# پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر

**امیرحسین جلالی فراهانی***



## چکیده

*گرچه فضای سایبر ـ این پدیدهٔ شگفت‌انگیز قرن بیست و یکم ـ بسیاری از عرصه‌ها را با تحولات بنیادین مواجه کرده، سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است. اما با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است. در این میان، پیشگیری وضعی یکی از اقدامات مهم محسوب می‌شود، اما با محدودیتهایی مواجه است که از جملهٔ آنها نقض موازین حقوق بشر است. ماهیت فضای سایبر به گونه‌ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است. اما تدابیر پیشگیرانهٔ وضعی از جرائم سایبر، عمدتاً به گونه‌ای اجرا می‌شوند که این سه اصل حقوق بشری را نقض می‌کنند. این مقاله درصدد است ضمن تبیین انواع تدابیر پیشگیری وضعی از جرائم سایبر، به تبیین چالشهای حاکم بر این تدابیر با موازین حقوق بشر بپردازد.*

**واژگان کلیدی:** *جرائم سایبر، پیشگیری از جرم، پیشگیری وضعی، آزادی بیان، جریان آزاد اطلاعات، حریم خصوصی، حقوق بشر.*

## مقدمه

بشر در طول حیات خود با دوره‌های گوناگونی از تحول و تکامل مواجه بوده است. زمانی کشاورزی محوریت داشت، اما بشر پس از مدتی به این نتیجه رسید که با تحقق یک جامعهٔ

* پژوهشگر و کارشناس ارشد حقوق جزا و جرم‌شناسی.

صنعتی می‌تواند به آرزوهای خود دست یابد. لذا تمام همّ خـود را در ایـن راه نهـاد و دورانـی صنعتی را رقم زد که اوج آن را در سدهٔ نوزدهم میلادی شاهد هستیم.

اما از اواخر این قرن و اوایل قرن بیستم، زمزمه‌های محوریت یافتن عنـصر دیگـری شـنیده شد. این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بـود، بـه تدریج با پا گذاشتن به سدهٔ بیستم موقعیت خود را تثبیت کرد و تا آنجا پیش رفت که به دوران صنعتی پایان داد و بشر را وارد عصر پساصنعتی یا پسامدرن کرد. (شـورای عـالی انفورماتیـک، شمارهٔ ۵۲: ۷۲)



آری، این عنصر با ارزش اطلاعات نام دارد وحدود یک قرن است که بشر تـلاش خـود را صرف تجلی آن در تمامی عرصه‌های سیاسـی، اقتـصادی، اجتمـاعی و فرهنگـی کـرده اسـت. بی‌تردید هر کاری ابزاری می‌خواهد و ابزار تحقق یک جامعهٔ بـه واقـع اطلاعـاتی (Information Society)، فناوری اطلاعات و ارتباطات (Information and Communication Technology) اسـت. دلیـل اشاره به عامل ارتباطات در کنار اطلاعـات، بـه لحـاظ جایگـاه ویـژهٔ آن در توسـعه و تکامـل اطلاعات است. ارتباط و به تبع آن ابزارهای ارتباطی، از همان ابتدا از عناصر حیـاتی محـسوب می‌شدند و می‌توان گفت اگر وجود نداشتند، بشر هیچ‌گاه نمی‌توانست به ایـن حـد از رشـد و بالندگی برسد.

دو فناوری در عرصهٔ فناوری اطلاعات و ارتباطات نقش تعیین‌کننده‌ای به عهده داشته‌اند که عبارت‌انـد از: رایانـه (Computer) و مخـابرات (Telecommunication). هـدف از اختـراع رایانـه، تسریع و تسهیل پردازش اطلاعات بود که به خوبی به ثمر نشست و مخـابرات نیـز بـه عنـوان مهم‌ترین ابزار ارتباطی، در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است.

از حدود نیم‌قرن اخیر، به تدریج با کشف قابلیتهای شگرف ناشی از تلفیق این دو فنـاوری، انقلابی در عرصهٔ فناوری اطلاعات و ارتباطات رقم خـورد. اوج ایـن انقـلاب را مـی‌تـوان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دههٔ نود مـیلادی بـه بعـد، تحـولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها که خود از بسیاری سیستمهای رایانه‌ای متـصل به یکدیگر تشکیل شده‌اند، به مدد فناوریهای پیشرفتهٔ مخابراتی با یکدیگر ارتباط برقـرار کـرده و فضایی با ویژگیهای کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند که عده‌ای آن را فـضای

مجازی (Virtual Space) نامیده‌اند و عده‌ای هم عنوان فـضای سـایبر (Cyber Space) را بـرای آن برگزیده‌اند.*

اما ناگفته پیداست که فضای سایبر همانند دیگر عناصـر زنـدگی اجتمـاعی، از گزنـد یـک پدیدهٔ بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده اسـت. بـه طـور کلـی، آنچه امروز تحت عنوان جرم سایبر (Cyber Crime) قرار مـی‌گیـرد، دو طیـف از جـرائم اسـت: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سـایبر بـدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهـد، ارتکابـشان را تـسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیـه امنیـت ملـی و حتـی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه امـوال و اشـخاص را در برمـی‌گیرنـد. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترس غیرمجاز به داده‌ها یا سیستمها یا پخش برنامه‌هـای مخـرب نظیر ویروسها، جز در فضای سایبر قابلیت ارتکاب ندارنـد و بـه همـین دلیـل بـه آنهـا جـرائم سایبری محض (Pure Cyber Crime) نیز گفته می‌شود. (Casey, 2001: 8)

همان‌گونه که ملاحظه می‌شود، به لحاظ امکان سوء استفادهٔ دوجانبه‌ای که از فـضای سـایبر وجود دارد، ضروری است برای آن چاره‌ای اندیشه شود. با توجه بـه رویکـرد کلـی مقابلـه بـا جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارت‌اند از: اقدامات کیفری و غیرکیفری. در زمینهٔ اقدامات کیفری سعی مـی‌شـود از طریق جرم‌انگاری هنجارشکنیها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفـری گذشته، ارعاب‌انگیزی مؤثری دربارهٔ مجرمان بالقوه یا مکرر صورت گیرد تا به ایـن ترتیـب، از ارتکاب جرم بازداشته شوند. (نیازپور، ۱۳۸۲: ۱۲٤) اما رویکرد دوم که در بـستر جـرم‌شناسـی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسـی و .... پدیـد آمـده،

* اصطلاح فضای سایبر، برای اولین بار در سال ۱۹۸۲ در یک داستان علمی ـ تخیلی بـه کـار رفـت و در سـال ۱۹۹۰ پروفسور جان پری بارلو به هنگام صحبت در یک کنفرانس آنلاین، از آن استفاده کرد و آن را بر سر زبانها انداخت. (دی‌آنجلیز، ۱۳۸۳: ۷)

اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. در این زمینه، تاکنون الگوهای مختلفی در عرصهٔ جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. از مهم‌ترین و مؤثرترین این الگوها می‌توان به پیشگیری اجتماعی (Social Prevention) و پیشگیری وضعی (Situational Prevention) از جرائم اشاره کرد. به طور خلاصه، در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آنها، به ویژه قشر جوان و نوجوان جامعه، و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد. اما در پیشگیری وضعی، هدف سلب فرصت و ابزار ارتکاب جرم از مجرم با انگیزه است. (نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸) راجع به این مدل که موضوع این تحقیق نیز است، در جای خود بیشتر بحث خواهد شد.

با اینکه اتخاذ تدابیر پیشگیرانه نسبت به اقدامات کیفری از محاسن بسیاری برخوردار است، نباید از یاد برد که در اینجا نیز باید اصول و هنجارها را رعایت کرد. سیاستهای پیشگیری، به ویژه پیشگیری وضعی، برخلاف سیاستهای کیفری، تمامی افراد جامعه را دربرمی‌گیرند، زیرا پر واضح است که شناسایی مجرمان بالقوه امکان‌پذیر نیست. لذا این اقدامات باید به نحوی اجرا شوند که افراد جامعه از حقوق اساسی‌شان محروم نگردند. (نجفی ابرندآبادی، ۱۳۸۳: ۵۵۹)

آنچه در این مقاله مورد بررسی قرار می‌گیرد، تدابیر پیشگیری وضعی از جرائم سایبر و چالش آنها با رعایت موازین حقوق بشر است. این موضوع از آن جهت مورد توجه قرار گرفته که دو نکتهٔ اساسی را می‌توان راجع به فضای سایبر برشمرد: ۱. این فضا با امکاناتی که در اختیار مجرمان قرار می‌دهد، از یک سو ارتکاب جرائم را سهل‌تر می‌سازد و نسبت به دنیای فیزیکی خسارات بسیار بیشتری را وارد می‌کند و از سوی دیگر، به لحاظ فرامرزی بودن آن و امکان ارتکاب جرم بدون نیاز به حضور فیزیکی مجرمان، تعقیب و پیگرد و در نهایت دستگیری آنها با مشکلات بسیاری همراه شده است. به این ترتیب، پیشگیری از وقوع این جرائم بسیار باصرفه‌تر و کم‌هزینه‌تر از طی فرایند رسیدگی کیفری آنها و تحمل خسارات بی‌شمار است. ۲. همچنین نباید از خاطر دور داشت که هدف اصلی از ایجاد فضای سایبر،

نزدیک شدن به آرمانهای جامعهٔ اطلاعاتی است. لذا مبارزه با سوء استفاده‌های این فضا، به هر شکل که باشد، نباید در تحقق این هدف خدشه‌ای ایجاد کند.*

بنابراین، آنچه در اینجا واجد اهمیت است اینکه میان این دو دغدغهٔ بزرگ گونه‌ای تعادل حقوقی واقع‌گرایانه و منصفانه برقرار شود که این خود نیازمند تجزیه و تحلیل مسائل گوناگونی است که سعی می‌شود در حد این مقاله به آنها پرداخته شود.

برای نیل به این مقصود لازم است ابتدا به مفهوم پیشگیری وضعی (الف) و ماهیت جرائم سایبر (ب) اشاره‌ای شود. سپس از انواع اقدامات و تدابیر پیشگیری وضعی از چنین جرائمی (ج) بحث به میان آید و در نهایت ضمن بررسی انعکاس موازین حقوق بشر در فضای سایبر (د)، به تبیین چالشهای پیشگیری وضعی از جرائم سایبر با موازین حقوق بشر (هـ) پرداخته شود.



