سال پنجم/ شماره هشتم/ بهار ۱۳۸۹

جرائم سایبر

دکتر صدیقه بابران- استادیار و عضو هیات علمی گروه ارتباطات، دانشگاه آزاداسلامی واحد تهران مرکزی
s.babran@yahoo.com

انسیه محمودی- کارشناس ارشد علوم ارتباطات اجتماعی

ensiyemahmoodi@yahoo.com

چکیده

جوامع غربی با دومین انقلاب صنعتی روبرو هستند، یعنی انقلاب اطلاعات. این انقلاب، که ماشین را جایگزین فکر بشر می کند، در مقایسه با انقلاب صنعتی و ماشینی قرن نوزدهم که ماشین را جایگزین کار یدی کرد، قابلیت تغییر و تحول بیشتری دارد. انقلاب اطلاعاتی و ارتباطی؛ رسانه های جدیدی (مانند تلویزیون های ماهواره ای، بازی های کامپیوتری، دیسک های فشردهٔ موسیقی، فیلم و بالاخره اینترنت و محیط وب) را خلق کرده است که هر یک در ساختن دنیای ذهنی انسان معاصر نقشی خاص بر عهده دارند.

تجلی پیروزمند استفاده از رایانه نه تنها مزایایی دارد بلکه باعث شده است فعالیتهای سیستمهای رایانه ای و تامین امنیت آنها در کارهای تجاری، اداری و اجتماعی اهمیت حیاتی یابند. برای مثال در بعد تجاری، اثر عملیات مالی از طریق رایانه و به شکل پرداخت از حساب بانکی انجام می شود. به علاوه، شرکتهای تجاری بیشماری مهمترین اسرار خود را در حافظهٔ رایانه نگهداری می کنند. سیستمهای اداری پیشرفته نیز به فناوری رایانه و بانکهای داده وابسته اند. به علت همین وابستگی است که افزایش جرائم علیه سیستمهای پردازش داده طی دههٔ اخیر در بسیاری از کشورها خطری برای شرکتها، اقتصاد کشور و کل اجتماع محسوب می شود.

در سالهای اخیر این خطر، فزآینده شناخته شده و باعث شکل گیری دغدغه های ملی و بین المللی در مورد تهدید جدید که «جرائم سایبر» نام دارد شده است.

در این نوشتار سعی بر این است تا با تبیین مفهوم و ماهیت جرم سایبر، شناسایی مشخصه های این جرم، انواع مختلف آن، ارائهٔ الگوهای پیشگیری بین المللی و مبارزه با این جرم از طریق بررسی های علمی و حقوقی موجود در سطح ملی و بین المللی، مسیری در جهت برخورد با این معضلات، مشکلات و نواقص موجود در قوانین کشوری فراهم آید، با توجه به وسعت مباحث پیرامون هریک از این موضوعات سعی شده است اهم عناوین و مباحث مرتبط با جرائم سایبر به صورت شناخت موضوعات کلی، ارائه و یادآوری شود. امید است این نوشتار دستمایه ای باشد برای مسئولان و صاحبنظران تا نسبت به این مهم در سیاستگذاری ها، قانونگذاری ها و امور اجرایی مربوطه توجه ویژه ای مبذول کنند.

واژه های کلیدی: جرائم سایبر، پیشگیری از جرم، پیشگیری وضعی، آزادی بیان، جریان آزاد اطلاعات، حریم خصوصی، حقوق بشر

مقدمه

بشر در طول حیات خود با دوره های 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 صنعتی می‌تواند به آرزوهای خود دست یابد. لذا تمام همّ خود را در این راه نهاد و دوران صنعتی را رقم زد که اوج آنرا در سدهٔ نوزدهم میلادی شاهد هستیم.

اما از اواخر این قرن و اوایل قرن بیستم، زمزمه‌های محوریت یافتن عنصر دیگری شنیده شد. این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بود، به 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.

این عنصر با ارزش، «اطلاعات» نام دارد و حدود یک قرن می باشد که بشر تلاش خود را صرف تجلی آن در تمامی عرصه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی کرده است. بی‌تردید هر کاری ابزاری می‌خواهد و ابزار تحقق یک جامعهٔ اطلاعاتی، فناوری اطلاعات و ارتباطات است. دلیل اشاره به عامل ارتباطات در کنار اطلاعات، به لحاظ جایگاه ویژهٔ آن در توسعه و تکامل اطلاعات می باشد. ارتباط و به تبع آن ابزارهای ارتباطی، از همان ابتدا از عناصر حیاتی محسوب می‌شدند و می‌توان گفت اگر وجود نداشتند، بشر هیچگاه نمی‌توانست به این حد از رشد و بالندگی برسد (asey , 2001 : 8) .

دو فناوری در عرصهٔ فناوری اطلاعات و ارتباطات نقش تعیین‌کننده‌ای به عهده داشته‌اند که عبارتند از: رایانه و مخابرات. هدف از اختراع رایانه، تسریع و تسهیل پردازش اطلاعات بود که به خوبی به ثمر نشست و مخابرات نیز به عنوان مهمترین ابزار ارتباطی، در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است.

از حدود نیم قرن اخیر، به تدریج با کشف قابلیتهای شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصهٔ فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که از دههٔ ۹۰ میلادی به بعد، تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها که خود از بسیاری سیستمهای رایانه‌ای متصل به یکدیگر تشکیل شده‌اند، به مدد فناوریهای پیشرفتهٔ مخابراتی با یکدیگر ارتباط برقرار کرده و فضایی با ویژگیهای کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند که عده‌ای آن را فضای مجازی نامیده‌اند و عده‌ای هم عنوان فضای سایبر را برای آن برگزیده‌اند.

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

قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترسی غیرمجاز به داده‌ها یا سیستمها یا پخش برنامه‌های مخرب نظیر ویروسها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می‌شود (asey, 2001: 8).

همانگونه که ملاحظه می‌شود، به لحاظ امکان سوء استفادهٔ دوجانبه‌ای که از فضای سایبر وجود دارد، ضروری است برای آن چاره‌ای اندیشه شود. با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارتند از: اقدامات کیفری و غیرکیفری. در زمینهٔ اقدامات کیفری سعی می‌شود از طریق جرم‌انگاری، هنجارشکنی ها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفری گذشته، ارعاب‌انگیزی موثری دربارهٔ مجرمان بالقوه یا مکرر صورت گیرد تا به این ترتیب، از ارتکاب جرم بازداشته شوند (نیازپور، ۱۳۸۲: ۱۲۴).

اما رویکرد دوم که در بستر جرم‌شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی و .... پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. در این زمینه، تاکنون الگوهای مختلفی در عرصهٔ جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. از مهمترین و موثرترین این الگوها می‌توان به پیشگیری اجتماعی و پیشگیری وضعی 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، 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 یا انگیزه است (نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸).

راجع به این مدل (پیشگیری وضعی) که موضوع این مقاله 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 در بر می‌گیرند، 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، 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 فرآیند 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.

فضای سایبر چیست

برای درک مفهوم جرائم سایبر، درک تعریف سایبر اسپیس و ویژگی‌های آن ضروری است.

واژهٔ سایبر از لغت یونانی Kybernetes به معنی فرمانروایی و حکومت مشتق شده است. نخستین بار اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام «توربرت وینر» در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین انسان و ماشین» در سال ۱۹۴۷ به کار برده شده است. سایبرنتیک علم کنترل و انتقال پیام ها در سیستم‌های انسانی و ماشینی می باشد (معتمدنژاد، ۱۳۸۳: ۴۲).

واژهٔ «فضای سایبر» را نخستین بار «ویلیام گیبسون» نویسندهٔ داستان علمی تخیلی در کتاب نورومانسر در سال ۱۹۸۴ به کار برده است.

مفهوم سایبر اسپیس چیز جدیدی نیست. سایبر اسپیس با اختراع «الکساندر گراهام‌بل» یعنی تلفن در سال ۱۸۷۶ پدید آمد (صدیق بنای،۱۳۸۹).

سایبر اسپیس را می توان چنین تعریف کرد:

محیطی است مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراههای اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طور کلی هر آنچه که در کرهٔ خاکی به صورت ملموس و فیزیکی وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس استفاده‌کنندگان و کاربران می‌باشند و از طریق کامپیوتر اجزاء آن و شبکه‌های بین‌المللی به هم مرتبط می‌باشند.

