پیشگیری از جرائم رایانه‌ای

امیرحسین جلالی فراهانی*

چکیده: امروزه بحث فناوری اطلاعات و ارتباطات نوین، که تجلی روشن آن فضای تبادل اطلاعات (فضای سایبر) است، مسئله جدیدی را با عنوان پاسخگویی به سوءاستفاده‌هایی که از فضای تبادل اطلاعات به عمل می‌آید پیش روی دانشمندان علوم جنائی قرار داده است. این مقاله بررسی طرق پیشگیری کیفری و غیرکیفری از جرائم رایانه‌ای در ابعاد خرد و کلان را مورد بررسی قرار می‌دهد. این بحث در قالب دو بخش دنبال می‌شود. در بخش اول، پس از مختصر توضیحی راجع به ماهیت جرائم رایانه‌ای، به اقدامات انجام شده در دیگر کشورها و عرصه بین‌الملل و همچنین کشورمان در حوزه پیشگیری کیفری از جرائم رایانه‌ای اشاره می‌شود. در بخش دوم، پیشگیری غیرکیفری از جرائم رایانه‌ای بر مبنای الگوی پیشگیری وضعی و اجتماعی دنبال می‌شود و در هر یک از این مباحث به محدودیت‌های حاکم بر این پیشگیری‌ها و اقدامات انجام شده در کشورمان اشاره می‌شود. در پایان، با تأکید بر مزایا و محدودیت‌های حاکم بر هر یک از این مدل‌های پیشگیری، پیشنهادهایی مطرح می‌گردد.

کلید واژه‌ها: *جرم رایانه‌ای ـ فضای تبادل اطلاعات ـ پیشگیری کیفری ـ پیشگیری اجتماعی ـ پیشگیری وضعی.*

---

* دانشجوی کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه امام صادق(ع).

مقدمه:

بشر در طول حیات خود اعصار گوناگونی را پشت سر گذاشته و هر یک از آنها را با الهام از تحول عظیمی که در آن عصر پدید آمده و گامی از رشد و تکامل بشری را رقم زده نامگذاری کرده است، مانند: عصر آتش، عصر آهن و عصر حاضر که **عصر فناوری اطلاعات و ارتباطات** نام گرفته است.

هنوز نیم‌قرن از اختراع اولین رایانه نمی‌گذرد، آن هم رایانه‌ای سی تنی که البته سرعت عمل آن از ابتدایی‌ترین ماشین حساب‌های دیجیتال امروزی نیز کمتر بود،[1] اما به هر حال تحولی شگرف در دنیای علم و فناوری محسوب می‌شد و از همین رو رایانه‌ها در این مدت کم به خوبی توانستند جای خود را در تمامی شئون زندگی انسان باز کنند و به نوعی خود را در تمامی پیشرفت‌ها سهیم سازند. این اقبال عمومی و بهره‌برداری روزافزون از سیستم‌های رایانه‌ای زمانی شتاب بیشتری به خود گرفت که در ابتدای دههٔ نود میلادی امکان متصل شدن آنها به یکدیگر در سراسر جهان فراهم شد. در این زمان بود که مشاهده شد مرزها و موانع فیزیکی بی‌اثر شده و به نوعی رؤیاهای جهانی بشر واقعیت یافته است.

اما از آنجا که این پدیدهٔ شگفت‌انگیز از همان بدو تولد در دسترس همگان قرار گرفت، هرکس مطابق اغراض و مقاصد خود از آن سود می‌جست و نتیجه آن شد که بعضی از این بهره‌برداری‌ها جنبه سوءاستفاده به خود گرفت و بالطبع سیاستگذاران خرد و کلان را واداشت که تدبیری بیندیشند. این سوءاستفاده‌ها که در مجموع جرائم رایانه‌ای نام گرفته‌اند، طیف جدیدی از جرائم هستند که به سبب ویژگی‌های متمایزی که با جرائم سنتی دارند، تصمیم‌گیران جامعه را بر آن داشته‌اند تا در ابعاد مختلف

1. Casey, Eoghan, Digital Evidence and Computer Crime, First Edition, 2001, p42.

اقدامات متمایزی را طرح‌ریزی کنند. آنچه این مقاله مورد بررسی قرار می‌دهد، پیشگیری از این طیف نوظهور جرائم است.

موضوعاتی که در باب پیشگیری از جرائم رایانه‌ای مطرح شده، بر مبنای چهارچوب کلی ارکان پیشگیری از جرائم می‌باشد تا قابلیت کاربردی خود را حفظ کند و از حالت تئوری و انتزاعی به دور باشد.

بر این اساس، در بخش اول پیشگیری کیفری از جرائم رایانه‌ای مورد بررسی قرار می‌گیرد که به لحاظ ضرورت، در ابتدا مختصر توضیحی راجع به ماهیت این جرائم ارائه می‌شود. سپس به تحول قوانین و مقررات مربوط در دیگر کشورها و عرصهٔ بین‌الملل اشاره می‌شود و در نهایت وضعیت کشورمان مورد بررسی قرار می‌گیرد. در بخش دوم، پیشگیری غیرکیفری از این جرائم با تکیه بر مدل پیشگیری اجتماعی و وضعی مطرح می‌شود و در انتهای هر مبحث به محدودیت‌های هر یک از این تدابیر پیشگیرانه و اقداماتی که تاکنون در کشورمان به انجام رسیده اشاره‌ای می‌گردد. در پایان نیز ضمن نتیجه‌گیری از مباحث مطرح شده، نکاتی که به نظر می‌رسد توجه به آنها می‌تواند مفید باشد مورد تأکید قرار می‌گیرد.

۱. *پیشگیری کیفری از جرائم رایانه‌ای*

همان طور که گفته شد، به لحاظ سیر منطقی و آشنایی بیشتر با این طیف نوظهور از جرائم پیش از وارد شدن به مبحث اصلی، توضیحاتی راجع به جرائم رایانه‌ای داده می‌شود. بدیهی است، بررسی جامع این نوع جرائم خود مجال دیگری می‌طلبد که از حوصلهٔ این مقاله خارج است.

۱ـ۱. *جرائم رایانه‌ای*

آنچه امروزه جرم رایانه‌ای، جرم اینترنتی، جرم سایبر یا حتی جرم علیه فناوری اطلاعات و ارتباطات نام گرفته است، در واقع همگام با رشد و تکامل عصر حاضر توسعه یافته و هر روز جلوه‌های نوین و متنوع‌تری از آن مشاهده

می‌شود. اما اولین نکته‌ای که در درک مفهوم جرائم رایانه‌ای باید مدنظر داشت، این است که مفهوم رایانه فقط گزینه‌هایی که ذهن ما به آنها معطوف می‌شود، مانند رایانهٔ رومیزی یا قابل حمل را در برنمی‌گیرد، بلکه همان طور که **کنوانسیون بین‌المللی جرائم سایبر**[1] (مصوب ۲۰۰۱) به این موضوع صراحتاً اشاره کرده، «سیستم رایانه‌ای یک دستگاه یا مجموعه‌ای از دستگاه‌های متصل به هم یا مرتبط با هم است که به وسیلهٔ یک برنامه، داده‌های دیجیتال را به طور خودکار پردازش می‌کند.»[2] با اینکه بحث راجع به این تعریف بسیار است و خود مجال دیگری می‌طلبد، اما قدر مُتیقّن محرز است که حوزهٔ تحت شمول سیستم رایانه‌ای بسیار گسترده‌تر از حوزهٔ متصور ماست و همه دستگاه‌هایی که برنامه‌ای داشته باشند که داده‌های دیجیتال را پردازش کند، در برمی‌گیرد، مانند تلفن‌های همراه امروزی، سیستم‌های پی‌جو[3]، تلفن‌های ثابت حافظه‌دار و موارد دیگر. هرچند این واقعیت نیز انکار نمی‌شود که مثال کامل این تعریف همان رایانه‌های رومیزی یا قابل حمل است.

نکتهٔ دیگری که باید به آن توجه داشت، مفهوم **فضای تبادل اطلاعات** است. با اینکه حدود دو دهه از به کارگیری این اصطلاح در حوزه فناوری اطلاعات و ارتباطات نوین می‌گذرد، ولی همچنان میان صاحب‌نظران اختلاف نظرهای بنیادینی مشاهده می‌شود، به گونه‌ای که هنوز بر سر واقعی یا مجازی بودن آن هم اختلاف نظر دارند. با این حال، تعریف ساده و مورد قبولی که می‌توان از آن ارائه داد عبارت است از: «فضای واقعی و محسوس میان سیستم‌های رایانه‌ای که داده‌های دیجیتال در آن در جریان هستند.»[4]

---

1. Cyber Crime Convention, http://conventions.coe.int/Treaty/en/Reports/Html/.

۲. بند الف ماده یک از فصل اول این کنوانسیون.

3. Pagers.

4. Glossary: The Convoluted Terminology Of Information Warfare, Compiled by

البته لازم به ذکر است تا اوایل دههٔ ۹۰ میلادی که سیستم‌های رایانه‌ای ارتباط جهانی با یکدیگر نیافتند و شبکه‌های اطلاع‌رسانی رایانه‌ای به مفهوم امروزی خود به فعالیت نپرداختند، این فضا جایگاه واقعی خودّ را پیدا نکرد، والّا مفهوم آن حتی نسبت به یک سیستم رایانه‌ای مستقل نیز صدق می‌کند.

به نظر می‌رسد اگر ما این مفهوم جامع را برای فضای تبادل اطلاعات بپذیریم، دیگر به کارگیری اصطلاحاتی نظیر جرم اینترنتی یا حتی جرم شبکه‌ای (که حوزهٔ بسیار محدودی را در بر می‌گیرند) صحیح نخواهد بود. حتی اصطلاحی که امروزه تحت عنوان جرم علیه فناوری اطلاعات و ارتباطات به کار می‌رود نیز صحیح نمی‌باشد. چرا که این حوزه حداقل تا به امروز در کشور ما علاوه بر فناوری دیجیتال، فناوری آنالوگ را هم در برمی‌گیرد که این امر بار مفهوم فضای تبادل اطلاعات را گسترده‌تر می‌کند و با اصول حقوقی در تعارض است. اما از آنجا که اصطلاح جرم سایبر هنوز در جامعهٔ حقوقی و فنی، حتی در عرصهٔ جهانی، جایگاه واقعی خود را نیافته است، ما از همان اصطلاح جرم رایانه‌ای، اما در همان مفهوم موسع آن استفاده می‌کنیم. مؤید این کلام کنوانسیون بوداپست است که با اینکه عنوان جرائم سایبر دارد، اما جهت ملموس‌تر کردن مقررات خود سیستم رایانه‌ای را تعریف کرده و آن را مبنای عمل خود قرار داده است. بنابراین، ملاحظه می‌شود که این دو عنوان عملاً با یکدیگر تفاوتی ندارند.

