پژوهش حقوق کیفری، سال پنجم، شماره هجدهم ، بهار ۱۳۹۶، ص ۱۰۰ - ۶۹

نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت‌مدار از جرائم سایبری

زهرا فرهادی آلاشتی* عبدالرضا جوان جعفری بجنوردی**

(تاریخ دریافت : ۹۴/۱۰/۱۵ تاریخ پذیرش : ۹۵/۱۰/۱)

چکیده؛

ماهیت فناورانه برخی از تدابیر موقعیت‌مدار سایبری می‌تواند منجر به نقض حق آزادی جریان اطلاعات کاربران از طریق سلب و یا محدودیت آنان در دریافت، انتقال و اشتراک محتویات مورد نظرشان شود. تعهدات بین-المللی حاکمیت‌ها به صیانت از موازین حقوق بشری، آنان را از به‌کارگیری حداکثری این تدابیر باز می‌دارد. تأمین نظم و امنیت عمومی تا جایی مورد پذیرش است که کرامت انسانی آماج احتمالی بزه حفظ گردد و منجر به امنیتی شدن جو حاکم نگردد. از همین‌رو، استفاده از تدابیر پیشگیرانه موقعیت‌مدار تا جایی قانونی است که همگان در معرض اتهام قرار نگیرند و حق قانونی استفاده از شبکه جهانی اینترنت، با انگیزه کاهش احتمالی فرصت‌های بالقوه بزه، از کاربران سلب نگردد. هدف اصلی این نوشتار، ارزیابی نقض حق جریان آزاد اطلاعات در جریان به‌کارگیری رایج‌ترین تدابیر پیشگیرانه موقعیت‌مدار از بزه سایبری و بررسی آثار سوء احتمالی آن خواهد بود.

کلیدواژگان: پیشگیری موقعیت‌مدار، جرائم سایبری، جریان.آزاد اطلاعات، حقوق بشر. .

---

* دانش آموخته کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی دانشگاه فردوسی مشهد.

** دانشیار حقوق جزا و جرم شناسی دانشگاه فردوسی مشهد (نویسنده مسئول): Javan-j@um.ac.ir

مقدمه؛

با ورود ابزارهای فناوری اطلاعات و ارتباطات به زندگی بشر، جوامع از عصر ارتباطات ساده‌ی نخستین به عصر ارتباطات پیشرفته‌ی الکترونیکی گذر کرده‌اند تا جایی که به کمک این ابزارها، مرزهای جغرافیایی پشت سرگذاشته می‌شوند و کاربران فارغ از هرگونه مرزهای ملی و منطقه‌ای با یکدیگر در ارتباط بوده و «*دهکده جهانی*»[1] را تشکیل می‌دهند. دهکده‌ای که ساکنان آن با یکدیگر در ارتباط هستند و عقاید، نظرات و اطلاعات مورد نظر خود را با دیگران به اشتراک می‌گذارند. این ابزارها فرصتی بی‌نظیر برای رشد همگان فراهم آورده‌اند تا جائی‌که امروزه، برخلاف قرون گذشته، حق آگاهی و دانش‌اندوزی منحصر به قشر و طبقه‌ی اجتماعی خاصی نبوده و فرصت تعالی فکری همگان فراهم شده است.

آنچه فضای سایبر را از سایر ابزارهای ارتباط‌جمعی متمایز می‌سازد، دو مؤلفه‌ی سرعت انتقال اطلاعات و نقشی است که کاربران در اشتراک اطلاعات دارند. «در اینترنت، مخاطب از وضعیت انفعالی و کنش‌پذیری خارج شده و به‌طور فعال در فرآیند ارتباط مشارکت دارد. این تحول تا حدی ادامه داشته که مخاطب تبدیل به کاربر شده است. به‌عبارت‌دیگر مخاطب به همراه و تولید-کننده محتوا تبدیل شده، چون تولیدکننده‌ی محتوا هم هست و نقش مهمی در تولید دارد و در آن تأثیرگذار است» (رضایی و بابازاده مقدم، ۱۳۹۳: ۴۸). با پیشرفت فناوری‌های شبکه جهانی اینترنت، کاربران از «حالت انفعالی وب» که مشابه سایر ابزارهای ارتباط‌جمعی بوده است، به حالت «فعال فناوری وب» گذر نموده و به بازیگران اصلی جریان اطلاعات تبدیل شده‌اند.[2] در

1. Global village

۲. تا به امروز، وب‌سایت‌ها به ۴ نسل تقسیم شده‌اند. در نسل اول وب‌ها که وب ۱,۰ نام دارند، اطلاعات توسط گروه معدودی از افراد که بوجودآورندگان و اداره‌کنندگان وب هستند، در اختیار کاربران گذاشته می‌شود و کاربران هیچ نقشی در تولید محتوا نخواهند داشت؛ بنابراین، اطلاعات به حالت عمودی و از بالا به پایین در اختیار دیگران قرار داده می‌شود و اشتراک-گذاری اطلاعات امکان نخواهد داشت. درمقابل، وب ۲,۰ که از آن به *«وب مشارکتی»* نیز تعبیر می‌شود، دربردارنده‌ی دسته‌ای از سایت‌ها و نرم‌افزارهای خدماتی اینترنتی هستند که تعامل کاربران با یکدیگر را تسهیل می‌نمایند و امکان اشتراک اطلاعات

حال حاضر، «کاربران اینترنت ضمن اینکه می‌توانند از اطلاعات موجود در شبکه‌ی مذکور استفاده کنند، خود نیز می‌توانند خواسته، اندیشه و اطلاعات خود را به‌منظور عرضه‌ی آن به سایر کاربران، وارد شبکه‌ی مذکور نمایند» (فضلی، ۱۳۹۱: ۶۶).

به‌موازات همین تأثیر شگفت‌انگیز فضای سایبر بر زندگی انسان معاصر، تأمین نظم و امنیت آن نیز در کانون توجه قرار دارد و به‌عنوان یکی از مهم‌ترین دغدغه‌های حاکمیت‌ها شناخته می‌شود؛ چراکه، امروزه فضای سایبر به یکی از لوازم ضروری زندگی انسان معاصر تبدیل شده است و ارتباط مداوم وی با این فضا، فرصت مناسبی را نیز برای بزه‌کاران احتمالی فراهم نموده است؛ بنابراین می‌توان بر آن بود که شرایط تحقق نظریه‌ی «فعالیت روزانه»[1] در فضای سایبر فراهم

را فراهم می‌کند. شبکه‌های اجتماعیِ تلفن‌های هوشمند و رایانه‌ها، ویکی‌ها، وبلاگ‌ها، سایت‌های اشتراک فیلم و عکس نمونه‌هایی از وب دو هستند.

نسل سوم وب که از آن به وب ۳٫۰ تعبیر می‌شود، نسل هوشمند وب است که هنوز به درجهٔ تکامل نرسیده است. شاخصه‌های بسیاری را برای وب ۳ برشمرده‌اند که مهمترین آنها را می‌توان، «*مفهومی بودن*» (Semantic web) دانست. در این حالت، نرم‌افزارهای وب قادر به درک موارد درخواستی کاربران هستند. تمام ابزارها به پایگاه‌های داده متصل بوده و کاربران در تمام جنبه‌های زندگی خود از این فناوری استفاده خواهند نمود. به عنوان نمونه، دیوارها، خودروها، وسایل منزل و هرآنچه که انسان در زندگی روزمره از آنها استفاده می‌نماید و هوشمند شده‌اند به شبکه جهانی اینترنت متصل هستند، بنابراین همانگونه که مشخص است عمل جستجو و جریان آزاد اطلاعات در این نسل از وب، بسیار آسانتر خواهد بود. به عنوان نمونه، زمانیکه کاربر واژه‌ی جریان آزاد اطلاعات را بر روی دیوار هوشمند خانه خود جستجو نماید، وب ۳ می‌داند که این واژه به چه معنا است، در چه زمینه‌هایی بکار می‌رود،چه افرادی در مورد آن اظهار نظر کرده‌اند، چه چالش‌هایی برای تحقق آن وجود داد و به عبارت بهتر، فناوری هوش مصنوعی این امکان را به این وب می‌دهد که در بسیاری از موارد همانند انسان به تجزیه و تحلیل ابعاد مختلف موضوع بپردازد. نسل چهارم یا همان وب ۴٫۰، که صرفاً نظریه‌های آن برای استفاده عمومی مطرح می‌شود و در حد آزمایشگاهی مورد امتحان قرار گرفته است، فاصله بین انسان و دستگاه‌ها را از بین می‌برد و نیازی به ورود دستگاه نخواهد بود. به عنوان نمونه، در صورت تصور سایت تبیان در ذهن، دستگاه خود به این سایت وارد شده و آنچه را که کاربر در نظر داشته است، جستجو می‌نماید. با توجه به مطالب گفته شده می‌توان دریافت که هر چه از نسل‌های وب می‌گذرد، جریان آزاد اطلاعات تسهیل شده و زندگی انسان مدرن به بستری برای تحقق هر چه بیشتر این حق تبدیل می‌شود.

۱. نظریه «فعالیت روزانه» (Routine activity theory) در سال ۱۹۷۹ توسط لورنس کوهن و مارکوس فلسون مطرح شد. بنابر این نظریه جرم زمانی اتفاق می‌افتد که بزهکار هدفی مناسب را بیابد و موقعیت و فرصت ارتکاب بزه مهیا باشد؛ بنابراین

شده است؛ چراکه به علت وابستگی بسیاری از فعالیت‌های انسان معاصر به این فضا و عدم ارتقاء امنیت دستگاه‌ها توسط کاربران آسیب‌پذیر، این فضا جذابیتی دوچندان برای ارتکاب جرم ایجاد کرده است.

گستره‌ی کلان خسارات ناشی از جرائم سایبری سبب شده است تا کنگره‌های اخیر پیشگیری از جرم و عدالت کیفری سازمان ملل متحد نیز به همکاری بین‌المللی برای پیشگیری از این جرائم تأکید فراوانی نمایند. به‌عنوان نمونه، در کنگره‌ی دوازدهم تأکید فراوانی به پیشگیری از جرائم سایبری علیه کودکان به‌عنوان کاربران آسیب‌پذیر شده است: *«ما آسیب‌پذیری کودکان را درک می‌کنیم و از بخش خصوصی درخواست می‌کنیم از تلاش‌هایی که با هدف پیشگیری از سوءاستفاده و استثمار جنسی کودکان از طریق اینترنت صورت گرفته، حمایت کند و آن‌ها را ارتقا دهد»* (UN General Assembly 2013: para40).