جرائم سایبری

جرائم سایبر زیر مجموعهٔ جرم کامپیوتری است. اصطلاح جرم سایبر به جرائم جنایی ارتکابی با استفاده از اینترنت یا سایر شبکه‌های کامپیوتری اطلاق می‌شود.

جرم به معنای چالش مجرم برای چیرگی بر قواعد و آزمایشی برای ارزش ها و تعهدهای مردم مطیع قانون است. بی شک با تغییر جامعه، شکل جرائم نیز تغییر می کند. فناوری های جدید، فرصتهای جدیدی را برای مجرمان پدید می آورد و فناوری های اطلاعاتی و ارتباطاتی، جرائم اطلاعاتی و ارتباطاتی را به دنبال دارد. منظور از جرائم جدید هم اشکال جدید جرائم قدیمی و هم جرائمی بی سابقه است که فقط در محیط رایانه ای امکان بروز دارد.

ویژگی های جرائم سایبر

۱. تخصصی و علمی بودن

این دست از جرائم عمدتا از سوی افراد آگاه به علوم رایانه ای رخ می دهد، که در اغلب موارد عمدی و از روی تجربه یا عداوت صورت می گیرد. لذا کمتر می توان کسانی را که دارای اطلاعات رایانه ای نیستند در زمرهٔ بزهکاران رایانه ای دید. (به ویژه جرائمی، از قبیل سابوتاژ، دسترسی غیر مجاز، جاسوسی و...).

از سوی دیگر نیاز به ابزار و نرم افزارهای خاصی است که کار با آنها تنها از عهدهٔ برخی از متخصصان بر می آید. از این رو در مرحلهٔ کشف این دسته از جرائم نیاز به متخصصان رایانه ای است.

۲. دارای حیثیت عمومی و خصوصی بودن

جرائم مجازی را نمی توان منحصر در یک حیث نمود، چرا که از یک طرف در رابطه با دولت و فضای عمومی جامعه است و از طرف دیگر به اشخاص حقیقی یا حقوقی خصوصی خسارت مادی و معنوی می زند و احیانا حریم خصوصی افراد را هدف می گیرد. با توجه به پیشرفت علم وگستردگی کاربرد اینترنت در جهان امروز، در بسیاری از کشورهای جهان مقررات و شرایط ویژه ای برای حمایت از حقوق کاربران اینترنتی وضع شده است و این مقررات بیش از آنکه جنبهٔ کنترل و نظارت توسط دولت ها داشته باشد به طور خاص در زمینهٔ حمایت از کاربران اینترنت و شهروندان آن کشورها است.

در این راستا می توان جرائم امنیتی؛ همچون جاسوسی در فضای مجازی، حملات تروریستی، تخریب

داده ها، اختلال در سیستم های رایانه ای و داده ها و... جرائم فرهنگی؛ همچون هرزه نگاری و دیگر جرائم محتوایی را واجد حیثیت عمومی دانست (United Nations, 1992).

۳. پیچیدگی خاص

فضای مجازی، دنیای بیکرانی از امکانات و قابلیت های بیشمار است که بدون محدودیت، در دسترس همگان قرار دارد و هر فرد با هر انگیزه ای می تواند از این موهبت استفاده کند. این حجم گسترده از امکانات، قدرت پیچیده کردن نحوهٔ ارتکاب جرم و گمنام کردن هویت مجرم را افزایش می دهد، که این خود دستگیری و تعقیب مجرمان را دشوار ساخته است. هکرها و کرکرها با استفاده از شیوه های مختلف و به صورت گمنام اطلاعات را مورد حمله قرار می دهند، بدون اینکه ردی ازخود باقی گذارند.

۴. دشوار بودن تعیین صلاحیت کیفری

با توجه به نوظهور بودن جرائم رایانه ای، هنوز در سطح بین المللی قانون یا عرف جدی در مورد صلاحیت کیفری در این جرائم شکل نگرفته و در سطح ملی نیز دسته ای از کشورها، چون آلمان همان قوانین رایج در دیگر جرائم را در این جرائم حاکم کرده اند. برخی کشورها اقدام به تصویب قوانین جدیدی کرده اند که در این میان دو رویهٔ کلی حاکم است:

الف. محل استقرار سیستم های رایانه ای به عنوان محل ارتکاب جرم مجازی (کشورهایی چون سنگاپور و مالزی)؛ ب. محل حضور بارگذار و پیاده ساز شبکه ای به عنوان محل ارتکاب جرم، (همچون ایالت آرکانزاس و کارولینای شمالی).

با وجود چنین رویکردهایی مشکل اصلی، تعیین هویت مجرم است؛ زیرا بر فرضی که نظریهٔ محل استقرار سیستم را شناسایی کنیم، باز هویت کاربر مجرمی که از آن استفاده کرده و یا حتی یافتن محل استقرار رایانه دشوار است و در نظر دوم نیز مشکل هویت مجرم همچنان لاینحل است. در نتیجه تعیین صلاحیت کیفری همچنان دشوار می نماید (United Nations, 1992).

۵. جهانی بودن

فناوری اطلاعات و ارتباطات الکترونیکی، به دلیل گستردگی در سراسر جهان، از چند جهت جرائم مجازی را از سایر جرائم ممتاز می کند.

در جرائم امنیتی و تروریستی که مجرمان درصدد انعکاس هرچه بیشتر اقداماتشان هستند، فضای مجازی، محیط مطلوبی برای اینگونه اقدامات است؛ زیرا که هر اختلالی در آن به خوبی انعکاس جهانی داشته و به راحتی اعتبار یک کشور یا مجموعهٔ خاصی را لکه دار می کند. در جرائمی، چون کلاهبرداری، فرد می تواند از کشوری دور دست به اشکال مختلف فرد دیگری را در کشوری دیگر فریب دهد. در جرائمی چون اختلال در داده ها، اختلال در سیستم، جعل دسترسی و شنود و دریافت غیرمجاز و... مجرم به راحتی می تواند ابزار و نرم افزارهای مورد نیاز را جهت ارتکاب جرم چه از طریق اینترنت و غیره تهیه کند و یا با افراد متخصص در این جرائم همکاری کند (ibid).

طبقه بندی جرائم رایانه ای - سایبری

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، براساس نسلهای تکاملی سیستمهای رایانه‌ای نبوده و معیارهای دیگری مدنظر قرار گرفته است.

۱. نسل اول جرائم رایانه‌ای: همانگونه 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 فوریه ۱۹۴۶ چرخانیده شد. در آن زمان، عمده 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 می شد، بیشتر رویکردی

امنیتی داشت (دزیانی، ۱۳۷۶: ۷۴).

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 ۱۹۸۶ راجع به جرائم 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 دیگر، جعل و ایجاد اختلال به قصد جلوگیری از کارکرد سیستمهای رایانه‌ای یا مخابراتی صورت گرفته باشد.

ب. نقض حقوق انحصاری مالک یا برنامه ی رایانه‌ای حفاظت شده به قصد بهره‌برداری تجاری از آن و ارائه به بازار.

پ. 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، ۱۳۸۴: ۷).

همانگونه که ملاحظه می‌شود، این توصیه‌نامه که مبنای قانونگذاری های بعدی قرار گرفت، کاملاً در مسیر تامین 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 خودپیشگیری را در مباحث جرم‌شناختی آن زمان بی‌تاثیر دانست.

۲. نسل دوم جرائم رایانه‌ای: این نسل از جرائم پل ارتباطی میان نسل اول و سوم بوده و 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 بوده 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: ۴).

به این ترتیب، سیستمهای رایانه‌ای در صورتی در دوران نسل دوم، ایمن محسوب می‌شدند که داده‌های موجود در آنها از سه مولفه برخوردار بودند:

الف محرمانگی: داده‌ها در برابر افشا یا دسترسی غیرمجاز حفاظت شده باشند؛ ب. تمامیت: داده‌ها در برابر هرگونه تغییر یا آسیب حفاظت شده باشند؛ و پ. دسترس‌پذیری : با حفظ کارکرد مطلوب سیستم، داده‌ها همواره در دسترس مجاز قرار داشته باشند.

