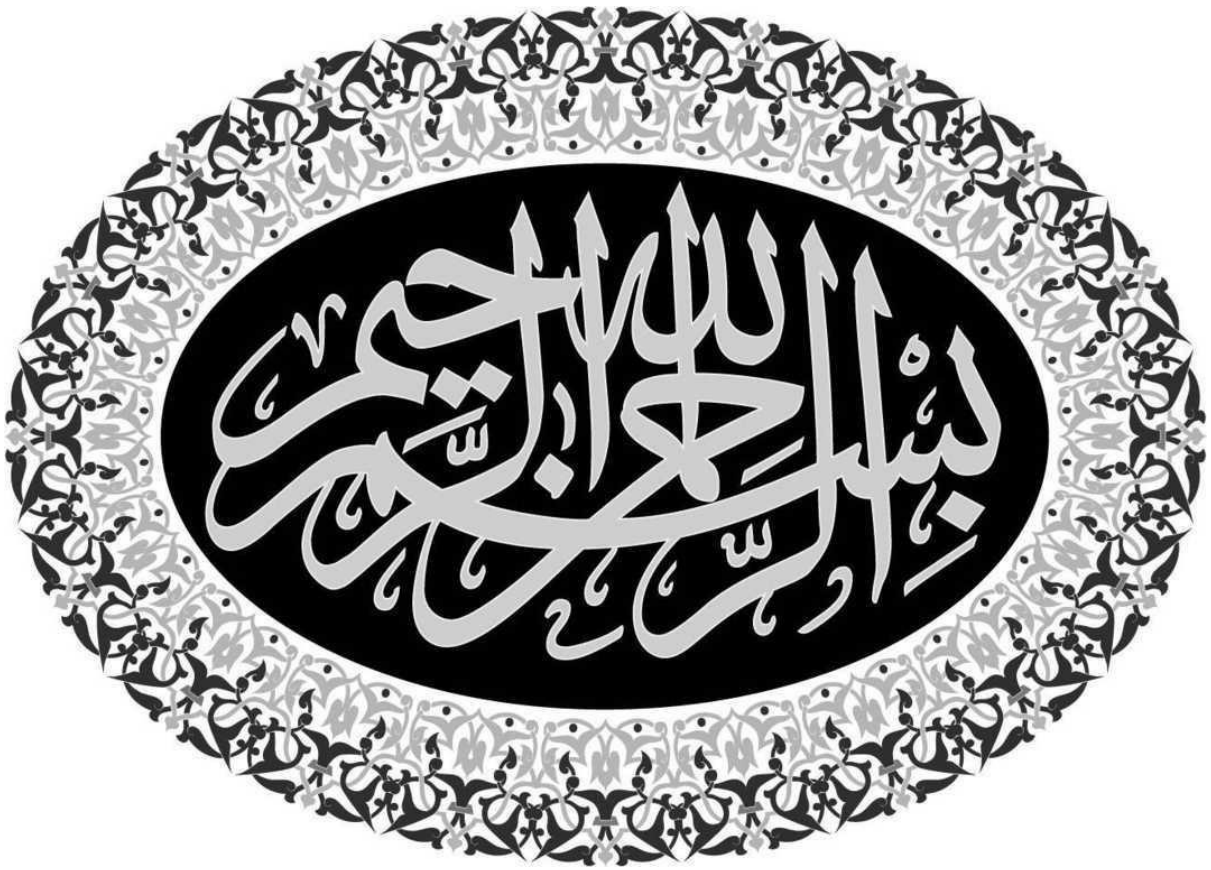


دانشکده معارف اسلامی و حقوق

پایان‌نامه کارشناسی ارشد رشته معارف اسلامی و حقوق

گرایش جزا و جرم‌شناسی

جرایم علیه حیثیت معنوی اشخاص در فضای سایبر و اعاده حیثیت آن

استاد راهنما: دکتر علی غلامی

استاد مشاور: دکتر سلمان عمرانی

دانشجو: مسعود پیرهادی

شهریور ۹۴

بسم الله الرحمن الرحیم

تأییدیه اعضای هیأت داوران حاضر در جلسه دفاع از پایان‌نامه کارشناسی ارشد

اعضای هیأت داوران نسخه نهایی پایان‌نامه **آقای مسعود پیرهادی** شماره دانشجویی ۸۶۳۰۳۰۵۴۹ با عنوان **«جرایم علیه حیثیت معنوی اشخاص در فضای سایبر و اعادهٔ حیثیت آن»** را از نظر شکل و محتوایی بررسی نموده و پذیرش آن را برای تکمیل درجه کارشناسی ارشد پیشنهاد می‌کنند.

اعضای هیأت داوران	نام و نام خانوادگی	رتبه علمی	امضاء
۱) استاد راهنما	دکتر علی غلامی	استادیار	۹۴/۷/۲۹
۲) استاد مشاور	دکتر سلمان عمرانی	استادیار	
۳) استاد داور	دکتر سید بشیر حسینی	استادیار	

٤) نماینده شورای تحصیلات تکمیلی دانشکده : دکتر سلمان عمرانی .....

شکر شایان نثار ایزد منان که توفیق را رفیق راهم ساخت تا این پایان نامه را به پایان برسانم از استاد فاضل و اندیشمند جناب آقای دکتر علی غلامی به عنوان استاد راهنما که همواره نگارنده را مورد لطف و محبت خود قرار داه‌اند،کمال تشکر را دارم و اگر نبود حلم و علم ایشان، اثری از این پایان‌نامه نبود.

از استاد فرهیخته و فرزانه جناب آقای دکتر سلمان عمرانی به عنوان استاد مشاور که با نظارت و مشاورت عالمانه و دلسوزانه، بنده را به مسیر صحیح پژوهش رهنمون ساختند، صمیمانه سپاسگزارم.

چکیده

باگسترش فناوری‌های پیشرفته، جرایم ارتکابی نیز متنوع و متفاوت شده‌اند و بسیاری از قوانین و رویه‌های پیشین برای مواجهه با این جرایم ناکارامد به نظر می‌رسند.

یکی از مصادیق مهم فناوری پیشرفته، فضای سایبر و ابزارها و موارد مرتبط با آن مانند رایانه، تلفن همراه هوشمند و شبکه اجتماعی است. هر روزه در فضای سایبر، جرایم بسیاری اتفاق می‌افتد که بسیاری از آن‌ها، علیه حیثیت معنوی اشخاص ارتکاب می‌یابد. جرایمی مانند توهین، افترا و نشر اکاذیب رایانه‌ای که با توجه به چالش‌های فضای مجازی مانند گستره و سرعت انتشار در آن، حیثیت معنوی اشخاص را گاهی بیش از جرایم در فضای حقیقی دچار خدشه می‌کند و آن‌طور که می‌توان در فضای حقیقی، اعاده حیثیت نموده و خسارت معنوی وارد آمده به اشخاص را جبران نمود، در فضای مجازی چنین امکانی وجود ندارد. در واقع قوانین فعلی، امکان اعاده حیثیت اشخاص را از جرایم سایبری ایجاد نمی‌کند و می بایست با اتخاذ روش‌های پیشگیرانه و آموزش‌های شهروندی، مانع ارتکاب جرایم علیه حیثیت معنوی اشخاص در فضای سایبر شد.

کلمات کلیدی

حیثیت معنوی، جرم علیه حیثیت معنوی، جرم رایانه‌ای، جرایم سایبری، فضای سایبر، اعاده حیثیت

فهرست

مقدمه

رایانه، در سال‌های اخیر به صورت حیرت‌آوری وارد زندگی انسان‌ها شده است؛ به نحوی‌که زندگی بدون رایانه و امکانات آن، دشوار به نظر می‌آید. تعداد قابل توجهی از مردم دنیا اساس زندگی خود را بر مبنای تکنولوژی تنظیم کرده‌اند و از امکانات و تسهیلات آن بهره می‌برند، تسریع در تبادل اطلاعات با سرعت و دقتی بالا صورت می‌پذیرد. از سوی دیگر، پیوند رایانه‌ها به هم در قالب شبکه‌های اطلاع‌رسانی، بر شتاب گردش اطلاعات در جهان افزوده است و امکان به‌دست آوردن اطلاعات، افزایش چشمگیری پیدا کرده است.

علی‌رغم نکات پیش‌گفته در مزایای رایانه و فضای سایبر[1] از آن‌جا که این محیط، مخفی، آزاد و نامحدود است، احتیاج به نظم دارد و اگر خلاف این باشد، هر «صفحه» از این محیط می‌تواند صحنه جرم و آشفتگی بسیار باشد. امروزه مجرمان حیطه سایبر، از رایانه به عنوان کانونی مخفی، امن و مطمئن در راستای رسیدن به مقاصد شوم خود بهره می‌گیرند. در حقیقت، حس پوشیده ماندن اعمال ارتکابی و عدم کشف آن‌ها که ناشی از عدم نظارت دقیق و مؤثر بر محیط سایبر است و نیز این موضوع که آثار جرایم ارتکابی در این محیط معمولاً باقی نمی‌ماند، به بزهکاران این دنیای خیالی، فراغ بال می‌دهد که به دور از دیدگان شماتت‌بار پلیس و مردم، خواسته‌های شریرانه خود را به راحتی به معرض اجرا بگذارند (شیرزاد، ۱۳۸۸، ص ۱۱).

امروزه تقریباً می‌توان با قاطعیت مدعی شد که اکثریت قریب به اتفاق افراد، آشنایی اجمالی با فضای مجازی دارند و بسیاری از افراد هم بخش زیادی از اوقات خود را در فضای اینترنت سپری می‌کنند. واقعیتی که هیچ کس از آن بی اطلاع نیست آن است که اینترنت و فضای مجازی همان قدر که به شئون زندگی بشر کمک می‌کند می‌تواند در صورت استفاده ناصحیح، آسیب‌های جبران ناپذیری وارد سازد. به دیگر سخن می‌توان گفت قربانیان جرایم سایبری در واقع قربانیان تبعات منفی پیشرفت تکنولوژی هستند.

[1] Cyber space

محدودیت‌های موجود در فضای واقعی و جذابیت‌هایی که در فضای سایبر موجود است افراد را بیشتر به استفاده از اینترنت جذب می‌کند و چون اکثر استفاده‌کنندگان این پدیده جوانان هستند، بنابراین گرایش و تأثیرهای منفی و آسیب زا، بیشتر بر روی جوانان است. مع‌الاسف جایگاه اینترنت در کشور ما آنچنان که باید علمی و کارامد نیست، این در حالی است که افراد در راستای پیشبرد اهداف مورد نظر به منظور ارتقای سطح علمی کشور کمتر از اینترنت استفاده می‌کنند زیرا آمارها[1] نشان می‌دهد که اکثر کاربران اینترنت، بیشتر اوقات خود را در شبکه‌های اجتماعی، سایت‌های اشتراک‌گذاری فیلم و عکس، سایت‌های دانلود و ... می‌گذرانند.

در حال حاضر آنچنان که شایسته است استفاده درستی از اینترنت نمی‌شود. از این روست که ما باید آموزش استفاده درست از اینترنت را در صدر اهداف آموزشی خود قرار دهیم. در این میان خانواده‌ها برای آموزش صحیح استفاده از اینترنت بسیار مؤثرند، امروزه برخی خانواده‌ها فقط به خرید رایانه اکتفا می‌کنند و معتقدند که خود فرزندان، استفاده از آن را یاد می‌گیرند. در صورتی که باید ابتدا فرهنگ استفاده و تذکرهای لازم را به اضافه آموزش مناسب به فرزندان خود بدهند و سپس وسیله را مهیا کنند.

جرایم علیه اخلاق و عفت عمومی عبارتست از هر نوع عمل، رفتار وگفتاری که خلاف عفت و پاکدامنی جامعه باشد. این جرایم، متنوع و متعددند. برخی از آنها از جمله جرایم حدی می باشند، مثل زنا و لواط و بعضی تعزیری هستند، مانند روابط نامشروع مادون حد و عرضه و خرید و فروش صور قبیحه. وقوع برخی از این جرایم (اعم از حدی و تعزیری) با ظهور اینترنت از محیط فیزیکی به محیط مجازی انتقال یافته است.

در علت‌شناسی این قبیل جرایم می‌توان علل بسیاری از جمله عوامل فرهنگی، سیاسی، مشکلات روحی و روانی نظیر افسردگی، عصبانیت، حسادت، انتقام‌جویی، حس‌تنفر، تفریح و سرگرمی، خودکم بینی و حقارت،

---

۱ Alexa، پایگاه رتبه دهی به سایت‌های دنیا می‌باشد که رتبه‌بندی ارائه شده توسط این سایت در بخش ایران، اثباتی بر این ادعاست.

حس رقابت و ... را نام برد. حال آن که فقر فرهنگی و پایبند نبودن به ارزش‌های جامعه و باورهای دینی یکی از عوامل مهم ارتکاب این قبیل جرایم در فضای مجازی می‌باشد.

دسته‌ای از جرایم علیه اشخاص، آسیب روحی و معنوی و حیثیتی را برای بزه‌دیده به همراه می‌آورند که این قبیل جرایم را جرایم علیه حیثیت معنوی اشخاص می‌نامند، از جمله توهین، افترا، اشاعه و نشر اکاذیب و ... . حیثیت معنوی افراد چه از منظر عقل و چه از منظر نقل از اهمیت ویژه‌ای برخوردار است. از زمان ظهور و بروز فناوری‌های مرتبط با رایانه، جرایم علیه حیثیت معنوی اشخاص از طریق رایانه و در فضای سایبر به وفور اتفاق می‌افتد.

فضای سایبر شرایطی را به وجود آورده که بزهکاران می‌توانند به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بارآورده و در عین حال ناشناخته باقی بمانند. هتاکی و اهانت، نشر اکاذیب از طریق سامانه‌های رایانه‌ای، نقض حریم خصوصی افراد، شنود غیرمجاز و انتشار اسرار خصوصی اشخاص، نمونه‌ای از جرایم سایبری است که بی‌توجهی به اصول اخلاقی و موازین شرعی موجد آن است. بخش عمده‌ای از جرایم رایانه‌ای ارتکابی در کشور نیز برخاسته از مشکلات روحی و روانی بزهکاران فضای مجازی می‌باشد.

در این پژوهش ابتدا به مفهوم، ارکان و مصادیق جرم علیه حیثیت معنوی اشخاص و سپس تمایزات وقوع چنین جرایمی در فضای سایبر نسبت به فضای حقیقی پرداخته‌ایم. در ادامه مفهوم و شیوه‌های اعاده حیثیت و چالش‌های اعاده حیثیت در فضای سایبر آمده‌اند. در انتها نیز جمع‌بندی و پیشنهادات، پایان بخش این پژوهش خواهد بود.

اهمیت پژوهش

جرم علیه حیثیت معنوی اشخاص، قدمتی به اندازه تاریخ بشر دارد. اما با بروز و ظهور عرصه‌های جدید در ارتباط میان انسان‌ها، صورت‌های متفاوتی به خود گرفته است. در واقع یکی از مؤلفه‌های پرداختن به

موضوع جرم، بستر وقوع جرم و ابزار ارتکاب جرم است. این بستر و ابزار با پیشرفت فناوری تغییر می‌یابد و در نتیجه باید به وقوع جرم متناسب با این تغییرات پرداخت.

طبق دسته‌بندی‌های مشهور اجتماعی، جوامع به سه نسل سنتی، صنعتی و اطلاعاتی تقسیم می‌شوند. همانطور که با ورود از دوره سنتی به دوره صنعتی و با اختراع ابزارهایی مانند ماشین چاپ و در نتیجه انتشار کتاب‌ها و روزنامه‌ها، جرایم نیز متناسب با این فضا تغییر کردند، امروزه نیز با پایان عصر صنعتی و گذار به عصر اطلاعاتی و دانشی، جرایم متفاوت شده‌اند و شناخت این عرصه مطالعه و بررسی جدیدی می‌طلبد.

تعدادی از فناوری‌های مهم عصر امروز، رایانه، تلفن همراه، اینترنت و فضای مرتبط با آن یعنی فضای مجازی است. روزانه در این فضا جرایم بسیاری علیه حیثیت معنوی اشخاص ارتکاب می یابد که به دلیل نبود سامان روشن و قوانین متقن پیگیری جدی نمی‌شوند. اگرچه در چند سال اخیر پیشرفت‌هایی در این عرصه به وقوع پیوسته اما تا نقطه مطلوب فاصله زیادی احساس می‌شود.

پایان‌نامه پیش رو، مطالعه ماهیت، اهمیت و چالش‌های جرم علیه حیثیت معنوی اشخاص در فضای سایبر و اعاده حیثیت آن است.

سؤال اصلی پژوهش

با توجه به تفاوت فضای سایبر و حقیقی آیا امکان اعاده حیثیت معنوی اشخاص در آن وجود دارد؟

فرضیه

جرایم علیه حیثیت معنوی اشخاص در فضای سایبر به گونه‌ای است که گاهی اعاده حیثیت بسیار دشوار و گاهی غیرممکن می‌باشد.

پیشینه پژوهش

در اواسط دهه ۹۰ میلادی با توسعه شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم رایانه-ای، تحت عنوان جرایم سایبری یا مجازی شکل گرفت. جرایم نسل سوم رایانه‌ای که به جرایم در محیط مجازی معروف است، غالباً از طریق شبکه جهانی اینترنت به وقوع می‌پیوندد.

در مقاله‌ای با عنوان «پیشگیری از جرایم سایبر در پرتو موازین حقوق بشر» این‌گونه آمده است: «ماهیت فضای سایبر به گونه‌ای است که پیشگیری وضعی، یکی از تدابیر ناگریز و لازم‌الاجرا محسوب می‌شود. حتی در دنیای فیزیکی نیز این سخن، صادق است. زیرا تنها گزینه‌ای است که می‌تواند دو ضلع مثلث جرم، یعنی فرصت و ابزار ارتکاب جرم را هدف قرار دهد. بنابراین، باید یک راه حل بینابین اتخاذ شود که به موجب آن ضوابطی که تدوین می‌گردد، بر اساس قواعد و مقررات حقوقی و همچنین ملاحظات حاکم بر فضای سایبر باشد تا علاوه بر صیانت از امنیت ملی و نظم، سلامت یا اخلاق عمومی، به دیگر موازین حقوق بشر، یعنی آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی نیز خدشه‌ای وارد نگردد. بی‌تردید مراجعه به تجارب دیگر کشورها با رعایت شرایط خاص کشورمان، چنانچه بر پایه‌ی دیدگاه‌های واقع‌گرایانه‌ی حقوقی ـ فنی باشد، می‌تواند نتایج مطلوبی را پدید آورد.» (جلالی فراهانی، ۱۳۸۴،ص ۱۳)

با مروری بر قوانین جزایی و قانون مطبوعات و جرایم رایانه‌ای می‌توان به فقدان قانون جامعی پیرامون جرایم رایانه‌ای اذعان کرد.

یکی از قوانین در زمینه جرایم مربوط به فضای مجازی و رایانه‌ای، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است. در این قانون در فصل اول، جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی شامل دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای و در فصل دوم، جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی شامل جعل رایانه‌ای، تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی ذکر شده‌اند. همچنین در فصل سوم، سرقت و کلاهبرداری مرتبط با رایانه و در فصل چهارم، جرایم

علیه عفت و اخلاق عمومی و در فصل پنجم، هتک حیثیت و نشر اکاذیب و در نهایت در فصل ششم سایر جرایم جرم‌انگاری شده‌اند.

سامان پژوهش

به منظور شناخت هر چه بیشتر و بهتر جرایم علیه حیثیت معنوی اشخاص در فضای سایبر ابتدا می‌بایست تعاریف این جرایم در دنیای حقیقی، تاریخچه آنان و عناصر و ارکان آن‌ها را شناخت. در گام بعدی و برای احتراز از اشتباه در موضوعات این جرایم، مصادیق در فضای حقیقی ذکر می‌شود و سپس امکان سنجی وقوع این جرایم در فضای سایبر بررسی می‌شود. این سیر باید طی شود تا به نقطه‌ای برسیم که امکان وقوع جرایم در فضای سایبر در وهله نخست و شیوه‌های ارتکاب آن، چالش‌های پیشگیری و برخورد با آن و راه‌حل‌ها مشخص شود. بنابراین بخش اول این پژوهش به تعاریف، مفاهیم و تاریخچه اختصاص دارد. در فصول این بخش مفهوم، ارکان و مصادیق جرم علیه حیثیت معنوی اشخاص ارائه شده و در ذیل آن، انواع جرایم و مجرمین فضای سایبر شرح داده شده‌اند و بعد از دسته‌بندی جرایم سایبری، جرایم علیه حیثیت معنوی اشخاص در محیط سایبر ذکر شده و هر کدام به تفصیل شرح داده شده‌اند. در بخش دوم این پژوهش، اعاده حیثیت از جرایم علیه حیثیت معنوی اشخاص در فضای سایبر بررسی شده و در فصول آن مفهوم و شیوه‌های اعاده حیثیت و چالش‌های آن در فضای سایبر بیان شده‌اند. در پایان نیز نتایج حاصل از پژوهش و پیشنهاداتی در جهت اصلاح و بهبود مشکلات ناشی از جرم علیه حیثیت معنوی اشخاص در فضای سایبر ارائه شده‌اند.

بخش اول: جرایم علیه حیثت معنوی اشخاص در فضای سایبر

پایان‌نامه پیش رو شامل دو بخش کلی است، که هر یک مشتمل بر دو فصل می‌باشد. بخش نخست پایان‌نامه پیرامون جرایم علیه حیثیت معنوی اشخاص در فضای سایبر می‌باشد، که رویکرد اصلی در آن، نفس جرایم علیه حیثیت معنوی اشخاص نیست، بلکه تأکید اصلی، بر ارتکاب آن در فضای سایبر بوده است.

۱-۱- فصل اول: مفهوم، ارکان و مصادیق جرم علیه حیثیت معنوی

در فصل نخست بخش اول، ابتدا به مفهوم جرایم علیه حیثیت معنوی اشخاص، سپس به ارکان و عناصر تشکیل‌دهنده این جرایم و در نهایت به مصادیق جرایم علیه حیثیت معنوی اشخاص پرداخته شده است.

۱-۱-۱- جرایم علیه اشخاص

امروزه با توجه به نفوذ عمیق رایانه در همه عرصه‌ها و جنبه‌های زندگی انسان، بسیاری از جرم‌های سنتی قابلیت ارتکاب با رایانه را دارند. در نامه‌ی الکترونیکی دان پارکر[۱] به پروفسور سوزان برنر[۲] چنین اظهار شده است: «زمانی فرا می‌رسد که می‌توانیم قوانین مربوط به جرم‌های سایبری را کنار بگذاریم، زیرا بیشتر جرم‌ها به نحوی با استفاده از رایانه ارتکاب خواهند یافت و همه جرم‌ها، جرم سایبری خواهند بود.» (سوزان برنر، ۲۰۰۱، ص ۴۸)

تصور اینکه مجرم از راه دور و با استفاده از رایانه به قتل یا ضرب و جرح و وارد آوردن آسیب بدنی به فرد دیگر اقدام کند، دشوار است. با این حال مهم‌ترین مصداق‌های جرم علیه اشخاص یعنی قتل عمدی و غیر-عمدی و ایراد آسیب بدنی عمدی و غیرعمدی را می‌توان از رهگذر دست‌یابی به سیستم رایانه بیمارستان‌ها و تغییر دادن علامت‌ها و نسخه‌های یک بیمار مرتکب شد.

---

۱. Dann Parker

۲ Susan Brenner

همچنین جرایم قذف، توهین، افترا و نشر اکاذیب که از جرم‌های علیه حیثیت معنوی اشخاص است و سایر جرایم غیرجسمی علیه اشخاص را نیز می‌توان در مقیاسی بسیار گسترده‌تر از گذشته با رایانه مرتکب شد.

پس از این توضیح، ارتکاب جرایم علیه اشخاص را که به جرایم علیه تمامیت جسمانی و جرایم علیه حیثیت معنوی افراد تقسیم می‌شود، در محیط مجازی بررسی می‌کنیم.

۱-۱-۱-۱- جرایم علیه تمامیت جسمانی

صدمات بدنی به اشخاص از نظر شدت و یا ضعف صدمات یا کیفیت صدمه، دارای آثار و نتایج متفاوت است که گاه نتیجه آن، سلب حیات از شخص زنده می‌شود و گاهی موجب اختلالات خفیف‌تری می‌گردد که به صورت مرض یا سلب قدرت کارکردن و غیره در می‌آید.

۱-۱-۱-۱-۱-قتل

در قوانین جزایی اهمیت زیادی به قتل نفس داده شده است. به نظر قانون‌گذار، مقام فرد در جامعه بسیار محترم و ارجمند است. کسی که مرتکب قتل نفس می‌شود عضوی از اعضای فعال جامعه را از بین می‌برد. این جنایت، اولیای دم را متضرر و نظم جامعه را مختل می‌سازد.

هدف ما در اینجا بیان خصوصیات انواع قتل و نحوه آنها نیست، زیرا در قوانین موضوعه و کتب حقوق جزای اختصاصی، شرایط اختصاصی قتل به طور مفصل بررسی شده است.

بحث ما در اینجا این است که آیا امکان ارتکاب قتل از طریق رایانه وجود دارد؟

به عبارت دیگر، آیا قتل رایانه‌ای وجود دارد یا خیر. در وهله اول به نظر می‌رسد که ارتکاب قتل از طریق رایانه غیر قابل تصور است و امکان تحقق آن وجود ندارد، ولی مواردی را می‌توان فرض کرد که امکان ارتکاب قتل از طریق رایانه وجود داشته باشد. هر چند تاکنون اتفاق نیفتاده و یا اگر هم اتفاق افتاده، اطلاعی در دست نیست.

فرض کنیم شخصی از طریق گفتگوی اینترنتی (چت[1]) در حالی‌که از وضعیت روحی و روانی طرف مقابل اطلاع دارد، عمداً و به قصد قتل، خبر ناگواری به دروغ به وی بدهد و شخص مذکور به محض شنیدن آن خبر، فوت کند، یا اینکه این خبر ناگوار را از طریق پست الکترونیک به صندوق الکترونیکی طرف مقابل بفرستد. آیا در چنین صورتی نمی‌توان شخصی که فعلی را به قصد قتل انجام داده (اطلاع دادن خبر دروغ ناگوار) قاتل دانست؟

یا در مورد مثال بالا (طرف به جای اطلاع دادن خبر ناگوار)، ضمن اطلاع از وضعیت مخاطب (مثل کم سن بودن مجنی علیه)، عمداً و به قصد قتل تصویر وحشتناکی را می‌فرستد و طرف به محض باز کردن پست الکترونیک خویش، در اثر مشاهده تصویر، حیات خود را از دست می‌دهد. آیا این‌ها را می‌توان مجازات کرد؟

همچنین در موردی که هدایت هواپیما از طریق رایانه صورت می‌گیرد، شخصی که سیستم هواپیما را بر عهده دارد عمداً هواپیما را به مسیر دیگری منحرف می‌کند، تا اینکه به کوه برخورد کند و این اتفاق هم می‌افتد و هواپیما سقوط می‌کند. در اینجا قتل سرنشینان از طریق سیستم رایانه‌ای است.

همچنین اگر شخصی با ورود به سیستم رایانه‌ای بیمارستان و تغییر دادن علامت‌ها و نسخه‌ها سبب شود که داروی دیگری به بیمار داده شود و در نتیجه فرد بمیرد، قتل با ابزار رایانه رخ داده است.

در این موارد می‌توان امکان تحقق قتل از طریق رایانه را تصور کرد و با شرایطی که در قانون موضوعه برای قتل لازم شمرده است، انطباق داد.

پروفسور برنر در این خصوص اظهار می‌دارد: «این جرم در واقع همان جرم سنتی قتل نفس است که در سبکی غیر سنتی و به وسیله مجرمی که احتمالاً در زمان وقوع مرگ، صدها یا هزاران مایل دورتر از بزه‌دیده است، ارتکاب می‌یابد. در ماجرای قتل رایانه‌ای، رایانه فقط ابزار ارتکاب جرمی است که به اندازه

[1] chat

خود بشریت قدمت دارد. انسان‌ها فناوری را برای هدف‌های مختلف مشروع و نامشروع به کار می‌گیرند. در اینجا رایانه جانشین خنجر، تفنگ و سم و دیگر وسایلی شده است که برای گرفتن جان دیگران مورد استفاده قرار می‌گیرد. مراجع قضایی نیز اغلب جرم قتل نفس را بر اساس آلت قتاله ارزیابی نمی‌کنند؛ یعنی «قتل با خنجر» و «قتل با سم» با یکدیگر تفاوتی ندارند. بنابراین، به نظر می‌رسد که لازم نیست که استفاده از رایانه در مورد قتل را در قوانین کیفری قدیمی نیز وارد کنیم. این نمونه‌ای بارز از وضعیتی است که در آن، قوانین کیفری سنتی برای پرداختن به موضوع استفاده از رایانه در ارتکاب عمل بزه کارانه، کافی و کارامد هستند.» (سوزان برنر، ۲۰۰۱، ص ۵۲)

۱-۱-۱-۱-۲- جنایات کمتر از نفس

از دیدگاه قانون مجازات اسلامی جنایت بر اعضا همانند جنایت بر نفس مذموم است و اگر شخصی درباره دیگری مرتکب جنایتی گردد و آسیبی به او برساند ضامن است و فرقی نمی‌کند که آسیب و صدمه واقع شده با چه وسیله و ابزاری صورت گرفته باشد. جنایت بر اعضا مثل قتل نفس به سه نوع ارتکاب می‌یابد: عمدی، شبه عمد و خطای محض.

سؤالی که در اینجا مطرح می‌شود این است که آیا جنایت بر اعضا از طریق رایانه قابل تحقق است یا خیر.

مواردی را می‌توان تصور کرد که امکان ارتکاب جنایت کمتر از نفس از طریق رایانه قابل تحقق و ممکن است، هر چند شاید تا به حال ارتکاب نیافته باشد.

چنانچه شخصی از طریق رایانه و در فضای مجازی، اشعه‌ای را که برای انسان مضر است به رایانه شخص دیگری ارسال کند و طرف مقابل در اثر برخورد با اشعه، بینایی خود را از دست بدهد، مسلماً در این صورت شخص فرستنده ضامن است. یا اینکه شخص با علم به وضعیت روحی و روانی طرف مقابل، تصویر وحشتناکی به او بفرستد و شخص با مشاهده آن تصویر، از ترس لال شود و دیگر نتواند صحبت کند.

یا زمانی که شخصی از طریق رایانه (و از طریق گوشی) با دیگری صحبت می‌کند، صدای ناهنجاری پخش کند که سبب شود در اثر آن پرده گوش طرف مقابل از بین برود و یا شنوایی‌اش کم شود.

یا در مورد مثال هواپیما در قتل نفس، سبب شود که به جای وقوع قتل، عده‌ای از مسافران صدمه ببینند. همچنین به تازگی گزارش شده است که امکان ارسال بو از طریق رایانه فراهم شده است و پیش‌گامان این طرح در ادامه تلاش‌هایشان بوی لیمو یا توت‌فرنگی را به فضای اینترنت کشانده‌اند. بو همانند طیف رنگی که مشتمل بر رنگ‌های مختلف است، از حدود هزار بخش تشکیل شده است. نتایج تحقیقات نشان می‌دهد شصت قسمت از طیف بو را می‌توان به فضای اینترنت وارد ساخت (آلبرت بن شاب، ۱۳۸۴، ص ۵۷).

در این صورت اگر کسی بوی یک ماده سمی مثل اسید نیتریک را برای دیگری بفرستد، در صورت ایجاد صدمه ضامن است.

این موارد امکان تحقق جنایت بر اعضا را از طریق رایانه نشان می‌دهد که مسلماً شخص جانی ضامن است و وسیله ارتکابی تأثیری در تحقق جنایت ندارد.

