

# پیشگیری اجتماعی از جرائم و انحرافات سایبری<sup>۱</sup>

امیرحسین جلالی‌فراهانی\*

رضا باقری‌اصل\*\*

تاریخ دریافت ۸۶/۴/۱۱

تاریخ پذیرش ۸۶/۸/۶

انسان امروزی در دنیای جدیدی به نام فضای سایبر قرار دارد که ویژگی‌های آن از دنیای فیزیکی متمایز است. این فضا با دارا بودن توانمندی‌هایی برای پیشرفت بهینه امور مرسوم پیشرفت‌های فناوری اطلاعات و ارتباطات الکترونیکی بوده و بشر را از به‌کارگیری بدون تبعیض و فراگیر آن در تمام عرصه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی، صنعتی، بهداشت و درمان و حتی نظامی ناگزیر کرده است. انعطاف‌پذیری و سادگی بی‌نظیر در امر کاربری، موانعی مانند محدوده سنی و میزان دانش و مهارت را از میان برداشته است؛ اما این وضعیت دغدغه‌هایی را هم برمی‌انگیزد، زیرا امکان انواع سوءاستفاده‌ها به‌طور غیرقابل باوری افزایش می‌یابد. از این رو باید برای بهره‌برداری صحیح و سودمند از امکانات، هنجارهایی را وضع و با ناهنجاری‌ها مقابله کرد. با این حال، از آنجاکه این هنجارها بر مبنای ویژگی‌های منحصر به فرد فضای سایبر تنظیم می‌شوند و برای آنها در دنیای فیزیکی مشابهی وجود ندارد؛ چنانچه کاربران - که همانند کودکان نوپا در این دریای بی‌کران رها هستند - مورد اطلاع‌رسانی کافی و صحیح قرار نگیرند؛ هرگونه مقابله با هنجارشکنی‌های سایبری با ایرادات جدی حقوقی مواجه خواهد بود.

در این مقاله راهکارهای پیشگیری اجتماعی از جرائم سایبری بررسی می‌شود. بدیهی است

۱. گفتنی است در همایش اخلاق و فناوری اطلاعات که در آذرماه ۱۳۸۵ در مرکز تحقیقات مخابرات ایران برگزار شد، این مبحث با رویکرد اخلاق سایبری ارائه شده است.

\* پژوهشگر دفتر فناوری‌های نوین، مرکز پژوهش‌های مجلس شورای اسلامی.

E-mail: Jalalyfarahany1979@gmail.com

\*\* مدیر دفتر فناوری‌های نوین، مرکز پژوهش‌های مجلس شورای اسلامی.

E-mail: bagheriasl@yahoo.com

توجه به محدودیت‌ها و موانع ذاتی این فضا، به اتخاذ راهکارهای منطقی و واقع‌گرایانه کمک خواهد کرد.

کلیدواژه‌ها: فضای سایبر؛ جرم سایبر؛ پیشگیری اجتماعی سایبری



پژوهشگاه علوم انسانی و مطالعات فرهنگی  
پرتال جامع علوم انسانی

## مقدمه

بشر در دوران حیات خود، همواره در تلاش بوده تا با کشف یا ابداع ابزارهای کاراتر، مسیر رشد و پیشرفت خود را با سرعت و سهولت بیشتری سپری کند. در این راه، ابزارهای مختلف بر زندگی وی تأثیرات متفاوتی داشته است. بسیاری از این ابزارها، فقط یک حوزه یا موضوع خاصی را تحت الشعاع قرار داده‌اند؛ اما برخی از آنها با برخورداری از آثار بنیادین توانسته‌اند دوران جدیدی را رقم بزنند.

بی‌تردید، امروزه فناوری اطلاعات و ارتباطات الکترونیکی<sup>۱</sup> دارای چنین ویژگی بزرگی است. اطلاعات<sup>۲</sup> ماهیت علوم را تشکیل می‌دهد و رشد و پیشرفت آنها در گرو تحلیل<sup>۳</sup> و پردازش<sup>۴</sup> صحیح اطلاعات است. از این رو یکی از رؤیاهای بشر، دستیابی به ابزاری بود که بتواند اطلاعات را با سرعت بیشتر و حفظ دقت و صحت، تحلیل و پردازش کند. حدود نیم‌قرن پیش، ابزاری به نام رایانه الکترونیکی<sup>۵</sup> به جهانیان عرضه شد که با وجود قدرت محاسبه و پردازش بسیار کم آن ماشین نسبت به حساب‌های الکترونیکی کوچک امروزی، تحول عظیمی را نوید می‌داد.<sup>۶</sup>

پس از مدتی پدیدآوردگان این ابزار دریافته‌اند که قابلیت‌های رایانه به مراتب بیش از آن است که فقط برای محاسبه و دیگر پردازش‌های محدود به کار رود و به راحتی می‌توان کارکردهای آن را به حدی توسعه و ارتقا داد که در موارد طراحی، حروفچینی، چندرسانه‌ای<sup>۷</sup> و بسیاری کارکردهای جذاب دیگر، به ابزاری بی‌رقیب تبدیل شود. این دیدگاه باعث شد رایانه‌ها در سطح گسترده‌ای به کار گرفته شوند و هر کس با برخورداری از اندک دانش و مهارت فنی، توانایی بهره‌برداری از آن را به دست آورد. به تدریج

---

1. Information and Communication Technology

2. Information

3. Analyze

4. Process

5. Electronic Computer

6. Casey, Eoghan, *Digital Evidence and Computer Crime*, Academic Press, 2001, P. 31.

7. Multimedia

از آنجا که رایانه‌های شخصی<sup>۱</sup> امور کاملاً متفاوت و متنوعی را با بازدهی بالا به انجام می‌رسانند، به یک میز کار<sup>۲</sup> منحصربه‌فرد تبدیل شدند.<sup>۳</sup>

اما آنچه به موازات ساده‌سازی و تنوع بخشیدن به کارکردهای انعطاف‌پذیر رایانه‌ای، بهره‌برداری گسترده‌تر و متنوع‌تر از این سیستم‌ها را به نحو باور نکرده‌ی در سراسر جهان توسعه داد؛ امکان اتصال آنها به یکدیگر از طریق ارتباطات الکترونیکی<sup>۴</sup> بود. کارکردها و اطلاعات میان رایانه‌ها به اشتراک گذاشته شد و به تدریج شبکه جهانی به وجود آمد و فضایی به نام فضای سایبر<sup>۵</sup> شکل گرفت که از دنیای فیزیکی به‌طور کامل متمایز بود، داستان‌های تخیلی مثالی از به‌کارگیری این ابزار و ویژگی‌های خاص آن است.<sup>۶</sup>

تمام این پدیده‌های تأثیرگذار و تحول‌آفرین، متناسب با شرایط جدیدی که بنیان می‌نهند، مستلزم هنجارهای<sup>۷</sup> نوینی هستند. برای مثال، تا زمانی که مردم از چهارپایان برای حمل و نقل استفاده می‌کردند؛ یکسری هنجارهای لازم‌الاتباع وجود داشت؛ اما از زمانی که انواع وسایل نقلیه موتوری، زمینی، هوایی و دریایی به خدمت گرفته شد، دیگر آن هنجارها کارایی خود را از دست داده یا به حوزه بسیار کوچکی محدود شدند.

هدف از وضع و اجرای این هنجارها، بهره‌برداری صحیح و سودمند از ابزارهای نوظهور است. به بیان دیگر، از آنجا که درباره نحوه بهره‌برداری از آنها و تمیز رفتارهای هنجارمند از ناهنجاری‌ها، هیچ‌گونه پیشینه و سابقه‌ای وجود ندارد؛ عاقلانه و منطقی است که فلسفه تولید و ماهیت آنها و همچنین انواع سوءاستفاده‌های احتمالی از آنها را برای کاربران شرح دهند.

1. Personal Computers (PC)

2. Desktop

۳. محمدحسن دزبانی، جزوه آموزشی حقوق سایبر و جرائم سایبری، جلد اول، ۱۳۸۴، ص ۴۴.

4. Electronic Communication (EC)

5. Cyber Space

۶. نام فضای سایبر ابتدا در سال ۱۹۸۲ در یک داستان تخیلی به کار رفت. ر.ک. جینا دی آنجلیز، جرائم سایبر، ترجمه

سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳، ص ۷.

7. Norms

با توجه به وضعیت خاص حاکم بر فضای سایبر، ضرورت هنجارگزینی در این باره بیشتر احساس می‌شود؛ زیرا اول اینکه میان این فضا و دنیای فیزیکی هیچ شباهتی وجود ندارد و چنانچه فرض بر این است که کاربران می‌توانند امور سایبری را با دنیای فیزیکی مقایسه کنند و هنجارهای حاکم بر آن را در اینجا نیز اجرا کنند؛ اشتباه است. برای مثال، این فضا همانند دنیای فیزیکی در مکان و زمان محصور نیست و همه چیز در آن ماهیت جهانی دارد. حال چگونه می‌توان هنجارهای حاکم بر یک محدوده زمانی و مکانی مشخص را در دنیای بی‌کران سایبری، لازم‌الاجرا دانست؟

دوم اینکه، برخلاف امور دنیای فیزیکی – که معمولاً می‌توان بر اساس شخصیت افراد، سن، جنسیت، موقعیت اجتماعی، میزان سواد و بسیاری مؤلفه‌های دیگر، مخاطبان آنها را شناسایی کرد – در فضای سایبر به دلیل وجود برخی ویژگی‌های منحصر به فرد، به ویژه سادگی و تنوع جذاب کارکردهای انعطاف‌پذیر رایانه‌ای و همچنین امکان ناشناس ماندن<sup>۱</sup> یا اتخاذ انواع هویت‌های دیگر، هر کس می‌تواند به هر امری مبادرت ورزد. لذا باید به همان گستردگی اقدام به وضع هنجارهای خاص کرد.

به علاوه کدام ابزار یا پدیده نوظهور را در دوران تاریخ بشر می‌توان یافت که به این گستردگی بتواند تمام حوزه‌های خرد و کلان را تحت الشعاع خود قرار دهد، تاحدی که هیچ واژه و ابایی در به کارگیری پسوند الکترونیکی (پیشوند-E) وجود نداشته باشد. هر آنچه با عنوان تجارت و دادوستد الکترونیکی<sup>۲</sup>، پول و بانکداری الکترونیکی<sup>۳</sup>، آموزش الکترونیکی<sup>۴</sup>، نشر الکترونیکی<sup>۵</sup>، انواع ارتباطات الکترونیکی، دادرسی الکترونیکی<sup>۶</sup> و حتی حکمرانی یا دولت الکترونیکی<sup>۷</sup> به کار می‌رود، همگی در فضای سایبر ریشه دارد. با اینکه

1. Anonymity
2. E-commerce and E-business
3. E-cash and E-banking
4. E-learning
5. E-publishing
6. E-trial
7. E-governance or E-government

تمام این موارد از کارکردهای رایانه‌ای تقریباً مشابهی استفاده می‌کنند؛ اما هنجارهای متفاوتی بر آنها حاکم است.

به این ترتیب، مسئله هنجارمندسازی فضای سایبر به یک معادله چندمجهولی شبیه است. در این فضا، همه موارد به هم مرتبط و بر هم تأثیرگذارند؛ آن هم نه در یک گستره محدود و مشخص؛ بلکه در یک دنیای بی‌کران - که درحقیقت هیچ حدودمرزی برای آن قابل تصور نیست. با وجود این، نمی‌توان این فضا را به حال خود رها کرد. چرا که در این صورت، نه فقط این فناوری در خدمت رشد و تعالی جامعه نخواهد بود؛ بلکه فروپاشی بنیان‌های آن را تسریع و تسهیل نیز خواهد کرد و به تدریج یک جامعه سایبری ناهنجار که هرج و مرج در آن رواج دارد؛ جایگزین جامعه هنجارمند فیزیکی خواهد شد. با این تفاوت که اصلاح و هنجارپذیرسازی آن، اگر غیرممکن نباشد، بسیار دشوار خواهد بود.