## الف. مفهوم پیشگیری وضعی

همان‌گونه که در مقدمه اشاره شد، کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب یک جرم، سه عامل باید جمع شوند. مهم‌ترین آنها که قاعدهٔ مثلث جرم را هم تشکیل می‌دهد، انگیزهٔ مجرمانه (Motive) است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه (Intention) می‌شود. برای از بین بردن این عامل، ضروری است تدابیر پیشگیرانهٔ اجتماعی اتخاذ گردد. اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت (Opportunity) و ابزار ارتکاب جرم (Means) جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد. زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند. هرچند در عین حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرائم نادیده گرفت.** به هر حال، آنچه در پیشگیری

---

* اتحادیهٔ مخابرات بین‌الملل (ITU) در سال ۲۰۰۳ با برگزاری اجلاس جهانی جامعهٔ اطلاعات (WSIS) در ژنو که قرار است به صورت دوسالانه برگزار شود و امسال نیز در تونس برگزار می‌شود، پیش‌نویس اعلامیه‌ای تحت عنوان «اعلامیهٔ اصول» (Declaration of Principles) را به تصویب نمایندگان ملتها رسانده که به موجب آن همگی بر تحقق آرمانهای بزرگ جامعهٔ اطلاعاتی در سراسر جهان تأکید کرده‌اند.

** هم اکنون در کشور ما نرم‌افزارهای آموزشی دسترس غیرمجاز (هک، Hacking) که از آن به عنوان مادر جرائم سایبر یاد می‌کنند، به آسانی توزیع می‌شود و حتی کلاسهای آموزشی آن نیز بدون هیچ محدودیتی برگزار می‌گردد، بی‌آنکه مراجع قانونی کوچک‌ترین تعرضی به آنها نمایند.

وضعی از جرائم اولویت دارد، حفظ آماجها (Targets) و بزه‌دیدگان از تعرض مجرمان است. (صفاری، ۱۳۸۰: ۲۹۲)

در این زمینه، شیوه‌های مختلفی از سوی جرم‌شناسان ارائه شده که از مهم‌ترین آنها می‌توان به شیوه‌های دوازده‌گانهٔ کلارک، جرم‌شناس انگلیسی، اشاره کرد که آنها را در سه گروه چهارتایی قرار داده است (ابراهیمی، ۱۳۸۳: ۱۸):

۱. دشوار ساختن ارتکاب جرم از طریق: الف. حفاظت از آماجها و قربانیان جرم؛ ب.کنترل و ایجاد محدودیت در دسترس به موقعیتهای جرم‌زا؛ ج. منحرف کردن مجرمان؛ و د. برچیدن ابزار ارتکاب جرم.

۲. افزایش خطرپذیری مجرمان از طریق: الف. مراقبت از ورودیها و خروجیها؛ ب. مراقبت رسمی؛ ج. مراقبت غیررسمی؛ و د. مراقبت طبیعی.

۳. کاهش جاذبه از آماجها و قربانیان جرم از طریق: الف. حذف آماجهای جرم؛ ب.علامت‌گذاری اموال؛ ج. تقلیل فرصتهای وسوسه‌انگیز؛ و د. وضع قواعد خاص.

بدیهی است بحث راجع به هر یک از این شیوه‌ها خود مجال دیگری می‌طلبد و در اینجا فقط برای آشنایی با این حوزه و همچنین تطبیق آنها با شیوه‌هایی که نسبت به جرائم سایبر به اجرا درمی‌آیند، به آنها اشاره شد.

## ب. ماهیت جرائم سایبر

همان گونه که در مقدمه اشاره شد، فضای سایبر از تلفیق فناوریهای رایانه و مخابرات به وجود آمده است. شورای اروپا در یکی از جزوات آموزشی خود، مفهوم فضای سایبر را ترکیبی از رایانه، مودم (Modem) و ابزار مخابراتی دانسته که از قابلیت شبیه‌سازی (Simulation) و مجازی‌سازی (Virtualization) برخوردار باشد. اما نکتهٔ قابل توجه در اینجا این است: هنگامی که پیشینهٔ جرائم سایبر بررسی می‌گردد، ملاحظه می‌شود بیشتر بر روی جرائم مرتبط با رایانه (Computer- Related Crime) بحث شده است. (United Nations; 1992)

جرائم رایانه‌ای ـ سایبری را در قالب سه نسل مورد بررسی قرار می‌دهند که در اینجا به

فراخور هر یک با رویکرد پیشگیری مطالبی عنوان می‌شود*. پیش از هر چیز باید خاطرنشان کرد که طبقه‌بندی این جرائم در قالب سه نسل، بر اساس نسلهای تکاملی سیستمهای رایانه‌ای نبوده و معیارهای دیگری مدنظر قرار گرفته است (انزالی، ۱۳۷٤: ۳۷)

**۱. نسل اول جرائم رایانه‌ای:** همان گونه که از عنوان پیداست، این نسل به ابتدای ظهور سیستمهای رایانه‌ای، به ویژه زمانی که برای اولین بار در سطح گسترده‌ای در دسترس عموم قرار گرفتند، مربوط می‌شود. اولین سیستم رایانه‌ای به مفهوم امروزی ENIAC نام داشت که سوئیچ آن در فوریهٔ ۱۹٤٦ چرخانیده شد. اما حدود سه دهه طول کشید که امکان تولید انبوه این سیستمها در قالب سیستمهای شخصی (Personal Computer) و رومیزی (Desktop) فراهم گشت و تعداد بیشتری از مردم توانستند آنها را بخرند و در امور مختلف از آنها استفاده کنند. بدیهی است سوء استفاده از این سیستمها از این زمان مورد توجه قرار گرفت و تلاشهایی جهت مقابله با آنها به عمل آمد.

گفتنی است سوء استفاده‌هایی که در این دوره از سیستمهای رایانه‌ای می‌شد، از لحاظ نوع و حجم خسارات محدود بود که آن هم از قابلیت محدود این سیستمها نشأت می‌گرفت. در آن زمان، عمدهٔ اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستمها و به تبع آن دستکاری داده‌ها مربوط می‌شد. لذا تدابیری که جهت مقابله با آنها اتخاذ می‌گردید، بیشتر رویکردی امنیتی داشت. به عنوان مثال، برای حفظ امنیت پردازشگرهای داده‌های الکترونیکی (EDP) هفت مؤلفه تعیین شده بود که عبارت بودند از: ۱. امنیت اداری و سازمانی؛ ۲. امنیت پرسنلی؛ ۳. امنیت فیزیکی؛ ٤. امنیت مخابرات الکترونیکی؛ ۵. امنیت سخت‌افزاری و نرم‌افزاری؛ ٦. امنیت عملیاتی؛ و ۷. برنامه‌ریزی احتیاطی. (دزیانی، ۱۳۷٦: ۷٤)

چنین رویکردی را می‌توان در قوانین کیفری راجع به جرائم رایانه‌ای نیز مشاهده کرد. به عنوان مثال، فهرست سازمان توسعه و همکاری اقتصادی که در سال ۱۹۸٦ راجع به جرائم

* شایان ذکر است رویکرد تقسیم‌بندی این جرائم به سه نسل در میان دانشمندان اروپایی شایع است و در میان دانشمندان امریکایی، این جرائم از همان ابتدا بر اساس نقشی که سیستمهای رایانه‌ای یا به طور کلی فضای سایبر در آنها به عهده داشته‌اند، تقسیم می‌شوند. به عنوان مثال، در گزارش گروه کاری ریاست جمهوری ایالات متحده راجع به اقدامات غیرقانونی در اینترنت که در مارس ۲۰۰۰ منتشر شد، جرائم این حوزه در سه گروه بررسی شده‌اند: ۱. رایانه‌ها به عنوان اهداف جرم؛ ۲. رایانه‌ها به عنوان دستگاههای ذخیره‌ساز ادلهٔ جرم؛ و ۳. رایانه‌ها به عنوان ابزارهای ارتباطات. برای مطالعهٔ مباحث مفصل راجع به این موضوع بنگرید به: (Casey, 2001: 15).

رایانه‌ای منتشر شد، حاوی این سوء استفاده‌های عمده از سیستمهای رایانه‌ای و مخابراتی در آن زمان بود که از دولتها خواسته شد برای مقابله با آنها قوانین کیفری مناسبی وضع کنند:

الف. ورود، تغییر، پاک کردن و یا متوقف کردن عمدی داده‌ها یا برنامه‌های رایانه‌ای که به قصد انتقال غیرقانونی وجه یا هرچیز با ارزش دیگری صورت گرفته باشد؛

ب. ورود، تغییر، پاک کردن و یا متوقف کردن عمدی داده‌ها یا برنامه‌های رایانه‌ای که به قصد جعل صورت گرفته باشد؛

ج. ورود، تغییر، پاک کردن و یا متوقف کردن عمدی داده‌ها یا برنامه‌های رایانه‌ای یا هرگونه ایجاد اختلال دیگر که به قصد جلوگیری از کارکرد سیستمهای رایانه‌ای یا مخابراتی صورت گرفته باشد؛

د. نقض حقوق انحصاری مالک یا برنامهٔ رایانه‌ای حفاظت شده به قصد بهره‌برداری تجاری از آن و ارائه به بازار؛

هـ . شنود یا دستیابی عمدی و غیرمجاز به سیستمهای رایانه‌ای یا مخابراتی، چه با نقض تدابیر امنیتی و چه با هدف سوء یا مضر صورت گرفته باشد. (دزیانی، ۱۳۸٤: ۷)

همان گونه که ملاحظه می‌شود، این توصیه‌نامه که مبنای قانون‌گذاریهای بعدی قرار گرفت، کاملاً در مسیر تأمین امنیت سیستمهای رایانه‌ای تدوین شده بود. به این ترتیب می‌توان گفت، منظور از پیشگیری از جرائم رایانه‌ای در آن زمان، تکیه بر ابعاد امنیتی با رویکرد فنی و پرسنلی بوده که البته نباید عدم رشد و شکوفایی خود پیشگیری را در مباحث جرم‌شناختی آن زمان بی‌تأثیر دانست.

**۲. نسل دوم جرائم رایانه‌ای:** نکتهٔ قابل توجهی که می‌توان در بارهٔ این نسل از جرائم بیان کرد این است که پیش از آنکه به عنوان یک نسل از جرائم با ویژگیهای خاص مورد توجه قرار گیرد، پل ارتباطی میان نسل اول و سوم بوده است. دلیل بارز آن هم عمر بسیار کوتاه این نسل است که به سرعت با ظهور نسل سوم منتفی شد.

