فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال سیزدهم
شمارهٔ سوم، پاییز ۱۳۹۷

پیشگیری اجتماعی از جرائم سایبری

(در پرتو اجماع بین‌المللی بر منشورهای رفتاری)

تاریخ دریافت: ۹۷/۰۱/۲۲ **تاریخ پذیرش: ۹۷/۰۵/۱۶**

از صفحهٔ ۸۱ تا ۱۰۰

مهدی مقیمی[۱]

چکیده

فراملی بودن جرم سایبری سبب شده است، دغدغه دولت‌ها از سطح حاکمیتی و ملی فراتر رود و عرصهٔ بین‌المللی با چالش جدی روبه‌رو شود. بنابراین، منطق حاکم بر پیشگیری اجتماعی از جرم سایبری نیز متفاوت از فضای سنتی است. منطقی‌ترین گزینه برای ایجاد گفتمانی مشترک و هماهنگ با هدف پیشگیری اجتماعی از جرم بین‌المللی سایبری، پیش‌بینی سیاست‌هایی توسط سازمان ملل متحد است که مورد اجماع بین‌المللی باشد. هدف مقالهٔ حاضر، بررسی تحلیلی و انتقادی بسته‌ها و توصیه‌های سازمان ملل دربارهٔ پیشگیری اجتماعی از جرائم سایبری است. این پژوهش به شیوهٔ توصیفی- تحلیلی با استفاده از منابع کتابخانه‌ای و با مراجعه به مهم‌ترین اسناد بین‌المللی انجام شده است. یافته‌های این تحقیق نشان داد که مبارزه با جرم سایبری از حاکمیت انحصاری دولت‌ها خارج شده و کارآیی در پیشگیری از این جرم، منوط به ایجاد یک وفاق بین‌المللی در این حوزه است. با ملاحظهٔ منشور ملل متحد، گسترده‌ترین و هدفمندترین سازمان بین‌المللی موجود برای ایجاد اجماع در پیشگیری اجتماعی از جرم سایبری، سازمان ملل متحد است. نتایج این تحقیق نشان داد که توصیه‌های پیشگیرانهٔ سازمان ملل را می‌توان در چارچوب «منشورهای رفتاری سایبری» در نظر گرفت؛ منشورهایی که مسئولیت‌هایی برای «سیاست‌گذاران و تولیدکنندگان سایبری» و «ارائه‌دهندگان و کاربران خدمات سایبری» در نظر گرفته است.

کلید واژه‌ها: جرم سایبری، پیشگیری اجتماعی، منشورهای رفتاری سایبری، سازمان ملل متحد.

استناد: مقیمی، مهدی(پاییز ۱۳۹۷). پیشگیری اجتماعی از جرائم سایبری(در پرتو اجماع بین‌المللی بر منشورهای رفتاری). *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۱۳(۵۱)، صص ۱۰۰-۸۱.

۱. استادیار جرم‌شناسی دانشگاه علوم انتظامی امین، m60_moghimi@yahoo.com

مقدمه

در عرصهٔ فناوری‌های سایبری، دو فناوری یعنی «رایانه» و «مخابرات» نقش تعیین‌کننده‌ای دارند (جلالی فراهانی، ۱۳۹۲، ص۱۱). با کشف قابلیت‌های شگرف ناشی از تلفیق این دو فناوری، فضایی با ویژگی‌های کاملاً جدا از دنیای فیزیکی به وجود آورده‌اند که با عنوان «فضای سایبر» شناخته می‌شود. بدیهی است، فضای سایبر قابلیت‌ها و امکانات شگفت‌انگیزی به وجود آورده است؛ اما همانند دیگر عناصر زندگی اجتماعی، از گزند سوءاستفاده، به ویژه جرم، در امان نمانده است. مفهوم جرم سایبری، مفهومی نسبتاً جدید و تا حدودی مبهم است؛ اما با جمع‌بندی تعاریف ارائه شده می‌توان گفت، جرم سایبری مجموعه‌ای از سوءاستفاده‌ها و رفتارهای زیان‌باری است که «از طریق رایانه و سایر فناوری‌های اطلاعاتی و ارتباطی»، «علیه این نوع فناوری‌ها» یا «در فضای فراهم‌شده توسط این فناوری‌ها» واقع می‌شود. ازاین رو، بدون تأکید فراوان به واژگان این عرصه، به نظر می‌رسد واژهٔ «جرم سایبری» به تمام رفتارهای زیان‌بار مرتبط با فناوری‌های سایبری اشاره دارد.

همانند سایر جرائم، یکی از بهترین روش‌های مبارزه با جرم سایبری، پیشگیری از این جرم است. معمولاً برای پیشگیری از هر یک از جرائم، باید تحلیل‌هایی صورت گیرد تا بتوان فرآیند پیشگیری را معین کرد. دربارهٔ جرم سایبری نیز باید در ابتدا به ماهیت فراملی آن توجه کرد. به دلیل بین‌المللی بودن فناوری‌های سایبری (به ویژه اینترنت)، معمولاً این جرم به صورت بین‌المللی محقق می‌شود (یزدان‌پناه‌درو و کامران، ۱۳۹۴، ص۶۷). به همین دلیل، پیشگیری و مبارزه با این جرم، با اقدامات مستقل کشورها محقق نخواهد شد. با توجه به تحولاتی که در قرن حاضر در عرصه‌های مختلف اتفاق افتاده است، دولت‌ها نیازمند ایجاد تشکیلات منظمی هستند تا بتوانند با همکاری و همبستگی بین‌المللی، در رسیدن به اهداف مشترک، یکدیگر را یاری کنند (مشهدی و تسخیری، ۱۳۹۲، صص۱۵-۱۶). در این میان، مبارزه با جرم، توجه روزافزون سازمان‌های بین‌المللی را به خود جلب کرده است. در این شرایط باید سازمان‌های بین‌المللی که تنها علت وجودی آن‌ها برطرف کردن مشکلات بین‌المللی است، به جرم فراملی نیز به عنوان مسئله‌ای بین‌المللی نگریسته و برای برطرف ساختن آن تلاش کنند (زیبر، ۱۳۹۰، ص۳۵۵). آنچه در این زمینه اهمیت دارد، ایجاد گفتمان مشترک بین‌المللی برای پیشگیری از جرم سایبری است. برای ایجاد این گفتمان، سازمان‌های بین‌المللی باید به

جرم سایبری به منزلهٔ دغدغه یا مشکلی بین‌المللی بنگرند. در میان انواع سازمان‌های بین‌المللی، سازمان ملل متحد در توسعه و ایجاد همکاری‌های گستردهٔ سیاسی و اقتصادی میان نظام‌های گوناگون اجتماعی، اقتصادی، سیاسی و حقوقی نقش چشمگیری دارد. هم‌اکنون این سازمان، به واسطهٔ انتقال تجربه‌ها، ابتکارها و گسترش فعالیت‌هایش، کانون اصلی گردهمایی‌ها و انجام مذاکره دربارهٔ صلح، امنیت و نظم بین‌المللی است (مادهٔ ۵۵ و ۵۶ منشور). در میان جرائم فراملی، جرم سایبری یکی از بین‌المللی‌ترین مصادیق جرائم فراملی و به تبع آن، یکی از محوری‌ترین جرائم مورد توجه سازمان ملل طی دهه‌های اخیر بوده است. گرچه کشورهای عضو، در متضرر بودن از جرم سایبری، با یکدیگر هم عقیده‌اند، اما بر سر سازوکارهای پیشگیری از این جرم هرگز اتفاق نظری وجود ندارد. در واقع، عرصهٔ بین‌المللی، عرصه‌ای بسیار متنوع، متعدد و واگراست. از این رو، پیش از هر چیز ایجاد وفاق بین‌المللی دربارهٔ این مسئله بین‌المللی ضرورت می‌یابد.