با توجه به مطالب فوق، می‌توان در تعریف جرم سایبر یا رایانه‌ای گفت: «هرگونه فعل یا ترک فعلی که در فضای تبادل اطلاعات از طرف قانونگذار جرم قلمداد شود، جرم سایبر یا رایانه‌ای محسوب می‌شود»، حال چه نظیر آن در دنیای فیزیکی وجود داشته باشد، مثل جعل، کلاهبرداری، هرزه‌نگاری یا پول‌شویی که در اینجا فضای تبادل اطلاعات این جرائم را تسهیل و تسریع

Randall Whitaker, Ph.D.

می‌کند و به آنها جلوه‌ای نو می‌بخشد، چه اینکه یک «**جرم صرف سایبر**»[۱] محسوب شود، مثل نشر ویروس یا دسترسی غیرمجاز که ارتکاب این اعمال فقط در فضای تبادل اطلاعات متصور است. البته باید اذعان داشت به لحاظ ادغام و درهم تنیدگی بیش از حد فعالیت‌های امروزی با فضای تبادل اطلاعات، به طور مشخص نمی‌توان جرائم را بر این مبنا تفکیک کرد.[۲]

۱-۲. *پیشگیری کیفری از جرائم رایانه‌ای*

بحث پیشگیری از جرم یا به عبارت بهتر اتخاذ تدابیر مناسب جهت جلوگیری از وقوع یا تکرار جرم، موضوعی نیست که به عصر حاضر تعلق داشته باشد. از همان ابتدا که بشر با نقض ارزش‌های خود مواجه شد، همواره در این فکر بود که با اتخاذ تدابیری، از ارتکاب چنین اعمالی جلوگیری کند. اما از آنجا که در هر دوره رویکرد خاصی نسبت به جرم وجود داشته، مسلماً تدابیر پیشگیرانه‌ای هم که اتخاذ می‌شده، جلوه‌های متفاوتی داشته است. البته لازم به ذکر است که عده‌ای پیشگیری از جرائم را فقط در مفهوم غیرکیفری یا به عبارت بهتر غیرقهرآمیز آن جست‌وجو می‌کنند.[۳]

این گروه از دانشمندان علوم جنایی، پیشگیری در معنای اخص را فقط شامل اقدامات غیرقهرآمیز می‌دانند و برای ضمانت اجراهایی که از طرف قانونگذار وضع می‌شود، هیچ تأثیری قائل نیستند. آنچه به طور خلاصه در

---

1. Pure Cyber Crime.

۲. تعاریفی که تاکنون در منابع مختلف ارائه شده، هیچ یک جنبهٔ حقوقی ندارند، بلکه بیشتر سعی شده ماهیت این جرائم تبیین گردد. به عنوان مثال مراجعه کنید به:
Casey, Eoghan, Digital Evidence and Computer Crime, First Edition, 2001, pp. 8-9.

۳. بحث غیرقهرآمیز بودن پیشگیری از جرم، برای اولین بار توسط انریکو فری، واضع جامعه‌شناسی جنایی تحت عنوان«هم ارزهای کیفری» مطرح شد. ر.ک: نیازپور (امیرحسن)، **پیشگیری از بزهکاری در قانون اساسی ایران و لایحهٔ قانونی پیشگیری از وقوع جرم**، مجله حقوقی دادگستری، شمارهٔ ۴۵، زمستان ۱۳۸۲، ص ۱۲۵.

جواب این گروه می‌توان بیان داشت، این است که همان طور که آنها نیز معتقدند، برای حقوق کیفری دو کارکرد یا کار ویژه مقرر شده است:

۱ـ ارعاب‌انگیزی؛ و ۲ـ عبرت‌انگیزی که نسبت به هر دو گروه مرتکبان جرائم و مجرمان بالقوه صدق می‌کند و به عبارت دیگر علاوه بر پیشگیری از وقوع، از تکرار جرم نیز جلوگیری می‌کند. البته در صورتی این دو کارکرد محقق می‌شود که همان طور که سزاره بکاریا و جرمی بنتام به عنوان پایه‌گذاران حقوق کیفری نوین بیان داشته‌اند، تدابیر کیفری از حتمیت، قطعیت و تناسب برخوردار باشند. در این صورت، مجرم که یک انسان حسابگر و دوراندیش فرض می‌شود، منفعتی که قرار است از ارتکاب جرم به دست آورد را با مشقتی که قرار است به طور حتم تحمل کند می‌سنجد و بدیهی است این خود یک عامل بازدارندهٔ بسیار خوب از ارتکاب یا تکرار جرم محسوب می‌شود.(۱)

نکتهٔ دیگری که باید به آن توجه داشت، این است که هر جامعه‌ای از طریق جرم‌انگاری یا جرم‌زدایی، ارزش‌های مورد قبول خود را به اعضایش اعلان می‌کند. در واقع، کشورهای دیگر با مطالعهٔ مجموعه قوانین کیفری یک کشور در می‌یابند که چه هنجارها و ارزش‌هایی برای آن موضوعیت دارد. بنابراین، می‌توان گفت مقررات کیفری، تریبون اعلام هنجارهای رسمی یک جامعه هستند و از اهمیتی برخوردارند که نمی‌توان از آنها چشم‌پوشی کرد.

از طرف دیگر، امروزه در نحوهٔ تحمیل ضمانت اجراهای قهرآمیز تحولات شگرفی رخ داده و حتی‌المقدور سعی شده به اصلاح و بازپذیرسازی مجرمان توجه شود. لذا، آن گونه که می‌توان از این تدابیر تجدیدنظر شده انتظار داشت که در پیشگیری از تکرار جرائم مؤثر واقع

---

۱. بکاریا (سزاره)، **جرائم و مجازات‌ها**، ترجمهٔ اردبیلی (محمدعلی)، انتشارات دانشگاه شهید بهشتی، چاپ دوم، ۱۳۷۴، ص ۹۶.

شوند، از تدابیر پیشگیرانهٔ غیرقهرآمیز که عمدتاً ناظر به پیشگیری از وقوع جرم هستند، نمی‌توان چنین توقعی داشت.

۱-۲-۱. *پیشگیری کیفری از جرائم رایانه‌ای در دیگر کشورها و عرصهٔ بین‌الملل*

جرائم رایانه‌ای به عنوان جلوه‌ای نوین از بزهکاری، از کارکردهای پیشگیرانهٔ مستقیم و غیرمستقیم ضمانت اجراهای قهرآمیز مستثنی نیستند و به همین خاطر، تمامی کشورها می‌کوشند با تصویب قوانین کیفری جدید یا اصلاح قوانین جزایی خود، این طیف جدید از جرائم را نیز در قلمرو حقوق کیفری خود وارد کنند.

اولین قانون در زمینهٔ جرائم رایانه‌ای در سال ۱۹۷۸ در ایالت فلوریدای ایالات متحده به تصویب رسید که با توجه به شرایط آن زمان فقط به کلاهبرداری[۱] و تعرض رایانه‌ای[۲] اشاره کرده بود. اما کشورهای دیگر و حتی دولت فدرال ایالات متحده تقریباً از سال ۱۹۸۰ به بعد اقدام به قانونگذاری در این حوزه کردند، به گونه‌ای که ابتدا دولت فدرال کانادا در سال ۱۹۸۳ در این زمینه قانون تصویب کرد و دولت فدرال ایالات متحده نیز در سال ۱۹۸۴ قانون سوءاستفاده و کلاهبرداری کامپیوتری[۳] را به تصویب رساند که به دلیل عدم وجود هیچ پیشینه‌ای در این حوزه، با مشکلات بسیاری مواجه شد، به گونه‌ای که تا سال ۱۹۹۰ این قانون چهار بار اصلاح شد و کماکان نیز بخش‌هایی از آن با ابهام مواجه است. دیگر کشورها نیز در اثر رویارویی با انواع سوءاستفاده‌های کامپیوتری، به تدریج اقدام به وضع قوانین و مقرراتی در این زمینه کرده‌اند.[۴]

---

1. Computer Fraud.
2. Intrusion.
3. US Federal Computer Fraud & Abuse Act.
4. Casey, Eoghan, Digital Evidence and Computer Crime, Second Edition, 2004, Chapter 2, p 26.

انعکاس این موضوع در قوانین و مقررات بین‌المللی را نیز نباید نادیده گرفت، چرا که تقریباً از همان ابتدای مطرح شدن جرائم رایانه‌ای، سازمان‌های بین‌المللی مهمی مانند سازمان توسعه و همکاری اقتصادی (OECD)، انجمن بین‌المللی حقوق جزا(AIDP) و سازمان ملل متحد به تعریف و طبقه‌بندی این جرائم پرداختند و پلیس بین‌الملل (اینترپل) نیز راهکارهای محرمانهٔ متنوعی جهت مقابله با این جرائم به همکاران خود در سراسر جهان ارائه کرده است،[۱] و بالاخره این موضوع تا حدی در عرصهٔ بین‌الملل دنبال شد که سرانجام در سال ۲۰۰۱ **کنوانسیون بین‌المللی جرائم** سایبر در بوداپست به همت شورای اروپا و چند کشور غیراروپایی به تصویب رسید و در آنجا اعضا مکلف شدند حداقل نسبت به جرائم مندرج در آن کنوانسیون مقررات کیفری مناسبی تدوین و به تصویب برسانند.[۲]

شاید مهم‌ترین دلیلی که می‌توان برای این توجه فوق‌العاده بیان داشت، طیف وسیع جرائمی است که امکان ارتکاب آنها در فضای تبادل اطلاعات وجود دارد. امروزه بحث **حفظ امنیت ملی در فضای تبادل اطلاعات** به یکی از چالش‌های اصلی کشورها بدل شده است، چرا که علاوه بر جرائمی مثل تبلیغ علیه یک کشور و اهانت به مقدسات آن، امکان هدف قرار دادن زیرساخت‌های اساسی آنکه به فضای تبادل اطلاعات متصل است نیز وجود دارد و ممکن است خساراتی که به بار می‌آید، از تهاجمات نظامی بسیار بیشتر باشد. به عنوان مثال، درست یک هفته پس از واقعهٔ یازدهم سپتامبر ۲۰۰۱، ویروسی به نام «نیمدا» در سیستم‌های رایانه‌ای ایالات متحده منتشر

---

۱. حسن بیگی (ابراهیم)، **آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی**، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی، ۱۳۸۲، صص۲۳۷-۲۵۳.

