره برخی موضوعات مانند مسائل مذهبی، اخلاقی یا سیاسی تعصب دارند و می‌کوشند از دسترس دیگران به سایتهایی که مغایر با اعتقاداتشان است جلوگیری کنند. اما آنچه بیشتر به گستره اعمال این محدودیتها دامن می‌زند، گنجانیدن طیف وسیعی از موضوعات مشکوک یا به اصطلاح خاکستری در فهرستهای سیاه است. مراجع مذکور این کار را برای تحقق هرچه بیشتر اهدافشان انجام می‌دهند، فارغ از اینکه این اقدام تا چه حد می‌تواند از دسترس افراد به مطالب معتبر و مجاز جلوگیری نماید.

بند هفتم: کارکرد انطباقی

دومین مانع بزرگ، کارکرد انطباقی و نه هوشمندانه این ابزارهاست. همان‌طور که می‌دانیم، اصطلاحات یا تصاویر مندرج در فهرستهای سیاه، تنها در متون یا محتواهای غیرمجاز به کار نمی‌روند و بسیار اتفاق می‌افتد که به لحاظ کاربرد آنها در محتواهای مجاز، از دسترس به آنها جلوگیری می‌شود. به عنوان مثال، با درج واژه sex در موتورهای جست‌وجو که یکی از واژگان پر بسامد در اینترنت است، فیلترها به سرعت فعال می‌شوند، در حالی که بسیار اتفاق می‌افتد که از آن واژه در متون معتبر علمی و ادبی نیز استفاده شود. اما جالب اینجاست که چنانچه در فهرست فیلترها شقوق دیگر نگارش این کلمه، نظیرesx ، درج نشده باشد، با وجود دارا بودن محتوای غیرمجاز، آن فیلترها فعال نخواهند شد و از دسترس به آنها جلوگیری نخواهند کرد.امروزه در بسیاری از کشورها حفظ امنیت ملی، نظم، سلامت یا اخلاق عمومی و احترام به حقوق یا آزادیهای اساسی دیگران، جزء مؤلفه‌هایی است که به رسمیت شناخته شده و دولتها تلاش می‌کنند از آنها به بهترین وجه پاسداری کنند. از سوی دیگر، فضای سایبر جلوه دیگری به این مفاهیم بخشیده و باید مطابق با ویژگیهای خاص آن برنامه‌ریزی کرد. اگر تعداد بسیار کمی از گروههای یک جامعه به فکر تهیه انواع ابزارهای محدودکننده یا سلب‌کننده دسترس هستند، خیل عظیمی هم برای خنثا کردن آن ابزارها تلاش می‌کنند و در میان این

گروه می‌توان چهره‌های موجه بسیاری نظیر دانشجویان و دانش‌پژوهان را یافت که برای احقاق حق خود، یعنی بهره‌برداری علمی و سودمند از این فضا، سعی می‌کنند دست به کاری بزنند که شاید غیرقانونی نیز تلقی شود.آنچه نباید از نظر دور داشت اینکه در تمامی کشورها، حتی آنهایی که خود را مهد مردم‌سالاری می‌دانند، خط قرمزهایی وجود دارد. در کشوری مثل ایالات متحده یا کشورهای اروپایی، از ابزارهایی نظیر فیلترها به وفور استفاده می‌شود، اما برای کاستن از مضرات آنها، سعی شده برنامه‌ریزی مفصلی در زمینه مخاطب‌شناسی (کسانی که این ابزارها برای آنها به کار می‌رود)، شناسایی هرچه دقیق‌تر محتواهای غیرمجاز و پرهیز از گنجانیدن موارد مشکوک به آنها و در نهایت بهره‌گیری چندبعدی از این ابزارها انجام شود. به عنوان مثال، در کنار فهرستهای متنی، از فهرستهای تصویری یا دیگر شناسه‌ها استفاده می‌شود تا ضعف این ابزارها به حداقل برسد. از جمله در ایالات متحده برای هر طیف و گروه سنی از افراد جامعه، ابزار خاصی به کار می‌رود. بنابراین، فیلتری که در یک مدرسه برای کودکان به اجرا درمی‌آید، برای سیستمهای رایانه‌ای دانشگاه به کار نمی‌رود و در آنجا سعی می‌شود از ابزارهای کمتر محدودکننده استفاده شود تا در فعالیتهای پژوهشی دانشجویان خللی وارد نشود.به نظر می‌رسد با یک برنامه‌ریزی صحیح و اقتباس از الگوهای مفیدی که اکنون در دیگر کشورها به اجرا درمی‌آید، علاوه بر حفظ ارزشهای مورد قبول جامعه، می‌توان به گونه‌ای مؤثر از جرائم سایبر پیشگیری کرد.