با در نظر گرفتن ویژگی‌های تخصصی جرم سایبری، ماهیت فضای سایبری و نیز فنی بودن این دست جرائم (کاستلز[1]، ۲۰۱۴، ص۱۱۲)، صرفاً طیف خاصی از اسناد سازمان ملل متحد به ارائه تدابیر پیشگیرانهٔ اجتماعی برای مبارزه با جرم سایبری پرداخته‌اند. هدف از اعمال تدابیر پیشگیرانهٔ اجتماعی در محیط سایبری، ایجاد فرهنگ سایبری برای مبارزه و کاهش جرائم سایبری است. ایجاد فرهنگ سایبری در اسناد سازمان ملل متحد معمولاً در قالب «منشورهای رفتاری» در نظر گرفته شده است. هدف مقالهٔ حاضر، مطالعه و تحلیل مجموعه ضوابط و معیارهایی است که سازمان ملل متحد به عنوان منشور رفتاری و در راستای ایجاد فرهنگ سایبری با هدف پیشگیری اجتماعی از جرائم سایبری به کشورهای عضو توصیه کرده است.

مدل اجتماعی پیشگیری از جرم درصدد یافتن عوامل اجتماعی ارتکاب جرم و حذف آن از بستر جامعه است (محمدنسل، ۱۳۹۳، ص۶۷). پیشگیری اجتماعی دارای مزایای بی‌شماری است، اما اجرای طرح‌های پیشگیری اجتماعی دارای چند ایراد کلی نیز است؛ از جمله اینکه حوزه‌های دسترسی به هدف‌های پیشگیری اجتماعی، بسیار متنوع و وسیع است، به طوری که حتی با سرمایه‌گذاری‌های هنگفت و کلان، نتیجهٔ موردنظر (کاهش جرم) حاصل نمی‌شود یا گاهی مداخلات پیشگیرانه، ۲۰ الی ۳۰ سال بعد نتیجه می‌دهد

1. Castells

و غیره. لذا برای برخورداری از مزایای حداقلی این رهیافت، متخصصان کوشیده‌اند با ارائه الگوهای محدودتر و مشخص‌تر، گروه‌های اجتماعی خاص را هدف قرار دهند. این تدابیر که عمر چند ده‌ساله نیز دارند با عنوان «منشورهای رفتاری[1]» یا «مرامنامه‌ها/کردارنامه‌ها[2]» معروف شده‌اند.

منشور رفتاری سایبری: منشور رفتاری، مجموعه قواعد وضع شده برای دست‌اندرکاران یک حوزهٔ خاص است تا آن‌ها با ماهیت کار خود و همچنین عواقبی که در اثر نقض شرایط حاکم بر آن متحمل خواهند شد، آشنا شوند. معمولاً منشورهای رفتاری را برای مشاغل یا فناوری‌های مختلف به ویژه مشاغل یا فناوری‌هایی تدوین می‌کنند که از حساسیت زیاد برخوردارند. در زمینهٔ فضای سایبری، مسئولیت‌های دست‌اندرکاران در قبال عناصر محیط سایبری مانند کارکنان، مشتریان، تأمین‌کنندگان، رقبا، رسانه‌های گروهی، مدیران، کارشناسان، کارگران، شهروندان و غیره مورد توجه قرار می‌گیرند (آدام[3]، ۲۰۱۵، صص۲۳۵-۲۳۶). منشور متناسب با نقش و موقعیت افراد مختلف در فضای سایبری، مسئولیت‌ها و وظایفی پیش‌بینی می‌کند که بخش قابل‌توجهی از این وظایف، از ارتکاب جرم سایبری پیشگیری می‌کند؛ اما ارتباط منشورها با پیشگیری اجتماعی از جرم سایبری، آن است که تدوین این دست منشورها می‌تواند به ایجاد فرهنگ سایبری کمک کند. با تدوین این نوع منشورها در فضای سایبری، رعایت اخلاق در زندگی و ارتباطات اجتماعی سایبری شکل گرفته و نهادینه می‌شود. با نگاهی دیگر، فقدان منشورهای رفتاری، با توجه به ویژگی‌های خاص فضای سایبری، توجیه عقلانی و اجتماعی ندارد (همایش جهانی برای تنظیم‌کنندگان مقررات[4]، ۲۰۱۳، صص۵۴-۵۵). در این زمینه، لازم به ذکر است که برای نهادینه‌سازی و اجرای منشورهای رفتاری، پیش از هر چیز باید مخاطبان آن را شناسایی و گستره و نحوهٔ عملکرد آن‌ها را احصا کرد. از یک نگاه، اصول چنین منشوری باید دارای طیف مخاطبان، گروه‌های مختلف سنی،

1.Charter of Conduct/ethics
2.Codes of Conduct/ethics
3.Adam
4.Global Symposium for Regulators (GSR)

تحصیلی، اقتصادی، اجتماعی، فرهنگی، عمومی/خصوصی و غیره باشد. به‌طور کلی، می‌توان فعالان فضای سایبری را عبارت دانست از سیاست‌گذاران، تولیدکنندگان محصولات، ارائه‌دهندگان خدمات و کاربران فضای سایبری.

روش‌شناسی تحقیق

روش تحقیق مقالهٔ حاضر توصیفی- تحلیلی است. این تحقیق به توصیف و تحلیل چندجانبهٔ اسناد سازمان ملل متحد دربارهٔ پیشگیری اجتماعی از جرم سایبری پرداخته است. روش گردآوری داده‌ها، کتابخانه‌ای و اسنادی است. مقالهٔ حاضر با بررسی طیف وسیعی از اسناد سازمان ملل متحد (کنوانسیون، قطعنامه، پیش‌نویس معاهدات، معاهدات الگو و غیره) و نیز مراجعه به کتب، مقالات علمی، سایت‌های معتبر اینترنتی و سایر آثار پژوهشی موجود، به تحلیل موضوعات و محورهای مقاله پرداخته است.

یافته‌های تحقیق

در یک نگاه، فعالان فضای سایبری شامل سیاست‌گذاران، تولیدکنندگان محصولات، ارائه‌دهندگان خدمات و کاربران فضای سایبری است. سیاست‌گذاران فضای سایبری اشخاص حقیقی و حقوقی هستند که به‌نوعی در تصمیم سازی و تصمیم‌گیری برای این فضا نقش دارند. به همین ترتیب، تولیدکنندگان فناوری‌های سایبری نیز اشخاصی هستند که با توجه به نظام سیاست‌ها و تصمیم‌های جاری، به تولید فناوری سایبری می‌پردازند. قاعدتاً نقش، وظایف و مسئولیت‌های این دو دسته اشخاص، در روند فرهنگ‌سازی فضای سایبری تأثیری شگرف خواهد داشت. ارائه‌دهندگان خدمات سایبری، در مفهوم عام، عواملی هستند که به هر شکل اطلاعات و خدمات سایبری به ویژه اینترنتی را در اختیار کاربران یا مشترکان قرار می‌دهند. در ادامه به تفصیل، به بررسی نقش پیشگیرانهٔ ارائه‌دهندگان خدمات سایبری از منظر اجماع بین‌المللی پرداخته خواهد شد.