هم اکنون، این سه مولفه در حوزهٔ جرائم نسل سوم از جایگاه ویژه‌ای برخوردارند و حتی در اسناد قانونی به صراحت به آنها اشاره شده است (Siber, 1995).

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 عبارتند از: دسترسی غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم و سوء استفاده از دستگاهها.

این دوره با وجود عمر کوتاه خود، تاثیر 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.

۳. نسل سوم جرائم رایانه‌ای: از اوایل دهۀ ۹۰م. با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصۀ بین‌الملل و به ویژه ظهور شبکۀ جهانی وب که به فعالیت این شبکه‌ها ماهیتی تجاری بخشید، بحث راجع به ابعاد گوناگون فضای سایبر به ویژه مسائل حقوقی آن، وارد مرحلۀ جدیدی شد. زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقه‌ای، محلی و در حوزه‌های محدودی نظیر سیستمهای تابلوی اعلانات که عمدتاً جهت بارگذاری و پیاده‌سازی برنامه‌ها، پیامها و همچنین ارتباطات پست الکترونیک به کار می‌رفتند به فعالیت می‌پرداختند. به همین دلیل، همانند آنچه در سند 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 خصیصۀ فضای سایبر، بین‌المللی بودن یا به عبارت بهتر فرامرزی بودن آن است. شبکه‌های پیشین به صورت محلی یا حداکثر منطقه‌ای قابل بهره‌برداری بودند. اما به مدد سیستمهای ارتباطی بی‌سیم و باسیم، نظیر شبکه‌های ماهواره‌ای یا خطوط فیبر نوری، این امکان فراهم گشته است.

ب. برخورداری از طریق شبکه‌های اطلاع‌رسانی رایانه‌ای، یکی از جلوه‌های نوین این فضاست که پیش از این حداقل به این شکل وجود نداشت.

پ. دیگر مزیتی که می‌توان برای فضای سایبر یا به عبارت بهتر شبکه‌های اطلاع‌رسانی رایانه‌ای کنونی برشمرد، ظرفیت بالای آنهاست؛ تا حدی که ارائۀ خدمات ذخیرۀ داده‌ها در نقاط دوردست به یکی از فعالیتهای متداول در فضای سایبر تبدیل شده است (Usdoj, 2002: 52).

ویژگیها و خصوصیات منحصر به فرد این فضا، همگی باعث شده‌اند جرائم رایانه‌ای که پیش از این گسترۀ محدودی را در بر می‌گرفتند و خسارات نسبتاً ناچیزی را هم به بار می‌آوردند، اکنون به جرائم سایبری تبدیل شوند که به راحتی امکان ارزیابی گسترۀ این جرائم و خسارات ناشی از آنها وجود ندارد. آنچه امروز تحت عنوان تروریسم سایبر مورد توجه قرار گرفته، از همین واقعیت نشات می‌گیرد. تعرض به

شبکه‌های حیاتی متصل به فضای سایبر، نظیر بیمارستانها، نیروگاههای بزرگ و تخریب آنها می‌تواند خساراتی معادل جنگهای تسلیحاتی یا حتی فراتر از آن را به بار آورد. هم اکنون بحث هرزه‌نگاری در عرصهٔ اینترنت، به ویژه هرزه‌نگاری کودکان ، 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 تا تعرض به شبکه‌های بنگاههای اقتصادی و بانکها، از جمله جرائم شایع در این فضا هستند (جلالی فراهانی، ۱۳۸۴: ۱۰۹).

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، 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، در ادامه به بررسی واکنش های کشورها و سازمان های مختلف جهانی در رابطه با جرائم سایبر پرداخته می شود.

واکنش های جهانی در رابطه با جرائم سایبر

اول: واکنش تقنینی کشورها در مورد جرائم سایبر

تا دهۀ ۱۹۷۰ میلادی کشورهای مختلف در چارچوب قوانین سنتی با جرائم سایبر برخورد می‌کردند؛ اما پیشرفت فناوری اطلاعات، تنوع و کثرت سوء استفاده‌هایی که از این فناوری به عمل آمد، حقوق جزای سنتی کشورها را به چالش کشید.

یکی از علل به چالش کشیده شدن حقوق جزای سنتی این بود که قوانین کیفری کشورها تا قبل از شیوع جرائم سایبری غالباً به حمایت از اهداف و موضوعات ملموس می‌پرداختند. با رشد فناوری رایانه، اطلاعات و داده‌های رایانه‌ای به عنوان یک موضوع غیرملموس، غیر قابل رؤیت و با ارزش، موضوع جرم سایبری قرار گرفت. حقوق جزای ماهوی که حمایت از ارزشها را بر عهده دارد در برابر تجاوز و تعدی به این ارزشها با نگرشی جدید واکنش نشان داد. این نگرش طی مراحلی موجب اصلاح سیستم‌های قضایی شد.

پروفسور «زیبر آلمانی» (پدر حقوق کیفری اطلاعات) به پنج مرحله از این مراحل به ترتیب زیر اشاره کرده است:

اولین مرحله، اصلاح سیستم‌های قضایی غرب بود، که در حمایت از محرمانگی (حقوق خصوصی و فردی) در دهه‌های ۱۹۷۰و۱۹۸۰ ظاهر شد. این تقنین، واکنشی در برابر چالش‌های جدید مربوط به حقوق خصوصی و فردی بود که به واسطۀ امکانات جمع‌آوری، ذخیره‌سازی و انتقال داده‌ها از طریق تکنولوژی جدید با مسائل جدید مواجه شده بود. لذا قوانینِ جدیدِ حمایت از داده‌ها، در حمایت از حقوق خصوصی و فردی شهروندان از جنبۀ اداری، مدنی و کیفری در کشورهای مختلف تصویب شد. قوانین کانادا و استرالیا در سال ۱۹۷۲، سوئد ۱۹۷۳، آمریکا ۱۹۷۴، آلمان۱۹۷۷، فرانسه، نروژ، اتریش و دانمارک ۱۹۸۸، ایسلند ۱۹۸۱، بریتانیا ۱۹۸۴، ایرلند، ژاپن و هلند ۱۹۸۸ تصویب شده‌اند و بعضاً این قوانین جدید مورد اصلاح قرار گرفته‌اند (خرم آبادی، ۱۳۸۸).

مرحلهٔ دوم از موج قوانین اصلاحی ناظر بر جرائمِ اقتصادی مرتبط با رایانه در اواخر دههٔ ۱۹۷۰ و دههٔ ۱۹۸۰ است. آمریکا درسال ۱۹۷۶ (در سطح ایالات)، ایتالیا ۱۹۷۸، استرالیا ۱۹۷۹، بریتانیا۱۹۸۱، آمریکا ۱۹۸۴ (درسطح فدرال)، دانمارک وکانادا ۱۹۸۵، آلمان۱۹۸۶، سوئد و شیلی۱۹۸۷، اتریش، ژاپن و نروژ ۱۹۸۷، فرانسه و یونان ۱۹۸۸، فنلاند و بریتانیا ۱۹۹۰ قوانینی در خصوص جرائم رایانه‌ای اقتصادی وضع کرده‌اند که بعضی از این قوانین چند بار اصلاح شده‌اند.

مرحلهٔ سوم قوانین اصلاحی در دههٔ ۱۹۸۰ ناظر بر جرائم مالکیت معنوی مرتبط با رایانه است.

بعد از اینکه برنامه‌های رایانه‌ای در دههٔ ۱۹۷۰ تحت حمایت حق اختراع قرار گرفت، قوانین اصلاحی برنامه های رایانه‌ای را مشمول مالکیت معنوی (کپی رایت) قرار دادند. کشور آمریکا در سال ۱۹۸۰، مجارستان ۱۹۸۳، استرالیا، هند و مکزیک ۱۹۸۴، شیلی، آلمان، فرانسه، ژاپن و انگلستان در ۱۹۸۵، برزیل، کانادا و اسپانیا در ۱۹۸۸، دانمارک، کلمبیا و سوئد ۱۹۹۰ و نروژ در ۱۹۹۱ قوانین مربوط به مالکیت معنوی (کپی رایت) خود را اصلاح کرده‌اند و پیشرفت‌های کلی در زمینهٔ حمایت جزایی از مالکیت معنوی نیز حاصل شده است.