۲. لازم به ذکر است که در ۷ نوامبر ۲۰۰۲ نیز پروتکلی تحت عنوان جرم‌انگاری اعمال با ماهیت نژادپرستی و بیگانه‌ستیزی از طریق سیستم‌های رایانه‌ای نیز به این کنوانسیون الحاق شده است. http://conventions.coe.int/Treaty/en/Reports/Html/

شد و خسارات فراوانی به بار آورد. این واقعه چنان مورد توجه قرار گرفت که ایالات متحده تدوین استراتژی امنیت فضای تبادل اطلاعات را در دستور کار قرار داد و تا سپتامبر ۲۰۰۲ پیش‌نویس این استراتژی را تهیه کرد که در فوریهٔ ۲۰۰۳ نسخهٔ نهایی آن تصویب و ابلاغ شد.[۱] همچنین، گروه‌های سازمان‌یافته‌ای که همواره به آنها به عنوان معضلی فراملی و بین‌المللی نگریسته شده است، از این فضا حداکثر بهره‌برداری را به عمل می‌آورند که نمونه‌های آن را می‌توان در پول‌شویی با پول الکترونیک[۲]، سازمان‌دهی فعالیت‌های تروریستی در سراسر جهان، که **تروریسم سایبر** نام گرفته است، قاچاق مواد مخدر و زنان و کودکان مشاهده کرد.[۳] این چالش‌ها سوای از سوءاستفاده‌های جزئی است که در سطح وسیع و به شیوه‌های بسیار گوناگون در فضای تبادل اطلاعات انجام می‌شوند که از آن میان می‌توان به سرقت اطلاعات و نرم‌افزار، نقض حقوق مالکیت فکری افراد، توهین و تهدید اشاره کرد.

اما توجه به این نکته نیز ضروری است که جرائم رایانه‌ای و به خصوص مرتکبان آن از خصوصیات منحصربه‌فردی برخوردارند که آنها را با دیگر جرائم متفاوت می‌سازد و به همین دلیل، حتی کشورهایی که برای انعکاس هنجارهای حاکم بر فضای تبادل اطلاعات ضمانت اجراهای قهرآمیز مقرر

---

۱. حسن بیگی (ابراهیم)، **آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی**، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی، ۱۳۸۲، ص ۳۱۶.

2. Ehrlich, Timothy, To Regulate or Not? Managing The Risks of E-Money and Its Potential Application In Money Laundering Schemes, Harvard Journal of Law and Technology, Volume 11, Number 3, Summer 1998.

3. Richards, James, Transnational Criminal Organizations, Cyber Crime and Money Laundering: A Handbook for Law Enforcement Officers, Auditor, (1998).

کرده‌اند، در اجرا با لحاظ این شرایط و اوضاع و احوال به نحو دیگری عمل کرده‌اند که توجه به آنها نیز حائز اهمیت است. به عنوان مثال، در موارد متعددی دیده شده نفوذگران رایانه‌ای که متخصصین ماهری هستند، به جای حبس‌های سنگینی که در قانون مقرر شده، به خدمت در یک سازمان و ارائه خدمات فنی محکوم شده‌اند. کوین میتنیک، بزرگترین نفوذگر رایانه‌ای در دنیا، محکوم شد که تا پنج سال از سیستم رایانه‌ای استفاده نکند.(۱)

۱-۲-۲. پیشگیری کیفری از جرائم رایانه‌ای در ایران

از آنجا که بیش از چند سال از ورود فناوری اطلاعات و ارتباطات نوین به کشورمان نمی‌گذرد، بالطبع مسائل جانبی مربوط به آن نیز به تازگی مطرح شده و نمی‌توان انتظار داشت که همانند کشورهای پیشرو در این حوزه، اقدامات وسیعی انجام شده باشد. البته باید به این نکته نیز توجه داشت که بحث راجع به این نوع فناوری با دیگر فناوری‌های جدیدی که وارد کشور می‌شود، تا حدود زیادی متفاوت است. همان طور که پیش از این بیان شد، فضای تبادل اطلاعات، از چنان انعطاف‌پذیری‌ای برخوردار است که تقریباً می‌توان گفت در تمامی عرصه‌ها وارد شده و آنها را متحول کرده است. از طرف دیگر، قابلیت‌ها و امکاناتی که در اختیار نوع بشر قرار می‌دهد، چنان وسیع و گسترده است که روزبه‌روز بهره‌برداری از آن وسیع‌تر می‌شود و چهره‌های جدیدی به خود می‌گیرد. بنابراین، بدیهی است که سیاستگذاران و تصمیم‌گیران جامعهٔ ما باید به فکر چاره‌ای اساسی باشند.(۲) طبق آمارهای رسمی، تنها بیش از ده میلیون نفر از شبکهٔ اینترنت استفاده می‌کنند که اگر

---

1. Casey, Eoghan, Digital Evidence and Computer Crime, First Edition, 2001, p12.

۲. در میزان توجه و اهمیت دادن جامعهٔ ما به این حوزه همین بس که در طی سال جاری (۱۳۸۳) چندین همایش ملی و بین‌المللی در زمینه‌های بررسی ابعاد حقوقی فناوری اطلاعات و ارتباطات، دولت الکترونیک، تجارت الکترونیک، پول الکترونیک و بانکداری الکترونیک برگزار شده است.

بهره‌برداران از تلفن‌های همراه، تجارت و بانکداری الکترونیک و بسیاری دیگر از سیستم‌ها و دستگاه‌هایی که با دنیای دیجیتال سر و کار دارند را به این رقم بیفزاییم، حداقل نیمی از جمعیت کشورمان را دربرخواهد گرفت.

البته باید خاطرنشان کرد که تاکنون در حوزه‌های مختلف، اقداماتی قانونی جهت برخورد با برخی سوء استفاده‌های مورد نظر به عمل آمده است. به عنوان مثال، در اردیبهشت ۱۳۷۹، قانون اصلاح قانون مطبوعات به تصویب رسید و مطابق تبصرهٔ ۳ مادهٔ یک این قانون، کلیه نشریات الکترونیک مشمول این ماده قرار گرفتند که بدین ترتیب همه مسئولیت‌های کیفری، حقوقی و اجرائی این قانون نسبت به ناشران الکترونیک نیز قابل اعمال خواهد بود. هرچند باید اذعان داشت که به لحاظ فقدان تعریف مشخصی از نشر الکترونیک و ناشران الکترونیک و همچنین از آنجا که موضوع اولیه این قانون نشریات فیزیکی است، اجرای آن نسبت به نشریاتی که در قالب حامل‌های داده (نظیر لوح‌های فشرده) یا در فضای تبادل اطلاعات منتشر می‌شوند با ابهاماتی مواجه است.

همچنین، در آبان ۱۳۷۹ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای در راستای قانون حمایت از حقوق مؤلفان، مصنفان و پدیدآورندگان مصوب ۱۳۴۸ در ۱۷ ماده به تصویب رسید که در ماده ۱۳ آن برای ناقضان حقوق مزبور ضمانت اجرای کیفری پیش‌بینی شده است. هرچند باید اظهار داشت، که اجرای این قانون نیز به خاطر بروز یک سری ایرادهای آئین‌نامه‌ای که ریشه در خود قانون داشت، تا مدتی دَر هاله‌ای از ابهام بود.

اما در بهمن ۱۳۸۲، قانون تجارت الکترونیک که در قالب طرح به مجلس شورای اسلامی ارائه شده بود، در ۷۹ ماده به تصویب رسید که باب چهارم آن از مواد ۶۷ تا ۷۷ تحت عنوان جرائم و مجازات‌ها صراحتاً به تحمیل ضمانت اجرای کیفری به متخلفین این قانون پرداخته است. این باب به طور

کلی شامل چهار مبحث است: مبحث اول که در ماده ۶۷ آمده است، به کلاهبرداری کامپیوتری و مبحث دوم در ماده ۶۸ به جعل کامپیوتری اشاره دارد. مبحث سوم که به نقض حقوق انحصاری در بستر مبادلات الکترونیک پرداخته است خود شامل دو فصل است. فصل اول که مواد ۶۹ و ۷۰ به آن اختصاص یافته‌اند، با اشاره به مواد این قانون، تخلفات مربوطه را جرم‌انگاری کرده است. فصل دوم نیز که تحت عنوان حمایت از «داده‌پیام‌های شخصی/حمایت از داده» است، در مواد ۷۱، ۷۲ و ۷۳ منعکس شده است. مبحث چهارم این باب که تحت عنوان نقض حفاظت از «داده پیام» در بستر مبادلات الکترونیک است، خود شامل چهار فصل است: فصل اول که راجع به نقض حق مؤلف است، در ماده ۷۴ منعکس شده است. فصل دوم هم که ماده ۷۵ به آن اختصاص دارد راجع به نقض اسرار تجاری است. فصل سوم با عنوان نقض علایم تجاری در ماده ۷۶ آمده است و فصل چهارم نیز که ماده ۷۷ به آن اختصاص دارد، معلوم نیست از لحاظ عنوان و محتوا چه سنخیتی با سه فصل فوق دارد؛ چراکه به طور کلی تکلیف سایر جرائم، آئین دادرسی و مقررات مربوط به صلاحیت جزائی و روش‌های همکاری بین‌المللی قضائی جزائی مرتبط با بستر تبادلات الکترونیک را روشن می‌کند.

