مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات (سال دوم)
شماره۶/ زمستان ۱۳۹۵ / ص۴۹-۴۲

بررسی تفصیلی جرائم سایبری در ایران و ارائه راهکارهایی در مقابله با آن

فرهنگ افراسیابی [۱]، ایمان رهبر [۲]

[۱] عضو هیئت علمی دانشگاه پیام نور مرکز داراب

[۲] کارشناسی ارشد مکاترونیک(ارتباطات انسان، ماشین، کامپیوتر)

نام نویسنده مسئول:

ایمان رهبر

چکیده

امروزه بحث فناوری اطلاعات و ارتباطات نوین که تجلی روشن آن فضای تبادل اطلاعات (فضای سایبر[۱]) است، مسئله‌ی جدیدی را با عنوان پاسخگویی به سوءاستفاده‌هایی که از فضای تبادل اطلاعات به عمل می‌آید پیش روی دانشمندان علوم جنائی قرار داده است. تمایل روزافزون به استفاده از این فضای اینترنت شرایط و بستر مساعدی برای ظهور جرائم سایبری به وجود آورده است. در این مقاله به بررسی جرائم سایبری در ایران، برای تدوین قوانین مرتبط با آن‌ها، تشریح بیشتر مصادیق جرائم سایبری، باهدف شناخت دقیق‌تر برای مبارزه با آن‌ها، ارائه راهکارهای مفید در جهت پیشگیری یا حداقل کاهش آسیب‌های ناشی آن پرداخته‌شده است. مهم‌ترین راهکارهای ارائه‌شده عبارت‌اند از: برنامه ریزی گسترده صدا و سیما برای آگاه سازی مردم از طریق ساخت برنامه های مربوطه ، در اولویت قرارگرفتن این معضل اجتماعی و آگاه سازی مسئولین از اهمیت بسیار زیاد این موضوع در جامعه و لطمات جبران ناپذیر آن در صورت عدم اقدام به موقع ، فرهنگ سازی عهده دار شدن بخشی از مسئولیت آگاه سازی توسط مردم ، استفاده از مراکز عمومی نظیر دانشگاهها ، مدارس ،مساجد و حوزه ها بعنوان مراکز تاثیرگذار ، استفاده ازکشورهای موفق در این زمینه .

واژگان کلیدی: جرائم سایبری- طبقه‌بندی جرائم- راهکارهای مقابله با آن

[۱] سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است.

مقدمه

اواخر قرن بیستم و در عصر فرا صنعتی، جهان شاهد ظهور پدیده‌های شگرف در اثر پیشرفت‌های علمی و فناوری‌های نوین بود. پدیده‌هایی که در حقیقت به معنای تولد جهانی دیگر با شرایط و ویژگی‌هایی متفاوت با جهان کنونی بود. ابداعی که دنیای اقتصاد، سیاست و فرهنگ را مجذوب خود ساخت. این دنیای جدید فضای مجازی یا فضای سایبر نام گرفت. [1] دسترسی میلیون‌ها نفر به اینترنت در سرتاسر جهان موجب ارتباط و تعامل بیشتر انسان‌ها شده و دهکده جهانی را میسر کرده است. فرصت‌های بسیاری برای ایجاد ارتباط با افراد جدید امکان‌پذیر شده،و موجب توسعه شبکه‌های حرفه‌ای شخصی شده است و برخورد با موقعیت‌های جدید را برای افرادی که به‌گونه‌ای انحراف را پیش‌گرفته‌اند، به‌صورت شبانه‌روزی ایجاد نموده است. [2]. فضای مجازی را می‌توان فضایی که در آن فعالیت‌های گوناگون در ابعاد داده‌کاوی و اطلاع‌رسانی، ارتباطات و ارائه خدمات، مدیریت از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد، تعریف کرد. [3] که منشأ تحولات گوناگونی در زندگی بشر بوده، البته به همان اندازه که شرایط زندگی را بهبود بخشیده است، زمینه ارتکاب جرم را نیز مساعد کرده است.سرعت ارتباطات به بزهکاران اجازه داد که آسان‌تر دست به ارتکاب جرم بزنند. و پیامد فنون و شیوه‌های جدید زندگی دامن زدن به اشکال نوین بزهکاری ازجمله جرائم فضای مجازی بود. [4]. جرائم سایبری نشانگر فعالیت‌های غیرقانونی و خلافکارانه مبتنی بر رایانه‌ای است که از طریق کاربرد شبکه جهانی آزاد و فنّاوری اطلاعات و ارتباطات ناشی می‌شود. این جرائم فقط رایانه را شامل نمی‌شود بلکه با افزایش امکانات اینترنت، جرائم مربوط به آن نیز رو به فزونی می‌باشد[5] . تحقیقات موجود، نشان‌دهنده افزایش شکل‌های متنوعی از جرائم سایبری شامل هک کردن، حدس زدن کلمه رمز دیگران، توزیع ویروس، پورنو گرافی و کلاه‌برداری در کشورهای مختلف است که پیامدهای مالی، روانی و احساسی مخربی به همراه داشته است [6].ویژگی‌های منحصربه‌فرد اینترنت ازجمله محتوای تحریک‌آمیز، سهولت دسترسی، آسودگی کار با رایانه، هزینه پایین، همگی موجب استقبال فرد به استفاده از اینترنت شده است.امکانات وسیع این دنیای مجازی به حدی است که تمامی افراد به‌خصوص جوانان و دانشجویان که بیشترین کاربران اینترنت در ایران به شمار می‌روند، را به خود جذب کند [7]. و به طور کلی همه این عوامل باعث شده که فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نماند . [8]. با توجه به مطالب فوق اهمیت مسئله‌ی جرائم سایبری و مبارزه با آن‌ها روشن است .و به همین دلیل در این مقاله به بررسی جرائم سایبری، طبقه‌بندی، مصادیق جرائم سایبری و درنهایت ارائه راهکارهای مقابله با جرائم سایبری پرداخته‌شده است.