از این رو باید برای رفع این معضل - که تمام ارکان جامعه را به دلیل وابستگی مفرط به فضای سایبر به طور جدی تهدید می‌کند - راه‌حلی اساسی یافت. در ابتدا باید به وضع هنجارهای سایبری پرداخت تا کاربران بتوانند سره را از ناسره تمیز دهند. البته فرض بر عدم آگاهی کاربران از وجود و محتوای این هنجارهاست و باید اقدامات لازم را برای اطلاع‌رسانی و رشد آگاهی آنها انجام داد.

در مرحله دوم بر حسن اجرای هنجارهای موضوعه سایبری نظارت می‌شود؛ زیرا با فرض آگاهی مخاطبان از آنها، مقابله با هرگونه ناهنجاری توجیهی خواهد داشت. بروز یک واکنش مؤثر، متناسب و بازدارنده<sup>۱</sup> نه فقط از ارتکاب ناهنجاری‌های بعدی کاربر هنجارشکن جلوگیری می‌کند؛ بلکه به دیگر کاربران - که به‌طور بالقوه آماده ارتکاب

۱. این سه صفت (Effective, Proportionate, Dissuasive) اصولاً برای واکنش‌های کیفری به کار می‌روند و آن‌چنان جامع تلقی می‌شوند که در بسیاری از کنوانسیون‌های کیفری بین‌المللی و منطقه‌ای به کار رفته‌اند و از دولت‌های عضو خواسته شده واکنش‌های کیفری‌شان را به گونه‌ای تدوین و اجرا کنند که از این ویژگی‌ها برخوردار باشند. برای مثال، ر.ک. کنوانسیون جرائم سایبر (ماده ۱۳)، ضمانت اجراها و تمهیدات) و کنوانسیون ملل متحد برای مبارزه با فساد (از جمله ماده ۲۶، مسئولیت اشخاص حقوقی).

چنین ناهنجاری‌هایی هستند - هشدار می‌دهد و در صورت وجود سایر شرایط، آنها را نیز از این کار بازمی‌دارد.

مجموع این اقدامات یک فرایند را تشکیل می‌دهند. در اینجا می‌توان از الگوهای مشابه سازنده اقتباس کرد. فرایند علم پزشکی یکی از رایج‌ترین و ملموس‌ترین این الگوهاست. در علم پزشکی اصل بر این است که ابتدا با اجرای دستورالعمل‌هایی از بروز بیماری جلوگیری می‌شود که در اصطلاح به آن پیشگیری<sup>۱</sup> می‌گویند؛ اما چنانچه افراد به هر دلیل بیمار شوند، درمان<sup>۲</sup> در دستور کار قرار می‌گیرد.

این الگو درباره رفتارهای ناهنجار نیز قابل اجراست. قانون‌گذار از میان رفتارهای ناهنجار، جرائم<sup>۳</sup> را متمایز و برای آنها ضمانت‌اجراهای<sup>۴</sup> ویژه‌ای اعمال می‌کند که ماهیت کیفری داشته و مجازات<sup>۵</sup> نامیده می‌شوند.<sup>۶</sup> برای پیشگیری از وقوع جرم، به علم جرم‌شناسی<sup>۷</sup> نیاز است. حدود یک‌ونیم قرن پیش، برخی از دانشمندان حقوق کیفری با مطالعه علل و عوامل گوناگون پدیدآورنده جرائم، سعی در ارائه راهکارهای پیشگیرانه داشتند. این حوزه در سه دهه اخیر، با پیشرفت‌های چشمگیر، توجه صاحب‌نظران و سیاست‌گذاران را به خود جلب کرده تا حدی که کمتر مرجع یا نهاد مطالعاتی یا سیاست‌گذاری حقوق کیفری را می‌توان یافت که به مطالعات جرم‌شناختی نپردازد.<sup>۸</sup>

هم‌اکنون اهمیت تدابیر پیشگیرانه بر همگان محرز شده است، زیرا علاوه بر اینکه از بروز ناهنجاری‌ها و آسیب‌های گوناگون جلوگیری می‌کند؛ انواع هزینه‌های مربوط به اعمال

1. Prevention

2. Treatment

3. Crime, Offence

4. Sanction

5. Punishment

۶. علی حسین نجفی ابرندآبادی و حمید هاشم‌بیگی، *دانشنامه جرم‌شناسی*، انتشارات دانشگاه شهید بهشتی، ۱۳۷۷، ص ۶۲.

7. Criminology

۸. علی حسین نجفی ابرندآبادی، *تقریرات درس جرم‌شناسی (پیشگیری)*، تنظیم مهدی سیدزاده، مجتمع آموزش عالی

قم، دوره کارشناسی ارشد، نیم‌سال دوم ۱۳۸۱-۱۳۸۲، ص ۳۴.

هرگونه ضمانت اجراهای کیفری را در تمام مراحل رسیدگی تا مجازات به حداقل می‌رساند. گفتنی است دو شاخه حقوق کیفری و جرم‌شناسی، با وجود تعامل نزدیک با یکدیگر، حوزه‌های یکسانی را دربر نمی‌گیرند. یکی از مهم‌ترین وجوه تمایز آنها، پابندی حقوق کیفری به اصول لازم‌الاتباع حقوقی، مانند اصل قانونی بودن جرائم و مجازات‌هاست.<sup>۱</sup> به موجب این اصل، فقط فعل یا ترک فعلی قابل مجازات است که از سوی قانون‌گذار، جرم‌انگاری<sup>۲</sup> شده باشد.<sup>۳</sup> اما جرم‌شناسی به چنین اصولی پایبند نیست و حتی برای دستیابی به نتایج بهتر، مطالعات خود را علاوه بر جرائم، به انحرافات<sup>۴</sup> نیز توسعه داده است. انحراف همانند جرم، نوعی هنجارگریزی بوده؛ اما با این تفاوت که ضمانت اجرای آن به جای کیفر و مجازات، تقبیح و سرزنش اجتماعی است و به‌طور کلی آن دسته از رفتارها و حالاتی که فرد را در آستانه ارتکاب جرم قرار می‌دهند، در جرم‌شناسی مطالعه و بررسی می‌شوند. درحقیقت، انحراف یک اماره و پیشگویی از وقوع جرم است. البته مصادیقی از آن در قالب جرائم مانع یا بازدارنده،<sup>۵</sup> جرم‌انگاری شده‌اند. مانند سرعت غیرمجاز که می‌تواند به مرگ بیانجامد یا حمل اسلحه سرد و گرم که می‌تواند به قتل منجر شود.<sup>۶</sup>

از این رو، می‌توان جرم‌شناسی را یکی از ابزارهای بسیار مفید برای هنجارمند ساختن جامعه

۱. حسین میرمحمدصادقی، *تقریرات درس حقوق جزای عمومی*، دانشگاه امام صادق (ع)، تنظیم امیرحسین جلالی‌فراهانی، نیم‌سال دوم ۱۳۸۰-۱۳۸۱، ص ۲۰.

## 2. Criminalization

۳. اصل ۳۶ قانون اساسی کشورمان مقرر می‌دارد: «حکم به مجازات و اجرای آن، باید تنها از طریق دادگاه صالح و به موجب قانون باشد». همچنین، ماده (۲) قانون مجازات اسلامی، مصوب ۱۳۷۰ مقرر می‌دارد: «هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد، جرم محسوب می‌شود».

## 4. Deviation

### 5. Accessory Offences

جهت مطالعه مباحث درباره این گونه جرائم: ر.ک. علی‌حسین نجفی ابرندآبادی، *تقریرات درس جرم‌شناسی*، دوره کارشناسی، دانشگاه امام صادق (ع)، نیم‌سال ۱۳۸۱-۱۳۸۲، ص ۱۳۰۳.

۶. علی‌حسین نجفی ابرندآبادی، *تقریرات درس جرم‌شناسی (انحراف)*، دوره دکتری حقوق کیفری و جرم‌شناسی، مجتمع آموزش عالی قم، تنظیم علی‌مراد حیدری، نیم‌سال ۱۳۸۲-۱۳۸۳، ص ۱۷۱۲.



و پیشگیری از وقوع ناهنجاری‌ها دانست؛ زیرا برخلاف حقوق کیفری با محدودیت مواجه نیست و از آنجا که به انحرافات نیز می‌پردازد، حوزه وسیع‌تری از ناهنجاری‌ها را دربرمی‌گیرد و در نتیجه بیشتر ناهنجاری‌های اخلاقی مورد مطالعه و اقدامات جرم‌شناسی قرار می‌گیرند.

از آغاز فراگیری رایانه‌ها و به تبع آن پیدایش فضای سایبر، مسائل مربوط به مقابله کیفری با برخی ناهنجاری‌ها و جرائم<sup>۱</sup> رایانه‌ای و سایبری مطرح بود و اکنون نیز بسیاری از کشورهای جهان، قوانین کیفری مورد نیاز و همچنین اسناد بین‌المللی و منطقه‌ای گوناگونی را تصویب کرده‌اند که از جمله مهم‌ترین آنها می‌توان به کنوانسیون اروپایی جرائم سایبر<sup>۲</sup> - که ماهیت بین‌المللی هم دارد<sup>۳</sup> - اشاره کرد. کشورهای غیراروپایی هم می‌توانند به این کنوانسیون پیوندند.<sup>۴</sup> در کشور ما نیز، به جز تعدادی قوانین پراکنده،<sup>۵</sup> یک لایحه با عنوان «لایحه جرائم رایانه‌ای» - که با رعایت اصول و ضوابط خاص این فضا تدوین شده - در مجلس شورای اسلامی مراحل تصویب نهایی را می‌گذراند.

بنابراین با توجه به رشد نگران‌کننده ناهنجاری‌های سایبری - که فقط بخش کوچکی از آنها در حوزه حقوق کیفری می‌گنجد - هنوز مطالعات جرم‌شناختی سایبری به‌طور جدی پیگیری نشده است تا براساس آن بتوان تدابیر پیشگیرانه سایبری را استخراج کرد.

در این مقاله، به دلیل گستردگی این حوزه، یکی از شاخه‌های پیشگیری از جرائم و انحرافات سایبری، یعنی پیشگیری اجتماعی از جرائم و انحرافات سایبری، مورد بررسی قرار می‌گیرد. در این راستا، ابتدا به کلیاتی درباره مفهوم و ماهیت پیشگیری اجتماعی از

1. Cyber Crime

2. European Convention on Cyber Crime, 2001.

<http://conventions.coe.int/treaty/en/reports/html>.

۳. بتول پاکزاد، «اقدامات سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرائم رایانه‌ای»، مجموعه مقالات همایش

بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴، ص ۸۱

۴. ماده (۳۷) کنوانسیون.

۵. عبدالصمد خرم‌آبادی، «سابقه پیدایش، تعریف و طبقه‌بندی جرائم رایانه‌ای»، مجموعه مقالات همایش بررسی ابعاد

حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴، ص ۴۶.

جرائم می پردازیم. سپس نحوه اجرای کارکردهای پیشگیرانه اجتماعی بر ناهنجاری‌های سایبری را بررسی می‌کنیم و در پایان برای دستیابی به نگاهی واقع‌بینانه و منطقی از این الگو، محدودیت‌ها و موانع آن را تشریح کرده و نتیجه‌گیری می‌نماییم.