۱-۱-۱-۲- جرایم علیه حیثیت معنوی اشخاص

حیثیت معنوی افراد مانند تمامیت جسمانی آن‌ها مورد احترام می‌باشد و هیچ‌کس نمی‌تواند به حیثیت معنوی دیگران تعرض کند. در این میان حرمت و شرف اشخاص از اهمیت اساسی برخوردار است. جرایم علیه حیثیت معنوی اشخاص، جرایمی است که غالباً به وسیله گفتار و کتابت در فضای حقیقی و مجازی واقع می‌شود. بزه‌های علیه حیثیت معنوی، به رفتارهایی گفته می‌شود که روان آدمی را هدف می‌گیرد. در فضای سایبر که محل حضور ذهن فرد است، جرایم علیه اشخاص با روان و حیثیت معنوی آنان ارتباط می‌یابد.

در این میان رایانه در تحقق این جرایم نقش بسزایی دارد که ما در این بحث به بررسی برخی از آن‌ها از جمله توهین، افترا، قذف و نشر اکاذیب که بیشتر قابلیت ارتکاب با رایانه را دارند، می‌پردازیم.

۱-۱-۱-۱-۱- توهین

یکی از مواردی که در قوانین جرایم رایانه‌ای می‌بایست بیشتر مورد توجه قرار گیرد، توهین است. معنای لغوی توهین در کتب لغت این‌گونه آمده است: «توهین مصدر لازم به معنای خوار کردن، خوار داشتن، سبک داشتن، خفیف کردن، سست کردن است.» (معین، ۱۳۶۳، ص ۱۱۷۱)

توهین در جای دیگری این‌گونه توصیف شده است: «توهین، به معنای خوارکردن و تحقیر و تخفیف کردن و از مصادیق هتک حرمت است.» (هاشمی، ۱۳۸۴، ص ۲۷۹)

توهین در اخلاق اسلامی از جمله رذایل اخلاقی است که به شدت از آن نهی شده است. کما اینکه از امیرالمؤمنین علیه السلام نقل شده که فرمودند: «إنَّ اللَّهَ حَرَّمَ الْجَنَّةَ عَلَى كُلِّ فَحَّاشٍ بَذِيٍّ قَلِيلِ الْحَيَاءِ لَا يُبَالِي مَا قَالَ وَلَا مَا قِيلَ لَهُ...» خداوند بهشت را بر هر فحاش بی‌آبرو و کم‌شرمی که باکی از آنچه گوید و آنچه به او گویند ندارد حرام کرده است.(مجلسی، ۱۳۷۸، ص ۲۰۷)

توهین لفظی را فحش می‌نامند که هر کلام زشت و رکیک و مستهجن را در بر می‌گیرد. توهین فعلی، کارهایی مثل آب دهان به روی کسی انداختن و هل دادن تحقیرآمیز را در بر می‌گیرد (میر محمد صادقی، ۱۳۸۶، ص ۱۵۲).

ماده ۶۰۸ (۸۴۰) قانون مجازات اسلامی در این باره می‌گوید: «توهین به افراد از قبیل فحاشی و استعمال الفاظ رکیک چنانچه موجب حد قذف نباشد، به مجازات شلاق تا ۷۴ ضربه و پنجاه هزار تا یک میلیون ریال، جزای نقدی محکوم می‌شود.»

قانون‌گذار علاوه بر ماده ۶۰۸ (۸۴۰) قانون مجازات اسلامی با توجه به شخصیت و مقام طرف اهانت، مواد دیگری را تصویب کرده است. از جمله مواد ۵۱۳ (۷۴۴)، ۵۱۴ (۷۴۵) و ۶۰۹ (۸۴۱) قانون مجازات اسلامی، ماده ۲۰ لایحه قانونی استقلال کانون وکلای دادگستری و ماده ۳۰ قانون مطبوعات.

منطوق صریح ماده ۶۰۸ (۸۴۰) قانون مجازات اسلامی، نفس توهین را مستلزم مجازات قلمداد کرده است و می‌دانیم که توهین به روش‌های مختلفی صورت می‌گیرد که این ادعای ما را مواد قانونی ۶۹۷ (۹۲۱) تا ۷۰۰ (۹۲۴) قانون مجازات اسلامی تأیید می‌کند. یکی از این روش‌ها کاربرد اینترنت است که امروزه بسیار شایع می‌باشد. ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی کاملاً مشمول توهین اینترنتی می‌شود، در این ماده آمده است: «... در روزنامه، جراید، نطق در مجامع یا به هر وسیله دیگر...» و قید «به هر وسیله دیگر» بیانگر این موضوع است که قانون‌گذار می‌خواهد به هر نحوی که شده است، جلوی چنین جرمی را بگیرد و اصل جرم از نظر او دارای اهمیت است که یکی از این راه‌ها اینترنت می‌باشد.

ماده ۷۰۰ (۹۲۴) قانون مجازات اسلامی نیز به توضیح هجو اینترنتی و یا ارسال هرزنامه به پست الکترونیک و انتساب غیر واقعی آن به غیر می‌پردازد.

۱-۱-۱-۱-۱-۱- توهین رایانه‌ای

توهین رایانه‌ای نوع جدیدی از جرم توهین سنتی است که در آن وسیله ارتکاب، رایانه، تبلت، تلفن‌های هوشمند و هر وسیله ای شبیه به رایانه می‌باشد.

آن‌چه در اینجا مد نظر است، نحوه تحقق اصل جرم توهین است؛ یعنی امکان تحقق توهین در فضای مجازی، وجود دارد یا خیر.

در قانون جرایم رایانه‌ای که به قانون جدید مجازات اسلامی ملحق شده، به جرم توهین اشاره نشده است. گرچه همان‌گونه که ذکر شد توهین یکی از مصادیق بارز هتک حرمت و حیثیت است؛ چرا که با توهین به فرد، حرمت او از بین می‌رود و انتشار آن در اینترنت جرم خواهد بود.

از دیدگاه جرم‌شناختی، توهین در فضای مجازی قابل قیاس با توهین سنتی نمی‌باشد؛ زیرا در توهین سنتی ممکن است فرد در مقابل عده‌ای محدود مورد اهانت واقع شود؛ اما آسیب ناشی از توهین در فضای مجازی به مراتب بیشتر از توهین سنتی است. شاید بتوان در توهین سنتی اعاده حیثیت نمود؛ اما در توهین

مدرن که گستره نشر آن را می توان جهانی در نظر گرفت، اعاده حیثیت بسیار مشکل و غالباً غیرممکن است و به همین جهت، نیاز به شدت عمل بیشتری دارد. اگرچه جنبه‌های خشن توهین سایبری نسبت به مواردی چون قتل، ضرب و جرح و تجاوز کمتر نمایان می‌باشد، اما درست به همان اندازه واقعی است و گاه نتایج وخیم‌تری در پی دارد و هزینه‌ای سنگین‌تر را بر جامعه تحمیل می‌کند (سلیمی و داوری، ۱۳۸۶، ص ۲۱۸). بنابراین، علاوه بر الفاظ، هر گونه عکس، کاریکاتور، فیلم، صوت یا تصویر که عرفاً توهین تلقی شود، موجب هتک حیثیت خواهد بود.

مفاد ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی به طور صریح شرط تحقق جرم را بیان می‌کند و می‌گوید: «هر کسی به قصد اضرار به غیر یا تشویش اذهان ...». این تعلیل گویای این مطلب است که هرگاه این قصد حاصل شود، ملازمه‌اش مجازات مذکور در ماده قانونی است. به بیان دیگر نوعی تلازم وضعی بین قصد و مجازات وجود دارد. حال هر چیزی این ملازمه را به وجود بیاورد، به تبع آن مجازات مذکور باید جاری گردد و می‌توان گفت که از طریق رایانه قصد فوق حاصل می‌گردد؛ یعنی هم اضرار مادی و هم اضرار معنوی حاصل می‌شود و اینترنت به عنوان ابزاری پیشرفته برای چنین جرایمی در محیطی باز محسوب می‌شود.

علاوه بر موارد مذکور، جز در موارد تصریح‌شده در قانون مثل ماده ۵۱۷ (۷۴۸) قانون مجازات اسلامی، در حضور شخص مورد توهین، علنی بودن ضرورتی ندارد. با این حال، توهین سایبری، یک توهین علنی است؛ زیرا هیچ فضایی علنی‌تر از فضای مجازی نیست. در توهین سایبری، خواه فرد مورد اهانت حضور داشته باشد و خواه حضور نداشته باشد، توهین علنی است.

اینترنت می‌تواند یکی از مصادیق ماده ۶۹۹ (۹۲۳) قانون مجازات اسلامی باشد، چون در آن ذکر شده است: «... به نحوی متعلق به او قلمداد نماید» و قید «به نحوی» بسیار کلی و جامع است، یعنی قانون‌گذار هر کسی که از هر راهی چنین جرمی را مرتکب گردد، مجازات می‌کند و امروزه از طریق اینترنت ارتکاب چنین

جرمی ممکن است و صورت هم گرفته است. اساساً با قید مذکور، ماده فوق مفهومش بر اتهام اینترنتی بار می‌شود و تهمت اینترنتی یکی از مصادیق آن محسوب می‌شود.

امروزه شبکه اینترنت که هدفش اطلاع‌رسانی است، در دایره مطبوعات و زیر مجموعه جراید بوده و می‌توان گفت که اگر مواد قانونی موجود شامل جراید و روزنامه‌ها باشد، شبکه اینترنت نیز می تواند در دسته جراید قرار گیرد و مشمول احکام آن گردد. می‌توان گفت:

الف) توهینی که از طریق اینترنت صورت می پذیرد، جرم است.

ب) هر جرم درخور کیفر و مجازات می‌باشد.

ج) بنابراین توهینی که از طریق اینترنت صورت می‌پذیرد به خاطر جرم بودن در خور کیفر و مجازات می‌باشد.

هر کسی (انسان عاقل، بالغ، مختار و قاصد) از طریق اینترنت دشنام بدهد، یا عملی را انجام دهد که دیگری را متهم به اموری نماید که شرع ممنوع کرده است و صحت و سقم این نسبت ناروا را نتواند ثابت کند، عمل وی جرم محسوب شده و درخور مجازات می‌باشد.

در نمونه زیر پایگاه اطلاع‌رسانی یکی از مسئولین کشور با انتشار تصویری ذیل خبر «انتخاب مردم باب میل صدا و سیما نبود» در تاریخ ۱۹ بهمن ۹۲ به رئیس جمهور سابق کشور توهین کرده است.

تصویر شماره ۱، صفحه خبر پایگاه اطلاع‌رسانی حجت الاسلام هاشمی رفسنجانی

همانطور که در تصویر مشاهده می‌شود، عبارت «محمود رفت» با عبارت مشهور «شاه رفت» این همانی شده و مشخصاً توهین صورت گرفته است.

۱-۱-۱-۱-۲- افترا

افترا به معنی بهتان، تهمت زدن و به دروغ کارهای ناروا را به کسی نسبت دادن می‌باشد (انوری،۱۳۸۲، ص ۵۴). ریشه لغوی این واژه «فری» و «فریه» است. در فرهنگ لغات قرآن نیز به همین معنا استعمال شده است: «أَمْ يَقُولُونَ افْتَرَاهُ قُلْ فَأْتُواْ بِسُورَه مِّثْلِهِ»[۱]؛ «آیا می‌گویید که پیامبر (ص) در تبلیغ و بیان کلام الله مجید، چیزی را به دروغ به خدا نسبت داده است، پس بگو سوره‌ای مانند آن بیاورید.»

مبنای جرم انگاری این عمل خلاف اخلاق را در کتاب‌های فقهی نیز می‌توان یافت. فقیهان در بحث از قذف، که در ادامه به آن خواهیم پرداخت، از «حدالفریه» سخن گفته اند (علامه حلی، ۱۳۷۶، ص ۵۹). بر این اساس، جرم افترا در ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی به این شرح تبیین شده است: «هر کس به وسیله اوراق چاپی یا خطی یا به وسیله درج در روزنامه و جراید یا نطق در مجامع یا به هر وسیله دیگر به کسی امری را صریحاً نسبت دهد یا آنها را منتشر نماید که مطابق قانون آن امر جرم محسوب می‌شود و نتواند صحت آن اسناد را ثابت نماید، جز در مواردی که موجب حد است، به یک ماه تا یک سال حبس و تا ۷۴ ضربه شلاق یا یکی از آنها حسب مورد محکوم خواهد شد.»

تبصره: در مواردی که نشر آن امر اشاعه فحشا محسوب گردد هر چند بتواند صحت اسناد را ثابت نماید مرتکب به مجازات مذکور محکوم خواهد شد.

افترا از جمله جرایم عمدی است و مرتکب باید در انتساب عمل مجرمانه و کذب بودن موارد استناد، علم و آگاهی داشته باشد. همین اندازه که اسناد دهنده می‌داند و آگاه است که آن عمل مجرمانه‌ای را که به دیگری نسبت می‌دهد بی اساس و دروغ است، به عنوان مفتری قابل تعقیب می‌باشد. علاوه بر آن، مفتری باید عالم به کذب و دروغ بودن آن نیز باشد؛ بنابراین هرگاه مرتکب در نتیجه اشتباه یا سهل‌انگاری، عمل

[۱]. یونس (۱۰)، آیه ۳۸

مجرمانه‌ای مرتکب شود و چنین امری ثابت شود، چنین شخصی به عنوان مفتری قابل مجازات نیست، زیرا فاقد سوء نیت است.

افترا به اشخاص حقیقی و حقوقی (اگر چه از طریق انتشار عکس یا کاریکاتور باشد) در اجرای بند ۸ ماده ۶ قانون مطبوعات (مصوب ۱۳۶۴ – اصلاحات ۱۳۷۹)، به وسیله نشریات منع شده است. در همین خصوص ماده ۳۰ قانون مطبوعات می گوید: «انتشار هر نوع مطلب مشتمل بر تهمت یا افترا یا فحش و الفاظ رکیک یا نسبت‌های توهین آمیز و نظایر آن نسبت به اشخاص ممنوع است. مدیرمسئول جهت مجازات به محاکم قضایی معرفی می‌گردد و تعقیب جرایم مزبور موکول به شکایت شاکی خصوصی است و در صورت استرداد شکایت، تعقیب در هر مرحله‌ای که باشد متوقف خواهد شد.

تبصره یک: «در موارد فوق شاکی اعم از حقیقی یا حقوقی می‌تواند برای مطالبه خساراتی که از نشر مطالب مذکور بر او وارد آمده، به دادگاه صالحه شکایت نموده و دادگاه نیز مکلف است نسبت به آن رسیدگی و حکم متناسب صادر نماید.»

تبصره دو: «هرگاه انتشار مطالب مذکور در ماده فوق راجع به شخص متوفا بوده، ولی عرفاً هتاکی به بازماندگان وی به حساب آید، هر یک از ورثه قانونی می‌تواند از نظر جزایی یا حقوقی طبق ماده و تبصره فوق اقامه دعوی کند.»

تبصره سه ماده اول قانون مذکور در این راستا مقرر داشته است: «کلیه نشریات الکترونیکی مشمول مواد این قانون است.»

بنابراین می‌توان گفت که در مورد افترای رایانه‌ای قانون‌گذار ایران، به طور صریح واکنش نشان داده است، ولی این واکنش، مختص نشریات الکترونیکی است. شایان ذکر است که این تبصره قانون، از جامعیت کافی که شامل خبرگزاری‌ها، پایگاه‌های اطلاع‌رسانی، شبکه‌های اجتماعی و وبلاگ‌ها شود، برخوردار نیست.

۱-۱-۱-۱-۲-۱- افترای رایانه‌ای

حال سؤال این است که آیا رایانه و اینترنت می‌تواند وسیله اسناد تحقق این جرم قرار گیرد؟ به عبارت دیگر آیا عبارت "به هر وسیله دیگر" شامل رایانه هم می‌شود؟ مثلاً شخص از طریق گفتگوی مکتوب اینترنتی (چت)، فرستادن ایمیل یا با نقاشی و کاریکاتور طرف مقابل را به ارتکاب عملی که در قانون جرم است، متهم کند.

برخی بدون این که اشاره‌ای به رایانه و اینترنت داشته باشند، معتقدند که راه‌های مذکور در ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی اصولا به صورت نوشته یا گفتار است و لذا در تسری طرق ارتکاب جرم افترا به موارد دیگر مماثلت و مشابهت باید رعایت گردد (گلدوزیان، ۱۳۸۸، ص ۱۱۲). با این تفسیر، رایانه و اینترنت شامل ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی نمی‌باشد و تفسیر مضیق قوانین کیفری نیز چنین اقتضا می‌کند. اما در این باره نظریات مخالفی هم وجود دارد که در کتاب جرایم علیه اشخاص آمده است(آقایی نیا، ۱۳۸۷، ص ۵۹).

به نظر می رسد که ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی اطلاق دارد. ضمناً هدف قانون‌گذار از به کار بردن "به هر وسیله دیگر" عمدی بوده تا راه‌های اسناد افترا را محدود نکند. به عبارت دیگر، هدف مقنن پرداختن به اصل جرم افترا بوده است و نه این که نوع وسیله را بیان کند. چه تفاوتی می‌کند که شخص از طریق رایانه و انتشار در اینترنت عمل مجرمانه را به دیگری نسبت دهد و یا از طریق یک نوشته، که در اولی حتی آثارش مخرب‌تر از دومی است. بنابراین هر چند جهت رفع ابهامات، نص قانونی خاصی را در این مورد می طلبد، ولی در حال حاضر به نظر می‌رسد طبق ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی چنین افتراهایی جرم و قابل مجازاتند.

بنابراین، می‌توان گفت که در مورد افترای رایانه‌ای، قانون‌گذار ایران، صریحاً واکنش نشان داده است، ولی این واکنش، مختص نشریات الکترونیکی است.

در مورد افترای رایانه‌ای، ماده ۱۶ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ می‌گوید: «هر کس به وسیله سامانه‌های رایانه ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

همچنین در تبصره ماده مذکور آمده است: «چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.»

قابل ذکر است که اگر تغییر یا تحریف به صورت مستهجن باشد علاوه بر این که به فرد بزه‌دیده آسیب جدی می‌رسد، نوعی اشاعه فحشا نیز می‌باشد که جرم از زمره جرایم علیه عفت و اخلاق عمومی محسوب می‌شود و نمایش آن طبق بند اول ماده ۶۴۰ (۸۶۷) قانون مجازات اسلامی، عفت و اخلاق عمومی را جریحه‌دار می‌نماید. پس لازم است قانون‌گذار در این مورد شدت عمل بیشتری به خرج دهد.

نکته دیگری که در اینجا قابل توجه است بحث افترای عملی است که موضوع ماده ۶۹۹ (۹۲۳) قانون مجازات اسلامی به این شرح است: «هر کس عالماً عامداً به قصد متهم نمودن دیگری آلات و ادوات جرم یا اشیایی را که یافت شدن آن در تصرف یک نفر موجب اتهام او می‌گردد بدون اطلاع آن شخص در منزل یا محل کسب یا جیب یا اشیایی که متعلق به اوست بگذارد یا مخفی کند یا به نحوی متعلق به او قلمداد نماید و در اثر این عمل شخص مزبور تعقیب گردد، پس از صدور قرار منع تعقیب و یا اعلام برائت قطعی آن شخص، مرتکب به حبس از شش ماه تا سه سال و یا تا ۷۴ ضربه شلاق محکوم می‌شود.»

حال پرسش این است که آیا این جرم از طریق رایانه قابل تحقق است؟ به عبارتی دیگر، امکان تحقق جرم افترای عملی رایانه‌ای وجود دارد؟

فرض کنید شخصی با تغییر دادن داده‌ها و یا درج اطلاعات کذب در سایت شخص دیگر، مرتکب افترای عملی شود یا فردی با نفوذ[1] در سایت دیگر و تعبیه تصاویر موهن یا مستهجن برای دارنده سایت تبعاتی ایجاد کرده و مسئولیت کیفری متوجه او کند؛ در چنین شرایطی مجرم، مرتکب افترای عملی شده است، زیرا شخص متخلف سعی دارد با عمل خود، ارتکاب عمل ممنوع یا مجرمانه‌ای را به دارنده سایت منسوب نماید (اصلانی، ۱۳۸۹، ص ۱۰۳).

به عنوان نمونه در مطلبی که خبرآنلاین و تعداد دیگری از پایگاه‌های اینترنتی به قلم صادق زیباکلام منتشر کرده‌اند، اقدام شهرداری تهران در نصب بیلبوردهایی در جهت شناساندن ماهیت واقعی سران برخی کشورهای زیاده خواه غربی، اقدامی سیاسی و در راستای جلب آرای عمومی به سمت شهردار تهران برای ریاست جمهوری دوره بعد قلمداد شده است.

[1] penetrate

تصویر شماره ۲، صفحه خبر پایگاه خبری خبرآنلاین

پس از انتشار این نامه و واکنش های مختلف به آن، غیر واقعی بودن چنین ادعا و انتسابی از جانب زیباکلام محرز شد؛ بنابراین نامه سرگشاده وی را می‌توان مصداق افترا دانست.

تصویر شماره ۳، صفحه خبر خبرگزاری فارس

اگر چه بعد از چند روز، صادق زیباکلام طی نامه‌ای از شهردار تهران عذرخواهی کرد و خبر عذرخواهی وی در پایگاه‌های اینترنتی منتشر شد، اما به اندازه اصل خبر حاوی افترا، در شبکه‌های اجتماعی انتشار نیافت. از این روست که عذرخواهی وی، اعاده حیثیت از مفتری علیه نخواهد کرد.

۱-۱-۱-۱-۳- قذف

یکی دیگر از انواع جرایم، جرم قذف می‌باشد که قانون مجازات اسلامی بر اساس منابع فقهی در ماده ۲۴۵ در تعریف آن آورده است: «قذف نسبت دادن زنا یا لواط است به شخص دیگر، هر چند مرده باشد.»

واژه قذف در کتب لغت به معنی «افکندن، پرتاب کردن، دور انداختن و تهمت و افترا بستن» می‌باشد (عمید، ۱۳۸۹، ص ۱۵۷۲).

در مکتب اسلام از تعرض به حیثیت افراد، مانند تعرض به جان و مال او نهی شده است. از جمله تعرضات بر حیثیت، نسبت دادن زنا یا لواط به افراد پاک‌دامن و مؤمن است که در اصطلاح فقهی آن را «قذف»

می‌گویند. قذف از گناهان کبیره‌ای است که وعده عذاب دنیوی و اخروی به مرتکب آن داده شده[1] و روایات متعددی، بر حرمت آن دلالت دارند؛ از این رو اختلافی نیز در آن نیست.

ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی صراحتاً مواردی که موجب حد است را از شمول ماده خارج دانسته است. منظور از موارد موجب حد، مواردی است که جرم مورد انتساب، زنا یا لواط باشد. در چنین مواردی نسبت‌دهنده مرتکب جرم قذف شده و به موجب ماده ۲۵۰ قانون مجازات اسلامی به هشتاد ضربه تازیانه محکوم می‌شود. این مجازات صراحتاً در قرآن پیش‌بینی شده است[2].

قذف که به عنوان یکی از جرایم مشمول حد شناخته شده است یکی از مصادیق جرم افترا است و قاذف، کسی است که با دروغ به منظور هتک حرمت و حیثیت دیگری، منحصراً نسبت خلاف واقع زنا یا لواط را به او می‌دهد. به همین مناسبت می‌توان قذف را نوعی افترای خاص نامید. حتی در ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی، حکم افترای مشمول حد، استثنا شده است. منبع و ریشه اصلی این تفاوت در نظام کیفری اسلام، حکم قرآنی است از جمله: «وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَه شُهَدَاء فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَه وَلَا تَقْبَلُوا لَهُمْ شَهَادَه أَبَدًا وَأُولَئِکَ هُمُ الْفَاسِقُونَ»[3]«آنان که به زنان با عفت مؤمنه نسبت زنا دهند آن گاه چهار شاهد بر دعوی خود نیاورند آنان را به هشتاد تازیانه کیفر دهید و دیگر هرگز شهادت آنان را نپذیرید که مردمی فاسق هستند.»

در قذف لازم است که اتهام به لفظ صریح باشد؛ مانند «تو زنا کردی»، «تو لواط نمودی»، «تو زنا کاری»، «ای لواط کننده» و مانند این‌ها. همچنین لازم است که قذف‌کننده معنای الفاظ را بداند؛ پس اگر یک نفر یکی از این لفظ‌ها را بگوید در صورتی که معنای آن را نمی‌داند قاذف نیست، هر چند مخاطب، معنای آن را بداند.

---

[1]. آیه ۴ و ۲۳ سوره نور.

[2]. آیه ۳ سوره نور.

[3]. آیه ۴ سوره نور.

ولی بر عکس کسی که معنای لغت را می‌داند اگر به کسی که آن را نمی‌داند بگوید قاذف است و حد دارد (بای و پورقهرمانی، ۱۳۸۸، ص ۶۸).

لازم به ذکر است همان طور که در مورد افترا گفتیم، گاه معنی لغوی واژه مورد استفاده عبارت از نسبت دادن جرم (مثلاً ارتکاب زنا یا لواط) به دیگری است. لیکن در عرف مردم چنان واژه‌ای آن معنی را نرسانده و صرفاً برای دشنام دادن به کار می‌رود. در چنین مواردی، طبق تصریح برخی از فقیهان، گوینده محکوم به حد قذف نشده، بلکه به خاطر دشنام‌گویی و اذیت کردن دیگری تعزیر می‌شود (شهید اول، ۱۳۸۲، ص ۲۴۷).

در همین راستا، ماده ۲۴۸ قانون مجازات اسلامی مقرر داشته است که هر گاه قرینه‌ای در بین باشد که نشان دهد منظور کسی از این که به دیگری گفته است که او فرزند مشروع پدرش نمی‌باشد، قذف نبوده است، حد قذف علیه گوینده ثابت نمی‌شود (میرمحمد صادقی، ۱۳۸۷، ص ۷۸).

این مسأله نشانگر لزوم وجود عنصر معنوی یا سوء نیت در مرتکب جرم قذف می‌باشد، که در مواد دیگری از قانون مجازات اسلامی نیز به آن تصریح شده است. از جمله، ماده ۲۴۶ قانون مجازات اسلامی بر لزوم وجود «قصد نسبت دادن زنا» تصریح کرده و بر لزوم آگاهی نسبت‌دهنده به معنی لفظ مورد استفاده تأکید کرده است.

در همین زمینه ماده ۲۴۶ قانون مجازات اسلامی می‌گوید: «قذف باید روشن و بدون ابهام بوده و نسبت‌دهنده به معنای لفظ آگاه باشد، اگر چه شنونده معنای آن را نداند.»

نکته‌ای که در اینجا باید توجه داشت و می‌توان از آن امکان تحقق برخی صور قذف رایانه‌ای را استنباط کرد، کتبی یا شفاهی بودن قذف می‌باشد. به عبارت دیگر آیا قذف به صورت کتبی تحقق می‌یابد یا خیر.

آنچه بدواً به ذهن می‌رسد با توجه به کتب فقهی و ماده ۲۴۶ قانون مجازات اسلامی، شرط تحقق قذف، لفظ می‌باشد و قذف به صورت کتبی تحقق پیدا نمی‌کند؛ ولی این استنباط درست نیست، زیرا با توجه به تعریف قذف از نظر فقه و قانون، نسبت دادن زنا و لواط، ملاک است و نوع وسیله در آن دخالتی ندارد.

همچنین در تبصره ماده ۲۴۶ قانون مجازات اسلامی، صراحتاً بیان داشته که قذف، علاوه بر لفظ با نوشتن، هرچند به شیوه الکترونیکی محقق می‌شود.

۱-۱-۱-۱-۳-۱- قذف رایانه‌ای

حال با توجه به مسائل فوق، سؤال این است که آیا امکان تحقق قذف رایانه‌ای وجود دارد؟ به نظر می‌رسد که جواب مثبت باشد. مثل اینکه شخصی با دیگری در گفتگوی اینترنتی (چت) به طرف مقابل نسبت زنا یا لواط دهد؛ یا با ارسال ایمیل، صاحب ایمیل یا دیگری را به زنا و لواط متهم کند. همچنین است پخش فیلم برخط[۱] در اینترنت و ارسال عکس یا کاریکاتور که به صراحت بر اتهام زنا یا لواط دلالت کند. در این مثال‌ها چنانچه شرایط تحقق قذف وجود داشته باشد، قذف موجب حد، تحقق می‌یابد.

در جواب ممکن است گفته شود که این استدلال درست نیست. زیرا در قذف، لفظ مادی و واقعی شرط است نه لفظ مجازی؛ یعنی لفظی که با زدن یک دکمه می‌آید و با زدن دکمه‌ای از بین می‌رود و یا لفظی که از طریق امواج ظاهر می‌شود. در جواب باید گفت که این نظر مخدوش است؛ زیرا اولاً آنچه ملاک حرمت است، نسبت زنا یا لواط به دیگری با هر وسیله‌ای است و به عبارتی وسیله در تحقق این جرم دخالت ندارد، چنانکه ماده ۶۹۷ (۹۲۱) قانون مجازات اسلامی نیز مؤید آن است. ثانیاً وسیله (رایانه) مستقلاً از خود اراده ندارد، بلکه وجودش (کنترلش) بستگی به اراده انسان است و الفاظی هم که به صورت مجازی عرضه می‌شود از انسان صادر می‌شود نه از خود وسیله (رایانه).

[۱] online

با این اوصاف، اگر شخصی نسبت زنا و یا لواط را به قصد شوخی به ایمیل دیگری بفرستد، یا نابالغی هنگام گفتگوی اینترنتی (چت) نسبت زنا یا لواط به طرف مقابل بدهد، قذف محقق نمی‌شود.

در نمونه زیر یکی از شخصیت‌های فرهنگی در مورد قشر وسیعی از هنرمندان سینمای ایران از واژه «فاحشه» استفاده کرده که مصداق قذف است. با وجود عذرخواهی چندین‌باره و اصلاح سخنان خود، به دلیل ویژگی‌های ذاتی فضای مجازی[1] همچنان این مطلب در فضای مجازی در دسترس عموم است و به اعتبار و حیثیت بخش زیادی از هنرمندان لطمه می‌زند.

تصویر شماره ۴، صفحه خبر پایگاه خبری آفتاب

[1] در بخش دوم به تفصیل به ویژگی‌های فضای مجازی پرداخته شده است.

پایگاه‌های خبری بعضاً در این فضا به نحوی عمل می‌کنند که نسبت به اخبار جنجالی (فارغ از علم به صحت و سقم یا مجرمانه بودن یا نبودن محتوا) تمام توان خود را در جهت انتشار هر چه بیشتر مطلب به کار می‌گیرند ولی در مورد نامه‌های اعتذار، تکذیبیه‌ها و ... این همت مشاهده نمی‌شود.

به عنوان مثال چنانچه یک پایگاه خبری، مطلبی حاوی یک جرم رایانه‌ای مانند نشر اکاذیب، توهین، افترا و ... تنظیم کند و به زعم خود، آن خبر را دارای برد مناسب خبری و جریان‌ساز بداند، برای انتشار هر چه بهتر و بیشتر آن در فضای مجازی از هیچ تلاشی فروگذار نخواهند کرد. خبر مزبور را از طرق پیامک انبوه (که معمولاً به نمایندگان مجلس و اعضای شورای شهر، خبرنگاران، فعالان رسانه‌ای و فرهنگی، دانشجویان و نخبگان ارسال می‌شود.)، ایمیل انبوه، بازنشر در شبکه‌های اجتماعی مبتنی بر نت و نرم‌افزارهای تلفن همراه، خبرخوان‌ها و درخواست از سایر پایگاه‌های خبری و خبرگزاری‌ها مبنی بر نقل مطلب اشاعه خواهند داد؛ لیکن در صورت تکذیب خبر مورد بحث، نهایت همکاری آنان درج خبر تکذیبیه خواهد بود، آن هم نه با تنظیم مناسب خبر و انتشار یکسان آن با خبر اولیه.