۱-جرائم سایبری

جرائم سایبری به جرائمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی واقع می شود. [9]. و فعالیت‌هایی هستند که در ان ها رایانه‌ها، تلفن‌ها و تجهیزات خانگی و سایر امکانات فنّاورانه برای اهداف نامشروعی چون کلاه‌برداری، سرقت، خرابکاری الکترونیکی، تجاوز به حقوق مالکیت افراد، سوءاستفاده جنسی از زنان و کودکان و شکستن و وارد شدن به سیستم‌های کامپیوتری و شبکه‌ها مورداستفاده قرار می‌گیرد[10]

این جرائم به فرد اجازه می‌دهد که ارتباط گمنامی برقرار کند، ازاین‌رو ویژگی مهم فضای سایبر ازجمله عدم تماس چهره به چهره و عدم وجود پلیس و نهادهای نظارتی، باقی نماندن آثاری از رد پای مجرمین و آزادی بی‌حدوحصر در اینترنت شرایط مناسبی را برای مجرمان فراهم می‌سازد تا مرتکب جرم شوند [11] سرعت وقوع جرم، تعداد زیاد بزه دیده در فضای سایبر از دیگر ویژگی‌های جرائم سایبری است. [8]به همین دلیل جرائم سایبری امروز گسترش بسیار زیادی یافته است . جرائمی نظیر سرقت هویت افراد، جنایات جنسی مثل پورنو گرافی کودکان، قاچاق جنسی کودکان و حتی فحشا، کشف رمز عبور خصوصی و آزار و اذیت‌های اینترنتی ازجمله جرائم در فضای مجازی می‌باشند و انسان‌ها از آن در امان نیستند.[12]

۲-طبقه‌بندی جرائم سایبری در ایران

۱- جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی شامل (دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای).
۲- جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، شامل (جعل رایانه‌ای، تخریب و اخلال درداده‌ها یا سامانه‌های کامپیوتری و مخابراتی)
۳- سرقت و کلاه‌برداری رایانه‌ای.
۴- جرائم علیه عفت و اخلاق عمومی.
۵- هتک حیثیت و نشر اکاذیب [13]

۳-توصیف مصادیق جرائم سایبری در ایران

الف - هرزه‌نگاری سایبری:

ساخت و ایجاد سایت‌هایی با محتویات مستهجن نظیر عمل آمیزش جنسی، از طریق سیستم رایانه به‌صورت واقعی و یا به‌صورت مونتاژ شده همچنین انتشار عکس‌ها و فیلم‌های مستهجن جهت تحریک و منافی عفت در اینترنت و تولید سی‌دی‌های با محتویات هرزه‌نگاری بزرگ‌سالان و کودکان در فضای مجازی و فروش آن‌ها از طریق اینترنت و لینک آدرسشان در سایت‌های دیگر و ایجاد سایت‌هایی جهت ثبت‌نام از افراد در توریست‌های جنسی، همگی عنصر مادی جرائم محتوا می‌باشند که از طریق سایت‌ها، پست الکترونیکی توسط رایانه و اینترنت قابل تحقق است. علاوه بر وب‌سایت‌ها، موضوعات مستهجن می‌توانند از راه‌های: مبادله با استفاده از سامانه‌های اشتراک‌گذاری فایل، مبادله در اتاق‌های گپ‌زنی نیز منتشر شوند [14].