## ۱ مفهوم پیشگیری اجتماعی از جرم و انحراف

در مقدمه تا حدودی اهمیت پیشگیری از وقوع ناهنجاری‌های مجرمانه و منحرفانه تبیین شد. اهمیت این اقدامات به حدی است که بسیاری از دانشمندان حقوق کیفری معتقدند که اگر ضمانت اجرای کیفری نیز کارکرد پیشگیرانه نداشته باشند، اجرای آنها هیچ فایده‌ای نخواهد داشت. به بیان دیگر، همان‌گونه که انتظار می‌رود تدابیر پیشگیرانه از وقوع انحرافات و جرائم جلوگیری کنند؛ ضمانت اجرای کیفری نیز باید چنان مؤثر، متناسب و بازدارنده به اجرا درآید که در محکومین کیفری و مرتکبین بالقوه ارباب و عبرت کافی ایجاد کنند تا از تکرار و همچنین وقوع جرائم در آینده پیشگیری شود.<sup>۱</sup>

در مقدمه به الگوی پزشکی به‌عنوان مثالی از الگوی پیشگیرانه اشاره شد. به این ترتیب که در سه مرحله با عناوین اولیه، ثانویه و ثالث از بروز بیماری پیشگیری شده یا به درمان آن پرداخته می‌شود. همچنین، براساس سن افراد، بر پیشگیری از بزه‌کاری و بزه‌دیدگی کودکان تأکید شده است.<sup>۲</sup>

هریک از این الگوها، نواقص و کاستی‌هایی دارند. اما توجه جرم‌شناسان و متخصصان پیشگیری به یکی از این الگوها با عنوان پیشگیری اجتماعی<sup>۳</sup> و وضعی<sup>۴</sup> جلب شده تا حدی که درباره عناوین مجرمانه بسیار مهمی از جمله فساد<sup>۵</sup> و جنایات سازمان‌یافته فراملی<sup>۶</sup>، در

۱. برنار بولک، کیفرشناسی، ترجمه علی حسین نجفی ابرندآبادی، چاپ سوم با اضافات، انتشارات مجد، ۱۳۸۲، ص ۳۲.

۲. علی حسین نجفی ابرندآبادی، تقریرات درس جرم‌شناسی (پیشگیری)، تنظیم محمدعلی بابایی، دوره دکتری دانشگاه تربیت مدرس، نیم‌سال اول ۱۳۷۹-۱۳۸۰، ص ۷۴۸.

3. Social Prevention
4. Situational Prevention
5. Corruption
6. Transnational Organized Crime

اسناد بین‌المللی به این الگوها اشاره شده است.<sup>۱</sup>

بسیاری از دانشمندان حقوق کیفری در علت گرایش به این الگو معتقدند که جرم از سه عنصر قانونی، مادی و معنوی تشکیل شده است؛ یعنی تا زمانی که فعل یا ترک فعلی در مجموعه قوانین لازم‌الاجرای جزایی پیش‌بینی نشده باشد و یک انسان واجد شرایط مصرح در قانون با قصد مجرمانه خود<sup>۲</sup> مرتکب آن نشود، جرمی محقق نشده است. برخی دیگر از جرم‌شناسان معتقدند برای اینکه یک جرم براساس مبانی جرم‌شناختی، یعنی علت‌شناسی جرم، محقق شود، باید سه عنصر انگیزه،<sup>۳</sup> فرصت<sup>۴</sup> و ابزار<sup>۵</sup> با یکدیگر جمع شوند. انگیزه، با قصد مجرمانه متفاوت است و در واقع هدف ارتکاب آن را تشکیل می‌دهد. برای مثال، قصد قتل یک شکل بیشتر ندارد و آن آمادگی ذهنی و روانی مجرم، برای ارتکاب جرم است؛ اما انگیزه قتل می‌تواند بسیار متنوع باشد؛ مانند انتقام، کسب ثروت و ...<sup>۶</sup> بنابراین، اگر انگیزه مجرمانه‌ای در فرد ایجاد نشود؛ قصد مجرمانه نیز در او شکل نخواهد گرفت. به بیان دیگر، انگیزه بر قصد مقدم است و به این دلیل، چنانچه بتوان انگیزه‌های مجرمانه را خنثی کرد، جرمی ارتکاب نخواهد یافت. از این رو با توجه به اهمیت این عنصر، از انگیزه به‌عنوان قاعده مثلث جرم یاد می‌شود.

با این حال، بسیاری از افراد برای عملی ساختن انگیزه‌های مجرمانه و منحرفانه خود، مترصد دستیابی به دو عنصر دیگر، یعنی فرصت و ابزار مناسب نیز هستند و در صورت عدم یکی از این دو عنصر، امکان تحقق انگیزه وجود نخواهد داشت. در این میان، به تجربه

1. United Nations Office on Drugs and Crime, *the Global Program against Corruption, UN Anti-Corruption Toolkit*, Third Edition, Vienna, September 2004, P. 24.

2. Mens Rea

3. Actus Reus

4. Motive

5. Opportunity

6. Tool

7. Shinder, Debra Littlejohn, *Scene of the Cyber Crime, Computer Forensics Hand Book*, Syngress Publication, 2002, P. 353.

۸. بند «۳» ماده (۲۲) قانون مجازات اسلامی، مصوب ۱۳۷۰ تأکید دارد، احراز انگیزه در اصل مسئولیت کیفری بی‌تأثیر و تنها در تخفیف یا تشدید مجازات مؤثر است.

ثابت شده که جلوگیری از فرصت ارتکاب، نه فقط به مراتب نتیجه‌بخش‌تر از جمع‌آوری یا ممانعت از دستیابی به ابزار ارتکاب است؛ بلکه در بسیاری موارد، به دلیل ماهیت دوگانه ابزارها، نمی‌توان نسبت به آنها هیچ اقدامی انجام داد. برای مثال، به این دلیل که امکان ارتکاب قتل با چاقو وجود دارد، نمی‌توان تمام چاقوها را از سطح جامعه جمع‌آوری کرد و این کار نه عاقلانه بوده و نه با واقعیات منطبق است. از این رو برای پیشگیری از دستیابی به این دو عنصر، راهکارهای «آماج‌محور»<sup>۱</sup> یا «بزه‌دیدة‌محور»<sup>۲</sup> در دستور کار قرار می‌گیرد تا علاوه بر امکان‌پذیری و سهولت برنامه‌ریزی و اجرا، نتیجه بهتری نیز به دست آید.<sup>۳</sup> مجموعه اقدامات را «پیشگیری وضعی از جرائم» می‌گویند.<sup>۴</sup>

وظیفه رفع انگیزه‌های مجرمانه و منحرفانه به عهده کارکردهای پیشگیرانه‌ای است که از آنها به عنوان «پیشگیری اجتماعی» یاد می‌شود. به طور کلی، این کارکردها در دو شاخه «پیشگیری اجتماعی جامعه‌مدار» و «پیشگیری اجتماعی رشد‌مدار» قرار می‌گیرند.

#### ۱-۱ پیشگیری اجتماعی جامعه‌مدار

این تدابیر سعی در برطرف کردن زمینه‌های اجتماعی بروز انگیزه‌های مجرمانه و منحرفانه را دارند. با برنامه‌ریزی صحیح در حوزه اشتغال و از میان بردن نسبی فقر، می‌توان امیدوار بود که زمینه‌های بروز انگیزه‌های مالی یا حتی انتقام‌جویانه - که در اثر احساس فقیر بودن به افراد جامعه دست می‌دهد - تا حد زیادی برطرف شود و یا اینکه اگر افراد جامعه از مضرات و لطمات ناشی از اعتیاد به مواد مخدر یا روان‌گردان آگاهی یابند، از آلوده شدن به این مخدرات خودداری خواهند کرد و نه فقط از مجرم شدن خود جلوگیری می‌کنند؛ بلکه زمینه

1. Target-based

2. Victim-based

3. Ibid, P. 354.

۴. برای مطالعه مباحث مربوط به پیشگیری وضعی از جرائم با رویکرد پیشگیری وضعی از جرائم سایر و دیگر مباحث پیرامون آن، ر.ک. امیرحسین جلالی‌فراهانی، «پیشگیری وضعی از جرائم سایر در پرتو موازین حقوق بشر»، فصلنامه تخصصی فقه و حقوق، شماره ۶، ۱۳۸۴.

بروز انگیزه‌های مجرمانه بسیار وحشتناک‌تر بعدی - که در اثر اعتیاد به این مواد در آنها به وجود می‌آید - از جمله سرقت، قتل و یا به فحشا کشاندن نزدیکان نیز از میان می‌رود.<sup>۱</sup> با نگاهی اجمالی درمی‌یابیم که در راستای تحقق اهداف پیش‌بینی شده برای تدابیر پیشگیرانه اجتماعی جامعه‌مدار، باید به مؤلفه‌ها و ابعاد بسیار متنوعی توجه کرد و این در حالی است که تحقق هریک از این اهداف چندان نمی‌تواند انتظارات متخصصین پیشگیری را برآورده سازد. زیرا اجرای هریک از آنها به یک یا چند ارگان از نهاد گسترده دولت مربوط می‌شود و هماهنگی میان آنها در راه رسیدن به این مقصود، خود سیاست‌گذاری کلان و بلندمدتی می‌طلبد. از این رو برای اینکه از مزایای این رهیافت (حتی به میزان کم) محروم نمانیم؛ متخصصان با ارائه الگوهای محدودتر و مشخص‌تر کوشیده‌اند که گروه‌های اجتماعی خاص را هدف قرار دهند. چنین عملی باعث می‌شود که بتوان از اقدامات انجام شده در مقاطع مختلف ارزیابی به عمل آورد و با توجه به نتایج به دست آمده، جرح و تعدیل‌هایی را در صورت نیاز برای بازدهی حداکثر خط‌مشی‌های اعمال شده انجام داد.

یکی از مهم‌ترین اقداماتی که به نظر می‌رسد زمان انجام آن به قبل از مطرح شدن الگوی پیشگیری اجتماعی باز می‌گردد؛ تدوین کدهای رفتاری<sup>۲</sup> برای مشاغل مختلف است، به خصوص آنهایی که حساسیت ویژه‌ای را برمی‌انگیزند.<sup>۳</sup> منظور از کد رفتاری، مجموعه قواعد وضع شده برای دست‌اندرکاران یک حوزه خاص است تا آنها با ماهیت کار خود و همچنین عواقب نقض شرایط حاکم بر آن آشنا شوند. این گزینه به حدی اهمیت دارد که نه فقط در قوانین و مقررات ملی، بلکه در اسناد ارشادی و الزام‌آور مختلف بین‌المللی نیز برای برخی مشاغل و حوزه‌های حساس، از کشورها خواسته شده تا کدهای لازم‌الاجرای را در قالب قانون یا مقررات دولتی وضع کرده و به اجرا درآورند. برای مثال

۱. علی حسین نجفی ابرندآبادی، *تقریرات درس جرم‌شناسی (پیشگیری)*، ص ۱۲۶۱.

2. Codes of Conduct

3. United Nations Office on Drugs and Crime, *the Global Program Against Corruption, UN Anti-Corruption Toolkit Third Edition*, Vienna, September 2004, P. 212.