آنچه این نسل از جرائم را از دو نسل دیگر متمایز می‌سازد، توجه به «داده‌ها» سوای از «واسط» آنهاست. این رویکرد که از اواخر نسل اول زمزمه‌های آن شنیده می‌شد، به دلیل محوریت یافتن داده‌ها اتخاذ گردید. دلیل آن هم این بود که در دوران نسل اول، سیستمهای رایانه‌ای به تازگی پا به عرصه گذاشته بودند و عمدتاً به شکل سیستمهای شخصی یا رومیزی

بودند و به همین دلیل به تنهایی مورد توجه قرار گرفته بودند. اما به تدریج با توسعه و ارتقای فناوری رایانه و به کارگیری آن در بسیاری از ابزارها و به عبارت بهتر رایانه‌ای شدن امور، به تدریج ابزارهای رایانه‌ای جایگاه خود را از دست دادند و محتوای آنها یعنی داده‌ها محوریت یافت. بدیهی است در این مقطع مباحث حقوقی و به تبع آن رویکردهای مقابله با جرائم رایانه‌ای نیز تغییر یافت، به نحوی که تدابیر پیشگیرانه از جرائم رایانه‌ای با محوریت داده‌ها و نه واسطشان تنظیم شدند. حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل مشاهده است (دزیانی، ۱۳۸۳: ٤)



به این ترتیب، سیستمهای رایانه‌ای در صورتی در دوران نسل دوم ایمن محسوب می‌شدند که داده‌های موجود در آنها از سه مؤلفه برخوردار بود: ۱. محرمانگی (Confidentiality): داده‌ها در برابر افشا یا دسترس غیرمجاز حفاظت شده باشند؛ ۲. تمامیت (Integrity): داده‌ها در برابر هرگونه تغییر یا آسیب حفاظت شده باشند؛ و ۳. دسترس‌پذیری (Accessibility): با حفظ کارکرد مطلوب سیستم، داده‌ها همواره در دسترس مجاز قرار داشته باشند.

هم اکنون، این سه مؤلفه در حوزه جرائم نسل سوم از جایگاه ویژه‌ای برخوردار شده‌اند و حتی در اسناد قانونی به صراحت به آنها اشاره شده است. برای مثال، عنوان اول از بخش اول فصل دوم کنوانسیون جرائم سایبر (بوداپست، ۲۰۰۱)، به جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری داده‌ها و سیستمهای رایانه‌ای اختصاص دارد. در ذیل این عنوان، پنج مادّه به طور مفصل جرائم این حوزه را برمی‌شمرند که عبارت‌اند از: دسترس غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم، و سوء استفاده از دستگاهها*.

این دوره با وجود عمر کوتاه خود، تأثیر بسزایی در تحول نگرش به جرائم رایانه‌ای داشت. حتی می‌توان گفت، تقریباً از این زمان بود که اصطلاحاتی نظیر جامعهٔ اطلاعاتی یا حقوق کیفری اطلاعات به طور رسمی در اسناد قانونی وارد شد (Sieber, 1995). در ادامه به بررسی نسل سوم از این جرائم می‌پردازیم.

**۳. نسل سوم جرائم رایانه‌ای**: از اوایل دههٔ نود، با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصهٔ بین‌الملل و به ویژه ظهور شبکهٔ جهانی وب (World Wide Web)که به فعالیت

---

* برای ملاحظهٔ این کنوانسیون، پروتکل الحاقی و گزارشهای توجیهی آن به این سایت مراجعه فرمایید:
Cyber Crime Convention at http://conventions.coe.int/Tteaty/en/Reports/Html

این شبکه‌ها ماهیتی تجاری بخشید، بحث راجع به ابعاد گوناگون فضای سایبر به ویـژه مـسائل حقوقی آن، وارد مرحلهٔ جدیدی شد. زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقـه‌ای و محلـی و در حوزه‌های محدودی نظیر سیستمهای تابلوی اعلانات (Bulletin Board System) کـه عمـدتاً جهت بارگذاری (Loading) و پیاده‌سازی (Downloading) برنامه‌ها و پیامها و همچنین ارتباطـات پست الکترونیک به کار می‌رفتند به فعالیت می‌پرداختند. به همین دلیل، هماننـد آنچـه در سـند سازمان توسعه و همکاری اقتصادی آمده، به صورت کاملاً محدود به آنها اشاره کرده‌اند.

در حال حاضر، فضای سایبر از قابلیتهایی برخوردار است که پیش از آن یا وجود نداشته یا به شکل محدودتری قابل بهره‌برداری بوده‌اند. مهم‌ترین این ویژگیها عبارت‌اند از: **الف.**مهم‌ترین خصیصهٔ فضای سایبر، بین‌المللی بودن یا به عبارت بهتر فرامرزی بـودن آن اسـت. شـبکه‌هـای پیشین به صورت محلی یا حداکثر منطقه‌ای (Local Area Network) قابل بهره‌برداری بودنـد. امـا به مدد سیستمهای ارتباطی بی‌سیم و باسیم، نظیر شبکه‌های ماهواره‌ای یا خطـوط فیبـر نـوری، این امکان فراهم گشته است. **ب.** ویژگی مهم دیگـر فـضای سـایبر، برخـورداری از قابلیتهـای چندرسانه‌ای (Multimedia) در سراسر جهان است. برگزاری جلسات کنفرانس زنده بـا قابلیـت انتقال صوت و تصویر با کیفیت و وضوح بالا از طریق شبکه‌های اطلاع‌رسانی رایانه‌ای، یکی از جلوه‌های نوین این فضاست که پیش از این حداقل بـه ایـن شـکل وجـود نداشـت. **ج.** دیگـر مزیتی که می‌توان برای فضای سایبر یا به عبارت بهتر شبکه‌های اطلاع‌رسـانی رایانـه‌ای کنـونی برشمرد، ظرفیت بالای آنهاست؛ تا حدی که ارائهٔ خدمات ذخیـرهٔ داده‌هـا در نقـاط دوردسـت (Remote Computing Service) به یکی از فعالیتهای متداول در فضای سایبر تبـدیل شـده اسـت. (USDOJ, 2002: 52)

این ویژگیها و خصوصیات منحصر به فرد این فضا، همگی باعث شده‌انـد جـرائم رایانـه‌ای که پیش از این گسترهٔ محدودی را در برمی‌گرفتند و خسارات نسبتاً ناچیزی را هم به بـار مـی‌آوردنـد، اکنون به جرائم سایبری تبدیل شوند که به راحتی امکان ارزیابی گسترهٔ این جرائم و خـسارات ناشی از آنها وجود ندارد. آنچه امروز تحـت عنـوان **تروریـسم سـایبر** (Cyber Terrorism) مـورد توجه قرار گرفته، از همین واقعیت نشأت می‌گیرد. تعرض به شبکه‌های حیاتی متصل به فضای سایبر، نظیر بیمارستانها و نیروگاههای بزرگ و تخریب آنها می‌تواند خساراتی معادل جنگهـای

تسلیحاتی یا حتی فراتر از آن را به بار آورد*. هم اکنون بحث هرزه‌نگاری در عرصهٔ اینترنت، به ویژه هرزه‌نگاری کودکان (Child Pornography)، به یک معضل بین‌المللی تبدیل شده است، به نحوی که در سال ۱۹۹۹، اجلاس یونسکو با بررسی آن، اعلامیه‌ای را جهت مقابله با آن صادر کرد. (حسینی، ۱۳۸۲: ۷۵) انواع سوء استفاده‌های مالی از این فضا نیز بسیار گسترده است. از پول‌شویی الکترونیکی به عنوان یک جرم سازمان‌یافته گرفته (جلالی فراهانی، ۱۳۸٤: ۱۰۹) تا تعرض به شبکه‌های بنگاههای اقتصادی و بانکها، از جمله جرائم شایع در این فضا هستند.

این مثالها و بسیاری مصادیق دیگر حاکی از این است که ضرورت اتخاذ تدابیر پیشگیرانه برای مقابله با جرائم سایبر بیش از پیش احساس می‌شود. در این مقطع، به لحاظ پیشرفت علوم مرتبط با جرم‌شناسی و تنوع تدابیر پیشگیرانه، می‌توان بهتر از گذشته در این زمینه تصمیم‌گیری کرد. اما این نکتهٔ بسیار مهم را نیز نباید از خاطر دور داشت که به لحاظ ماهیت فنی فضای سایبر و آنچه باید و می‌توان انجام داد، در اینجا نیز عمدهٔ تدابیر رویکرد امنیتی دارند که البته بر پایهٔ مطالعات جرم‌شناختی در مورد مجرمان و بزه‌دیدگان و همچنین بستر ارتکاب این جرائم به اجرا درمی‌آیند.

به هر حال، با توجه به اینکه اکنون با جرائم سایبر مواجه هستیم و تدابیر مورد بحث جنبهٔ تاریخی ندارند و به اجرا درمی‌آیند، گفتار بعد به بررسی انواع و نحوهٔ کارکرد آنها اختصاص یافته است.

## ج. انواع تدابیر پیشگیری وضعی از جرائم سایبر

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

**۱. تدابیر محدودکننده یا سلب‌کنندهٔ دسترس:** این تدابیر، در زمرهٔ مهم‌ترین تدابیر پیشگیرانهٔ وضعی از جرائم سایبر قرار دارند که نمونه‌های اولیهٔ آن برای جلوگیری از جرائم نسل اول نیز به کار می‌رفت. در اینجا سعی می‌شود با نصب سیستمها یا برنامه‌های خاص بر روی گرههای (Nodes)

* درست یک هفته پس از واقعهٔ یازدهم سپتامبر ۲۰۰۱، ویروسی به نام «نیمدا» در شبکه‌های رایانه‌ای ایالات متحده منتشر شد و خسارات فراوانی به بار آورد. این واقعه چنان مورد توجه قرار گرفت که ایالات متحده تدوین استراتژی امنیت فضای سایبر را در دستور کار قرار داد که تا سپتامبر ۲۰۰۲ پیش‌نویس آن تهیه شد و در فوریهٔ ۲۰۰۳ به تصویب رسید و ابلاغ شد. (حسن‌بیگی، ۱۳۸۲: ۳۱٦)

دسترس به شبکه، یعنی کامپیوترهای شخصی، مسیریابها (Routers)، سیستمهای ارائه‌دهندگان خدمات شبکه‌ای و از همه مهم‌تر ایجادکنندگان نقطهٔ تماس بین‌المللی، از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی جلوگیری شود. این سیستم‌ها و برنامه‌ها عمدتاً در سه قالب دیوارهای آتشین (Firewall)، فیلترها (Filtering) و پراکسیها (Proxy) هستند. این ابزارها حاوی فهرستی از موضوعات مجاز (White List) یا غیرمجاز (Black List) هستند و بر اساس فرایند انطباق عمل می‌کنند. (Thornburgh, 2004: 51) بعضی از آنها مانند فیلترها و دیوارهای آتشین یک سویه عمل می‌کنند، یعنی فقط از ورودیهای غیرمجاز جلوگیری می‌کنند، اما بعضی دیگر دوسویه عمل می‌کنند و علاوه بر ورودیها، از خروجیها هم مراقبت می‌نمایند. (Shinder, 2002: 349)

**۲. تدابیر نظارتی** (Monitoring Measures): نظارت شبکه‌ای شاید بیش از آنکه یک اقدام پیشگیرانه (Preventive) باشد، از لحاظ بازدارندگی (Deterrence) مورد توجه قرار می‌گیرد. این اقدام به دو شکل فنی و انسانی قابل اجراست. در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیهٔ فعالیتهای شبکه‌ای اشخاص، حتی ضرباتی که بر روی صفحه کلیدشان زده‌اند یا نقاطی را که به وسیلهٔ ماوس بر روی آنها کلیک کرده‌اند ضبط می‌کنند. سپس مأمور مورد نظر می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد.