مرحلهٔ چهارم اصلاحات بین‌المللی قوانین، در مورد قوانین آیین‌دادرسی است. بسیاری از کشورها مانند آمریکا، کانادا، آلمان و دیگر کشورهای اروپایی قوانینی را در خصوص تفتیش و توقیف داده‌های رایانه‌ای وضع کرده‌اند.«در این خصوص می‌توان به تدوین قوانین انگلیس در سال ۱۹۸۴، دانمارک ۱۹۸۵، آمریکا ۱۹۸۶ و هلند ۱۹۹۴ اشاره کرد».

مرحلهٔ پنجم اصلاح قوانین، در مورد جرائم مربوط به محتواست. به عنوان مثال بسیاری از کشورها قوانینی وضع کردند که تهیه، توزیع، عرضه و نگهداری پورنوگرافی (هرزه نگاری) کودکان از طریق سیستم‌ها و شبکه‌های رایانه‌ای را جرم تلقی کرده است.

در سال ۲۰۰۰ موسسهٔ بین‌المللی «مک کانل» مطالعه‌ای در مورد وضعیت قوانین وضع شده در ارتباط با جرائم سایبری در چهار گوشهٔ جهان به عمل آورده است. این موسسه از کشورها خواسته است که

چنانچه قوانین و یا پیش‌نویس قوانینی در این خصوص دارند ارسال کنند، در غیر این صورت اعلام نمایند که هیچ اقدام مثبتی انجام نداده‌اند (همان).

کشورهایی که قوانین خود را ارائه کرده‌اند به گونه‌ای مورد ارزیابی قرار گرفته‌اند که مشخص شود آیا قوانین جزایی آنها فضای شبکه‌های رایانه‌ای را شامل می‌شود یا نه؟ و آیا انواع جرائم سایبری را پوشش می‌دهد یا نه؟

۳۳ کشور (از بین بیش از ۵۰ کشور) مورد بررسی تا آن تاریخ نسبت به روز آمد کردن قوانین خود به منظور برخورد با انواع جرائم رایانه‌ای هیچ اقدامی انجام نداده بودند ولی اکثراً در حال تهیهٔ پیش‌نویس قوانین بودند. این کشورها عبارتند از:

ایران، آلبانی، بلغارستان، بوروندی، کوبا، دومینیکن، مصر، اتیوپی، فیجی، گامبیا، مجارستان، اردن، نیکاراگوئه، قزاقستان، لیتوانی، لبنان، لسوتر، مالت، مولداوی، مراکش، زلاندنو، نیجریه، رومانی، آفریقای جنوبی، ویتنام، یوگسلاوی، زامبیا، زیمباوه. ۱۰ کشور از کشورهای مورد بررسی برای برخورد با حداکثر پنج نوع از جرائم سایبری، قانون وضع کرده‌اند که عبارتند از: برزیل، کانادا، شیلی، چین، چک، دانمارک، مالزی، لهستان، اسپانیا و فرانسه. ۹ کشور نیز برای برخورد با بیش از شش نوع از انواع جرم سایبری، قانون وضع کرده‌اند که عبارتند از: آمریکا، انگلیس، ترکیه، پرو، ژاپن، موریس، استونی، استرالیا و هند. کشور فیلیپین برای اکثر جرائم سایبری قانون وضع کرده است (خرم آبادی، ۱۳۸۸).

از نیمهٔ دوم دههٔ ۱۳۷۰ شمسی و بالاخص از ابتدای دههٔ ۱۳۸۰ که استفاده از رایانه های شخصی توسط سازمانهای اداری، موسسات خصوصی و افراد حقیقی در ایران گسترش یافته و دسترسی به خدمات متعدد اینترنت امکانپذیر شده، ارتکاب جرائم سایبری در کشورمان نیز از رشد نسبتا سریعی برخوردار شده است. اشاعهٔ فحشا و منکرات، انتشار عکس ها، تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسائل قومی و نژادی، انتشار مطالب نژاد پرستانه، انتشار اسناد و مسائل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا نسبت به مقامات دولتی، اشخاص حقیقی و

حقوقی، سرقت ادبی و غیره از جمله جرائمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب سایتها و وبلاگها، پست الکترونیک، گروههای خبری، چت (گپ زدن) و سایر سرویسهای اینترنت به وقوع پیوسته اند. قانونگذار در سال ۱۳۷۹ در برابر برخی از جرائم سایبری واکنش نشان داده و با الحاق تبصرهٔ سه به مادهٔ یک قانون مطبوعات مقرر داشته «کلیهٔ نشریات الکترونیکی مشمول مواد این قانون است».

اولین واکنش قانونی ایران در برابر بعضی از جرائم سایبری، قانون اصلاح قانون مطبوعات مصوب ۱۳۷۹/۱/۳۰ مجلس شورای اسلامی می باشد که در تاریخ ۱۳۷۹/۲/۷ مورد تائید شورای نگهبان قرار گرفته است (خبرنامه کانون وکلای کرمانشاه: ۳۲).

دومین واکنش قانونی کشور ما در مقابل این نوع جرائم، از طریق وضع «قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای» به عمل آمد. این قانون در تاریخ ۱۳۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی رسید. مادهٔ ۱۳ قانون مذکور نقض حقوق پدید آورندگان آن دسته از نرم افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است.

سومین عکس العمل قانونگذار ایران در مقابل جرائم سایبری در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد. به موجب مادهٔ ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و افشاء غیر مجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آنرا ندارند، سرقت و یا تخریب حاملهای داده و سوء استفادهٔ مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان، جرم تلقی و مرتکب، حسب مورد به مجازات جرم ارتکابی محکوم می‌شود.

چهارمین واکنش قانونی مرتبط با جرائم سایبری از طریق تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد۷۷، ۷۶، ۷۵، ۷۴، ۶۹،۶۸،۶۷،۶۶

این قانون، کلاهبرداری، جعل، دستیابی و افشاء غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و غیره... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است.

هر یک از چهار قانون فوق الذکر در بستر خاص خود قابلیت اعمال دارند. مثلا قانون مطبوعات صرفاً نسبت به جرائم سایبری ارتکابی در قالب نشریات الکترونیکی، قانون مجازات نیروهای مسلح صرفا در مورد بعضی از جرائم سایبری نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم سایبری ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند (همان).

برای مقابله با سایر سوء استفاده‌های سایبری مانند سوء استفاده از محیط سایبر به منظور نفوذ به حریم خصوصی افراد، تخریب، سرقت، توقف و تغییر داده‌هایی که فاقد شرایط مقرر در قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای هستند، سوءاستفاده‌های مالی رایانه‌ای خارج از بستر تجارت الکترونیک و سایر سوء استفاده های رایانه‌ای، نیاز به یک قانون جرائم رایانه‌ای پیشرفته و جامع الاطراف می‌باشد.

شورای عالی توسعهٔ قضایی قوهٔ قضائیه، پیش نویس قانون جرائم رایانه‌ای و آئین دادرسی آنرا در سال ۱۳۸۲ تهیه و طی جلسات متعددی با حضور حقوقدانان و متخصصان امور رایانه مورد بررسی قرار داد، تا پس از تصویب رئیس قوهٔ قضائیه به عنوان لایحهٔ جرائم رایانه‌ای از طریق هیات دولت به مجلس شورای اسلامی تقدیم شود. با این حال، سرعت تصویب و لازم‌الاجرا شدن قوانین حمایتی رایانه‌ای به هیچوجه با توسعهٔ کمی و کیفی این فناوری در کشورمان تناسب نداشته است و گام‌های نخستین قانونگذاری نیز شامل حوزه‌های محدودی نظیر حمایت از مالکیت فکری رایانه‌ای می‌شده که البته آنها نیز تمامی جنبه‌های حمایتی را در بر نمی‌گیرند. در همین راستا و با هدف تدوین یک قانون کیفری نسبتا جامع برای مقابله با سوء استفاده‌های سایبری، شورای عالی توسعهٔ قضایی قوهٔ قضاییه در ابتدای سال ۱۳۸۱ با همکاری شورای عالی اطلاع‌رسانی وقت، طرح تدوین لایحهٔ مبارزه با جرائم رایانه‌ای را آغاز کرد. پس