الف) تدابیر ویژهٔ سیاست‌گذاران و تولیدکنندگان سایبری: نگاه کلی و در واقع، چشم‌انداز سازمان ملل متحد در حوزهٔ پیشگیری اجتماعی از جرم سایبری را می‌توان به طور ویژه در اسناد سیاست‌گذار این سازمان واکاوی کرد؛ برای مثال، بند ۳۵

«بیانیهٔ اصول اجلاس عالی سران جهان دربارهٔ جامعهٔ اطلاعاتی[1]» (ژنو، ۱۲ دسامبر ۲۰۰۳) و به همین ترتیب، بند ۲۴ و ۶۷ دهمین کنگرهٔ سازمان ملل متحد دربارهٔ پیشگیری از جرم و اصلاح بزهکاران[2] که پیشنهاد می‌کند، مسئولیت‌هایی به این شرح در نظر گرفته شود: «توزیع مطالب غیرقانونی، مباحثی دربارهٔ نقش و مسئولیت‌های ارائه‌دهندگان خدمات اینترنت مطرح کرده است... ارائه‌دهندگان اینترنت عموماً هیچ تعهد قانونی جهت نظارت یا احتمالاً مسدودسازی محتوایی که به وسیلهٔ رایانه‌شان انتقال می‌یابند را ندارند. با وجود این، عموماً از یک ارائه‌دهندهٔ خدمات اینترنت خواسته می‌شود تا تمام قدم‌های معقول جهت پیشگیری از توزیع بیشتر مطالب غیرقانونی در صورت آگاه شدن از ماهیت این کار را بردارد... »[3]. وظایف و انتظارات یاد شده در این اسناد، صرفاً از سوی کسانی قابل‌اجرا و اِعمال است که به نوعی در راه‌اندازی و تصمیم‌گیری دربارهٔ فضای مجازی نقش دارند. این نقش‌آفرینان از دو دسته اشخاص خارج نیستند؛ سیاست‌گذاران و تولیدکنندگان فضای سایبری.

۱- سیاست‌گذاران فضای سایبری: دولت، تصمیم سازان، قانونگذاران و غیره باید سیاست‌های خاص و گام‌های راهبردی برای فرهنگ‌سازی در فضای سایبری را اجرا کنند. در یک نگاه کلی، مهم‌ترین و شاخص‌ترین اسناد سازمان ملل متحد در این زمینه عبارت‌اند از: «بستهٔ ابزار اتحادیهٔ بین‌المللی مخابرات برای ارتقای فرهنگ امنیت سایبری[4]» (۲۰۰۹)، بازنگری شده در سال ۲۰۱۵ و «رهنمود سازمان ملل متحد برای قانونگذاران و سیاست‌گذاران دربارهٔ حمایت برخط از اطفال و نوجوانان[5]» (۲۰۰۸)، بازنگری شده در سال ۲۰۱۴. در یک جمع‌بندی از این دو سند، می‌توان اصلی‌ترین تدابیر مربوط به سیاست‌گذاران فضای سایبری برای ترویج فرهنگ سایبری را عبارت دانست از:

- ایجاد آگاهی عمومی در خصوص موضوعات مربوط به مراقبت و نظارت در فضای

1. World Summit on the Information Society, Declaration of Principles, Geneva, Wsis, 2003
2. Tenth UN Congress on the Prevention of Crime and Treatment of Offenders "Crime and Justice
3. A/CONF.187/10
4. ITU Toolkit for Promoting a Culture of Cybersecurity
5. Guidelines for Policy Makers on Child Online Protection

سایبری و تعیین و شناسایی خط‌مشی‌ها، بهترین اقدامات، ابزار و منابع برای تطبیق و استفاده در کشورشان؛

- شناسایی مخاطرات و آسیب‌پذیری کاربران در فضای سایبری؛

- محفوظ نگهداشتن منابع برای استفاده عموم؛

- ایجاد سهولت در مشارکت‌های راهبردی بین‌المللی برای تعریف و انجام ابتکارات ملموس پیشگیرانه در ارتباطات اینترنتی؛

- ایجاد ظرفیت، کسب مهارت لازم و توسعهٔ راهکارهای هشداردهنده برای مقابله با تهدیدهای در حال رشد برای کاربران، زمانی که در اینترنت جستجو می‌کنند و به صورت برخط به اطلاعات دست می‌یابند.

علاوه بر مزایای متعدد در این دو سند، هرگز نمی‌توان مسئله مهمی چون شکاف دیجیتال در برخی کشورهای جهان سوم را از یاد برد. سازمان ملل متحد علاوه بر ملاحظات یاد شده، یک چک لیست (فهرست موضوعات) ارزیابی نیز برای کشورها تدوین کرده است. این چک لیست در واقع فهرست موضوعاتی است که برای ترویج فرهنگ جهانی سایبری لازم است و باید در سطح ملی تدوین شود و محور آن، اقدامات آموزشی، بازدارنده و تنبیهی باشد.

در ایران، در جلسه بیست و دوم شورای عالی فضای مجازی مورخ ۱۳۹۴/۱/۳۰، عنوان «طرح جامع توسعهٔ فضای مجازی سالم و ایمن» تصویب شد، اما همان‌طور که تعریف این طرح نشان می‌دهد، مبنای اصلی و محور آن پالایه (فیلتر) است. در همین راستا، لازم به ذکر است که «نظام جامع اینترنت سالم» نیز در یکی از کارگروه‌های تخصصی، فرهنگی و اجتماعیِ مرکز ملی فضای مجازی، در حال بررسی و تدوین است. یکی از ابعاد مختلف این نظام جامع نیز پالایهٔ فضای مجازی است. به همین ترتیب، پیش‌نویس «سیاست‌ها و ضوابط حاکم بر شبکه‌های اجتماعی برخط» توسط مرکز ملی فضای مجازی کشور تدوین شده، اما تاکنون به تصویب شورای عالی فضای مجازی کشور نرسیده است.