ب- فروش محصولات غیرقانونی[1] و آموزش تولید آن‌ها

فروش مواد مخدر، مشروبات الکلی، داروهای روان‌گردان و غیرمجاز و ....، تبلیغ و ترویج مصرف مواد مخدر و مواد روان‌گردان. امروز دیگر ما با باندهای فیزیکی و مافیایی مواد مخدر در جامعه مواجه نیستیم، امروز شاهد فعالیت بیش از ۱۶هزار وب‌سایت در فضای مجازی هستیم که نحوه تولید شیشه را در کشور آموزش می‌دهند [15]. فروش اینترنتی انواع مواد اعتیادآور ایرادش این است که فروشنده مواد و قاچاقچیان را تا خانه‌های مردم می‌آورد. هر جا که رایانه باشد و کاربری که بتواند وارد سایت شود، قاچاقیان هم همان‌جا هستند و بدون جلب‌توجه، جنس خود را می‌فروشند. پس با این شیوه هیچ جا امن نیست، حتی اتاق یک نوجوان و دفتر کار یک جوان که می‌تواند محفلی برای ردوبدل جنس باشد. [16]

ج - قماربازی آنلاین[2]

در این نوع سایت‌ها و بازی‌ها در ابتدا و مراحل ابتدایی اتفاق خاصی نمی‌افتد اما بعد از پشت سر گذاشتن مراحل اولیه و زمانی که کاربر جذب این بازی‌ها شد بحث اصلی یعنی پیشنهادهای مالی و جابه‌جایی آن بین کاربران آغاز می‌شود و بازیکنان برای ادامه مراحل مجبور به پرداخت هزینه‌هایی خواهند شد و ازاینجا به بعد بحث کلاه‌برداری‌ها و ضررهای مالی پیش می‌آید. [17]

د - جرائم مربوط به مالکیت معنوی[3]

حقـــوق مـــالکیت فـکـــــری که بیشتر در ایران با عنوان مالکیت معنوی از آن یاد می‌شود عمدتاً موضوعاتی را که زاده فکر و اندیشه بشر است شامل می‌شود که بر اساس آن حقوقی برای پدیدآورنده اثر شناخته می‌شود که همواره افراد جامعه مکلف به رعایت آن هستند. کشورها برای رعایت این حق از سوی افراد جامعه به وضع قوانینی پرداخته‌اند که تا قبل از ظهور اینترنت و شبکه‌های رایانه‌ای تا حدودی قابل‌اعمال بود؛ ولی امروز حقوق مالکیت فکری یکی از حوزه‌های اصلی اختلافات قانونی در شبکه‌های رایانه‌ای و اینترنت است. به دلیل اینکه مالکیت فکری در ایران آن‌چنان‌که باید رعایت نمی‌شود، بنابراین یکی از زیرمجموعه‌های اصلی آن‌که همان قانون کپی‌رایت است چندان جدی گرفته نمی‌شود. مالکیت فکری در این فضا به دودسته تقسیم‌بندی می‌شود یک دسته شامل همان آثار فیزیکی هستند که در محیط بیرونی وجود دارند مانند کتاب، نقاشی، عکس، مقاله و ... که به‌صورت دیجیتالی درآمده و در فضای سایبر به نمایش گذاشته می‌شوند. دسته دیگر هم مربوط به خود فضای مجازی است که شامل اطلاعات، طراحی وب‌سایت و ... می‌شود. گفته می‌شود مالکیت فکری در ایران به دو بخش ادبی (کتاب، نرم‌افزار، عکس ...) و صنعتی (علامت تجاری، اختراع و...) تقسیم می‌شود و این در حالی است که در کشورهای دیگر مالکیت فکری چندین بخش مجزای دیگر را نیز شامل می‌شود.

ه - افترا و نشر اکاذیب[4]

مجرم می‌تواند در فضای سایبر به انتشار اکاذیب علیه افراد، سازمان‌ها، دولت و ...بپردازد. ابزارهای وب، پست الکترونیک، شبکه‌های اجتماعی مجازی جزء ابزارهای او محسوب می‌شود [18]. این ابزارهای می‌توانند اطلاعات غلط و افتراآمیز به‌خصوص در شبکه‌های اجتماعی مجازی و اتاق‌های گپ‌زنی، بدون تأیید توسط ناظران و مدیران گروه‌ها در معرض نمایش قرار دهند.

---

[1] Selling illegal products
[2] Online Gambling
[3] Intellectual Property Crimes
[4] Cyber Defamation

و - جرائم علیه مذهب[1]

بیانات نوشتاری ضد مذهبی، تهمت به مذهب، یا انتشار کاریکاتور می‌باشد [14]. نشر محتوای الحادی و مخالف موازین اسلام. اهانت به دین مبین اسلام و مقدسات آن، تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام، همچنین نقل مطالب از نشریات و رسانه‌ها احزاب گروه‌های داخلی خارجی منحرف و مخالف اسلام و تبلیغ از آن‌ها.