کنگره‌ی سیزدهم سازمان ملل نیز همچون کنگره‌های پیشین دغدغه افزایش جرائم سایبری را داشته و به استفاده از ابزارهای «فاوا» برای تأمین امنیت این فضا تأکید نموده است. بند نهم اعلامیه‌ی این کنفرانس به نقش مثبت پیشرفت‌های اقتصادی، اجتماعی و فناوری‌ها برای تسهیل فرآیند پیشگیری از جرم اذعان نموده و بر یافتن تدابیری خاص برای تأمین محیط سایبری امن و مناسب تأکید نموده است (UNODC,2015).

استفاده از ابزارهای فناوری اطلاعات و ارتباطات در قالب تدابیر پیشگیرانه‌ی موقعیت‌مدار، یکی از سریع‌ترین روش‌های تأمین فضای نسبتاً امن و پیشگیری از خسارات کلان سایبری است؛ چراکه در این نوع از جرائم، هر دو طرف درگیر در قضیه (بزه‌کار و نظام عدالت کیفری) از فناوری واحدی برای نیل به مقصود خود استفاده می‌نمایند و تنها تفاوت آن‌ها در روزآمدی و استفاده حداکثری از فناوری‌های موجود است. نظریه‌ی پیشگیری موقعیت‌مدار به‌عنوان یکی از

در صورت عدم وجود هر کدام از این شرایط، بزه واقع نخواهد گردید. فعالیت‌های روزانه این فرصت را برای بزهکاران فراهم می‌کنند تا هدف مورد نظر خود را که فاقد تدابیر محافظتی کافی است، بیابند.

نظریات پیشگیرانه کنشی، درنتیجه شکست تدابیر پیشگیرانه اجتماعی، در اواخر دهه ۱۹۷۰ و توسط وزارت کشور بریتانیا مطرح شد. این تدابیر درصدد کاهش بزه‌کاری از طریق دست‌کاری در فرصت‌های پیش‌جنایی هستند؛ بنابراین پیشگیری موقعیت‌مدار درصدد شناخت شخصیت بزه-کار و همچنین علل اجتماعی، اقتصادی و فرهنگی بزه نیست، بلکه سعی در دست‌کاری موقعیت-های ارتکاب بزه و برهم زدن آن‌ها دارد. درنتیجه با مداخله در عوامل محیطی و زمانی سعی در کاهش منافع احتمالی ارتکاب بزه برای بزه‌کاران دارد. کلارک بر این عقیده است که «پیشگیری موقعیت‌مدار درصدد کاهش انگیزه‌های ارتکاب بزه از طریق تعالی جامعه و نهادهای آن نیست، بلکه تمرکز آن بر کاهش فرصت‌ها و موقعیت‌های ارتکاب بزه از طریق کاهش جذابیت است» (Clarke, 1992: 4).

امروزه تدابیر موقعیت‌مدار با استفاده از روش‌های سلبی و ایجابی، سعی در محافظت از آماج احتمالی و افزایش هزینه‌های ارتکاب بزه برای بزه‌کاران سایبری دارند تا جایی‌که «بازار امنیت سایبری»[1]، یکی از پردرآمدترین صنایع روز به شمار می‌رود، لیکن یکی از انتقادات صحیحی که همواره به تدابیر موقعیت‌مدار وارد است، دخالت در حریم شخصی افراد و یا محدود ساختن استفاده آن‌ها از حقوق بنیادین است (بابایی و نجیبیان، ۱۳۹۰: ۱۶۲). احترام به حقوق مدنی و سیاسی آماج احتمالی بزه، نه فقط در اسناد خاص حقوق بشری، بلکه در اسناد و رهنمودهای مختص پیشگیری از جرم نیز مورد تأکید قرار گرفته است. به‌عنوان نمونه، بر اساس اعلامیه‌ی دوازدهمین کنگره‌ی پیشگیری از جرم و عدالت کیفری سازمان ملل، آن نظام عدالت کیفری کارآمد، مؤثر و انسان‌مدار است که بر مبنای صیانت از حقوق بشر در اجرای عدالت و پیشگیری از بزه عمل نماید. بند ۲۶ رهنمود پیشگیری از جرم سازمان ملل متحد نیز بر استفاده از تدابیر پیشگیرانه موقعیت‌مدار تأکید نموده است، لیکن قبل از اشاره به این مهم، قسمتی را تحت عنوان «حقوق بشر، حاکمیت قانون، فرهنگ قانون‌مداری»[2] قید کرده و به حاکمیت قانون و صیانت از حقوق

1. Cyber Security Market
2. Human rights/rule of law/culture of lawfulness

بشر در جریان پیشگیری از بزه تأکید نموده است. بر اساس بند ۱۲ این رهنمود: «حاکمیت قانون و آن دسته از اصول حقوق بشری که در اسناد بین‌المللی به رسمیت شناخته شده‌اند، در تمام فرآیند پیشگیری از جرم باید توسط کشورهای عضو این اسناد، مورد احترام قرار گیرند. فرهنگ قانون‌مداری باید در فرآیند پیشگیری از جرم به‌طور فعالانه ترویج شود» (E/RES/2002/13).

این مهم به فضای سایبر نیز تسری یافته و امروزه یکی از دغدغه‌های رایج برای پیشگیری از جرائم سایبری رعایت این حقوق است. چراکه ماهیت فناورانه برخی از تدابیر نظارتی، سالب و یا محدود-کننده‌ی پیشگیرانه موقعیت‌مدار منجر به نقض این حقوق می‌شوند. آنچه در این اثر مورد تأکید است، مورد دستخوش قرار دادن «جریان آزاد اطلاعات»[1] در فرآیند پیشگیری موقعیت‌مدار از جرائم سایبری است. ابتدائاً لازم به ذکر است که حق جریان آزاد اطلاعات و شرایط و ضوابط حاکم بر آن نخستین بار در ماده ۱۹ اعلامیه جهانی حقوق بشر به رسمیت شناخته شده است. بر اساس این ماده: «هر کس حق آزادی عقیده و بیان دارد و حق مزبور شامل آن است که از داشتن عقاید خود بیم و اضطرابی نداشته باشد و در جست‌وجو، دریافت و انتشار اطلاعات و افکار به تمام وسایل ممکن و بدون ملاحظات مرزی آزاد باشد» (UN General Assembly,1948).

این ماده سرآغازی برای پذیرش بسیاری از حقوق بنیادینی است که لازمه‌ی زندگی آزاد به‌شمار می‌آیند. یکی از بایسته‌های تحقق حق آزادی بیان، آزادی جست‌وجو،[2] دریافت[3] و انتشار[4] اطلاعات است که حق جریان آزاد اطلاعات را نیز در برمی‌گیرد.[5]

مشکل از آنجایی آغاز می‌شود که استفاده از تدابیر پیشگیرانه‌ی موقعیت‌مدار از یک‌سو و صیانت از حقوق کاربران از سوی دیگر، در زمره‌ی تکالیف قانونی مسئولین این حیطه می‌باشد. درحالی‌که «از نظر فنی و تخصصی، ممکن است با کاربرد تدابیر پیشگیری وضعی در فضای

1. Free Flow of Information
2. Seek
3. Receive
4. Impart

۵. هر گونه تحقق حق آزادی بیان مستلزم آزادی مطبوعات، آزادی تجمعات، آزادی جریان اطلاعات، آزادی دسترسی به اطلاعات می باشد.

سایبری، شاهد برخی اختلالات همچون کاهش سرعت شبکه، بسته شدن اشتباهی برخی از سایت‌ها و وبلاگ‌ها به جهت پالایه، محدودیت‌های بی‌جهت برای ورود به برخی از فضاها، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و... بود» (مقیمی، ۱۳۹۵: ۱۲۳).

صیانت از موازین حقوق بشری در جریان پیشگیری از موقعیت‌های پیش‌جنایی همواره ممکن نبوده و این مهم مورد تصدیق اسناد عام و خاص حقوق بشری قرار گرفته است و با توجه به نوع حقوق مورد حمایت، در برخی از موارد می‌توان برخی از حقوق را در جریان پیشگیری از بزه تعلیق و یا تحدید نمود. درحالی‌که دسته‌ای دیگر از حقوق از هرگونه تعلیق و یا تحدید مصون هستند. حق جریان آزاد اطلاعات، در زمره‌ی حقوق دسته نخست قرار داشته و با رعایت شرایط مندرج در اسناد مرجع حقوق بشری، قابل تحدید و حتی تعلیق می‌باشد.[1] در این قسمت با رجوع بند سوم ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی محدودیت‌های وارد بر حق آزادی جریان اطلاعات را تبیین می‌نماییم. بنا بر این بند:

«اعمال حقوق مذکور در بند ۲ این ماده مستلزم حقوق و مسئولیت‌های خاص است و لذا ممکن است تابع محدودیت‌های معینی شود که در قانون تصریح شده و برای امور ذیل ضرورت داشته باشد

۱. ماده ۴ میثاق بین‌المللی حقوق مدنی و سیاسی پیرامون تعلیق حقوق مدنی و سیاسی است. بنابر این ماده:

«۱- هر گاه یک خطر عمومی استثنایی (فوق‌العاده) موجودیت ملت را تهدید کند و این خطر رسماً اعلام بشود کشورهای طرف این میثاق می‌توانند تدابیری خارج از الزامات مقرر در این میثاق به میزانی که وضعیت حتماً ایجاب می‌نماید اتخاذ نمایند، مشروط بر این که تدابیر مزبور با سایر الزاماتی که بر طبق حقوق بین‌الملل به عهده دارند مغایرت نداشته باشد و منجر به تبعیضی منحصراً براساس نژاد، رنگ، جنس، زبان، اصل و منشأ مذهبی یا اجتماعی نشود.۲- حکم مذکور در بند فوق هیچ‌گونه انحراف از مواد ۶ ـ ۷ (بندهای اول و دوم) ماده ۸ ـ ۱۱ ـ ۱۵ ـ ۱۶ ـ ۱۸ را تجویز نمی‌کند. ۳- دولتهای طرف این میثاق که از حق انحراف استفاده می‌کنند، مکلفند بلافاصله سایر دولتهای طرف میثاق را توسط دبیرکل ملل متحد از مقرراتی که از آن انحراف ورزیده و جهاتی که موجب انحراف شده است مطلع نمایند و در تاریخی که به این انحراف‌ها خاتمه می‌دهند مراتب را به وسیله اعلامیه جدیدی از همان مجری اطلاع دهند»

الف) احترام حقوق یا حیثیت دیگران.