برخی پایگاه‌های خبری به علت جریان‌سازی سیاسی و اجتماعی، برخی برای کسب بازدید بیشتر و جذب مخاطب و برخی برای دشمنی با یک شخص یا گروه خاص با هزینه و فایده کردن انتشار خبر حاوی محتوای مجرمانه، اقدام به درج این مطلب خواهند کرد، چرا که فایده دنیوی انتشار خبر کذب یا حاوی توهین و افترا و اثرگذاری آن به مراتب بیشتر از تکذیبیه احتمالی ثانویه است.

۱-۱-۱-۱-٤- نشر و اشاعه اکاذیب

انتشار و اشاعه‌ی با سوءنیت اخبار دروغ و وقایع خلاف واقع به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی را نشر اکاذیب گویند. به عبارت دیگر، مقصود از اشاعه اکاذیب آن است که مرتکب، مطالب و کارهایی را که می‌داند حقیقت ندارد، عالماً و عامداً علیه شخص حقیقی یا حقوقی یا مقامات رسمی شایع و اظهار کند.

در جرم نشر اکاذیب، لزوماً توهین یا افترایی نسبت به دیگری انجام نمی‌شود. برای مثال کسی که به قصد بدبین‌کردن مردم نسبت به دیگری یا برای تحریک کردن آنها به رأی ندادن به وی در انتخابات، او را دارای تابعیت مضاعف یا همسر دوم اعلام می‌کند و یا به قصد گسیل شدن مأموران مالیاتی به تجارتخانه وی و ایجاد مزاحمت، وی را برخوردار از درآمدهای نجومی قلمداد می‌نماید، یا به قصد معامله نکردن سایر تجار با وی او را ورشکسته معرفی می‌کند، در صورت صحت نداشتن این گونه شایعات، مرتکب جرم نشر اکاذیب خواهد شد، در حالی که این اعمال توهین یا افترا محسوب نمی‌شوند. همین طور، این جرم، با توجه به استعمال عبارت «به قصد اضرار به غیر» در صدر ماده، تصریح مذکور در ذیل ماده، علیه اشخاص حقوقی نیز قابل ارتکاب می‌باشد (میرمحمد صادقی، ۱۳۸۷،ص ۵۴).

عنصر مادی این جرم، اظهار و نشر اکاذیب یا نسبت دادن عمل خلاف حقیقت به شخص حقیقی یا حقوقی یا مقامات رسمی است که به یکی از راه‌های مذکور در ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی محقق می‌شود. در حقیقت دو جرم در این ماده بیان شده است، اظهار اکاذیب و نسبت دادن مطلب غیرواقعی به شخص یا اشخاص حقوقی یا مقامات رسمی.

اشاعه اکاذیب باید به وسیله نامه، شکوائیه، مراسله، عریضه، گزارش یا توزیع هر گونه اوراق چاپی یا خطی با امضا یا بدون امضا یا به عنوان نقل قول صریح یا ضمنی از شخص حقیقی یا حقوقی یا مقامات رسمی صورت گیرد (میرمحمد صادقی، ۱۳۸۷، ص ۴۹).

از مصادیق مذکور در این ماده می‌توان استنباط کرد که اظهارات شفاهی از شمول ماده خارج است و ظاهراً رویه قضایی نیز همین را تأیید می‌کند.

بنابراین با توجه به وحدت ملاک، به نظر می‌رسد تسری این نظریه به ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی با مشکلی مواجه نباشد، زیرا مکتوب بودن، منصرف از وسیله‌ای است که متن روی آن نوشته می‌شود

و در نتیجه نوشتن مطالب کذب روی دیوار معابر نیز از مصادیق اشاعه اکاذیب می‌باشد (آقایی نیا، ۱۳۸۷، ص ۵۴)

نکته‌ای که در بحث عنصر مادی باید خاطر نشان کرد این است که جرم اشاعه اکاذیب از جمله جرایم مطلق است و تحقق ضرر مادی یا معنوی، شرط تحقق این جرم نمی‌باشد (زراعت، ۱۳۹۲، ص ۸۱).

نشر اکاذیب با هتک حرمت و حیثیت تفاوت دارد، چرا که در نشر اکاذیب حتما مطالب کذب، انتشار می‌یابد و واقعیت ندارد، اما در هتک حیثیت هم واقعیت و اسرار خصوصی فرد فاش می‌شود و هم ممکن است با اشاعه کذب، حیثیت شخص خدشه‌دار گردد.

۱-۱-۱-۱-٤-۱- نشر اکاذیب رایانه‌ای

در قانون مجازات جرایم رایانه‌ای، نشر اکاذیب رایانه‌ای پیش بینی شده است. طبق ماده ۱۸ قانون مذکور «هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده به نحوی از انحاء، ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.»

با توجه به توضیحاتی که داده شد، آیا امکان تحقق چنین جرمی در فضای مجازی وجود دارد؟ همچنین آیا ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی قابل تطبیق با نشر اکاذیب رایانه‌ای است یا خیر.

در جواب باید گفت که هر چند قانون‌گذار وسایل ارتکاب جرم را برشمرده، اما احصای طرق ارتکاب جرم به معنی حصری بودن آنها نیست. بلکه با توجه به فلسفه تشریع مواد مذکور که حفظ حیثیت و شئون افراد است، به نظر می‌رسد این جرم با هر وسیله‌ای که بتوان اکاذیبی را اظهار و حیثیت افراد را جریحه‌دار

ساخت از قبیل اینترنت و ... قابل تحقق است (آقایی نیا، ۱۳۸۷، ص ۵۶). البته حتی اگر مقید به مصادیق ذکر شده در ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی باشیم، باز هم امکان تحقق آن از طریق رایانه وجود دارد. مثلاً در مصداق «مراسلات»، مقصود از مراسله هر نوع مکتوبی است که شخص برای دیگری از طریق تلفنگرام، تلگرام و یا حتی از طریق پست الکترونیکی می‌فرستد.

نظریه اراده حقوق قوه قضائیه نیز مؤید این مطلب است که «اگر به وسیله اینترنت یا مشابه به آن هم جرمی به کسی نسبت داده شود و نسبت‌دهنده نتواند صحت آن انتساب و اسناد را ثابت نماید، مورد شمول ماده (۶۹۷) ۹۲۱ قانون مجازات اسلامی خواهد بود (ایرانی ارباطی، ۱۳۸۸، ص ۱۱۲).

در نمونه زیر، بخش فارسی‌زبان خبرگزاری العربیه، خبری با این عنوان روی خروجی پایگاه خود قرار داده است: «سپاه پاسداران شهر اصفهان را به توپ بست!»

تصویر شماره ۵، صفحه خبر خبرگزاری العربیه فارسی

با بررسی واقعیت ماجرا متوجه می‌شویم که در تاریخ مذکور، تنها دو گلوله در حوالی پارکی در سپاهان‌شهر اصفهان شلیک شده که در این ماجرا هیچ خسارت مالی یا جانی نیز به کسی وارد نیامده است.

بنابراین خبر العربیه، به وضوح حاوی نشر و اشاعه اکاذیب است.

۱-۱-۱-۱-۵- هتک حرمت

هتک در کتب لغت به معنای پرده دریدن، پاره کردن پرده و مفتضح ساختن یا رسوا کردن کسی بیان شده است (عمید، ۱۳۸۹، ص ۱۴۲۳).

هتک حرمت عبارت است از یک فعلی که با هدف تنزل ارزش واقعی یک فرد در میان جامعه موجب لطمه به حیثیت و آبروی آن فرد می‌شود. حفظ حرمت، آبرو و حیثیت معنوی اشخاص یکی از قواعد اخلاقی، مذهبی و حقوقی در تمام کشورهای جهان است (میر محمدصادقی، ۱۳۸۷، ص ۶۸).

در نظام حقوقی، هتک حرمت ممکن است دوگونه باشد. گاهی هتک حرمت به صورت گذرا و زودگذر است که آن را در اصطلاح "هتک حرمت گذرا" می‌نامند، ولی هرگاه هتک حرمت و اظهارات توهین‌آمیز به صورت غیرموقت و تقریباً دائم باشد، آن را هتک حرمت "پایدار" می‌نامند.

در این جرم، ماده ۷۰۰ (۹۲۴) قانون مجازات اسلامی را می‌توان به عنوان عنصر قانونی قلمداد کرد که مقرر می‌دارد: « هر کس با نظم یا نثر یا به صورت کتبی یا شفاهی کسی را هجو کند و یا هجویه را منتشر نماید به حبس از یک تا شش ماه محکوم می‌شود.»

۱-۱-۱-۱-۵-۱- هتک حرمت رایانه‌ای

ابتدا بایستی مشخص نمود که هتک حرمت‌های صورت گرفته از طریق اینترنت و شبکه‌های اجتماعی از چه نوع بوده تا برپایه این بحث به بررسی ارکان مسئولیت ناشی از هتک حرمت از طریق اینترنت پرداخت (صادقی، ۱۳۸۸، ص ۱۵۹).

در خصوص انتشار گفتارهای توهین‌آمیز از طریق شبکه‌های اجتماعی و اینترنت، برخی معتقدند که مانند برنامه‌های رادیو و تلویزیون بوده و بر همین اساس بایستی آنها را در دسته هتک حرمت‌های گذرا تلقی نمود، اما برخی دیگر نظر مخالف دارند (انصاری، ۱۳۸۲، ص ۹۵).

یک پیامی که در صفحه یک سایت اینترنتی قرار دارد، قطعاً به صورت گذرا نبوده و با توجه به گستردگی خدمات دسترسی به اینترنت، قابل رؤیت برای میلیون‌ها نفر در سراسر جهان خواهد بود. از این رو چه بسا اثرات سوء ناشی از هتک حرمت در فضای مجازی بیش از نشریات و روزنامه‌ها یا حتی برنامه‌های رادیو و تلویزیون باشد.

در یکی از نمونه‌های مشهور هتک حرمت رایانه‌ای، جریانی در شبکه‌های اجتماعی و به ویژه فیسبوک به راه افتاد و عده‌ای با انتشار مطالب سخیف و زننده نسبت به ساحت مقدس امام هادی علیه السلام، هتاکی کردند. این کار بر اساس قوانین مجازات اسلامی قدیم و جدید، جرم بوده و مجازات سنگینی دارد.[1]

۱-۱-۱-۱-٦- افشای سر

سر «عبارت است از امری که نوعاً داعی بر اخفای آن وجود داشته باشد.»

فاش ساختن سر به معنای اعلام و اظهار آن به دیگران است که ممکن است این اعلام از طریق گفتگو و محاوره عادی، مکاتبه، انتشار از طریق مطبوعات، رسانه‌ها و رایانه‌ها صورت گیرد و طبیعتاً در حالات اخیر (انتشار از طریق مطبوعات، رسانه‌ها و اینترنت) برای ارتکاب جرم می‌توان کیفیات مشدده در نظر گرفت.

افشای اسرار دیگران و آشکار ساختن امور نهان افراد از اعمالی است که اخلاقاً مذموم بوده و در شرع نیز – چنان‌که از خلال روایات به دست می‌آید- گناهی بزرگ تلقی شده است. از امیرالمؤمنین علیه السلام نقل شده که فرمودند: «کسی که پرده از روی اسرار برادر مسلمانش بردارد، خداوند عیوب اسرار او را بر ملا می‌کند.» (شرح غررالحکم و دررالکلم، ۱۳۴۲، ص۳۷۱)

افشای اسرار دیگران آثار زیان‌بار اجتماعی به دنبال داشته و موجب بدبینی و آسیب‌های مادی و معنوی می‌شود. در این قسمت ابتدا به مطالعه این موضوع می‌پردازیم که آیا افشای سر در قوانین موجود، جرم

[1] به سبب جلوگیری از اشاعه فحشا، از آوردن تصاویر و مطالب مربوط پرهیز شده است.

انگاشته شده است یا نه و در صورت جرم‌انگاری آیا امکان تحقق این جرم از طریق رایانه متصور است یا خیر.

ماده ۶۴۸ (۸۷۲) قانون مجازات اسلامی مقرر نموده است: «اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هرگاه در غیر از موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شوند.» ماده مزبور از ماده ۲۲۰ قانون مجازات عمومی[1] و نیز از ماده ۳۷۸ قانون مجازات فرانسه اقتباس شده است (بای و پورقهرمانی، ۱۳۸۸، ص ۵۲).

چنان‌که ملاحظه می‌شود، مقنن، تنها افشای اسرار دیگران از ناحیه افرادی را جرم تلقی کرده است که به مناسبت شغل یا حرفه خود محرم اسرار می‌گردند، اما افشای اسرار از سوی دیگر افراد مشمول حکم ماده نمی‌گردد. وجه این تفکیک بنابر آن‌چه گفته شده آن است که تخلف از این تکلیف اخلاقی و شرعی (حفظ سر) تا حدودی که مربوط به روابط و منافع بین فردی مردم باشد، جنبه جزایی پیدا نمی‌کند، زیرا اگر کسی به یکی از نزدیکان خود اعتماد کند و سری را به او بسپارد، ولی آن شخص، سر مذکور را فاش سازد، ضرر و پشیمانی مستقیم آن، عاید صاحب سر خواهد گردید؛ ولی اگر سری به اشخاصی مانند پزشک و وکیل دادگستری که به اعتبار شغل و حرفه و وضع خاص اجتماعی خود طرف اطمینان و اعتماد جامعه هستند سپرده شود و آنان سر را فاش کنند، ضرر عمده این خیانت در امانت عاید جامعه شده و موجب بی‌اعتمادی گروهی از مردم به این افراد و در نتیجه عدم مراجعه به آن‌ها خواهد شد.

[1]. ماده ۲۲۰ مقرر می‌داشت: «اطبا و جراحان و قابله‌ها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هر گاه در غیر از مواردی که بر حسب قوانین ملزم می‌باشد، اسرار مردم را افشا کنند از یک ماه تا یک سال حبس تأدیبی و از ۲۰۵ الی دو هزار ریال غرامت محکوم خواهند شد.»

جرم افشای سر از جرایم عمدی است؛ به این معنا که افشا کننده سر در صورتی بزه‌کار شناخته می‌شود که با علم به محرمانه بودن سر، اقدام به افشای آن نموده باشد. همچنین اگر شخصی بر اثر سهل‌انگاری و بی‌دقتی موجب فاش شدن سر دیگری که نزد اوست گردد، مشمول ماده ۶۴۸ (۸۷۲) قانون مجازات اسلامی نخواهد بود.

۱-۱-۱-۱-۶-۱- افشای سر رایانه‌ای

ماده ۱۷ قانون جرایم رایانه‌ای که به قانون مجازات اسلامی مصوب ۱۳۹۲ الحاق گردیده است، بیان می‌دارد: «هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

پنهان ماندن هویت نویسندگان و منتشرکنندگان مطالب در فضای مجازی، انگیزه زیادی به مجرمین برای افشای اسرار می‌دهد. اگرچه راه‌هایی برای یافتن هویت عاملان فعالیت‌های مختلف در فضای مجازی وجود دارد، اما همچنان برای افرادی که بخواهند اسراری را افشا کنند، تا حدود زیادی امن محسوب می‌شود.

با مطالعات انجام شده، نمونه‌ای از افشای سر رایانه‌ای در ایران یافت نشد، اما در یکی از نمونه‌های مشهور، شخصی به نام «جولین آسانژ[1]» که یک نظامی سابق ارتش آمریکاست، با سرقت اطلاعات سری و فرار به کشور دیگر، اقدام به انتشار این اسرار نموده است.

سند زیر، افشای «نصب کابل‌های مخفی در سفارتخانه‌های آمریکا» است که قطعاً از نظر سیستم قضایی آن کشور جرم افشای سر محسوب می‌شود.

[1] Julian Paul Assange

تصویر شماره ۶، سند افشا شده توسط ویکی لیکس

ترجمه سند فوق به این شرح است: «ویکی لیکس در یکشنبه ۲۸ نوامبر ۲۰۱۰ منتشر کرد، ۲۵۱,۲۸۷ تلگرام سفارتخانه‌های آمریکا نشت اطلاعاتی پیدا کرد. بزرگترین اسناد محرمانه‌ای که در حوزه عمومی منتشر شده است. این اسناد به مردم نشانه‌هایی بی سابقه از فعالیت‌های دولت آمریکا در کشورهای دیگر را ارائه می‌کند. تلگرام‌هایی که از حیث زمانی سال‌های ۱۹۶۶ تا فوریه ۲۰۱۰ را دربرمی‌گیرد و مشتمل بر مکالمات و مکاتبات بین ۲۷۴ سفارتخانه در کشورهای سراسر دنیا با دپارتمان دولتی در واشنگتن آمریکاست. ۱۵۶۵۲ تلگرام در دسته‌بندی محرمانه قرار می‌گیرد. تلگرام‌ها نمایانگر جاسوسی‌های گسترده آمریکا و فساد وسیع و جرایم علیه حقوق بشر می‌باشد.

این اسناد تفاوت آمریکا بین آنچه نشان می‌دهد با آن چیزی که در پنهان عمل می‌کند را به وضوح بیان می‌کند. کودکان آمریکایی که به مدرسه می‌روند تصورشان این است که جرج واشنگتن دروغ نمی‌گفت پس جانشین او هم نباید دروغ بگوید.»

۱-۱-۱-۱-۷- پورنوگرافی

پورنوگرافی[۱] از کلمات یونانی Porno و graphy اخذ شده و در لغت به معنای هرزه‌نگاری درج محتوای مستهجن است.

در فرهنگ آکسفورد، پورنوگرافی به این صورت تعریف شده است: «موارد و موضوعات شامل توصیف صریح یا نمایش ارگان‌های جنسی یا فعالیت به منظور تحریک مشابه، غیر از احساسات زیباشناختی یا عواطف.»

در ماده ۷۴۲ (۹۶۳) و ۷۴۳ (۹۶۴) قانون مجازات اسلامی که ماده ۱۴ و ۱۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است، به همراه تبصره‌های این مواد، جرایم علیه عفت و اخلاق عمومی به تفصیل بیان شده است.

ماده ۷۴۲ (۹۶۳) قانون مجازات اسلامی مقرر می‌دارد: «هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

تبصره۱ـ «ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازاتهای فوق می‌شود. محتویات و آثار مبتذل به آثاری اطلاق می‌گردد که دارای صحنه و صور قبیحه باشد.

تبصره۲ـ هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون ریال تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.

[۱] pornography

تبصره۳ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفه‌ی خود قرار داده باشد یا به طور سازمان‌یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره۴ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.»

ماده ۷۴۳ (۹۶۴) قانون مجازات اسلامی مقرر می‌دارد: «هرکس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن، آن‌ها را تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آن‌ها را تسهیل نموده یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد. ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو میلیون ریال تا پنج میلیون ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم می‌شود.»

تبصره ـ «مفاد این ماده و ماده ۷۴۲ (۹۶۳) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.»

۱-۱-۱-۱-۷-۱- پورنوگرافی رایانه‌ای

هرزه‌نگاری رایانه‌ای، در واقع تولید، انتشار، خرید و فروش و یا هرگونه فعالیت رایانه‌ای مرتبط با محتوای جنسی است. از همین رو هرزه‌نگاری، جرمی مرتبط با محتواست و نمی‌توان آن را جرم جنسی تلقی کرد،

چراکه عملاً جرم جنسی در فضای مجازی قابلیت ارتکاب ندارد؛ اما در فضای مجازی انتشار محتوای پورنو و در نتیجه آن تحریک و تشویق افراد به انجام چنین جرایمی در فضای حقیقی به سادگی اتفاق می‌افتد.

محتوای پورنو می‌تواند از طریق سایت‌های هرزه‌نگار، از طریق دریافت پست‌های الکترونیک و یا در شبکه-های اجتماعی در معرض دید افراد قرار گیرد و معمولاً اغلب قربانیان چنین مسائلی، جوانان و نوجوانان هستند. همچنین پایگاه‌هایی برای وصل کردن افراد به هم برای ارتباط جنسی[1] در فضای مجازی وجود دارد. در ماده ۲۴۲ قانون مجازانت اسلامی آمده است: « قوادی عبارت از به هم‌رساندن دو یا چند نفر برای زنا یا لواط است.» این جرم و مجازات مترتب بر آن در مواد ۲۴۲ تا ۲۴۴ قانون مجازات اسلامی تبیین شده است.

۱-۱-۲- انواع جرایم سایبری

رایانه به واسطه از میان برداشتن محدودیت مکان فیزیکی و ویژگی‌های فرامکانی بودن، ارائه تعریف مشخص و مختار از جرم رایانه‌ای را با دشواری مواجه می‌کند؛ اما در یک تعریف کلی می‌توان گفت: «جرم رایانه‌ای توصیف فعالیت‌های تبهکارانه‌ای است که در آن‌ها رایانه‌ها و شبکه‌های ارتباطی، بخش لازمی برای جرم و جنایت است. در این جرایم، حضور ابزار فناوری اطلاعات به عنوان عامل اصلی برای ارتکاب جرم، کاملاً ملموس است.» (رجب‌پور کاشف، ۱۳۹۰، ص ۱۹)

در یک دسته‌بندی برای جرایم علیه حیثیت معنوی اشخاص در فضای سایبر می‌توان به موارد زیر اشاره کرد:

الف) جرایمی که مستقیماً یک دستگاه رایانه یا سیستم‌های آن را هدف قرار می‌دهند، مانند نفوذ و رمزشکنی.

ب) جرایمی که در آن‌ها از رایانه به عنوان یک رسانه استفاده می‌شود، مانند قمار از طریق اینترنت.

---

۱ اینگونه سایت‌ها date و یا match نامیده می‌شوند.

ج) جرایمی که رایانه صرفاً محل حادث شدن جرم بوده است، مانند نمایش یک آگهی غیرمجاز به منظور جذب مشتری به محل فروش (شیرزاد، ۱۳۸۸، ص ۱۱۴).

فضای سایبر هنوز در مراحل اولیه است. طبیعت این جرایم و سوءاستفاده‌های انجام شده در این دنیای جدید، با جرایم واقع شده در دنیای حقیقی به کلی متفاوت است. امنیت ناکافی تکنولوژی، همراه با طبیعت مجازی آن، فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران‌کننده‌ترین جنبه‌ی فضای سایبر، انتشار سریع اطلاعات در آن می‌باشد. مثلاً در لحظه‌ی کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود. در فضای سایبر برای جستجو و پیدا کردن این جرایم، کار، پیچیده‌تر می‌شود. در دنیای واقعی دزدی از بانک کاملاً مشخص است؛ چرا که بعد از سرقت در خزانه بانک، پولی موجود نیست، ولی در رایانه‌ها و پایگاه‌های داده‌ی اطلاعاتی، یک خزانه می‌تواند بدون هیچ نشانه‌ای خالی شود.

برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان طور که دقیقاً بوده باقی بگذارد. در فضای سایبر کپی دقیقاً مشابه نسخه اصل است. با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی را مثل پاک کردن اثر انگشت از بین ببرد (برومند باستانی، ۱۳۸۳، ص ۴۲).

ایجاد صفحه در برخی شبکه‌های اجتماعی به نام دیگران با هدف انتقام‌گیری و ریختن آبروی افراد، گذاشتن نظرات[۱] موهن در پایگاه‌های اینترنتی مختلف با هدف هتاکی به اشخاص، انتشار اسرار شخصی و خانوادگی دیگران با انگیزه‌هایی نظیر انتقام و هتک حیثیت افراد، انتشار یا تحریف عکس‌های خصوصی دیگران، نشر اکاذیب و افترا در اینترنت با هدف تشویش اذهان عمومی و بدبین کردن افراد به یکدیگر، ربودن داده‌های رایانه‌ای متعلق به دیگران و انتشار آن در محیط اینترنت و نقض حریم خصوصی افراد، همچون نفوذ

[۱] comment

به پست الکترونیک و سیستم رایانه‌ای افراد و سپس در دسترس قرار دادن آن برای دیگران و... تنها گوشه‌ای از اقدامات مجرمانه‌ای است که برخی افراد با انگیزه‌هایی مانند تفریح، انتقام، فرونشاندن عصبانیت، جلب توجه و باز نمودن عقده‌های روحی و روانی در حوزه فضای مجازی مرتکب می‌شوند که متأسفانه آسیب‌های جبران ناپذیری در پی دارد. هر چند قانون‌گذار در قوانین مختلف و از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ عناوین مجرمانه را احصا نموده و مجازات‌هایی را برای آن مقرر داشته است، اما اطلاع‌رسانی هر چه بیشتر و دقیق‌تر می‌تواند به پیشگیری از وقوع چنین جرایمی کمک کند.

تنوع انواع جرایم ارتکابی در فضای سایبر شامل جرایم نسل اول رایانه‌ای و جرایم بسیار جدید و بی‌سابقه می‌باشد که به شرح ذیل قابل تبیین است.

۱-۱-۲-۱- جرایم سنتی در محیط دیجیتال (جرایم نسل اول)

الف) جاسوسی رایانه‌ای: جاسوسی رایانه‌ای مانند جاسوسی در فضای حقیقی ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشا و انتقال و استفاده از اسرار است. فرد قربانی جرم با فاش شدن این اسرار، ضرر سیاسی، نظامی، مالی و تجاری می‌کند. گاهی در سطوح بالا ممکن است این جرم، امنیت ملی را با مخاطره مواجه کند.

ب) سابوتاژ[۱] رایانه‌ای: این جرم با جرم تخریب مشابهت بسیاری دارد. هدف مجرم، اخلال در نظام سیاسی و اقتصادی یک کشور و بالطبع اخلال در امر حکومت است. در واقع اصلاح، موقوف سازی، پاک کردن غیرمجاز داده‌ها یا عملیات رایانه به منظور مختل ساختن عملکرد عادی سیستم را سابوتاژ رایانه‌ای گویند.

[۱] sabotage

ج) جعل رایانه‌ای: واردکردن، تغییر، محو یا موقوف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای با اهداف سیاسی و اقتصادی، جعل رایانه‌ای قلمداد می‌شود. در جعل رایانه‌ای عمل ارتکابی بر داده‌ها اثر می-گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

د) افترا و نشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین وگسترده‌ترین سرویس شبکه‌های رایانه‌ای و بین‌المللی است، هرکاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی در آن تقلب کرد. این قابلیت پست الکترونیک می‌تواند ابزاری کارامد برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا و به عبارت بهتر جرایم علیه حیثیت معنوی اشخاص در فضای سایبر باشد. کنترل اطلاعات تهیه‌کننده و ارسال کننده با صعوبت زیادی همراه خواهد بود و در عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی وگسترده امنیتی مشکل بوده و تنها برای بخش کوچکی از داده‌ها میسر می‌باشد.

ه) تطهیر نامشروع پول: به‌دست آوردن پول از طریق غیر قانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم سنتی بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد. نحوه ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست-الکترونیک یا اینترنت بدون هیچ‌گونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را می‌نمایند و در تقاضای خود نحوه ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف مقابل، نوع و نحوه تنظیمات لازم را اعلام می‌دارند و اصولاً در زمان استرداد پول، یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب و با هدف خود هماهنگ می‌نمایند.

۱-۱-۲-۲- جرایم ناظر به کپی رایت برنامه‌ها

هرگونه تکثیر، ارسال، انتقال، پخش گسترده، توزیع، فروش و استفاده غیر مجاز از برنامه‌های رایانه‌ای را سرقت نرم‌افزار گویند.

۱-۱-۲-۳- تروریسم سایبر

والتر لاکور[۱] یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌الملل اشاره می‌کند که یک مقام رسمی سیا ادعا کرده است که می‌تواند «با یک میلیارد دلار و ۲۰ هکر ماهر، ایالات متحده آمریکا را فلج کند.» لاکور یادآوری می‌کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی، گروگان‌گیری یا بعضاً حمله ناگهانی به امکانات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیله حمله الکترونیکی به شبکه‌های رایانه‌ای وارد آید می‌تواند «بسیار غم‌انگیزتر باشد و اثرات آن تا مدت‌ها باقی بماند.»

لاکور معتقد است که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده‌تر از جنگ‌های بیولوژیک یا شیمیایی باشد.

از ویژگی‌های تروریسم سایبری، ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی وتبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از مشخصه‌های این نوع ارتباط، عدم توانایی پلیس در کنترل و شنود این ارتباطات می‌باشد. درسال ۱۹۹۱ حین جنگ اول خلیج فارس که توسط ائتلافی از چند کشور به رهبری ایالات متحده آمریکا علیه عراق درگرفت، یک جوان ۱۸ ساله فلسطینی، متهم به نفوذ به رایانه‌های پنتاگون شد. این مرد جوان، ظاهراً به اطلاعات سری مربوط به موشک پاتریوت[۲] دسترسی پیدا کرده بود که یک سلاح کلیدی آمریکا برای دفاع در مقابل حمله موشک‌های اسکاد عراق محسوب می‌شد. در نفوذ دیگری در همان جنگ، چندین جوان هلندی به رایانه‌های نظامی زمینی، هوایی و دریایی ایالات متحده آمریکا در ۳۴ سایت مختلف نفوذ کردند. نفوذکنندگان در یکی از حملات خود به داده‌های بسیار حساسی درباره پرسنل نظامی، نوع و میزان تجهیزات نظامی فرستاده شده به خلیج فارس، اهداف موشک‌ها و توسعه سیستم‌های تسلیحاتی دست یافتند. در واقع این نوجوانان هکرهایی بودند که تنها به خواندن این فایل‌ها اکتفا نکردند،

[۱] Walter Laqueur
[۲] patriot

بلکه اطلاعات مربوط به تحرکات ارتش و توانایی موشک‌ها را سرقت کردند و در اختیار عراقی‌ها قرار دادند. (جینا آنجلیز، ۱۹۹۹، ص ۱۰۵)

۱-۱-۳- انواع مجرمین سایبر

مطالعات عینی پرونده‌های جرایم سایبری نشان می‌دهد ایجاد شخصیت مجازی با ذهنیت عدم شناسایی و البته سهولت و گستردگی ارتکاب برخی بزه‌ها در فضای مجازی، بستر مناسبی برای بروز خلاءهای شخصیتی و روانی فراهم می‌سازد. همین امر سبب می‌شود جرایم ارتکابی در حوزه فضای مجازی از پیچیدگی خاصی برخوردار باشد که عدم توجه و رسیدگی کارشناسانه به آن، آسیب‌ها را مضاعف خواهد کرد. واکاوی شخصیت این گروه از بزهکاران نشان می‌دهد که آنان به نوعی فاقد قدرت انتزاعی بوده و قادر به تصور و تجسم عاقبت رفتار خود نمی‌باشند تا با مدد آن، خودکنترلی در جلوگیری از ارتکاب جرم در فضای مجازی داشته باشند. اینگونه افراد به نوعی تحت تأثیر حال می‌باشند و رفتارهای خود را بدون هرگونه محاسبه و اندیشه عمیق انجام می‌دهند و زمانی که به چنگ قانون می‌افتند تازه از آثار جبران ناپذیر رفتار مجرمانه خود آگاه می‌شوند.

به عنوان مثال در پرونده‌ای، بزهکار سایبری با ایجاد صفحه‌ای جعلی در یکی از شبکه‌های اجتماعی به نام یکی از دوستان خود و ارسال نامه‌های الکترونیکی رکیک در آن و ثبت تهمت‌های ناروا علیه حیثیت معنوی او مرتکب جرم می‌شود. یا در پرونده‌های متعدد دیگر، شوهر یا زن مبادرت به ایجاد صفحه‌ای جعلی در پایگاه‌های مختلف اینترنتی به نام فرد مقابل خود نموده و با هدف ریختن آبروی فرد مورد نظر تمام عکس‌های خصوصی وی را در اینترنت منتشر می‌کند. در موارد بسیاری، افراد مبادرت به انتشار مطالب کذب و بی ریشه علیه افراد مختلف در سایت‌های اینترنتی می‌نمایند و با این رفتار مجرمانه به دنبال انتقام یا تحت فشار قرار دادن و تهدید دیگران هستند.