ز- سرقت اطلاعات به‌صورت الکترونیکی[2]

سرقت اطلاعات ذخیره‌شده در دیسک‌ها و حافظه‌های ذخیره کننده داده. سرقت اطلاعات محرمانه و موجود در شبکه‌های مجازی. با ورود اپلیکیشن ها به فضای گوشی موبایل، دیگر گوشی یک ابزار شخصی نیست و آنچه درگوشی موجود است، مثل همه اطلاعات شخصی و هویتی و نیز فایل‌ها و عکس‌ها و پیام‌ها قابل‌دسترسی برای دیگران می‌باشند و دیگران به‌راحتی می‌توانند با استفاده از اطلاعات هویتی شخص، خود را بجای شخص موردنظر معرفی کنند. از طرف دیگر برخی از اپلیکشن های رایگان ممکن است قلابی باشند و تنها برای دسترسی به اطلاعات موجود درگوشی کاربر، طراحی‌شده باشد. [19]

ح - سابوتاژ (خرابکاری) و اخاذی رایانه‌ای

سابوتاژ کامپیوتری یعنی اصلاح و موقوف سازی و یا پاک کردن غیرمجاز داده‌ها و یا عملیات کامپیوتری به‌منظور مختل ساختن عملکرد عادی سیستم. سابوتاژ ممکن است وسیله‌ای برای تحصیل مزایای اقتصادی بیشتر نسبت به رقیبان یا پیشبرد فعالیت‌های غیرقانونی برای سرقت داده‌ها و برنامه‌ها به‌منظور اخاذی باشد. [20].

ط - پول‌شویی کامپیوتری

پول‌شویی و غارت یکی از جرائم کلاسیک بوده که دارای سابقه طولانی است. با پیشرفت فنّاوری این جرم از طریق کامپیوتر و اینترنت صورت می‌پذیرد. نحوه ارتکاب بدین‌صورت است که باندهای بزرگ نامشروع با ارسال ایمیل، پیشنهاد انجام یک کار تجاری را به شخصی می‌نمایند و بدون اینکه اثر و نشانی از خود بجای بگذارند پیشنهاد ارسال مبالغی پول به‌حساب شخصی را که برای او ایمیل فرستاده‌اند می‌نمایند و در تقاضای خود نحوه ارسال و سهم هر یک از طرفین را بیان نموده و در صورت توافق طرف مقابل (گیرنده ایمیل) نوع و نحوه تضمینات لازم را اعلام می‌کنند واصولا در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب و باهدف خود هماهنگ می‌نمایند. [21].

ی - هک کردن[3]

هک دسترسی‌پذیری بدون اجازه به سیستم‌های کامپیوتری، برنامه‌ها و اطلاعات و باز کردن فایل‌ها برای صدمه واردکردن است. [22].در طول چند سال گذشته، مجرمان به‌طور چشمگیری حملاتشان را روی رایانه‌های شخصی متمرکز کرده‌اند، به دلیل اینکه خیلی از رایانه‌های شخصی به‌خوبی محافظت نشده‌اند. علاوه بر این رایانه‌های شخصی ، اغلب حاوی اطلاعات خاصی هستند. برای مثال جزئیات کارت اعتباری و حساب بانکی و گذرواژه و اطلاعات حساس اغلب در سیستمهای رایانه‌ای ذخیره می‌شوند. با توجه به اتصال رایانه به اینترنت، مجرمان در هر نقطه از دنیا می‌توانند برای دسترسی به این اطلاعات از طریق اینترنت تلاش کنند. [14].

ک - ویروس-کرم[4]

ویروس رایانه‌ای یک برنامه است که بر روی برنامه‌های حقیقی سوار می‌شود. برای نمونه یک ویروس می‌تواند خود را به برنامه‌ای مثل یک برنامه «صفحه گسترده» متصل کند. هر بار که "صفحه گسترده" اجرا می‌شود، ویروس هم اجرا می‌شود و این شانس را دارد که دوباره تولید شود. یک کرم رایانه‌ای برنامه‌ای است که از شبکه‌های کامپیوتری و حفره‌های امنیتی برای تکثیر خود استفاده می‌کند. و یک کپی از کرم شبکه را برای ماشین دیگری که حفره امنیتی مشخصی دارد جست‌وجو می‌کند و با یافتن حفره امنیتی در ماشین جدید؛ خود را در آنجا هم کپی می‌کند. با راه یافتن کرم به ماشین جدید چرخه دوباره تکرار می‌شود و کرم دوباره ازاینجا در ماشین‌های جدید کپی می‌شود.[23]