۲- تولیدکنندگان فضای سایبری: تولیدکنندگان فضای سایبری به ویژه صنعت نرم‌افزار می‌تواند نقش حیاتی در ترویج فرهنگ جهانی سایبری و محدود کردن موارد نامناسب ایفا کند. ضرورت تدبیرگذاری در عرصهٔ تولید فناوری‌های سایبری به این دلیل است که صاحبان این نوع صنایع با برخورداری از دانش تخصصی در مورد

دارایی‌های سایبری، شبکه‌ها، سامانه‌ها، تأسیسات، کارکردها و دیگر قابلیت‌ها و استفاده از کارشناسان ماهر در پیشگیری از جرم سایبری می‌توانند تولیدات مطلوب‌تر و متناسب‌تری برای فضای سایبری ارائه دهند. به همین ترتیب، آن‌ها با استفاده از تخصص و تجربه در مورد جرائم، تهدیدها و آسیب‌پذیری‌های سایبری، توانایی لازم برای ابداع و ارائه فناوری‌هایی با هدف تمرکز، تسریع و کارایی اقدامات پیشگیرانه را دارند. بر همین اساس، سازمان ملل متحد در برخی اسناد خود به ارائه تدابیری با محوریت تولیدات فضای مجازی پرداخته است. مهم‌ترین اسناد صادره در این حوزه عبارت‌اند از:

- «رهنمود سازمان ملل متحد برای شرکت‌ها و صنعت فناوری اطلاعات و ارتباطات دربارهٔ حمایت برخط از اطفال و نوجوانان[1]» (۲۰۰۸)، بازنگری شده در سال ۲۰۱۴[2]؛
- «رهنمود سازمان ملل متحد برای والدین، معلمان و مربیان دربارهٔ حمایت برخط از اطفال و نوجوانان[3]» (۲۰۰۸)، بازنگری شده در سال ۲۰۱۴؛
- «رهنمود سازمان ملل متحد برای کودکان و نوجوانان دربارهٔ حمایت برخط از اطفال و نوجوانان[4]» (۲۰۰۸)؛ بازنگری شده در سال ۲۰۱۴.

محوری‌ترین تدبیر مندرج در این اسناد، آن است که شرکت‌های فناوری اطلاعات و ارتباطات باید دربارهٔ آنچه تولید می‌کنند مسئول تلقی شوند. در قبال این تعهد، از دولت‌ها خواسته شده که از تولیدکنندگان نرم‌افزار که به تولید بسته‌های امنیتی می‌پردازند حمایت کند.

در مجموع، با عنایت به اینکه تولیدات فضای سایبری از تنوع بسیار بالایی برخوردار است، این نوع ارائه تدبیر را نمی‌توان کافی تلقی کرد. شاید پیش‌بینی مسئولیت برای تولیدکنندگان فضای سایبری، راحت‌ترین، در دسترس‌ترین و بدیهی‌ترین پیشنهاد باشد؛

1. Guidelines for Industry on Child Online Protection
۲. لازم به ذکر است از میان اسناد چهارگانه یاد شده، فقط این سند با همکاری یونیسف تدوین شده است، سایر اسناد صرفاً توسط اتحادیهٔ بین‌المللی مخابرات تدوین شده‌اند.
3. Guidelines for Parents, Guardians and Educators on Child Online Protection
4. Guidelines for Children on Child Online Protection

بنابراین شایسته است با تفکیک فناوری‌های اطلاعاتی از فناوری‌های ارتباطی و نیز سخت‌افزارها از نرم‌افزارها، به شیوه‌ای عمیق‌تر به این امر پرداخت. قطعاً تأثیری که نرم‌افزارها بر ایجاد و کاربری فضای سایبری دارند، به مراتب وسیع‌تر و تأثیرگذارتر از سخت‌افزارها است. به همین ترتیب، تفکیک میان بخش عمومی از بخش خصوصی از اهمیتی خاص برخوردار است. در نظر گرفتن اهداف حاکم بر تولیدات سایبری نیز شایان توجه است. بی‌تردید یک تولید سایبری با هدف اداری، تأثیر چندانی بر فرهنگ‌سازی پیشگیرانه ندارد، اما یک نرم‌افزار تفریحی یا آموزشی می‌تواند تأثیری شگرف بر ترویج یا انحراف از قواعد پذیرفته‌شده در فضای سایبری داشته باشد. در ایران، «سیاست‌های حاکم بر برنامهٔ ملی بازی‌های رایانه‌ای» در ارتباط با بانیان فناوری‌های سایبری در بند ۱ و ۲ «مادهٔ ۱- سیاست‌ها» مقرر می‌دارد: اولویت‌بخشی به محتوا، فرهنگ‌سازی عمومی و جریان‌سازی فرهنگی در داخل کشور و در عرصهٔ بین‌الملل و مقابلهٔ مؤثر با تهاجم فرهنگی با تکیه بر اندیشه‌ها و ارزش‌های اسلامی و سبک زندگی ایرانی- اسلامی و تقویت و ارتقای سطح آموزش و تربیت سرمایه‌های انسانی متعهد، متخصص و کارآمد موردنیاز صنعت بازی‌های رایانه‌ای. گذشته از تأخیر غیرقابل توجیه در تصویب این سیاست، ورود رسمی بانیان فناوری‌های سایبری به عرصهٔ سیاست‌های مرتبط با فضای سایبری قابل توجه و تقدیر است. این تقدیر از آنجا ناشی می‌شود که بیشتر بانیان یاد شده، از بخش خصوصی هستند.

ب) تدابیر ویژهٔ ارائه‌دهندگان و کاربران خدمات سایبری: در نگاهی کلی می‌توان نقش‌آفرینان فضای سایبری را شامل طیفی گسترده دانست. بخشی از این طیف را می‌توان زیر عنوان ارائه‌دهندگان خدمات سایبری مطالعه و بررسی کرد. هر یک از این گروه‌ها با توجه به فعالیتی که به‌طور تخصصی در فضای سایبر انجام می‌دهند، می‌توانند ضمن ترویج فرهنگ سایبری، در حوزهٔ پیشگیری از جرائم سایبری وظایفی را عهده‌دار شوند. به عکس، نقش این دسته از دست‌اندرکاران فضای سایبری به‌گونه‌ای است که می‌توانند فرصت و ابزار ارتکاب جرم سایبری را برای سایران فراهم آورند یا اینکه رأساً مرتکب شوند.

مهم‌ترین سند سازمان ملل دربارهٔ ارائه‌دهندگان خدمات سایبری، «بستهٔ ابزار اتحادیهٔ بین‌المللی مخابرات برای ارتقای فرهنگ امنیت سایبری[1]» است. این سند به همهٔ ارائه‌دهندگان خدمات سایبری به عنوان یک شخص حقوقی نگریسته و براین اساس، وظایف و الزامات کاری و تخصصی آن‌ها را برشمرده است، اما این سند مرز روشنی میان ارائه‌دهندگان خدمات سایبری قائل نشده است[2]. از دیگر غفلت‌های این سند، می‌توان به عدم توجه به کاربران فضای سایبری اشاره کرد. کاربران فضای سایبری را می‌توان شامل طیفی وسیع اعم از تجار، اپراتورها، افراد حرفه‌ای و غیرحرفه‌ای و غیره دانست. ممکن است، ابتدا چنین پنداشته شود که کاربران همانند سایر حوزه‌های مشمول قواعد الزام‌آور منشورهای رفتاری، باید به عنوان گروه مستحق حمایت نگریسته شود، نه اینکه رأساً مخاطب ضمانت‌های اجرایی قرار گیرند (رحیمی‌مقدم و جلالی فراهانی، ۱۳۸۷، ص۱۰۹). در این زمینه، باید توجه داشت فضای سایبری، قابلیت‌ها و امکاناتی در اختیار آحاد کاربران قرار داده که هر یک به تنهایی می‌توانند در هیبت یک «ارائه‌دهندهٔ خدمات» ظاهر شوند. شرایط حساس و آسیب‌پذیری که این فضا برای امور گوناگون رقم زده، ایجاب می‌کند هر کس به نوبهٔ خود در برابر رفتارش مسئول شناخته شود. از دیگر نقاط ضعف این سند، این است که آنچه حلقهٔ وصل همهٔ این نقش‌آفرینان به یکدیگر محسوب شده، صرفاً اینترنت است. در حالی که گرچه اینترنت حلقهٔ وصل نقش‌آفرینان فضای سایبری است، اما امروزه در کنار اینترنت، امور جدیدی مانند دولت الکترونیک، سامانه‌های خدمات رسان در اینترنت و غیره نیز دارای چنان کارکردهایی هستند که اهمیت آن‌ها را نمی‌توان کمتر از اینترنت دانست.