مجرمین سایبری عمدتاً به دنبال اطلاعات افراد یا راه‌های نفوذ به سیستم‌ها هستند که با یک تقسیم‌بندی کلی می توانیم این مجرمین را به گروه‌های ذیل تقسیم کنیم:

۱-۱-۳-۱- هکر[۱]

در دهه‌ی ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه نویسی بسیار ماهر و باهوش باشد. بعدها در دهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به صورت ناشناس تبحر داشته باشد. این درست است که هکرهای کنجکاو می‌توانند سهواً باعث زیان‌های قابل توجهی شوند، اما جستجو برای یافتن اطلاعات وآموزش، نه انتقام‌گیری یا صدمه زدن به دیگران، عاملی است که باعث می‌شود اکثر هکرها سرگرمی خود را به نحوی بی‌رحمانه دنبال کنند.

۱-۱-۳-۲- کرکر[۲]

کرکرها به سیستم‌ها رخنه می‌کنند تا با انتشار انواع بحران‌سازهای رایانه‌ای اقدام به خرابکاری کنند یا فایل‌ها را پاک کنند یا بعضی انواع دیگر ویرانی را به بارآورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.

هکرها در یک مورد مهم با کرکرها تفاوت دارند. کارهایی که آنها انجام می‌دهند معمولاً از روی بدخواهی نیست. انگیزه بیشتر هکرها برای این کار، تمایل شدید به یادگیری نحوه کار سیستم رایانه، یافتن راهی برای ورود مخفیانه به آن‌ها و پیداکردن سوراخ‌های امنیتی این سیستم‌هاست. هیجان خواندن اطلاعاتی که می‌دانند اجازه دیدن آنها را ندارند یا انجام کاری که می‌دانند قانونی نیست به لذت دست زدن به چنین تجاربی توسط هکرها به عنوان سرگرمی می‌افزاید.

---

[۱] hacker
[۲] cracker

بحران‌سازهای رایانه‌ای از جمله برنامه‌هایی هستند که به تخریب یا آلوده کردن سیستم هدف اقدام می‌کنند و عمدتاً بسیار زیانبار هستند. به چند نمونه از این بحران سازها اشاره می‌کنیم:

الف) ویروس[1]: ویروس‌ها یا برنامه‌های خودهمانندساز، برنامه‌هایی هستندکه با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند و معمولاً از طریق یک لوح فشرده یا حافظه‌های همراه و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند. بعضی ویروس‌ها ممکن است قادر به حمله به فایل‌های سیستم و ذوب کردن مادربورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت و ازکارانداختن رایانه باشند.

ب) کرم[2]: کرم‌ها می‌توانند به یک سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه، برای مثال از طریق یک لوح فشرده، گسترش پیدا کنند. کرم‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آن‌که رایانه کند شود یا از کار بیفتد.

ج) بمب‌های منطقی: آن‌ها تعمداً زیانبار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند. آن‌ها طوری طراحی شده‌اند که طی یک دوره زمانی در رایانه غیرفعال باقی می‌مانند و سپس با سررسیدن تاریخی که برنامه آن‌ها مشخص شده است منفجر می‌شوند. اهداف این بمب‌ها متفاوت است (حسن بیگی، ۱۳۸۴، ص ۴۳).

[1] virus
[2] worm

۱-۱-۳-۳- فریکر تلفن[۱]

شکل دیگر از جرایم رایانه‌ای را "فریکرهای تلفن" مرتکب می‌شوند. فریکرها به جای دسترسی به سیستم‌های رایانه‌ای، ازطریق خطوط تلفن در دنیای سایبر گشت می‌زنند. فریکرها از میان اولین هکرها در دهه ۱۹۷۰ پدید آمدند. یکی از حوادثی که توسط فریکرها به وجود آمده بود، در سال ۱۹۷۷ مربوط به اداره پلیس شهر نیویورک می‌شد. فریکرها به سیستم تلفن این اداره نفوذ کرده بودند و متن ضبط شده‌ای را که به تماس‌گیرندگان خوش‌آمد می‌گفت تغییر داده بودند. در متن ضبط شده جدید گفته می‌شد که افسران پلیس مشغول خوردن نان شیرینی و نوشیدن قهوه هستند و فرصت جواب دادن به تلفن‌ها را ندارند. این پیام به تماس‌گیرندگان توجه می‌داد که در موارد اورژانس با شماره ۱۱۹ تماس بگیرند (حسن بیگی، ۱۳۸۴، ص ۶۲).

۱-۱-۳-٤- اسنیفر[۲]

اسنیفرها، دسته‌ی دیگری از مجرمین فضای سایبر هستند که کارشان شنود محتوای رد و بدل شده میان دو یا چند نفر یا سازمان در فضای مجازی است. فرض کنید فرد الف پیامی را از طریق پست الکترونیک یا چت برای فرد ب می‌فرستد. در این صورت اگر فرد ثالثی این پیام را در هنگام ارسال شنود کند، قطعاً عمل مجرمانه‌ای انجام داده است.

سال هاست که برای مقابله با این پدیده از رمزگذاری[۳] داده‌ها استفاده می‌شود، اما با پیشرفت دانش رمزنگاری، اسنیفرها هم پیشرفت کرده‌اند. آن ها می‌توانند با شنود غیرمجاز پیام مبادله شده، آن را رمزشکنی کرده و از محتوای آن مطلع شوند.

---

[۱] Phone freaker
[۲] sniffer
[۳] encoding

حساسیت و میزان خطر حضور اسنیفرها در فضای مجازی از آن روست که معمولاً پس از انجام جرم، دو طرف پیام (یعنی فرد الف و ب) از وقوع چنین جرمی مطلع نمی‌شوند و به همین علت پیگیری خاصی در مورد آن صورت نمی‌گیرد. فقط گاهی اوقات که شنود اطلاعات در سطح گسترده انجام شود و یا عملیات غیرمجاز شنود علیه افراد خاص و یا اطلاعات حساس انجام شود، سیستم‌های امنیتی و پلیس‌های سایبری کشورها، عامل شنود را کشف کرده و قانوناً علیه شنودکننده اقدام می‌کنند.

تجربه نشان داده که در اغلب مواقع، اسنیفرها تا مدت‌ها فقط اطلاعات به دست‌آورده‌ی خود را جمع‌آوری می‌کنند تا در زمان مورد نیاز مورد بهره‌برداری قرار دهند. این یکی دیگر از دلایلی است که این دسته از مجرمین دیر شناسایی می‌شوند.

۱-۱-۳-۵- فیشرها[۱]

خلاف اسنیفرها که اطلاعات را مدت‌ها جمع‌آوری می‌کنند تا در زمان نیاز از آن استفاده کنند، فیشرها در فضای مجازی، معمولاً به دنبال سرقت اطلاعات و عملیات سریع هستند. به عنوان مثال فرض کنید شخصی می‌خواهد با استفاده از درگاه اینترنتی بانک، یک کالا بخرد. در این صورت فرد مجرم (فیشر) می‌تواند یک صفحه‌ی تقلبی[۲] با گرافیک و ظاهری شبیه درگاه بانک به کاربر نمایش دهد. کاربر که نمی‌داند این همان صفحه‌ی واقعی بانک نیست، شماره کارت بانکی خود و رمز آن را در صفحه‌ی جعلی وارد می‌کند تا مبلغ کالای مورد نظرش را اینترنتی پرداخت کرده باشد. در این لحظه فیشر که به اطلاعات بانکی قربانی دست یافته، سریعاً وارد صفحه‌ی واقعی بانک شده و کل موجودی حساب قربانی را به حساب دیگری که پیش از این با اطلاعات جعلی در یک بانک گشوده است، منتقل می‌کند. در همین حین برای آن که قربانی بویی نبرد این پیغام یا چیزی شبیه این را به او نمایش می‌دهد: «در حال حاضر درگاه بانک به دلیل ترافیک

[۱] این لغت به معنای ماهی‌گیر است و در اصطلاح به کسی گفته می‌شود که همانند ماهیگیران با سرعت وارد عمل شده و داده‌ی مورد نیاز خود را می‌رباید.

[۲] fake

تراکنش ها قادر به انجام درخواست شما نیست. لطفاً ساعتی دیگر دوباره امتحان کنید.» پس از این کار، مجرم فوراً به یکی از شعب بانک مراجعه کرده و تمام حساب را خالی می‌کند و متواری می‌شود.

در فیشینگ، قربانی اگرچه شاید همان روز وقوع جرم متوجه می‌شود و رسماً شکایت می‌کند، اما از آن‌جا که فیشر خیلی سریع، عمل مجرمانه را انجام داده و ردی از خود به جا نگذاشته است، یافتن مجرم بسیار دشوار خواهد بود.

علی‌رغم نکات پیش‌گفته درباره تقسیم‌بندی جرایم سایبری، در حقوق موضوعه جرایم ارتکابی از طریق رایانه به پنج دسته تقسیم شده است که در ادامه به شرح تفصیلی آن پرداخته خواهد شد (بای و پورقهرمانی، ۱۳۸۸، ص ۵۸).

الف) جرایم علیه اشخاص

ب) جرایم علیه اموال و مالکیت

ج) جرایم علیه اخلاق و عفت عمومی و تکالیف خانوادگی

د) جرایم علیه آسایش و امنیت عمومی

ه) جرایم علیه مذهب

۱-۲- فصل دوم: تمایزات جرم علیه حیثیت معنوی در فضای سایبر نسبت به فضای حقیقی

گستره جرایم رایانه‌ای، بسیار وسیع است. در حقیقت، فضای سایبر همانند فضای واقعی، شاهد بروز انواع جرایم و جنایات می‌باشد، به گونه‌ای که بسیاری از آنچه در جهان واقعی رخ می‌دهد، در جهان مجازی اینترنت و شبکه‌های اطلاع‌رسانی نیز امکان وقوع دارد. با این تفاوت که به مدد فناوری‌های پیشرفته جهان مجازی، ارتکاب جرم و بزهکاری تسهیل شده و همگان امکان ارتکاب آن را خواهند داشت. مضافاً این‌که به علت تعداد زیاد کاربرها امکان ردگیری و دستگیری مجرمان خیلی کمتر از تعقیب مجرمان در جهان واقعی می‌باشد. بر این اساس می‌توان ویژگی‌های خاص جرایم رایانه‌ای را به این ترتیب برشمرد: «گستردگی، فراوانی، فرامرزی بودن، وقوع سهل و آسان، تنوع، جذابیت زاید الوصف، ابهام حقوقی»(شیرزاد،۱۳۸۸، ص۴۵).

قوانین قدیمی و کلاسیک برای جرایم سنتی در نظر گرفته می‌شود؛ اما جرایم مدرن مخصوصاً جرایم ناشی از فناوری‌های روز، امور حادث‌اند و تحت شمول مقررات جدید قرار می‌گیرند.

ظهور و بروز فناوری‌های مختلف منجر به گشوده شدن بابی از جرایم شده که پیش از این کمتر به آن توجه شده است. این نوع جرایم را مبتنی بر تکنولوژی مدرن می‌نامند.

۱-۲-۱- جرایم مبتنی بر تکنولوژی مدرن

برخی جرایم همچون جرایم علیه محیط‌زیست، هواپیماربایی و رایانه‌ای از دسته جرایم ناشی از پیشرفت تکنولوژی هستند. این ویژگی، خود دارای آثاری است که در ذیل به آن اشاره می‌شود:

۱-۲-۱-۱- عنصر مادی

عنصر مادی جرم عبارت است از فعل یا عمل خارجی که تجلی نیت مجرمانه ویا قصد جزایی است (اردبیلی، ۱۳۹۱، ص ۸۴). در خصوص عنصر مادی جرایم سنتی یا کلاسیک باید گفت، به دلیل وجود بسترهای متفاوت ارتکاب این دو نوع جرم، طبعاً عنصر مادی هر جرم با جرم دیگر تفاوت دارد؛ ولی

درجرایم رایانه‌ای خصوصاً در جرایم نسل اول[1]، شکل عنصر مادی تقریباً یکسان است. به عبارتی، اجزای جرم رایانه‌ای عبارت است از ورود، تغییر، محو، متوقف‌سازی، دست‌کاری و امثال آن‌ها در اطلاعات داده‌ها، برنامه‌ها یا سیستم‌های رایانه‌ای و شبکه‌های ارتباطات راه دور. همین ویژگی باعث بروز تفاوت در جرایم رایانه‌ای نسبت به جرایم سنتی است. برای مثال، در کلاهبرداری رایانه‌ای ورود یا تغییر داده‌های مالی موجب نقل و انتقال وجوه می‌شود. در واقع مال دیگری ربوده می‌شود، بدون اینکه آن فرد مستقیماً فریب بخورد یا حتی با مجرم مواجه شده باشد.

نکته‌ای که در اینجا باید خاطر نشان کرد آن است که در حالت کلی، عنصر مادی هر جرم عبارت است از فعل و ترک فعل. حال آیا تصور جرم رایانه‌ای که عنصر مادی آن ترک فعل و نگهداری باشد، ممکن است یا آن‌که همه جرایم رایانه‌ای به صورت فعل مثبت تحقق می‌یابد؟

برخی محققین ادعا کرده‌اند که در جرایم رایانه‌ای تاکنون ترک فعل، مصداق عینی نداشته است. به علاوه هر گونه بی احتیاطی، بی‌مبالاتی، نداشتن مهارت و ... که جزء مصادیق خطا هستند، باید در زمره تخلفات مدنی یا اداری بررسی شوند و نباید جزء موارد کیفری به حساب‌آید (حسینی خواه، ۱۳۷۷، ص ۹۴).

در نقد نظریه مزبور باید گفت:

اولاً: چه بسا ممکن است جرمی واقع شود که عنصر مادی آن ترک فعل باشد.

ثانیاً: رکن مادی برخی از جرایم هم‌اکنون نیز به صورت ترک فعل و نگه داشتن است. برای مثال، هرگاه شخصی مسئول فیلترگذاری سایت‌های ضداخلاقی بوده یا وظیفه مشابهی داشته باشد، لیکن به عمد و حتی با سهل‌انگاری و بی‌مبالاتی، از عهده این وظیفه خویش برنیاید، مرتکب جرمی رایانه‌ای شده است و

[1] در قسمت انواع جرائم سایبری به تفصیل توضیح داده شده است.

نیز هرگاه شخصی تصاویر مستهجنی را که از طریق پست الکترونیکی به او ارسال شده است در حافظه رایانه خود نگهداری نماید، در حالی که قانوناً موظف به حذف تصاویر مزبور بوده است، مرتکب جرم رایانه‌ای شده است که عنصر مادی آن را می‌توان هم ترک فعل و هم نگهداری فرض نمود.

ثالثاً: به فرض آن‌که در حال حاضر امکان تصور جرم رایانه‌ای با عنصر مادی ترک فعل و نگهداری وجود نداشته باشد، نباید عنصر مادی آن را تنها در فعل مثبت منحصر دانست. چنین رویکردی با توجه به توسعه شتابان فناوری اطلاعات، دایره تعریف را مضیق‌تر کرده و کارایی تعریف را از آن خواهد گرفت.

نکته دیگری که در بحث عنصر مادی جرایم رایانه‌ای قابل توجه است، زمان و مکان ارتکاب این جرایم است.

در حالت سنتی و مرسوم برای ارتکاب جرایم مراحل مختلفی باید طی شود:

الف) مرحله قصد ارتکاب جرم؛

ب) مرحله تهیه مقدمات؛

ج) مرحله شروع به اجرا؛

د) مرحله اجرای جرم.

در مرحله عملیات اجرایی، شروع به اجرا ممکن است به سرانجام نرسد که گاهی به علت انصراف ارادی است و گاه غیرارادی. در این صورت بحث شروع به جرم یا جرم عقیم و محال مطرح می‌شود. اگر مجرم موفق به ارتکاب جرم شود و عمل خود را به اتمام برساند، با جرم تام روبه‌رو می‌شویم.

ولی در جرایم رایانه‌ای غالباً پس از قصد مرتکب و تهیه مقدمات (رایانه و اجزای آن و برنامه‌ریزی یک عملیات تخریبی رایانه‌ای) جرم شروع شده و عملیات اجرایی در کسری از ثانیه به وقوع می‌پیوندد. فرد مرتکب از لحظه ورود داده غیر واقعی تا کسب مال، زمان بسیار کمی را طی می‌کند. از لحظه ارسال تا دریافت مطالب افتراآمیز در کل شبکه، فقط ثانیه‌ای یا کمتر زمان می‌گذرد (دزیانی، ۱۳۷۳، ص ۹۶).

تعیین زمان دقیق ارتکاب جرم می‌تواند در تعیین مدت مرور زمان، قانون حاکم و صـــلاحیت دادگاه تأثیر بسـزایی داشته باشد. البته در مورد جرایمی که در زمان مشخص اتفاق می‌افتد، مشکل خاصی در تعیین زمان جرم پیش نمی‌آید، ولی در مورد جرایمی که در زمان خاص اتفاق نمی‌افتد، در تعیین میزان وقوع جرم با مشکل روبه‌رو می‌شویم.

یک برنامه‌نویس رایانه که در یک بانک مشـغول کار است، می‌تواند برنامه نوشته شده برای رایانه‌های بانک را به نحوی تنظیم کند که تا مدت مشـخصـی تمام مسـائل، به خوبی و بدون اشکال پیش بروند، ولی پس از این مدت معین (که با محاسبات برنامه‌نویس تعیین شده است) ناگهان روش کار عوض شده و رایانه از تمام حسـاب‌های بانکی مبلغ ناچیزی برداشـت و به حساب برنامه‌نویس واریز کند و او این مبلغ هنگفت را از حســـابش خـارج کرده و متواری شـــود. دربـاره زمان وقوع چنین جرمی چگونه می‌توان نظر داد؟ آیا هنگامی که این برنامه با قصـد سـوء نوشـته می‌شـده است زمان ارتکاب جرم است یا زمانی که جرم محقق می‌شـود؟ در صورتی که در این هنگام عمل مجرمانه‌ای از سوی شخص مذکور سر نمی‌زند. آیا می‌توان این قضـیه را با نظریاتی مثل تحقق عنصـر مادی حل کرد؟ مثلاً شـخص برنامه‌نویس را در زمان دادن برنامه (بر فرض امکان کشـف جرم در این زمان)، به این اتهام که سوءنیت داشته محاکمه نمود یا این کار قبل از وقوع جرم خلاف عدالت اسـت و با این اسـتدلال فقط وقتی جرم محقق می‌شود، می‌توان مرتکب را تحت پیگرد قرار داد؟

بحـث دیگر در مورد مکـان ارتکاب جرایم رایانه‌ای اســـت که این مورد می‌تواند از دو منظر حقوق جزای اختصـاصـی و حقوق جزای بین‌الملل مطرح شـود. از منظر حقوق جزای اختصـاصـی برخی جرایم می‌تواند بسـته به مورد، در یک یا چند شـهر ارتکاب یابند؛ مثلاً در جرم کلاهبرداری، عمل ارتکابی می‌تواند در یک شـهر یا چند شـهر به صـورت مباشـرت یا مباشـرت و معاونت تحقق یابد و از منظر حقوق جزای بین‌الملل، مکان می‌تواند چند جا باشد.

فردی که مطالب افتراآمیز را در سراسر شبکه منتشر می‌کند، در یک لحظه زمانی بسیار کوتاه بیش از چند کشور و به عبارتی چند میلیون سایت را درگیر می‌کند؛ یا کسی که ویروسی را نوشته و منتشر می‌کند، با یک فعل چندین سایت را در اقصی نقاط دنیا آلوده می‌کند (دزیانی، ۱۳۷۳، ص ۶۹). با این قابلیت و مشخصه محل وقوع جرم، محل شروع، محل اتمام جرم، کشف ادله و ... در نگاه اول مفقود و کشف آن غیر ممکن به نظر می‌رسد.

۱-۲-۱-۲- عنصر معنوی

عمل مجرم علاوه بر اینکه در قانون ذکر می‌شود و تحقق خارجی می‌یابد، باید توأم با سوءنیت و قصد مجرمانه یا تقصیر جزایی باشد. در جرایم سنتی یا کلاسیک اصل بر عمدی بودن جرایم است؛ اما در جرایم رایانه‌ای به واسطه ماهیت فضای سایبر، درصد جرایم ناشی از بی‌مبالاتی افزایش یافته است، به گونه‌ای که به طور یکسان یا حتی فراتر از جرایم عمدی با انواع جرایم ناشی از بی‌مبالاتی مواجه می‌شویم. از سویی تبلور این رویکرد در نوع مسئولیت کیفری و افراد دارای مسئولیت کیفری، به خوبی قابل مشاهده است.

تعدادی از افراد مشغول به کار در زمینه فناوری به واسطه نوع مسئولیت و فعالیت و همچنین به واسطه تدابیری که باید بیاندیشند یا به واسطه چارچوب وظایف حرفه‌ای که برای آنان تعیین شده است، دارای مسئولیت هستند و این مسئولیت غالباً به خاطر بی‌مبالاتی به وجود می‌آید.

۱-۲-۲- وجود تخصص خاص در مرتکبین جرایم رایانه‌ای

در برخی جرایم، ارتکاب جرم، مستلزم آشنایی با تکنیک یا تکنولوژی خاصی است. در جرایم رایانه‌ای، رایانه هدف، وسیله یا واسطه ارتکاب جرم است؛ بنابراین مجرم تا حدی از تخصص را دارا است.

بسته به نوع جرم رایانه‌ای، گاه آشنایی کلی با این تکنولوژی کافی و گاه نیاز به تخصص در سطح بالاست. سطح مهارت معمول در مجرمان رایانه‌ای محور برخی از مباحث را تشکیل می‌دهد. برخی عقیده

دارند سطح مهارت، شاخصی برای مجرمان رایانه‌ای به شمار نمی‌آید؛ حال آن‌که بعضی دیگر بر این باورند که مجرمان بالقوه رایانه‌ای، افرادی باهوش و دارای انگیزه‌اند که آماده رویارویی با چالش‌های تکنولوژی هستند، یعنی همان خصایصی که در کارمندان بخش داده‌پردازی بسیار مورد پسند است (پلی وانجوک[۱]، ۲۰۰۲، ص ۲۳).

تجربه نشان داده است که طیف گسترده‌ای از افراد، مرتکب جرایم رایانه‌ای شده‌اند: دانشجویان، افراد مبتدی، تروریست‌ها و اعضای گروه‌های جرایم سازمان‌یافته. معمولا سن مجرمان بین پانزده تا پنجاه سال است و دامنه مهارت آن‌ها از سطح تازه‌کار تا حرفه‌ای را شامل می‌شود (پاکزاد، ۱۳۷۵، ص ۷۴).

هر فردی با هر سنی و با داشتن مهارتی نه چندان زیاد و با انگیزه چالش‌های فنی، امکان کسب منابع، اشتهار یا انتقام یا اشاعه باورهای عقیدتی، یک مجرم رایانه‌ای بالقوه محسوب می‌شود.

مطابق مطالعات انجام شده بیشترین تهدیدها علیه منابع رایانه‌ای سازمانی، از جانب کارمندان است و در واقع جرایم رایانه‌ای غالباً جرایمی با منشأ داخلی به شمار می‌آیند (تنن باوم[۲]، ۲۰۰۵، ص ۲۷۱).

خصوصیات مجرمان رایانه‌ای که نخستین بار توسط اف بی‌آی (FBI) [۳] تهیه شده، به چهار دسته طبقه‌بندی شده‌اند:

الف) خصوصیات سازمانی؛ [۴]

ب) خصوصیات عملیاتی؛[۵]

ج) خصوصیات رفتاری؛[۶]

---

۱ - Polivanjuk

۲ Andrew Stuart Tanenbaum

۳ - Fedral Bureau of Investigation (دفتر فدرال تحقیقات)

۴ -organization Charcterstics

۵ -Operational charcterstics

۶ -behavioral charcterstics

د) خصوصیات منابع [1] (دزیانی، ۱۳۷۳، ص ۷۵).

۱-۲-۲-۱- خصوصیات سازمانی

این خصوصیات روش‌هایی را مورد بحث قرار می‌دهد که مجرمان رایانه‌ای توسط آن خود را گروه‌بندی می‌کنند. جاسوسان و مجرمان جرایم سازمان‌یافته به طور آشکار و قوی، با تشکیلاتی منسجم، فعالیت می‌کنند. در سایر موارد، مجرمان رایانه‌ای بیشتر اوقات یا به طور انفرادی کار می‌کنند و یا گروه‌های بسیار محدودی را تشکیل می‌دهند. در عین حال، سه یا چهار مجرم رایانه‌ای ممکن است با هم جمع شده و فناوری روز را با یکدیگر مبادله کنند.

اکثر قریب به اتفاق جرایم به ویژه جرایم رایانه‌ای، دارای جذابیت و انگیزه بسیار قوی برای محقق شدن می‌باشند. این جذابیت و انگیزه از حرص و طمع شروع و به چالش‌های هوشمندانه ختم می‌شود. از دید برخی صاحب‌نظران، میان مرتکبین جرایم رایانه‌ای و مرتکبین انواع دیگر جرایمی مانند اخاذی و کلاهبرداری تفاوت چندانی وجود ندارد.

نفوذکنندگان غیرمجاز و مؤسسات جاسوسی هر دو ممکن است ارتباطات بین‌المللی داشته باشند. نفوذکنندگان غیرمجاز، افراد خبره‌ای هستند که در نفوذ به سیستم‌ها با یکدیگر همکاری می‌نمایند.

۱-۲-۲-۲- خصوصیات عملیاتی

خصوصیات عملیاتی، روش‌هایی را که مجرمان برای ارتکاب جرم به کار می‌گیرند، مورد بحث قرار می‌دهد. از لحاظ برنامه‌ریزی، جرایم رایانه‌ای در برخی موارد بسیار دقیق و موشکافانه برنامه‌ریزی می‌شوند. در موارد دیگر به دلیل ضعف سازمان‌های پیشگیری‌کننده، مجرمان توانسته‌اند از فرصت‌های به دست آمده استفاده کنند.

[1] - resource charcterstics

از لحاظ سطح مهارت و تخصص، هر چند که سطح مهارت‌ها گوناگون و متفاوت است، مجرمان رایانه‌ای نوعاً از مهارت و دانش بالایی برخوردارند. این افراد وقت زیادی را برای بررسی و زمینه‌سازی انجام عمل مجرمانه اختصاص می‌دهند. همچنین با توجه به انگیزه‌ها و میزان تخصص، روش‌ها و راهکارهای متفاوت در ارتکاب جرم انتخاب می‌شود.

۱-۲-۲-۳- خصوصیات رفتاری

خصوصیات رفتاری، خصوصیات مجرمان رایانه‌ای را شرح می‌دهد و اینکه انگیزه آنها چه بوده است؟ علاقمندی‌شان چیست؟ چه نقطه ضعفی باعث شده تا مرتکب جرم رایانه‌ای شوند؟

در برخی موارد، بیش از یک عامل محرک وجود دارد. یک کارمند ناراضی تصمیم می‌گیرد از مدیر خود انتقام بگیرد و مبالغی از حساب او را به حساب خود منتقل سازد.

از لحاظ ویژگی‌های فردی باید گفت که این ویژگی، یک شاخص فردی با ذکر مشخصات جزئی به شمار نمی‌رود، بلکه صرفاً نکاتی درباره میزان بهره هوشی یا نشانه‌های منحصر به فردی است که مجرمان رایانه‌ای در طبقه‌بندی‌های مختلف می‌توانند داشته باشند.

از لحاظ نقاط ضعف باید گفت که برخی از مجرمین کار خود را جرم نمی‌دانند. برخی دیگر از نفوذکنندگان غیرمجاز، خود را قهرمانانی می‌دانند که جامعه را یاری می‌دهند تا آسیب‌پذیری خود را بشناسد و در پی درمان آن برآید. مجرمان رایانه‌ای همانند دیگر مجرمان، نوعاً آن هنگام که به نهایت آزمند و آلوده می‌شوند، در چنگ قانون گرفتار می‌آیند. در این مواقع اعتماد به نفس آن‌ها، آنچنان زیاد می‌شود که به علت غرور و زیاده‌روی از خود ردپا بر جا می‌گذارند.

۱-۲-۲-٤-خصوصیات منابع

این خصـــوصـــیات در مورد منابعی بحث می‌کند که در اختیار مجرمان رایانه‌ای بوده یا به آنها نیاز دارند. مجرمان به چه آموزش‌ها و ابزار و تشـکیلاتی برای رسـیدن به اهداف خود نیاز دارند؟ چه کسی قادر است به آن‌ها کمک کند؟

از لحاظ آموزشـی، مهارت‌های آموزشـی از دوره‌های رسمی گرفته تا تجربیات به‌دست‌آمده در طول کار را شامل می‌شود. هر چند سطح آموزش‌ها بالاتر باشد، میزان تخصص و مهارت فرد نیز بالاتر می‌رود.

از لحاظ ابزار مورد نیاز، در بیشـــتر موارد، جرایم رایانه‌ای با تجربیات عمده رایانه‌ای می‌تواند انجام شـود. با یک رایانه و مودم مربوط، اگر مجرم مسـتقیماً به سیستم رایانه‌ای هدف دسترسی داشته باشد، دیگر نیازی به تجهیزات نخواهد داشـت. البته در بسیاری موارد به تجهیزات بیشتری نیاز است؛ مثلاً برای برقراری ارتباط و استراق سمع الکترونیکی، تجهیزاتی باید فراهم شود.

از لحاظ سـاختار پشـتیبانی، نفوذکنندگان غیرمجاز را همتایان‌شـان حمایت و پشـتیبانی می‌کنند و سـرویس‌های جاسـوسـی از طریق دولت‌های خود پشتیانی می‌شوند، ولی بسیاری از مجرمان رایانه‌ای بدون هیچ‌گونه پشتیبانی و حمایتی، صرفاً با اتکا بر دانش خود به راحتی کار خود را انجام می‌دهند.

۱-۲-۲-۵- انواع تخصص‌ها در مرتکبین جرایم رایانه‌ای

مرتکبین جرایم رایـانـه‌ای معمولاً بـه دانش و مهـارت‌هایی تسـلط دارند که در چهار مورد زیر قابل دسته‌بندی است:

الف) تسـلط به شبکه: هر جرم رایانه‌ای در قالب یک ارتباط مجازی ارتکاب می‌یابد؛ به این معنی که یک شخص با یک رایانه که به هیچ شبکه متصل نبوده و با رایانه‌ها و پایگاه‌های دیگر در ارتباط نیست، قادر به انجام جرم هم نیسـت. بنابراین هر مجرمی باید به عنوان یک مهارت پیش‌نیاز برای ارتکاب جرم به کار با شـبکه تسـلط داشـته باشـد. برخی شـبکه‌ها دارای تعداد کاربر پایین هستند و به داخل یک سازمان محدود

می‌شـوند که به آن شـبکه داخلی یا اینترانت[۱] می‌گویند. برخی نیز گسـترده و جهانی‌اند که بارزترین مصداق شبکه‌های بزرگ، خود اینترنت است. کار با هر یک از این دو نوع شبکه، مهارت‌های خاص خود را می‌طلبد که گاهی اوقات وجوه مشترک نیز دارند.