---

[1] Crimes Against Religion
[2]Theft of information contained in electronic from
[3] Hacking
[4] Virus-worm

ل - اسب ها یا ویروس‌های تروجان[1]

لغت تروجان برگرفته از افسانهٔ یونانی جنگ تروا است. در این داستان یونانی‌ها از طریق هدیه دادن اسب چوبی بزرگی به دشمنانشان، تعدادی سرباز به قلعهٔ آن‌ها فرستادند؛ سپس این سربازها از داخل اسب بیرون آمده و درب قلعه را باز کردند تا دیگر افراد به داخل قلعه بیایند و قلعه را فتح کنند. این مثال دقیقاً عملی است که تروجان با کامپیوتر شما انجام می‌دهد. تروجان ابتدا به قسمت های مختلف نفوذ می‌کند؛ سپس، راهی برای آسیب به آن‌ها پیدا خواهد کرد. و یک برنامه غیرمجاز است که به نظر سیستم مجاز می‌رسد و به‌صورت مخفیانه درون سیستم به انجام فعالیت‌های غیرقانونی می‌پردازد. تروجان، برنامه مخربی است که به‌صورت یک نرم‌افزار جالب به نظر می‌رسد. برعکس ویروس‌ها، تروجان‌ها تکثیر نمی‌شوند؛ ولی به‌اندازهٔ ویروس‌ها مخرب هستند. یکی از انواع تروجان‌ها، برنامه‌ای است که ادعا می‌کند، کامپیوتر شمارا از آسیب ویروس‌ها نجات می‌دهد؛ اما در حقیقت ویروس‌ها را با سیستم شما آشنا و به آن‌ها معرفی می‌کنند.

م - پست الکترونیک جعلی[2]

بسیاری از پیام‌های الکترونیکی که روزانه در دنیای اینترنت مبادله می‌شوند را هرزنامه‌ها[3]تشکیل می‌دهند که از طریق ایمیل های جعلی منتشر می شوند. این ایمیل‌های جعلی چندی است در ایران نیز با افزایش چشمگیری روبرو بوده و در بسیاری مواقع باعث فریب کاربران به دلیل ناآگاهی آن‌ها می‌شود. امروزه هرزنامه (اسپم) به پدیده‌ای بحرانی در دنیای اینترنت و کاربران شبکه تبدیل‌شده به‌نحوی‌که این پیام‌های ناخواسته روزانه آدرس‌های پست الکترونیک کاربران را هدف حمله خود قرار می‌دهند و در بسیاری از مواقع نیز موفق به فریب کاربران می‌شوند. ای میل ناخواسته تنها یک اختلال شبکه و یا مزاحمت اینترنتی نیست بلکه این پدیده باهدف فریب کسانی که در اینترنت جستجو می‌کنند روش‌های مختلف را برای دسترسی به اطلاعات شخصی، اطلاعات مربوط به هویت و حتی حساب مالی کاربران امتحان می‌کند به‌خصوص که اغلب این پیام‌ها با خطر بالای ویروس‌ها نیز همراه هستند. [24]

ن - فیشینگ[4]

واژه فیشینگ در زبان انگلیسی نیز یک واژه جدید است که برخی آن را مخفف عبارت: شکار کردن رمز عبور کاربر از طریق یک طعمه[5] و برخی دیگر آن را استعاره ای از کلمه ماهیگیری[6]تعبیر کرده‌اند. سازندگان این واژه کوشیده‌اند با جایگزین کردن Ph به‌جای F مفهوم فریفتن را به مخاطب القا کنند. فیشینگ در اصطلاح کامپیوتری به معنای شبیه‌سازی قسمت‌هایی از یک سایت اینترنتی (مثلاً یک صفحه از سایت) آشنا و یا معروف است که به‌وسیله آن بتوان کاربر را گمراه کرده و اطلاعات شخصی وی را به دست آورد. این اطلاعات می‌تواند شامل نام کاربری و کلمه‌ی عبور فرد در آن سایت یا اطلاعاتی مربوط به شماره‌حساب بانکی فرد و خیلی موارد دیگر باشد.