جدی‌ترین اقدامی که تاکنون در قلمرو جرائم رایانه‌ای انجام شده اشاره کنیم، تهیه پیش‌نویس لایحه قضایی مبارزه با جرائم رایانه‌ای توسط قوه قضائیه است که در صورت تصویب می‌توان آن را اولین سند نسبتاً جامع در زمینه پیشگیری کیفری از جرائم رایانه‌ای به شمار آورد. این لایحه طی مدت ۱۸ ماه کار مستمر گروهی از کارشناسان فنی و حقوقی در کمیته مبارزه با جرائم رایانه‌ای شورای عالی توسعه قضائی، تهیه شده است. طبق آخرین پیش‌نویس،[1] این لایحه به طور کلی شامل چهار بخش در قالب ۴۱ ماده

۱. جهت ملاحظه آخرین پیش‌نویس ر.ک: www.itna.ir

است. بخش اول شامل کلیات است که در آن همانند قانون تجارت الکترونیک یک سری اصطلاحات مهم مطرح شده در لایحه تعریف شده تا حدمقدور از بروز شبهه جلوگیری شود. بخش دوم به جرائم و مجازات‌ها می‌پردازد. این بخش شامل هشت فصل است. فصل اول آنکه راجع به جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی است، خود شامل سه مبحث می‌شود. مبحث اول راجع به دسترسی غیرمجاز، مبحث دوم راجع به شنود و دریافت غیرمجاز و مبحث سوم راجع به جرائم علیه امنیت ملی است. فصل دوم نیز که به جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی اختصاص دارد، خود شامل سه مبحث است. مبحث اول راجع به جعل، مبحث دوم راجع به تخریب و ایجاد اختلال در داده‌ها و مبحث سوم راجع به اختلال در سیستم می‌باشد. فصل سوم نیز به کلاهبرداری اختصاص دارد و در فصل چهارم جرائم مرتبط با محتوا آمده است. فصل پنجم راجع به افشای سر است و در فصل ششم مسئولیت کیفری ارائه دهندگان خدمات تبیین شده است. فصل هفتم در قالب یک ماده که در دو بند تشریح شده، سایر جرائم را مطرح می‌کند. فصل هشتم این بخش نیز به تخفیف و تشدید مجازات‌ها می‌پردازد.

بخش سوم که آئین دادرسی جرائم رایانه‌ای را مطرح می‌کند، خود شامل دو فصل است. فصل اول راجع به صلاحیت است و فصل دوم که تحت عنوان جمع‌آوری ادله الکترونیک می‌باشد، شامل پنج مبحث است. مبحث اول به نگهداری داده‌ها، مبحث دوم به حفظ فوری داده‌ها، مبحث سوم به افشای داده‌ها، مبحث چهارم به تفتیش و توقیف داده‌ها و سیستم‌ها و مبحث پنجم به شنود داده‌ها اشاره دارد. بخش چهارم این لایحه نیز راجع به معاضدت بین‌المللی است.

آنچه باید مورد توجه قرار گیرد این است که مبنای تدوین این لایحه کنوانسیون جرائم سایبر است. هرچند باید اذعان داشت که برخی از مقررات

آن نظیر نقض حق نشر[1] مورد اشاره قرار نگرفته است که به نظر می‌رسد علت اصلی آن فراهم نبودن زمینه‌های لازم، نظیر پیوستن به یک سری کنوانسیون‌های دیگر بوده است. اما آنچه در چشم‌انداز تصویب این لایحه مشاهده می‌شود، الحاق به این کنوانسیون بین‌المللی است که در نوع خود مزایای بسیاری را برای کشورمان به ارمغان خواهد آورد.

نکته آخر در این قسمت اینکه هم اکنون یک سری اقدامات دیگر در قالب طرح و لایحه مراحل تصویب خود را طی می‌کنند که با تصویب آنها، حوزه پیشگیری کیفری از جرائم رایانه‌ای در کشورمان گسترده‌تر نیز خواهد شد که از جمله آنها می‌توان به طرح استفاده از شبکه‌های اطلاع‌رسانی رایانه‌ای که یک فوریت آن نیز به تصویب رسیده و لایحه «قانون آزادی اطلاعات» اشاره کرد.[2]

۲. پیشگیری غیرکیفری از جرائم رایانه‌ای

پیشگیری تنها به حوزهٔ علوم جنایی محدود نمی‌شود و در هر حوزه‌ای که یک سری ناهنجارها وجود داشته باشد، سعی می‌شود از طریق اتخاذ تدابیر پیشگیرانه از وقوع آنها جلوگیری شود، چرا که این اتفاق نظر وجود دارد که «پیشگیری بهتر از درمان است». البته این نکته قابل توجه نیز وجود دارد که ممکن است یک پدیده در چند حوزه ناهنجار محسوب شود و به این ترتیب، از ابعاد مختلف در کانون توجه قرار گیرد. جرم یا بزه در مفهوم عام خود (و نه در تعریف مضیق قانونی آن) یکی از این پدیده‌هاست که در حوزه‌های دیگری مثل علوم اجتماعی، روان‌شناسی و... نیز مورد توجه قرار می‌گیرد.

همین چندگانه‌نگری به پدیدهٔ جرم باعث شده که در عصر حاضر (به

---

1. Copyright.

۲. جهت ملاحظه این لایحه ر.ک: www.itna.ir

خصوص سی سال اخیر)، بررسی کارکردهای پیشگیرانهٔ غیرکیفری در حوزهٔ علوم جنایی به طور جدی مورد توجه قرار گیرد و تا آنجا پیش رود که عده‌ای حوزهٔ پیشگیری از جرائم را فقط اقدامات غیرقهرآمیز بدانند. خصوصاً آنکه در چند دههٔ اخیر ناکارامدی اقدامات قهرآمیز و کیفری جهت مقابله با جرائم به ویژه در زمینهٔ پیشگیری از وقوع آنها به طرق مختلف به اثبات رسیده است.(۱)

در این راستا، الگوهای گوناگونی از رشته‌های مختلف در حوزهٔ علوم جنایی پیاده شده‌اند که البته هر یک بعد خاصی را مدنظر قرار داده‌اند و به همین خاطر با نواقصی مواجه می‌باشند. اما کامل‌ترین الگویی که تا به حال ارائه شده، پیشگیری اجتماعی و وضعی از جرائم است(۲) که ما نیز سعی می‌کنیم همین الگو را در مورد جرائم رایانه‌ای بررسی کنیم.

۲-۱. پیشگیری اجتماعی از جرائم رایانه‌ای

همان‌گونه که از نام این پیشگیری پیداست، مجموعه اقدامات و تدابیری است که بر خود فرد تأثیر می‌گذارد و از این طریق خلأها و ناهنجاری‌های وی را برطرف می‌کند. این تأثیرگذاری از دو جهت صورت می‌گیرد: از یک سو نحوهٔ تربیت و آموزش فرد در طول رشد، بخصوص در دوران کودکی تحت‌نظر قرار می‌گیرد تا از شکل‌گیری خصوصیات مجرمانه در او جلوگیری شود،(۳) به همین دلیل، این نوع پیشگیری، پیشگیری رشدمدار و زودرس نامیده می‌شود. اما روی دیگر تأثیرگذاری پیشگیری اجتماعی، مداخله در

---

۱. نجفی‌ابرندآبادی (علی‌حسین)، **تقریرات درس جرم‌شناسی دوره کارشناسی ارشد**، نیم سال دوم تحصیلی ۸۲-۸۱، مجتمع آموزش عالی قم، تنظیمی سبدزاده (مهدی)، ص ۱۵۶.

۲. نجفی‌ابرندآبادی (علی‌حسین)، **تقریرات درس جرم‌شناسی دورهٔ دکتری**، نیم‌سال اول تحصیلی ۸۰-۷۹، دانشگاه تربیت مدرس، تنظیمی بابایی (محمدعلی)، ص ۱۸.

۳. کاری‌یو (روبرو)، **مداخلهٔ روان‌شناختی ـ اجتماعی زودرس در پیشگیری از رفتارهای مجرمانه**، ترجمه نجفی‌ابرندآبادی (علی‌حسین)، مجلهٔ تحقیقات حقوقی، شمارهٔ ۳۶-۳۵، سال ۱۳۸۱، ص ۲۷۴.

محیط‌های تربیتی و آموزشی خرد و کلان مسلط بر فرد است، مانند خانواده، مدرسه، محیط‌های فرهنگی، اجتماعی، اقتصادی و... تا از طریق بالا بردن سطح آگاهی آنها و هدایتشان به سمت قانونمندی و هنجارمندی، زمینه‌های رشد خصوصیات مجرمانه در فرد را خنثی کنند. با این توضیح، باید گفت پیشگیری اجتماعی در حوزهٔ جرائم رایانه‌ای از اهمیت قابل توجهی برخوردار است و در توجیه آن حداقل می‌توان به دو دلیل اشاره کرد:

۱ـ جرائم رایانه‌ای از ویژگی‌هایی برخوردارند که اتخاذ تدابیر پیشگیرانهٔ وضعی که در بخش بعد مورد بررسی قرار می‌گیرند را تا حد زیادی خنثی می‌کنند.

۲ـ طیف وسیعی از مجرمان و بزهدیدگان این جرائم را افراد کم‌سال و جوان تشکیل می‌دهند[۱] و همان طور که گفته شد، این گروه مخاطبان اصلی تدابیر پیشگیرانه اجتماعی هستند. به این ترتیب، چنانچه یک برنامهٔ منسجم و کارامد برای این گروه طرح‌ریزی شود و آنها با این دنیای جدید و خطرات بالقوهٔ آن آشنا شوند، تا حد زیادی می‌توان از الحاق آنها به طیف مجرمان و بزهدیدگان جلوگیری کرد.

البته باید خاطرنشان ساخت که آموزش و آگاه‌سازی افراد بزرگسال از خطرات و آسیب‌پذیری‌های این دنیای جدید نیز امری ضروری است. چرا که بخش بزرگی از بزهدیدگی جرائم رایانه‌ای به خاطر ناآشنایی یا کمی آگاهی از فضای تبادل اطلاعات است و بنابراین می‌توان گفت، پیشگیری اجتماعی در جرائم رایانه‌ای نسبت به افراد بزرگسال نیز نتیجه‌بخش می‌باشد.