به هر وصف، با عنایت به تدابیر مندرج در این سند، نمی‌توان تفکیک روشنی میان ارائه‌دهندگان خدمات سایبری و وظایف پیشگیرانهٔ آن‌ها قائل شد؛ بنابراین باید برای تفکیک این گروه‌ها از یکدیگر به آثار علمی و تخصصی مراجعه کرد. با توجه به نقش و جایگاه ارائه‌دهندگان خدمات سایبری، می‌توان ارائه‌دهندگان خدمات سایبری را در چهار دستهٔ متمایز به این شرح از یکدیگر تفکیک کرد: ارائه‌دهندگان خدمات نام دامنه[3]؛

1.ITU Toolkit for Promoting a Culture of Cybersecurity

۲. در این سند، یک عنوان کلی یعنی «ارائه‌دهندگان خدمات اینترنتی» برای همهٔ دست‌اندرکاران این عرصه در نظر گرفته شده است.

3.Domain Name Providers

ارائه‌دهندگان خدمات میزبانی[1]؛ ارائه‌دهندگان خدمات دسترسی[2] و ارائه‌دهندگان محتوای الکترونیکی[3].

۱- ارائه‌دهندگان خدمات نام دامنه: از نظر فنی، «نام دامنه[4]»، نشانی اینترنتی (مانند .com، .net و غیره) وب‌سایت‌ها است. در واقع نام دامنه، معادل گذرنامه یا کد ملی در فضای سنتی است. با توجه به گستردگی فضای سایبری و کاربری‌های متنوع آن، نام‌های دامنه نیز می‌توانند متعدد و متنوع باشند. بر این اساس، نام دامنه نشان‌دهندهٔ هدف، محتوا و خلاصه مطالب وب‌سایت است. از دیدگاه فرهنگ‌سازی سایبری، اولین گام برای ثبت‌نام در فضای سایبری، انتخاب نام دامنه است. این بدان معناست که سایت‌هایی که دارای نام دامنهٔ مشخص هستند، دارای هویت نیز هستند، اما متقاضیان برخورداری از نام دامنه، هرگز به‌تنهایی نمی‌توانند این نام را برای خود بسازند یا از فضای سایبری بگیرند، بلکه این امر معمولاً توسط یک شخص حقوقی به ویژه یک شرکت خصوصی اینترنتی انجام می‌شود. آنچه در این روند اهمیت دارد، متقاضیِ استفاده از نام دامنه نیست، بلکه شرکت ارائه‌دهنده این نام است. در واقع، این شرکت به عنوان یک ناظر تخصصی در این روند عمل می‌کند؛ یعنی نظارت بر محتوا و اهداف سایتی که قرار است دارای هویت شود. از این رو، با توجه به حیطهٔ فعالیت و اطلاعاتی که در اختیار این شرکت قرار می‌گیرد، برای این شخص حقوقی مسئولیت‌های زیر پیش‌بینی شده است: ارائه دامنه براساس اصول فنی؛ ارائه دامنه براساس موازین قانونی و حفظ و عدم افشای اطلاعات شخص یا سازمان متقاضی نام دامنه.

۲- ارائه‌دهندگان خدمات میزبانی: به‌طور کلی، سایت‌ها از مجموعه‌ای از فایل‌های مختلف مانند تصاویر، متون، فایل‌های برنامه‌نویسی شده به زبان‌های مختلف و سایر موارد تشکیل می‌شود که به منظوری خاص به شکلی با هم مرتبط شده‌اند، اما برای اینکه امکان بازدید از این سایت‌ها در فضای سایبری فراهم شود، یک رایانه کارساز

1.Hosts
2.Access Providers
3.Content Providers
4.Domain

(سرور) به هر یک از سایت‌ها، فضایی را اختصاص می‌دهد. این بدان معناست که هر یک از سایت‌های موجود در فضای سایبری، از یک کارساز تغذیه می‌شوند. با اختصاص این فضا، هر یک از سایت‌ها می‌توانند محتوای خود (فایل‌ها، عکس‌ها و غیره) را به نمایش گذارند. فضای اختصاص داده‌شده به سایت دقیقاً مانند فضای رایانهٔ شخصی هر فرد است؛ با این تفاوت که فضای اختصاص‌یافته در اینترنت قرار دارد و در تمام طول شبانه‌روز، از تمامی نقاط جهان قابل‌دسترسی است. وجود همین تفاوت، مبنایی برای خدمات میزبانی فراهم می‌کند. به عبارت دیگر، در فضای سایبری، اطلاعات سایت باید روی رایانه‌ای قرار داشته باشد که ۲۴ ساعته به اینترنت متصل است تا کاربران سراسر جهان بتوانند در هر لحظه به آن دسترسی داشته باشند. این ابررایانه متصل به اینترنت، «میزبان وب[1]» نامیده می‌شود.

از دیدگاه فرهنگ‌سازی سایبری، ارائه‌دهندگان خدمات میزبانی، اطلاعات راجع به امور گوناگون اجتماعی را در اختیار دارند. در واقع، تمام محتوای سایت‌ها در اختیار ارائه‌دهندگان خدمات میزبانی است. کاربران و مخاطبان سایت‌های اینترنتی معمولاً برای استفاده از محتوای سایت‌ها باید اطلاعات هویتی خود را ارائه دهند. گاهی علاوه بر اطلاعات هویتی، اطلاعات مالی مانند شماره حساب برای خرید محصول و غیره نیز نیاز است؛ بنابراین در میان این محتوا، اطلاعات شخصی افراد، جایگاه حساس و تعیین‌کننده‌ای دارد. به همین ترتیب، بسیاری از امور مانند آموزش، کسب و کار و بانکداری الکترونیکی، بدون دسترسی به اطلاعات شخصی کاربران امکان‌پذیر نیست. در عین حال، خطرهای گوناگونی این اطلاعات را تهدید می‌کند؛ بنابراین ارائه‌دهندگان خدمات میزبانی، نقش تأثیرگذاری در پیشگیری از جرائم مرتبط با این حوزه خواهند داشت. در این رابطه، علاوه بر اسناد یاد شده تاکنون، اتحادیهٔ بین‌المللی مخابرات در «توصیه‌نامهٔ ۱۱۹۵» با عنوان «طرح تعامل‌پذیری برای حفاظت از خدمات و محتوا[2]» (۲۰۱۱)، به ارائه تدابیر پیشگیرانهٔ اجتماعی برای ارائه‌دهندگان خدمات دسترسی و خدمات میزبانی اقدام کرده است. براساس این سند، ارائه‌دهندگان خدمات میزبانی در راستای ترویج فرهنگ سایبری مکلف هستند سه اصل بنیادین را در حوزهٔ فعالیت خود

1.Web Hosting
2.X.1195, Service and content protection (SCP) interoperability scheme

رعایت کنند: تضمین حریم خصوصی و محرمانگی؛ صحت و تمامیت (اعتمادپذیری) و دسترس‌پذیری.