فیشینگ یک نمونه از فن مهندسی اجتماعی به‌منظور گمراه کردن کاربران اینترنتی برای به دست آوردن اطلاعت محرمانه آنان است. در این فن فیشرها[7]با طراحی یک سایت که شبیه به سایت موردنظر می‌باشد، کار خود را آغاز می‌کنند. پس از انجام این مرحله آن‌ها باید روشی را پیدا کنند که قربانیان خود را مجبور کنند تا در سایت آن‌ها واردشده و اطلاعات محرمانه خود را وارد کنند که بهروش‌های مختلفی این کار عملی می‌شود. مثلاً با ساخت یک خبر دروغین، قربانیان را به سایت خود کشانده و... بقیه مراحل انجام می‌شود. [25]

۴- راهکارها

الف- وقوف مسئولین به اهمیت موضوع : شاید مهم‌ترین بخش پیشگیری از این جرائم این باشد که مسئولین امر، به اهمیت بسیار زیاد فضای سایبر واقف باشند و به‌جای آنکه صورت‌مسئله را به‌صورت فیلتر کردن شبکه‌های مجازی پاک کنند؛ دنبال راه‌حلی برای حل مسئله باشند و این امر تا زمانی که انسان به اهمیت یک موضوع پی نبرد امکان‌پذیر نخواهد بود. چراکه فضای سایبر و شبکه‌های اجتماعی نه سیاه سیاه است و نه سفید سفید. بلکه هم جنبه مثبت دارد و هم جنبه منفی و همچنان که سوءاستفاده از آن ممکن است، درعین‌حال برای انجام کارهای آموزشی یا پیام‌رسانی و یا هر امر دیگر که نیاز به برقراری ارتباط سریع با مخاطبین است هیچ‌چیز نمی‌تواند جایگزین این

---

[1] Trojan Horse
[2] Fake email
[3] Spams
[4] Phishing
[5] Password Harvesting Fishing
[6] Fishing

[۷] کسانی که عمل فیشینگ را انجام می دهند

شبکه‌ها شود؛ بنابراین باید مسئولین اقدامشان را معطوف به این امر کنند و درواقع با آموزش، ایجاد فضاهای مفرح و شاد سالم در فضای مجازی و... پادزهری در برابر زهر سوءاستفاده کنندگان تزریق کنند.

ب- نقش صداوسیما: یکی از مواردی که برای انسان این شائبه ایجاد می‌شود که هنوز مسئولین، فضای مجازی را آن‌چنان جدی نگرفته‌اند و در پی کاهش آسیب‌ها و آشنا کردن مردم با جرائم سایبری اقدامی شایسته و بایسته انجام نمی‌دهند رویکرد صداوسیما به این موضوع هست. چراکه متأسفانه با نگاهی هرچند سطحی و گذرا به برنامه‌های صداوسیما هر بیننده‌ای به عدم توجه این نهاد مهم و تأثیرگذار در عرصه اجتماعی، به این موضوع پی می‌برد درحالی‌که معضلات و آسیب‌های ناشی از این فضای جدید برای مردم، رفته‌رفته بیشتر می‌شود و برای آن اگر اقدامی عاجل و عقلانی صورت نگیرد شاید در سال‌های آتی تبدیل به بزرگ‌ترین معضل اجتماعی کشور شود تا جایی که مثلاً تعداد افرادی که اعتیاد بسیار شدید به این شبکه‌های اجتماعی پیداکرده‌اند که بر روی زندگی عادی آن‌ها تأثیرات بسیار مخربی گذاشته باشد از معتادین به مواد مخدر بیشتر باشد؛ و یا تعداد افرادی که در اثر آثار سوء این شبکه‌ها کانون گرم خانواده‌شان رو به سردی می‌گراید و یا به طلاق منجر می‌شود از سایر آسیب‌های ناشی از فضای واقعی بیشتر باشد؛ بنابراین لازم است که صداوسیما به این مسئله توجه بسیار زیادی داشته باشد و با تولید برنامه‌های آموزشی و نمایشی و روشنگرانه، مردم را با آسیب‌های این شبکه‌ها ، و آنچه تحت عنوان جرائم سایبری تعریف می‌شود آشنا کند و حتی برای پیشگیری از آسیب‌ها، باید با توجه به نو بودن این فضا برای عامه مردم، روش صحیح استفاده از آن را آموزش داد و اینکه چگونه می‌توانیم از این فضا برای بهبود زندگی خود استفاده کنیم، چراکه امکانات این فضا برای استفاده بهینه و صحیح در زندگی آن‌قدر زیاد می‌باشد که هیچ‌چیزی واقعاً چنین ابزاری ندارد.

ج- سرمایه‌گذاری روی مراکز عمومی: یکی از راه‌های بسیار تأثیرگذار برای آموزش مردم استفاده از مراکزی نظیر دانشگاه‌ها، حوزه‌ها، مدارس، مساجد و ... است که ضمن انجام آموزش‌ها و اقدامات فیزیکی، می‌توان با ایجاد گروه‌ها و کانال‌ها در شبکه‌های مجازی، تأثیر بسیار زیادی بر مخاطبین گذاشت و مردم را در برابر خطرات و آسیب‌های آن واکسینه کرد.