می‌توان از پیش‌نویس سند بنگلور درباره اصول بین‌المللی رفتار قضایی<sup>۱</sup> - که مقامات قضایی آسیا و آفریقا در فوریه ۲۰۰۱ آن را تنظیم کرده و به تصویب رساندند - نام برد.<sup>۲</sup> به این ترتیب، انتظار می‌رود متصدیان این حوزه‌های حساس - که برای آنها کد رفتاری تدوین شده - با آگاهی بیشتر و دقیق‌تر از ماهیت حرفه‌ای که به آن اشتغال دارند، زمینه‌های مجرمیت یا انحراف و همچنین بزه‌دیدگی خود را شناسایی و از آنها پرهیز کنند. البته این مجموعه دستورالعمل‌های رفتاری فقط به ابعاد منفی قضیه نمی‌پردازند؛ بلکه برای تقویت حس وظیفه‌شناسی و همچنین عوامل خودکنترلی خنثی‌کننده انگیزه‌های مجرمانه و منحرفانه، به‌ویژه منفعت‌طلبی و انتقام، مؤلفه‌های تشویقی و حمایتی ویژه‌ای نیز در نظر گرفته می‌شود.

## ۲-۱ پیشگیری اجتماعی رشدمدار

تدابیر پیشگیرانه اجتماعی رشدمدار دومین اقدام مهم برای خنثی‌سازی عوامل اجتماعی جرم‌زا و انحراف‌زا است. منظور از پیشگیری رشدمدار، مجموعه اقداماتی است که در دوران رشد و تکامل شخصیتی و جسمی کودکانی به اجرا درمی‌آید<sup>۳</sup> که در معرض

1. Bangalore Draft: International Principles for Judicial Conduct.

2. Ibid, P. 219

۳. براساس بیشتر اسناد معتبر بین‌المللی که در قوانین داخلی کشورها نیز انعکاس گسترده‌ای یافته، منظور از کودک (Child)، تمام اشخاص زیر ۱۸ سال تمام هستند و باید آنها را از صغار (Minor) تمیز داد. درباره مقابله با زمینه‌های مجرمانه فضای سایر درباره کودکان، تاکنون اقدامات گسترده‌ای در عرصه‌های مختلف بین‌المللی انجام شده که از جمله مهم‌ترین آنها می‌توان به این موارد اشاره کرد: ۱. کنفرانس پکن در سال ۱۹۹۹ که با هدف مبارزه با استفاده از اینترنت برای استثمار کودکان برگزار شد، ۲. کنفرانس بین‌المللی وین در سپتامبر ۱۹۹۹ با هدف مبارزه با هرزه‌نگاری اطفال در اینترنت برگزار شد، ۳. اجلاس یونسکو در سال ۱۹۹۹ در پاریس به منظور بررسی معضلات سوءاستفاده جنسی از کودکان، هرزه‌نگاری کودکان و کودک‌دوستی در اینترنت برگزار شد، ۴. کنوانسیون جرائم سایبر تأکید خاصی بر این موضوع داشته است، به‌نحوی که تنها جرم علیه محتوای (Content Related Crime) مورد اشاره هرزه‌نگاری کودکان است (ماده ۹). جهت مطالعه مطالب مربوط به این اسناد، ر.ک. بیژن حسینی، جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، سال تحصیلی ۱۳۸۱-۱۳۸۲، ص ۴۸. همچنین حسن عالی‌پور، جرائم مرتبط با محتوای سیاه فناوری اطلاعات، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴، ص ۲۲۰.

ارتکاب این اعمال قرار دارند. زندگی در جامعه و تماس اجتناب‌ناپذیر با افراد گوناگون، آشنایی با انواع جرائم و انحرافات را ناگزیر می‌سازد. از این رو همه کودکان در معرض ارتکاب جرم قرار دارند.<sup>۱</sup>

با توجه به اینکه پیشگیری رشدمدار، برخلاف پیشگیری جامعه‌مدار با قشر جوان و نوجوان سروکار دارد؛ خط‌مشی‌ها و اقدامات آن، رویکردی تربیتی و آموزشی داشته و در این نوع پیشگیری قدرت شناخت و تمیز آنها تقویت می‌شود و مهارت‌های زندگی اجتماعی را می‌آموزند تا بتوانند به هنگام مواجهه با معضلات، به‌ویژه طیف گسترده جرائم و انحرافات، واکنش‌های منطقی و صحیح از خود بروز دهند. آنها می‌آموزند که چگونه خشونت خود را مهار کنند؛ انگیزه‌های مالی‌شان را فروشانند و به بهانه تفریح و سرگرمی، برای دیگران دردسر ایجاد نکنند. تمام اینها الفبای یک زندگی متمدن و هنجارمند است که گروه‌های کم‌سال باید فراگیرند. البته کودکان در معرض خطر به توجه بیشتری نیازمند هستند.

## ۲ پیشگیری اجتماعی از جرائم و انحرافات سایبری

پس از آشنایی اجمالی با ماهیت و کارکرد پیشگیری اجتماعی از جرائم و انحرافات، در این فصل، نحوه اعمال آن بر جرائم و انحرافات سایبری بررسی می‌شود. برای تدوین و اجرای کارآمد و مؤثر این راهکارها، باید مطالعات مقدماتی فراگیر و عمیقی انجام داد. از جمله مهم‌ترین این مطالعات، شناسایی هویت و خصوصیات بزهکاران و منحرفان سایبری براساس انگیزه‌هایشان و همچنین، شناسایی هویت و خصوصیات بزه‌دیدگان سایبری و تعیین میزان خطرپذیری آنها برای سمت‌وسو دهی نوع و میزان آموزش‌های پیشگیرانه است. سپس با توجه به نتایج به‌دست آمده، می‌توان راهکارهای قابل اجرا و مؤثری را پیشنهاد داد.

۱. امیرحسین نیازپور، «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، مجله حقوقی دادگستری، سال ۶۷، شماره ۴۵، دوره جدید، زمستان ۱۳۸۲، ص ۱۳۸.

۲-۱ ویژگی‌های بزهکاران و بزه‌دیدگان سایبری از دیدگاه پیشگیری اجتماعی  
انگیزه‌های منحرفانه و مجرمانه شایع سایبری را می‌توان در چهار گروه اصلی ذیل بررسی کرد:<sup>۱</sup>

#### ۲-۱-۱ سرگرمی و تفریح

بیشتر هکرهای<sup>۲</sup> جوان در این گروه قرار می‌گیرند. البته در این باره تقسیمات دقیق‌تری نیز ارائه شده است. برای مثال، گروهی از آنها فقط به دلیل اینکه از یادگیری نحوه کارکرد سیستم‌ها از راه آزمون و خطا لذت می‌برند؛ هک یا نفوذ غیرمجاز<sup>۳</sup> می‌کنند. گروهی دیگر، به دلیل کنجکاوی و کشف موضوعات جدید به این عمل مرتکب می‌شوند و برخی دیگر نیز این گونه اقدامات را یک نوع بازی تلقی می‌کنند. برای مثال، درهم شکستن تداویر امنیتی یک شبکه می‌تواند هدف، و نابودسازی آن شبکه پیروزی باشد. با توجه به اینکه این اقدام هکرها مادر جرائم و انحرافات سایبری به‌شمار می‌آید؛ تقریباً بروز هر انگیزه‌ای در آنها ممکن است. از این رو به دلیل اهمیت بسیار این موارد در مطالعات جرم‌شناختی، در شاخه‌های تخصصی‌تر، مانند خرده‌فرهنگ‌های مجرمانه<sup>۴</sup> نیز مطالعه می‌شوند.

#### ۲-۱-۲ کسب منافع مالی

سوءاستفاده‌های رایانه‌ای با انگیزه مالی آغاز شده و<sup>۵</sup> با پیدایش فضای سایبر، این انگیزه قوت بیشتری یافته است؛ زیرا علاوه بر امکان انواع سوءاستفاده‌ها از داده‌های واجد ارزش مالی، مانند سرقت شماره کارت‌های اعتباری، میزان نتیجه‌بخش بودن جرائم مالی در دنیای فیزیکی نیز به نحو قابل توجهی افزایش یافته است. یک کلاهبردار که در دنیای فیزیکی فقط می‌توانست قشر بسیار محدودی از افراد جامعه را تحت تأثیر قرار داده و تعداد کمی را

1. Shinder, Debra Littlejohn, *Scene of the Cyber Crime, Computer Forensics Hand Book*, Syngress Publication, 2002, P. 129.

2. Hackers

3. Unauthorized Intrusion

4. Criminal Subcultures

۵. محمدحسن دزیانی، «شروع جرائم کامپیوتری-سایبری»، *خبرنامه انفورماتیک*، شماره ۹۳، ۱۳۸۴، ص ۴.



از میان آنها بفریید، در فضای سایبر با میلیون‌ها مخاطب مواجه بوده که به دلیل شرایط خاص حاکم بر این فضا، احتمال فریفتن این افراد بسیار بیشتر است.

#### ۲-۱-۳ انتقام، اعتقادات یا گرایش‌های مختلف

این انگیزه در طیف خاصی از افراد به وجود می‌آید. برای مثال، کارمندی که به ناحق از محل کارش اخراج شده، سعی می‌کند با نفوذ به شبکه شرکت و تخریب یا سرقت اطلاعات واجد ارزش، انتقام بگیرد و یا اینکه تروریست‌ها با هدف وارد آوردن خسارات اساسی به دولت، یا گروه مورد نظر خود، انواع تهاجمات سایبری را علیه آنها تدارک می‌بینند.<sup>۱</sup>

#### ۲-۱-۴ انگیزه‌های جنسی

فضای سایبر بر این گونه مسائل، تأثیر جدی گذاشته است. از مهم‌ترین گروه‌های فعال جنسی سایبری می‌توان به ناشران انواع اطلاعات الکترونیکی مکتوب، صوتی، تصویری، ویدئویی در قالب‌های مختلف و به صورت زنده یا غیر زنده، کودکان دوستان،<sup>۲</sup> آزارگران و آزاربینان جنسی<sup>۳</sup> و انواع متجاوزان به عنف، اشاره کرد.<sup>۴</sup> همچنین با شناسایی بزهدیدگان سایبری و نوع خطراتی که آنها را تهدید می‌کند، می‌توان در سمت و سو دهی و شدت و ضعف تمهیدات پیشگیرانه، تصمیمات صحیح‌تری اتخاذ کرد. برای مثال، چنانچه متصدیان شبکه‌ها و سیستم‌های رایانه‌ای حوزه‌های حساس مختلف احتمال دهند که از سوی بزهدکاران در معرض ترفندهای مهندسی اجتماعی<sup>۵</sup> و مهندسی اجتماعی معکوس<sup>۶</sup> قرار می‌گیرند؛ در نحوه تعامل خود با افراد درون و

۱. امیرحسین جلالی‌فراهانی، «تروریسم سایبری»، فصلنامه تخصصی فقه و حقوق، شماره ۱۰، پاییز ۱۳۸۵، ص ۹۸.

۲. Pedophiles

۳. Sadomasochistic Sex

۴. حسن عالی‌پور، «جرائم مرتبط با محتوای سیاه فناوری اطلاعات»، مجموعه مقالات همایش بررسی ابعاد حقوقی

فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴، ص ۲۲۴.