۳- ارائه‌دهندگان خدمات دسترسی: ارائه‌دهندگان خدمات دسترسی به فضای سایبری، پل ارتباطی میان دنیای فیزیکی با فضای سایبری محسوب می‌شوند. به واسطهٔ وجود این گروه است که کاربران می‌توانند به سایت‌ها وارد شوند (کوپارو[1]، ۲۰۱۵، ص۴۳). بنابراین، وظیفهٔ این گروه، ایجاد دسترسی به فضای سایبری است. اما همان‌طور که کاربران به سایت‌ها دسترسی می‌یابند، نفوذگرها، بدافزارها، جاسوس افزارها و غیره نیز به واسطهٔ همین دسترسی، می‌توانند وارد فضای سایبری شوند. از این رو، می‌توان مسئولیت این دسته از ارائه‌دهندگان را پیش‌بینی کرد. تأمین امنیت سخت‌افزاری و نرم‌افزاری (شبکه و اطلاعات) از مهم‌ترین وظایف این اشخاص محسوب می‌شود. این گروه باید از طریق تدابیری همچون پالایش، نصب دیوار آتشین و غیره، از ورودهای غیرمجاز جلوگیری کنند (فرومن[2]، ۲۰۱۵، ص۴۳۰). علاوه بر این مسئولیت، از دیدگاه فرهنگ‌سازی سایبری، یکی از مهم‌ترین اصول حاکم بر رفتارهای این گروه، نظارت بر حفظ حریم برخط افراد است. از آنجا که دسترسی به فضای مجازی توسط این گروه فراهم می‌شود، می‌توانند علاوه بر امکان‌پذیر ساختن شنود و ردیابی ارتباطات الکترونیک، دسترسی به موارد حساس را میسر سازند؛ مثل پایگاه‌های داده‌ای که ورود افراد غیرمجاز به آن‌ها ممنوع است و اطلاعات شخصی[3] و اطلاعات شخصی حساسی[4] که خود جهت پیشبرد فعالیت‌های شبکه‌ای جمع‌آوری کرده‌اند. در این زمینه، برخی ارائه‌دهندگان خدمات دسترسی، بر روی بعضی برنامه‌های جستجوی اینترنتی، بخش‌های معینی برای نظارت ایجاد کرده‌اند که با فعال کردن آن‌ها می‌توان دسترسی کاربران به ویژه کودکان به سایت‌های اینترنتی غیرمجاز را محدود کرد. این کنترل را می‌توان با برنامه‌های نرم‌افزاری خاص که روی رایانه نصب می‌شوند، انجام داد. در ایران همان‌طور که یاد شد، در این زمینه، مادهٔ

1.Capurro
2.Frohmann
3.Personal Information
4.Sensitive Personal Information

۲۱ قانون جرائم رایانه‌ای سال ۱۳۸۸ قابل استناد است. نکتهٔ قابل ذکر در این باره آن است که ارائه‌دهندگان خدمات دسترسی صرفاً دسترسی به فضای سایبری را امکان‌پذیر می‌سازند؛ بنابراین تمام هدف و تمرکز تدابیر پیشگیرانه باید بر این امر تمرکز یابد.

۴- ارائه‌دهندگان محتوای سایبری: بسیاری از کاربران فضای سایبری اغلب اوقات از طریق آی پاد، سایت‌های ویدئویی، سایت‌های شبکه‌های اجتماعی، اتاق‌های گفتگو، دوربین‌های وب‌کم، PDAها و گوشی‌های هوشمند، عملاً در فضای سایبری هستند. برخی کاربران نیز در فضای مجازی فعالیت نمی‌کنند؛ بلکه زندگی می‌کنند. دوستانی از نقاط مختلف با فرهنگ و عقاید مختلف پیدا می‌کنند، هیچ مرزی در دسترسی اطلاعات و محتوا برای آن‌ها وجود ندارد، آن‌ها همانند بسیاری از کاربران دیگر این فضا، به دلیل این ویژگی فضای مجازی که حیات افراد مساوی فعالیتشان است، باید شب و روز وقت بگذارند (اسپکتور[1]، ۲۰۱۱، ص۸۹).

وجود اطلاعات متعدد در اینترنت مزایای پرشماری برای کاربران فراهم می‌کند، اما تهدیدات جدی را نیز با خود به ارمغان می‌آورد؛ مانند دسترسی به مواد مضر و غیرقانونی مخدر، الکل، سیگار، قمار و بسیاری از موارد پرخطر دیگر؛ مطالب و تصاویر غیراخلاقی مانند هرزه‌نگاری، بهره‌کشی جنسی، انتشار اطلاعات شخصی، تهدید با تعالیم مذهبی منحرف، کم شدن توانایی‌های یادگیری و قرار گرفتن در معرض خشونت و قلدری. بنابراین، بدیهی به نظر می‌رسد که خطرات گوناگون فضای سایبری و به ویژه جرم سایبری، این گروه از جامعه (کاربران) را هدف قرار خواهد داد. همهٔ این نوع تهدیدها را می‌توان به‌نوعی با «محتوای سایبری» مرتبط دانست. در این زمینه، علاوه بر سایر اسناد یاد شده، «رهنمود سازمان ملل متحد برای شرکت‌ها و صنعت فناوری اطلاعات و ارتباطات دربارهٔ حمایت برخط از اطفال و نوجوانان» و «بستهٔ ابزار اتحادیهٔ بین‌المللی مخابرات برای ارتقای فرهنگ امنیت سایبری» دارای تدابیر منحصربه‌فردی است.

۵- تدابیر ویژه کاربران خدمات سایبری: در برداشتی کلی، «رهنمود سازمان ملل متحد برای شرکت‌ها و صنعت فناوری اطلاعات و ارتباطات دربارهٔ حمایت برخط از اطفال و نوجوانان» و «بستهٔ ابزار اتحادیهٔ بین‌المللی مخابرات برای ارتقای فرهنگ

1. Spector

امنیت سایبری» در پی آموزش «آموزش امنیت در اینترنت[1]» هستند. تحقیقات نشان داده بسیاری از کاربران از طریق تجربه یاد گرفته‌اند، چگونه در اینترنت از خود محافظت کنند، اما این فرآیند آموزشی به آن‌ها یاد می‌دهد، برای عدم مواجهه با محتوای نامناسب، چه کارهایی انجام دهند یا ندهند. بر همین اساس، تدبیر اساسی در این زمینه آن است که باید در پی ایجاد مجموعه‌ای از توانمندی‌ها بود که به کاربران، توانایی شناسایی محتوای موردنیاز آن‌ها را می‌دهد تا این اطلاعات را به شکل مؤثر بازیابی کرده و یافته‌ها را ارزیابی کنند. اصولاً محتوای مناسب، محتوایی است که کاربران بتوانند آن را در مجموعهٔ دانش خود وارد کنند و برای تحقق یک هدف خاص از آن‌ها استفادهٔ مؤثری به عمل آورند. به همین ترتیب، کاربران باید شرایط اقتصادی، حقوقی و اجتماعی حاکم بر استفاده از محتوای فضای سایبری را درک کنند و با رعایت موازین اخلاقی و قانونی به آن‌ها دسترسی یابند.