اما مهم‌ترین نکته‌ای که باید در بحث پیشگیری اجتماعی از جرائم

---

۱. در این زمینه می‌توان به مثال‌های بسیاری اشاره کرد. اما در یک مورد، یک نوجوان پانزده سالهٔ نروژی به نام جان جوهانسن الگوریتم رمزنگاری محتوای دستگاه‌های دی‌وی‌دی که برای استفاده مجاز طراحی شده بود را شکست و با قرار دادن کد رمزگشای آن در شبکه جهانی وب، خسارات هنگفتی را به صاحبان این صنعت وارد آورد.

رایانه‌ای مدنظر داشت، این است که ما در این حوزه با مجرمان و بزهدیدگان عادی مواجه نیستیم. هر دو گروه، علاوه بر اینکه از دانش کافی بهره‌برداری از فضای تبادل اطلاعات برخوردارند، ابزارها و لوازم مورد نیاز آن را نیز در اختیار دارند. تمامی این افراد از بهرهٔ هوشی بالایی برخوردارند و اصولاً اشخاص با بهرهٔ هوشی پایین نمی‌توانند مجرم یا حتی گاه بزهدیدهٔ جرائم رایانه‌ای باشند. شاید از این لحاظ بتوان مجرمان جرائم رایانه‌ای را در جرگهٔ **مجرمان یقه سفیدی** که پروفسور ادوین ساترلند برای اولین بار از آنها سخن گفته بود قرار داد و به این ترتیب چنین نتیجه‌گیری کرد که تدابیر پیشگیرانهٔ اجتماعی برای گروه به اصطلاح یقه آبی که جرائم آنها بیشتر جنبهٔ خشونت‌آمیز دارد و در آنها نقش فسفر کم‌رنگ است، کارایی ندارد.

البته اشاره به این نکته نیز مفید است که متأسفانه وجود این عامل مشترک در میان تمامی جرائم رایانه‌ای و قرار گرفتن این مجرمان در طبقهٔ یقه‌سفیدها موجب شده که تا به امروز آن چنان که باید در حوزهٔ پیشگیری غیرکیفری مورد توجه قرار نگیرند. هرچند این معضل تنها متوجه این گروه از جرائم یقه سفیدها نیست و همان طور که مارک آنسل در کتاب دفاع اجتماعی خود اشاره کرده[1]، با اینکه جرائم یقه سفید آثار بسیار زیانبارتری برای جامعه دارند، اما از آنجا که جرائم خشونت‌آمیز نمود بیشتری دارند و مسلماً دولت‌ها نیز بهتر می‌توانند از آنها بهره‌برداری سیاسی داشته باشند و تا حدودی می‌توان گفت بخشی از جرائم یقه‌سفید نیز به خود آنها مربوط می‌شود، عملاً بحث راجع به پیشگیری و مقابله با این جرائم با جدیت دنبال نمی‌شود.

---

۱. آنسل (مارک)، **دفاع اجتماعی**، ترجمهٔ آشوری (محمد) و نجفی‌ابرندآبادی (علی‌حسین)، چاپ سوم، ۱۳۷۵، ص ۱۱۹.

۲-۱-۱. محدودیت‌های پیشگیری اجتماعی از جرائم رایانه‌ای

با اینکه پیشگیری اجتماعی یکی از کامل‌ترین الگوهای پیشگیری است، اما باز هم با محدودیت‌ها و نواقصی مواجه است. در این بخش به‌طور مختصر به نارسایی‌های این حوزهٔ پیشگیری نسبت به جرائم رایانه‌ای اشاره می‌کنیم.

همان‌طور که اشاره شد، کارکرد اصلی پیشگیری اجتماعی، تربیت و آموزش است. بنابراین، اگر این خط‌مشی نسبت به یک مجرم یا بزهدیدهٔ بالفعل یا بالقوه کارگر نباشد، باید به دنبال طرق دیگر پیشگیری رفت. اتفاقاً در جرائم رایانه‌ای نمونه‌های این چنین بسیار است. زیرا همان طور که گفته شد، کسانی که با فضای تبادل اطلاعات در ارتباط‌اند، از بهرهٔ هوشی نسبتاً بالایی برخوردارند و در حقیقت خود می‌دانند که چه می‌کنند و اگر قبح یا خطرپذیری عملی برایشان مسجل نشود، به راحتی از انجام آنچه منجر به بزهکاری یا بزهدیدگی می‌شود، سر باز نمی‌زنند. گروه کوچکی از مجرمان که از بهرهٔ هوشی بسیار بالایی برخوردارند و تعدادشان در سراسر جهان بسیار کم است، خطرناک‌ترین و زیانبارترین جرائم رایانه‌ای را مرتکب می‌شوند و مسلم است که اتخاذ تدابیر پیشگیرانهٔ اجتماعی نسبت به چنین اشخاصی پاسخگو نمی‌باشد، یا حتی کارمند شرکتی که به قصد انتقام یا تحصیل نامشروع منافع مادی علیه شرکت خود مرتکب جرم رایانه‌ای می‌شود، ممکن است اتخاذ چنین تدابیری نسبت به وی ثمربخش نباشد.

به نظر می‌رسد مهم‌ترین عاملی که پیشگیری اجتماعی از جرائم رایانه‌ای را با شکست مواجه می‌سازد، امکان ارتکاب این‌گونه جرائم در خلوت می‌باشد. مسلماً تربیت و آموزش، برای تلقین شخص به خودداری از ارتکاب جرم و نقض نکردن هنجارهاست. اما باید دید این راهکار تا چه اندازه در جلوگیری از ارتکاب جرم در خلوت اشخاص مؤثر است. بسیار دیده شده شخصیت اشخاص در دنیای فیزیکی با فضای تبادل اطلاعات نمودهای کاملاً متفاوتی داشته‌اند. ممکن است شخص در دنیای فیزیکی استاد

دانشگاه، مدیر کل یک شرکت، یک چهرهٔ مذهبی متشخص یا انسانی فرهیخته باشد، ولی در فضای تبادل اطلاعات که در خلوت خود به آن راه یافته است، تمایلات منحرفانهٔ سادیستی یا مازوخیستی خود را بروز دهد. امکان ارتکاب انواع بسیاری از جرائم رایانه‌ای در خلوت، بی‌آنکه عامل مداخله‌گری هم وجود داشته باشد، ظرفیتی است که فضای تبادل اطلاعات به بشر ارزانی داشته است و معضلی است برای سیاستگذاران خرد و کلان جامعه که چگونه با این گونه ناهنجاری‌ها برخورد کنند.(۱)

بنابراین، به طور خلاصه می‌توان چنین نتیجه گرفت که پیشگیری اجتماعی از جرائم رایانه‌ای با دو معضل اساسی مواجه است: ۱ـ تنوع بسیار گستردهٔ این جرائم، از جرائم علیه امنیت ملی گرفته تا جرائم سازمان‌یافته و جرائم فردی مثل آزار و اذیت، باعث شده مرتکبان و بزهدیدگان این جرائم، قشرهای مختلف جامعه و حتی دولت‌ها را نیز دربرگیرد. به این ترتیب، بدیهی است وضع تدابیر پیشگیرانهٔ اجتماعی که بتواند تمامی جرائم این حوزه را در برگیرد، کاری بس دشوار است و ممکن است در بعضی زمینه‌ها هم پاسخگو نباشد. ۲ـ امکان ارتکاب جرائم رایانه‌ای در خلوت، ثمربخش بودن این گونه تدابیر پیشگیرانه را با اما و اگرهایی مواجه ساخته است.

۲ـ۱ـ۲. پیشگیری اجتماعی از جرائم رایانه‌ای در ایران

از ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای که به معنای واقعی کلمه به فضای تبادل اطلاعات در کشور عینیت بخشیده‌اند، بیش از چند سال نمی‌گذرد و به همین خاطر نباید انتظار داشت که نسبت به چالش‌های ناشی از آن، اقدامات قابل توجهی صورت گرفته باشد. اما اقبال گسترده و روزافزون جامعهٔ ما،

---

۱. در کتاب Digital Evidence and Computer Crime (Eoghan Casey, 2001) که توسط نگارنده در دست ترجمه است، نمونه پرونده‌های بسیار جالبی ارائه شده که توجه به آنها می‌تواند تا حدود زیادی تمایزات شگفت‌انگیز فضای تبادل اطلاعات و دنیای فیزیکی و قابلیت‌های فوق‌العادهٔ آن را از دیدگاه جرم‌شناختی روشن کند.

همانند جامعهٔ جهانی، برای بهره‌برداری از این فضا به ما این هشدار را می‌دهد که هرچه سریع‌تر باید به فکر چاره‌جویی باشیم. با اینکه تاکنون مطالب و برنامه‌های پراکنده و متنوعی در زمینه چالش‌های مختلف این فضا در رسانه‌های ارتباط جمعی کشورمان منتشر شده است، اما به نظر می‌رسد باید اقدامات نظام‌مند و هدف‌داری انجام شود. به عنوان مثال، چندی است طرح اتصال تمامی مدارس کشور به شبکهٔ جهانی اینترنت مطرح شده است و به این ترتیب، به قشر نوجوان ما که مخاطب اصلی پیشگیری اجتماعی از جرائم محسوب می‌شوند، اجازه داده می‌شود بدون هیچ گونه آموزش صحیح و آشنایی با خطرات و آسیب‌های این فضا به آن دسترسی یابند. چه خوب است متصدیان فرهنگی جامعهٔ ما که متولی آشنا کردن قشر نوجوان و جوان ما با فناوری‌های نوین شده‌اند، اقدامات مؤثری در زمینهٔ آگاه‌سازی آنها از چالش‌ها و آسیب‌های این فضا نیز انجام دهند.

البته لازم به ذکر است که بحث پیشگیری اجتماعی تنها به گروه فوق محدود نمی‌شود و همان‌طور که می‌دانیم اقشار گوناگون با آگاهی‌های مختلف و در زمینه‌های مختلف با این فضا ارتباط برقرار می‌کنند که ضروری است برای هر یک از آنها به فراخور نوع بهره‌برداری‌شان برنامه‌های آموزشی تدارک دیده شود.