شایان ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر بداند فعالیتهایش تحت نظارت قرار دارد، زیرا همان‌طور که می‌دانیم، نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد. اکنون بسیاری از محیطهای گپ شبکه‌ای (Chat Rooms)، به ویژه آنها که مورد اقبال قشر جوان و نوجوان است، تحت نظارت فنی یا زنده قرار دارند.

اما مهم‌ترین مزیت این اقدام نسبت به اقدامات محدودکننده یا سلب‌کنندهٔ دسترس این است که در عین اثرگذاری بازدارنده که پیشگیرانه نیز تلقی می‌شود، در فعالیت کاربران خللی ایجاد نمی‌کند و از این لحاظ اشکالی به وجود نمی‌آورد، اما خود آن با ایرادات مهم حقوقی مواجه است که در جای خود به آن خواهیم پرداخت.

**۳. تدابیر صدور مجوز** (Verification or Authentication Technologies): در اینجا تلاش می‌شود بر اساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری شود. نمونهٔ

سادهٔ این اقدام، به کارگیری گذرواژه (Password) است که در گذشته و اکنون جایگـاه خـود را حفظ کرده است. به این ترتیب، تنها کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار لازم، گذرواژهٔ مربـوط را دریافـت کننـد. ممکن است این مجوز بر اساس سن، جنس، ملیت، مذهب یـا گرایـشهای خـاص فکـری داده شود. امروزه در این حوزه پیشرفتهای بسیاری صورت گرفته است. به عنوان مثال، برای ارتقای هرچه بیشتر امنیت، چندی است از شیوه‌های بیومتریک نیز استفاده می‌شود. به عنوان مثـال، بـه جای یا علاوه بر گذرواژه، از اسکن عنبیه یا شبکیهٔ چشم یا اثر انگشت نیز برای شناسایی فـرد استفاده می‌شود تا ضریب خطا به حداقل برسد.



به نظر می‌رسد تدابیر این حوزه نسبت به دو حوزهٔ دیگر ایرادات اساسی ندارد، اما خالی از اشکال هم نیست و حداقل به دو نقـص مهـم آن مـی‌تـوان اشـاره کـرد: ۱. نـسبت بـه تمـامی حوزه‌های فضای سایبر قابل اجرا نیست و موارد استفادهٔ آن بسیار محدود اسـت. ۲. ایـن ایـراد که البته راجع به دیگر ابزارهای پیشگیرانه نیز صادق است، به پیشرفت لحظه‌شـمار فناوریهـای موجود در فضای سایبر مربوط می‌شود. ممکـن اسـت یـک سیـستم اکنـون بـا بهـره‌گیـری از ابزارهای صدور مجوز، از ایمنی قابـل قبـولی برخـوردار باشـد، امـا بـه نظـر نمـی‌رسـد هـیچ متخصصی بتواند این ایمنی را تا مدت مشخصی تضمین نماید، زیـرا ایـن فنـاوری در معـرض آزمون و خطای هزاران نفر از سراسـر جهـان قـرار دارد و بـه زودی نقـاط ضـعف آن کـشف می‌شود. (Board On Children, Youth, And Families, 2004: 50)

**٤. ابزارهای ناشناس‌کننده** (Anonymizers) **و رمزگذاری** (Encryption): این دو اقدام تا حـدی از لحاظ کارکرد با یکدیگر تفاوت دارند، اما از آنجا که یک هدف را دنبال می‌کننـد، در اینجـا بـا هم بررسی می‌شوند. همان گونه که از این اصطلاحات پیداست، این ابزارها ماهیت اصلی یـک مفهوم را پنهان یا غیرقابل درک می‌کنند تا غیرقابل شناسایی و تشخیص گردد. ناشناس‌کننده‌هـا هویت اشخاص را در فضای سایبر پنهان می‌کنند و از این طریق به آنها امکان می‌دهند با ایجـاد حریم بیشتر به فعالیت شبکه‌ای بپردازند. این اقدام به ویژه برای زنان و کودکان یا به طور کلـی اشخاصی که به هر دلیل آسیب‌پذیرند سودمند است، زیرا بی‌آنکه فرصت شناسایی خـود را بـه مجرمان سایبر بدهند، می‌توانند به فعالیتهای شبکه‌ای بپردازند. (Thornburgh, 2001: 66)

اما از ابزارهای رمزنگاری بیشتر برای محتوای ارتباطات استفاده می‌شود. در اینجا بر اسـاس

کدهای خاصی متن اصلی به رمزنوشته (Cipher Text) تبدیل می‌شود و گیرنده در مقصد به وسیلهٔ کلیدی که در اختیار دارد، آن را رمزگشایی (Decryption) می‌کند. متأسفانه ابزارهای متنوع و بسیاری در فضای سایبر برای شنود و دستیابی به ارتباطات افراد وجود دارد که بهره‌گیری از برنامه‌های رمزنگاری می‌تواند خطر این گونه تعرضات را کاهش دهد. (Shinder, 2002: 378)

با این حال، نباید از یاد برد که امکان استفاده از این ابزارها برای مجرمان نیز وجود دارد. آنها با پنهان کردن هویت یا رمزنگاری محتوای مجرمانهٔ ارتباطاتشان، امکان شناسایی خود را کاهش می‌دهند. لذا این گزینه نسبت به سه تدبیر پیشگیرانهٔ قبل از این ضعف برخوردار است که در کنار از بین بردن برخی از فرصتهای ارتکاب جرم، زمینهٔ ارتکاب ایمن برخی دیگر از جرائم را هم فراهم می‌آورد*.



## د. انعکاس موازین حقوق بشر در فضای سایبر

پس از آشنایی با ماهیت جرائم سایبر و نیز پیشگیری وضعی و انواع تدابیر آن در زمینهٔ جرائم مزبور، اینک نوبت بررسی چالشهای تدابیر پیشگیری وضعی با موازین حقوق بشر است. اما لازم است ابتدا ببینیم اتخاذ تدابیر پیشگیری وضعی ممکن است به رعایت نشدن کدام موازین حقوق بشری بینجامد.

پیش از هر چیز، در خور ذکر است منظور از موازین حقوق بشر، اصول و هنجارهایی است که در اعلامیهٔ جهانی حقوق بشر (۱۹٤۸) و میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹٦٦) منعکس شده‌اند. سه اصل از اصول این اسناد به طور قابل توجهی تحت تأثیر فضای سایبر قرار گرفته‌اند که در اینجا به آنها پرداخته می‌شود.

**۱. تأثیر فضای سایبر بر آزادی عقیده و بیان** (Freedom of Expression): یکی از اصول مهمی که در اعلامیهٔ حقوق بشر و شهروند فرانسه مصوب ۲٦ اوت ۱۷۹٦ مورد تأکید تدوین‌کنندگان آن قرار گرفته است، آزادی عقیده و بیان است. همان‌طور که می‌دانیم، یکی از اهداف انقلاب کبیر فرانسه، برپایی یک جامعهٔ مردم‌سالار بود؛ یعنی جامعه‌ای عاری از استبداد و خودکامگی تا هر

* البته باید گفت این موضوع در مورد نظارت شبکه‌ای نیز صادق است. اکنون ابزارهای نظارتی بسیاری در سطح شبکه‌ها وجود دارند که مجرمان می‌توانند برای ارتکاب جرائم بسیاری از آنها استفاده کنند.

کس بتواند با ابراز عقاید و دیدگاههای خویش، در سرنوشت مملکتش سهیم باشد. بی‌تردید تحقق این مهم منوط به آزادی انجام چنین کاری بود و به همین دلیل به صراحت از سوی انقلابیون در این منشور مورد تأکید قرار گرفت و پس از آن در اعلامیهٔ جهانی حقوق بشر و دیگر اسناد مربوط به رسمیت شناخته شد. (بسته‌نگار، ۱۳۸۰: ۵۱)

در این زمینه، مادّهٔ ۱۹ اعلامیه اشعار می‌دارد:

هرکس حق آزادی عقیده و بیان دارد و این حق مستلزم آن است که از داشتن عقیده بیم نداشته باشد و در دریافت و انتشار اطلاعات و افکار، به تمام وسایل ممکن، بدون ملاحظات مرزی، آزاد باشد.

این مادّه چنان صراحت و جامعیتی دارد که به نظر می‌رسد نیازی به تفسیر و روزآمد کردن آن نیست و به حتم در هر زمان و در تمامی شرایط و اوضاع و احوال صادق است.

از آنجا که این اعلامیه جنبهٔ الزام‌آور نداشت و از طرف دیگر، ضرورت ایجاب می‌کرد این اصول از سوی کشورها رعایت گردد، در سال ۱۹٦٦ سند بین‌المللی دیگری به نام میثاق بین‌المللی حقوق مدنی و سیاسی به تصویب رسید و در ۲۳ مارس ۱۹۷٦ لازم‌الاجرا شد. اما از آنجا که برخی از الزامات به کشورها تحمیل شده بود، تمامی اصول و هنجارهای مورد بحث از آن قالب مطلق خود که اعلامیهٔ حقوق بشر بر آن تأکید داشت خارج شدند و به کشورها اجازه داده شد در برخی موارد مهم محدودیتهایی را اعمال کنند*. به عنوان مثال، در بند یک مادّهٔ ۱۸ میثاق آمده: «۱. هرکس حق آزادی فکر، وجدان و مذهب دارد. ... .» اما در بند ۳ آن نیز قید شده:

آزادی ابراز مذهب یا معتقدات را نمی‌توان تابع محدودیتهایی نمود، مگر آنچه منحصراً به موجب قانون برای حمایت از امنیت، نظم، سلامت یا اخلاق عمومی یا حقوق و آزادیهای اساسی دیگران ضرورت داشته باشد.