بخش سوم: تقابل پیشگیری وضعی از جرائم رایانه‌ای با حریم خصوصی

همان‌گونه که اشاره شد، فضای سایبر بر خلاف اصول گذشته، زمینه‌های تهدید و تعرض به این اصل را بیشتر کرده است. از آنجا که این اصل به حریم و خلوت افراد مربوط می‌شود، نسبت به دیگر اصول بیشتر مورد توجه قرار گرفته و در این زمینه قوانین و مقررات سخت و لازم‌الاجرایی به تصویب رسیده که آنها را به اجمال بررسی خواهیم کرد.

اما پیش از پرداختن به قوانین و مقررات حمایتی از حریم آن‌لاین افراد، به تأثیر ابزارهای پیشگیرانه از جرائم سایبر آن اشاره می‌شود. به طور کلی، دو ابزار پیشگیرانه از چهار ابزار فوق، حریم الکترونیکی افراد را تهدید می‌کنند: ۱۰ ابزارهای نظارتی که با توجه به توضیحاتی که

درباره آنها داده شد، تردیدی در تعرض‌آمیز بودن آنها نیست. این اقدام پیشگیرانه که در عین حال بازدارنده نیز می‌باشد، تأثیرات سوء مستقیم و غیرمستقیم بسیاری بر فعالیتهای شبکه‌ای می‌گذارد. چنانچه در محیطی این حس در مردم بیدار شود که به دلیل بی‌اعتمادی به آنها، همواره تحت نظارت قرار دارند، این امر به شدت در نحوه فعالیت آنها تأثیر خواهد گذاشت. اکنون فعالیتهای مختلف اقتصادی، اجتماعی، فرهنگی و سیاسی بسیار متنوعی در فضای سایبر جریان دارد که تمامی آن به خاطر آزاد و عاری بودن این فضا از هرگونه محدودیت است. اما چنانچه کاربران شبکه‌ای احساس کنند فعالیتهای آنها تحت نظارت مستمر زنده یا غیرزنده قرار دارد، بی‌تردید در نحوه فعالیت خود تجدیدنظر خواهند کرد که این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد.

به هر حال، با اذعان به اینکه ضروری است برای مقابله با جرائم بسیار متنوع سایبر اقدامات نظارتی اعمال شود، این نظارت باید به نحوی باشد که اعضای این فضا احساس نکنند به آنها به دید مجرم نگریسته می‌شود.

دومین ابزاری که البته به صورت غیرمستقیم حریم افراد را تهدید می‌کند، سیستمهای تأیید هویت است. در فضای سایبر، برای اینکه به اشخاص اجازه ورود به محیطهای خاصی داده شود، برخی اطلاعات که شامل اطلاعات شخصی یا حتی اطلاعات شخصی حساس می‌شود، از آنها اخذ می‌گردد. نگرانی‌ای که در اینجا وجود دارد، راجع به امکان سوء استفاده متصدیان این سایتها از این اطلاعات یا امکان افشای آنها به دلایل مختلف، نظیر فقدان یک سیستم امنیتی کارآمد جهت حفاظت از این اطلاعات، است.