۵. Social Engineering

۶. Reverse Social Engineering

برون‌سازمانی احتیاط بیشتری خواهند کرد.<sup>۱</sup> همچنین با توجه به اینکه هم‌اکنون گروه بزرگی از کاربران شبکه‌ای را قشر جوان و نوجوان جامعه تشکیل می‌دهند، ضروری است تدابیر پیشگیرانه اجتماعی رشدمدار با توجه به انواع خطرات سایبری طراحی و اجرا شود. برآیند این اقدامات آگاهی‌بخش، چه برای بزه‌کاران و چه برای بزه‌دیدگان بالقوه، انگیزه‌های مجرمانه و منحرفانه را کاهش خواهد داد. با رشد آگاهی بزه‌دیدگان، بزه‌کاران بالقوه درمی‌یابند که هزینه جرمشان بالا رفته و دیگر ارتکاب آن مقرون‌به‌صرفه نیست که این خود سالب انگیزه مؤثری به شمار می‌آید.<sup>۲</sup>

پیشگیری اجتماعی از جرائم و انحرافات سایبری از اهمیت مضاعف و ویژه دیگری نیز برخوردار است. به‌طور کلی، دانشمندان حقوق کیفری جرائم را به دو گروه جرائم فطری یا طبیعی<sup>۳</sup> و جرائم قراردادی<sup>۴</sup> تقسیم کرده‌اند. جرائم فطری به اعمالی گفته می‌شود که وجدان بشری کلیت آنها را پذیرفته و به این دلیل هرکس در هر گوشه جهان، با هر گرایش مذهبی، قومیتی، نژادی و ... آنها را مذموم می‌شمرد؛ مانند قتل، سرقت و تجاوز به عنف.

اما جرائم قراردادی که نوع و تعداد آنها به مراتب از جرائم فطری بیشتر است؛ زاینده ذهن قانون‌گذاران جوامع بوده و در اثر پیدایش ابزارهای جدید به وجود می‌آیند.<sup>۵</sup> برای مثال، قوانین و مقررات راهنمایی و رانندگی که در اثر پیدایش انواع وسایل نقلیه موتوری وضع شده است. همچنین، پیدایش فناوری رایانه و به تبع آن فضای سایبر، قانون‌گذاران کشورها را به تصویب قوانین و مقررات مختلف برای حوزه‌های گوناگون واداشته است. از این رو با توجه

1. Casey, Eoghan, *Digital Evidence and Computer Crime*, Academic Press, 2001, P. 172.

۲. موضوعات مربوط به هزینه جرم از سوی دانشمندان، نظریه‌پردازی شده که دیدگاه‌های اقتصادی داشتند و از پیشگامان آنها می‌توان به ژرمی بنتام اشاره کرد که مبدع نظریه فایده‌گرایی واکنش اجتماعی بود. ر.ک. علی حسین نجفی ابرندآبادی و حمید هاشم‌بیگی، همان، ص ۳۱.

3. Natural Crimes

4. Contractual or Conventional Crimes

۵. اولین دانشمندی که این طبقه‌بندی را انجام داد، گاروفالو، قاضی ایتالیایی به سال ۱۸۸۵ بود. ر.ک. علی حسین نجفی ابرندآبادی و حمید هاشم‌بیگی، همان، ص ۱۷۴.

به اینکه اکثر افراد جامعه نمی‌توانند سوءاستفاده‌های احتمالی از این ابزارها را با مراجعه به فطرت خود شناسایی کنند؛ متولیان این حوزه‌ها موظفند درباره آموزش و رشد آگاهی افراد نسبت به اقدامات غیرقانونی و نامشروع، به‌ویژه جرائمی که ضمانت اجرای کیفری دارند، تمهیدات پیشگیرانه اجتماعی وسیع‌تر و جدی‌تری را در دستور کار خود قرار دهند.

## ۲-۲ پیشگیری اجتماعی جامعه‌مدار سایبری

اشاره شد که این اقدامات در دو حوزه عام و خاص قابل اجراست. در اینجا درباره پیشگیری جامعه‌مدار خاص با محوریت کدهای رفتاری مباحثی مطرح می‌شود.

به‌طور کلی، با کدهای رفتاری می‌توان گروه‌های خاصی را - که وظیفه‌ای به آنها سپرده شده - در برابر اعمالشان پاسخ‌گو دانست. از جمله این گروه‌ها، گروه مشاغل هستند که در حوزه‌های مختلف به فعالیت می‌پردازند و از آنجا که به متصدیان شبکه‌ای خود، داده‌های واجد ارزشی واگذار می‌کنند تا با رعایت سه اصل محرمانگی<sup>۱</sup>، تمامیت<sup>۲</sup> و دسترس‌پذیری<sup>۳</sup> آنها را به کار گیرند، ضروری است متناسب با حرفه، نوع و میزان اطلاعات و دیگر شرایط، کد رفتاری لازم‌الاجرای مربوط را برای آنها تدوین کنند. گفتنی است، در این باره تاکنون برای بعضی مشاغل و موضوعات حساس، از سوی مراجع مهم و معتبر بین‌المللی، کدهای رفتاری نمونه‌ای منتشر شده است. برای مثال، امروزه برای فعالان عرصه تجارت الکترونیکی و بازاریابی شبکه‌ای<sup>۴</sup> کدهای رفتاری متحدالشکلی تدوین شده تا از وقوع جرائم و تخلفات مربوط به پیام‌های تجاری ناخواسته الکترونیکی (اسپم)<sup>۵</sup> جلوگیری شود.<sup>۶</sup>

گروه دیگری که کدهای رفتاری برای آنها از جمله ضروریات شغلی است؛

1. Confidentiality
2. Integrity
3. Availability
4. Network Marketing
5. Spam

۶. مرکز پژوهش‌های مجلس شورای اسلامی، «اسپم: جلوه سیاه تبلیغات در سیستم‌های پیام‌رسان الکترونیکی»، شماره

ارائه‌دهندگان خدمات شبکه‌های اطلاع‌رسانی رایانه‌ای هستند. آنها پل ارتباطی میان دنیای فیزیکی با فضای سایبر محسوب می‌شوند و نسبت به بقیه دست‌اندرکاران این حوزه، هم دارای ابتکار عمل متنوع‌تر و گسترده‌تری بوده و هم مسئولیت‌های خطیری برعهده دارند. این افراد به راحتی می‌توانند امکان نفوذ به سایت‌ها را فراهم کنند یا اطلاعات حساس و کلیدی سایت‌ها را در اختیار افراد ناصالح قرار دهند. به دلیل وجود چنین اوضاعی، بر نحوه عملکرد ارائه‌دهندگان خدمات شبکه‌ای، بیشتر نظارت می‌شود که از جمله مهم‌ترین این نظارت‌ها عبارت است از اقدامات انجام شده برای نظارت بر حفظ حریم آن‌لاین افراد از سوی ارائه‌دهندگان این خدمات.<sup>۱</sup> آنها به راحتی می‌توانند علاوه بر امکان‌پذیر ساختن شنود و ردیابی ارتباطات الکترونیک، دسترسی به پایگاه‌های داده‌ای — که ورود افراد غیرمجاز به آنها ممنوع است — یا اطلاعات شخصی<sup>۲</sup> و شخصی حساسی را میسر سازند<sup>۳</sup> که خودشان برای پیشبرد فعالیت‌های شبکه‌ای جمع‌آوری کرده‌اند.<sup>۴</sup>

### ۲-۳ پیشگیری اجتماعی رشمدهار سایبری

علاوه بر نسل جوان و نوجوان جامعه ما، تمام جوامع توانسته‌اند با فضای سایبر تعامل بهتری داشته باشند. نسل گذشته امور خود را در دنیای فیزیکی انجام می‌دادند و اکنون نیز لزومی نمی‌بینند که با فضای جدید انس بگیرند. حال آنکه نسل امروز با این فضا بزرگ شده و از همان ابتدا هر آنچه پیرامون خود مشاهده کرده‌اند رنگ و بوی سایبری داشته است.

این وضعیت، بیم و امیدهایی را نیز به همراه دارد. از یک سو، می‌توان امیدوار بود که

۱. از جمله مهم‌ترین اسنادی که تاکنون در این حوزه به تصویب رسیده، دستورالعمل پارلمان و شورای اروپا درباره پردازش داده‌های شخصی و حمایت از حریم ارتباطات الکترونیکی (2002/58/EC) است.

2. Personal Information

3. Sensitive Personal Information

۴. برای مطالعه مسئولیت‌های کیفری احتمالی ارائه‌دهندگان خدمات ر.ک. به: مهدی فضلی، بررسی مسئولیت کیفری ارائه‌دهندگان خدمات اینترنتی، پایان‌نامه دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه تهران، پردیس قم،

نسل جدید در برپایی هرچه سریع‌تر یک جامعه اطلاعاتی<sup>۱</sup> تمام‌عیار، مبتنی بر اصول و قواعد حاکم بر این فضا همت گمارد و از سوی دیگر، باید آنها را از خطرات و آسیب‌های فراوان این فضا آگاه کرد تا با گرفتار شدن در آنها، نتیجه مغایر حاصل نشود.

این امر مهم به عهده متولیان عرصه‌های مختلف فضای سایبر است تا با همکاری متخصصان پیشگیری اجتماعی، بر پایه اصول و ضوابط پیشگیری رشدمدار، از بزهکاری و بزه‌دیدگی جوانان و نوجوانان پرنشاط و پرانرژی در این فضای ناشناخته جلوگیری کنند. در ادامه راهکارهای قابل اجرا درباره کودکان که متولیان تربیتی و آموزشی را هدف قرار می‌دهند، به اجمال بررسی می‌شوند:

### ۱-۳-۲ اقدامات مداخله‌آمیز والدین

اولین محیطی که توجه متصدیان پیشگیری رشدمدار را به خود جلب می‌کند؛ خانواده و به تبع آن والدین است. چنانچه بتوان در ابتدای امر توصیه‌ها و آموزش‌های لازم را به والدین منتقل و آنها را با خطرات و همچنین مزایا و مطلوبیت‌های فضای سایبر آشنا کرد، می‌توان تا حدود زیادی به ثمربخشی اهداف این تدابیر امیدوار بود. برای مثال، برنامه آموزشی والدینی که فرزندان‌شان با اینترنت کار می‌کنند، می‌تواند حاوی این نکات باشد: ایجاد حس مسئولیت‌پذیری و توانایی انتخاب گزینه‌های سالم به هنگام استفاده از اینترنت (به بیان دیگر، نحوه استفاده صحیح از اینترنت)، تصمیم‌گیری به‌جا و مناسب درباره محتوایی که قرار است مشاهده کنند و آموزش نحوه رویارویی با محتوای نامناسبی که ممکن است مشاهده کنند و کاهش عواقب آن. درحقیقت ابتدا باید به والدین چگونگی اتخاذ این رهیافت‌ها را نسبت به کودکان‌شان آموزش داد.<sup>۲</sup>

1. Information Society

گفتنی است ما برای برپایی این جامعه الزام قانونی نیز داریم برای مثال، ماده (۴۴) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی کشور مصوب ۱۳۸۳ چنین مقرر کرده است: «دولت موظف است به منظور استقرار جامعه اطلاعاتی و تضمین دسترسی گسترده، امن و ارزان شهروندان به اطلاعات مورد نیاز، اقدام‌های ذیل را به عمل آورد: ...».

2. Thornburgh, Dick & S. Lin Herbert, Editors, *Youth, Pornography and the Internet*, National Academy Press, 2004, P. 218.

## ۲-۳-۲ تدابیر همیاری همسالان

علاوه بر والدین، مربیان و دیگر مسئولین آموزشی و تربیتی فرزندان، از دیگر عوامل مهمی که می‌توانند در شکل‌گیری شخصیت کودکان در استفاده از فضای سایبر نقش مهمی ایفا کنند؛ فرزندان یا اطرافیان بزرگ‌تر از آنها هستند. البته سپردن چنین مسئولیتی به آنها، برای خودشان نیز مفید خواهد بود؛ زیرا برای حفظ وجهه خود در برابر کوچک‌ترها، سعی می‌کنند مرتکب اقدامات ناشایست نشوند. چرا که به‌خوبی می‌دانند کوچک‌ترها رفتارهایشان را تعقیب کرده و منتظر تقلید از آنها هستند.