ب) حفظ امنیت ملی یا نظم عمومی یا سلامت یا اخلاق عمومی» (UN General Assembly: 1966).

دولت‌ها حق نقض آزادی بیان به‌صورت خودسرانه و خارج از ضوابط قانونی را ندارند، بلکه با رعایت سایر شرایط، صرفاً امکان محدود ساختن، «موارد انحصاری» بر شمرده‌شده در اسناد بین‌المللی حقوق بشری را خواهند داشت. به‌عنوان نمونه، احترام به حقوق و آزادی‌های دیگران،[1] صیانت از امنیت ملی،[2] نظم، سلامت یا اخلاق عمومی[3] در زمره‌ی مهم‌ترین محدودیت‌های مندرج در میثاق بین‌المللی حقوق مدنی و سیاسی و کنوانسیون اروپایی و آمریکایی حقوق بشر هستند. محدودسازی این حق در فضای سایبر نیز به علت تأمین نظم عمومی این فضا صورت می‌گیرد.

البته صرف تأمین نظم و پیشگیری از بزه که یکی از ضروریات این امر است، منجر به مشروعیت تحدید این حق نمی‌شود، بلکه بنا بر اصل قانونی بودن، هرگونه تحدید حق آزادی بیان باید مطابق با قانون باشد. البته لازم به ذکر است که صرف تصریح در قانون کافی نیست. بنا به نظریه‌ی عمومی شماره ۳۴ کمیته‌ی حقوق بشر سازمان ملل متحد، قانون باید در دسترس عموم مردم قرار داشته باشد و محدودیت‌ها و استثنائات را بدون هرگونه ابهام مشخص کرده باشد. همچنین، قانون باید به‌گونه‌ای باشد که افراد توانایی تطبیق فعالیت‌های خود با آن را داشته باشند و به‌عبارت‌دیگر، قانون توانایی عملی شدن در جامعه را داشته باشد. به‌علاوه، قانونی که به‌موجب آن محدودیت‌ها مشخص می‌شود نباید مخالف اهداف و مقررات برشمرده در کنوانسیون حقوق مدنی و سیاسی باشد و حقوق غیرقابل تبعیض[4] برشمرده در میثاق را نقض ننماید (GC No. 34, Para: 25). با توجه به نظر کمیته مشخص می‌شود که هرگونه سلب و یا محدودیت دسترسی به فضای سایبر با

1. Respect for the rights or reputations of others
2. Protection of public order (order public)
3. Protection of public health or morals.
4. Non-discrimination

هدف پیشگیری از موقعیت‌های پیش‌جنایی احتمالی نیز باید در قانون تعیین شود و قانون مذکور نباید ابهامی داشته باشد.

همچنین هرگونه اقدامی برای محدود ساختن حق آزادی بیان در راستای اهداف برشمرده شده، مستلزم «ضرورت» اتخاذ تدابیر مورد نظر برای نیل به اهداف برشمرده شده در اسناد عام حقوق بشری است. ضرورت در جایی معنی پیدا می‌کند که راه دیگری برای صیانت از اهداف یادشده و آزادی بیان وجود نداشته باشد و باید یکی از آن‌ها را بر دیگری ترجیح داد؛ بنابراین چنانچه بتوان تدابیری را اتخاذ کرد که منجر به جمع موارد فوق شود، باید آن را به‌کار بست و آزادی بیان را محترم شمرد. در انتها لازم به ذکر است که کنوانسیون اروپایی حقوق بشر شرایط «جامعه دموکراتیک و تناسب» اقدامات مورد نظر با اهداف برشمرده را نیز علاوه بر شرایط سه‌گانه‌ی مندرج در میثاق حقوق مدنی و سیاسی برشمرده است. علی‌رغم عدم قید این شرط در میثاق، نظریات عمومی شماره ۲۷ و ۳۴ میثاق بین‌المللی حقوق مدنی و سیاسی، شرط تناسب را به رسمیت شناختند و قید کرده‌اند که تدابیر اتخاذی نباید گسترده[1] باشند. بنا بر نظریه‌ی عمومی ۲۷ میثاق، «اقدامات محدودکننده باید مطابق با اصل تناسب باشند و همچنین باید از میان تدابیر موجود برای نیل به اهداف برشمرده شده کم‌ترین حد مداخله‌آمیزی را داشته باشند. آن‌ها باید متناسب با اهدافی مورد حمایت باشند» (GC No. 27, para: 14) درحالی‌که یکی از مهم‌ترین ایرادات وارد بر برخی از تدابیر پیشگیرانه‌ی موقعیت‌مدارِ سایبری، عدم رعایت شرط تناسب است.

به‌منظور تأمین فضای سایبری امن و در قالب قیود برشمرده شده، ایرادی بر عدم برخورداری مطلق از این حق در راستای پیشگیری موقعیت‌مدار از بزه سایبری وارد نیست. چراکه، در صورتی می‌توان از این حق بهره برد که امنیت داده‌های در حال گردش حفظ شوند و از بزه‌دیدگی احتمالی کاربران پیشگیری شود. در غیر این صورت، ذی‌حقان – که در این بستر کاربران هستند–

1. Overbroad

دچار آسیب شده و از استیفای حق قانونی خود باز خواهند ماند؛ بنابراین یکی از علل اصلی تحدید حق آزادی جریان اطلاعات در جریان پیشگیری موقعیت‌مدار از ارتکاب بزه، صیانت از بزه‌دیدگی احتمالی کاربران است.

لیکن، مشکل از آنجایی آغاز می‌شود که در برخی از موارد به علت استفاده گسترده و نابه‌جا از تدابیر پیشگیرانه موقعیت‌مدار سالب و یا محدودکننده‌ی دسترسی، حق جریان آزاد اطلاعات کاربران «نقض» می‌شود. همان‌گونه که مشاهده می‌شود در اینجا از واژه‌ی نقض و نه تحدید استفاده کرده‌ایم؛ چراکه تحدید، قانون‌مدار بوده و با رعایت شرایط و موازین خاصی تحقق می‌یابد، درحالی‌که نقض به عدول از شرایط قانونی اشاره می‌کند؛ بنابراین در این حالت حق آزادی جریان اطلاعات به‌صورت غیرقانونی توسط مراجع قانونی نقض خواهد شد. به‌عبارت‌دیگر، آنان به علت پیشگیری از بزه‌دیدگی بالقوه کاربران از مخاطرات احتمالی سایبری، آنان را بزه‌دیده بالفعل اعمال غیرقانونی خود قرار می‌دهند. در این نوشتار به دنبال بررسی این موضوع هستیم که آیا ممکن است تدابیر رایج پیشگیرانه‌ی موقعیت‌مدار از جرائم سایبری، منجر به تحدید حق جریان آزاد اطلاعات شوند؟ و در صورت مثبت بودن پاسخ، آیا این محدودیت‌ها در چهارچوب اسناد مرجع حقوق بشری صورت می‌گیرند؟

۱. پالایشگرها؛ .

امروزه از پالایشگرها به‌منظور سلب دسترسی به محتویات نژادپرستانه، نفرت‌انگیز، هرزه‌نگاری، مغایر اخلاق عمومی، مخل نظم عمومی، حقوق دیگران و مواردی ازاین‌دست استفاده می‌شود و از ورود کاربران به موقعیت‌های تهدیدآمیز جلوگیری می‌گردد. با استفاده از تقسیم‌بندی پیشنهادی کلارک، می‌توان نرم‌افزارهای پالایشگر را در زمره‌ی تدابیر افزایش تلاش[1] ارتکاب بزه قرار داد. پالایشگرها دسترسی بزه‌کاران با انگیزه به آماج مورد نظرشان را دشوار می‌نمایند. پالایشگرها موانع موقتی برای بزه‌کار ایجاد می‌نمایند و سعی در دلسرد نمودن وی از ارتکاب

1. Increase the Effort

بزه دارند، لیکن این روش‌ها نمی‌توانند دسترسی کاربران به صفحات مورد نظرشان را برای همیشه مسدود نمایند و شیوه‌های بسیاری همچون میزبان‌های میانی عبور بزه‌کاران از این روش را بسیار آسان نموده است.

تدابیر موقعیت‌مدار پالایشگر منحصر به دشوار ساختن ارتکاب بزه برای بزه‌کار نیستند و از بزه‌دیدگی احتمالی کاربران نیز پیشگیری می‌نمایند و یکی از علل اصلی استفاده از این تدابیر هم صیانت از آماج احتمالی است. به‌عنوان نمونه، با پالایش درگاه‌های بانکی تقلبی می‌توان از جرم «فیشینگ» پیشگیری نمود و یا با مسدود ساختن صفحات گروه‌های تروریستی، امکان سرقت اطلاعات شخصی کاربران از طریق نفوذ به دستگاه‌های آن‌ها وجود نخواهد داشت.

پالایشگرها بر اساس «فهرست سفید»[1] یا «فهرست سیاهی»[2] که برای آن‌ها تعیین می‌شود، فعالیت می‌نمایند. «فهرست سفید، اجازه دسترسی به مشخصات تعیین‌شده را می‌دهد. درحالی‌که فهرست سیاه اجازه دسترسی به مشخصات تعیین‌شده را نخواهد داد» (Schwabach, 2006: 173). عموماً مواردی همچون نام دامنه،[3] نشانی پروتکل اینترنت،[4] مکان‌یاب یکنواخت منبع وب،[5] کلید واژگان[6] و تصاویر در این فهرست‌ها گنجانیده می‌شوند و منجر به دسترسی و یا عدم دسترسی کاربران به محتویات مجرمانه خواهند گردید. به‌عنوان نمونه، چنانچه عبارت «پورنو» در فهرست سیاه قرار گیرد، هرگونه دسترسی به این عبارت برای کاربران غیرممکن خواهد شد.