نکته‌ای که در این بخش از رهنمودها می‌توان به آن اشاره کرد، نوع مسئولیت است. در فضای سایبری و برای ترویج فرهنگ سایبری باید در نظر داشت، در بسیاری از کشورهای غربی، در کنار نظریه‌های رایج مسئولیت مانند عمد، تقصیر و غیره، «نظریهٔ مراقبت» به تأسی از مسئولیت مدنی وارد عرصهٔ جزایی شده است. طبق نظریهٔ مراقبت، اشخاص (اعم از حقیقی و حقوقی) به خاطر زندگی در عرصهٔ اجتماع باید حد معقولی از مراقبت‌ها را معمول دارند و اگر این مراقبت فراموش شود، شخص به خاطر بی‌مبالاتی قابل‌تعقیب است (کوپارو[2]، ۲۰۱۵، ص۴۳). باید به کاربران آموخته شود که تفاوت بین درست یا غلط در فضای سایبری، همان است که در دنیای واقعی وجود دارد و هر چه که می‌خوانند و می‌بینند، صحیح نیست. بنابراین، محور اصلی این رهنمودها، آموزش تدابیر کاربری صحیح است.

نتیجه‌گیری

مسائل فضای ارتباطی جدید در هر سطحی، تابعی از فرامتغیرهای اساسی فضای سایبری هستند. مواردی همچون «سریع شدن فضا»، «قابلیت دسترسی دائم»، «فرامکانی» و «فرازمانی»، «جهانی»، «سیال»، «تشدید واقعیت» و «چندرسانه‌ای»

1.Internet Safety Education
2.Capurro

بودن، فرامتغیرهای این فضا هستند که زندگی در جهان دوم و دوفضایی امروزه را تحت تأثیر قرار می‌دهند. یکی از مهم‌ترین این تأثیرها، پیدایش جرم سایبری است. حال با عنایت به ویژگی‌های یاد شده از فضای سایبری، این جرم به‌طور ذاتی می‌تواند فراملی باشد. فضای سایبری، محیطی همه‌گیر است که جرائم ارتکابی در آن را در فضایی جهانی مطرح می‌سازد. ایجاد قاعده و نظم بین‌المللی در این فضا مستلزم ایجاد تعهد به مجموعه قواعد بسیار عام و فراگیری است که با وجود تنوع فرهنگی، سیاسی، اقتصادی و غیره، موجب الزام جهانی و کاهش جرم سایبری شود. در این راستا، کارآمدترین سازمان بین‌المللی برای ایجاد نظم در فضای سایبری، سازمان ملل متحد است.

تدابیر پیشگیرانهٔ اجتماعی مطرح‌شده توسط سازمان ملل متحد تا حدودی با تأخیر توصیه شده‌اند. با نگاهی اجمالی به اسناد این سازمان می‌توان ملاحظه کرد که نخستین تلاش منسجم این سازمان برای ارائه تدابیر پیشگیرانهٔ اجتماعی به سال ۲۰۰۸ بازمی‌گردد. این در حالی است که فناوری‌های اطلاعاتی و ارتباطی تا آن سال رشد شایان توجهی داشته‌اند؛ به ویژه اینکه بسیاری از آثار علمی، تحقیقاتی، نشست‌ها و همایش‌های ملی و بین‌المللی حتی یک یا دو دههٔ پیش از آن سال، به واکاوی تدابیر پیشگیرانهٔ اجتماعی دربارهٔ جرم سایبری پرداخته بوده‌اند. البته ناگفته نماند که پیش از سال ۲۰۰۸، تلاش‌هایی در این زمینه توسط سازمان ملل متحد شده بود، اما انسجام لازم را نداشتند. در راستای سیاست‌های ترسیم شده در عرصهٔ بین‌المللی و برای اعمال هرچه بهتر پیشگیری اجتماعی از جرائم سایبری پیشنهاد می‌شود:

- در ایران با استفاده از اسناد و علوم مرتبط، «نظام پیشگیری اجتماعی از جرم سایبری» تدوین شود. براساس نظام پیشگیری اجتماعی از جرم سایبری می‌توان بسیاری از نقاط ضعف را دریافت و مسیر آینده را بهتر ترسیم کرد. چنانچه این نظام دربارهٔ چند جرم بین‌المللی مانند تروریسم، پولشویی و غیره نیز ترسیم شده و با یکدیگر مقایسه شوند؛ ملاحظات چشمگیری برای سیاست‌گذاری‌های بعدی در حوزهٔ پیشگیری اجتماعی از جرم سایبری به دست خواهد داد.

- صرف‌نظر از سایر عرصه‌های فضای مجازی، پیشنهاد می‌شود در عرصهٔ ملی و زیر نظر «مرکز ملی فضای مجازی»، «اداره/معاونت/کمیسیون ملی پیشگیری اجتماعی از جرم سایبری» تأسیس شود. هم اکنون ساختار سازمانی و ملی مرتبط با پیشگیری

اجتماعی از جرم سایبری از جمله مسائل فعلی کشور و چالشی محسوب می‌شود که در اولویت است. در اداره/معاونت/کمیسیون ملی پیشگیری اجتماعی از جرم سایبری لازم است یک «انجمن»، «اتحادیه» یا «ائتلاف» نیمه دولتی به عنوان «بانک اطلاعاتی» تشکیل شود. این بانک باید با مشارکت بخش خصوصی اداره شود. در واقع، بخش دولتی بانک اطلاعاتی، امور شکلی، اداری، صلاحیتی و غیره را انجام می‌دهد و بخش خصوصی، امور علمی و محتوایی را بر عهده خواهد داشت. نحوهٔ ادارهٔ آن نیز باید به صورت مشارکتی باشد. تشکیل این بانک می‌تواند یکی از مهم‌ترین دغدغه‌های سازمان ملل، یعنی ابهام در نرخ جرم سایبری را نیز تا حدود زیادی برطرف سازد. وجود ابهام در میزان واقعی جرم سایبری، دغدغه‌ای است که در بسیاری از کنگره‌های پنج سالانه مطرح شده و از سویی، هرگونه سیاست‌گذاری در عرصهٔ پیشگیری از جرم سایبری، منوط به شناخت صحیح وضعیت موجود، یعنی نرخ جرم سایبری است. عملکرد این انجمن، اتحادیه یا ائتلاف تنها در صورتی کارآمد خواهد بود که به درستی و دقت در پی ایجاد همکاری‌های عمومی- خصوصی باشد. البته در آثار علمی موجود و نیز بسیاری از اسناد منطقه‌ای و بین‌المللی، ضرورت وجود بخش‌های مورد اشاره به دقت یادآوری شده اما آنچه در این میان مهم است، حلقهٔ وصل عناصر یاد شده است. به نظر می‌رسد بهترین حلقهٔ وصل برای عناصر یاد شده، تأسیس «اتاق فکر سایبری» یا با نگاهی اختصاصی‌تر، «اتاق فکر پیشگیری از جرم/رویداد سایبری» باشد. در حقیقت اتاق فکر، محلی برای تصمیم سازی است. با توجه به برخورداری عناصر یاد شده از ظرفیت علمی، تجربی و کارشناسی قابل‌قبول، تمام گزینه‌های ممکن در این حوزه تنظیم و تدوین خواهد شد و مسیر عقلانی و منطقی پیشگیری از جرم سایبری، بهتر ترسیم خواهد شد. هم‌اکنون علم مدیریت نیز، منطقی‌ترین گزینه برای ترسیم مسیر حرکت را تأسیس یک اتاق فکر می‌داند.