همان گونه که ملاحظه می‌شود، در اینجا به استثنائات کلی و مهمی اشاره شده که هر دولتی می‌تواند برای توجیه اقدامات خود به آنها تمسک جوید. (ساندرا کولیور، ۱۳۷۹: ۱۷۷) با اینکه در این سند قید شده کلیهٔ اقدامات باید به موجب قانون و با توجه به سایر الزامات حقوق بین‌الملل باشد، به نظر می‌رسد ابزار بازدارندهٔ مهمی تلقی نشود. لذا برای اینکه این

* البته شایان ذکر است مادّهٔ ۲۹ اعلامیه نیز بهره‌برداری از حقوق مورد اشاره را در چهارچوب قانون و در پرتو رعایت حقوق و آزادیهای دیگران و مقتضیات اخلاقی و نظم عمومی و رفاه همگان که شایستهٔ یک جامعه مردم‌سالار است به رسمیت شناخته است.

اقدامات تحت ضوابط دقیق‌تری اجرا شود، در اول اکتبر ۱۹۹۵، گروهی از متخصصان حقوق بین‌الملل، امنیت ملی و حقوق بشر، بیانیهٔ ژوهانسبورگ را درباره نحوهٔ تعامل امنیت ملی با آزادی بیان و دسترس به اطلاعات منتشر کردند. (نمک‌دوست تهرانی، ۱۳۸٤) این بیانیه که مشتمل بر ۲۵ اصل است، تلاش کرده حدود و ثغور اصول حقوق بشر راجع به آزادی بیان و دسترس به اطلاعات را در تقابل با ضرورت حفظ امنیت و مصلحت ملی مشخص کند. اصل اول این بیانیه، همانند اصول پیش‌بینی شده در اعلامیهٔ حقوق بشر و میثاق، آزادی عقیده، بیان و اطلاعات را به رسمیت می‌شناسد، اما در همان جا اشاره می‌کند که ممکن است تحت شرایط خاصی، مانند حفظ امنیت ملی، محدودیتهایی وضع شود، ولی در ادامه می‌کوشد این محدودیتها را در قالب زیر اصلهای ۱ـ۱، ۱ـ۲، و ۱ـ۳ تشریح نماید و از ابهام خارج کند.



حال باید دید با ظهور فضای سایبر، این اصل در چه وضعیتی قرار می‌گیرد. بی‌تردید این فضا با گسترهٔ نامحدود و قابلیتهای بی‌شمار خود، مؤثرترین کمک را به تحقق هرچه کامل‌تر این اصل کرده است. زیرا اگر در گذشته‌ای نه چندان دور شخصی می‌خواست عقیدهٔ خود را به اطلاع دیگران برساند، یا باید به اطرافیان خود اکتفا می‌کرد یا با صرف هزینه و وقت بسیار، به تدریج به گوش دیگران می‌رساند. اما اکنون این امکان فراهم آمده که کلام خود را از پشت سیستم رایانه‌ای در منزل خود، آن هم به شکل دوسویه، به اطلاع تمامی جهانیان برساند، یعنی به طور همزمان از نظرها و دیدگاههای مخاطبان خود نیز بهره‌مند شود. این ویژگی مزیت بزرگی است که دیگر رسانه‌های ارتباط جمعی از آن بی‌بهره‌اند.

از سوی دیگر، این فضا با چالشهایی در خصوص سوء استفاده‌های بسیار متنوع مواجه است که ضروری است با آنها مقابله شود تا امنیت، نظم، سلامت یا اخلاق عمومی یا حقوق و آزادیهای دیگران حفظ شود. حال باید دید تا چه اندازه می‌توان این دو دغدغهٔ به ظاهر یا واقعاً متناقض را با یکدیگر جمع کرد. گفتار بعد به بررسی این موضوع اختصاص دارد.

**۲. تأثیر فضای سایبر بر جریان آزاد اطلاعات** (Free Flow of Information): یکی از اصولی که همواره در اسناد بین‌المللی حقوق بشر در کنار و هم‌ارز آزادی عقیده و بیان به آن تأکید شده، جریان آزاد اطلاعات است. بی‌تردید آزادی عقیده و بیان زمانی در معنای واقعی خود تحقق خواهد یافت که بتوان اطلاعات را بی‌هیچ محدودیتی در جامعه منتشر کرد. در اعلامیهٔ جهانی حقوق بشر به صراحت به این اصل اشاره نشده، اما از مفاد مربوط به آزادی بیان و دیگر موارد

پیش‌بینی شده، کاملاً لزوم رعایت چنین قاعده‌ای استنباط می‌شود. به عنوان مثال، در مادّهٔ ۱۹ به اشخاص حق داده شده در دریافت و انتشار اطلاعات و افکار به تمام وسائل ممکن و بدون ملاحظات مرزی آزاد باشند. بی‌تردید تا زمانی که اطلاعات که مظهر تجلی عقاید و افکار در جامعه است، آزادانه جریان نداشته باشد، نمی‌توان تحقق اهداف متعالی آزادی عقیده و بیان را انتظار داشت.

اما نکتهٔ مهمی که باید در اینجا مد نظر قرار داد این است که در این حوزه ما با دو اصطلاح مواجهیم که با وجود تشابه ظاهری، از لحاظ ماهیت با یکدیگر تفاوت دارند. یک اصطلاح جریان آزاد اطلاعات بود که در فوق توضیحاتی راجع به آن داده شد. اما اصطلاح دوم، آزادی اطلاعات (Freedom of Information) یا به عبارت بهتر حق دسترس به اطلاعات است که آن نیز نقش مهمی در تحقق اهداف آزادی بیان دارد که مهم‌ترین آن نهادینه شدن مردم‌سالاری است. منظور از قاعدهٔ دوم، که اتفاقاً در اسناد حقوق بشر نیز به آن اشاره شده، این است که دولت حق ندارد جامعه را از دسترس به اطلاعات مربوط به امور حکومتی و دولتی محروم سازد و حتی موظف است به بهترین وجه آن را تأمین کند. به عنوان مثال، مادّهٔ ۱۱ بیانیه ژوهانسبورگ اشعار می‌دارد:

هر کس حق کسب اطلاعات از مقامات دولتی را داراست، اگرچه مربوط به امنیت ملی باشد... .

اما همان گونه که دربارهٔ آزادی بیان نیز اشاره شد، بهره‌برداری از این حقوق مطلق نیست و در هر صورت باید خط قرمزهایی رعایت شود. اما برای روشن بودن این حدود و ثغور، همان مادّه در ادامه مقرر می‌دارد:

... مگر آنکه دولت بتواند اثبات کند اعمال محدودیت به موجب قانون بوده و برای حفظ مصلحت مشروع امنیت ملی در یک جامعهٔ مردم‌سالار ضروری است.

این بیانیه در مواد قبل و بعد خود این مفاهیم را به خوبی موشکافی کرده است که مجال پرداختن به آنها در اینجا فراهم نیست.*

اما از نظر فضای سایبر، باید گفت از آنجا که ابزار خوبی برای ابراز عقیده و بیان محسوب

* گفتنی است تاکنون بیش از چهل کشور جهان در این زمینه قوانینی تصویب کرده‌اند. حتی بعضی کشورها نظیر انگلستان سعی کرده‌اند با اصلاح قوانینی زیربنایی، نظیر قوانین راجع به حمایت از داده‌ها (حریم خصوصی)، زمینه‌های قانونی دسترس افراد به اطلاعات را هرچه بیشتر فراهم کنند.

می‌شود، بالطبع نقطه عطفی را در جریان آزاد اطلاعات فراهم آورده است. این فضا با قابلیتهای شگفت‌آور خود، آنچه را یک جامعهٔ اطلاعاتی تمام عیار برای به جریان انداختن آزاد اطلاعات نیاز دارد در اختیارش گذاشته است.

همچنین فضای سایبر تحقق اصل آزادی اطلاعات را نیز با چشم‌انداز جدیدی مواجه کرده است. امروزه آنچه از دولت الکترونیک (E-government) به مفهوم واقعی آن خواسته می‌شود، چیزی جز این نیست که با در دسترس قرار دادن اطلاعات راجع به امور اداری و جاری کشور، مردم بتوانند بدون مراجعه به نهادهای دولتی یا خصوصی و پشت سر گذاشتن مشکلات بسیار، از طریق سیستمهای رایانه‌ای خود و اتصال به سایتهای مربوط، نیازهایشان را برآورده سازند.

در همین حد اشاره می‌گردد که اجرایی شدن دولت الکترونیک در تمامی عرصه‌ها، خود می‌تواند به عنوان عامل پیشگیرانه از جرائم مهم محسوب شود. آنچه امروز تحت عنوان جرم فساد (Corruption) در عرصهٔ بین‌الملل مطرح است، یکی از راهکارهای مهم پیشگیری از آن شفاف‌سازی امور دولتی و خصوصی از طریق در دسترس قرار دادن اطلاعات صحیح و اطلاع‌رسانی دقیق و به موقع به مردم است که هر دوی آنها با تحقق دولت الکترونیک میسر می‌شود. (United Nations, 2003: 24)

**۳. تأثیر فضای سایبر بر حریم خصوصی**: یکی دیگر از اصول اساسی حقوق بشر که زمینه‌های توجه به آن به قبل از اعلامیهٔ جهانی حقوق بشر برمی‌گردد، رعایت حریم خصوصی افراد است*. حدود صد سال پس از تصویب قانون اساسی ایالات متحده به سال ۱۸۹۰، یکی از مسائلی که شهروندان ایالات متحده را به شدت نگران کرد، سوء استفاده مأموران و مجریان قانون از اختیاراتشان برای مداخله در امور خصوصی مردم بود. دو قاضی به نامهای ساموئل وارن (Samuel Warren) و لوئیس براندیس (Louis Brandis)، مطالبی راجع به آن نوشتند و به دولت هشدار دادند نباید با توسل به معاذیری چون اجرای قانون، در امور خصوصی دیگران دخالت کند و بدون اجازه به محیطی پا گذارد که صاحبش حق دارد در آن خلوت کند**.



* شایان ذکر است حریم خصوصی (Privacy) که در امریکا و کشورهای تابع آن رواج یافته، معادل حمایت از داده‌ها (Data Protection) است که بیشتر در کشورهای اروپایی رواج دارد.

** حق تنها ماندن (Let To Be Alone) اصطلاحی است که از آن زمان به عنوان معادلی رسا برای تبیین مفهوم حریم خصوصی به کار رفته است.