---

1. Whitelist
2. Blacklist

۳. نام دامنه که معادل انگلیسی Domain Name System (DNS) می‌باشد، به نشانی اصلی وب‌سایت‌اطلاق می‌شود. به عنوان نمونه؛ نام دامنه خبرگزاری دانشجویان ایران www.isna.ir می‌باشد.

۴. نشانی پروتکل اینترنت (Internet Protocol Address) معرف دستگاه متصل به شبکه است. «هنگامی که دستگاه رایانه و یا هر وسیله دیگری که به شبکه اینترنت متصل می‌شود، نشانی پروتکل اینترنت مختص به خود را دریافت می‌نماید» (Harwood & others, 2015:445).

۵. مکانیاب یکنواخت منبع وب (Uniform Resource Locator)، نشانی کامل صفحه درخواستی از وب‌سایت مورد نظر می‌باشد. به عنوان نمونه، نشانی صفحه اجتماعی خبرگزای ایسنا، http://www.isna.ir/fa/service/Social است..

6. Key words

با توجه به هدف استفاده از تدابیر پالایشگر و قوانین کشور مورد نظر، نرم‌افزارها و سخت-افزارهای مذکور در سطوح خرد و یا کلان به‌کار گرفته می‌شوند. پالایشگرها می‌توانند «از سوی کاربران نهایی، ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت‌ها) یا ارائه‌دهنده‌ی خدمات اینترنتی، از سوی ایجادکننده نقطه‌ی تماس بین‌المللی و بر روی موتور جستجو» اعمال شوند (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۷).

در نظام حقوقی کشورمان، بالاترین سطح استفاده از این تدابیر در بعد داخلی لازم‌الاجرا می‌باشد؛ زیرا ماده ۲۱ قانون جرائم رایانه‌ای، ارائه‌دهندگان خدمات دسترسی یا همان میزبان‌های داخلی را موظف به استفاده از پالایشگرها نموده است. بر اساس این ماده: «ارائه‌دهندگان خدمات دسترسی موظف‌اند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. درصورتی‌که عمداً از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه‌ی دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه‌ی نخست به جزای نقدی از بیست میلیون (۲۰,۰۰۰,۰۰۰) ریال تا یک‌صد میلیون (۱۰۰,۰۰۰,۰۰۰) ریال و در مرتبه‌ی دوم به جزای نقدی از یک‌صد میلیون (۱۰۰,۰۰۰,۰۰۰) ریال تا یک میلیارد (۱,۰۰۰,۰۰۰,۰۰۰) ریال و در مرتبه‌ی سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

یکی از ایرادات وارد بر این ماده، عدم تبیین محتویات ناشی از جرائم رایانه‌ای و محتویات مرتبط با جرائم رایانه‌ای می‌باشد. به نظر می‌رسد منظور از «محتویات ناشی از جرائم رایانه‌ای»، ماحصل رفتار مجرمانه بزه‌کار و به عبارتی، نتیجه‌ی فعل مجرمانه وی است. به‌عنوان نمونه، چنانچه فردی با استفاده از سامانه‌های رایانه‌ای یا مخابراتی، صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی در شبکه‌های اجتماعی و وب‌سایت‌ها منتشر کند و در دسترس دیگران قرار دهد، بر اساس ماده ۱۷ قانون جرائم رایانه‌ای محکوم خواهد

شد و با شکایت شاکی و حکم مقام قضایی، ارائه‌دهندگان خدمات دسترسی موظف به حذف محتویات مذکور خواهند بود.

درحالی‌که، منظور از «محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود»، محتویات مرتبط با جرائم رایانه‌ای است. به‌عنوان نمونه، کاربری که خواهان نفوذ به دستگاه دیگران می‌باشد و سابقه ارتکاب بزه مذکور را ندارد، با رجوع به وب‌سایت‌های نشردهنده‌ی جاسوس افزارها،[1] نرم‌افزارهای مورد نیاز را بارگیری می‌نماید و شیوه‌ی استفاده از آن را با استفاده از توضیحات ارائه‌شده در وب‌سایت می‌آموزد و سؤالات و مشکلات احتمالی ناشی از عدم اجرای برنامه را با سایر کاربران و یا مشاور سایت در میان می‌گذارد. هرگونه اجازه‌ی گردش آزادانه‌ی اطلاعات از این نوع، منجر به بزه‌دیدگی شمار فراوانی از کاربران خواهد گردید؛ بنابراین ارائه‌دهندگان خدمات دسترسی با استناد به ماده‌ی مذکور موظف به پالایش محتویات مجرمانه یادشده خواهند بود. جرائمی همچون فروش، انتشار یا در دسترس قرار دادن غیرمجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می‌کند[2]، انتشار فیلترشکن‌ها و آموزش روش‌های عبور از سامانه‌های فیلترینگ[3] و فعالیت‌های رایانه‌ای شرکت‌های هرمی در زمره‌ی محتویات مورد نیاز و مرتبط با جرائم رایانه‌ای هستند.

فهرست مصادیق محتویات مجرمانه‌ی موضوع این ماده توسط کارگروه تعیین مصادیق محتوای مجرمانه تعیین می‌شود. این کارگروه، «در محل دادستانی کل کشور متشکل از وزیر یا نماینده‌ی وزارتخانه‌های آموزش‌وپرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صداوسیما و فرمانده‌ی نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضایی

1. Spywares

۲. موضوع ماده ۲۵ قانون جرایم رایانه‌ای.

۳. بند ج ماده ۲۵ قانون جرایم رایانه‌ای.

و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی می‌باشد» (عباسی کلیمانی و اکبری، ۱۳۹۴:۲۰۰).

این مصادیق تحت نه عنوان محتوا علیه عفت و اخلاق عمومی، محتوا علیه مقدسات اسلامی، محتوا علیه امنیت و آسایش عمومی، محتوا علیه مقامات و نهادهای دولتی و عمومی، محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود (محتوای مرتبط با جرائم رایانه‌ای)، محتوایی که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرائم)، محتوای مجرمانه‌ی مربوط به امور سمعی و بصری و مالکیت معنوی، محتوای مجرمانه‌ی مرتبط با انتخابات مجلس شورای اسلامی و مجلس خبرگان رهبری و محتوای مجرمانه‌ی مرتبط با انتخابات ریاست جمهوری از قوانین گوناگون مرتبط با این حیطه احصاء شده‌اند.[۱]

هرگونه پیشگیری از موقعیت‌های پیش‌جنایی احتمالی و صیانت از آماج بزه باید در چهارچوب موارد برشمرده و یا قوانین خاص باشد؛ بنابراین در فرآیند پیشگیری از جرم، باید به اصل قانونی بودن پیشگیری از ارتکاب بزه پایبند بود و نمی‌توان از انحرفات سایبری پیشگیری نمود. به‌عبارت‌دیگر، همان‌گونه که امکان محکوم ساختن افراد به علت ارتکاب اعمال انحرافی وجود ندارد، به‌طریق‌اولی نیز امکان محدود ساختن و یا نقض حق جریان آزاد اطلاعات کاربران به علت ارتکاب اعمال انحرافی سایبری، وجود نخواهد داشت.

اگر چه که به‌کارگیری تدابیر پالایشگر، سبب کاهش آثار زیان‌بار ناشی از گردش اطلاعات مجرمانه شده است، لیکن انتقادات بسیاری نیز به سبب تحدید و یا سلب بهره‌مندی کاربران از بسیاری از حقوق و آزادی‌های اساسی آن‌ها که در گرو استفاده از فضای سایبر است، وارد است. به‌عبارت‌دیگر، این ابزارها مشکلات فراوانی را برای کاربران به‌هنجار که درصدد استفاده صحیح از شبکه هستند، ایجاد می‌نمایند. در این قسمت بر آن هستیم با دیدی آسیب‌شناسانه به طرح و بررسی این ایرادات و ارزیابی آن‌ها بپردازیم.

---

۱. مذکور در: http://internet.ir/crime_index.html

۱-۱. پالایش بیش از اندازه؛[1]

امروزه پالایش بیش از اندازه به یکی از چالش‌های جدی فراروی آزادی جریان اطلاعات تبدیل گردیده است تا جایی که کمیته‌ی وزیران شورای اروپا در توصیه‌نامه‌ی اخیر خود که با عنوان «آزادی اینترنت» منتشر کرده است، از دولت‌های عضو درخواست نموده به‌منظور دستیابی به اهداف مشروع خود، پالایش مؤثر و کارآمد را سرلوحه‌ی خود قرار دهند و از پالایش بیش‌ازاندازه محتویات درخواستی کاربران که مانع جریان آزاد اطلاعات است، اجتناب نمایند (CM, 2015). پالایش بیش‌ازاندازه «در جایی بروز می‌یابد که تولیدکنندگان فیلترها برای به حداکثر رساندن کارآیی برنامه‌ی خود چنان حساسیت آن را بالا می‌برند که هرگونه مورد مشکوک را دسترس‌ناپذیر می‌سازد» (جلالی فراهانی، ۱۳۸۶: ۷۴). در این قسمت به‌طور خلاصه به ارزیابی چالش‌هایی که در نتیجه‌ی مصادیق دوگانه‌ی پالایش بیش‌ازاندازه به‌وقوع می‌پیوندد، خواهیم پرداخت.