- یکی از مباحث محوری برای پیشگیری اجتماعی از جرم سایبری، ترویج فرهنگ سایبری است. در ایران، رویکرد فعلی سیاست‌گذاری فضای مجازی بیشتر مبتنی بر الگوهای پیشین مواجهه با مسائل فرهنگی است. این رویکرد با دوران فعلی یعنی عصر انقلاب فناوری اطلاعات و ارتباطات تناسب ندارد. بر همین اساس، پیشنهاد می‌شود برای ترویج فرهنگ سایبری، در ابتدا سازوکاری برای حصول توافق و اجماع نسبی در سطح عالی سیاست‌گذاران، دستگاه‌های حاکمیتی و بین حاکمیت، بخش

خصوصی، نهادهای مدنی و مردم ایجاد شود. در این راستا، باید از اسناد بالادستی نظیر قانون اساسی، سیاست‌های کلی نظام در افق چشم‌انداز و نقشهٔ مهندسی فرهنگی بهره‌برداری شود. در تدوین فرهنگ سایبری باید توجه داشت که نمی‌توان اسنادی را تنها براساس آرمان‌ها و آرزوها و بدون توجه به داشته‌ها و توانایی‌ها تدوین کرد و انتظار تحقق آن را داشت. هرچند در سیاست‌گذاری ممکن است سندنویسی هم انجام شود، اما سیاست‌گذاری قابل‌تقلیل به سندنویسی نیست و هر سندی را نمی‌توان سند سیاستی خواند. سند سیاستی باید بتواند به‌طور واقع‌بینانه‌ای به تعارض‌ها و تزاحم‌ها بپردازد و برای حل آن‌ها و یا ترجیح میان آن‌ها جهت‌دهی عملیاتی ارائه دهد.

منابع

منابع فارسی

- جلالی فراهانی، امیرحسین (پاییز۱۳۹۲). پیشگیری از جرائم رایانه‌ای. *نشریهٔ حقوقی دادگستری*. ۷(۵۸)، صص۹ - ۲۱. بازیابی از: http://yon.ir/ZSpQo
- رحیمی‌مقدم، مهدی و جلالی فراهانی، امیرحسین (بهار۱۳۸۷). جرم سایبری. *نشریهٔ حقوق کیفری دانشگاه رضوی*. (۳۳)، صص۳۳ - ۴۵.
- زیبر، اولریش (۱۳۹۰). *جرائم رایانه‌ای* (محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی، مترجمان). تهران: انتشارات گنج دانش.
- سیاست‌های حاکم بر برنامهٔ ملی بازی‌های رایانه‌ای (۱۳۹۴)، مصوب جلسهٔ بیست و ششم شورای عالی فضای مجازی.
- قانون جرائم رایانه‌ای. ۱۳۸۸.
- محمدنسل، غلامرضا (۱۳۹۳). *جستارهایی در پیشگیری از جرم*. تهران: دانشگاه علوم انتظامی امین.
- مشهدی، علی و محمدصالح تسخیری (۱۳۹۲). *بایسته‌های حقوق سازمان‌های بین‌المللی* (ویرایش۱). تهران: نشر خرسندی.
- یزدان‌پناه‌درو، کیومرث و کامران، حسن (بهار۱۳۹۴). تروریسم در فضای مجازی و اثرات آن بر حوزهٔ جغرافیای سیاسی. *فصلنامهٔ جغرافیای*. ۱۳(۴۴)، صص۲۵-۴۵. بازیابی از: http://yon.ir/rxj3y

منابع انگلیسی

- A/CONF.187/10.
- Adam, A. (2015). Cyber ethics in a different voice, International Review of Information Ethics, Vol. 13, No.10 December.
- Capurro, R. (2015). Localizing the Internet: Ethical Aspects in Intercultural Perspective, Third Edition, Munich: Fink Verlag ICIE Book Series – Schriftenreihe des ICIE.
- Castells, Manuel (2014). Identity and Change in the Network Society, Second Edition, Conversation with Manuel Casells by Harry Kreisler.
- Capurro, R. (2015). Localizing the Internet: Ethical Aspects in Intercultural Perspective, Third Edition, Munich: Fink Verlag ICIE Book Series – Schriftenreihe des ICIE.
- Frohmann, B. (2015). Cyber Ethics: Bodies or Bytes?, The International Information & Library Review, Volume 32, Issues 13-14, September. Retrived from: *www.i-r-i-e.net/inhalt/007/irie_007_full*
- Global Symposium for Regulators (GSR) (2013). The Role and Responsibilities of an Effective Regulator, a Background paper on Cybersecurity, November.
- Guidelines for Industry on Child Online Protection(2008). Retrived from: *www.i-r-i-e.net/inhalt/007/irie_007_full*
- Guidelines for Industry on Child Online Protection (2008). Retrived from: *www.itu.int/.../ITU_Regional-Review_of-National-Activities-o*
- Guidelines for Parents, Guardians and Educators on Child Online Protection (2008). Retrived from: *www.tusla.ie/uploads/content/CF_WelfarePracticehandbook*
- Guidelines for Policy Makers on Child Online Protection (2008). Retrived from: *www.itu.int/en/cop/.../guidelines-policy%20makers-e*
- ITU Plenipotentiary Conference, Guadalajara (Mexico) (2010). Retrived from: *www.itu.int/plenipotentiary/2010*
- ITU Toolkit for Promoting a Culture of Cybersecurity (2009). Retrived from: *www.itu.int/ITU.../cybersecurity/.../itu-*

cybersecurity-work-
- ITU-D Study Group Q 22/1: Securing information and communication networks: best practices for developing a culture of cybersecurity. Retrived from: *www.itu.int/en/cop/.../guidelines-policy%20makers-e*
- Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000). Retrived from: *http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx*
- RESOLUTION 130 (Rev. Guadalajara, 2010). Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. Retrived from: */www.itu.int/osg/csd/cybersecurity/.../RESOLUTION_130.*
- Spector, M. (2011). Exploring the relationship between Internet ethics in university students and the big five model of personality, Computers & Education, Vol. 84 (1).
- World Summit on the Information Society, Declaration of Principles, Geneva, Wsis (2003). Retrived from: */www.itu.int/osg/csd/cybersecurity/.../RESOLUTION_131.*
- X.1195, Service and content protection (SCP) interoperability scheme. Retrived from: *www.itu.int/ITU.../cybersecurity/.../itu-cybersecurity-work*