۲-۲. پیشگیری وضعی از جرائم رایانه‌ای

همان طور که از نام این پیشگیری پیداست، به جای تکیه بر فرد، بر محیط توجه دارد. آن هم محیطی که ممکن است در آن یک انسان متعارف مرتکب جرم شود. آنچه در این نوع پیشگیری مفروض گرفته می‌شود، این است که انسان علی‌الاصول منطقی و حساب‌شده عمل می‌کند و مرتکب ریسک شدید نمی‌شود. بر این اساس، آنچه در این نوع پیشگیری دنبال می‌شود، این است که با جاذبه‌زدایی از سیبل جرم، بالا بردن هزینه و کاهش احتمال نتیجه‌گیری از جرم، زمینهٔ ارتکاب آن را از بین ببریم یا تا حد قابل قبولی پایین

بیاوریم.[۱] این نوع پیشگیری اساساً بزهدیده‌مدار تلقی می‌شود و بنابراین، با پیشگیری اجتماعی که بزهکار را در کانون توجه خود قرار می‌دهد، متفاوت است. هرچند در اینجا نیز مجرم به صورت غیرمستقیم مطرح می‌باشد.[۲]

پس از این توضیح مختصر، در زمینهٔ پیشگیری وضعی از جرائم رایانه‌ای باید گفت با اینکه مشکلات بسیاری بر سر راه آن وجود دارد، اما باز هم از جایگاه خاصی برخوردار است. یکی از دلایلی که می‌توان جهت توجیه پیشگیری وضعی از این جرائم برشمرد، قابلیتی است که فضای تبادل اطلاعات فراهم آورده است. همان طور که گفته شد، جرم رایانه‌ای به گونه‌ای است که نمی‌توان با دست تهی مرتکب آن شد و باید علاوه بر صرف اندیشه کافی، ابزارها و لوازم مورد نیاز را هم در اختیار داشت. اما این بدین معنا نیست که برای ارتکاب قسمت عمده‌ای از این جرائم باید تخصص و مهارت فوق‌العاده داشت، بلکه اگر از دانش کافی جهت بهره‌برداری ابتدایی از سیستم‌های رایانه‌ای برخوردار باشید، خود فضای تبادل اطلاعات امکاناتی در اختیار شما قرار می‌دهد که زمینه برای وقوع جرم مساعد می‌شود. از این رو، آنچه در پیشگیری وضعی از جرائم رایانه‌ای دنبال می‌شود، این است که با اتخاذ تدابیر فنی، از بهره‌برداری از این گونه قابلیت‌های جرم‌برانگیز این فضا جلوگیری شود. به عبارت دیگر، مخاطبان اصلی پیشگیری وضعی از جرائم رایانه‌ای کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای تبادل اطلاعات در اختیار آنها قرار می‌دهد مرتکب جرم شوند، نه اینکه خود دست به ابتکار عمل بزنند که در این صورت، همان‌طور که در ادامه توضیح داده خواهد شد، از

---

۱. صفاری (علی)، **مبانی نظری پیشگیری وضعی**، مجلهٔ تحقیقات حقوقی، شماره ۳۳-۳۴، ص۲۹۲.

۲. نجفی‌ابرندآبادی (علی‌حسین)، **تقریرات درس جرم‌شناسی دوره کارشناسی ارشد**، نیم سال دوم تحصیلی ۸۲-۸۱، مجتمع آموزش عالی قم، تنظیمی سیدزاده (مهدی)، ص ۱۷۱.

پیشگیری وضعی کاری ساخته نخواهد بود.

دلیل مهم دیگری که باعث شده پیشگیری وضعی در جرائم رایانه‌ای با تمام کاستی‌های آن دنبال شود، بحث **شبکه‌های اطلاع‌رسانی رایانه‌ای** است. تقریباً می‌توان گفت هرگونه اقدامی در فضای تبادل اطلاعات مستلزم این است که از طریق شبکه‌های اطلاع‌رسانی رایانه‌ای بدین فضا وارد شویم، آن هم شبکه‌هایی که در دنیای امروز به طور تخصصی فعالیت می‌کنند و هر یک به ارائه یک نوع خدمات در فضای تبادل اطلاعات می‌پردازند و از همه مهم‌تر اینکه تحت نظارت دولت و مقررات قانونی لازم‌الاجرا هستند. در حقیقت، این شبکه‌ها پل ارتباطی ما با فضای تبادل اطلاعات هستند و به این ترتیب اگر در این پل ارتباطی اقدامات پیشگیرانهٔ وضعی مؤثری اعمال شود، می‌توان امیدوار بود که تا حدودی از وقوع جرائم در فضای تبادل اطلاعات جلوگیری می‌شود. این وضعیت مزیتی برای پیشگیری وضعی از این جرائم محسوب می‌شود که پیشگیری وضعی از جرائم سنتی از آن بی‌بهره است. چرا که در آنجا هیچ عامل مؤثری را نمی‌توان میان سیبل جرم و مجرم قرار داد. آنچه امروزه در قالب نصب دیوار آتشین[۱] یا پالایه (Filtering) در این شبکه‌ها انجام می‌شود، چیزی جز پیشگیری وضعی نمی‌باشد. در اینجا به مجرمان اجازه داده نمی‌شود که به راحتی به مقصود خود نائل شوند.[۲] همچنین، با پیدایش پدیده‌هایی چون پلیس گشت سایبر[۳]، پیشگیری وضعی در این فضا جلوه‌های دیگری نیز به خود گرفته است که البته با الهام از نتایج مثبت پلیس گشت پیاده به عنوان یک اقدام وضعی پیشگیرانه به اجرا در آمده است.[۴] اما

---

1. Firewall.

۲. البته باید خاطرنشان کرد که پیشگیری وضعی تنها به شبکه‌های اطلاع‌رسانی رایانه‌ای ختم نمی‌شود، بلکه برنامه‌های ویروس‌یاب یا کوکی‌یابی که اشخاص نیز بر روی رایانه‌های شخصی‌شان اجرا می‌کنند نیز پیشگیری وضعی محسوب می‌شود.

3. Cyber Patrol.

۴. نجفی‌ابرندآبادی (علی‌حسین)، **پیشگیری از بزهکاری و پلیس محلی**، مجلهٔ تحقیقات حقوقی،

اینکه تا چه اندازه این اقدامات در فضای تبادل اطلاعات پاسخگو باشند، هنوز تردیدهایی وجود دارد.

البته این نکته را نباید از یاد برد که از آنجا که شبکه‌های اطلاع‌رسانی رایانه‌ای نقش مهمی در فضای تبادل اطلاعات به عهده دارند، می‌توان در زمینهٔ پیشگیری اجتماعی از جرائم رایانه‌ای نیز اعتبار ویژه‌ای برای آنها باز کرد و به یقین می‌توان گفت یکی از عوامل مؤثری هستند که می‌توانند نقش مهمی در این زمینه بر عهده داشته باشند. به عنوان مثال، هر یک از این شبکه‌ها می‌توانند در سایت‌های خود بر اساس نوع خدماتی که ارائه می‌دهند، مخاطبان خود را با خطرات و آسیب‌هایی که ممکن است متوجه آنها باشد آشنا کنند و از طرف دیگر با هشدارهای لازم و تبیین این موضوع که سوءاستفاده از خدماتشان با چه عواقبی مواجه می‌باشد، از بروز جرائم رایانه‌ای نیز جلوگیری کنند.

آخرین دلیلی که می‌توان جهت توجیه پیشگیری وضعی از جرائم رایانه‌ای ذکر کرد، به ویژگی منحصربه‌فرد فضای تبادل اطلاعات مربوط می‌شود. در این فضا شخص می‌تواند بر خلاف دنیای فیزیکی در یک زمان در چند نقطه ظاهر شود و با انجام یک عمل بر چند نقطه تأثیر بگذارد. به عنوان مثال، یک مجرم می‌تواند از طریق شبکه به تعداد بسیاری کامپیوتر میزبان متصل شود و به طور همزمان در فعالیت تمامی آنها اختلال ایجاد کند یا با آنها ارتباط زنده برقرار کند و مرتکب اشکال مختلفی از عناوین مجرمانه شود. البته باید توجه داشت که این خصیصه سوای از حوزهٔ تأثیرگذاری فضای تبادل اطلاعات است که نسبت به دنیای فیزیکی، حوزه بسیار گسترده‌تری را دربرمی‌گیرد. نشر مطالب تحریک‌آمیز علیه امنیت ملی یا مطالب توهین‌آمیز نسبت به مقدسات مذهبی یا تصاویر حاوی هرزه‌نگاری کودکان در این فضا، گستره‌ای

شماره ۲۶ـ۲۵، سال ۱۳۷۸، ص۱۳۸.

به بزرگی این جهان را دربرمی‌گیرد، در حالی که اگر قرار باشد این عمل در دنیای فیزیکی به همان اندازه گستردگی داشته باشد، می‌بایست ده‌ها هزار عکس یا اوراق مربوطه چاپ و تکثیر شود که البته هنوز هم در تأثیرگذاری آن به اندازهٔ این فضا تردید وجود دارد. از این رو، حتی اگر در پیشگیری از این گونه جرائم درصد کمی توفیق وجود داشته باشد و لازم باشد هزینه‌های گزافی برای آن صرف شود، به نظر می‌رسد نسبت به زیانبار بودن این جرائم، باز هم قابل قبول و توجیه‌پذیر باشد.

۲ـ۲ـ۱. *محدودیت‌های پیشگیری وضعی از جرائم رایانه‌ای*

همان طور که اشاره شد، پیشگیری وضعی در فضای تبادل اطلاعات با محدودیت‌های بسیاری مواجه است که البته بخشی از آنها نسبت به فضای فیزیکی هم صادق هستند. به طور کلی، این محدودیت‌ها را می‌توان در دو بخش مورد بررسی قرار داد: ۱ـ محدودیت‌های فنی؛ ۲ـ محدودیت‌های قانونی.