از آن، پیش‌نویس مذکور تقدیم رئیس وقت قوهٔ قضاییه شد که در شورای عالی مسئولان قضایی مورد بررسی قرار گرفت و پس از تائید آن از سوی ایشان، تقدیم دولت شد که دولت نیز آنرا به مجلس شورای اسلامی تقدیم کرد. در سال ۱۳۸۴، کمیتهٔ تخصصی تشکیل شده در کمیسیون حقوقی و قضایی مجلس شورای اسلامی، متشکل از تعدادی از نمایندگان کمیسیون، لایحه را بررسی و تصویب کردند، لیکن نوبت به طرح لایحه در کمیسیون نرسید و عملا بررسی آن به دورهٔ هشتم مجلس شورای اسلامی موکول شد. در شهریورماه ۱۳۸۷ کمیسیون حقوقی و قضایی مجلس به طور جدی لایحه را بررسی و تصویب کرد و برای تصویب نهایی به صحن علنی مجلس ارجاع داد که تا پایان آن سال ادامه یافت و پس از یکبار ارجاع به شورای نگهبان و رفع ایرادهای مبتنی بر شرع و قانون اساسی وارده از سوی آن شورا، نهایتا در تیرماه سال ۱۳۸۸ برای دولت از سوی مجلس شورای اسلامی ابلاغ شد. این قانون مصوب، مشتمل بر سه بخش اصلی می باشد که به ترتیب به جرائم و مجازات‌ها، آیین دادرسی و سایر مقررات، اختصاص یافته است (خبرنامه کانون وکلای کرمانشاه: ۳۲).

دوم: فعالیت سازمانهای بین‌المللی در خصوص جرائم سایبری

به لحاظ خصیصهٔ فراملی جرائم سایبری، اقدامات بین‌المللی فراوانی برای دستیابی به سیاست جنایی بین‌المللی ناظر بر این جرائم انجام شده است. فعالیت‌های بین‌المللی برای مبارزه با جرائم سایبری از دههٔ ۱۹۸۰ شروع شد. سازمان‌هایی مانند سازمان همکاری و توسعهٔ اقتصادی، انجمن بین‌المللی حقوق جزا، سازمان ملل متحد، اینترپل، شورای اروپا و مجمع کشورهای شرکت‌کننده در کنفرانس بین‌المللی مبارزه با جرائم سایبر (۲۰۰۱) بوداپست، اقدامات ارزنده‌ای را در این خصوص انجام داده‌اند.

۱. سازمان همکاری و توسعهٔ اقتصادی

اولین کوشش بین‌المللی در مورد بحث و بررسی مشکلات حقوق جزا در برابر جرم سایبری توسط سازمان همکاری و توسعهٔ اقتصادی صورت پذیرفت. این سازمان در سال ۱۹۷۷ شروع به اتخاذ رهنمودهایی ناظر به حمایت از حقوق فردی و جریان فراملی داده‌های شخصی کرد. کمیتهٔ تخصصی این سازمان، کار خود

را در زمینهٔ ایجاد هماهنگی بین‌المللی بین قوانین کیفری برای مبارزه با جرائم اقتصادی رایانه‌ای شروع کرد و در سال ۱۹۸۹ لیستی از سوء استفاده‌های رایانه‌ای را ارائه داد. در سال ۱۹۸۹ این سازمان کارش را در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد (خرم آبادی، ۱۳۸۸).

۲. سازمان ملل متحد

در هفتمین کنگرهٔ سازمان ملل متحد در سال ۱۹۸۵ «جرم سایبری» از جمله موارد مطروحه در گزارش دبیر کل این سازمان بود. به عنوان برنامهٔ تدارکاتی هشتمین کنگرهٔ سازمان ملل متحد، اجلاس مقدماتی منطقه‌ای آسیا و اقیانوس آرام، نگرانی خود را دربارهٔ آثار پیشرفت‌های تکنولوژی و انعکاس آن در جرائم سایبر اعلام داشت. در اجلاس مقدماتی منطقه‌ای اروپا پیشنهاد شد که مبارزهٔ بین‌المللی با جرائم رایانه‌ای از سوی هشتمین کنگرهٔ سازمان ملل متحد و کنگره‌های پس از آن مورد حمایت و توجه قرار گیرد. در دوازدهمین اجلاس عمومی کنگرهٔ هشتم که در سال ۱۹۹۰ برگزار شد، نمایندهٔ کانادا پیش‌نویس قطعنامه‌ای را در مورد جرائم رایانه‌ای تسلیم کنگره کرد. در سیزدهمین اجلاس عمومی کنگرهٔ هشتم، قطعنامهٔ مذکور پذیرفته شد. در این قطعنامه از کشورهای عضو خواسته شده است که به تلاشهای خود در زمینهٔ مبارزه با جرائم رایانه‌ای از طریق مدرنیزه کردن قوانین و دادرسی های ملی، ارتقاء ضوابط پیشگیرانه و امنیتی رایانه، اتخاذ تدابیری برای ایجاد حساسیت در مردم و قوهٔ قضائیه برای جلوگیری از جرائم رایانه‌ای و... شدت بخشند و از دبیر کل سازمان خواسته شد تا موضوع انتشار یک نشریهٔ فنی در مورد جلوگیری و تعقیب جرائم رایانه‌ای را مد نظر قرار دهد.

مجمع عمومی سازمان ملل متحد در قطعنامهٔ شماره ۴۵/۱۲۱ خود اسناد و قطعنامه‌های مصوبهٔ هشتمین کنگره را پذیرفت و از دولتها خواست تا در تبیین قوانین و دستورالعمل‌های تعیین‌کنندهٔ خط مشی خود و براساس شرایط اقتصادی، اجتماعی، حقوقی، فرهنگی و سیاسی در کشور از قطعنامه‌های مزبور تبعیت کنند

۳. انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا که یک سازمان غیر دولتی است در سال ۱۹۹۰ جرم سایبری را به عنوان یک موضوع مورد بحث برای اعضای خود مطرح کرد. در سال ۱۹۹۲ یک نشست مقدماتی پیرامون این جرم در دانشگاه ورتسبورگ آلمان برگزار و قطعنامه‌ای در مورد فهرست جرائم رایانه‌ای صادر کرد. در سال ۱۹۹۴ در نشست نهایی خود در ریودوژانیرو و در نشستهای بعدی خود مصوباتی در این خصوص داشته است (همان).

۴. یونسکو

در اجلاس سال ۱۹۹۹ یونسکو در پاریس که با حضور ۳۰۰ نفر از متخصصان در حوزهٔ مراقبت و محافظت از اطفال، متخصصان اینترنت و تهیه‌کنندگان خدمات اینترنتی و... به منظور بررسی راههای مبارزه با سوء استفادهٔ جنسی از اطفال، پدوفیلی (کودک دوستی به منظور سوء استفادهٔ جنسی) و هرزه نگاری اطفال در اینترنت تشکیل شد، اعلامیهٔ مورخه ۱۹۹۹/۱/۱۹ یونسکو که یک برنامهٔ عملی برای مبارزه با جرائم اینترنتی علیه اطفال می باشد، صادر شد.

۵. شورای اروپا

شورای اروپا در سال ۱۹۸۵ موضوع جرم رایانه ای را از طریق یک کمیتهٔ تخصصی مورد مطالعه و بررسی قرار داده است. کمیتهٔ منتخب کارشناسان جرم رایانه‌ای کار خود را در سال ۱۹۸۵ شروع و در سال ۱۹۸۹ یک توصیه نامه و یک گزارش به کمیتهٔ اروپایی مسائل ناشی از جرم ارائه کرد. کمیته نیز پس از تصویب، آنرا به کمیتهٔ وزرای شورای اروپا فرستاد و در سپتامبر ۱۹۸۹ به عنوان یک توصیه نامه تحت عنوان R(89) 9 مورد تصویب نهایی قرار گرفت. توصیه نامهٔ دیگری در زمینهٔ آیین‌دادرسی جرائم فناوری اطلاعات در سال ۱۹۹۵ تحت عنوان توصیه نامهٔ R(95)13 توسط این شورا تصویب شده است.