ب) تسـلط به سـیستم‌های عامل[۲] و پایگاه‌های داده[۳]: هر مجرم، پس از استفاده از شبکه و دستیابی به رایانه، حافظه‌های جانبی و یا سـامانه قربانی، تنها گام اول را پیموده اسـت. مجرم برای تخریب، سـرقت، تحریف و یا تغییر اطلاعات در رایانه قربانی نیاز به دانستن دانش و مهارت‌های مرتبط با رایانه و سیستم‌های عامل و پایگاه‌های داده آن دارد.

بـه عنوان مثال سـیسـتم‌های عامل متن باز[۴] مانند لینوکس[۵]، در برابر حملات سـایبری از ویندوز[۶] مقاوم‌ترند و نقاط ضعف کمتری دارد. اگر مجرم به شبکه مسلط باشد اما با دانش سیستم عامل و پایگاه داده آشـنا نباشد، مانند سارقی است که به منزل فرد دیگر ورود می‌کند اما به دلیل نداشتن چراغ قوه، قادر نیست عمل مورد نظر خود را انجام داده و کالای با ارزشی سرقت کند.

ج) تسلط به ابزارها: در حال حاضر، ابزارهای متعددی برای انجام انواع جرایم سایبری تولید شده‌اند. این ابزارها هر یک برای هدفی سـاخته شـده‌اند، مثلاً برای سـرقت اطلاعات و یا از کار انداختن سـیسـتم قربانی. برای انجام جرم با این ابزارها کافی اسـت مجرم به سـیستم قربانی از طریق شبکه دست پیدا کرده و سـپس ابزار مورد نظر را فعال کند. ابزار، خود عمل مجرمانه را انجام داده و سپس سابقه کار خود را به طور خودکار از سیستم قربانی پاک می‌کند تا قربانی متوجه وقوع جرم نشود.

---

[۱] intranet
[۲] Operating system
[۳] Database
[۴] Open source
[۵] Linux
[۶] Windows

د) مهندسی اجتماعی[1]: به مجموعه تکنینک‌های غیر فنی برای دستیابی به اطلاعات پیش‌نیاز برای انجام یک جرم رایانه‌ای، مهندسی اجتماعی گویند. در سال ۹۳، یک حمله سایبری به وبسایت یکی از بانک‌های معتبر کشور انجام شد. در بررسی‌های به عمل آمده مشخص شد که مجرمان، کارکنان سابق یک شرکت رایانه‌ای در زمینه امنیت اطلاعات بودند. آن‌ها با برقراری ارتباط با واحد فناوری اطلاعات بانک، به مسئولین بانک پیشنهاد کرده بودند برای بالا بردن امنیت سایت حاضرند پروژه‌ای با هزینه پایین برای بانک انجام دهند و در خلال جلسات توجیهی پروژه، اطلاعات مهمی از سیستم‌های رایانه‌ای بانک از جمله نوع سیستم عامل و زبان برنامه‌نویسی نرم‌افزار بانک کسب کرده بودند. سپس با این ادعا که پروژه سنگین‌تر از آن است که در ابتدا توجیه شده، اعلام کرده بودند قادر به انجام پروژه نیستند. چند ماه بعد نیز با همان اطلاعات حمله بسیار ماهرانه‌ای به سایت بانک انجام داده و ضمن ایجاد اختلال در آن و آسیب به حیثیت معنوی بانک به عنوان یک شخص حقوقی، مقادیر زیادی پول جابجا کرده بودند. به مجموعه این فعالیت‌ها که معمولاً در قالب سناریوهایی قبل از وقوع جرم اصلی انجام می‌شود، به صورت خلاصه مهندسی اجتماعی می‌گویند.

۱-۲-۳- عدم تخمین میزان جرایم ارتکابی

تعیین شمار واقعی جرایم رایانه‌ای امری دشوار است. با افزایش بهره‌گیری از رایانه در تمام عرصه‌های زندگی و همچنین سهولت استفاده از آن، امروز جرایم رایانه‌ای می‌تواند توسط هر کسی یا علیه هر کسی ارتکاب یافته و به تهدید علیه هر شهروندی تبدیل شود. با آنکه تحقیقات به عمل آمده نشان می‌دهد که جرایم رایانه‌ای رو به افزایش‌اند، آمار موجود نمی‌تواند ما را به نتیجه مطلوبی رهنمون سازد. به دلیل این‌که این آمار منعکس کننده تعداد جرایم مکشوفه است و نه تعداد جرایم واقعی و در جرایم رایانه‌ای

[1] Social engineering

رقم سیاه[1] بالاست، به گونه‌ای که بین میزان مجرمیت واقعی تا مجرمیت ظاهری، فاصله زیادی وجود دارد. انجمن بین‌المللی حقوق جزایی در گردهمایی خود درباره جرایم رایانه‌ای و دیگر جرایم علیه تکنولوژی اطلاعاتی که از تاریخ ۵ الی ۸ اکتبر ۱۹۹۲ در ورتسبورگ[2] آلمان برگزار شد، گزارشی درباره جرایم رایانه‌ای بر پایه گزارش‌های دریافتی از کشورهای عضو ارائه کرد که مطابق آن تخمین زده می‌شود تنها پنج درصد جرایم رایانه‌ای به مقامات مجری قانون گزارش شده‌اند (نشریه بین‌المللی سیاست جنایی، ۱۹۹۲، ص ۲۲). این مسئله علل متعددی دارد:

اول اینکه جرایم رایانه‌ای ماهیتاً از خصوصیاتی برخوردارند که به نظر می‌رسد کمتر قابل گزارش باشند. یک مجرم زبده رایانه‌ای غالباً مدرکی به جا نمی‌گذارد، چون اطلاعات به جای اینکه از محل خود برداشته شوند، قابل نسخه برداری‌اند. سوابق عمل نیز می‌تواند پاک شود. قربانی که کارش بر مبنای اشتهار به مورد اعتماد بودن استوار است –همانند یک بانک یا شرکت بیمه– بعید است این واقعیت را که سوابق اطلاعاتی آن دست‌کاری شده و مجرم نیز گریخته است، علنی سازد.

دوم اینکه تکنولوژی پیشرفته و سرعت بالای عملیات، موجب کشف دشوار جرایم رایانه‌ای است (باستانی، ۱۳۸۳، ص ۵۲).

سوم، خلاف بیشتر جرایم مرسوم، بزه‌دیدگان ناآگاه، اغلب بعد از وقوع جرم، به وسیله مأموران از اینکه متحمل وقوع جرم رایانه‌ای شده اند مطلع می‌شوند. بسیاری از بزه‌دیدگان، برنامه‌ریزی لازم را برای مقابله با حوادث مربوط به جرایم رایانه‌ای ندارند (عبقری، ۱۳۷۷، ص ۴۹).

چهارم، عمده دلیل وجود رقم سیاه، عدم تمایل بزه‌دیدگان برای اعلام وقوع جرایم رایانه‌ای پس از کشف می‌باشد. در بخش تجارت این عدم تمایل به دو امر مربوط می‌شود. برخی بزه‌دیدگان ممکن است به

[1] رقم سیاه به میزان جرایمی گفته می‌شود که بنا به ملاحظاتی در آمارها محاسبه نمی‌شوند.

[2] Würzburg

دلیل هراس از تبلیغات سوء، رسوایی و یا از دست دادن حسن شهرت خود تمایلی به فاش ساختن اطلاعات نداشته باشند. دیگر بزه‌دیدگان نیز از سلب اعتماد سرمایه‌گذاران و یا عامه مردم و پیامدهای اقتصادی ناشی از آن واهمه دارند.

۱-۲-٤- گستردگی صدمات و خسارات

در جرایم سنتی گاه مجرم برای حصول موفقیت در ارتکاب جرم باید مسیر دشواری طی کند تا در نهایت بتواند مالی دریافت کند یا خسارتی به دیگری وارد آورد. حجم مال به دست‌آمده یا خسارت وارده در جرایم سنتی محدود است، اما در جرم رایانه‌ای به دلیل سهولت ارتکاب و حجم زیاد موضوعات، سرعت عملکرد رایانه، عدم نیاز به تخصص یا تخصص بالا، عدم نیاز به حضور فیزیکی مرتکب در محل و ... حجم صدمات و خسارات وارده می‌تواند به چندین برابر جرایم سنتی برسد.

وسعت خسارات وارده ناشی از یک نفوذ غیرقانونی یا گسترش ویروس در اینترنت می‌تواند در کسری از ثانیه، صدها هزار کاربر در سراسر جهان را متحمل خسارت کند.

عواقب جرایم رایانه‌ای علاوه بر خسارت اقتصادی سنگین می‌تواند تهدیدی جدی برای امنیت بشر باشد. وابستگی امور حساس کشورها در زمینه‌های پزشکی، مخابراتی، هواپیمایی، امور امنیتی و نظامی و ... به عملکرد رایانه‌ها باعث می‌شود، تا کوچک‌ترین اختلال و خدشه در کار این سیستم‌ها، عواقب وخیم و جبران‌ناپذیری را به دنبال داشته باشد (عبقری، ۱۳۷۷، ص ۵۶).

مطالعات آماری بیانگر جایگاه مهم جرایم رایانه‌ای در میان تمامی خطرات وابسته به رایانه است و به موجب ارقام منتشره از سوی باشگاه فرانسوی امنیت رایانه در سال ۱۹۹۱، ۱۰/۴ میلیارد فرانک خسارت رایانه‌ای در شرکت‌ها و مؤسسات فرانسوی گزارش می‌شود که بیش از نیمی از آن ناشی از اعمال مجرمانه می‌باشد (باستانی، ۱۳۸۳، ص ۱۰۹).

کانون وکلای آمریکا در سال ۱۹۸۷ دست به انجام مطالعاتی زد. از سیصد شرکت و اداره دولتی، ۷۲ واحد ادعا داشتند که در فاصله زمانی دوازده ماه قبل از شروع مطالعات مذکور، بزه‌دیده جرایم رایانه‌ای بوده‌اند و طبق برآورد، خساراتی بین ۱۴۵ تا ۷۳۰ میلیون دلار متحمل شده‌اند. مطالعات مشابهی که در کشورهای دیگر انجام شده، بیانگر سوءاستفاده‌ها و خسارات قابل ملاحظه و گسترده‌ای است (پاکزاد، ۱۳۷۵، ص ۵۲).

۱-۲-۵- فراملی بودن جرایم رایانه‌ای

جرم رایانه‌ای به دلیل ماهیتش اختصاص به محیط فیزیکی محدود ندارد و می‌تواند به آسانی در سطح گسترده‌ای ارتکاب یابد. چون دنیای جدید به شدت به اطلاعات وابسته است، جرایم رایانه‌ای به راحتی در مقیاس بین‌المللی به وقوع می‌پیوندد و مسافت، زمان و مکان، مانعی برای آن به حساب نمی‌آید.

حضور فیزیکی شخص در محل وقوع حادثه معنایی ندارد؛ مثلاً برای سرقت از بانک، مدت مشخصی لازم است که سارق با حضور در محل، دست به چنین عملی بزند، ولی ارتکاب جرم رایانه‌ای در مدتی کوتاه و بدون حضور در محل امکان‌پذیر است. به عنوان مثال، در سال ۱۹۹۰ چهار جوان در مدرسه دالتون آمریکا از طریق یک سیستم رایانه‌ای با شبکه اطلاعات و ارتباطات رایانه‌ای کانادا ارتباط پیدا کرده و اطلاعاتی به دست آوردند (جبلی طاهری، ۱۳۷۲، ص ۱۰۱).

مثال جالب دیگر در مورد فراملی بودن جرایم رایانه‌ای، ویروس‌ها یا کرم‌های رایانه‌ای است. اگر ویروسی بر یک نقطه از سیستم اثر بگذارد، اثر مخرب آن می‌تواند با سرعتی بسیار زیادگسترش یابد و برنامه‌های کل شبکه بین‌المللی را مبتلا سازد. در سال ۱۹۸۸، کرم اینترنتی[1] که توسط یک دانشجوی آمریکایی ساخته شده بود، در طی چند روز نزدیک شش هزار سیستم رایانه‌ای را از طریق اینترنت مختل

[1] Internetworm

کرد (پـاکزاد، ۱۳۷۵، ص ۵۸). در حال حاضـــر تمام حوزه‌های اقتصـــادی از جمله بانکداری و هواپیمایی بین‌المللی، به شدت و حتی به طور انحصاری به شبکه‌های مخابراتی بین‌المللی وابسته‌اند.

عـامـل بین‌المللی در ارتکاب جرایم رایانه‌ای، قانون را با مســـائل و چالش‌های تازه‌ای مواجه کرده اسـت؛ مثلاً دسـت‌یابی به سـیسـتم‌ها ممکن اسـت در یک کشور و پردازش در کشور دیگر صورت گیرد و نتایج آن در کشـور سـوم به دست آید. کاربران غیرمجاز می‌توانند به صورت غیرفیزیکی در یک کشور وارد عمل شـده و به صـورت الکترونیکی از شـبکه‌ای به شـبکه دیگر سـراسـر جهان را بپیمایند و به راحتی به بانک‌های اطلاعاتی مسـتقر در قاره‌ای دیگر دسترسی یابند و در نتیجه این قابلیت، حاکمیت‌ها، صلاحیت‌ها، قوانین و قواعـد گونـاگونی وارد صـــحنه می‌شـــوند. ســـرعت، تحرک، انعطاف، اهمیت و ارزش مبادلات الکترونیکی بیش از هر جرم فراملی، قوانین و مقررات موجود در حقوق جزای بین‌الملل را با مشـکل مواجه می‌کند و مســـائل پیچیده‌ای را مطرح می‌ســـازد؛ از جمله چگونه می‌توان تعیین کرد که جرم واقعاً در کدام کشـور واقع شـده است. چه کسی باید صلاحیت رسیدگی قضایی به دعاوی را داشته باشد. به منظور فراهم سـاختن امکان تحقیق و رسـیدگی مؤثر، همکاری بین‌المللی در مسـائل کیفری از اهمیت بسـیار برخوردار است.

۱-۲-٦- مشکلات تعقیب و آیین دادرسی جرایم رایانه‌ای

نوین بودن جرایم رایانه‌ای و شـــیوه ارتکاب این گونه جرایم، نحوه رســـیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش‌هایی روبه‌رو کرده است.

مشـــکلات اولیه در تحقیقات مقدماتی بروز می‌کند، چون عنصـــر مادی جرم رایانه‌ای از طریق وارد کردن، محو، تغییر و ... داده‌ها، اطلاعات، برنامه‌ها وسیستم رایانه‌ای، مخابراتی و ... تحقق می‌یابد.

مقامات تعقیب و تحقیق دارای اختیاراتی هسـتند که در قوانین دادرسی کیفری به‌آن اشاره شده است و به هنگام بازجویی، بازرسی، معاینه محل، توقیف اشیای مربوطه و ... بر چگونگی کار آن‌ها حکم‌فرماست،

اما در جرایم رایانه‌ای با محیط‌های دیجیتالی سروکار داریم و به تبع خصایص این محیط‌ها، قواعد مرسوم تغییر می‌یابند.

حقوق جزا پیوسته به حمایت یا بحث از اشیا و موضوعات و اهداف مادی، ملموس و فیزیکی پرداخته و کمتر به اشیا، موضوعات و اهداف غیر مادی، غیر ملموس و غیر فیزیکی پرداخته است. از این رو، قواعد دادرسی برای همان اهداف یاد شده تبیین شده اند (دزیانی، ۱۳۷۳، ص ۸۲).

در یک محیط دیجیتال چه چیزی را می‌توان توقیف کرد؟ آیا داده‌ها و اطلاعات را می‌توان توقیف کرد؟ کسب، ذخیره سازی و ارائه داده‌ها و اطلاعات به عنوان اشیای موضوع توقیف آیا می‌تواند همچون موارد فیزیکی تحت شمول قواعد مرسوم دادرسی قرار گیرد؟ آیا قواعد مربوط به تفتیش اماکن می‌تواند کاربردی در محیط دیجیتال داشته باشد؟ در جرایم رایانه‌ای گاه مکان ارتکاب با مکان ادله فرق دارد. گاه تجهیزات مربوط، در رایانه شخص ثالث و در یک محیط دیگر است. گاه فرد برنامه را پنهان می‌کند. آیا می‌توان قواعد مورد بحث استراق سمع در حالات مرسوم را برای شنودهای الکترونیکی در محیط‌های رایانه‌ای به کار گرفت (برومند باستانی، ۱۳۸۲، ص ۲۹).

دشوارترین بخش از مشکلات، ناظر به ادله اثبات دعواست. ادله اثبات به تبع جرم مطرح می‌شود؛ از این رو تعریف دلیل رایانه‌ای، نوع دلیل، منابع آن، شیوه تحصیل آن، قابلیت قبول، نحوه ارائه و چگونگی صدور حکم بر مبنای آن در محیط‌های دیجیتالی همه از موارد مورد بحث است که تا حد زیادی قوانین مرسوم در مورد آنها صادق است.

به عنوان مثال محل وقوع جرم در شرایطی که یک فرد در هواپیما یا کشتی از اینترنت استفاده می‌کند و همزمان مرتکب جرایم رایانه‌ای می‌شود کجاست؟ یا امکان تعقیب کسی که از پراکسی‌های زنجیره‌ای[1] استفاده می‌کند و موقعیت جغرافیایی و مختصات وی دائم در حال تغییر است به چه نحو است؟

[1] Chain proxy

بخش دوم: اعاده حیثیت از جرایم علیه حیثیت معنوی اشخاص در فضای سایبر

این پژوهش به اعاده حیثیت از جرایم علیه حیثیت معنوی اشخاص در فضای سایبر، امکان و عدم امکان، شیوه‌ها و چالش‌های این فضا پرداخته شده است.

۲-۱- فصل اول: مفهوم و شیوه های اعاده حیثیت

در این قسمت، مفهوم اعاده حیثیت و شیوه‌های آن، به خصوص در فضای سایبر بررسی شده است و دو تعریف مشهور از اعاده حیثیت بیان شده است.

۲-۱-۱- مفهوم اعاده حیثیت

اعاده در لغت به معنای اعطاء، بازگرداندن، رجعت، جبران‌کردن و برگرداندن است. اما حیثیت در لغت به معنای آبرو، اعتبار، حقوق، اهلیت و شخصیت می‌باشد. اعاده حیثیت نیز اعطاء و بازگرداندن حقوق و اعتباراتی است که به موجب حکم دادگاه یا قانون از مجرم به جهت ارتکاب جرم سلب گردیده است (شاملو، ۱۳۸۰، ص ۶۱).

اعاده حیثیت به لحاظ لغوی از دو کلمه عربی «اعاده» و «حیثیت» ترکیب یافته است که اعاده به معنای بازگردانیدن (معین، ۱۳۸۲، ص ۱۳۴) و حیثیت به معنای اعتبار و آبرو (معین، ۱۳۸۲، ص ۳۹۴) است و گفته شده اعاده حیثیت «بازگشت به اهلیتی است که شخص به علتی آن را از دست داده است (جعفری لنگرودی، ۱۳۶۳، ص ۷۸).

اعاده حیثیت در حقوق ایران به یک مفهوم یکتا استعمال نشده است. به‌طور کلی در مقررات و متون حقوقی، اعاده حیثیت در دو مورد استفاده شده است:

الف) اعاده حیثیت در بیان نخست، نهادی حقوقی است که با لغو نمودن محکومیت از اسناد کیفری مرتکب، سبب اسقاط مجازات تبعی و از بین رفتن محکومیت قضایی شده و حقوقی را به شخص باز

می‌گرداند. فلذا با اعاده حیثیت شخص، تبعات ناشی از محکومیت قبلی لغو شده و او مثل یک شهروند عادی، اجازه ایفای همه حقوق خود را مجدداً به‌دست می‌آورد.

ب) در تعریف دوم اعاده حیثیت، این مفهوم قرابت معنایی زیادی با مفهوم جبران خسارت معنوی دارد. در این مفهوم، اعاده حیثیت، تدبیری برای بازگرداندن حیثیت و آبروی از بین‌رفته مجنی علیه به شمار می‌رود. حفظ حرمت و حیثیت اشخاص از چنان درجه‌ای از اهمیت برخوردار است که در اصل بیست و دو قانون اساسی به آن صریحاً اشاره شده است: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.»

ماده ۶۹۸ (۹۲۲) قانون مجازات اسلامی نیز مقرر می‌دارد «هرکسی به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله نامه یا شکواییه یا مراسلات یا عرایض یا گزارش یا توزیع هرگونه اوراق چاپی یا خطی با امضا یا بدون امضا اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را برخلاف حقیقت راسا یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی تصریحا یا تلویحا نسبت دهد، اعم از این‌که از طریق مزبور به نحوی از انحا ضرر مادی یا معنوی به غیر وارد شود یا نه، علاوه بر اعاده حیثیت در صورت امکان، باید به حبس از دو ماه تا دو سال و یا شلاق تا ۷۴ ضربه محکوم شود.»

طرقی که در موارد مزبور برای اعاده حیثیت انتخاب می‌شود یکسان نیست ولی در برخی موارد با دخالت مقام قضایی صالح، درج حکم در جراید و مطبوعات یکی از شیوه‌های منطقی برای اعاده حیثیت است؛ چنان‌که ماده ۲۷ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مصوب۱۳۴۸، ذیل ماده ۱۷ قانون اقدامات تأمینی و ماده ۲۹۸ قانون آیین دادرسی در امور کیفری به این شیوه اشاره دارد. ماده ۱۰ قانون مسؤلیت مدنی مصوب ۱۳۳۹ نیز همین راه‌حل را تجویز کرده است.

۲-۱-۲- انواع اعاده حیثیت

اعاده حیثیت به دو صورت اتفاق می‌افتد:

۲-۱-۲-۱- اعاده حیثیت قضایی

اعاده حیثیت و حقوق اجتماعی سلب شده مجرم بخاطر رعایت شرایط قانونی و مقرر در حکم دادگاه از سوی بزهکار به موجب حکم دادگاه را گویند پس به حکمی که دادگاه در مورد اعاده حیثیت بدهد، اعاده حیثیت قضایی می‌گویند. در قوانین کیفری ایران، این نوع از اعاده حیثیت را فقط می‌توان در لایحه شماره ۱۳۹۴/۳۸۳۸ سال ۱۳۱۸ که از طرف وزارت عدلیه تهیه و به مجلس شورای ملی پیشنهاد شد، ملاحظه کرد. به موجب ماده ۶۱ لایحه مزبور: «نسبت به محکومانی که مجازات اصلی درباره آنها اجرا و یا به یکی از علل قانونی اسقاط شده باشد و پنج سال از روز تمام شدن مجازات اصلی و یا اسقاط آن گذشته و مستمرا رفتار پسندیده از آنها به ظهور رسیده باشد، به تقاضای محکوم علیه، حکم به اعاده حیثیت داده می‌شود.»(معینی، ۱۳۷۹، ص ۸۳۳)

ظاهراً وزارت عدلیه وقت، قبل از تصویب لایحه مزبور آن را مسترد می‌کند و بعد از این مورد تا زمان حاضر هیچ مصوبه‌ای که بر مطالبه اعاده حیثیت قضایی از طرف محکومان تصریح کند، ملاحظه نمی‌شود.

۲-۱-۲-۲- اعاده حیثیت قانونی

هرگاه به موجب قانون مدتی معین از محکومیت بزهکار گذشته باشد و در طی این مدت مرتکب جرم جدیدی نشود یا دستورات دادگاه را نقض ننماید، به حکم قانون اهلیت و حقوق سلب شده به وی بازگردانده می‌شود. پس اگر قانون حکم اعاده را بدهد، آن را اعاده قانونی حیثیت خوانند (شاملو، ۱۳۸۰، ص ۵۱؛ جعفری لنگرودی، ۱۳۷۸، ص ۸۴).

انسان‌ها از حیث شخصی و شهروندی و از آن جهت که انسان هستند عموماً دارای حیثیت فردی و اجتماعی می‌باشند. از آنجایی که تعقیب کیفری و به طریق اولی محکومیت کیفری، حیثیت افراد را شدیداً

خدشه‌دار کرده و از اعتبارات و امکانات حضور در اجتماع و مشارکت اجتماعی محروم می‌کند، لذا مجرمی که حیثیت او به واسطهٔ ارتکاب جرم از دست رفته مطابق شرایط قانونی و رعایت تشریفات ویژه می‌تواند حیثیت از دست داده را دوباره به دست آورد و این امر در حقوق جزائی اصطلاحاً اعاده حیثیت گفته می‌شود. حیثیت مجرم معمولاً با عنوان سوءپیشینه کیفری و ثبت آن در سجل کیفری مخدوش گردیده و تا اعاده آن همچنان بسیاری از حقوق اجتماعی وی مسلوب می‌ماند.

۲-۱-۳- اعاده حیثیت در قوانین ایران

اعاده حیثیت در قوانین ایران دارای سیر تطوری است که در این پژوهش، این امر در قوانین جزایی قدیم و جدید مورد مداقه قرار گرفته است.

۲-۱-۳-۱- اعاده حیثیت در قوانین جزایی قدیم

قانون مجازات عمومی آزمایشی ۱۳۰۴ مواد ۵۶ تا ۵۹ خود را در مبحث سوم به اعاده حیثیت اختصاص داده بود که البته ماده ۵۶ درج محکومیت در شناسنامه کیفری محکوم را شامل می شد. طبق ماده ۵۶ «کلیه احکام قطعی که بر محکومیت متهمین به جنحه و جنایات صادر می‌شود باید در سجل کیفری محکومین درج گردد.» طبق ماده ۵۷، «اگر کسی به مجازات تأدیبی محکوم شده باشد و در مدت ۵ سال از تاریخ اتمام مجازات محکومیت جزایی جدیدی نداشته باشد، به اعاده حیثیت نائل شده و محکومیت سابق او از سجل جزایی او محو خواهد شد.» وفق ماده ۵۸ «درباره اشخاصی هم که به مجازات جنایی محکوم شده اند، مجری خواهد بود مشروط بر این که در ظرف ۱۰ سال از تاریخ اتمام مجازات محکومیت جزایی جدید نداشته باشد.» و بالاخره حسب ماده ۵۹ «اگر اشخاصی که برای ارتکاب جرم سیاسی محکوم به حبس تأدیبی می‌شوند در ظرف یک سال از تاریخ اتمام مجازات و اشخاصی که برای ارتکاب همان جرم محکوم به مجازات جنایی می‌شوند در ظرف ۵ سال از تاریخ اتمام مجازات مجدداً محکومیت جزایی نداشته باشند، به اعاده حیثیت نائل شده و محکومیت آنها از سجل جزایی محو خواهد شد.»

قانون‌گذار مهلت اعاده حیثیت را در جرایم سیاسی با توجه به طبیعت این جرایم کمتر تعیین نموده و از این حیث ارفاق بیشتری را نسبت به مرتکبین این اعمال رعایت کرده بود. مواد ۵۷ و ۵۸ قانون اصلاحی مجازات عمومی ۱۳۵۲ نیز به اعاده حیثیت اختصاص داشت و ماده ۵۷ در مورد جرایم عادی و ماده ۵۸ در مورد جرایم سیاسی بود. طبق ماده ۵۷ «در مورد جرایم عمدی، کسانی که به این حبس جنحه‌ای محکوم می شوند ظرف ۵ سال و کسانی که به حبس جنایی محکوم می شوند ظرف ۱۰ سال از تاریخ اتمام مجازات مذکور یا شمول مرور زمان، به اعاده حیثیت نائل می شوند و آثار تبعی محکومیت آنان زائل می‌گردد مگر اینکه به موجب قانون ترتیب دیگری مقرر شده باشد.» در مورد جزاهای تکمیلی یا اقدامات تأمینی مندرج در حکم، اعاده حیثیت و رفع محرومیت موکول به خاتمه اجرای آن‌ها یا شمول مرور زمان بود (تبصره ۱ ماده ۵۷) و در مورد جرایم قابل گذشت (تبصره ۲ ماده ۵۷) در صورتی که پس از صدور حکم قطعی با گذشت شاکی یا مدعی خصوصی اجرای مجازات موقوف می‌شد، محکوم‌علیه به اعاده حیثیت نائل می‌گردید.

طبق ماده ۵۷ «در مورد جرایم سیاسی کسانی که به مجازات‌های جنحه‌ای محکوم می‌شوند ظرف ۱ سال و کسانی که به مجازات‌های جنایی محکوم می‌شوند ظرف ۵ سال از تاریخ اتمام مجازات حبس یا شمول مرور زمان، در صورتی که محکومیت به جنایت و جنحه مؤثر جدید نداشته باشند، به اعاده حیثیت نائل می‌گردد مگر اینکه در قانون ترتیب دیگری مقرر شده باشد. «در این قانون نیز بازاجتماعی شدن محکومان، در مورد جرایم عادی طولانی‌تر از جرایم سیاسی می‌باشد.

قبل از قانون اصلاح دو ماده و الحاق یک ماده و تبصره به قانون مجازات اسلامی مصوب ۱۳۷۵ در قانون مجازات اسلامی ۱۳۷۰ در مورد اعاده حیثیت همانند مرور زمان ماده‌ای وجود نداشت، زیرا طبق مقررات جزایی اسلام علی‌الاصول فردی که مجازات خود را تحمل کند می‌تواند فوراً به جامعه برگردد و مسئله بازاجتماعی شدن یا اعاده حیثیت به شکل مطرح شده در حقوق جزای عرفی در قواعد شرعی مطرح نمی‌شد.

بنابراین، باید توجه کرد که قاضی می‌تواند در برخی موارد با مجازات‌های تتمیمی، کیفر اصلی را طولانی کند و بدین ترتیب بزهکار را از ورود به جامعه مدتی محروم سازد. طبق ماده ۱۹ قانون مجازات اسلامی مصوب ۱۳۷۰ «دادگاه می‌تواند کسی را که به علت ارتکاب جرم عمدی به تعزیر یا مجازات بازدارنده محکوم کرده است به عنوان تتمیمی حکم تعزیری یا بازدارنده مدتی از حقوق اجتماعی محروم و نیز از اقامت در نقطه یا نقاط معینی ممنوع یا به اقامت در محل معینی مجبور نماید.» همان‌گونه که ملاحظه می‌شود این مسئله به اعاده حیثیت ربطی ندارد؛ هرچند پس از مدت محرومیت می‌توان گفت که محکوم از اعاده حیثیت طبق اصول کلی برخوردار می‌گردد اما می‌توان استنباط کرد که در باب تعزیرات و مجازات‌های بازدارنده اگر کسی به مجازات ماده ۱۹ محکوم نشود بلافاصله با اجرای کیفر اصلی به اعاده حیثیت نائل می‌گردد. قانون اساسی در این مورد به اعاده حیثیت اشاره کرده که البته با آنچه در زمینه بازاجتماعی مجرم عنوان گردید، تفاوت دارد. طبق اصل ۱۷۱ «هرگاه در اثر تقصیر یا اشتباه قاضی در موضوع یا در حکم یا در تطبیق حکم بر مورد خاص، ضرر مادی یا معنوی متوجه کسی گردد، در صورت تقصیر، مقصر طبق موازین اسلامی ضامن است و در غیر این صورت خسارت به وسیله دولت جبران می‌شود و در هر حال از متهم اعاده حیثیت می‌گردد.» قانون روشن نساخته که ترتیب این اعاده حیثیت چگونه است.

ماده ۱۰ قانون مسئولیت مدنی مصوب ۱۳۳۹، در ارتباط با اعاده حیثیت می گوید: «کسی که به حیثیت و اعتبارات شخصی یا خانوادگی او لطمه وارد شود می‌تواند از کسی که لطمه وارد آورده است جبران زیان‌های مادی و معنوی خود را بخواهد. هرگاه اهمیت زیان و نوع تقصیر ایجاب نماید دادگاه می‌تواند در صورت اثبات تقصیر علاوه بر صدور حکم خسارت مالی حکم به رفع زیان از طریق دیگر از قبیل الزام به عذرخواهی و درج حکم در جراید و امثال آن نماید.»