۲ـ۲ـ۱ـ الف) محدودیت‌های فنی:

به نظر می‌رسد بزرگ‌ترین مشکلی که در زمینه پیشگیری وضعی از جرائم رایانه‌ای وجود دارد، توسعه و ارتقای فناوری، آن هم به صورت ثانیه‌شمار می‌باشد که البته بر هیچ کس پوشیده نیست که بخشی از این رشد و توسعه را مجرمان رایانه‌ای به عهده دارند. به کرات مشاهده می‌شود، چند روز از اجرای یک طرح فنی پیشگیرانهٔ وضعی نمی‌گذرد که راه‌های خنثی‌کنندهٔ آن در فضای تبادل اطلاعات در اختیار همگان قرار می‌گیرد و عملاً پیشگیری وضعی مزبور کان لم یکن می‌شود. این معضل هنگامی بیشتر در کانون توجه قرار می‌گیرد که هزینهٔ مالی و فرصت تهیهٔ یک برنامه یا ابزار پیشگیرانه را که بعضاً بسیار هنگفت است نیز به آن بیفزاییم. بنابراین، همان طور که در دنیای فیزیکی این ایراد گرفته می‌شود، این نوع پیشگیری یک حالت مسکن و

مقطعی دارد و راه‌حل اساسی تلقی نمی‌شود.[۱]

دومین محدودیت فنی که پیشگیری وضعی از جرائم رایانه‌ای با آن مواجه است، وجود ابزارها و فناوری‌هایی در فضای تبادل اطلاعات می‌باشد که این امکان را در اختیار اشخاص قرار می‌دهد که در نهایت با ناشناس ماندن[۲] و پنهان کردن محتوای فعالیت‌های خود، به بهره‌برداری از این فضا بپردازند. به عنوان مثال، محیط‌هایی وجود دارند که به اشخاص این امکان را می‌دهند که به صورت زنده با یکدیگر ملاقات می‌کنند و با اطمینان از ورود اشخاص بیگانه جلوگیری کنند. بدون تردید، چنین فضاهایی برای ارتکاب اعمال مجرمانه بسیار جذاب می‌باشند و عملاً می‌توان گفت با توجه به محدودیت‌های فنی و قانونی‌ای که وجود دارد، تعقیب و پیگرد فعالیت‌های مجرمانه در این فضاها با چالش‌های بسیاری مواجه است. البته این موضوع سوای از یک سری قابلیت‌ها می‌باشد که با استفاده از آنها می‌توان ماهیت بهره‌برداری خود را به گونه‌ای مشروع جلوه داد و عملاً تمهیدات پیشگیرانهٔ وضعی را دور زد یا از فناوری رمزنگاری[۳] استفاده و عملاً محتوای فعالیت‌های خود را پنهان کرد.

۲ـ۲ـ۱ـ ب) محدودیت‌های قانونی:

مهم‌ترین مشکل قانونی که پیشگیری وضعی از جرائم رایانه‌ای با آن مواجه است، بحث به خطر افتادن حریم خصوصی افراد در فضای تبادل اطلاعات است. حریم خصوصی[۴] یا آنچه از آن به عنوان «حق تنها ماندن»[۵] یاد می‌شود، برای اولین بار در سال ۱۸۹۰ میلادی توسط دو نویسندهٔ مشهور به

---

۱. نجفی‌ابرندآبادی (علی‌حسین)، **تقریرات درس جرم‌شناسی**، دوره کارشناسی ارشد، نیم‌سال دوم تحصیلی ۸۲ـ۸۱، مجتمع آموزش عالی قم، تنظیمی سیدزاده (مهدی)، ص ۱۸۵.

2. Anonymity.

3. Encryption.

4. Privacy.

5. Let to be alone.

نام‌های ساموئل وارن و لوئیس براندیس مطرح شد. در آن زمان که حدود یک قرن از تصویب قانون اساسی ایالات متحده می‌گذشت، دولت با دستاویزهای مختلف قانونی سعی می‌کرد در زندگی خصوصیِ افراد مداخله کند و از این طریق برای آنها مشکلاتی ایجاد می‌کرد. این اقدامات، انتقادهای گسترده‌ای را برانگیخت، تا آنجا که دیوان عالی ایالات متحده برای اولین بار راجع به این موضوع تصمیماتی اتخاذ کرد و به این ترتیب، پس از مدتی قوانین مختلفی در سطح فدرال در حمایت از حریم خصوصی به تصویب رسید. حتی در اصلاحیهٔ چهارم قانون اساسی نیز به صراحت به این موضوع اشاره شده است.(۱)

با ظهور فناوری‌های نوینی چون تبادل الکترونیک اطلاعات، حریم خصوصی افراد در معرض تعرضات بیشتری قرار گرفت، به همین دلیل ایالات متحده با تصویب قوانینی نظیر **قانون حمایت از حریم خصوصی ارتباطات الکترونیک**(۲) صراحتاً به حمایت از آن پرداخت و دولت را در تدوین تدابیر پیشگیرانه وضعی، بخصوص شنود ارتباطات الکترونیک، با محدودیت‌های بسیاری مواجه کرد.(۳)

البته باید توجه داشت که لزوم پرداختن به حریم خصوصی به حوزهٔ بین‌الملل نیز کشیده شده است و از آن جمله می‌توان به قطعنامه‌های اتحادیهٔ اروپا در لزوم رعایت حریم خصوصی افراد اشاره کرد.(۴) حتی کنوانسیون

---

1. Bortner, Mark, Cyber Laundering: Anonymous Digital Cash and Money Laundering, 1996.
2. Electronic Communication Privacy Act (1986).
۳. البته باید خاطرنشان کرد که وزارت دادگستری ایالات متحده جهت تبیین مفاهیم مذکور، در سال ۱۹۹۴ کتابچه‌ای راهنما با عنوان «تفتیش و توقیف کامپیوترها و تحصیل ادلهٔ الکترونیک در تحقیقات جنائی» منتشر کرده که در سال‌های ۱۹۹۸ و ۲۰۰۲ نیز آن را مطابق شرایط جدید اصلاح و روزامد کرده است.
۴. در این زمینه می‌توان به دستورالعمل EC/۶۶/۹۷ پارلمان و شورای اروپا به تاریخ ۱۵ دسامبر

جرائم سایبر در ماده ۱۵ خود با عنوان شروط و تضمین‌ها، دولت‌های عضو را موظف کرده به هنگام وضع قوانین و مقررات مطابق این کنوانسیون، حقوق و آزادی‌های فردی از جمله رعایت حریم خصوصی افراد را مطابق قوانین و مقررات بین‌المللی دقیقاً رعایت کنند.

بنابراین، همان طور که ملاحظه می‌شود، از آنجا که تدابیر پیشگیرانهٔ وضعی به طور مستقیم یا غیر مستقیم (مانند تدابیر خودتقنینی[1] شبکه‌های اطلاع‌رسانی رایانه‌ای که به موجب قانون اتخاذ می‌کنند) به دولت‌ها مربوط می‌شود و این احتمال وجود دارد که آنها با مستمسک قرار دادن مبارزه با جرائم و تعقیب و پیگرد مجرمان به حریم خصوصی افراد تعرض کنند، باید با وضع قوانین جامع و کارامد، اعمال اختیار و صلاحدید آنها را محدود به مصرحات قانونی کرد و مستلزم سیر تشریفات قانونی دانست.[2]

بدون تردید، حریم خصوصی یکی از ارکان اصلی پابرجا ماندن فضای تبادل اطلاعات محسوب می‌شود و اگر ذره‌ای در حمایت از آن تردید شود، به شدت در میزان بهره‌برداری از آن تأثیر نامطلوب خواهد داشت و خسارات هنگفتی به بار خواهد آمد. نمونهٔ بارزی که می‌توان ذکر کرد، انجام عملیات بانکی از طریق شبکه‌های اطلاع‌رسانی است که حریم خصوصی در آنها از جایگاه حساسی برخوردار است و اگر خدشه‌ای به این اصل مهم در فضای

۱۹۹۷ راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی در حوزهٔ ارتباطات مخابراتی و دستورالعمل 58/EC پارلمان شورای اروپا به تاریخ ۱۲ ژولای ۲۰۰۲ راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی در حوزهٔ ارتباطات الکترونیک اشاره کرد.

1. Self-regulating Measures.

۲. از آنجا که امروزه مباحث راجع به حریم خصوصی به یکی از مباحث مهم در حوزه حقوق بشر تبدیل شده است، بحث تقابل تدابیر پیشگیرانه و رعایت موازین مذکور اهمیت ویژه‌ای یافته است. جهت مطالعه این مباحث ر.ک: نجفی‌ابرندآبادی (علی‌حسین)، **پیشگیری عادلانه از جرم، علوم جنایی**، مجموعه مقالات در تجلیل استاد دکتر محمد آشوری، انتشارات سمت، ص ۵۵۹، ۱۳۸۳.

تبادل اطلاعات وارد شود، عرصهٔ تجارت الکترونیک که امروزه به شدت مورد توجه دولت‌ها قرار گرفته است، با شکست مواجه خواهد شد.

اما مشکل بزرگ حقوقی دیگری که پیشگیری وضعی با آن مواجه است، **اصل آزادی جریان اطلاعات**[۱] **و حق بهره‌برداری مشروع اشخاص از اطلاعات** است. همان طور که گفته شد، پیشگیری وضعی، خصوصاً در فضای تبادل اطلاعات یک پیشگیری فنی و غیرارادی محسوب می‌شود و چنانچه به خوبی طرح‌ریزی و اجرا نشود، ممکن است علاوه بر اطلاعات غیرقانونی، از دسترسی به اطلاعات قانونی و مشروع نیز جلوگیری کند و به این ترتیب، متصدیان اجرایی این نوع پیشگیری با تخلف زیر پا گذاشتن این اصل مواجه شوند. این مشکل از این جهت نیز خودنمایی می‌کند که شبکه‌های اطلاع‌رسانی رایانه‌ای بعضاً برای اینکه در معرض این گونه اتهامات قرار نگیرند، به طور کلی از انجام وظایف قانونی خود جهت اجرای اقدامات پیشگیرانه وضعی نیز سرباز می‌زنند و در اینجاست که لزوم وضع مقرراتی شفاف و راهگشا به خوبی احساس می‌شود.[۲]

البته باید خاطرنشان کرد که اخیراً این دو معضل بزرگ حقوقی در بحث خودتقنینی شبکه‌های اطلاع‌رسانی رایانه‌ای به طور خاص مورد توجه قرار گرفته است. چراکه به موجب اختیارات قانونی که به متصدیان شبکه‌ها اعطا شده است، آنها می‌توانند از لحاظ مدیریتی و فنی اقداماتی انجام دهند که خواسته یا ناخواسته به این دو موضوع مهم حقوقی لطمه وارد نشود. بنابراین، هدایت صحیح قانونی شبکه‌ها به وضع تدابیر مناسبی که این گونه چالش‌ها را برنینگیزند، از اهمیت خاصی برخوردار است.