کمیتهٔ وزراء شورای اروپا درسال ۱۹۹۷ کمیتهٔ دیگری به نام کمیتهٔ متخصصان جرائم سایبر را تشکیل

داد. این کمیته پیش‌نویس کنوانسیون جرائم سایبر و گزارش توجیهی آنرا در سال ۲۰۰۰ تهیه کرد. کنوانسیون جرائم سایبر درسال ۲۰۰۱، در یک کنفرانس بین‌المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (آمریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل شد، به تصویب رسید که کاملترین سند بین‌المللی در مورد جرائم رایانه‌ای می‌باشد (خرم آبادی، ۱۳۸۸).

اصول حاکم برحقوق بین الملل اینترنت

اصول حاکم بر اینترنت از چند جهت حائز اهمیت هستند. اولا اینکه برای آشنایی بیشتر با این محیط می توان به سراغ این اصول رفت و با توجه به آنها شناخت بیشتری را از واقعیت های محیط وب و به ویژه جرائم سایبر به دست آورد. از سوی دیگر شناخت آنها می تواند تاثیر بسزایی در قانونگذاری و ایجاد قواعد حقوقی داشته باشد چرا که برای صحت و سلامت یک قانونگذاری یکی از اصولی ترین قدم ها شناخت اصول حاکم بر پدیده می باشد به همین دلیل مهمترین این اصول را ذکر می کنیم.

۱. اصل آزادی دسترسی به اطلاعات:

عده ای از کارشناسان تلاش فراوانی به خرج می دهند تا از نفوذ دولتها به عرصهٔ مدیریت اینترنت جلوگیری کنند؛ ولی حتی اگر در این راه موفق نباشند مطمئناً نخواهند گذاشت اصل آزادی دسترسی به اطلاعات مورد خدشه واقع شود. البته این اصل با یکسری چالش هایی مواجه است. برای مثال آمار و ارقام دربارهٔ کاربران اروپایی و آمریکایی اینترنت در مقایسه با کاربران آفریقایی، وضعیت وحشتناکی را به نمایش می گذارد. از سوی دیگر و از آنجا که قریب به ۷۰ درصد اینترنت با زبان انگلیسی نگاشته شده است می توان تصور کرد که تا چه اندازه متکلمان به سایر زبان ها توان استفاده از آنرا خواهند داشت. با همهٔ این احوال و با همهٔ اعتراضاتی که مبدعان و مدیران اینترنت به این امر داشته اند لیکن تلاش جهانی بر این است تا اصل آزادی دسترسی به اطلاعات همچنان بی خدشه باقی بماند.

۲. اصل تخصصی بودن ادارهٔ اینترنت:

دانشمندان معتقدند اصولا دولتها قادر به ادارهٔ اینترنت نیستند؛ زیرا این مساله یک امر کاملا تخصصی است. از همین رو دولتها، ITU را برای قائم مقامی برگزیده اند. اتحادیهٔ بین المللی مخابرات، یک نهاد تخصصی سازمان ملل است و وظایف آن بیشتر از همه، به حال و روز اینترنت می آید.

۳. همیشه در دسترس بودن و پاسخگویی به همه:

اینترنت به شکلی طراحی شده است که امکان تعطیلی برای آن وجود نداشته باشد. علاوه بر آن، امکانات لازم برای دستیابی به اینترنت برای همهٔ مردم به صورت یکسان وجود داشته و به عبارتی، سهل الوصول ترین راه برای دستیابی به اطلاعات به شمار می رود.

این اصل نتیجهٔ عملی اصل اول یعنی آزادی دسترسی به اطلاعات به شمار می آید.

۴. اصل تمرکز زدایی و عدم امکان اخراج:

تمرکز زدایی در محیط سایبر به این معناست که هیچکس نمی تواند با به تعطیلی کشاندن یک کامپیوتر خاص، اینترنت جهانی را خاموش کند. طراحان اینترنت سعی کرده اند اوضاع به شکلی پیش رود که اگر یک قسمت از مراکز مدیریت اینترنت خراب شد مراکز دیگر وظایف آنرا به عهده بگیرند. این مساله بر امکان دوام شبکه می افزاید. مسالهٔ بعد، عدم امکان اخراج هیچ کاربر توسط هیچ مرجع موجود می باشد. یعنی تا هر وقت، هر فرد با هر عقیده ای می تواند در محیط اینترنت باقی بماند و علاوه بر کسب اطلاعات و دانایی به بسط و گسترش عقاید خویش بپردازد. این امکان که یک پلیس در شبکه وجود داشته باشد هر چند به راحتی می تواند فراهم شود لیکن با اصل عدم امکان اخراج، سازگاری ندارد.

بسیاری از اتاق های گفتگو برای رعایت اصول خود، به این راه حل متوسل می شوند؛ لیکن اصل اساسی در اینترنت، عدم توسل به چنین حربه ای است. شاید نتوان گفت که تمامی اصول حاکم بر وب در همین اصول قرار دارد لیکن آنچه حائز اهمیت به نظر رسیده در این اصول جمع آوری گردیده است.

چالشهای پیشگیری وضعی از جرائم سایبر با موازین حقوق بشر

گرچه فضای سایبر این پدیدهٔ شگفت‌انگیز قرن بیست و یکم، بسیاری از عرصه‌ها را با تحولات بنیادین مواجه کرده؛ اما سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است. 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. کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند (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:

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

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

۳. کاهش جاذبه از آماجها و قربانیان جرم از طریق: الف. حذف آماجهای جرم؛ ب.علامت‌گذاری اموال؛ پ. تقلیل فرصتهای وسوسه‌انگیز؛ و ت. وضع قواعد خاص (ابراهیمی، ۱۳۸۳: ۱۸).

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.

آنچه در این قسمت مورد بررسی قرار می‌گیرد، تدابیر پیشگیری وضعی از جرائم سایبر و چالش آنها با رعایت موازین حقوق بشر است.

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.

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 دسترسی، 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 دسترسی دیگران به سایتهایی که مغایر با اعتقاداتشان است جلوگیری کنند. اما آنچه بیشتر به گسترهٔ اعمال این محدودیتها دامن می‌زند، گنجاندن 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 دسترسی افراد به مطالب معتبر و مجاز جلوگیری کند.

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 دسترسی به آنها جلوگیری می‌شود. به عنوان مثال، با درج واژه ای خاص در موتورهای جستجو که در مجامع عمومی شرم به زبان راندن آن واژه وجود دارد، فیلترها به سرعت فعال می‌شوند، در حالی که بسیار اتفاق می‌افتد که از آن واژه در متون معتبر علمی و ادبی نیز استفاده می شود (Thornbburgh , 2004 : 267).

امروزه در بسیاری از کشورها حفظ امنیت ملی، نظم، سلامت یا اخلاق عمومی و احترام به حقوق یا آزادیهای اساسی دیگران، جزء مولفه‌هایی است که به رسمیت شناخته شده و دولتها تلاش می‌کنند از آنها به بهترین وجه پاسداری کنند. از سوی دیگر، فضای سایبر جلوهٔ دیگری به این مفاهیم بخشیده و باید مطابق با ویژگیهای خاص آن برنامه‌ریزی کرد. اگر تعداد بسیار کمی از گروههای یک جامعه به فکر تهیهٔ انواع ابزارهای محدودکننده یا سلب‌کنندهٔ دسترسی هستند، خیل عظیمی هم برای خنثی کردن آن ابزارها تلاش می‌کنند و در میان این گروه می‌توان چهره‌های موجه بسیاری نظیر دانشجویان و دانش‌پژوهان را یافت که برای احقاق حق خود، یعنی بهره‌برداری علمی و سودمند از این فضا، سعی می‌کنند دست به کاری بزنند که شاید غیرقانونی نیز تلقی شود.