۲-۱-۳-۲- اعاده حیثیت در قانون مجازات اسلامی مصوب ۹۲

در قانون مجازات اسلامی جدید، در دو مورد بحث اعاده حیثیت مطرح شده است

الف) ذیل فصل دوم این قانون که پیرامون مجازات‌های تکمیلی و تبعی است، تبصره دوم ذیل ماده ۲۶ مقرر می‌دارد: «هر کس به عنوان مجازات تبعی از حقوق اجتماعی محروم گردد پس از گذشت مواعد مقرر در ماده(۲۵) این قانون اعاده حیثیت می‌شود و آثار تبعی محکومیت وی زائل می‌گردد مگر در مورد بندهای(الف)، (ب) و(پ) این ماده که از حقوق مزبور به طور دائمی محروم می‌شود.»

ب) ذیل فصل ششم قانون مجازات اسلامی که پیرامون تکرار جرم است، ماده ۱۳۷ مقرر می‌دارد: «هر کس به موجب حکم قطعی به یکی از مجازاتهای تعزیری از درجه یک تا شش محکوم شود و از تاریخ قطعیت حکم تا حصول اعاده حیثیت یا شمول مرور زمان اجرای مجازات، مرتکب جرم تعزیری درجه یک تا شش دیگری گردد، به حداکثر مجازات تا یک و نیم برابر آن محکوم می‌شود.»

واضح است که این دو قانون، پاسخگوی مفهوم اعاده‌ی حیثیت در فضای حقیقی است و از آن‌جا که اثر جرم در فضای مجازی با اثر جرم در فضای حقیقی متفاوت بوده و علاوه بر گستره‌ی انتشار جرم در فضای مجازی، مانایی تأثیر جرم در این فضا، عملاً اعاده‌ی حیثیت در فضای مجازی را ناممکن می‌کند[1]، نمی‌توان از مجرم سایبری اعاده‌ی حیثیت نمود. فلذا دو قانون پیش‌گفته به این مسأله نپرداخته‌اند.

با مرور انجام شده در تمامی قوانین اعاده‌ی حیثیت، روشن می‌شود که در زمینه‌ی اعاده‌ی حیثیت در فضای مجازی با خلاء قانونی روبرو بوده و نیاز به وضع قوانینی در جهت پیشگیری و مجازات متناسب با جرم ارتکاب یافته ضروری می‌باشد.

[1] در فصل دوم این بخش، به تفصیل به چالش‌های اعاده‌ی حیثیت در فضای مجازی پرداخته‌ایم.

۲-۲- فصل دوم: چالش های اعاده حیثیت در فضای سایبر

شاکله بخش دوم پژوهش بر اعاده حیثیت از جرایم علیه حیثیت معنوی اشخاص در فضای سایبر بنیان شده است، همانطور که در بخش اول به اقتضاء مطالب بیان شد، اعاده حیثیت در فضای سایبر با صعوبت فراوان و گاه عدم امکان روبه‌روست، در فصل دوم از بخش دوم به چالش‌های این امر پرداخته شده است.

۲-۲-۱- گستره انتشار[۱]

اگرچه فضای سایبر و شبکه‌ی جهانی وب دو تعریف مجزا اما نزدیک به هم دارند، در یک نگاه کل به جزء می‌توان آن‌ها را هم‌ارز درنظر گرفت. شبکه‌ی جهانی وب (www)[۲] آن‌طور که از نام آن برمی‌آید، همچون یک تار عنکبوت گسترده است که در سرتاسر کره‌ی زمین تنیده شده و از همین رو شاید نتوان رسانه‌ای یافت که گستره‌ای وسیع‌تر از آن داشته باشد.

این گستردگی در بسیاری از موارد مستقل از شرایط است. این بدان معناست که تولیدکننده و یا انتشاردهنده‌ی یک مطلب در فضای سایبر هرچه قدر هم که خرد باشد، از گستره‌ی انتشاری، معادل با یک تولیدکننده و یا انتشاردهنده‌ی کلان برخوردار است. این خود یکی از وجوه قابل تأمل در ارتباط با ارتکاب جرایم در فضای سایبر است. چه این که رسانه‌های کلان به جهت حیثیت و اعتباری که دارند، برای ارتکاب جرایم، انگیزه‌ی کمتری داشته و از کاسته شدن اعتبار خود واهمه دارند. اما رسانه‌های خرد چنین ملاحظه‌ای ندارند و لذا می‌توانند نسبت به ارتکاب جرم، بالقوه جرأت بیشتری داشته باشند.

گستردگی بی‌حدوحصر در انتشار اخبار، اطلاعیه‌های عمومی و پیام‌های شخصی، فیلم‌ها و تصاویر در فضای مجازی بدین معنی نیست که هرکس به همه چیز دسترسی دارد، اما هرکس که اراده کند مطلبی را در سرتاسر فضای وب نشر دهد، قطعاً کار دشواری نخواهد داشت.

---

۱ propagation range

۲ World Wide Web

پیام‌های اینترنتی می‌توانند از نوع تک‌فرستنده – تک‌گیرنده[1] باشند. برای مثال وقتی دو نفر با هم چت می‌کنند، با مسامحه می‌توان گفت که فقط همان دو نفر پیام را می‌بینند (لفظ با مسامحه از آن رو استفاده شده که سرویس‌دهنده‌ی ابزار چت و احیاناً شنودکننده‌ها[2] نیز می‌توانند به پیام دسترسی داشته باشند.)

نوع دیگر پیام در فضای سایبر از نوع تک‌فرستنده به تمام گیرندگان یا همان انتشار عمومی است. برای مثال خبری که در خروجی یک سایت خبرگزاری یا پایگاه اطلاع‌رسانی درج می‌شود، برای همه قابل رؤیت خواهد بود. باز این بدان معنا نیست که همه آن را می‌بینند، بلکه همه می‌توانند آن را ببینند.

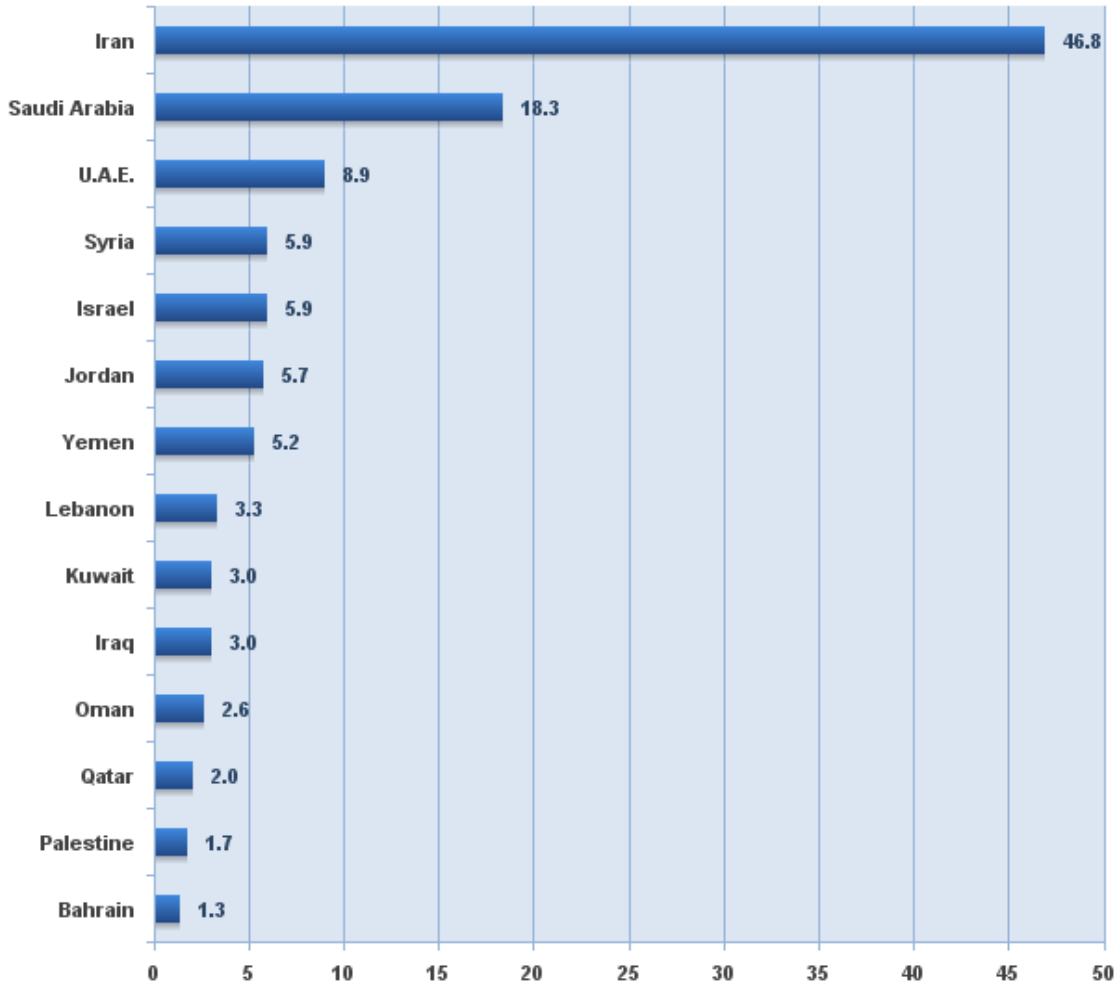
از آن‌جا که جرایم مورد نظر در این پایان‌نامه، «جرایم علیه حیثیت معنوی اشخاص» می‌باشد، علی-القاعده مجرم یا مجرمین، بیشتر مایلند از پیام‌های نوع دوم، یعنی پیام‌هایی که توسط یک فرستنده (خود مجرم) روی شبکه‌ی جهانی وب قرار گرفته و برای تمام کاربران اینترنت قابل رؤیت باشد، استفاده کنند. نکته‌ی قابل ملاحظه‌ی دیگر آن است که ضریب نفوذ اینترنت در تمام دنیا و همچنین در کشور ما در حال رشد است. این بدان معناست که گستره‌ی انتشار فضای سایبر اگرچه بسیار وسیع است، اما در همین حد هم نخواهد ماند و روزبه‌روز گسترده‌تر خواهد شد. این مسأله بر پیچیدگی بررسی وقوع جرم در این فضا می‌افزاید.

آمارها نشان می‌دهد که ایران در دی ماه ۱۳۹۳ با ۴۶,۸ بیشترین درصد استفاده‌کنندگان از اینترنت را در منطقه خاورمیانه (غرب آسیا) داشته است.

---

۱ end to end

۲ Sneefer



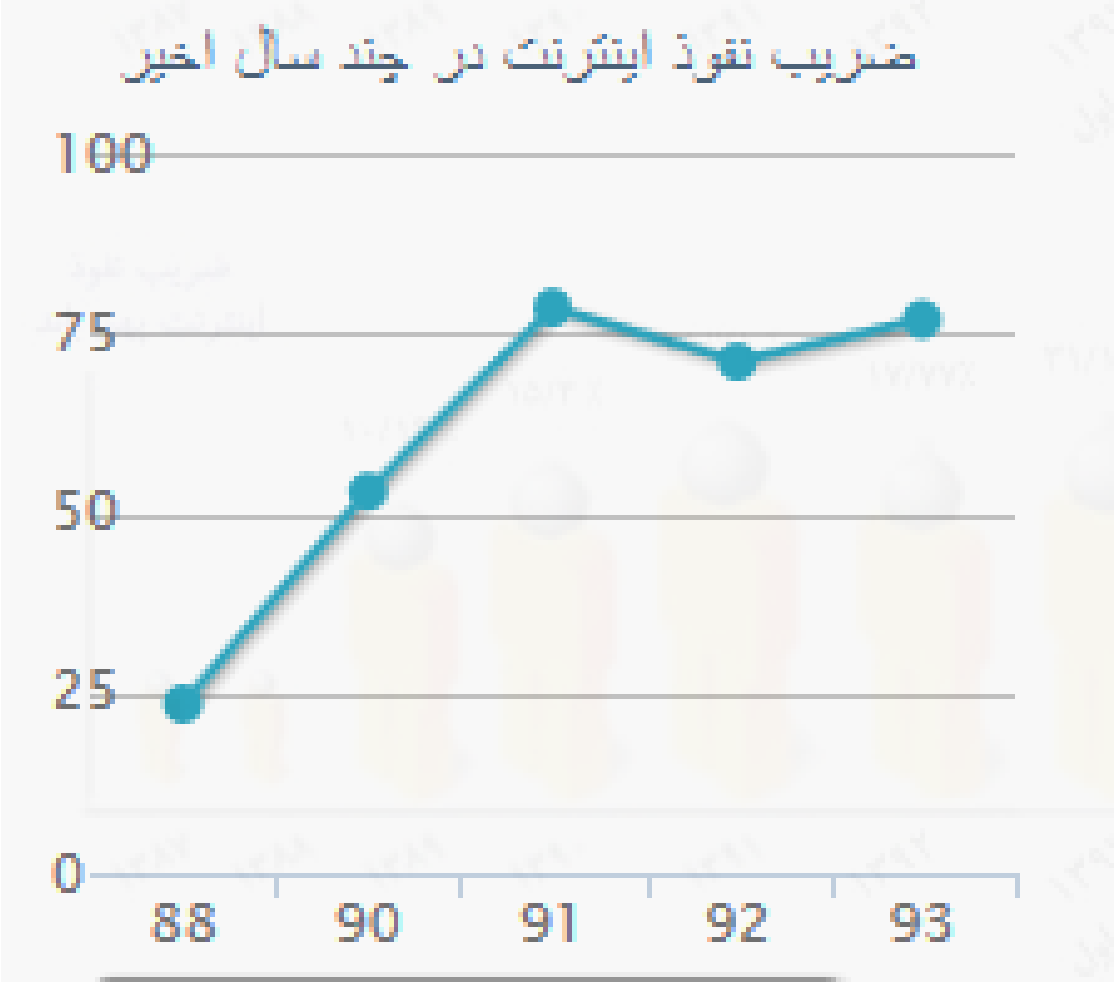
نمودار شماره ۱، درصد کاربران اینترنت در خاورمیانه (غرب آسیا) – ۳۱ دسامبر ۲۰۱۴ (۹۳/۱۰/۱۰ شمسی)[۱]

غیر از درصد کاربران، ضریب نفوذ اینترنت[۲]، شاخصی جهانی برای مطالعه‌ی درصد کاربران فعال فضای مجازی است. ضریب نفوذ اینترنت، اگرچه تعاریف مختلفی دارد، اما در تعریف سازمان فناوری اطلاعات ایران، «کاربر اینترنت کسی دانسته می‌شود که دست کم در یک سال گذشته یک بار به اینترنت متصل شده و از آن استفاده کرده باشد.»[۳]

[۱] این آمار توسط وبسایت جهانی آمار در فضای مجازی www.internetworldstats.com منتشر شده است. بدیهی است که رژیم غاصب صهیونیستی از منظر نگارنده کشور محسوب نمی‌شود.

[۲] Internet Penetration Rate

[۳] وزارت بازرگانی ایالات متحده آمریکا کاربر اینترنت را کسی می‌داند که دست کم سه سال سن دارد و *در حال حاضر* از اینترنت استفاده می‌کند.



نمودار شماره ۲، میزان ضریب نفوذ اینترنت در سال‌های اخیر

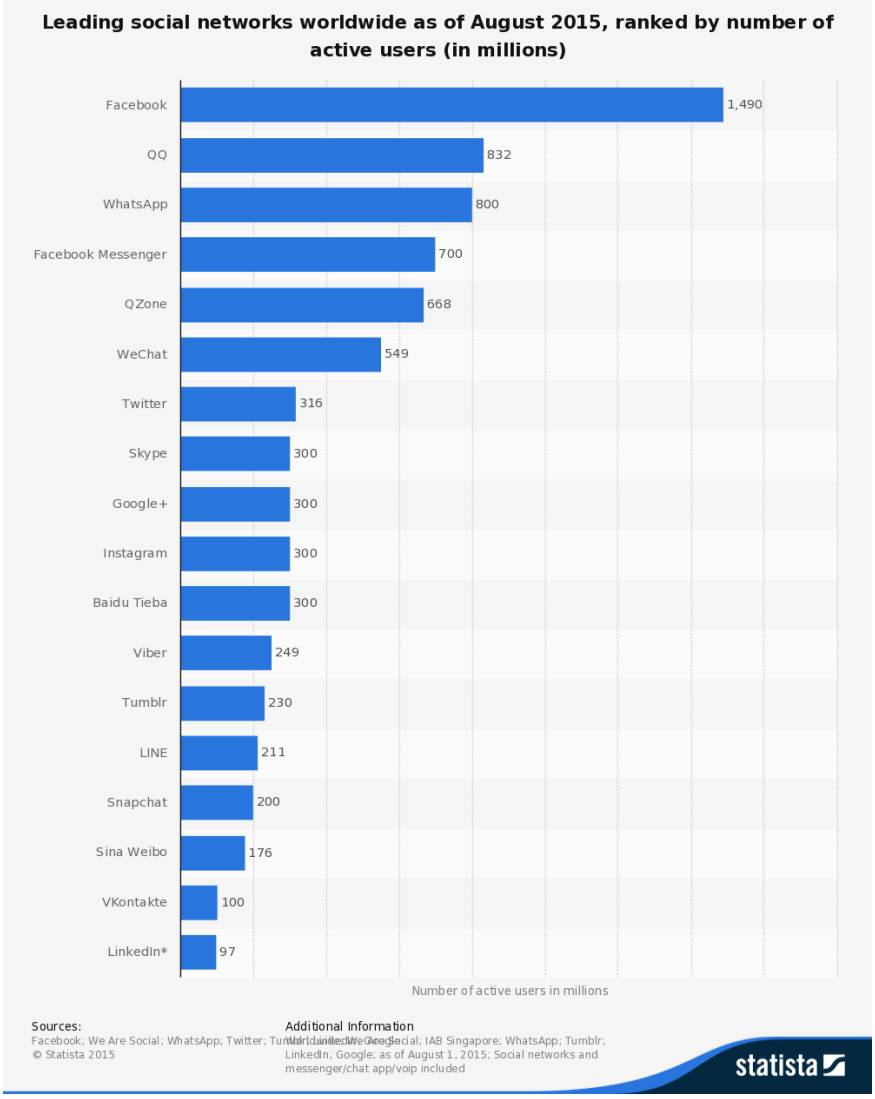
علاوه بر موضوع افزایش ضریب نفوذ اینترنت، امروزه ابزارها، سایت‌ها و امکاناتی برای کمک به انتشار قوی‌تر و گسترده‌تر پیام‌ها به وجود آمده‌اند که شبکه‌های اجتماعی، پایگاه‌های بارگذاری فیلم و عکس و خبرخوان‌ها از این دسته‌اند. برای فهم بهتر این موضوع مثالی می‌زنیم. فرض کنید شخصی در وسط یک اجتماع بزرگ مردمی با صدای بلند اقدام به توهین به شخصی نماید، یا از قول او مطلبی نقل کند که او نگفته باشد و یا هر کار دیگری که جرم علیه حیثیت معنوی تلقی گردد. این جرم اگرچه در علن صورت می‌گیرد، اما همه متوجه آن نمی‌شوند. حال فرض کنید او بتواند از امکانی مانند بلندگو برای انتشار سخن خویش استفاده کند. در این صورت پیام به جمعیت بسیار بیشتری می‌رسد و جرم ابعاد وسیع‌تری پیدا می‌کند.

استفاده از شبکه‌های اجتماعی و یا خبرخوان‌ها دقیقاً مانند همان بلندگو عمل می‌کند. یعنی پیام یا فیلم یا عکس که در اینترنت منتشر شده را در قالب‌های ساده‌تر و با قدرت نشر بیشتری در معرض عموم می‌گذارد. چه این که آن‌ها بیشتر در معرض استفاده‌ی عموم هستند و ممکن است تعداد کاربرانی که به آن‌ها رجوع می‌کند، چند برابر یک تولیدکننده یا انتشاردهنده‌ی معمولی باشد.

در حال حاضر شبکه‌های اجتماعی متعددی به زبان‌ها و با کارکردهای مختلف وجود دارند که از مهم‌ترین آن‌ها می‌توان به فیسبوک[۱]، توییتر[۲] و اینستاگرام[۳] اشاره کرد. برخی از این شبکه‌های اجتماعی گستره کاربران توزیع شده‌تری[۴] دارند، مانند فیسبوک و برخی اغلب کاربرانشان در یک یا دو کشورند، مانند شبکه اجتماعی کیوکیو[۵] که اغلب کاربرانش چینی هستند.

۱ Facebook
۲ Twitter
۳ Instagram
۴ distributed
۵ QQ

جدول زیر نام و تعداد کاربران ۱۸ شبکه اجتماعی پر مخاطب دنیا را نشان داده است. لازم به ذکر است اعداد درون جدول بر حسب میلیون هستند، به عنوان مثال، وایبر[۱] در دنیا ۲۴۹ میلیون کاربر دارد که در خط دوازدهم جدول نشان داده شده است.



نمودار شماره ۳، پربیننده ترین شبکه‌های اجتماعی دنیا

[۱] Viber

۲-۲-۲- سرعت و بلادرنگی[۱]

یکی از ویژگی‌های اختصاصی فضای سایبر به عنوان یک رسانه و رسانه‌های بزرگ و کوچکی که بر بستر آن فعالند، سرعت و بلادرنگی است. اقدام یا فعالیتی بلادرنگ نامیده می‌شود که در مقیاس نانوثانیه انجام پذیرد و هر نانوثانیه معادل یک میلیاردم ثانیه است.

ناگفته پیداست که هرچه فاصله‌ی تولید تا انتشار یک پیام اعم از متن، فیلم و یا عکس کمتر باشد، فرصت کمتری برای پیشگیری از وقوع جرم وجود خواهد داشت. در مورد رسانه‌های برخط[۲] این امکان تقریباً به صفر می‌رسد و شاید بتوان گفت پیشگیری نشدنی است.

غیر از این نکته، می‌توان به افزایش انگیزه‌ی مجرم در ارتکاب جرم به جهت سرعت بالا در انجام جرم اشاره کرد. وقتی مقدمات وقوع جرم مفصل و زمان‌بر باشد، انگیزه‌ی درونی افراد برای انجام جرم کمتر شده و ترس از ارتکاب جرم در فرد افزایش پیدا می‌کند. حال اگر مقدمات وقوع جرم بسیار کم باشد- مثلاً در حد اتصال اینترنت- و تنها وسیله‌ی مورد نیاز برای ارتکاب جرم یک رایانه شخصی یا تلفن همراه هوشمند باشد، جرئت مجرمین برای ارتکاب جرم افزایش پیدا می‌کند.

نمونه‌ها در این مورد متعدد است. فرض کنید شایعه‌ای به اشتباه در میان برخی مردم و مسئولین مطرح شود که یکی از افراد تأثیرگذار جامعه از دنیا رفته است یا بیماری صعب‌العلاج دارد و به زودی درخواهد گذشت. قطعاً انتشار عمومی این شایعه توسط یک رسانه، از آن رو که موجب تضعیف جایگاه او در جامعه است، جرم محسوب می‌شود. بارها در کشور خودمان و در سایر کشورها، شب قبل از چاپ چنین مطالبی، مأمورین قضایی با حضور در چاپخانه، مانع از چاپ مطلب کذب شده و از واردشدن یک شوک

---

۱ Real- time
۲ Online

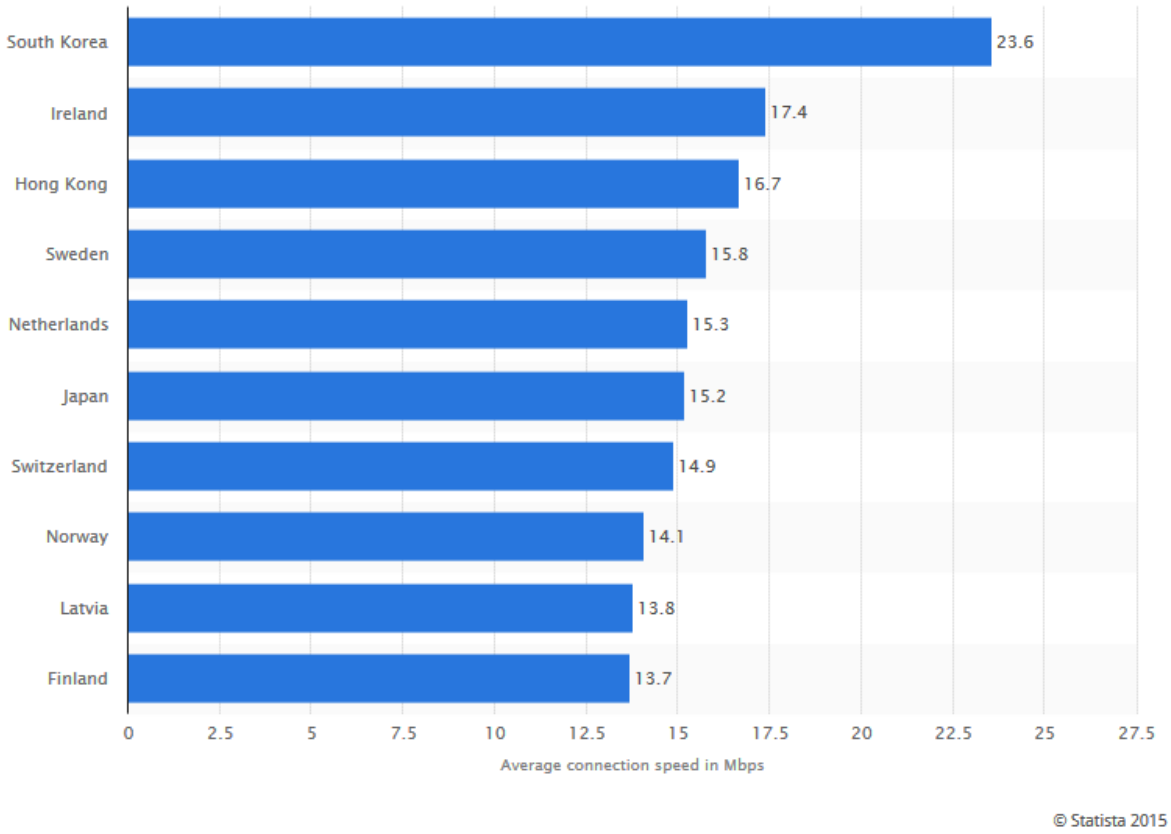
روانی به جامعه جلوگیری کرده‌اند. حال آنکه چنین کاری در موارد مشابه در رسانه‌های فضای سایبر قابل جلوگیری نیست.

در واقع توهین، افترا و خبر کذب در فضای سایبر، همچون تیری که از کمان رها شده باشد، سریع عمل می‌کند. چنین جرایمی نه تنها قابلیت پیش‌گیری و جلوگیری ندارند، بلکه پس از وقوع هم، آن‌طور که می‌شود با جرایم علیه حیثیت معنوی در رسانه‌های مکتوب مقابله کرد، در مورد رسانه‌های مجازی چنین امکانی وجود ندارد. به عنوان مثال، اگر روزنامه‌ای جرمی مرتکب شود که حیثیت معنوی شخصی یا اشخاصی را در معرض تهدید جدی قرار دهد، می‌توان روزنامه را از روی دکه‌های سطح شهرها جمع‌آوری نمود تا آسیب آن بیشتر نشود. اما در مورد رسانه‌های مجازی چنین کاری ممکن نیست. به فرض که یک پایگاه خبری شناسنامه‌دار، ناشر محتوای مجرمانه باشد. می‌توان طبق قانون از مسئولین آن خواست تا خبر حاوی محتوای مجرمانه را از خروجی خود بردارند، اما آن‌قدر این خبر توسط سایت‌های نامدار و گمنام دیگر نقل شده و در خبرخوان‌ها و شبکه‌های اجتماعی باز نشر می‌شود که حذف آن از خروجی یک پایگاه اطلاع‌رسانی تأثیری نداشته باشد.

غیر از سرعت بالای انتشار، مسئله‌ی دیگر، سرعت انتقال مطالب در فضای سایبر است. پست‌های الکترونیک در چند ثانیه و گاهی در واحدهای زمانی کمتر از ثانیه داده‌ها را منتقل می‌کند. داده‌هایی که ممکن است حاوی محتوای مجرمانه هم باشند.

سرعت اینترنت در نقاط مختلف دنیا بعضاً وابسته به سیاست‌های فرهنگی و بعضاً بسته به امکانات و سطح پیشرفت علم و تکنولوژی متفاوت است.

در نمودار پیش رو کشورهای با بیشترین سرعت اینترنت در دنیا به ترتیب مشخص شده‌اند.



نمودار شماره ۴، کشورهای دارای پرسرعت‌ترین اینترنت دنیا

کره‌جنوبی با میانگین سرعت ۲۳,۶ مگابیت در ثانیه دارای پرسرعت‌ترین اینترنت دنیاست.

در کشور ما نیز رشد سرعت اینترنت، بسیار بالا بوده ولی همچنان در رده کم سرعت‌ترین اینترنت‌های جهان به سر می‌برد.

۲-۲-۳- گمنامی عامل[۱]

گمنامی در اصطلاح فضای سایبر، به معنای عدم امکان دسترسی به هویت و مشخصات تولیدکننده و یا نشردهنده‌ی یک محتوا، اعم از متن، فیلم و یا عکس است. معنای این مطلب آن نیست که عامل انتشار اولیه و یا بازنشر هیچ محتوایی در فضای سایبر مشخص نیست، بلکه اگر عاملی بخواهد هویت خود را پنهان نگاه دارد، این کار چندان دشوار نخواهد بود.

ویژگی گمنامی، خاص رسانه‌های خرد فضای سایبر مانند وبلاگ‌ها، پست‌های الکترونیک و فعالیت در شبکه‌های اجتماعی بوده و قابل انطباق بر رسانه‌های کلان مانند خبرگزاری‌ها، پایگاه‌های اطلاع‌رسانی و پورتال‌های رسمی نیست.

یکی از راه‌های ایجاد گمنانی استفاده از پراکسی‌ها[۲] است. پراکسی‌ها به گونه‌ای عمل می‌کنند که کاربر پس از اتصال به آن، ردی از خود به جا نمی‌گذارد و دیگران آثار کار او را، آثار پراکسی می‌بینند. در واقع پراکسی دیواری است که عامل از پشت آن اقدام به فعالیت در فضای سایبر می‌نماید و دیگران فقط دیوار را می‌بینند. وی‌پی‌ان[۳] نوع دیگری از اتصال به اینترنت است که کاربرد مشابهی دارد.

انواعی از پروتکل‌های اینترنتی وجود دارند که موجب گمنامی عامل را فراهم می‌سازند. تأمین گمنامی عامل یکی از شاخه‌های علم امنیت اطلاعات[۴] است و ذاتاً مذموم نیست، بلکه استفاده‌هایی از این ویژگی فضای سایبر می‌شود که می‌تواند مخرب و مجرمانه باشد.