به تجربه ثابت شده که به‌کارگیری این اشخاص در کنترل بزه و دیگر انحرافات اجتماعی کودکان، از جمله مصرف مواد مخدر، فرار از مدرسه و ... موفق بوده است. از این رو به نظر نمی‌رسد در هدایت صحیح فعالیت‌های آن‌لاین کوچک‌ترها نتیجه مغایر حادث شود. درحقیقت این افراد که می‌توانند دانش آموزان، همسایگان یا بهتر از همه خواهر و برادرهای بزرگ‌تر باشند؛ علاوه بر اینکه به کوچک‌ترها نحوه استفاده صحیح از اینترنت را می‌آموزند، مراقب اشتباهات آنان نیز خواهند بود و چنانچه آموزش ببینند، می‌توانند با تذکرات صحیح، از ارتکاب مجدد آنها جلوگیری کنند.<sup>۱</sup>

۲-۳-۳ تدابیر کاربری صحیح<sup>۲</sup>

این خط‌مشی‌ها، مجموعه‌ای از راهکارها و انتظارات مربوط به نحوه فعالیت آن‌لاین افراد هستند که به نحو روزافزونی در منازل، مدارس و کتابخانه‌ها به‌کار می‌روند. مبانی نظری آنها مسئولیت‌پذیر کردن کودکان است در برابر محتوایی که ایجاد می‌کنند و رفتاری که بروز می‌دهند. کودکان یاد می‌گیرند در برابر مسائل مختلفی که ممکن است در فضای سایبر تجربه کنند؛ گزینش‌های شایسته‌ای داشته باشند و به‌این ترتیب، با مهارت‌های استفاده صحیح از اینترنت آشنا می‌شوند. البته برای مؤثر واقع شدن این خط‌مشی‌ها، باید در موارد

---

1. Ibid, P. 234

2. Acceptable Use Policies

نقض عمدی، واکنش یا ضمانت اجراهای متناسب اعمال کرد؛ مانند محرومیت از اینترنت، تماس با والدین، حبس دانش آموز (در مواردی که نقض به مدرسه مربوط می شود) و حبس در منزل (اگر موارد نقض به منزل مربوط است) اما باید از موارد نقض غیرعمدی و تصادفی نیز به عنوان فرصتی برای آموزش کاربران درباره نحوه اجتناب آنها از مواجهه با این گونه مسائل در آینده، نحوه برجیدن آنها از روی صفحه نمایش و در صورت لزوم، گزارش به ارائه دهندگان خدمات اینترنتی، بهره برداری کرد.<sup>۱</sup>

#### ۲-۳-۴ تدابیر کاهنده آثار سوء<sup>۲</sup>

یکی از نکات غیرقابل انکار این است که تمام اقداماتی که درباره عدم مواجهه کودکان با مسائل صریح جنسی به اجرا درمی آیند؛ صددرصد نتیجه بخش نیستند و بالاخره این امکان وجود دارد که کودکان به گونه های مختلف با این موضوعات مواجه شوند. از این رو اگر رویارویی با این محتوای ناشایست اجتناب ناپذیر است؛ باید با اتخاذ اقداماتی آثار نامطلوب مواجهه با این موارد را به حداقل رساند.<sup>۳</sup> آموزش به کودک می تواند به عنوان یک راهبرد مناسب به کار گرفته شود تا در صورت مواجهه با این گونه مسائل، آنها را گزارش کند و کمک بخواهد و والدین یا مربیان نباید کودکی را که در اثر مواجهه با این مسائل از آنها کمک طلبیده، مجازات کنند. برخوردهای نابه جا باعث می شود که کودکان در مواجهه با چنین صحنه هایی، از واکنش بزرگ ترهایشان بیشتر بیم داشته باشند. واکنش بیش از حد نه فقط اثر مثبت ندارد؛ بلکه می تواند آثار معکوس و عواقب ناهنجاری به دنبال داشته باشد. کودکان باید بتوانند چنین مسائلی را در فضایی آرام و آزاد و نه با اضطراب تنبیه و مجازات، مطرح کنند.

1. Board on Children, Youth and Families, Non Technical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet, Summary of a Workshop, National Academy Press, 2004, P. 62.
2. After the Fact Strategies
3. Thornburgh, Dick & S. Lin Herbert, Editors, *Youth, Pornography and the Internet*, National Academy Press, 2001, P. 240.

## ۲-۳-۵ تدابیر آموزشی

تدابیر آموزشی در دو شاخه ذیل مطرح می‌شوند:

الف) آموزش سلامت اینترنت<sup>۱</sup>

یکی از مقوله‌های اصلی در دنیای فیزیکی، بحث آموزش سلامت کودکان است. برای مثال، نحوه رد شدن از خیابان، برخورد با غریبه‌هایی که به آنها نزدیک می‌شوند و واکنش به آتش‌سوزی منزل را باید به آنها آموخت. هدف از آموزش کودکان این است که چنانچه به تنهایی با چنین اوضاعی مواجه شدند، چگونگی مقابله با آنها را بدانند.

آموزش سلامت کودکان در اینترنت هم، چنین هدفی را دنبال می‌کند. تحقیقات نشان داده که بسیاری از دانش‌آموزان با تجربه یاد گرفته‌اند چگونه در اینترنت از خود محافظت کنند. اما این فرایند آموزشی به کودکان یاد می‌دهد که برای عدم مواجهه با موقعیت‌های ناامن، چه کارهایی انجام دهند و چه کارهایی را انجام ندهند. همچنین، مهارت‌های تفکر و قضاوت به والدین، مربیان و دیگر اعضای جامعه - که می‌خواهند شیوه‌های مقابله با خطرات زندگی را به کودکان بیاموزند - آموزش داده می‌شود. در اینجا خطرات تبیین می‌شوند تا هنگامی که کودکان با آنها مواجه شدند؛ دچار سردرگمی نشوند.<sup>۲</sup>

ب) ادبیات اطلاعات و رسانه<sup>۳</sup>

ادبیات اطلاعات، مجموعه‌ای است از توانمندی‌ها که به افراد قدرت شناسایی اطلاعات مورد نیاز را می‌دهد تا بتوانند اطلاعات را به نحو مؤثر بازبایی و یافته‌ها را ارزیابی کنند و به شکل نقادانه‌ای منبع آن را جویا شوند؛ اطلاعات گزینش شده را در مجموعه دانش خود وارد کنند؛ برای تحقق یک هدف خاص از آنها استفاده مؤثری به عمل آورند؛ شرایط اقتصادی، حقوقی و اجتماعی حاکم بر استفاده از آنها را درک کنند و با رعایت موازین

1. Internet Safety Education

2. Ibid, P. 242

3. Information and Media Literacy



اخلاقی و قانونی به آنها دسترسی یابند و در نهایت مورد استفاده قرار دهند.<sup>۱</sup> ادبیات رسانه اصطلاح جدیدتری است که به دو شیوه بنیادین، مفهوم ادبیات اطلاعات را توسعه می‌دهد: اول اینکه مفهوم اطلاعات را به تمام اشکال رسانه‌ای و نه فقط چاپی تسری می‌دهد. هرچند که هیچ‌گاه ادبیات اطلاعات به نسخ چاپی محدود نبوده؛ اما در عمل آنچه ابتدا به ذهن متبادر می‌شود؛ نسخ چاپی است.

شیوه دوم که از گزینه اول نیز مهم‌تر است اینکه ادبیات رسانه توانایی تولید و برقراری ارتباط با دیگران را - که درحقیقت برای جلب منافع آنهاست - دربرمی‌گیرد. همچنین برخی تحلیل‌گران معتقدند آموزش رسانه بر اطلاعاتی متمرکز است که از طریق رسانه‌های ارتباط جمعی مانند روزنامه‌ها، برنامه‌های تلویزیونی و ... انتقال می‌یابند. برخی به این تعریف، میزان درک مخاطبان از محتوای رسانه را - که در تبیین مفهوم اطلاعات دریافتی به دست آورده‌اند - اضافه می‌کنند.

براساس نتایج تحقیق انجام شده، بیشتر مربیان و مسئولین کتابخانه‌ها بر نیاز به ادبیات رسانه و اطلاعات تأکید کرده‌اند. به عقیده آنان، نوجوانان، یعنی دانش‌آموزان، هیچ نظری درباره اطلاعات دریافتی از اینترنت ندارند. از این رو برای آنها باید دوره‌های آموزشی مهارت‌افزایی مربوط به ادبیات اطلاعات و رسانه را برگزار کرد.

### ۲-۳-۶ تدابیر الزام‌آور کاربری اینترنت

گروهی از دبیران برای آموزش استفاده صحیح از اینترنت به کودکان در قالب یک عمل الزام‌آور، برای هر مبحث درسی، فهرستی را از سایت‌های مجاز و مناسب تهیه کرده و در مهلت تقریبی متناسب از دانش‌آموزان می‌خواهند که به تمام این سایت‌ها مراجعه و مطالب درسی مربوط را مطالعه و استخراج کنند. به این ترتیب، دانش‌آموزان فرصتی برای پرداختن به محتوای ناسالم نخواهند داشت.

1. Board on Children, Youth and Families, Ibid, P. 50.

تعمیم این راهبرد، مستلزم تهیه محتوای اینترنتی سالم و آموزنده برای کودکان است. به این ترتیب دانش آموز فرصت مازادی ندارد تا خود را به محتوای ناسالم مشغول کند. این رویکرد را می‌توان برای آموزش مسائل حساس به کار برد. برای مثال، نهادینه کردن آموزش سلامت جنسی. این روش باعث می‌شود که کودکان کنجکاو به دنبال اطلاعات ناسالم و گمراه‌کننده نباشند.

نشریات الکترونیکی فعال در برنامه‌های آموزشی کودکان یا حتی مقاطع بالاتر می‌توانند نقش سازنده‌ای ایفا کنند. این نشریات می‌توانند فهرست جامعی از سایت‌های آموزشی را در قالب برنامه‌های آموزنده در اختیار مخاطبان قرار دهند تا علاوه بر برخورداری از جذابیت‌های آموزشی بیشتر، این راهبرد جنبه عمومی‌تری یابد.

#### ۲-۳-۷ تدابیر رسانه‌ای

بدیهی است بسیاری از والدین و مربیان، درباره ضرورت سلامت اینترنت یا ماهیت و میزان خطرات آن اطلاعات زیادی ندارند، از این رو یا با این قضیه خوش‌بینانه برخورد می‌کنند و برای حفاظت از فرزندانشان در برابر اینترنت هیچ اقدامی انجام نمی‌دهند یا اینکه با مبالغه‌آمیز خواندن خطرات، معتقدند هرزه‌نگاری و مرتکبان جنسی در اینترنت، به اندازه برنامه‌های تجاری شبکه‌های تلویزیونی ماهواره‌ای، گسترده‌اند.