د-پلیس سایبر: معمولاً مبارزه با جرائم نیاز به امکانات و صرف هزینه‌های هنگفتی دارد بنابراین پلیس نیز می‌تواند بخشی از بودجه خود را صرف پیشگیری و آموزش مردم قرار دهد؛ و مطمئناً این امر می‌تواند روزبه‌روز در کاهش جرائم سایبری موفق‌تر باشد.

ه- نقش مردم: قطعاً خود مخاطبین و کسانی که جو فضای مجازی را تجربه کرده‌اند و احیاناً از آن آسیب‌دیده‌اند و یا با عینک خوش‌بینانه، این فضا در بهبود زندگی آن‌ها نقش مثبت ایفا کرده است می‌توانند از هر نهادی یا وسیله‌ای در آگاهی بخشی و آموزش مردم مؤثرتر واقع شوند. به‌عنوان‌مثال زمانی که خود مردم به‌صورت خودجوش به اهمیت احترام به حریم خصوصی یکدیگر چه در فضای سایبر و چه در دنیای فیزیکی و واقعی پی ببرند و عزم خود را جزم کنند که در گفتگوهای خود و در گروه‌های مجازی خود این موضوع را به بحث و تبادل‌نظر بگذارند، یقیناً هیچ‌چیزی نمی‌تواند به‌اندازه آن، مردم را ترغیب و تشویق کند که به حریم خصوصی یکدیگر نزدیک نشوند و حتی در مواردی اگر سهواً کسی از زندگی خصوصی کسی آگاهی پیدا کرد، آن را منتشر نکند و نه آبروی یک انسان را خدشه‌دار کند و نه خود به‌عنوان یک مجرم سایبری معرفی کند و خود را در دردسر حتی بعضاً ناخواسته قرار دهد.

نتیجه‌گیری

الف . در عصر نوین اطلاعات، نیاز جوامع به رایانه و اینترنت بسیار افزایش‌یافته است. هر جه بیشتر فنّاوری کامپیوتری توسعه یابد جرائم سایبری نیز توسعه پیدا خواهد نمود. کشور ما ایران نیز از این قاعده مستثنی نیست و جرائم سایبری در آن در حال افزایش است. این جرائم به دلیل تأثیرات ناگواری که بر جامعه اطلاعاتی و کاربران دارد، برخورد جدی‌تری را از سوی دولتمردان سیاسی و قضایی می‌طلبد. حقوق ایران در این زمینه گرچه تلاش‌های مفیدی داشته، ولی همچنان نیاز به کار و پژوهش در ابعاد مختلف آن دارد.چراکه لازمه ایجاد امنیت و توسعه هر حوزه فناورانه، تصویب قوانین و مقررات قاعده‌مند و کارآمد است و فضای سایبری نیز از این قاعده مستثنا نیست.

ب . در جامعه‌ای که اطلاعات در آن، جزء باارزش‌ترین دارایی‌های کسب‌وکار و دولت است، لذا به‌منظور جلوگیری از سوءاستفاده از آن، داشتن یک رویکرد کلی‌نگر به مدیریت امنیت سیستم‌های اطلاعاتی الزامی است. باوجود روش‌ها و فن‌های متعدد برای جلوگیری، شناسایی و بررسی جنایات سایبری، بهترین شیوه در جهت مقابله با این جرائم تکیه بر تجربه متخصصان و متصدیان فناوری اطلاعات و حمایت‌های دانشگاهیان است.

ج . از آنجا که تغییرات در حوزه فناوری اطلاعات بسیار پرشتاب است، نباید انتظار داشته باشیم که قوانین جرائم سایبری برای مدت طولانی جوابگوی نیازهای فناوری اطلاعات جامعه باشند. از سوی دیگر نباید تصویب و اجرای قوانین جرائم سایبری را تنها راهکار مقابله بدانیم. اساسی‌ترین گام برای اجرایی کردن این قوانین آموزش و فرهنگ‌سازی عمومی در میان مردم است. که دولت و مردم و نهادهای عمومی و تاثیرگذار، در این امر خطیر باید کمک کنند . چراکه اجرای طرح‌های امنیت سایبری تنها مربوط به دولت نیست اجرای آن با همکاری همه بخش‌های خصوصی و شرکت‌های تجاری ممکن است سازمان‌ها می‌بایست اهمیت کافی به مسئله فناوری اطلاعات بدهند و مدیران آن را یک اولویت کاری بدانند و در جهت مقابله با این جرائم برنامه و هدف داشته باشند.