در چند گزارش که پس از کشف حمله‌ی ویروس استاکس نت[۵] به تأسیسات اتمی ایران منتشر شده بود، در بخش‌هایی از حمله به اطلاعات و داده‌های حساس تلاش شده بود تا پس از آن سابقه‌ی کار[۶] از

---

۱ Annonymity
۲ Proxy
۳ VPN
۴ Information Security
۵ Staxnet
۶ log

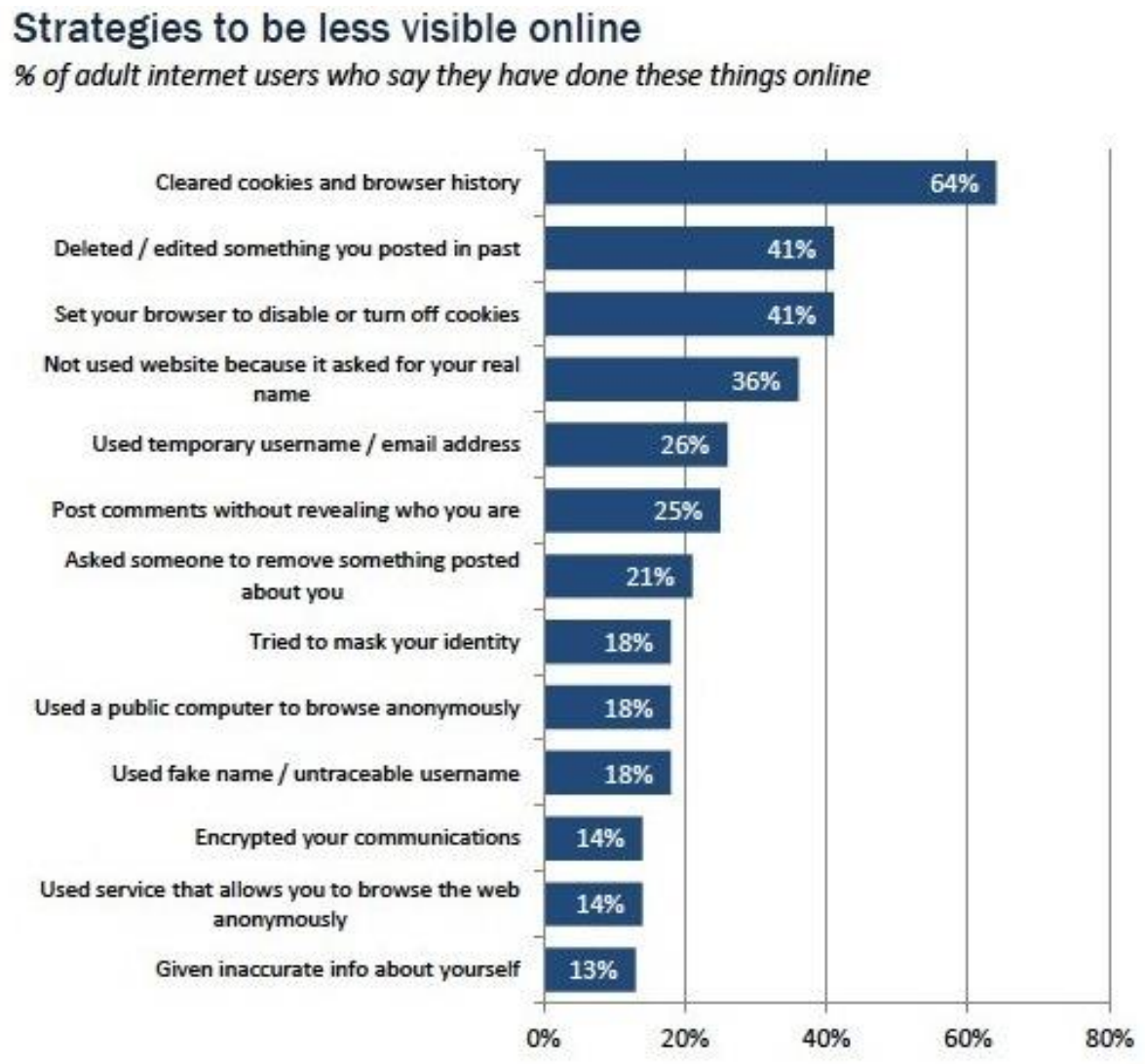
سامانه‌های اطلاعاتی ایران پاک شود و به همین دلیل شناسایی این فعالیت مخرب ماه‌ها به تأخیر افتاد. این در واقع یک نمونه‌ی عینی تلاش برای گمنامی عامل در یک حمله‌ی مخرب سایبری است.

نمونه‌های فراوانی از جرم علیه حیثیت معنوی در فضای سایبر وجود دارند که پایه‌ی اصلی آن‌ها گمنانی عامل بوده است. انتشار تصاویر خصوصی زندگی اشخاص مشهور در وب‌سایت‌های ثبت نشده و بی‌شناسنامه‌ی اینترنتی نوعی شایع از این جرم است.

ارسال انبوه پست‌های الکترونیک که منبع اولیه آن‌ها روشن نیست و در آن‌ها محتوای مجرمانه‌ای علیه حیثیت معنوی اشخاص منتشر شده نمونه‌ای دیگر است. گاهی نیز مانند آنچه در شبکه‌های اجتماعی رخ می‌دهد، یافتن عامل شدنی است اما آن‌قدر مطلب دست به دست شده که عملاً پیدا کردن عامل و منشأ اولیه خبر اگر نگوییم نشدنی است، لااقل بسیار دشوار و زمان‌بر خواهد بود.

به غیر از مجرمین فضای سایبر، جذابیت گمنامی، ترس، کنجکاوی و ... سبب می‌شود برخی کاربران عادی فضای اینترنت نیز علاقه‌مند به گمنام بودن در این فضا باشند.

در نمودار زیر که نتایج حاصل از آن مربوط به یک نظرسنجی اینترنتی است، حدود ۸۶ درصد از کاربران اینترنت علاقه‌ای به رصد[۱] و دنبال شدن در این فضا ندارند و دوست دارند به عنوان یک شخصیت گمنام در فضای اینترنت حضور داشته باشند. برای این کار این افراد از پاک کردن کوکی‌ها[۲] و تاریخچه[۳] تا تغییرات تنظیمات پیش‌فرض رایانه خود، ساختن ایمیل با نام جعلی و ... انجام می‌دهند.



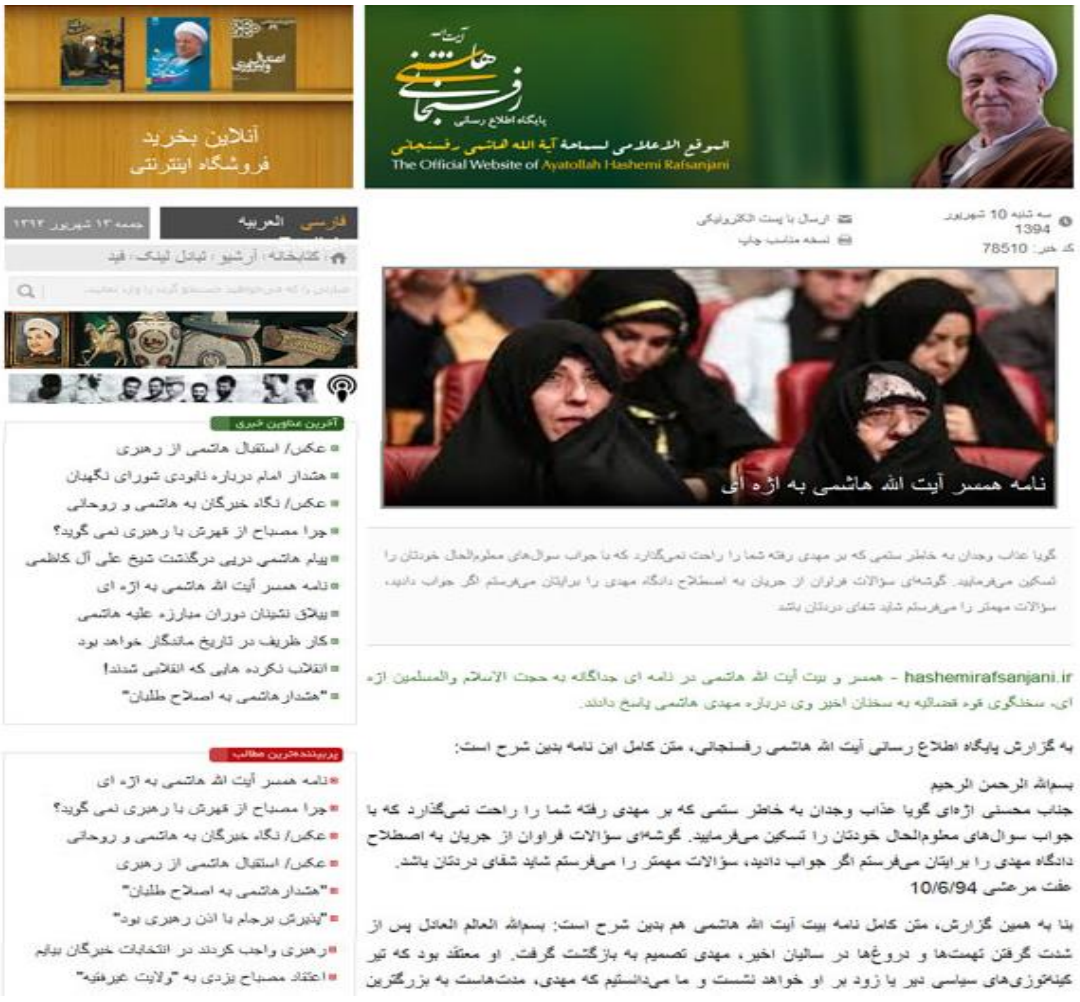
نمودار شماره ۵، اقدامات برای گمنام ماندن در فضای اینترنت

[۱] track
[۲] cookies
[۳] history

۲-۲-٤- مانایی محتوا در فضای سایبر

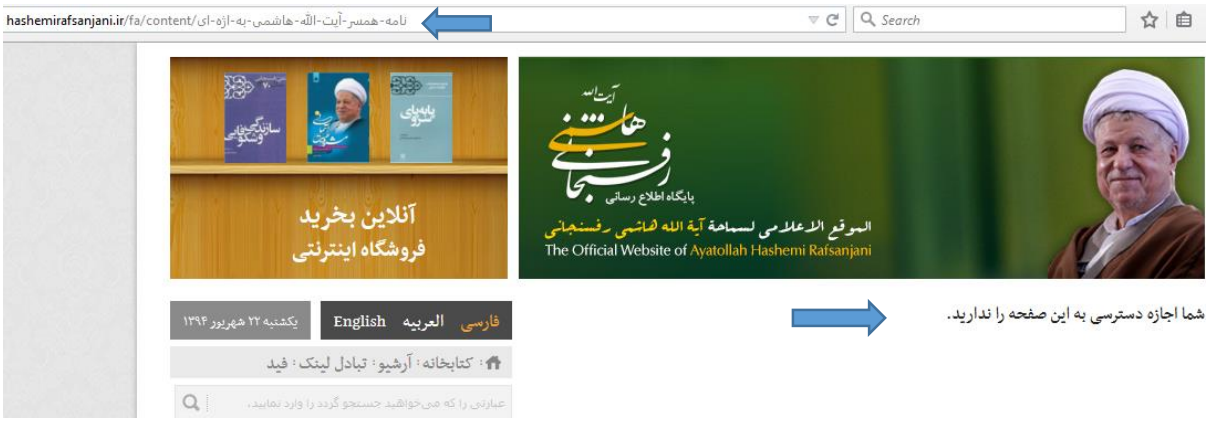
انتشار یک مطلب اعم از محتوای متنی، کاریکاتور، فیلم و یا عکس در اینترنت موجب مانایی آن مطلب در اینترنت می‌شود. حتی اگر منشاء اولیه انتشار محتوا، مطلب منتشره را از خروجی خود حذف کند، آن‌قدر این مطلب در فضای وب بازنشر شده که اصل مطلب از بین نرود و قابل یافتن باشد.

به عنوان نمونه در تاریخ ده شهریور ۹۴، خانم عفت مرعشی همسر حجت‌الاسلام هاشمی رفسنجانی نامه‌ای به جناب آقای محسنی اژه‌ای معاون اول و سخنگوی قوه قضاییه نوشت. پایگاه اطلاع –رسانی حجت-الاسلام هاشمی رفسنجانی متن نامه را بر خروجی وبسایت خود قرار داد ولی بعد از واکنش جناب آقای اژه‌ای و ارجاع این نامه به دادستان تهران اقدام به حذف این نامه از روی سایت خود نمودند.



تصویر شماره ۷، تصویر خبر پایگاه اطلاع‌رسانی حجت‌الاسلام هاشمی رفسنجانی

لیکن مانایی محتوا در این فضا باعث شد، این خبر در فضای مجازی باقی بماند.



تصویر شماره ۸، صفحه خبر حذف شده از پایگاه اطلاع‌رسانی حجت‌الاسلام هاشمی رفسنجانی

در نمونه‌ای دیگر می‌توان به حذف یک خبر از مرجع اصلی خبر اشاره کرد که به واسطه بازنشر در سایر رسانه‌ها در فضای مجازی مانایی یافته است.

خبر محکومیت قطعی داشتن حمید رسایی در دادگاه روحانیت، که توسط وکیل مهدی هاشمی بیان شده بود، از خروجی سایت خبرگزاری ایرنا حذف شد، ولی به واسطه بازنشر گسترده حتی پس از حدود ۸ ماه از حذف این خبر از مرجع اصلی هنوز در سایت‌های دیگر باقی مانده است.

تصویر شماره ۹، صفحه خبر حذف شده از وبسایت خبرگزاری جمهوری اسلامی (ایرنا)

تصویر شماره ۱۰، صفحه خبر وبسایت قدس‌آنلاین

یک مثال روشن دیگر از این موضوع RSS-R[1] است. RSS-R ها پایگاه‌های اینترنتی هستند که به محض انتشار یک مطلب در سایت‌ها، لینک و بخشی از محتوای آن را بر روی سرورهای خود ذخیره کرده و در خروجی خود نمایش می‌دهند. حتی اگر اصل محتوا از سایت اولیه حذف شده باشد، لینک و بخشی از محتوا به صورت دائمی در RSS-R ها قابل مشاهده‌اند.

[1] Rich Site Summary-Reader

برخی RSS-R ها به دلایل مختلف تمام محتوا را ذخیره می‌کنند و حتی پس از حذف این مطلب از منبع اصلی به صورت تمام و کمال کل خبر را در خود نگهداری می‌کنند.[۱]

بارها اتفاق افتاده که دولت‌های مقتدر دنیا در عرصه فضای مجازی تصمیم به حذف کامل یک محتوا از اینترنت گرفته‌اند و موفق نشده‌اند. به عنوان نمونه، دولت آمریکا بارها تلاش کرده که از انتشار تصاویر قربانیان بلایای طبیعی جلوگیری کند. در طوفان نیواورلئان[۲] که تصویر تعدادی از قربانیان توسط یک رسانه محلی منتشر شد، با وجود برخورد دولت و حذف مطلب از رسانه، آن تصاویر آن‌قدر انتشار و بازتاب پیدا کرد که دولت آمریکا تصمیم گرفت، در مواقع بحرانی، کمیته نظارت ویژه‌ای بر انتشار اخبار بحران تشکیل دهد؛ کمیته‌ای که پیش از انتشار هر مطلب آن را تأیید کند. از آن پس، در بحران‌های متعددی که در ایالات متحده آمریکا روی داده، می‌توان گفت، که با جستجو در اینترنت به ندرت شاهد تصویر ناراحت کننده‌ای از قربانیان خواهیم بود که مثالی از کار این کمیته ویژه، نظارت بر انتشار اخبار و تصاویر طوفان کاترینا[۳]ست.

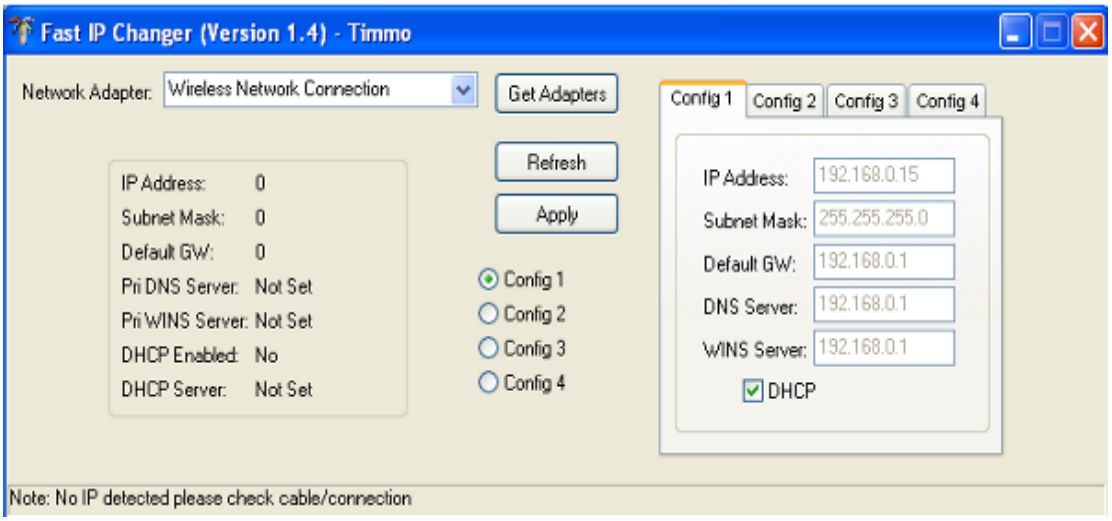
۲-۲-۵- یافتن مجرم

گاهی اوقات عامل انتشار یک خبر، رویداد، عکس و یا فیلم، مشخص است، اما یافتن او کار آسانی نیست. شاید بتوان این مطلب را این طور بیان کرد که در جرم سایبری عملاً محل وقوع جرم وجود ندارد. مجرم در فضای مجازی مرتکب جرم می‌شود، اما باید در فضای حقیقی و فیزیکی تعقیب شود و این در بسیاری از موارد ممکن نیست.

---

۱ Crawl
۲ New Orlean
۳ Katrina

در فضای سایبر هر دستگاهی که به اینترنت متصل می‌شود دارای یک شناسه‌ی عددی یا همان IP است[1]. این شناسه همانند کد ملی افراد یکتاست و هیچ دو دستگاهی که به اینترنت متصل می‌شوند، IP یکسان ندارند. از این رو مانند اثر انگشت عمل می‌کند و در واقع کمکی برای یافتن مجرم است.



عکس شماره ۱۱، تصویر نرم افزار تغییر IP

مجرمین سایبری از ابزارهایی مثل نرم‌افزار فوق برای تغییر موقعیت و مختصات ثبت شده خود بهره می‌برند که این امر برای یافتن مجرم، چالش مهمی ایجاد خواهد کرد.

متخصصان از روی کد شناسه‌ی یک دستگاه می‌توانند کشور، شهر و حتی حدود منطقه‌ی آن را بفهمند اما این کار با چالش‌هایی روبروست:

الف) قطعاً فردی که می‌خواهد عمل خلافی انجام دهد، مثلاً علیه حیثیت معنوی شخصی دیگر عکس و یا فیلمی منتشر کند این کار را از رایانه شخصی و یا محل کار خود انجام نمی‌دهد.

ب) ایراد اصلی این‌جاست که هر رایانه یک شناسه دارد و نه هر فرد. مثلاً اگر یک رایانه در یک محل عمومی مانند کافی‌نت باشد، روزانه ده‌ها نفر از آن استفاده می‌کنند و مشخص نیست اگر از طریق آن جرمی صورت پذیرفت، باید به سراغ چه کسی رفت.

---

[1] Internet Protocol

ج) مسئله‌ی دیگر آن است که در هر ساعت صدها جرم در فضای سایبر صورت می‌گیرد که بالقوه قابل تعقیبند اما در عمل به دلیل هزینه‌ی بالا، همه‌ی جرایم تعقیب نمی‌شوند. به همین دلیل است که پلیس‌های سایبری دنیا - در ایران پلیس فتا[1]- عموماً جرایم سایبری مهم‌تر مانند سرقت اطلاعات حساس سازمان‌ها، سرقت حساب کاربری افراد در بانک‌ها و جرایم علیه حیثیت معنوی چهره‌های شاخص را پیگیری می‌کنند و بسیاری از جرایم علیه حیثیت معنوی اشخاص معمولی تعقیب نمی‌شوند. این بدان معنا نیست که قابل تعقیب نیستند، بلکه آن‌قدر جرایم سایبری، گسترده و پرتعداد هستند که عملاً چنین جرایمی در اولویت بالایی قرار نمی‌گیرند.

در تفاوت یافتن مجرم و گمنامی عامل می‌توان گفت: گاهی اوقات، عامل[2] انجام‌دهنده یک کار یا منتشر کننده یک محتوا در فضای مجازی مشخص نیست. حتی مشخص نیست که عامل انتشار محتوا، یک انسان است یا یک ربات. در این صورت ویژگی گمنامی عامل است که برجسته می‌شود و مورد نظر است. اما گاهی عامل انجام کاری در فضای مجازی مشخص است ولی با توجه به ویژگی‌های شناسنامه‌ای مجازی، نمی‌توان او را به صورت یکتا در دنیای واقعی پیدا کرد. این مشکلی است که بسیاری از کشورها برای حل آن به سمت شبکه ملی داده رفته‌اند که در کشور ما هم این موضوع در دست بررسی و اقدام است.

---

۲ فتا مخفف فضای تبادل اطلاعات است.

[2] Agent

۲-۲-٦- پیشگیری

همان‌طور که پیش از این گفته شد، جرایم سایبری بسیار سریع و بلادرنگ به وقوع می‌پیوندند. از طرف دیگر این جرایم بسیار ساده قابل ارتکابند و نیاز به مقدمات مفصل و تجهیزات خاص ندارد. این دو مورد باعث می‌شود که جرایم سایبری عملاً قابل پیشگیری به صورت کامل نباشند.

به عنوان مثال فرض کنید مجرم می‌خواهد یک عکس از زندگی خصوصی فرد دیگری را در فضای عمومی نشر دهد. او می‌تواند به یک کافی‌نت مراجعه کرده و عکس مورد نظر را از روی حافظه‌ی فلش یا لوح فشرده‌ای که همراه خود دارد روی رایانه ذخیره کرده، با اتصال به اینترنت ظرف یک دقیقه یک وبلاگ راه‌اندازی کرده و تصویر مورد نظر را روی وبلاگ بارگذاری کند. این مثال کوچکی از چنین جرایمی است. حتی رسانه‌های بزرگ فضای سایبر هم می‌توانند جرایمی مرتکب شوند که عموماً قابل پیشگیری نیستند. یک مثال روشن این نکته اتفاقی است که بهار ۹۴ در سایت خبری «الف» رخ داد. در بخش نظرات[1] خوانندگان ذیل چند خبر، مطالبی توسط خوانندگان سایت ارسال شده بود که جرم علیه حیثیت معنوی اشخاص تلقی می‌شد. این مطالب پس از انتشار به بسیاری از وب‌سایت‌ها و وبلاگ‌ها و شبکه‌های اجتماعی راه یافته و حتی پس از آن که از سایت اولیه که مبدأ جرم بوده حذف شد، محتوای مجرمانه و آثار آن در فضای سایبر باقی ماند.

اگر به انواع پیشگیری در جرم‌شناسی نگاهی گذرا کنیم، پیشگیری غیر کیفری که مبتنی بر اتخاذ تدابیری با ماهیت غیر کیفری و در جهت پیشگیری از بزه و نه تکرار آن است محل بحث این پژوهش است وگرنه در فضای سایبر، پیشگیری کیفری که به منظور پیشگیری از تکرار جرم است آنچان که شایسته است نه موجبات تأدیب بزه‌کاران را فراهم می‌کند و نه دردی از دردهای بزه‌دیده تسکین می‌یابد. فلذا می‌بایست برای این

[1] Comment

چالش مهم فضای مجازی که سختی و صعوبت پیشگیری است، اقدامات اساسی اجتماعی و فرهنگی انجام داد.

۲-۲-۷- احراز اصالت[۱]

احراز اصالت به معنی تعیین و اثبات عامل حقیقی انجام یک عمل است. گاهی اوقات این مفهوم با گمنامی عامل اشتباه گرفته می‌شود در حالی که تقریباً این دو مفهوم عکس یکدیگرند. ویژگی گمنامی عامل یعنی در یک تراکنش[۲]، عامل انجام یک کار می‌تواند اگر بخواهد هویت خود را مخفی نگه دارد. احراز اصالت یعنی آن که عامل انجام یک کار یعنی فرستنده‌ی یک پیام متنی یا صوتی یا تصویری، چگونه به گیرنده اثبات کند که فرستنده همان خود واقعی اوست و این پیام توسط شخص دیگری ارسال نشده است.

در فضای سایبر پروتکل‌هایی برای احراز اصالت وجود دارد که عموماً قراردادهایی امریکایی یا اروپایی هستند. به عنوان مثال سردبیر یک سایت خبری حرفه‌ای وقتی می‌خواهد از طریق یک نرم‌افزار اینترنتی به یکی از اعضای هیئت تحریریه مطلبی ارسال کند تا در سایت منتشر کند، به مثابه یک کاربر معمولی نباید این عمل را انجام دهد چرا که ممکن است شخص دیگری با سرقت اطلاعات پست الکترونیک وی، پیام دیگری برای انتشار ارسال کند، وی نیاز دارد به نحوی به طرف مقابل (عضو هیئت تحریریه) اثبات کند که او به عنوان فرستنده، همان سردبیر اصلی سایت است. به این کار احراز اصالت می‌گویند.

امضای الکترونیک، یکی از راه‌های احراز اصالت است که کمتر در فضای مجازی و به خصوص فضای رسانه بهره‌گیری می‌شود.

---

۱ Auttentication
۲ transaction

۲-۲-۸- سادگی انجام جرایم سایبری

یکی دیگر از ویژگی‌های فضای سایبری که مجرمین را به ارتکاب جرم ترغیب می‌کند، سادگی انجام جرم است. به عنوان مثال، سرقت اطلاعات بانکی یک کاربر و خالی کردن حساب او از سرقت فیزیکی از یک بانک کار بسیار ساده‌تری است و احتمالاً ریسک و خطر کمتری دارد. دقیقاً مشابه همین، مثال‌هایی در جرایم علیه حیثیت معنوی اشخاص هم برقرار است. مثلاً کسی که می‌خواهد در فضای سایبر و از طریق یک وبلاگ، به شخص دیگری توهین کند، معمولاً نسبت به فردی که در دنیای واقعی توهین می‌کند نگرانی کمتری دارد، در حالی که انتشار یک توهین در فضای سایبر به عنوان یک فضای عمومی قطعاً تخریب بیشتری نسبت به حیثیت معنوی شخص وارد می‌کند.

نکته مهم دیگر فراوانی بیشتر جرایم سایبری نسبت به فضای واقعی است. جرایم فضای سایبر به علت سادگی ارتکاب، گستردگی موضوعات و موقعیت جرم و همچنین ابهام قانونی و امنیت نسبی آمار بیشتری نسبت به فضای حقیقی دارد.

به عنوان مثال محیط درج نظرات مخاطبان یک پایگاه خبری می‌تواند فضایی مناسب برای ارتکاب انواع جرایم سایبری باشد که البته ارتکاب این جرم بسیار ساده است ولی تبعات آن برای آن مجموعه خبری می‌تواند تا فیلتر شدن سایت و جریمه مدیرمسئول بالا باشد.

ایجاد یک وبلاگ به حدی ساده است که امروزه نوجوانان نیز به راحتی در سرویس‌های وبلاگ‌دهی عضو هستند و از خدمات آن استفاده می‌کنند. به وسیله همین وبلاگ‌ها می‌توان انواع جرایم سایبری را مرتکب شد و به علت عدم نیاز به ثبت در سامانه‌های نظارتی و ... احتمال خطر برای مجرمین این فضا بسیار اندک است.

یکی از راهکارهای فرار از متهم شدن به جرم سایبری، راه‌اندازی یک وبلاگ و درج محتوای مجرمانه و بازنشر آن توسط رسانه‌های اصلی است. با این روش گویی بار اصلی عمل مجرمانه به وبلاگ منتقل می‌شود.

بیشتر از سادگی ارتکاب جرم، برخورد حقوقی با جرم سایبری ساده انگاشته می‌شود. به نحوی‌که پس از درج محتوای مجرمانه به دادن تذکر و دستور برداشتن مطلب از خروجی سایت بسنده می‌شود. حال آنکه پیشتر نیز گفته شد محتوا در فضای سایبر ماناست و با حذف از یک سایت و دو سایت اعاده به وضع سابق اتفاق نمی‌افتد.

۲-۲-۹- تعدد وبسایت‌ها و خبرگزاری‌های مجازی

طبق آمار منتشره سازمان تنظیم مقررات رادیویی[1] که به ساماندهی موضوع اینترنت در کشور می-پردازد، چهارصدهزار سایت خبری و پایگاه اطلاع‌رسانی فارسی زبان وجود دارد که بسیاری از آن‌ها در سامانه‌های قانونی مرتبط مانند وزارت فرهنگ و ارشاد اسلامی ثبت رسمی نشده‌اند. در حالیکه در فضای حقیقی و در رسانه‌های مکتوب این عدد به ده هزار نمی‌رسد.

انعطاف بالای رسانه‌های فضای مجازی، تعامل دو سویه، سرعت انتشار بالا، قابلیت شخصی‌سازی و بسیاری از ویژگی‌هایی که در رسانه‌های مکتوب نیست سبب شده اقبال به سمت رسانه‌های فضای مجازی و در نتیجه تعدد وبسایت‌ها اتفاق افتد. همین امر سبب شده تا تیراژ کل روزنامه‌های کشور با بازدید یکی از خبرگزاری‌های مرجع برابری کند.

بالا بودن این تعداد علاوه بر دشوار ساختن امکان پیشگیری از وقوع جرم، نظارت بر عملکرد این پایگاه‌ها و در نتیجه اعاده حیثیت را با سختی زیاد همراه می‌کند؛ چه اینکه گاهی ممکن است جرم علیه حیثیت معنوی یک شخص در فضای مجازی صورت بگیرد و مجنی علیه از تبعات آن متضرر شود لیکن از وقوع جرم علیه خود مطلع نشود.

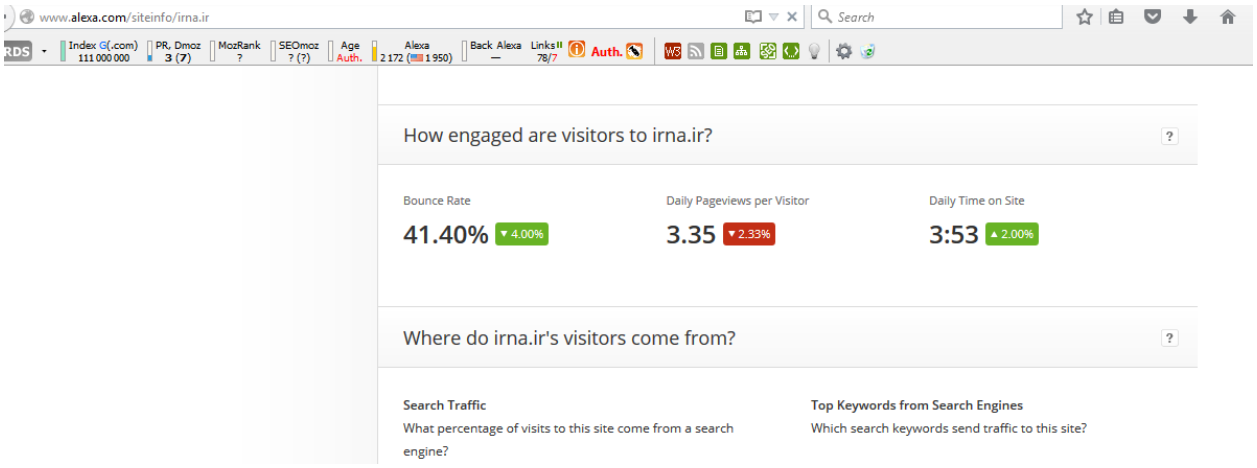
۱ برداشت شده از سایت این سازمان، تابستان ۹۴

۲-۲-۱۰- نرخ بازدید یک باره[۱]

یکی از ویژگی های وبسایت‌ها و خبرگزاری‌های مجازی، درصد بازدیدکنندگانی است که فقط یک بار به سایت وارد شده و حضور در سایت را ادامه نداده و در واقع سایت را ترک می‌کنند. این عدد مقداری بین صفر تا صد درصد دارد و هرچه نرخ بالاتر باشد، معنی آن این است که درصد بیشتری از بازدیدکنندگان فقط یک بار خبر سایت را می خوانند و در صورتی که خبر، اصلاحیه و یا تکمیل نیاز داشته باشد، بیننده دیگر از آن مطلع نخواهد شد. همچنین اگر اصل خبر غلط و دروغ باشد و بعدا تکذیب شود، بیننده ی خبر تکذیبیه ی آن را نخواهد دید.