گفتنی است برنامه‌های رسانه عمومی نمی‌توانند از این موضوعات پیچیده آموزش جامعی ارائه دهند. این برنامه‌ها برای انعکاس پیام‌های به نسبت ساده مناسبند. برای مثال، در ایالات متحده آمریکا در اواخر دهه ۱۹۸۰، یک برنامه تبلیغاتی گسترده با هدف آگاه‌سازی عمومی اعلام می‌داشت: «ساعت ده شب است، آیا می‌دانید فرزندتان کجاست؟». به این ترتیب، یک برنامه مشابه درباره سلامت اینترنت می‌تواند پیام‌هایی این‌چنینی منعکس کند: «فعالیت‌های آن‌لاین امروز فرزندتان چه بوده است؟»؛ یا «شما هم می‌توانید یاد بگیرید چگونه از فرزندتان در اینترنت محافظت کنید.»؛ یا برای ترغیب مردم به قرار دادن

کامپیوترها در قسمت عمومی منزل این پیام مفید است: «آیا به خودتان اجازه می‌دهید یک غریبه در اتاق خواب فرزندتان باشد؟»<sup>۱</sup>

### ۳ محدودیت‌های پیشگیری اجتماعی از جرائم و انحرافات سایبری

پس از آشنایی با انواع راهکارهای پیشگیرانه اجتماعی جامعه‌مدار و رشدمدار سایبری، در ادامه محدودیت‌های حاکم بر اجرای موفق آنها بررسی می‌شود. بی‌تردید، بررسی این محدودیت‌ها می‌تواند در اتخاذ تصمیمات واقع‌گرایانه و منطقی بسیار راهگشا باشد. برای درک بهتر، این محدودیت‌ها در سه گفتار مجزا بیان شده‌اند.

#### ۳-۱ محدودیت‌های ناشی از ماهیت تدابیر پیشگیرانه اجتماعی

یکی از نکات بسیار مهم درباره تدابیر پیشگیرانه اجتماعی این است که از نظر ماهیت زیربنایی و اساسی آن نمی‌توان انتظار داشت که همانند تدابیر پیشگیرانه وضعی یا ضمانت اجراهای کیفی و غیرکیفی، در کوتاه‌مدت نتایج محسوس و قابل مشاهده‌ای به دست آید. البته این مسئله هیچ‌گاه از دیدگاه جرم‌شناسان و متخصصان پیشگیری، یک نقطه ضعف محسوب نمی‌شود؛ زیرا این تدابیر، زیربنای فکری و شخصیتی بزهکاران و بزه‌دیدگان بالقوه را هدف قرار می‌دهند که در صورت توفیق، با رعایت هنجارها و ارزش‌های پذیرفته شده، جامعه‌ای سالم و متعهد به وجود خواهد آمد.

با وجود این، بیشتر مسئولان اجرایی، چنین دیدگاهی ندارند. آنها می‌خواهند در کوتاه‌مدت آثار مقابله با جرائم را مشاهده کنند و آن را در بیلان کاری‌شان به ثبت برسانند. بنابراین حاضرند برای انواع تدابیر پیشگیرانه وضعی و ضمانت اجراهای کیفی و غیرکیفی هزینه‌های بیشتری متحمل شوند؛ اما در کوتاه‌مدت نتایج مقطعی به دست آورند. از این رو چندان به سیاست‌های پیشگیرانه اجتماعی بها نداده و درباره میزان درصد افرادی

1. Thornburgh, Dick & S. Lin Herbert, Editors, Ibid, P. 255.

که انگیزه مجرمانه‌شان از بین رفته و به‌طور ارادی از ارتکاب جرائم خودداری کرده‌اند، آماری تهیه نمی‌شود. اما درباره نتیجه‌بخش بودن تدابیر پیشگیرانه وضعی یا ضمانت اجراهای کیفی و غیرکیفی که به کاهش ارتکاب جرائم و انحرافات در جامعه می‌انجامد؛ به کرات آمارهایی منتشر شده که بدیهی است ذهن افراد نیز به سمت آنها معطوف می‌شود.<sup>۱</sup>

گفتنی است تدوین یک راهبرد پیشگیرانه اجتماعی نتیجه‌بخش و کارآمد که بتواند تمام مخاطبان خود را در تمام محیط‌های اجتماعی عمومی و شخصی دربرگیرد، مستلزم هزینه هنگفت و به خدمت گرفتن نیروهای برنامه‌ریز و اجرایی بسیاری است. متولیان و مسئولان آموزشی و تربیتی به این موضوع واقفند که هر اندازه تدابیر اجتماعی صحیح‌تر و مناسب‌تر باشد می‌تواند آثار مطلوب جاودانه و همیشگی بر جای گذارد و همچنین تدوین یک برنامه اجتماعی نامناسب و ناقص یا به خدمت گرفتن نیروهای فاقد تخصص و تجربه، می‌تواند عواقب سوء عمیق و پایداری به دنبال داشته باشد. از این رو با توجه به این مسایل چندان رغبتی به سرمایه‌گذاری در این حوزه دیده نمی‌شود؛ زیرا تصور بر این است که یا باید به‌طور جدی وارد آن شد و سرمایه‌گذاری مالی و انسانی کلان و بلندمدتی انجام داد، یا اینکه بهتر است خود را درگیر آن نکرد تا عواقب سوء تربیت و آموزش ناقص و نادرست کودکان و نوجوانان بر جامعه تحمیل نشود.

## ۲-۳ محدودیت‌های ناشی از فضای سایبر

گفتیم که وظیفه اصلی تدابیر پیشگیرانه اجتماعی از میان بردن انگیزه مجرمانه در درون افراد است. اما این تدابیر زمانی مفید خواهند بود که اوضاع حاکم بر جامعه مناسب باشد. به بیان دیگر، نمی‌توان درحالی که بسترهای تقویت‌کننده انگیزه‌های مجرمانه هنوز در

۱. علی حسین نجفی ابرندآبادی، *تقریرات درس جرم‌شناسی (پیشگیری)*، تنظیم مهدی سیدزاده، مجتمع آموزش عالی قم، دوره کارشناسی ارشد، نیم‌سال دوم ۱۳۸۲-۱۳۸۱، ص ۱۲۸۵.

محیط‌های مختلف جامعه وجود دارد؛ انتظار داشت این تدابیر بتوانند از طریق آموزش و تربیت افراد زمینه‌های انگیزشی مجرمانه را برطرف کنند.

یکی از مهم‌ترین ویژگی‌های فضای سایبر، امکان‌پذیر بودن انجام تمام فعالیت‌های رایانه‌ای و به‌ویژه شبکه‌ای در خلوت<sup>۱</sup> است. خلوت از آن جهت برای تدابیر پیشگیرانه اجتماعی مانع ایجاد می‌کند که باعث می‌شود شخص بدون مشاهده کسی یا حتی بهتر از آن، بی‌آنکه کسی اجازه تعرض به حریمش را داشته باشد؛ براساس میلش عمل کند. بدیهی است وظیفه یا رسالت اصلی تدابیر اجتماعی، نهادینه کردن عدم توجه به انگیزه‌های مجرمانه و منحرفانه درونی است؛ اما نباید از یاد برد که محیط نیز بر غلیان یا فروکش کردن این انگیزه‌ها تأثیر قابل توجهی دارد. در دنیای فیزیکی، بسیاری از افراد حتی در جایی که تدابیر پیشگیرانه وضعی وجود ندارند که فرصت و ابزار ارتکاب جرم را از آنان سلب کنند، به دلیل اینکه در یک محیط بیگانه به سر می‌برند و انواع احتمالات از ذهنشان عبور می‌کند، انگیزه‌های درونی‌شان کمتر بیدار می‌شود. درحالی‌که در فضای سایبر این امکان وجود دارد که در خصوصی‌ترین و ایمن‌ترین مکان، شدیدترین ناهنجاری‌ها ارتکاب یابد. درحقیقت اگر کسی بتواند در این فضای بی‌کران در میان انواع فرصت‌های مغتنم مجرمانه و منحرفانه انگیزه‌هایش را سرکوب کند و لغزشی از او سر نزد، یکی از نمونه‌های بارز خودساخته سرکوب‌کننده هوای نفس خواهد بود.<sup>۲</sup>

این ویژگی یعنی امکان ارتکاب در حریم امن در کنار ناشناس نگه داشتن هویت واقعی، باعث شده بسیاری از افراد در فضای سایبر نسبت به دنیای فیزیکی، چهره یا شخصیت متفاوتی از خود بروز دهند. این افراد به دلایل بسیار در دنیای خارج هیچ‌گاه تمایلات منحرفانه و مجرمانه‌شان را بروز نمی‌دهند و نزد همگان به‌عنوان یک چهره معتبر و واجد احترام شناخته می‌شوند. اما زمانی که در خلوت پای رایانه‌شان می‌نشینند و به فضای

1. Privacy

معادل دقیق این اصطلاح، حریم خصوصی است. ولی در اینجا با توجه به تناسب مطلب، مشابه آن آمده است.

2. Thornburgh, Dick & S. Lin Herbert, Editors, Ibid, P. 257.

سایبر وارد می‌شوند، انواع تمایلات ناهنجارشان بیدار می‌شود. بسیار مشاهده شده که شخصی مربی برجسته یک مدرسه بوده و در تمام مدت زندگی‌اش هیچ خطایی انجام نداده؛ اما در فضای سایبر دارای شخصیت متفاوتی است و به گمان خود با پنهان کردن شخصیت واقعی‌اش، تمایلات آزارگری یا آزاربینی جنسی‌اش را بروز داده و تا آنجا پیش رفته که قربانی این اعمال شده است.<sup>۱</sup>

بنابراین فقط به تدابیر پیشگیرانه اجتماعی نباید بسنده کرد بلکه باید کوشید حداقل کودکان (به‌عنوان شاخص‌ترین گروه در معرض خطر) نتوانند در خلوت با فضای سایبر ارتباط برقرار کنند. از این‌روست که به والدین توصیه می‌شود سیستم‌های رایانه‌ای منازل را در اماکن عمومی قرار دهند؛ زیرا تعداد بسیار اندکی از افراد، آن‌هم در سنین نوجوانی و جوانی، با وجود کسب فرصت در حریم خود، می‌توانند انگیزه‌های مجرمانه و منحرفه‌شان را فرونشاند و سرکوب کنند. بنابراین متولیان تدابیر اجتماعی به اولیا و مربیان توصیه می‌کنند به‌همراه اجرای اقدامات بیان شده، به این واقعیات نیز توجه داشته باشند.

معضل دیگری که فضای سایبر - به‌طور خاص - برای تدابیر پیشگیرانه اجتماعی به‌وجود آورده؛ ایجاد یک دنیای دیگر با شرایط و مقتضیات مخصوص به خود است. پدیدآوردگان فضای سایبر از همان ابتدا معتقد بودند که این فضا ماهیت مجازی<sup>۲</sup> دارد و در واقع آن را در برابر دنیای فیزیکی - که از آن به‌عنوان دنیای واقعی<sup>۳</sup> نام می‌برند - قرار می‌دهند. این امر باعث شده که کاربران با تلقی مجازی بودن فضای سایبر سعی در اجرای رؤیاهای خود در این فضا داشته باشند. در حالی که یکی از قابلیت‌های این فضا مجازی‌سازی<sup>۴</sup> است و نباید آن را با مجازی بودن اشتباه گرفت.

1. Casey, Eoghan, "Digital Evidence and Computer Crime", Academic Press, 2001, P. 136.

این مسایل تا حدی جدی تلقی شده که برای آشنایی دقیق‌تر با ویژگی‌های روانی کاربران فضای سایبر، به‌ویژه بزهکاران و بزه‌دیدگان سایبری، متخصصان برای بعضی شاخه‌های علوم، مطالعات بنیادین جدیدی را تعریف کرده‌اند که از جمله آنها می‌توان به روان‌شناسی فضای سایبر و روان‌شناسی جنایی سایبری اشاره کرد.