تقریباً در همان زمان در کشورهای اروپایی نظیر سوئد نیز حرکتهای مشابهی آغاز شد. اما تا اوایل دههٔ ۱۹۷۰ قانون صریحی راجع به آن در این کشورها به تصویب نرسید. (Smith, 2002: 367) در این زمینه، مادّهٔ ۱۲ اعلامیهٔ حقوق بشر اشعار می‌دارد:

> زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات افراد نباید مورد مداخلهٔ خودسرانه قرار گیرد یا به شرافت، آبرو یا اعتبار آنها تعرض شود. این افراد حق دارند در برابر چنین تعرضاتی از حمایت قانون برخوردار باشند.

مادّهٔ ۱۷ میثاق نیز از لسان مشابهی برخوردار است.



با اینکه فضای سایبر ابزارهای متنوعی را جهت برقراری ارتباطات ایمن فراهم آورده، بر فرصتها و ابزارهای تعرض به آن نیز افزوده است. حریم خصوصی افراد در فضای سایبر را می‌توان در دو حوزه بررسی کرد: ۱. ارتباطات خصوصی یا غیرعمومی که به اشکال مختلف مکتوب، صوت، تصویر یا حتی چندرسانه‌ای به صورت همزمان یا غیرهمزمان در سراسر جهان برقرار می‌شوند؛ و ۲. پایگاههای داده‌ای (Databases) که حاوی اطلاعات شخصی (Personal Informations)اند یا حتی اطلاعات شخصی حساس (Sensitive Personal Informations) افراد را نگهداری می‌کنند و دسترس به آنها تقریباً با مشکلی مواجه نیست*. امروزه با وفور ابزارها و برنامه‌های شنود و دستیابی به ارتباطات و همچنین در دسترس قرار داشتن پایگاههای داده که البته بخشی از آن به ناچار برای تحقق اهداف و برنامه‌های دولت الکترونیک صورت می‌گیرد، رعایت این اصل در فضای سایبر به مراتب مشکل‌تر از دنیای فیزیکی است.

---

* بخش اول قانون حمایت از داده‌های انگلستان (Data Protection Act, 1998) در تعریف از داده‌های شخصی مقرر می‌دارد: «داده‌هایی که با زندگی شخصی افراد ارتباط دارد و می‌تواند از طریق معیارهای ذیل مشخص گردد: الف.از روی خود داده‌ها؛ یا ب. از روی داده‌ها یا اطلاعاتی که در اختیار کنترل‌کنندهٔ داده‌هاست یا احتمالاً قرار خواهد گرفت. همچنین اصطلاح مذکور شامل هرگونه عقیدهٔ مرتبط با اشخاص یا هرگونه نشانه‌ای دال بر مقاصد کنترل‌کننده یا اشخاص دیگر است که با افراد مذکور مرتبط باشد.» همچنین، در بخش دوم این قانون، داده‌های شخصی حساس تعریف شده است: «داده‌های شخصی‌ای که مشتمل بر اطلاعات ذیل باشد: الف. داده‌های مربوط به مسائل قومی و نژادی؛ ب. عقاید سیاسی؛ ج. اعتقادات مذهبی یا نظایر آن؛ د. عضویت در یک اتحادیهٔ تجاری (به آن مفهوم که مشمول قانون اتحادیه‌های تجاری و روابط کارگری مصوب ۱۹۹۲ قرار گیرد)؛ هـ . شرایط فیزیکی و روانی؛ و. مسائل جنسی؛ ز. ارتکاب یا ادعای ارتکاب هرگونه جرم؛ ح. هرگونه تعقیب کیفری در مورد جرائم ارتکابی یا جرائمی که ادعای ارتکاب آن توسط شخص مربوط مطرح شده و همچنین هر حکمی که از سوی هر دادگاه در اثر این تعقیب صادر شده باشد.»

## هـ. چالشهای پیشگیری وضعی از جرائم سایبر با موازین حقوق بشر

در این گفتار، تدابیر پیشگیرانه‌ای را که راجع به جرائم سایبر معرفی شده بود، در تقابل با موازین حقوق بشر بررسی می‌کنیم.

**۱. تقابل پیشگیری وضعی از جرائم رایانه‌ای با آزادی بیان و جریان آزاد اطلاعات**

از آنجا که این دو اصل از لحاظ ماهیت تقریبا مشابه یکدیگرند و حتی می‌توان آنها را لازم و ملزوم یکدیگر برشمرد و چون تدابیر پیشگیرانه از جرائم سایبر به یک شکل به آنها تعرض می‌کنند، در اینجا با یکدیگر بررسی خواهند شد.



همان‌گونه که اشاره شد، ماهیت آزادی بیان به گونه‌ای است که باید دیدگاهها و عقاید افراد بدون محدودیت در اختیار همگان قرار گیرد. این مبنا کاملاً با آنچه فضای سایبر فراهم می‌آورد منطبق است و حتی زمینه‌های شکوفایی آن به مراتب فراتر از آنچه تصور می‌رفت به وجود آمده است. از سوی دیگر، تدابیر محدودکننده یا سلب‌کنندهٔ دسترس، به ویژه فیلترینگ، مانع بزرگی در تحقق این اصل محسوب می‌شوند، زیرا از جریان آزاد اطلاعات جلوگیری می‌کنند. دلایل مختلفی باعث ایجاد محدودیت از سوی این ابزارها می‌شود که در اینجا به دو عامل مهم اشاره می‌شود:

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

**ب. کارکرد انطباقی:** دومین مانع بزرگ، کارکرد انطباقی و نه هوشمندانهٔ این ابزارهاست. همان‌طور که می‌دانیم، اصطلاحات یا تصاویر مندرج در فهرستهای سیاه، تنها در متون یا محتواهای غیرمجاز به کار نمی‌روند و بسیار اتفاق می‌افتد که به لحاظ کاربرد آنها در محتواهای

مجاز، از دسترس به آنها جلوگیری می‌شود. بـه عنـوان مثـال، بـا درج واژهٔ sex در موتورهـای جست‌وجو که یکی از واژگان پر بسامد در اینترنت است، فیلترها به سرعت فعال می‌شـوند، در حالی که بسیار اتفاق می‌افتد که از آن واژه در متون معتبر علمی و ادبی نیـز اسـتفاده شـود. امـا جالب اینجاست که چنانچه در فهرست فیلترها شقوق دیگر نگارش این کلمـه، نظیـر esx، درج نشده باشد، با وجود دارا بودن محتوای غیرمجاز، آن فیلترها فعال نخواهند شد و از دسترس به آنها جلوگیری نخواهند کرد. (Thornburgh, 2004: 267)

امروزه در بسیاری از کشورها حفظ امنیت ملی، نظم، سلامت یا اخلاق عمومی و احترام به حقوق یا آزادیهای اساسی دیگران، جزء مؤلفه‌هایی است که به رسمیت شناخته شـده و دولتهـا تلاش می‌کنند از آنها به بهترین وجه پاسداری کنند. از سوی دیگر، فضای سایبر جلوهٔ دیگـری به این مفاهیم بخشیده و باید مطابق با ویژگیهای خاص آن برنامه‌ریزی کرد. اگـر تعـداد بـسیار کمی از گروههای یک جامعه به فکر تهیهٔ انواع ابزارهای محدودکننده یا سـلب‌کننـدهٔ دسـترس هستند، خیل عظیمی هم برای خنثا کردن آن ابزارها تلاش می‌کنند و در میان این گروه می‌توان چهره‌های موجه بسیاری نظیر دانشجویان و دانش‌پژوهان را یافت که برای احقـاق حـق خـود، یعنی بهره‌برداری علمی و سودمند از این فضا، سعی می‌کنند دست بـه کـاری بزننـد کـه شـاید غیرقانونی نیز تلقی شود.

آنچه نباید از نظر دور داشت اینکـه در تمـامی کـشورها، حتـی آنهـایی کـه خـود را مهـد مردم‌سالاری می‌دانند، خط قرمزهایی وجود دارد. در کشوری مثل ایالات متحده یـا کـشورهای اروپایی، از ابزارهایی نظیر فیلترها به وفور استفاده می‌شود، اما بـرای کاسـتن از مـضرات آنهـا، سعی شده برنامه‌ریزی مفصلی در زمینهٔ مخاطب‌شناسی (کسانی که این ابزارها برای آنها به کـار می‌رود)، شناسایی هرچه دقیق‌تر محتواهای غیرمجاز و پرهیز از گنجانیدن مـوارد مـشکوک بـه آنها و در نهایت بهره‌گیری چندبعـدی از ایـن ابزارهـا انجـام شـود. بـه عنـوان مثـال، در کنـار فهرستهای متنی، از فهرستهای تصویری یا دیگر شناسه‌ها استفاده می‌شود تا ضعف این ابزارهـا به حداقل برسد. از جمله در ایالات متحده برای هر طیف و گروه سنی از افـراد جامعـه، ابـزار خاصی به کار می‌رود. بنابراین، فیلتری که در یک مدرسه برای کودکان به اجرا درمی‌آید، بـرای سیستمهای رایانه‌ای دانشگاه بـه کـار نمـی‌رود و در آنجـا سـعی مـی‌شـود از ابزارهـای کمتـر محدودکننده استفاده شود تا در فعالیتهای پژوهشی دانشجویان خللی وارد نشود.

به نظر می‌رسد با یک برنامه‌ریزی صحیح و اقتباس از الگوهای مفیدی که اکنـون در دیگـر

کشورها به اجرا درمی‌آید، علاوه بر حفظ ارزشهای مورد قبول جامعه، می‌توان به گونه‌ای مؤثر از جرائم سایبر پیشگیری کرد.

**۲. تقابل پیشگیری وضعی از جرائم رایانه‌ای با حریم خصوصی**

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



اما پیش از پرداختن به قوانین و مقررات حمایتی از حریم آن‌لاین افراد، به تأثیر ابزارهای پیشگیرانه از جرائم سایبر آن اشاره می‌شود. به طور کلی، دو ابزار پیشگیرانه از چهار ابزار فوق، حریم الکترونیکی افراد را تهدید می‌کنند: ۱. ابزارهای نظارتی که با توجه به توضیحاتی که دربارهٔ آنها داده شد، تردیدی در تعرض‌آمیز بودن آنها نیست. این اقدام پیشگیرانه که در عین حال بازدارنده نیز می‌باشد، تأثیرات سوء مستقیم و غیرمستقیم بسیاری بر فعالیتهای شبکه‌ای می‌گذارد. چنانچه در محیطی این حس در مردم بیدار شود که به دلیل بی‌اعتمادی به آنها، همواره تحت نظارت قرار دارند، این امر به شدت در نحوهٔ فعالیت آنها تأثیر خواهد گذاشت. اکنون فعالیتهای مختلف اقتصادی، اجتماعی، فرهنگی و سیاسی بسیار متنوعی در فضای سایبر جریان دارد که تمامی آن به خاطر آزاد و عاری بودن این فضا از هرگونه محدودیت است. اما چنانچه کاربران شبکه‌ای احساس کنند فعالیتهای آنها تحت نظارت مستمر زنده یا غیرزنده قرار دارد، بی‌تردید در نحوهٔ فعالیت خود تجدیدنظر خواهند کرد که این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد. به هر حال، با اذعان به اینکه ضروری است برای مقابله با جرائم بسیار متنوع سایبر اقدامات نظارتی اعمال شود، این نظارت باید به نحوی باشد که اعضای این فضا احساس نکنند به آنها به دید مجرم نگریسته می‌شود.