آنچه نباید از نظر دور داشت اینکه در تمامی کشورها، حتی آنهایی که خود را مهد مردم‌سالاری می‌دانند، خط قرمزهایی وجود دارد. در کشوری مثل ایالات متحده یا کشورهای اروپایی، از ابزارهایی نظیر فیلترها به وفور استفاده می‌شود، اما برای کاستن از مضرات آنها، سعی شده برنامه‌ریزی مفصلی در زمینهٔ مخاطب‌شناسی (کسانی که این ابزارها برای آنها به کار می‌رود)، شناسایی هرچه دقیقتر محتواهای غیرمجاز و پرهیز از گنجاندن موارد مشکوک به آنها و در نهایت بهره‌گیری چندبعدی از این ابزارها انجام شود. به عنوان مثال، در کنار فهرستهای متنی، از فهرستهای تصویری یا دیگر شناسه‌ها استفاده می‌شود

تا ضعف این ابزارها به حداقل برسد.

به نظر می‌رسد با یک برنامه‌ریزی صحیح و اقتباس از الگوهای مفیدی که اکنون در دیگر کشورها به اجرا درمی‌آید، علاوه بر حفظ ارزشهای مورد قبول جامعه، می‌توان به گونه‌ای موثر از جرائم سایبر پیشگیری کرد (Kent, 2004: 55).

۲. تقابل پیشگیری وضعی از جرائم رایانه‌ای با حریم خصوصی

همانگونه که اشاره شد، فضای سایبر برخلاف 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 تاثیر ابزارهای پیشگیرانه از جرائم سایبر آن اشاره می‌شود.

به طور کلی، دو ابزار پیشگیرانه، حریم الکترونیکی افراد را تهدید می‌کنند: اولین ابزار در این زمینه، ابزارهای نظارتی است که تردیدی در تعرض‌آمیز بودن آنها نیست. 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 تاثیر خواهد گذاشت. 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 تایید 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 می‌شود. نگرانی که در اینجا وجود دارد، راجع به امکان سوء استفادهٔ متصدیان این سایتها از این اطلاعات یا امکان افشای آنها به دلایل مختلف است (ibid).

این موضوع تا آن حد جدی تلقی شده که برای حمایت از کودکانی که چنین اطلاعاتی از آنان اخذ می‌شود، در سال ۱۹۹۹ در ایالات متحده قانون حمایت از حریم آنلاین کودکان 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 آزادی های 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 EEC/313/90 و EC/29/2001 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 می‌شود:

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 (EC/46/95)؛ 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 (EC/66/97)؛ و ۴. دستورالعمل پارلمان و شورای اروپا در خصوص پردازش داده‌های شخصی و حمایت از حریم ارتباطات الکترونیک (EC/58/2002).

اما در ایالات متحده، اولین قانون فدرال حمایت از حریم ارتباطات الکترونیک، در سال ۱۹۸۶ 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 به مجاز بودن ارائه‌دهندگان خدمات در نقض حریم افراد برای حفاظت از اموال، حقوق و دارایی هایشان اشاره کرد. همچنین قانون نحوهٔ استفاده از ابزارهای ثبت‌کننده و ردیاب، 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 می باشد 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 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 (United Nations,2004: 40).

راهکارهای مقابله با جرائم سایبر

کنترل دولتی

در این روش، سیاست کلی حاکم بر کشور اجازهٔ دسترسی به پایگاههای مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازهٔ اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.

کنترل سازمانی

روش دیگر، کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفادهٔ صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی تواماً انجام این وظیفه را تضمین کند.

کنترل فردی

کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمین های اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی، مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه‌های جهانی به عمل می آورد. این اعتقاد و فرهنگ در محدودهٔ خانواده نیز اعمال می‌شود. البته شیوهٔ اخیر در صورتی ممکن خواهد بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظهٔ خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند.

وجود یک نظام قانونمند اینترنتی

مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل تهاجم فرهنگی، اطلاعات نادرست و یا پیامدهای ضد اخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که ادارهٔ آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری کند. این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تاثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد (نایب، ۱۳۸۸).

سیاستگذاری ملی در بستر جهانی

واقعیت این است که مرور چند الگوی ملی می تواند ما را در سیاستگذاری های مبتنی بر فهم جهانی در حوزهٔ اینترنت یاری رساند، لذا معرفی اجمالی چند نمونه که با سه رویکرد تحول‌گرا، ثبات‌گرا و اعتدال‌گرا تناسب بیشتری دارند ضروری است.

الگوی آمریکایی

اینترنت در آمریکا هم به عنوان تهدید امنیتی و هم به عنوان بزرگترین فرصت ملی تلقی می‌شود. کاخ سفید در پنجم ژانویهٔ سال ۲۰۰۰ بیانیه‌ای را تحت عنوان «استراتژی امنیت ملی در قرن جدید» منتشر کرد. در این بیانیه ضمن برشمردن منافع حیاتی آمریکا، از اینترنت به عنوان مهمترین ابزار دیپلماسی مردمی نام برده شده است. پیشرفت جهانی تکنولوژیهای آزاد و اطلاع‌رسانی چون اینترنت توانایی شهروندان و موسسات را برای تاثیرگذاری بر سیستمهای دولتها تا حد غیرقابل تصوری بالا برده است. دیپلماسی مردمی یعنی تلاش برای انتقال اطلاعات و پیامهایمان به مردم جهان. توسعهٔ اینترنت در داخل و استفاده از آن برای تاثیرگذاری بر دیگران بخش مهمی از سیاستهای استراتژیک آمریکاست (Depts.State: 2000).

الگوی فلسطین اشغالی

این کشور در فاصلهٔ سال ۱۹۹۴ تا ۲۰۰۰ تبدیل به یک غول صنعت اینترنت شده است. فلسطین اشغالی در سطح داخلی چنین سیاستهایی اتخاذ کرده که عبارتنداز:

- اختصاص سه درصد از GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینهٔ تکنولوژی پیشرفته.

- آموزش مهارتهای پیشرفتهٔ رایانه‌ای در دوران سربازی و تداوم آموزش در دوران خدمت احتیاط.

- تولید Checkpoint با پیشینه و ریشه در کاربردهای نظامی و به عنوان یکی از قابل اطمینان‌ترین و پرفروشترین باروهای جهان (فایروال یا بارو، شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب سایتهای نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایی های افراد را از دسترس نیروهای متخاصم دور نگاه می‌دارد) که کشورهای عربی نیز به آن متکی هستند، یکی از سیاستهای جهانی کشور مذکور است.

الگوی چینی

چین رسماً اعلام کرده به دنبال برقراری توازن میان جریان آزاد اطلاعات و صیانت فرهنگ و ارزشهای اجتماعی خود می‌باشد. در اجرای این استراتژی، چین اقدامات زیر را انجام داده است:

- سرمایه‌گذاری عظیم در صنایع الکترونیک، مخابرات و رایانه
- اقدامات وسیع و سازمان یافته برای تکثیر، شکستن قفل و شبیه‌سازی نرم‌افزارها و برنامه‌های کاربردی رایانه‌ای و تقویت صنعت عظیم نرم‌افزار در چین.
- تاسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت
- همکاری شرکت با غولهای اینترنتی آمریکا برای ایجاد خدمات مبتنی بر وب با استانداردهای کیفی AOL و استانداردهای اخلاقی و قانونی چین
- جلب همکاری AOL و Netscape برای تولید یک پویشگر اینترنت به زبان چینی
- هزینهٔ عظیم برای فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت (نایب، ۱۳۸۸).

نتیجه گیری

پیشرفت تکنولوژی رایانه و توسعهٔ کاربرد آن، وابستگی تنگاتنگ زندگی مدرن امروزی به این فناوری را در تمامی زمینه های مختلف به ارمغان آورده است. به طوریکه امروزه عملا بدون وجود رایانه، حیات جامعهٔ جهانی مختل خواهد شد. به طور طبیعی هر نوآوری در زمینهٔ تکنولوژی و علوم به تبع خود توجه افراد سودجو و بزهکار را نیز جلب می کند و این افراد، امکاناتی را که می تواند در جهت اعتلای تمدن بشری، امنیت و رفاه به کار رود، در جهت منافع خود و ارضاء حوائج شخصی به کار می برند، به طوریکه جرائم مربوط به تکنولوژی رایانه ای امروزه توجه حقوقدانان، جرم شناسان، متخصصان رایانه و پلیس های جهان را به خود معطوف کرده است. به طور کلی همهٔ کشورها در قبال جرائم سایبری با یک مشکل واحد مواجه هستند: آنها همواره به حمایت از اهداف و اشیاء ملموس و قابل رویت پرداخته و

قوانین آنان نیز به طبع ناظر بر اینگونه اهداف و اشیا بوده است. از اواسط قرن بیستم به بعد، حقوق جزا با مشکل حمایت از اطلاعات و اشیاء ناملموس مواجه شده است که علت آن، تغییر الگوهای جامعهٔ امروزی از حالت صنعتی به فراصنعتی (جامعهٔ اطلاعاتی)، افزایش ارزش اطلاعات و تکمیل دکترین های حقوق اطلاعات است. نتیجه اینکه الگوهای فیزیکی در حقوق جزا تبدیل به الگوهای غیر فیزیکی شده است. به دنبال رشد سریع تکنولوژی کامپیوتری و پیدایش سه نسل از جرائم مربوط به این تکنولوژی در طول چهار دهه گسترش این فناوری در محدودهٔ شبکه های بین المللی و اینترنت (سایبر اسپیس) حقوق کیفری نیز تاکنون چهار مرحله تحول تقنینی را طی نموده است.