2. Virtual

3. Real

4. Virtualization

بیشتر کاربران شبکه‌ای از فضای سایبر این تصور را در ذهن دارند که فقط یکسری تصاویر و اعداد و ارقام در صفحه نمایشگر قابل رؤیتند، غافل از اینکه تمام افعال سایبری در زندگی فیزیکی آنان اثر و بازتاب مستقیم و واقعی دارند. البته این معضل تا حدود زیادی قابل حل است. حتی شاید بتوان امیدوار بود حل آن تا حدودی بتواند معضل قبلی را نیز برطرف کند؛ زیرا اگر افراد بدانند حتی در حریمشان نیز چشمان بیدار بسیاری مراقبشان است و سوابق فعالیت‌هایشان در موقعیت‌های متعددی به ثبت می‌رسد و از همه مهم‌تر این اعمال بر زندگی‌شان در دنیای فیزیکی، آثار مستقیم و غیرمستقیم بسیاری بر جای می‌گذارد؛ با احتیاط بیشتری عمل خواهند کرد.

معضل دیگر فضای سایبر برای تدابیر پیشگیرانه اجتماعی به ماهیت بین‌المللی یا به بیان بهتر فرامرزی این فضا مربوط می‌شود. گفتیم که تدابیر پیشگیرانه اجتماعی براساس هنجارها و ارزش‌های پذیرفته شده‌ای وضع می‌شوند که افراد حاضر در یک اجتماع مشخص - که معمولاً به مرزهای یک کشور محدود می‌شود - آنها را می‌شناسند و به آنها باور دارند. اما با ظهور فضای سایبر به تدریج باورهای اجتماعی مردم نیز دچار تحول شده است. امروزه برای شناخت آداب و رسوم و فرهنگ مردم سایر نقاط جهان، لازم نیست به آنجا سفر کنیم و به دلیل حضور موقتی در آنجا از آداب و رسوم آن مرز و بوم هیچ تأثیری نپذیریم؛ بلکه در هر زمان از شبانه‌روز می‌توانیم با مراجعه به فضای سایبر و با هزینه‌ای بسیار ناچیز، صدها هزار مطلب و تصویر از هنجارها و ارزش‌های مورد قبول دیگر کشورها را دریافت کنیم.

در جامعه ما به آنچه اعمال منافی عفت نامیده می‌شوند توجه ویژه‌ای شده و به همین دلیل در مجموعه قوانین جزایی مان نیز گستره و تنوع بیشتری لحاظ شده است. حتی برخی از این اعمال مستوجب سنگین‌ترین کیفرها هستند. این در حالی است که در بسیاری از کشورها بسیاری از این اعمال نه تنها جزئی از فرهنگ عامه به‌شمار می‌آیند، بلکه از سوی دولت‌ها نیز قانونمند شده‌اند. بنابراین هنگامی که کاربر ایرانی در جامعه مشترک سایبری با این چنین فرهنگ‌های رایجی مواجه می‌شود، ممکن است ابتدا با یک تعارض مواجه شود،

ولی پس از مدتی به عنوان یک واقعیت موجود می پذیرد. لذا آنچه که در دنیای خارج یک فعل ناهنجار یا حتی مجرمانه به شمار می آید، در فضای سایبر هنجارمند شده است. به هر حال، این معضل نیز یکی از واقعیات اجتناب ناپذیر فضای سایبر است که باید آن را پذیرفت و در جوامعی مانند جامعه ما منتظر چالش های جدی تری نیز بود. از این رو ضروری است با اتخاذ تدابیر پیشگیرانه اجتماعی، به ویژه از نوع رشدمدار و بالا بردن آگاهی کاربران جوان نسبت به این مسائل، میزان لطمات را به حداقل رساند.

### ۳-۳ محدودیت های ناشی از شکاف نسلی

امروزه استفاده از سیستم های رایانه ای همانند گذشته در انحصار قشر خاصی نیست و به دلیل فراگیری آن و امکانات بی شماری که فضای سایبر برای کاربری هر چه آسان تر آن فراهم آورده گروه های جوان و نوجوان، بیشتر از دیگران جلب شده اند. این در حالی است که تدوین کنندگان تدابیر پیشگیرانه اجتماعی با فضای سایبر رابطه عمیقی ندارند یا نمی توانند به اندازه جوانان و نوجوانان به فعالیت های شبکه ای بپردازند. این شکاف دیجیتال<sup>۱</sup> میان متولیان پیشگیری و بزهداران و بزهدیدگان باید برطرف شود؛ زیرا در این صورت، نمی توان به تأثیر گذار بودن آنها امیدوار بود. چرا که درک متقابل وجود ندارد.

### نتیجه گیری

در این مقاله راهکارهای جرم شناختی رشدمدار و جامعه مدار پیشگیری اجتماعی از ناهنجاری های مجرمانه و منحرفانه سایبری و میزان کارایی و نتیجه بخش بودن آنها ارائه شد و با توجه به محدودیت های حاکم، محرز شد که راه دشواری پیش رو است. اما آثار مثبت و سازنده آن، به مراتب از تمهیدات پیشگیرانه وضعی و ضمانت اجراهای کیفری و غیر کیفری، ماندگارتر و امیدوار کننده تر است. با یقین به این موضوع، اجرای مراحل ذیل

1. Digital Gap



مناسب به نظر می آید:

۱. ابتدا باید با توجه به شرایط اجتماعی و فرهنگی جامعه، شناخت صحیح و واقع‌گرایانه‌ای از کاربران فضای سایبر در حوزه‌های مختلف به وجود آید. هرچه حوزه‌ها و شاخه‌هایی که باید تحت شمول این گونه ضوابط هنجارمند به‌طور مشخص از یکدیگر تفکیک شوند، مجموع اقدامات پیشگیرانه موفق‌تر خواهند بود.

۲. سپس باید هنجارهای مربوط، با هدف اصلی بهره‌برداری مشروع و سودمند از این فضا و دوری جستن از هرگونه جرم، انحراف و حتی رفتارهای غیراخلاقی، وضع شوند.

۳. با توجه به راهکارهای دو حوزه جامعه‌مدار و رشد‌مدار — که به تفکیک تبیین شدند — باید کوشید این هنجارها به نحو مطلوب و مؤثر در میان اجتماعات خاص مخاطبان حوزه‌های مختلف تبیین و تشریح شوند.

۴. به هنگام تدوین این هنجارها نباید از راهکارهای پیشگیرانه وضعی و همچنین ضمانت‌اجراهای کیفری و غیرکیفری غافل شد؛ زیرا درحقیقت باید این تدابیر در آن هنجارها منعکس شوند و به اجرای صحیح آنها کمک کنند؛ زیرا اجرای مؤثر، متناسب و بازدارنده آنها به انعکاس صحیحشان در تدابیر پیشگیرانه اجتماعی وابسته است.

بهتر است به‌همراه حرکت پرشتاب و تا حدودی لگام‌گسیخته سایبری کردن امور خرد و کلان جامعه، به‌ویژه دسترس‌پذیر کردن هرچه بیشتر این فضا برای قشر جوان و نوجوان در محیط‌های مختلف — که نمونه بارز آن را در عزم دولت برای متصل کردن تمامی واحدهای آموزش عالی و مدارس به شبکه جهانی اینترنت شاهد هستیم — قدری به فکر ساماندهی این فضا براساس الگوهای خردگرایانه و واقع‌گرایانه باشیم تا بیش از این نسل جدید با چالش‌ها و مشکلات سایبری مواجه نباشند.

## منابع و مأخذ

بولک، برنار. کیفرشناسی، ترجمه علی حسین نجفی ابرندآبادی، چاپ سوم با اضافات، انتشارات مجد، ۱۳۸۲.

پاکزاد، بتول. «اقدامات سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرائم رایانه‌ای»، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴.

جلالی فراهانی، امیرحسین. «پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، فصلنامه تخصصی فقه و حقوق، شماره ۶، ۱۳۸۴.

جلالی فراهانی، امیرحسین. «تروویسم سایبری»، فصلنامه تخصصی فقه و حقوق، شماره ۱۰، ۱۳۸۵.

جینا، دی آنجلیز. جرائم سایبر، ترجمه سعید حافظی و عبدالصمد خرم آبادی، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳.

حسینی، بیژن. جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، سال تحصیلی ۱۳۸۲-۱۳۸۱.

خرم آبادی، عبدالصمد. «سابقه پیدایش، تعریف و طبقه‌بندی جرائم رایانه‌ای»، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴.

دزیانی، محمدحسن. جزوه آموزشی حقوق سایبر و جرائم سایبری، جلد اول، ۱۳۸۴ الف.

دزیانی، محمدحسن. «شروع جرائم کامپیوتری-سایبری»، خبرنامه انفورماتیک، شماره ۹۳، ۱۳۸۴ ب.

عالی‌پور، حسن. «جرائم مرتبط با محتوای سیاه فناوری اطلاعات»، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل، ۱۳۸۴.

فضلی، مهدی. بررسی مسؤلیت کیفری ارائه‌دهندگان خدمات اینترنتی، پایان‌نامه دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه تهران، پردیس قم، مهرماه ۱۳۸۴.

مرکز پژوهش‌های مجلس شورای اسلامی، «اسپم: جلوه سیاه تبلیغات در سیستم‌های پیام‌رسان

الکترونیکی»، شماره ۸۴۵۱، تیرماه ۱۳۸۶.

میرمحمدصادقی، حسین. *تقریرات درس حقوق جزای عمومی*، تنظیم امیرحسین جلالی فراهانی، دانشگاه امام صادق (ع)، نیم سال دوم ۱۳۸۰-۱۳۸۱.

نجفی ابرندآبادی، علی حسین. *تقریرات درس جرم‌شناسی*، دوره کارشناسی، دانشگاه امام صادق (ع)، نیم سال تحصیلی ۸۲-۱۳۸۱.

نجفی ابرندآبادی، علی حسین. *تقریرات درس جرم‌شناسی (پیشگیری)*، تنظیم مهدی سیدزاده، مجتمع آموزش عالی قم، دوره کارشناسی ارشد، نیم سال دوم ۱۳۸۱-۱۳۸۲.

نجفی ابرندآبادی، علی حسین. *تقریرات درس جرم‌شناسی (انحراف)*، تنظیم علی مراد حیدری، دوره دکتری حقوق کیفری و جرم‌شناسی، مجتمع آموزش عالی قم، نیم سال ۸۳-۱۳۸۲.

نجفی ابرندآبادی، علی حسین. *تقریرات درس جرم‌شناسی*، تنظیم محمدعلی بابایی، دوره دکتری دانشگاه تربیت مدرس، نیم سال نخست ۸۰-۱۳۷۹.

نجفی ابرندآبادی علی حسین و حمید هاشم‌بیگی. *دانشنامه جرم‌شناسی*، انتشارات دانشگاه شهید بهشتی، ۱۳۷۷.

نیازپور، امیرحسین. «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، *مجله حقوقی دادگستری*، سال ۶۷، شماره ۴۵، دوره جدید، زمستان ۱۳۸۲.

Board on Children, Youth and Families, *Non Technical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet, Summary of a Workshop*, National Academy Press, 2004.

Casey, Eoghan, "Digital Evidence and Computer Crime", Academic Press, 2001.

Shinder, Debra Littlejohn, *Scene of the Cyber Crime, Computer Forensics Hand Book*, Syngress Publication, 2002.

Thornburgh, Dick & S. Lin Herbert, Editors, *Youth, Pornography and the Internet*, National Academy Press, 2004.

United Nations Office on Drugs and Crime, *the Global Program against Corruption; UN Anti-Corruption Toolkit*, Third Edition, Vienna, September 2004.