مصداق نخست پالایش بیش‌ازاندازه زمانی به‌وقوع می‌پیوندد که کاربر محتویات دووجهی[2] را درخواست می‌نماید و محتویات مورد نظر مجرمانه نیستند، لیکن پالایشگر قادر به تشخیص ماهیت مجرمانه و یا غیر مجرمانه‌ی درخواست کاربر نیست و به‌همین علت دسترسی کاربر به محتویات مورد نظر را مسدود می‌نماید. یکی از نمونه‌های رایج این چالش را می‌توان در آگاهی کاربران از مباحث حوزه بهداشت و درمان دانست؛ چراکه در برخی از موارد، نرم‌افزارهای پالایشگر اجازه دسترسی کاربران به آن دسته از واژگان یا عباراتی که بین حوزه‌ی سلامت جسمانی و اعمال منافی عفت مشترک می‌باشند را نخواهند داد. در این حالت، نرم‌افزار به تطبیق واژه‌ی مورد نظر با فهرست سیاه تعریف‌شده خواهد پرداخت و ازآنجایی‌که واژه در فهرست وجود دارد، اجازه‌ی دسترسی کاربر به صفحه‌ی درخواستی را نخواهد داد، درحالی‌که واژگان و عبارات این حیطه، مفهومی دوگانه دارند و زمینه‌ای که در آن استفاده می‌شوند، حائز اهمیت

1. Over blocking filtering
2. Dubious contents

است. مثال سنتی که غالباً جرم‌شناسان و محققین «فاوا» در این حیطه از آن یاد می‌نمایند، ترکیب اضافی «سرطان سینه» است. زمانی که کاربر دستور جست‌وجوی این ترکیب اضافی را به مرورگر می‌دهد، نرم‌افزار پالایشگر این عبارت را به دو بخش سرطان و سینه تقسیم می‌نماید و به علت وجود واژه‌ی متأخر از آگاهی کاربران از مقالات و آخرین پژوهش‌هایی که پیرامون این بیماری مهلک صورت گرفته است، خودداری می‌نمایند.

نمونه‌ی دیگر چنین ضعفی را می‌توان در کاربست نرم‌افزارهای پالایشگر به‌منظور جلوگیری از بارگیری[1] غیرقانونی آثار دارای مالکیت معنوی مشاهده نمود. برای درک بهتر این موضوع، به «پرونده انجمن بلژیکی نویسندگان، آهنگ‌سازان و ناشران علیه شبکه‌ی اجتماعی نت‌لوگ»[2] که در تاریخ ۱۶ فوریه سال ۲۰۱۲ نزد دیوان دادگستری اتحادیه‌ی اروپا[3] اقامه شده است، اشاره می‌نماییم. شبکه‌ی اجتماعی نت‌لوگ همانند سایر شبکه‌های اجتماعی، کاربران متعددی داشت که در صفحات اختصاصی خود آثار هنری موسیقیایی و ویدئویی مورد علاقه‌ی خود را با دیگران به اشتراک می‌گذاشتند. امکانات موجود در این شبکه‌ی اجتماعی، ارتکاب جرم دسترسی غیر قانونی به آثار دارای مالکیت معنوی را تسهیل می‌نمود و به همین دلیل، انجمن خواستار دستور دادگاه مبنی بر توقف اشتراک‌گذاری رایگان آثار اعضای خود بود. به‌عبارت‌دیگر، انجمن درصدد حذف امکانات ارتکاب جرم و اتخاذ تمهیداتی برای جلوگیری از بزه‌دیدگی احتمالی اعضایش در آینده بود، لیکن دادگاه درخواست انجمن را نپذیرفت. آنچه این رأی را به رأیی مهم در حمایت از جریان آزاد اطلاعات برخط مبدل نمود، نگرش دادگاه به ترجیح حق جریان آزاد اطلاعات در برابر کاستی‌های موجود پالایشگرها است. بر اساس نظر دادگاه: «صدور دستور پالایش محتویات اشتراکی، جریان آزاد اطلاعات را تحت تأثیر قرار

1. Download
2. Netlog
3. The European Union Court of Justice

می‌دهد؛ چراکه نرم‌افزارهای پالایشگر همواره قادر به تمییز محتویات قانونی از غیرقانونی نخواهند بود» (SABAM v. NV: 2010, para 50).

به‌عبارت‌دیگر، دادگاه به این نکته واقف بود که فضای سایبر نقض حق مالکیت معنوی را تسهیل می‌نماید و حمایت از مالکین این آثار لازم است، لیکن هنگامی‌که حمایت از حق گروهی اندک در تضاد با حق اکثریت کاربران برای گردش آزادانه‌ی اطلاعات قرار می‌گیرد، حق اکثریت مقدم خواهد بود؛ چراکه پالایشگرها در بسیاری از موارد بین محتویات اشتراکی که مالک قانونی اجازه‌ی دسترسی عموم کاربران به آن‌ها را صادر کرده است و نیز مواردی که آثار قابل‌دسترس عمومی و رایگان هستند، قادر به تفکیک نخواهند بود و دسترسی به بسیاری از محتویات مجاز را غیرممکن می‌سازند.

مصداق دوم پالایش بیش‌ازاندازه زمانی به وقوع می‌پیوندد که پالایشگر قادر به تفکیک محتویات غیر مجرمانه‌ای که در کنار محتویات مجرمانه قرار دارند، نخواهد بود و به همین سبب، دسترسی کاربر به محتویات غیر مجرمانه را مسدود می‌نماید. این ایراد بر پالایشگرهای تک مؤلفه‌ای[1] وارد است؛ چراکه در پی تشخیص مجرمانه بودن محتویات صفحه یا وب‌سایت موردنظر، دسترسی کاربران به سایر محتویات را نیز غیرممکن خواهند ساخت. این اتفاق زمانی رخ خواهد داد که کاربر درصدد دسترسی به محتویاتی غیر مجرمانه، از وب‌سایت یا صفحه‌ای با ماهیت دوگانه است. ابتدائاً لازم به ذکر است که منظور از صفحات و یا وب‌سایت‌های با ماهیت دوگانه، آن دسته از صفحات و وب‌سایت‌هایی هستند که محتویات مجرمانه و غیر مجرمانه در آن‌ها توأماً وجود دارد؛ بنابراین زمانی که نام دامنه و یا مکان‌یاب یک‌نواخت منبع وب در فهرست سیاه گنجانیده شوند، درحالی‌که تمام محتویات موجود در آن وب‌سایت یا صفحه‌ی مجرمانه نمی‌باشند، حق جریان آزاد اطلاعات کاربران نقض خواهد گردید.

---

۱. لازم به توضیح است که سلب دسترسی به محتویات می‌تواند بر اساس یک شاخص و یا شاخص‌های متفاوت صورت گیرد. به عنوان نمونه، چنانچه پالایش صرفاً بر اساس واژگان باشد، پالایشگر مذکور تک مؤلفه‌ای و چنانچه بر اساس واژه، نشانی پروتکل اینترنت و تصویر باشد، پالایش سه مؤلفه‌ای می‌باشد.

یکی از اصولی که در دسترسی به اطلاعات دولتی وجود دارد و مقامات موظف به رعایت آن می‌باشند، عدم سلب دسترسی متقاضی به اطلاعات درخواستی، به علت وجود اطلاعات محرمانه در میان آن‌ها است که از آن به «اصل قابل تفکیک بودن اطلاعات» تعبیر می‌شود. بر اساس این اصل، «اگر اطلاعات درخواست‌شده فی‌نفسه، مشمول استثنائات آزادی اطلاعات نباشند ولی در سندی گنجانیده شده باشد که افشای آن به استناد استثناهای آزادی اطلاعات ممنوع است، باید این امکان برای متقاضی فراهم باشد که اطلاعات مورد درخواست وی از سایر قسمت‌های سند جدا شده و در اختیار او قرار گیرد» (انصاری، ۱۳۸۷: ۷۳). ازآنجایی‌که مبنای حقوق آزادی جریان اطلاعات و آزادی دسترسی به اطلاعات، آزادی بیان است و تفاوتی از این حیث میان آن‌ها وجود ندارد، رعایت این اصل برای حق جریان آزاد اطلاعات نیز ضروری است.

نمونه‌ی بارز چنین چالشی را می‌توان در کشور خودمان مشاهده نمود. به دلیل مجرمانه بودن برخی از محتویات وب‌سایت‌های اجتماعی و خبرگزاری‌ها، تمامی قسمت‌های این وب‌سایت‌ها برای کاربران ایرانی مسدود می‌شوند. درحالی‌که همه‌ی محتویات آن صفحه یا وب‌سایت نامناسب و یا حتی مجرمانه نیستند. کاربران ایرانی حق ایجاد صفحات شخصی در شبکه‌های اجتماعی همچون فیسبوک[1] و توئیتر[2] را ندارند و نمی‌توانند با دیگر کاربران در ارتباط باشند و آراء و اندیشه‌های خود را به دیگر کاربران انتقال دهند. همچنین، آن‌ها حق به اشتراک گذاشتن[3] و یا دریافت محتویات موجود در این وب‌سایت‌ها را ندارند و قادر نخواهند بود اخبار روز دنیا را از این منابع پیگیری نمایند. پژوهشگران و دانشجویان ایرانی قادر به دریافت جدیدترین نتایج تحقیقات علمی که به‌صورت فیلم در وب‌سایت یوتیوب به اشتراک گذاشته می‌شود، نیستند و

1. Facebook
2. Twitter
3. Sharing

نمی‌توانند سمینارها و کنفرانس‌های علمی برگزار شده در ایران را از این طریق با دیگر کاربران به اشتراک بگذارند.[۱]