نتیجه گیری

همان‌طور که می‌دانیم، مجازات حبس نه تنها در جامعه ما که در بسیاری جوامع یکی از متداول‌ترین کیفرهاست. همچنین همه ما کم و بیش با هزینه‌ها و آثار سوء آن آشنایی داریم. در وصف زندان همین بس که آن را دانشگاه مجرمان می‌دانند و به نظر می‌رسد آسیبی بالاتر از آن نمی‌توان برشمرد. به همین دلیل، در دهه‌های اخیر با انجام تحقیقات و مطالعات گسترده، ضمانت اجراهای جایگزینی مطرح شده که مجازاتهای جایگزین حبس یا مجازاتهای اجتماعی

نامیده می‌شود*. حتی در نحوه اجرای مجازات حبس نیز تحولات شگرفی به وجود آمده که از آن جمله می‌توان به آزادی مشروط، تعلیق مراقبتی، حبسهای خانگی، حبسهای آخر هفته و... اشاره کرد. بدیهی است تمامی این تحولات برای به حداقل رساندن آسیبها و آثار سوء مجازات، در عین حفظ آن، است و تاکنون در هیچ کشوری مشاهده نشده مجازات از صفحه قوانین کیفری حذف گردد .غرض از بیان این مثال اشاره به این نکته بود که ماهیت فضای سایبر به گونه‌ای است که پیشگیری وضعی یکی از تدابیر ناگریز و لازم‌الاجرا محسوب می‌شود. حتی در دنیای فیزیکی نیز این سخن صادق است، زیرا تنها گزینه‌ای است که می‌تواند دو ضلع مثلث جرم، یعنی فرصت و ابزار ارتکاب جرم را هدف قرار دهد. بنابراین، باید یک راه حل بینابین اتخاذ شود که به موجب آن ضوابطی که تدوین می‌گردد، بر اساس قواعد و مقررات حقوقی و همچنین ملاحظات حاکم بر فضای سایبر باشند تا علاوه بر صیانت از امنیت ملی و نظم، سلامت یا اخلاق عمومی، به دیگر موازین حقوق بشر، یعنی آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی نیز خدشه‌ای وارد نگردد. بی‌تردید مراجعه به تجارب دیگر کشورها با رعایت شرایط خاص کشورمان، چنانچه بر پایه دیدگاههای واقع‌گرایانه حقوقی ـ فنی باشد، می‌تواند نتایج مطلوبی را پدید آورد.

منابع و مآخذ

۱. بسته‌نگار، محمد، حقوق بشر از منظر اندیشمندان، شرکت سهامی انتشار ۱۳۸۹

۲. جلالی فراهانی، امیرحسین، »پول‌شویی الکترونیکی»، فصلنامه فقه و حقوق ۱۳۸۹

۳. جلالی فراهانی، امیرحسین، »پیشگیری از جرائم رایانه‌ای»، مجله حقوقی دادگستری ۱۳۹۲

۴.حسن‌بیگی، ابراهیم، »آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی»، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی ۱۳۹۴

۵.حسینی، بیژن،»جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن»، پایان‌نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات ۱۳۹۲

۶.دزیانی، محمد حسن، جرائم کامپیوتری، جلد اول، دبیرخانه شورای عالی انفورماتیک، ۱۳۹۰

۷.دزیانی، محمدحسن، «شروع جرائم کامپیوتری- سایبری»، خبرنامه انفورماتیک ۱۳۹۳

۸.دزیانی، محمدحسن، «مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کامپیوتری (سایبری) ، خبرنامه انفورماتیک ۱۳۹۰

۹.کولیور، ساندرا و دیگران، آقایی، علی اکبر (مترجم)، »آزادی، حق و امنیت»، فصلنامه مطالعات راهبردی ۱۳۹۴

۱۰.نجفی ابرندآبادی، علی حسین، تقریرات درس جرم‌شناسی (پیشگیری)، دوره کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیمی مهدی سیدزاده ۱۳۹۲

۱۱.نجفی ابرندآبادی، علی‌حسین، »پیشگیری عادلانه از جرم»، علوم جنایی، مجموعه مقالات در تجلیل از استاد آشوری، انتشارات سمت ۱۳۹۳