مرحلهٔ اول: مربوط به حمایت از اطلاعات خصوصی (دهه های ۷۰ و ۸۰ میلادی)

مرحلهٔ دوم: ایجاد و اصلاح قوانین ناظر به جرایم کامپیوتری (اواخر دههٔ ۸۰ میلادی)

مرحلهٔ سوم: وضع قوانین جهت حمایت از دارایی های غیر مادی (مالکیت فکری، دههٔ ۸۰ میلادی)

مرحلهٔ چهارم : تکوین مقررات آئین دادرسی کیفری (دههٔ ۹۰ میلادی)

در دههٔ ۹۰ جرائم در محیط سایبر تجلی کرد که حاصل تکنولوژی ارتباطاتی و مخابراتی ماهواره ای و پیدایش شبکه های بین المللی می باشد و با توجه به خصوصیت غیر ملموس و مجازی بودن محیط سایبر، مسائل جزایی آن به گونه ای متفاوت و کاملتر نسبت به جرائم رایانه ای نسل های قبل می باشد. به طور کلی جرائم رایانه ای و شبکه ای با اغلب جرائم متعارف و کلاسیک در چند مورد اختلاف اساسی دارند:

۱. با منابعی اندک خسارتی هنگفت می توانند وارد کنند.

۲. می توان بدون حضور فیزیکی در یک حوزهٔ قضایی معین در آن حوزه مرتکب اینگونه جرائم شد.

۳. در اغلب موارد غیر قانونی بودن و منشا آنها روشن و آشکار نیست.

۴. امروزه جرائم رایانه ای و اینترنتی غالبا در ابعاد بین المللی به وقوع می پیوندد.

جرائم رایانه ای و شبکه ای از حیث تعقیب و دادرسی نیز با چالش و تحول مواجه می باشد. آیین دادرسی

مدنی بایستی به دنبال یک تعقیب موثر جرم در زمینهٔ تکنولوژی اطلاعات باشد؛ زیرا این تکنولوژی رشد بسیاری در زمینه های اقتصادی و زندگی اجتماعی داشته و مشکلات جرم یابی خاصی را نیز به دنبال آورده است. در عین حال آیین دادرسی کیفری می بایستی به حمایت از آزادیهای مدنی، مظنونین و شهود بپردازد و در زمینهٔ تعقیب بین المللی جرائم می بایست بر مبنای تعاون و همکاری بین المللی با رعایت اصول حاکمیت و امنیت کشور مقابل صورت گیرد.

به نظر می رسد برای یک استراتژی جامع امنیت داده پردازی و کنترل جرم راه حل قانونی بایستی توسط ابزارها و تدابیر فرا قضایی همچون تدابیر امنیتی اختیاری توسط کاربران رایانه به کار گرفته شود. ضمن اینکه اجرای تدابیر امنیتی و جلوگیری از جرائم باید با توسعهٔ تکنولوژی همگام باشد.

ضمن تاکید بر راهکارهای مقابله با جرائم سایبر که در بالا به ذکر آن پرداختیم و با تاکید بر بومی سازی الگوهایی که در این زمینه قابلیت بیشتری دارند، در یک جمع بندی کلی می توان سیاست ها و راهبردهای موثر برای مبارزه با جرائم رایانه ای و پیشگیری از آنرا مبتنی بر اصول ذیل تدوین کرده و راهکارهای اجرایی آنرا در چارچوب ملی برنامه ریزی کرد:

۱. آگاهی دادن به شرکتها و ادارات در خصوص قابلیت خطر پذیری سیستم های رایانه ای و تشویق آنان به استفاده از تدابیر امنیتی

۲. ارتقاء تدابیر امنیتی استاندارد شده

۳. کاهش موقعیت های جرم زا و فرصت های استفاده از ابزار فنی در ارتکاب جرم

۴. تشویق بزه دیدگان به اعلام وقوع جرم

۵. تدوین قوانین مناسب و انجام اصلاحات ضروری در مقررات جاری کشورها

۶ همکاری همه جانبهٔ بین المللی در امر کشف جرائم رایانه ای، شبکه ها و تعقیب مرتکبان این دسته.

منابع

کتب فارسی

۱. معتمدنژاد، کاظم، ۱۳۸۳، وسایل ارتباط جمعی جلد نخست، تهران، انتشارات دانشگاه علامه طباطبایی

۲. نجفی ابرندآبادی، علی‌حسین، ۱۳۸۳، پیشگیری عادلانه از جرم، علوم جنایی، مجموعه مقالات در تجلیل از استاد آشوری، انتشارات سمت.

پایان‌نامه‌ها

۳. حسن‌بیگی، ابراهیم، ۱۳۸۲، آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تاکید بر جنبه‌های حقوقی و فنی، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی.

۴. حسینی، بیژن، ۱۲۸۲، جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن، پایان‌نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات.

مجلات

۵. ابراهیمی، شهرام، ۱۳۸۳، پیشگیری از جرم.

۶. جلالی فراهانی، امیرحسین، ۱۳۸۴، پول‌شویی الکترونیکی، فصلنامه فقه و حقوق، شماره ۴.

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

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

۹. دزیانی، محمدحسن، ۱۳۸۳، مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرائم کامپیوتری (سایبری)، خبرنامه انفورماتیک، شماره ۸۷.

۱۰. دزیانی، محمد حسن، ۱۳۷۶، جرائم کامپیوتری، جلد اول، دبیرخانه شورای عالی انفورماتیک.

۱۱. صفاری، علی، ۱۳۸۰، «مبانی نظری پیشگیری وضعی»، مجله تحقیقات حقوقی، شماره ۲۴-۳۳.

۱۲. نجفی ابرندآبادی، علی حسین، ۱۳۸۲، تقریرات درس جرم‌شناسی (پیشگیری)، دوره کارشناسی ارشد حقوق کیفری و

جرم‌شناسی، تنظیم مهدی سیدزاده، نیم‌سال دوم تحصیلی ۸۲-۱۳۸۱.

۱۳. نیازپور، امیرحسن، ۱۳۸۲، «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، مجله حقوقی دادگستری، شماره ۴۵.

کتب انگلیسی و منابع اینترنتی

۱۴. خرم آبادی، عبدالصمد، ۱۳۸۸، طبقه‌بندی جرائم رایانه‌ای، http://adl-e-adel.blogfa.com/post-105.aspx

۱۵. صدیق بنای، هلن، ۱۳۸۹، سایبر اسپیس، پایگاه اینترنتی آفتاب.

۱۶. نایب، مهرداد، ۱۳۸۸، امنیت شبکه چیست؟ http://ittop.ir/thread3981.html

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

18. Sieber,u.1995. Computer Crime and Criminal Information Law- New Trends in the International Risk and Information Society,

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

20. T. Kent, Stephen and I. Millett Lynette,2804. Who Goes There? Authentication Through the Lens of Privacy, National Academy Press.

21. United Nations.2004. Office on Drugs and Crime; the Global Program a gainst Corruption; UN Anti-Corruption Toolkit; Third Edition; Vienna; September.

22. United Nations, 1992. International Review of Criminal Policy- United Nations Manual on the Prevention and Control of Computer-Related Crime, Nos.

23. Us Dept. of state 2000 A National security strategy for a new century