د. آسیب‌پذیری درزمینه تأمین امنیت سایبری، امنیت ملی کشورمان را هدف قرار می‌دهد و این مسئله تهدیدی نگران‌کننده برای عموم هم‌وطنان و نهادها است. شرایط خاص کشورمان سبب شده تجربه مقابله با بسیاری از جرائم سایبری مدرن را نداشته باشیم و این موضوع می‌طلبد که از تجارب ارزشمند کشورهای توسعه بافته استفاده نماییم و دانشگاهیان نیز با طرح همایش‌ها و پایان‌نامه‌های مرتبط در این وادی گامی مثبت بردارند.

منابع و مراجع

[۱] زیبر، ا. جرایم رایانه ای ترجمه محمد علی نوری و رضا نخجوانی و مصطفی بختیاروند و احمد مقدم, تهران: گنج دانش, ۱۳۸۳.

[2] Reyns, B. W. and Henson, B."BEING PURSUED ONLINE (Applying Cyberlifestyle–Routine Activities)," Criminal Justice and Behavior, vol. 38, no. 11, 2011.

[۳] صدری، م. ر. و کروبی، م. ت., ابعاد حقوقی محیط سایبر در پرتو توسعه ملی، مجموعه سخنرانی ها و مقالات اولین همایش حقوق فناوری اطلاعات و ارتباطات کشور, تهران: بقعه, ۱۳۸۴.

[۴] باستانی، ب.، جرایم کامپیوتری و اینترنتی جلوه ای از بزهکاری،مجله تحقیقات حقوقی، ۱۳۸۲.

[5] Parker, D. B, Crime by Computer, New York, 1976.

[۶] علیوردی، نیا ا.، و ملک دار، ا.، نوع شناسی و تبیین نظری از دیدگاه جرم شناسی، گزیده مقالات همایش پیشگیری از آسیب های اجتماعی: آسیب های اجتماعی نو پدید، نظریات و راهکارها, تهران: انتشارات فرهامه, ۱۳۹۳.

[۷] پاشایی، ف.، نیک بخت نصرآبادی، ع. ر. و توکل، خ.، "تجربه جوانان از زندگی با اینترنت :مطالعه کیفی،مجله علوم رفتاری،" جلد ۴، ۱۳۷۸.

[۸] جلالی فراهانی، ا. ح.، پیشگیری وضعی از جرایم سایبردر پرتو موازین حقوق بشر،فقه و حقوق، ۱۳۸۴.

[۹] بیابانی، غ. ح. و هادیانفر، س. ک.، فرهنگ توصیفی علوم جنایی،چاپ اول, تهران: انتشارات مرکز تحقیقات کاربردی کشف جرایم و امنیت معاونت آگاهی ناجا، ۱۳۸۴.

[10] Speer, D. L., "The challenges of cyber crime.," Political science department. Crime Law & Social change, pp. 24-34, 2000.

[11] Higgins, G. E., S. E. Wolfe and M. L. Ricketts, "Digital Piracy A Latent Class Analysis," vol. 27, no. 1, pp. 24-40, 2009.

[12] Donner, C. M., Marcum, b., Catherine, d., Catherine, D., Jennings, C., Wesley, G., Higgins, d., George, E., Banfield and Jerry, "Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital," Computers in Human Behavior, vol. 34, p. 165–172, 2014**.**

[۱۳]امامی،ح.، "بررسی ابعاد جرایم اینترنتی،" مطالعات بین المللی پلیس،جلد ۵۳، ۱۳۸۹.

[۱۴]گرکی، م.، "جرایم سایبری: راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، نیروی انتظامی جمهوری اسلامی ایران، پلیس امنیت فضای تولید و تبادل اطلاعات،" ۱۳۸۹.

[15] "http://www.mehrnews.com/news/2301273," [Online].

[16] "http://press.jamejamonline.ir/Newspreview/1801103014633361956," [Online].

[17] "http://www.isna.ir/news/95093018678," 30 9 1395. [Online].

[۱۸]لک، ب.، "بررسی ابعاد جرایم اینترنتی"، مطالعات بین المللی پلیس,، جلد ۵۳، ۱۳۸۹.

[19] "http://news.ern-co.com/," 10 10 1395. [Online].

[۲۰]شفیعی، م. س. و شفیعی، ش.، "بررسی شیوه های ارتکاب جرم جرایم سایبری-شناسایی خلاءهای قانونی و اجرایی و راهکارهای پیشگیری،" ۱۳۹۴.

[۲۱]بشیری، ع.، "بررسی حقوقی جرایم رایانه ای در حقوق جزای عمومی"، ۱۳۹۲.

[22] Goodman, M. D. and Brenner, S. W., "The Emerging Consensus on Criminal Conduct in Cyberspace," international journal of law and information technology, vol. 10, no. 2, 2002.

[23] "http://www.hamshahrionline.ir/details/11924،"[Online]

[24] "http://www.cyberpolice.ir/information/10981," [Online].

[25] "http://www.antiphishing.org/consumer_recs.html," [Online].