علی‌رغم قانونی بودن پالایش محتویات شبکه، علت نقض حق جریان آزاد اطلاعات در این حالت را می‌توان در عدم رعایت قیود و شرایط لازم‌الاجرای پیشگیری از بزه دانست. برای درک بهتر این قضیه به پرونده‌ی «احمد یلدریم علیه دولت ترکیه»[۲] نزد دادگاه اروپایی حقوق بشر اشاره می‌نماییم. قضیه از این قرار است که بر اساس قسمت هشتم قانون انتشارات اینترنتی و مبارزه با جرائم اینترنتی[۳] مصوب سال ۲۰۰۷ این کشور، هرگونه توهینی به ملت ترک و مصطفی کمال آتاترک بنیان‌گذار حکومت جدید ترکیه ممنوع است. بنا به اذعان وزارت ارتباطات ترکیه تنها راه مسدود نمودن دسترسی کاربران به وب‌سایت مجرمانه، مسدود نمودن دسترسی آن‌ها به دامنه‌ی وب‌سایت‌های شرکت گوگل با نشانی www.googlewebsite.com می‌باشد. از همین‌رو، بنا به دستور دادگاه تمام وب‌سایت‌های مرتبط با شرکت گوگل، مسدود گردیدند. یلدیریم نزد دادگاه اروپایی حقوق بشر اثبات نمود که وب‌سایت وی هیچ ارتباطی با وب‌سایت مجرمانه مذکور نداشته و محتویات موجود در آن نیز مجرمانه نبوده‌اند، درحالی‌که دولت ترکیه با مسدود نمودن نام دامنه‌ی وب‌سایت میزبان، مانع از دسترسی و استفاده وی و سایرین از وب‌سایتش گردیده است. دادگاه اروپایی اعلام نمود که شرایط قانونی بودن، تناسب و ضرورت تدابیر اتخاذی با هدف مورد نظر رعایت نشده است. بنا بر نظر دادگاه: «دستور دادگاه ترکیه مبنی بر مسدود نمودن دسترسی کاربران به نام دامنه‌ی وب‌سایت‌های شرکت گوگل، نقض ماده ۱۰ اعلامیه اروپایی حقوق بشر است و حقوق بنیادینی که تضمین‌کننده‌ی آزادی بیان، آزادی دریافت و انتشار اطلاعات بدون محدودیت هستند را زیر پای گذاشته است... دادگاه ترکیه باید در نظر داشته باشد که حکم به پالایش وب‌سایت‌های شرکت گوگل

---

۱. البته لازم به ذکر است که در ماهیت مجرمانه برخی از محتویات وب‌سایت‌های یادشده تردیدی نیست. لیکن، نکته اساسی اینجاست که محتویات مجرمانه، نباید مانع از دسترسی کاربران به محتویات غیرمجرمانه گردند.

2. Ahmet Yildrim v. Turkey

3. Internet publications and combating Internet offences

کاربران را از دسترسی به شمار وسیعی از اطلاعات موجود در آن منع می‌نماید» (Ahmet Yildrim v. Turkey, 2013,paras:67-70).

بنابراین، همان‌گونه که مشاهده می‌نمایید پالایشگرهای تک‌مؤلفه‌ای نمی‌توانند به‌عنوان راه‌حل نهایی برقراری تعادل میان پیشگیری از بزه‌کاری سایبری از یک‌سو و صیانت از حق جریان آزاد اطلاعات کاربران از سوی دیگر به‌حساب آیند؛ زیرا چنانچه پالایشگرها صرفاً بر اساس واژگان تنظیم گردند و از معیارهای چندگانه‌ای همچون پالایش تصویر، جمله و صفحه استفاده ننمایند، احتمال نقض حق جریان آزاد اطلاعات کاربران بسیار فراوان خواهد بود. از طرف دیگر، چنانچه درصدد صیانت از حق جریان آزاد اطلاعات باشیم، محتویات چندوجهی را باید کاهش داد که در این حالت، احتمال بزه‌دیدگی کاربران و یا دسترسی به محتویات غیرقانونی افزایش خواهد یافت.

برای حل این مشکل، باید مؤلفه‌های موجود در فهرست سیاه پالایشگرها را افزایش داد و همچنین امکان تعیین حوزه‌ی درخواستی محتویات جست‌وجو شده را برای کاربران فراهم نمود، به‌عبارت‌دیگر، «نرم‌افزارها باید قادر باشند صحت یک واژه را در ضمن متن آن بررسی نمایند» (Chowhan & others, 2015: 359). کمیته‌ی وزیران شورای اروپا در فصل ششم توصیه‌نامه‌ی خود با عنوان «خودتنظیمی محتوای اینترنت»[1] به حاکمیت‌ها توصیه نموده است تا «امکانات مورد نیاز افزایش کیفیت پالایشگرهای محتوایی را فراهم نمایند» (CECM, 2001). به عنوان نمونه، بنا به توصیه‌ی این دستورالعمل، چنانچه کاربری درصدد دسترسی به محتویان علمی، دولتی و یا محتویات مناسب برای کودکان است، می‌بایست در موتور جست‌وجوگر وی گزینه‌هایی برای تعیین حیطه‌ی مورد نظر وی وجود داشته باشد تا پالایشگرها بتوانند پس از کاوش این عبارات در دسته‌بندی مورد نظر در فهرست سیاه خود، امکان دسترسی کاربران را فراهم نمایند.[2]

1. Self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services)

۲. البته در انتهای این بحث لازم به ذکر است که با بررسی تاریخ دو توصیه‌نامه مورد اشاره از شورای اروپا در این قسمت می‌توان دریافت که در طی ۱۴ سالی که از صدور توصیه‌نامه اول گذشته است، همچنان کشورهای عضو اتحادیه نتوانسته‌اند

۱-۲. پالایش فرامرزی؛

یکی از بایسته‌های پیشگیری از جرائم سایبری فرامرزی[1]، هماهنگی قوانین دخیل در پیشگیری است و به‌صرف اتکا به قوانین داخلی، نمی‌توان از بسیاری از جرائم احتمالی پیشگیری نمود. علی‌رغم نفوذ بی‌وقفه‌ی جرائم سایبری به خارج از مرزها و خسارات جبران‌ناپذیر حاصل از این جرائم، هنوز قانونی هماهنگ میان اعضای جامعه‌ی جهانی به‌منظور پیشگیری از این جرائم وجود نداشته و همین امر همکاری‌های منطقه‌ای و بین‌المللی برای پیشگیری از جرائم سایبری را با چالش‌های فراوانی مواجه ساخته است.[2] یکی از دغدغه‌های رایجی که در این راستا وجود دارد مصادیق غیرقانونی و مجرمانه‌ای است که دسترسی به آن‌ها ممنوع می‌باشد. اگرچه که قوانین داخلی سعی در ضابطه‌مند نمودن فعالیت‌های برخط کاربران داخلی می‌نمایند، لیکن نمی‌توان این مهم را نادیده گرفت که فضای سایبر، نیازمند قوانینی هماهنگ و نه یکسان، برای تمام اعضای جامعه‌ی جهانی است. عدم اجماع جامعه‌ی جهانی بر مصادیق جرائم سایبری، سبب گردیده است که در بسیاری از موارد، آنچه که در کشوری غیرقانونی می‌باشد در کشور دیگر قانونی بوده و پیشگیری از بزه احتمالی ممکن نباشد.

فقدان قوانین داخلی هماهنگ زمانی جریان آزاد اطلاعات را تحت تأثیر قرار می‌دهد که پالایش محتویات نامناسب در سطح ارائه‌دهندگان خدمات بین‌المللی انجام می‌شود و در برخی از موارد بر سر «محتویات قابل‌قبول»[3] اجماع وجود ندارد و امکان پالایش برخی از محتویات از سوی مقامات داخلی نیز وجود نخواهد داشت. به‌عبارت‌دیگر، «امروزه مشکلاتی پیرامون اجماع

سطح مطلوبی از پالایش مؤثر و کاستن از پالایش بیش از اندازه را فراهم نمایند. از همینرو، این شورا لازم دانسته است که در توصیه‌نامه اخیر خود، دوباره وظایف حاکمیت‌ها مبنی بر تناقض پالایش بیش از اندازه با آزادی جریان اطلاعات قانونی در فضای سایبر را یادآوری نماید.

1. Trans border / Transnational Cybercrime

۲. بر اساس بررسی‌های سازمان ملل متحد در سال ۲۰۱۳، از میان ۵۰ کشور از ۵ قاره آمریکا، آفریقا، آسیا، اروپا و اقیانوسیه، میانگین ۳۰ تا ۷۰ درصدی از جرایم سایبری فرامرزی گزارش شده است و بیشترین این آمار متعلق به قاره اروپا بوده است (United Nations Office On Drugs and Crime,2013:183).

3. Acceptable contents

بر تعریفی واحد از محتویات قابل‌قبول وجود دارد که مخالف با هنجارهای اعضای جامعه‌ی جهانی نیز نباشد» (Cooke, 2007: 364). در این حالت، گاه طرف مبدأ محتویاتی را غیرقانونی می‌داند که طرف مقصد آن‌ها را قانونی می‌شمرد و در صورت فقدان توافقنامه‌های دوجانبه میان طرفین، طرف مبدأ تعهدی مبنی بر پالایش محتویات مورد نظر نخواهد داشت.

به‌عنوان نمونه، کاربران شبکه‌های اجتماعی[1]، ممکن است متعلق به کشوری که شبکه‌ی مذکور در آن قانوناً به ثبت رسیده است، نباشند و از نقاط مختلف دنیا به عضویت این شبکه در آمده باشند. در این حالت، چنانچه برخی از صفحات کاربران از نظر قانونی که شبکه‌ی مذکور در آنجا به ثبت رسیده است، مجرمانه باشند؛ صاحبان امتیاز این شبکه‌ها، موظف‌اند از ادامه‌ی فعالیت آن‌ها خودداری نمایند، درحالی‌که چه‌بسا بر اساس قانون کشور برخی از کاربران، فعالیت‌های گروه‌های مذکور مجرمانه نبوده و کاربران آن کشور به‌موجب قوانین داخلی کشور متبوع‌شان حق دسترسی به آن‌ها را داشته باشند.[2]

«پرونده‌ی لیکرا علیه یاهو»[3] که در سال ۲۰۰۰ در دادگاه عالی فرانسه و سپس در دادگاه ایالات‌متحده آمریکا اقامه شده است، نمونه‌ی بارز چنین چالشی است. قضیه ازاین‌قرار بود که سایت حراج یاهو، وسایل با نشان نازیسم را حراج نموده بود و این حراج در وب‌سایت فرانسوی این شرکت با نام دامنه‌ی www. yahoofrance.com و همچنین در دامنه اصلی آن (www. Yahoo.com) برای کاربران فرانسوی موجود بود و آنان نیز می‌توانستند همانند سایر کاربران از این شرکت خرید برخط نمایند. دادگاه فرانسه به شرکت آمریکایی یاهو اعلام نمود که با استناد به ماده ۱-۶۴۵ قانون مجازات فرانسه هرگونه نشر، توزیع و دسترسی آثار مربوط به سازمان‌های مجرمانه، جرم است و به‌تبع قانون، این عمل در فضای برخط نیز نباید اتفاق بیافتد.