دومین ابزاری که البته به صورت غیرمستقیم حریم افراد را تهدید می‌کند، سیستمهای تأیید هویت است. در فضای سایبر، برای اینکه به اشخاص اجازهٔ ورود به محیطهای خاصی داده شود، برخی اطلاعات که شامل اطلاعات شخصی یا حتی اطلاعات شخصی حساس می‌شود، از آنها اخذ می‌گردد. نگرانی‌ای که در اینجا وجود دارد، راجع به امکان سوء استفادهٔ متصدیان این سایتها از این اطلاعات یا امکان افشای آنها به دلایل مختلف، نظیر فقدان یک سیستم امنیتی کارآمد جهت حفاظت از این اطلاعات، است. (Kent, 2004: 55) این موضوع تا آن حد جدی تلقی شده که برای

حمایت از کودکانی که چنین اطلاعاتی از آنان اخذ می‌گردد، در سال ۱۹۹۹ در ایالات متحده قانون حمایت از حریم آن‌لاین کودکان (The Children's Online Privacy Protection Act) به تصویب رسید.

اما راجع به اسناد بین‌المللی و منطقه‌ای دربارهٔ حمایت از این اصل، ابتدا باید به مادهٔ ۱۵ کنوانسیون جرائم سایبر اشاره کرد که با رویکردی عام از دول عضو خواسته است قوانین و مقررات خود را برای حمایت از حقوق و آزادیهای بشر که در کنوانسیون شورای اروپا، میثاق بین‌المللی حقوق مدنی و سیاسی و دیگر اسناد لازم‌الاجرای بین‌المللی منعکس شده تصویب کنند و به اجرا درآورند. این حاکی از توجه کامل واصفان این کنوانسیون به رعایت موازین حقوق بشر در فضای سایبر است. همچنین می‌توان به اسناد 90/313/EEC و 2001/29/EC شورای اروپا راجع به قواعد جامعهٔ اطلاعاتی اشاره کرد.

در حوزهٔ حریم خصوصی، مراجع قانون‌گذاری اروپا پیش از این دستورالعملهای مختلفی برای حمایت از حریم الکترونیکی اشخاص به تصویب رسانده‌اند که به طور فهرست‌وار به آنها اشاره می‌گردد: ۱. کنوانسیون شورای اروپا راجع به حمایت از اشخاص در برابر پردازش خودکار اطلاعات شخصی (۱۹۸۱) ؛ ۲. دستورالعمل اتحادیهٔ اروپا راجع به حمایت از داده‌ها (95/46/EC)؛ ۳. دستورالعمل مخابرات اتحادیهٔ اروپا برای حمایت از پردازش داده‌های شخصی و حریم افراد در حوزهٔ مخابرات که در آن مباحث مربوط به شبکه‌های اطلاع‌رسانی رایانه‌ای را هم مطرح کرده است (97/66/EC)؛ و ٤. دستورالعمل پارلمان و شورای اروپا در خصوص پردازش داده‌های شخصی و حمایت از حریم ارتباطات الکترونیک (2002/58/EC).

اما در ایالات متحده، اولین قانون فدرال حمایت از حریم ارتباطات الکترونیک (Electronic Communication Privacy Act - 18 USC 2701-2712)، در سال ۱۹۸٦ به تصویب رسید. ویژگی بارز این قانون این بود که بر خلاف اصلاحیهٔ چهارم قانون اساسی، تمامی افراد مرتبط با حوزهٔ ارتباطات الکترونیک، به ویژه ارائه‌دهندگان خدمات شبکه‌ای را تحت شمول خود قرار داده و برای نقض حریم افراد از سوی آنان، ضمانت اجراهای کیفری و غیرکیفری مقرر کرده است*. البته این قانون استثناهایی را در این زمینه برشمرده که از جمله آنها می‌توان

* در اصلاحیهٔ چهارم به صراحت از حریم افراد حمایت نشده و فقط از مجریان قانون خواسته شده تفتیش و توقیف اموال، جان، مکاتبات و دیگر اشیای افراد را مطابق قانون انجام دهند. اما حقوقدانان از مفاد آن قاعدهٔ «انتظار متعارف حفظ حریم خصوصی» (Reasonable Expectation of Privacy) را استنباط کرده و ملاک عمل خود قرار داده‌اند.

به مجاز بودن ارائه‌دهندگان خدمات در نقض حریم افراد برای حفاظت از اموال، حقوق و داراییهایشان اشاره کرد. همچنین قانون نحوهٔ استفاده از ابزارهای ثبت‌کننده و ردیاب (Pen Register And Trap And Trace Devices Statute - 18USC 3121-3127) ، راجع به نحوهٔ شنود و نظارت مجریان قانون بر ارتباطات مخابراتی و الکترونیکی است. (USDOJ,2002: 4)

اما مهم‌ترین نکته‌ای که باید راجع به قوانین مصوب در ایالات متحده به آن اشاره کرد، مواردی است که این کشور پس از واقعهٔ یازدهم سپتامبر در سال ۲۰۰۱ اعمال کرده است. کمتر از دو ماه از این واقعه نگذشته بود که قانون بسیار مفصلی تحت عنوان **قانون پاتریوت** (Patriot Act)* برای مبارزه با تروریسم و حفظ امنیت ملی به تصویب رسید که به موجب آن تمامی قوانین گذشتهٔ حمایت از حقوق بشر اصلاح شد و به مجریان قانون و دیگر اشخاص دست اندرکار، نظیر متصدیان شبکه‌ها، اجازه داده شد به حریم اشخاص، به ویژه حریم آنلاین آنها تعرض کنند. البته شایان ذکر است که این واقعه، خواسته یا ناخواسته، دیگر اهداف ایالات متحده را در خصوص فضای سایبر تأمین کرد (Cyber Democracy). پیش‌تر، این کشور مدعی برقراری مردم‌سالاری و رعایت حقوق تمامی کشورها در این فضا بود، اما با وقوع این حادثه از ادعای خود عدول نموده و حتی با دستاویز قرار دادن مبارزه با تروریسم و حفظ امنیت بین‌الملل، تدابیر امنیتی شدیدی (Cyber Security) را در مورد آن اعمال کرده است (United Nations, 2004: 40).



## نتیجه

با توجه به خسارات هنگفت و زیان‌باری که جرائم سایبر بر جوامع تحمیل می‌کنند، لازم است تدبیری اساسی دربارهٔ آنها اندیشیده شود. با اینکه در حال حاضر بسیاری از کشورها سعی کرده‌اند با وضع قوانین کیفری جدید یا اصلاح قوانین پیشین خود، امکان تعقیب و پیگرد و مجازات مجرمان سایبر را فراهم آورند، اما اجرای این قوانین با مشکلات عدیده‌ای مواجه

---

* عنوان کامل این قانون عبارت است از:
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

بوده و همین امر باعث شده است بحث پیشگیری از جرائم سایبر اهمیت ویژه‌ای یابد. (جلالی فراهانی، ۱۳۸۳: ۸۷)

در این میان، از آنجا که پیشگیری وضعی حتی در دنیای فیزیکی نیز ماهیتی فنی دارد، در حوزهٔ جرائم سایبر به طور خاص مورد توجه قرار گرفته است. البته باید گفت این اقدام با محدودیتهای فراوانی مواجه است که می‌توان آن را از ابعاد مختلف بررسی کرد. اما به طور کلی، در عمل سه عامل مانع تحقق اهداف پیشگیری وضعی از این جرائم می‌شوند که عبارت‌اند از: ۱. مجرمان سایبر، طیف خاصی از اشخاص را تشکیل می‌دهند. گروهی از آنها که از لحاظ تخصص و مهارت در سطح بالایی قرار دارند، واقعاً خطرناک هستند و متأسفانه تدابیر پیشگیرانه در برابر آنها یارای مقاومت ندارد. بنابراین، تنها انتظاری که می‌توان داشت این است که تلاش شود از ارتکاب جرم افراد نیمه‌حرفه‌ای یا آماتور جلوگیری گردد یا زمینهٔ بزه‌دیدگی افراد کاهش یابد. ۲. متأسفانه فضای سایبر با ویژگیهای منحصر به فرد خود، فی نفسه مانع تحقق اهداف پیشگیرانهٔ وضعی است. در این فضا انواع ابزارهای ارتکاب جرائم سایبر در اختیار همگان قرار دارد و هرکس می‌تواند به فراخور تخصص و مهارت خود از آنها استفاده نماید. انتقال سریع و بسیار سادهٔ اطلاعات و تجربیات حاصل از ارتکاب جرائم سایبر نیز می‌تواند مزید بر علت محسوب شود. ۳. از آنجا که این تدابیر صبغهٔ فنی دارند، چندان قابل اتکا نیستند، زیرا چندی نمی‌گذرد که ضعفها و نحوهٔ دور زدن آنها در فضای سایبر منتشر می‌شود؛ کما اینکه در کشورمان آنان که قصد خنثا کردن فیلترهای شبکه‌ای را دارند، در عمل با مشکلی مواجه نیستند.