---

۱. به لایحه «قانون آزادی اطلاعات» ر.ک: www.itna.ir.

2. Kosar, Carol and Lockhart, Ashe (Web Site Administrators), Internet Service Providers Liability, 1997.

۲-۲-۲. پیشگیری وضعی از جرائم رایانه‌ای در ایران

با توجه به توضیحاتی که داده شد، تا حدودی ماهیت پیشگیری از جرائم رایانه‌ای و مشکلات و محدودیت‌های ناشی از آن روشن شد. به نظر می‌رسد اجرای این نوع پیشگیری در کشور ما نیز با همان دو نوع محدودیتی که مورد بررسی قرار گرفت مواجه باشد، چرا که از یک طرف، کشور ما از لحاظ فناوری اطلاعات و ارتباطات نوین به سطحی نرسیده که رأساً اقدام به تولید ابزارهای پیشگیرانه نماید و از این لحاظ به خارج از کشور وابسته است و تا به حال نیز، متحمل هزینه‌های گزافی هم شده است. از طرف دیگر، به دلیل شفاف نبودن مقررات موجود، نحوهٔ به کارگیری این ابزارها نیز مشخص نمی‌باشد. به گونه‌ای که مشاهده می‌شود هر یک از ارائه‌دهندگان خدمات شبکه‌ای به نحو متفاوتی از آنها استفاده می‌کنند، در حالی که دسترسی به بعضی از سایت‌های غیرمجاز از طریق بعضی از ارائه‌دهندگان خدمات به سهولت امکان‌پذیر است، بعضی دیگر به نحوی حساسیت سیستم‌های خود را بالا برده‌اند که حتی سایت‌های علمی و پژوهشی معتبر یا سایت‌های نهادهای رسمی کشورمان را نیز پالایش می‌کنند.

البته باید خاطرنشان ساخت که هم اکنون در کشور ما حرکت رو به رشدی جهت سامان بخشیدن اقدامات پیشگیرانهٔ وضعی از جرائم رایانه‌ای در حال انجام است. به عنوان مثال، شورای عالی امنیت ملی به مدد متخصصان و کارشناسان ذی‌ربط، شورای عالی امنیت فضای تبادل اطلاعات کشور[1] را تشکیل داده است و به بررسی راهکارهای مقابلهٔ وضعی با این طیف از جرائم که در ابعاد خرد و کلان ارتکاب می‌یابند می‌پردازد. همچنین، از سوی شورای عالی انقلاب فرهنگی نیز دستورالعمل‌هایی برای نحوهٔ ارائهٔ خدمات

1. www.fata.ir.

به ارائه‌دهندگان خدمات شبکه‌ای ابلاغ شده است.[۱]

نتیجه‌گیری

مهم‌ترین چالشی که در وضع تدابیر پیشگیرانه کیفری وجود دارد، انتخاب نوع ضمانت اجراهای قهرآمیزی است که باید نسبت به نقض‌کنندگان هنجارهای حاکم بر فضای تبادل اطلاعات اتخاذ شود. ممکن است در نگاه اول این گونه به نظر رسد که می‌توان با شبیه‌انگاری این ناهنجاری‌ها با نظایر فیزیکی‌شان، به راحتی ضمانت اجراهای قهرآمیز این حوزه را نیز مقرر کرد. اما با اندکی دقت درمی‌یابیم که تجلی ناهنجاری‌ها در این فضا از خصوصیاتی برخوردار است که عدم التفات به آنها مقررات ناکارامدی را موجب می‌شود. به عنوان مثال، حوزهٔ تأثیرگذاری جرائم رایانه‌ای نسبت به نظایر سنتی آنها بسیار گسترده‌تر و بعضاً وخیم‌تر است و حتی اگر مبنای عمل ما تناسب جرم و مجازات هم باشد، به نظر می‌رسد این شبیه‌انگاری از وجههٔ حقوقی نیز برخوردار نمی‌باشد. همچنین، یکی از ویژگی‌های اصلی این جرائم، بین‌المللی بودن آنهاست و به نظر می‌رسد آن قدر که قانونگذاران داخلی مجبور هستند در حوزهٔ جرائم رایانه‌ای ملاحظات بین‌المللی را رعایت کنند، این الزام نسبت به جرائم فیزیکی که عمدتاً به مرزهای کشورها محدود هستند و تابع اصل سرزمینی می‌باشند وجود نخواهد داشت. از طرف دیگر، همان طور که اشاره شد، مجرمان رایانه‌ای از خصوصیاتی برخوردارند که هر نوع ضمانت اجرای قهرآمیزی نسبت به آنها نه تنها صحیح نیست که کارامد

۱. مصوب جلسات ۴۸۲، ۴۸۳، ۴۸۴، ۴۸۵، ۴۸۶، ۴۸۸ مورخ ۱۳۸۰/۹/۵، ۱۳۸۰/۵/۲۳، ۱۳۸۰/۶/۶، ۱۳۸۰/۷/۳، ۱۳۸۰/۷/۱۷ و ۱۳۸۰/۵/۱۵ شورای عالی انقلاب فرهنگی که پیرو تصویب و ابلاغ سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی مقام معظم رهبری (نامه‌های شمارهٔ ۱/۱۰۳۳ مورخ ۱۳۸۰/۳/۹ و ۱/۱۰۷۲ مورخ ۱۳۸۰/۳/۱۳) به تصویب رسیده است.

هم نمی‌باشد.

در مورد پیشگیری غیرکیفری از جرائم رایانه‌ای نیز در حد این مطلب توضیحات لازم داده شد و به نارسایی‌های آن اشاره شد. اما باید توجه داشت که علی‌رغم وجود تمامی این محدودیت‌ها، باز هم نمی‌توان نقش مهم پیشگیری غیرکیفری را انکار کرد. آنچه اهمیت دارد این است که با اتخاذ تدابیر مدبرانه و راهگشا، حتی‌المقدور موانع موجود را برطرف کنیم و بازدهی این اقدامات را به حداکثر برسانیم.

با توجه به توضیحاتی که آمد، مشخص می‌شود که جرائم رایانه‌ای در فضا و بستری ارتکاب می‌یابند که امکان شناسایی و مقابله با آنها بسیار دشوار است و از این لحاظ نسبت به نظایر فیزیکی‌شان، از رقم سیاه بالاتری برخوردارند و به همین دلیل از لحاظ تجزیه و تحلیل علمی و جرم‌شناختی این مشکل وجود دارد که نمی‌توان با استناد به آمار و ارقام به دست آمده تصمیمات دقیقی اتخاذ کرد. هرچند می‌توان با تکیه بر این نقطهٔ قوت که شبکه‌های اطلاع‌رسانی رایانه‌ای به عنوان پل ارتباطی میان مجرمان و فضای تبادل اطلاعات عمل می‌کنند، حداقل به یک سری آمار و ارقام دست یافت که البته نیاز به بهره‌گیری از یک سری ابزار و تجهیزات دارد که گفته شد با محدودیت‌های فنی و قانونی مواجه است.

نکتهٔ قابل توجه دیگر این است که بحث جرائم رایانه‌ای و تلاش در جهت پیشگیری از وقوع یا تکرار آنها و مقابله با مرتکبان و حمایت از بزهدیدگان، به یک حوزهٔ خاص منحصر نمی‌شود. کما اینکه به طور کلی این مبحث یک حوزهٔ میان‌رشته‌ای را تشکیل می‌دهد و از تعامل حقوق با فناوری به وجود آمده است. هرچند نباید دیگر حوزه‌ها نظیر علوم اجتماعی یا روان‌شناسی را نیز نادیده انگاشت. به هر حال، جریان بهره‌برداری از فضای تبادل اطلاعات خود به یک فرهنگ متمایز از فضای فیزیکی تبدیل شده است و مناسبات و ملاحظات خاص خود را دارد و به راحتی نمی‌توان با اتخاذ تدابیر یک سویه

یا دو سویه برای آن در ابعاد خرد و کلان تصمیم‌گیری کرد.

به نظر می‌رسد مهم‌ترین عامل عقب ماندن ما در وضع قوانین و تدابیر مناسب برای این حوزه، بیگانه بودن جامعهٔ حقوقی‌مان با مباحث نوین می‌باشد. بر هیچ کس پوشیده نیست که برای رسمیت یافتن یک هنجار در جامعه و قانونی شدن آن، راه صحیح این است که در ابتدا آن را در محافل علمی و حقوقی مانند دانشکده‌های حقوق و پژوهشکده‌های علمی مورد بررسی و تجزیه و تحلیل قرار دهند و هنگامی که نتایج مطلوبی به دست آمد، آن را به عنوان یک طرح یا لایحه مطرح کنند. حال اگر این حوزه‌ها با این مباحث نامأنوس باشند و درک صحیحی از آن نداشته باشند، مسلماً اقداماتی که انجام می‌شود از پختگی و جامعیت کامل برخوردار نخواهد بود و حتی ممکن است مشکلات بیشتری را هم موجب شود. بنابراین، توصیه می‌شود این حوزه‌های علمی به سمتی سوق داده شوند که مسائل مستحدثه و جدید برایشان قابل درک باشد و بتوانند از ابعاد مختلف آنها را مورد بررسی و تدقیق قرار دهند.

آخر سخن اینکه فضای تبادل اطلاعات چیزی نیست که بتوان در دنیای امروز از آن فاصله گرفت و عطایش را به لقایش بخشید. هر یک از ما هم از لحاظ فردی و هم در بعد زندگی اجتماعی خود ناگزیر از برقراری ارتباط با این فضا هستیم و همان طور که از مزایای شگفت‌انگیز آن بهره‌مند می‌شویم، با چالش‌های آن نیز مواجه هستیم. پس چه خوب است سیاستگذاران عرصه‌های خرد و کلان کشور، هم اکنون که تقریباً در ابتدای راه قرار داریم، با اتخاذ تدابیر مناسب، برای شهروندان خود از این فضا بستری بسازند که موجبات رشد و شکوفایی افراد جامعه را در تمامی ابعاد فراهم آورند.