---

1. Social networks

۲. به علت رواج شبکه‌های اجتماعی تلفن همراه در سالهای اخیر، احتمال طرح پرونده‌هایی با موضوعاتی این‌چنینی در دادگاه-های منطقه‌ای حقوق بشری در سالهای آتی بعید به نظر نمی‌رسد.

3. Licra v. Yahoo

بر اساس دستور دادگاه، شرکت آمریکایی یاهو باید دسترسی کاربران فرانسوی به مکان‌یاب منبع یک‌نواخت وب‌سایت حراج مسدود نماید. شرکت یاهو، از پذیرش دستور دادگاه فرانسوی امتناع نموده و پرونده را نزد دادگاه کل ناحیه شمالی کالیفرنیا[1] مطرح نمود. قاضی دادگاه اعلام نمود که تصمیم قاضی دادگاه فرانسه قابلیت اجرا برای شرکت آمریکایی را ندارد؛ زیرا بر اساس اصلاحیه‌ی نخست قانون اساسی ایالات‌متحده آمریکا، حق آزادی بیان به‌رسمیت شناخته شده است و این حق، مشمول استثناء برشمرده شده در قانون فرانسه نخواهد شد.

۲. کاهش پهنای باند؛

افزایش کیفیت گرافیکی شبکه و لزوم دسترسی سریع به اطلاعات، سبب گردیده است که پهنای باند بالا[2] جز لوازم ضروری استفاده از شبکه جهانی اینترنت به شمار آید. «پهنای باند بالا به معنی قابلیت اتصال سریع و همیشگی به اینترنت است» (Lin, 2006: 45)؛ بنابراین هرچه پهنای باند تخصیص داده شده به کاربران بیشتر باشد، دسترسی آنان به شبکه با سرعت و کیفیت بیشتری ممکن خواهد بود.

علی‌رغم تأثیر مثبت پهنای باند بالا بر فعالیت‌های کاربران، نمی‌توان این مهم را انکار نمود که «همان فناوری موجود در پهنای باند بالا که سبب دسترسی به اطلاعات و خدمات می‌شود، امکان نفوذ بزه‌کاران بالقوه به رایانه‌های شخصی کاربران را نیز فراهم می‌نماید» (Armistead, 2010: 172). نمونه‌ی بارز این وضعیت را می‌توان در بسیاری از کشورهای قاره‌ی آفریقا مشاهده نمود. امروزه این کشورها به مانعی جدی در فرآیند پیشگیری بین‌المللی از جرائم سایبری تبدیل شده‌اند؛ زیرا «تأمین پهنای باند بالا در سال‌های اخیر از یک‌سو و ضعف بنیادین قوانین آن‌ها از سوی دیگر، سبب شده است که شمار نفوذگران موجود در این قاره افزایش

1. District Court for the Northern District of California
2. Broadband

چشمگیری یافته و به مبدأ بسیاری از حملات سایبری تبدیل شود» (Kharouni, 2013: 8). به همین سبب تا زمانی‌که زیرساخت‌های لازم برای افزایش امنیت شبکه فراهم نگردد، ارتکاب جرم برای بزه‌کاران با پهنای باند بالا بسیار آسان است. درحالی‌که، پیشگیری از اعمال آن‌ها با مشکلات فراوانی روبرو خواهد بود. به‌عنوان‌مثال، به علت فقدان فناوری‌های نوین، پالایش محتوایی[1] سریع ممکن نخواهد بود و در نتیجه کاربران به بسیاری از اطلاعات مجرمانه دسترسی می‌یابند.[2]

اما کاهش نسبی پهنای باند که دربردارنده‌ی کاهش سرعت اینترنت نیز می‌باشد، در دو حالت کلی برای تأمین امنیت سایبری و پیشگیری از بزه رخ خواهد داد. حالت نخست، زمانی است که در سطح کلان و یا خرد پهنای باند کمتری در برخی از شرایط به کاربران اختصاص داده می‌شود تا از بزه‌دیدگی احتمالی آنان پیشگیری شود و یا بزه‌کاران موفق به ارتکاب بزه نشوند. در این حالت؛ گردش اطلاعات خراب‌کارانه‌ی تروریستی بین کاربران کاهش پیدا خواهد کرد، آن دسته از کاربرانی که درصدد دریافت محتویات صوتی و تصویری هرزه‌نگاری هستند، در بیشتر موارد ناکام می‌مانند، نفوذگران برای دسترسی غیر مجاز به محتوای ارسالی و رمزگشایی برخط آن‌ها و شناسایی قابلیت‌های نفوذ وب‌سایت‌ها با مشکلات بسیاری مواجه می‌شوند و یا از حملات سایبری در سطح کلان پیشگیری خواهد شد، بنابراین به‌منظور «رعایت مسائل ایمنی و فنی و برخی ملاحظات امنیتی، می‌توان به‌راحتی با کنترل استفاده‌ی غیرقانونی از پهنای باند بین‌المللی، از وقوع برخی جرائم پیشگیری نمود» (بهره‌مند و دیگران: ۱۳۹۳، ۱۶۰).

---

1. Content filtering

۲. مصداقی از کاهش پهنای باند به عنوان ابزار پیشگیری موقعیت‌مدار در کشورمان را می‌توان طبق اظهارات دبیر شورای عالی فضای مجازی در گفتگوی ویژهٔ خبری بهمن سال ۹۱ مشاهده نمود. ایشان با اشاره به حملات سایبری به فضای مجازی کشور، اذعان داشتند که برای مقابله با این نوع از حملات، پهنای باند درگاه بین‌المللی اینترنت باید کاهش یابد و «برخی از این حملات اعلام و بسیاری اعلام نمی‌شود ولی وقتی این حمله‌ها صورت می‌گیرد ما مجبور می‌شویم در درگاه بین‌المللی کشور ترافیک را کاهش دهیم، در آن مقطع اگر میزبانی سایتی در خارج باشد، احساس می‌کند که اینترنت کند شده است» (مذکور در : http://www.iribnews.ir/fa/print/24721).

همچنین، استفاده از میانبرها برای نظارت قانونی بر مسیرهای[1] فعالیت کاربران یکی دیگر از روش‌های نظارتی است که منجر به کاهش سرعت اینترنت کاربران در فرآیند پیشگیری می‌شود. میانبرها درعین‌حال که منجر به تأمین امنیت نسبی شبکه شده و ابزارهایی قانونی برای نظارت سایبری می‌باشند، لیکن، سرعت اینترنت کاربران را دستخوش تغییر قرار می‌دهند.

اگرچه که در مقام عمل با کاهش پهنای باند، می‌توان مانع از بزه‌کاری و بزه‌دیدگی بسیاری از کاربران عادی شد، لیکن نمی‌توان از این مهم چشم پوشید که این روش‌ها، تدبیری اخلاقی برای جلوگیری از جرائم سایبری نیستند؛ زیرا بزه‌کاری احتمالی گروهی اندکی سبب می‌شود که گروه بسیاری در معرض تهمت قرار گرفته و از فضای برخط باکیفیت مناسب محروم بمانند؛ بنابراین «نباید سرعت اینترنت را قربانی محافظت از کاربران آسیب‌پذیر نمود» (Jaishankar, 2011: 99)؛ زیرا سهل‌انگاری و یا عدم آگاهی از مخاطرات فضای سایبر توسط برخی از کاربران، نباید سبب شود که همگان تاوان کاستی‌های آنان را بدهند، بلکه این گروه باید دانش و آگاهی خود را افزایش دهند و به‌طور جداگانه مورد حمایت قرار گیرند. حمایت از این گروه می‌تواند از طرق مختلفی همچون نظارت کارفرما، مسئولین مدارس، والدین و مواردی ازاین‌دست باشد.

بنابراین، مشاهده می‌شود که تدابیر فوق در غالب موارد، صرفات مانع جریان آزاد اطلاعات باکیفیت برای گروهی که اغراض مشروع دارند، می‌شود. به‌عنوان نمونه، در صورت خرید اینترنتی نرم‌افزار با حجم بالا و ارسال گذرواژه آن با پست الکترونیکی برای کاربر، بارگیری[2] محتویات مورد نظر بسیار زمان خواهد برد. همچنین بارگذاری برخی از وب‌سایت‌هایی که قالب‌های باکیفیت بالا دارند، بسیار زمان‌بر بوده و اتصال بارها قطع خواهد شد[3] و یا محققی که

1. Routers
2. Download

۳. مشکل اخیر در سالیان اولی که دسترسی به شبکه در کشور آغاز شده بود، به خوبی محسوس می‌بود و کاربران در بسیاری از موارد توانایی دسترسی به وب‌سایت‌های با کیفیت بالای داخلی و خارجی را نداشتند.

در کنفرانسی بین‌المللی به‌عنوان سخنران دعوت شده است و باید از طریق شبکه‌ی اینترنت به‌صورت زنده سخنرانی نماید، به علت سرعت پایین اینترنت توانایی برقراری ارتباط نخواهد داشت و یا در صورت برقراری ارتباط، ترافیک داده‌ها همراه با نوسان ارسال خواهند گردید و در نتیجه، صوت و تصویر ارسالی کیفیت مطلوب نخواهد داشت.[۱]

برآمد؛

ابزارهای ارتباطی این امکان را برای انسان معاصر فراهم نموده‌اند که برخلاف پیشینیان خود، از تحولات جهان پیرامون خودآگاهی یابند و فارغ از مرزهای مادی و بدون هرگونه مانعی با ساکنین کره‌ی خاکی در ارتباط باشند. کاربران فضای سایبر قادر خواهند بود اندیشه‌ها و افکار خود را با سایر کاربران به اشتراک بگذارند و از نظرات و عقاید آن‌ها بهره‌مند شوند. از همین‌رو، می‌توان بر آن بود که ویژگی انتقال آزاد اطلاعات منجر به رشد سریع فضای سایبر و همگانی شدن آن گردیده است.