علاوه بر این محدودیتها، موانع حقوق بشری بسیاری نیز سد راه تدابیر پیشگیرانهٔ وضعی قرار دارد. در این مقاله سعی شد موانع حقوق بشری بررسی شود و در این زمینه، سه اصل مهم آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی انتخاب شد. در حال حاضر کمتر کشوری را می‌توان یافت که در قانون اساسی یا قوانین عادی خود به این اصول نپرداخته باشد. قانون اساسی کشور ما که به حق یکی از مترقی‌ترین قوانین اساسی دنیاست، به این اصول توجه ویژه‌ای داشته است. به عنوان مثال، اصل سوم قانون اساسی به بهترین وجه لزوم تحقق آزادی بیان و جریان آزاد اطلاعات را تبیین کرده و دولت را مکلف به اجرای آن کرده است:

دولت جمهوری اسلای ایران موظف است برای نیل به اهداف مذکور در اصل دوم، همهٔ امکانات خود را برای امور زیر به کار برد: .... ۲. بالا بردن سطح آگاهیهای عمومی در همهٔ زمینه‌ها با استفادهٔ صحیح از مطبوعات و رسانه‌های گروهی و وسایل دیگر. ... ٤. تقویت روح بررسی و تتبع و ابتکار در تمام زمینه‌های علمی، فنی، فرهنگی و اسلامی از طریق تأسیس مراکز تحقیق و تشویق محققان... ۷. تأمین آزادیهای سیاسی و اجتماعی در حدود قانون. ۸. مشارکت عامهٔ مردم در تعیین سرنوشت سیاسی، اقتصادی، اجتماعی و فرهنگی خویش.

همچنین اصل نهم مقرر می‌دارد:

... هیچ مقامی حق ندارد به نام حفظ استقلال و تمامیت ارضی کشور، آزادیهای مشروع را هرچند با وضع قوانین و مقررات سلب کند.

البته در دیگر اصول قانون اساسی نیز به این مهم اشاره شده که مجال پرداختن به آنها نیست. اما راجع به حریم خصوصی نیز می‌توان به اصول ۲۲ و ۲۵ اشاره کرد. اصل ۲۲ مقرر می‌دارد:

حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز می‌کند.

همان‌گونه که ملاحظه می‌شود، مضمون این اصل مشابه اصول پیش‌بینی شده در اعلامیهٔ جهانی حقوق بشر و میثاق است. همچنین اصل ۲۵ مقرر می‌دارد:

بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون.

بی‌تردید قید ابزارهای ارتباطی در این اصل جنبهٔ تمثیلی دارد و الا آنچه منظور واضعان قانون اساسی بوده، رعایت حریم خصوصی افراد است و ظرف و ابزار در اینجا اهمیتی ندارد. ناگفته پیداست مفاد پیش‌بینی شده در قانون اساسی، در کنار اسناد بین‌المللی که کشورمان به آنها متعهد شده (نظیر میثاق) و به موجب مادهٔ ۹ قانون مدنی در حکم قانون عادی محسوب می‌شوند، همگی بر لزوم رعایت هرچه دقیق‌تر این اصول تأکید دارند.

حال باید دید با توجه به محدودیتهای پیشگیری وضعی از جرائم سایبر از یک سو و ضرورت به کارگیری آنها از سوی دیگر، در کنار لزوم رعایت موازین حقوق بشر، چه تدبیری باید اندیشید. بدیهی است نمی‌توان از کنار گذاشتن این اقدامات سخن گفت، زیرا همان‌گونه که گفته شد، اکنون ضرورت اتخاذ آنها تا حدی محرز گردیده که در کشورهایی که خود را مهد دموکراسی می‌دانند و به طور مستمر برای حفظ موازین حقوق بشر قوانینی را تصویب

می‌کنند، این ابزارها در سطح گسترده‌ای به کار می‌روند. بنابراین، گره کار در جای دیگری است. شاید بررسی یک مثال ملموس، ماهیت این قضیه را روشن‌تر نماید.

همان‌طور که می‌دانیم، مجازات حبس نه تنها در جامعهٔ ما که در بسیاری جوامع یکی از متداول‌ترین کیفرهاست. همچنین همهٔ ما کم و بیش با هزینه‌ها و آثار سوء آن آشنایی داریم. در وصف زندان همین بس که آن را دانشگاه مجرمان می‌دانند و به نظر می‌رسد آسیبی بالاتر از آن نمی‌توان برشمرد. به همین دلیل، در دهه‌های اخیر با انجام تحقیقات و مطالعات گسترده، ضمانت اجراهای جایگزینی مطرح شده که مجازاتهای جایگزین حبس یا مجازاتهای اجتماعی نامیده می‌شود*. حتی در نحوهٔ اجرای مجازات حبس نیز تحولات شگرفی به وجود آمده که از آن جمله می‌توان به آزادی مشروط، تعلیق مراقبتی، حبسهای خانگی، حبسهای آخر هفته و... اشاره کرد. بدیهی است تمامی این تحولات برای به حداقل رساندن آسیبها و آثار سوء مجازات، در عین حفظ آن، است و تاکنون در هیچ کشوری مشاهده نشده مجازات از صفحهٔ قوانین کیفری حذف گردد.

غرض از بیان این مثال اشاره به این نکته بود که ماهیت فضای سایبر به گونه‌ای است که پیشگیری وضعی یکی از تدابیر ناگریز و لازم‌الاجرا محسوب می‌شود. حتی در دنیای فیزیکی نیز این سخن صادق است، زیرا تنها گزینه‌ای است که می‌تواند دو ضلع مثلث جرم، یعنی فرصت و ابزار ارتکاب جرم را هدف قرار دهد. بنابراین، باید یک راه حل بینابین اتخاذ شود که به موجب آن ضوابطی که تدوین می‌گردد، بر اساس قواعد و مقررات حقوقی و همچنین ملاحظات حاکم بر فضای سایبر باشند تا علاوه بر صیانت از امنیت ملی و نظم، سلامت یا اخلاق عمومی، به دیگر موازین حقوق بشر، یعنی آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی نیز خدشه‌ای وارد نگردد. بی‌تردید مراجعه به تجارب دیگر کشورها با رعایت شرایط خاص کشورمان، چنانچه بر پایهٔ دیدگاههای واقع‌گرایانهٔ حقوقی ـ فنی باشد، می‌تواند نتایج مطلوبی را پدید آورد.

* شایان ذکر است در این خصوص نیز لایحه‌ای تحت عنوان «لایحهٔ مجازاتهای اجتماعی» در مجلس در دست بررسی است.

## کتابنامه


۱. ابراهیمی، شهرام، *پیشگیری از جرم*، ۱۳۸۳.

۲. انزالی، امیراسعد، *کامپیوترهای امروزی*، مجتمع فنی تهران، ۱۳۷٤.

۳. بسته‌نگار، محمد، *حقوق بشر از منظر اندیشمندان*، شرکت سهامی انتشار، ۱۳۸۰.

٤. جلالی فراهانی، امیرحسین، «پول‌شویی الکترونیکی»، فصلنامهٔ *فقه و حقوق*، شمارهٔ ٤، ۱۳۸٤.

۵. جلالی فراهانی، امیرحسین، «پیشگیری از جرائم رایانه‌ای»، مجلهٔ *حقوقی دادگستری*، شمارهٔ ٤۷، ۱۳۸۳.

٦. حسن‌بیگی، ابراهیم، «*آسیب‌شناسی شبکهٔ جهانی اطلاع‌رسانی اینترنت و ارائهٔ راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی*»، پایان‌نامهٔ دکتری، دانشگاه عالی دفاع ملی، ۱۳۸۲.

۷. حسینی، بیژن، «*جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن*»، پایان‌نامهٔ مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، ۱۳۸۲.

۸. دزیانی، محمد حسن، *جرائم کامپیوتری*، جلد اول، دبیرخانهٔ شورای عالی انفورماتیک، ۱۳۷٦.

۹. دزیانی، محمدحسن، «شروع جرائم کامپیوتری- سایبری»، *خبرنامهٔ انفورماتیک*، شمارهٔ ۹۳، ۱۳۸٤.

۱۰. دزیانی، محمدحسن، «مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کامپیوتری (سایبری)»، *خبرنامهٔ انفورماتیک*، شمارهٔ ۸۷، ۱۳۸۳.

۱۱. صفاری، علی، «مبانی نظری پیشگیری وضعی»، مجلهٔ *تحقیقات حقوقی*، شمارهٔ ۳٤-۳۳، ۱۳۸۰.

۱۲. کولیور، ساندرا و دیگران، آقایی، علی اکبر (مترجم)، «آزادی، حق و امنیت»، فصلنامهٔ *مطالعات راهبردی*، شمارهٔ ٤۹، ۱۳۷۹.

۱۳. نجفی ابرندآبادی، علی حسین، *تقریرات درس جرم‌شناسی (پیشگیری)*، دورهٔ کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیمی مهدی سیدزاده، نیم‌سال دوم تحصیلی ۸۲-۱۳۸۱.

۱٤.نجفی ابرندآبادی، علی حسین، *تقریرات درس جرم‌شناسی*، دورهٔ کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیمی رضا فانی، نیم‌سال اول تحصیلی ۸۳-۱۳۸۲.
۱۵.نجفی ابرندآبادی، علی‌حسین، «پیشگیری عادلانه از جرم»، *علوم جنایی، مجموعه مقالات در تجلیل از استاد آشوری*، انتشارات سمت، ۱۳۸۳.
۱٦.نمک‌دوست تهرانی، حسن، *اصول ژوهانسبورگ: امنیت ملی، آزادی بیان و دسترسی به اطلاعات*، از سایت ایران و جامعهٔ اطلاعاتی، مرکز پژوهش‌های ارتباطات، ۱۳۸٤.
۱۷.نیازپور، امیرحسن، «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، مجلهٔ *حقوقی دادگستری*، شمارهٔ ٤٥، ۱۳۸۲.



18. Board on Children, Youth and Families, *Technical, Business and Legal Dimensions of Protecting Children from Pornography on the Internet*, National Academy Press, 2004.
19. Casey, Eoghan, *Digital Evidence and Computer Crime*, Academic Press, 2001.
20. Department of Economic and Social Affairs, *Internet Governance: A Grand Collaboration*, 2004.
21. Department of Justice of the United States, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2002.
22. Graham J. H. Smith, *Internet Law And Regulation*, Sweet & Maxwell, 2002.
23. ITU, *Declaration of Principles*, Document WSIS-03/GENEVEA/DOC/4-E, 12 December 2003.
24. Shinder, Debra Littlejohn, *Scene of the Cyber Crime, Computer Forensics Hand Book*; Syngress Publication, 2002.
25. Sieber,u. *Computer Crime and Criminal Information Law- New Trends in the International Risk and Information Society*, 1995.
26. T. Kent, Stephen and I. Millett Lynette, *Who Goes There? Authentication Through the Lens of Privacy*, National Academy Press, 2004.

27. Thornburgh, Dick & s. Lin Herbert, Editors, *Youth, Pornography and The Internet*, National Academy Press, 2004.

28. Transparency International, *Global Corruption Report; Special Focus: Access to Information*, 2003.

29. United Nations, *International Review of Criminal Policy- United Nations Manual on the Prevention and Control of Computer-Related Crime*, Nos. 43 and 44.