علی‌رغم تأثیر مثبت فضای سایبر بر حق جریان آزاد اطلاعات، نمی‌توان این مهم را نادیده گرفت که همین ویژگی سبب سهولت ارتکاب بزه برای بزه‌کاران سایبری و ایراد خسارات فراوان به کاربران شبکه گردیده است. امروزه بزه‌کاران نیاز به جابه‌جایی فیزیکی ندارند و با استفاده از فضای سایبر می‌توانند آماج مناسب خود را هزاران کیلومتر دورتر از خود شناسایی نمایند و خسارات کلانی را بر آن‌ها وارد نمایند. تدابیر موقعیت‌مدار سالب و یا محدودکننده‌ی دسترسی روشی مناسب و سریع برای پیشگیری از بزه‌دیدگی شمار فراوانی از کاربران به‌حساب می‌آیند و ارتکاب بزه برای بزه‌کاران احتمالی را دشوار می‌نمایند.

---

۱. لازم به ذکر است که انتقادات پیرامون سرعت پایین اینترنت، صرفاً محدود به دسترسی به شبکه از طریق رایانه نیست. بنابراین سرعت پایین اینترنت برای برقراری ارتباط از طریق گوشی‌های هوشمند تلفن همراه که از طریق اپراتورها پشتیبانی می‌شوند، نیز مشمول همین قاعده می‌شوند.

یکی از چالش‌های اساسی رویاروی نهادها و یا اشخاص ناظر و مسئول پیشگیری از بزه، صیانت از حقوق بنیادین بشری کاربران از یک‌سو و تأمین فضایی سایبری امن از سوی دیگر است. بر اساس اسناد بین‌المللی و منطقه‌ای حقوق بشری، هرگونه تحدید حق آزادی جریان اطلاعات کاربران برای تأمین نظم و امنیت عمومی باید در چهارچوب موارد برشمرده شده در این اسناد و با رعایت قیود ضرورت و تناسب تدابیر اتخاذی با هدف مورد نظر باشد. اگرچه که ابزارهای فناوری اطلاعات و ارتباطات می‌توانند از بزه‌دیدگی شمار فراوانی از آماج در معرض خطر پیشگیری نمایند، لیکن در برخی از موارد استفاده حداکثری و یا نابه‌جا از این ابزارها سبب نقض حقوق بنیادین بشری کاربران ازجمله حق آزادی جریان اطلاعات خواهد شد. از همین‌رو، در بسیاری از موارد در کنار پیشگیری از بزه‌کاری، بهره‌مندی کاربران از حق دسترسی و استفاده از شبکه نیز نقض خواهد شد.

یکی از بارزترین ابزارهای نقض حق آزادی جریان اطلاعات، استفاده از پالایشگرها است. پالایشگرهای تک‌مؤلفه‌ای قادر به تشخیص محتویات مجرمانه نیستند و صرفاً بر اساس مؤلفه‌ی مورد نظر (به‌عنوان نمونه نشانی پروتکل اینترنت و یا مکان‌یاب یک‌نواخت منبع وب و یا واژگان) فعالیت می‌نمایند. در این حالت، پالایشگرها قادر به تفکیک اطلاعات مجرمانه از غیرمجرمانه نبوده و دسترسی کاربران به اطلاعات غیرمجرمانه را هم مسدود می‌نمایند. برای پیشگیری از این حالت، باید از پالایشگرهای چندمؤلفه‌ای استفاده نمود و همچنین در کنار آن مخاطب‌شناسی شود.

پالایش فرامرزی اطلاعات در مواردی که معیارهای هماهنگی برای شناسایی محتویات مجرمانه وجود ندارد، نیز می‌تواند منجر به نقض حق آزادی جریان آن دسته از کاربرانی شود که متعلق به کشور مسدودکننده نمی‌باشند. در انتها نیز لازم به ذکر است که در برخی از موارد برای پیشگیری از حملات سایبری گسترده‌ای همچون حملات تروریستی و پیشگیری از بزه‌دیدگی سایبری کاربران و یا تا زمان ایجاد زیرساخت‌های پیشگیری از بزه، سرعت اینترنت ملی کاهش داده می‌شود و از آن به‌عنوان ابزاری برای تأمین فضای سایبری امن استفاده می‌شود، درحالی‌که،

فقدان امکانات و یا دانش و فناوری نباید منجر به نقض حقوق بنیادین بشری کاربران بالأخص حق آزادی جریان اطلاعات گردد. .

منابع؛ .

الف. فارسی

- انصاری، باقر (۱۳۹۰). *آزادی اطلاعات*، تهران: نشر دادگستر.
- بابایی، محمدعلی؛ نجیبیان، علی (۱۳۹۰). «چالش‌های پیشگیری وضعی از جرم»، مجله حقوقی دادگستری. دوره ۷۵: صص ۱۷۲-۱۴۷. .
- بهره‌مند، حمید؛ کوره‌پز، حسین محمد؛ سلیمی، احسان (۱۳۹۳). «راهبردهای وضعی پیشگیری از جرائم سایبری»، آموزه‌های حقوق کیفری دانشگاه علوم اسلامی رضوی، شماره ۷: صص ۱۷۶-۱۴۷.
- جلالی فراهانی، امیرحسین (۱۳۸۴). «پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، فقه و حقوق، سال دوم: صص ۱۶۳-۱۳۳.
- --------، -------- (۱۳۸۶). «مزیت‌ها و محدودیت‌های فضای سایبر در حوزه‌های آزادی بیان، آزادی اطلاعات و حریم خصوصی». مجله حقوقی دادگستری، دوره ۷۱، شماره ۵۹: صص ۱۰۰-۶۱.
- خانعلی‌پور واجارگاه، سکینه. (۱۳۹۰). *پیشگیری فنی از جرم* (چاپ اول). تهران: میزان.
- رضایی، مهدی؛ بابازاده مقدم، حامد. (۱۳۹۳). «اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا»، پژوهش حقوق عمومی، دوره ۱۵، شماره ۴۲: صص ۸۲-۴۳.
- عباسی کلیمانی، عاطفه؛ اکبری، فاطمه. (۱۳۹۴). *جرائم سایبری*، تهران: انتشارات مجد.
- فضلی، مهدی. (۱۳۹۱). *مسئولیت کیفری در فضای سایبر*، چاپ دوم، تهران: انتشارات خرسندی.
- هاتف، مهدی. (۱۳۸۸). «چالش‌ها و چشم اندازهای امنیت در فضای مجازی»، *دوماهنامه توسعه انسانی پلیس*، دوره ۶، شماره ۲۲: صص ۱۱۷-۹۳.

- معتمدنژاد، کاظم؛ معتمدنژاد، رویا. (۱۳۸۸). *حقوق ارتباطات*، جلد یکم (کلیات)، چاپ دوم، تهران: دفتر مطالعات و توسعه‌ی رسانه‌ها.
- مقیمی، مهدی (۱۳۹۵). *سیاست‌ها و تدابیر سازمان ملل متحد برای پیشگیری از جرم سایبری*. رساله دکتری، دانشگاه شهید بهشتی، تهران.

ب. انگلیسی

- Armistead, Leigh (2010).. *Proceeding of the 5th International Conference Information Warfare and Security: ICIW Paperback, 2010*, Academic Publishing International Ltd.
- Clarke, V. Ronald. (1992). *Situational Crime Prevention: Successful Case Studies,* Second Edition. United States of America: Harrow and Heston.
- Cooke, Louise (2006).*"Controlling the net: European approaches to content and access regulation"*, Journal of Information Science.
- Harwood, Michael & Adrian Rusen, Ciprian & Ballew, Joli. (2015). *IC3: Internet and Computing Core Certification Global Standard 4 Study Guide*. Canada: Sybex.
- Jaishankar, k. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. United States of America: CRC Press.
- Kharouni, Loucif (2013). Africa: A New Safe Harbor for Cybercriminals?. Trend Micro Incorporated.
- Lin, Chinlon (2006)..*Broadband Optical Access Networks and Fiber-to-the-Home: Systems (Technologies and Deployment Strategies)*, England: Wiley.
- Schwabach, Aaron. (2006). *Internet and the Law: Technology, Society, and Compromises*. United S tates of America: ABC-CLIO.
- Thierer, Adam; Crews Jr, Clyde Wayne (2003). *Who Rules the Net? Internet Governance and Jurisdiction.* United States of America: Cato Institute.

.

.

.

- *Ahmet Yildirim v. Turkey* (no.3111/10), European Court of Human Rights, *18/03/2013.*
- *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, Judgment of the European Union Court of Justice (Third Chamber),Case No: C 360/10, 16 February 2012.
- Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA v. Yahoo!)

- Broadband Commission for Digital Development (2011), ITU/UNESCO. Broadband: A platform for progress.
- Committee of Ministers on 5 September 2001 at the 762nd meeting of the Ministers' Deputies, (2001). Council of Europe committee of ministers Recommendation (2001) 8 to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services).
- Committee of experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT) MSI-INT (2014) 13 rev 21 April 2015,Draft Recommendation CM/Rec(2015)__ of the Committee of Ministers to member states on Internet freedom (adopted by the Committee of Ministers on -at the the meeting of the Ministers' Deputies.
- Draft Recommendation CM/Rec (2015) of the Committee of Ministers to member states on Internet freedom (adopted by the Committee of Ministers on 2015 at the meeting of the Ministers' Deputies).
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011).
- Committee of experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT) MSI-INT (2014) 13 rev 21 April 2015
- Recommendation CM/Rec (2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters(Adopted by the Committee of Ministers on 26 March 2 at the 1022nd meeting of the Ministers' Deputies).

- Promotion and protection of the right to freedom of opinion and expression. A/66/290. 10 August 2011.
- Human Rights Committee, General Comment No. 34 – Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34 (2011)..
- UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999.
- UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
- UN General Assembly, Follow-up to the 12th United Nations Congress on Crime Prevention and Criminal Justice and preparations for the 13th United Nations Congress on Crime Prevention and Criminal Justice: resolution / adopted by the General Assembly, 12 March 2013, A/RES/67/184.
- UN Economic and Social Council (ECOSOC), UN Economic and Social Council Resolution 2002/13: Action to Promote Effective Crime Prevention , 24 July 2002, E/RES/2002/13.
- UN Human Rights Committee (HRC), CCPR General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service, 12 July 1996, CCPR/C/21/Rev.1/Add.7
- United Nations Office On Drugs and Crime Vienna (2013). Comprehensive Study on Cybercrime.
- United Nations Office on Drugs and Crime (UNODC),13th UN Congress on Crime Prevention and Criminal Justice, Doha, Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, 12 –19 April 2015.