با توجه به این ویژگی، اگر در سایتی خبری قرار بگیرد که هتک حیثیت معنوی شخص یا اشخاصی محسوب شود، عملاً امکان اعاده ی حیثیت وجود ندارد، حتی اگر خبر اصلاح و یا تکذیب شود.

برای نمونه نرخ بازدید یک باره‌ی چند خبرگزاری معتبر کشور طبق آمار جهانی الکسا[۲] در خرداد ۹۴ به این شرح است :

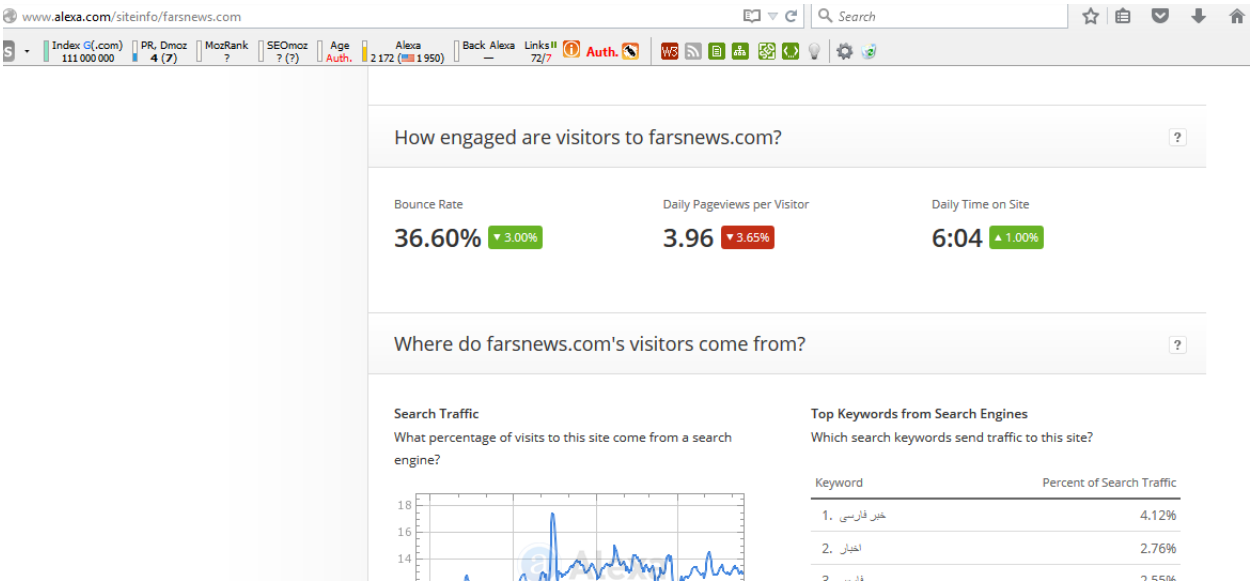


تصویر شماره ۷، نرخ بازدید یکباره خبرگزاری ایرنا

۲ Bounce rate
۳ www.alexa.com

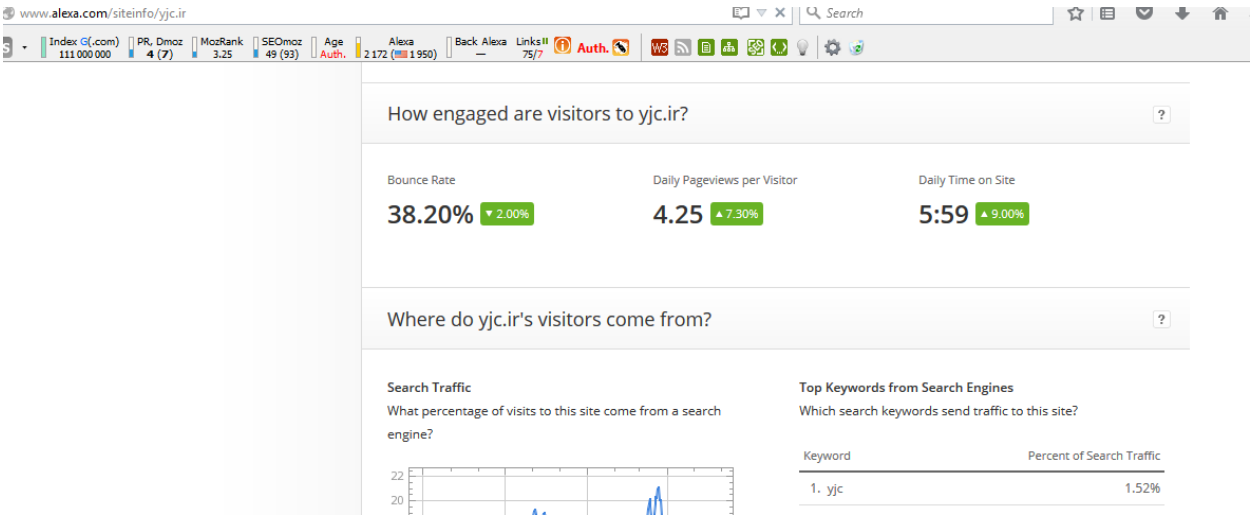
طبق تصویر بالا، نرخ بازدید یک باره ی سایت خبرگزاری جمهوری اسلامی ایران (ایرنا)، ۴۱/۴۰ ٪ درصد است. این یعنی از هر ۱۰۰ نفر بازدید کننده ی سایت ایرنا، ۴۱ نفر فقط یک بار به سایت رجوع می‌کنند.

نمونه ی دیگر وبسایت خبرگزاری فارس به عنوان پربازدیدترین خبرگزاری رسمی فارسی زبان است.



تصویر شماره ۸، نرخ بازدید یکباره خبرگزاری فارس

طبق تصویر بالا، از هر ۱۰۰ نفر بازدیدکننده ی سایت خبرگزاری فارس، حدود ۳۷ نفر بازدیدکننده ی یک‌باره محسوب می شوند.



تصویر شماره ۹، نرخ بازدید یکباره خبرگزاری باشگاه خبرنگاران

طبق تصویر بالا، از هر ۱۰۰ نفر بازدیدکننده‌ی خبرگزاری باشگاه خبرنگاران صدا و سیما، حدود ۳۸ نفر بازدیدکننده‌ی یک‌باره محسوب می شوند.

۲-۲-۱۱- رشد فزاینده کاربران فضای سایبر

الف) میزان رشد کاربران فضای سایبر در ایران

در سال های اخیر نفوذ روز افزون فضای سایبر در زندگی تمام مردم به دلایلی همچون پایین بودن هزینه استفاده از آن، افزایش چشم‌گیر بهره‌وری، بی انتها بودن در بسیاری از سطوح اجتماعی و نامتقارن بودن در آسیب‌پذیری موجب شده دول مختلف در دوران کنونی، این فضای قدرتمند را به عنوان یکی از مهمترین شقوق حکومت خود مد نظر قرار دهند.

برای درک بهتر تأثیر فضای سایبر به بررسی میزان رشد کاربران فضای مجازی در ایران می‌پردازیم.

منبع	درصد	جمعیت	تعداد کاربران	سال
www.itu.int	۳٫۸ %	۶۹,۴۴۲,۹۰۵	۲۵۰,۰۰۰	۲۰۰۰
www.itu.int	۷٫۵ %	۶۹,۴۴۲,۹۰۵	۵,۵۰۰,۰۰۰	۲۰۰۲
www.itu.int	۱۰٫۸ %	۶۹,۴۴۲,۹۰۵	۷,۵۰۰,۰۰۰	۲۰۰۵
www.itu.int	۳۴٫۹ %	۶۵,۸۷۵,۲۲۳	۲۳,۰۰۰,۰۰۰	۲۰۰۸
Internetworldstats	۴۸٫۵ %	۶۶,۴۲۹,۲۸۴	۳۲,۲۰۰,۰۰۰	۲۰۰۹
Internetworldstats	۴۳٫۲ %	۷۶,۹۲۳,۳۰۰	۳۳,۲۰۰,۰۰۰	۲۰۱۰
Internetworldstats	۵۳٫۳ %	۷۸,۸۶۸,۷۳۱	۴۲,۰۰۰,۰۰۰	۲۰۱۲
Internetworldstats	۵۷٫۲ %	۸۱,۸۲۴,۲۷۰	۴۶,۸۰۰,۰۰۰	۲۰۱۵

جدول شماره ۱، میزان رشد کاربران فضای مجازی در ایران

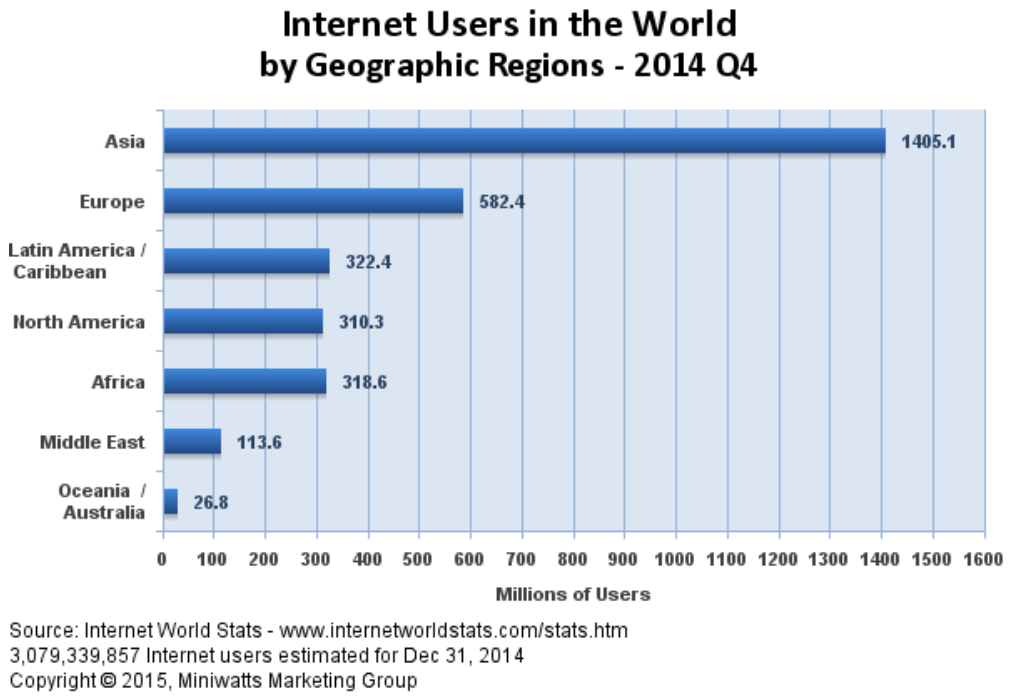
ب) میزان رشد کاربران فضای سایبر در جهان

میزان رشد کاربران فضای سایبر در جهان نیز آمار جالبی دارد، جدول ذیل نمایش دهنده تعداد کاربران فضای سایبر در جهان به تفکیک سال و قاره می‌باشد .

مناطق جهان	جمعیت در سال ۲۰۱۵	کاربران اینترنت در سال ۲۰۰۰	آخرین آمار	درصد جمعیت	میزان رشد از سال ۲۰۰۰ تا ۲۰۱۵
آفریقا	1,158,353,014	4,514,400	**318,633,889**	27.5 %	6,958.2 %
آسیا	4,032,654,624	114,304,000	**1,405,121,036**	34.8 %	1,129.3 %
اروپا	827,566,464	105,096,093	**582,441,059**	70.4 %	454.2 %
خاور میانه	236,137,235	3,284,800	**113,609,510**	48.1 %	3,358.6 %
آمریکای شمالی	357,172,209	108,096,800	**310,322,257**	86.9 %	187.1 %
آمریکای لاتین و کارائیب	615,583,127	18,068,919	**322,422,164**	52.4 %	1,684.4 %
اقیانوسیه	37,157,120	7,620,480	**26,789,942**	72.1 %	251.6 %
WORLD TOTAL	**7,264,623,793**	**360,985,492**	**3,079,339,857**	**42.4 %**	**753.0 %**

جدول شماره ۲، تعداد کاربران فضای سایبر در جهان

کاربران فضای مجازی و اینترنت در دنیا به روایت آمارهای جهانی اینترنت در قاره‌های مختلف به شرح زیر است.



جدول شماره ۳، میزان کاربران اینترنت در قاره‌های مختلف دنیا

۲-۲-۱۲- اثر اولیه خبر کذب

در فضای اطلاع‌رسانی و خبر، معمولاً خبر آن رسانه‌ای در ذهن مردم می‌نشیند و از سوی آن‌ها مقبول می افتدکه پیش از دیگر اخبار به اطلاع مردم برسد. از آنجا که در حال حاضر معمولاً اولین رسانه‌ها در انتشار یک خبر، رسانه‌های مجازی و نه رادیو و تلویزیون و رسانه‌های مکتوب هستند، «اثر اولیه خبر کذب» را معمولاً در زمره ویژگی‌های اطلاع‌رسانی در فضای مجازی به حساب می‌آورند.

در میان فعالان رسانه‌ای مثال مشهوری هست که اگر به فرد گرسنه‌ای غذای سالم داده نشود، او خود احتمالاً خود را با خوردن غذای ناسالم سیر می‌کند. دقیقاً همین مسئله در فضای خبر اتفاق می‌افتد. به عنوان مثال فرض کنید صدای مهیبی در اثر انفجار یک مخزن گاز در یک روز معمولی در شهر تهران شنیده شود. پس از وقوع این اتفاق، عموم افراد تلاش می‌کنند از علت صدای مهیب با خبر شوند، در چنین شرایطی اگر رسانه‌های آگاه و منصف، سریع وارد عمل نشوند و اطلاع‌رسانی صحیح صورت نگیرد، رسانه‌های مجازی نامعتبر، خبری به جامعه تزریق می‌کنند که به مثابه غذای ناسالم ذهن مردم را پر می کند. به عنوان مثال این

خبر از طریق چند سایت نامعتبر منتشر می‌شود که علت صدا، انفجار یک بمب بوده و در اثر آن یک مسئول بلندپایه دولتی جان باخته است. در چنین شرایطی اگر خبر درست با تأخیر به دست مردم برسد، دیگر خیلی کسی شنوای آن نیست.

همانطور که از مثال برمی‌آید، سرعت در اطلاع‌رسانی موضوعیت دارد و این بار معمولا به دوش رسانه‌های مجازی است. چه آنکه بلافاصلاه پس از وقوع یک پدیده، ذهن‌های کنجکاو عطشی برای دانستن علت پدیده دارند که در صورتیکه این عطش با شنیدن خبر غلط فروکش کند، دیگر جویای علت اصلی پدیده نخواهد بود و در صورتیکه خبر صحیح به افراد برسد، در صحت آن تشکیک خواهند کرد.

۲-۲-۱۳- ترافیک بالای شبکه‌ها

همیشه جرم سایبری، همراه با سرقت داده‌ها و یا تغییر اطلاعات نیست. گاهی مجرمان با انگیزه‌های مختلف بنا دارند صرفاً توانایی یک سازمان را در ارائه خدمات به شهروندان مختل کرده و با صدمه به اعتبار سازمان و اعتماد مشتریان به آن، حیثیت معنوی سازمان را به عنوان یک شخص حقوقی مورد خدشه قرار دهند.

به عنوان مثال، تا کنون حملات متعددی به سایت‌های معتبر خدمات‌رسانی، خبری و یا فروش اینترنتی در سطح دنیا اتفاق افتاده که قصد مجرمان سرقت اطلاعات نبوده است؛ بلکه مجرمان با روانه کردن سیل زیادی از درخواست‌ها[1] به سرور میزبان، آن را کند کرده‌اند و با این کار تا چند ساعت بعد، هر مخاطب که به سایت مراجعه کرده با پیام «سرور سایت مشغول است، لطفا تلاش خود را چند دقیقه بعد تکرار کنید.»، مواجه می‌شود. حال فرض کنید این سایت، یک پایگاه فروش اینترنتی باشد. اگر مشتریان چند بار با چنین پیام‌هایی مواجه شده و قادر به خرید کالای مورد نظر و یا دریافت خدمات مطلوب در زمان مورد انتظار نباشند، دیگر کمتر به آن سایت مراجعه خواهند کرد. بنابراین در این حالت، علاوه بر وقوع جرم علیه حیثیت معنوی، قربانی ضرر مالی هم می‌کند.

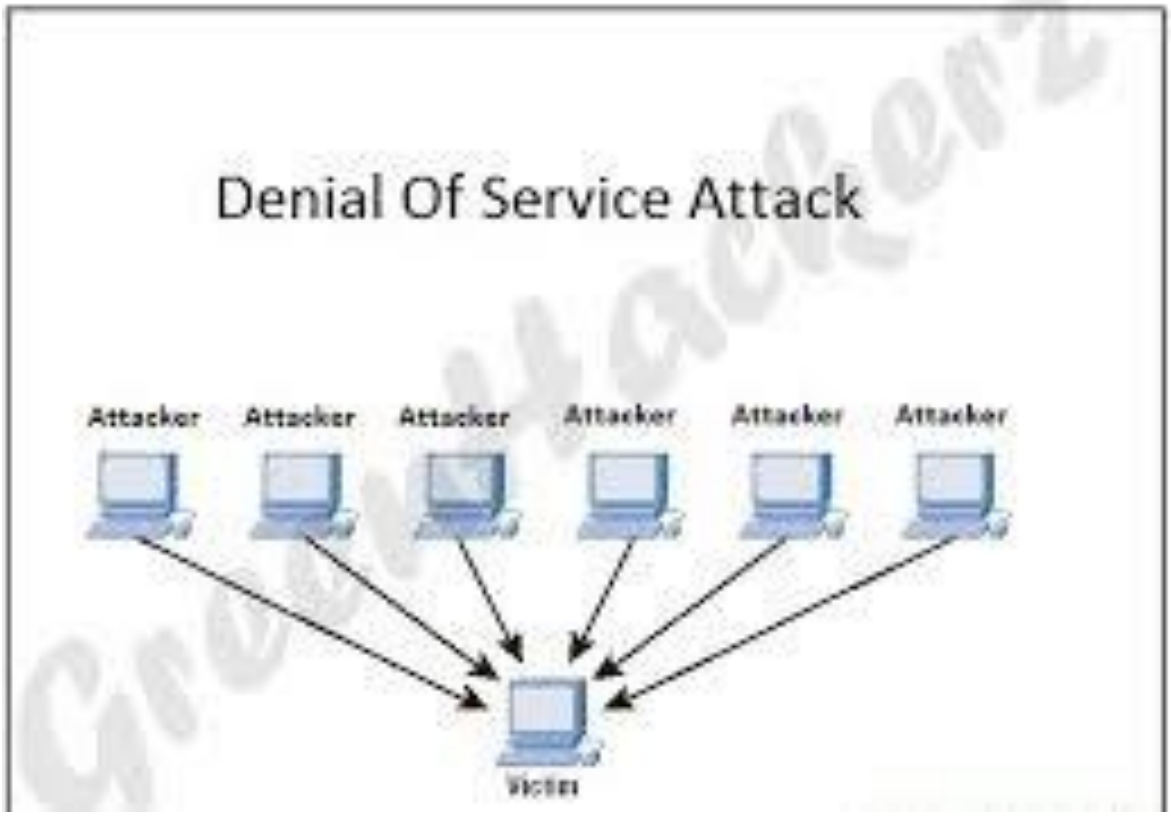
در فضای مجازی به این علت که مانند فضای حقیقی روز و شب و ساعت کاری وجود ندارد و مخاطبان پایگاه‌ها، از اقصی نقاط دنیا هستند، همواره سایت‌های پربازدید و یا پرتال سازمان‌های خدمات‌دهنده مردمی با درخواست‌های متعدد مواجه است. در چنین شرایطی اگر مجرمان با فرستادن درخواست‌هایی که قانوناً جرم نیستند، اما به علت اینکه تعدادشان بسیار زیاد است، سرور میزبان را کند کرده و یا آن را از کار

[1] request

بیاندازند، در واقع نوعی حمله سازمان‌یافته به سایت انجام دادند که به آن حمله داس[1] یا انکار سرویس می‌گویند.

چنین حمله‌ای معمولاً در مورد سایت‌های خدماتی، موتورهای جستجو و یا سایت‌های فروش اینترنتی پربازدید مورد استفاده قرار می‌گیرد و هدف، وارد کردن خدشه به اعتبار سایت میزبان است.

در سال گذشته، سایت‌های گوگل، یاهو و ای بی[2] مورد چنین حمله‌هایی قرار گرفتند. همچنین از سایت‌های خبری پربازدید داخلی، سایت خبرگزاری فارس مورد چنین حمله‌ای قرار گرفته است.



تصویر شماره ۱۰، حمله انکار سرویس توسط ۶ مهاجم سایبری به یک قربانی

[1] Denial of service
[2] ebay

نتیجه‌گیری و پیشنهادات

با مطالعات و بررسی‌های انجام شده، این نکته روشن می‌شود که رشد تکنولوژی و به ویژه فناوری مجازی، از سایر وجوه مرتبط با آن از جمله قوانین حقوقی مورد نیاز و ابزارهای نظارتی مناسب سریع‌تر است. این بدان معناست که متناسب با بروز پدیده‌های جدیدی مانند شبکه‌های اجتماعی و ابزارهای ارتباط موبایلی و طبیعتاً روزامد شدن جرایم ارتکابی در این فضا، قانون پیش‌بینی نشده است.

با توجه به چالش‌های فضای مجازی و خواص ذاتی آن که در بخش دوم این پایان نامه به تفصیل شرح داده شد، عملاً اگر محتوای مجرمانه‌ای علیه حیثیت معنوی شخصی در فضای مجازی منتشر شود، امکان اعاده حیثیت و جبران خسارت معنوی به طور کامل وجود ندارد. با توجه به این نکته موارد زیر پیشنهاد می‌گردد:

الف) روزامد و کارامد کردن قوانین «مجازات اسلامی» و «جرایم رایانه‌ای» و تدوین قوانین جدید و تشدید مجازات جرم علیه حیثیت معنوی اشخاص در فضای مجازی. این امر باید به نحوی باشد که در هزینه – فایده کردن شخص علاقه‌مند به بزه، این امر، محرز شود که هزینه بزه ارتکابی بسیار بیشتر از فایده احتمالی آن خواهد بود.

ب) تلاش در جهت تمرکز و تأکید کلیه اقدامات حقوقی و فنی بر پیشگیری از وقوع جرم علیه حیثیت معنوی اشخاص در فضای مجازی. اغلب قوانین و مقررات ما بر پایه مجازات جرم واقع شده برنامه-ریزی شده، در صورتیکه رویکرد اصلی در تدوین قوانین به خصوص در فضای سایبر باید جنبه پیشگیرانه داشته باشد وگرنه نمی‌تواند جامعه را از سقوط در جرم و ارتکاب بزه حفظ کند.

ج) گنجاندن ضرورت‌های اخلاقی و مسائل فنی فعالیت در فضای مجازی در محتوای آموزش شهروندی، آموزش‌های تبلیغی رسانه‌های جمعی و آموزش‌های کودکان و نوجوانان از طریق کتب و محتوای

درسی مدارس و سازمان‌های ذی‌ربط. می‌بایست متناسب با افزایش ضریب‌نفوذ اینترنت در کشور و ارتقای کمی و کیفی امکانات سایبری به آموزش‌های این حوزه نیز توجه اساسی کرد وگرنه استفاده درست و کاربردی از این فضا محقق نمی‌شود.

د) طراحی و پیاده‌سازی راه حل‌های فنی از جمله شناسنامه‌دار کردن اشخاص در فضای مجازی و راه‌اندازی شبکه ملی داده در کشور. طرح شناسنامه‌دار کردن افراد در فضای مجازی و اختصاص کد یکتا به هر کس می‌تواند تا حد زیادی موجبات پیشگیری از وقوع جرم را فراهم آورد. طرحی که در کشورهای توسعه‌یافته در حال انجام است و نتایج مطلوبی برای آنان در بر داشته است. با راه‌اندازی این طرح، پس از مدتی می‌توان علاوه بر پیشگیری‌های احتمالی و قطعی به نتایج مطلوب فرهنگی، اجتماعی، اقتصادی و سیاسی رسید. با آنالیز رفتار مخاطبان فضای مجازی می‌توان علاقه‌مندی‌ها، حساسیت‌ها، وقت‌گذاری‌ها و بسیاری اطلاعات مفید جمع‌آوری کرد و در برنامه‌ریزی‌های کلان از آن استفاده کرد.

۳- منابع فارسی

۳-۱- کتاب

۱. اردبیلی، محمدعلی، حقوق جزای عمومی، ج۱، تهران: نشر میزان، ۱۳۹۱.

۲. استفانی، گاستون؛ لواسور، ژرژ و بولوک، برنار، حقوق جزای عمومی، حسن دادبان، ج ۲، تهران: انتشارات دانشگاه علامه طباطبائی، ۱۳۷۷,

۳. ۳اصلانی، حمیدرضا، حقوق فناوری اطلاعات، تهران: نشر میزان، ۱۳۸۹.

۴. افراسیابی، محمد اسماعیل، حقوق جزای عمومی، ج۱، تهران: انتشارات فردوسی، ۱۳۷۶.

۵. امامی، سید حسن، حقوق مدنی، ج۳، تهران: نشر اسلامیه، ۱۳۴۰.

۶. انوری، حسن، فرهنگ فشرده سخن، ج۱، تهران: انتشارات سخن، ۱۳۸۲.

۷. ایرانی ارباطی، بابک، مجموعه نظرهای مشورتی جزایی، جلد اول، تهران: انتشارات مجد ، ۱۳۸۸.

۸. آقایی نیا، حسین، جرایم علیه اشخاص، ج۲، تهران: نشر میزان، ۱۳۸۷.

۹. آیتی، حمید، حقوق آفرینشهای فکری با تأکید بر حقوق آفرینشهای ادبی و هنری، ج۱، تهران: نشر حقوقدانان، ۱۳۷۵.

۱۰. باستانی، برومند، جرایم رایانه‌ای و اینترنتی جلوه ای نوین از بزهکاری، تهران: انتشارات بهنامی، ۱۳۸۳.

۱۱. بای، حسین علی و پور قهرمان، بابک، بررسی فقهی حقوقی جرایم رایانه‌ای، قم: انتشارات پژوهشگاه علوم و فرهنگ اسلامی، ۱۳۸۸.

۱۲. تننباوم، آندرو اس، شبکه های رایانه‌ای، عین الله جعفر نژاد قمی، تهران: انتشارات علوم رایانه، ۱۳۸۳.

۱۳. جعفر بن حسن حلی، شرائع الاسلام، ابوالقاسم‌ابن‌احمدیزدی، ج ۲، تهران: نشر دانشگاه تهران، ۱۳۶۱.

۱۴. جعفرنژاد قمی، عین الله و عباس نژاد، رمضان، مبانی فناوری اطلاعات، تهران: نشر علوم رایانه، ۱۳۸۷.

۱۵. جعفری لنگرودی، محمد جعفر، ترمینولوژی حقوق، تهران: نشر گنج، ۱۳۸۸.

۱۶. جلالی فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، تهران: انتشارات خرسندی، ۱۳۸۹.

۱۷. حر عاملی، محمد بن حسن، تفصیل وسائل الشیعه إلی تحصیل مسائل الشریعه، علی افراسیابی، ج۸، قم: نشر مؤسسه آل البیت علیهم السلام لاحیاء التراث، سال ۱۳۷۱.

۱۸. حسن بیگی، ابراهیم، حقوق و امنیت در فضای سایبر، تهران: انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، ۱۳۸۴.

۱۹. زراعت، عباس، شرح قانون مجازات اسلامی، ج ۲، تهران: نشر ققنوس، ۱۳۹۲.

۲۰. زمانی، سید قاسم و بهراملو، مهناز، حقوق نشر و اینترنت، تهران: نشر خرسندی، ۱۳۸۶.

۲۱. سلیمی، علی و داودی، محمد، جامعه‌شناسی کجروی، قم: نشر پژوهشگاه حوزه و دانشگاه، ۱۳۸۶.

۲۲. شامبیاتی، هوشنگ، حقوق جزا و جرم‌شناسی، تهران: انتشارات مجد، ۱۳۸۸.

۲۳. شاملو احمدی، محمد حسین، فرهنگ اصطلاحات و عناوین جزایی، تهران: نشر دادیار، ۱۳۸۰.

۲۴. شکری، رضا و سیروس، قادر، قانون مجازات اسلامی در نظم حقوق کنونی، تهران: نشر مهاجر، ۱۳۹۰.

۲۵. شیرزاد، کامران، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، تهران: نشر بهینه فراگیر، ۱۳۸۸.

۲۶. صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، تهران: نشر میزان، ۱۳۸۸.

۲۷. عالی پور، حسن، حقوق کیفری فناوری اطلاعات، تهران: انتشارات خرسندی، ۱۳۹۰.

۲۸. عاملی، سید سعیدرضا، رویکرد دوفضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی، تهران: انتشارات امیر کبیر، ۱۳۹۰.

۲۹. علی‌آبادی، عبد الحسین، حقوق جنائی، ج ۲، تهران: انتشارات فردوسی، ۱۳۶۸.

۳۰. عمید، حسن، فرهنگ فارسی، ج۱، تهران: نشر فرهنگ اندیشمندان، ۱۳۸۹.

۳۱. قاجارقیونلو، سیامک، مقدمه حقوق سایبر، تهران: نشر میزان، ۱۳۹۱.

۳۲. کاتوزیان، ناصر، دوره مقدماتی حقوق مدنی: اموال و مالکیت، تهران: نشر میزان، ۱۳۹۲.

۳۳. گلدوزیان، ایرج، بایسته‌های حقوق جزای اختصاصی، تهران: نشر میزان، ۱۳۸۸.

۳۴. گلدوزیان، ایرج، حقوق جزای اختصاصی، تهران: انتشارات دانشگاه تهران، ۱۳۹۱.

۳۵. معین، محمد، فرهنگ فارسی معین، ج ۱، تهران: انتشارات امیرکبیر، ۱۳۶۳.

۳۶. میرزای قمی، ابوالقاسم، جامع الشتات، ابوالقاسم گرجی، تهران: انتشارات دانشگاه تهران، ۱۳۸۷.

۳۷. میرمحمد صادقی، حسین، حقوق کیفری اختصاصی، جرایم علیه اشخاص، تهران: نشر میزان، ۱۳۸۷.

۳۸. میر محمد صادقی، حسین، جرایم علیه امنیت و آسایش عمومی، تهران: نشر میزان، ۱۳۸۶.

۳۹. نوربها، رضا، زمینه حقوق جزای عمومی، تهران: نشر گنج دانش، ۱۳۸۰.

۴۰. هاشمی، سید محمد، حقوق بشر و آزادی‌های اساسی، تهران: نشر میزان، ۱۳۸۴.

۴۱. هوگز، دونا.م، «گردشگری جنسی در اینترنت»، ماهنامه سیاحت غرب، هیئت مترجمین مرکز پژوهش‌های اسلامی صدا و سیما، شماره ۲۶(۱۳۸۲)، ۳۸-۴۴.

۳-۲- مقاله

۱. انصاری، باقر، «حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران»، مجله دانشکده حقوق و علوم سیاسی، شماره ۶۶ (زمستان ۱۳۸۳): ۱-۵۴.

۲. انصاری، باقر، «مقدمه ای بر مسئولیت مدنی ناشی از ارتباطات اینترنتی»، مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران، شماره ۶۲ (زمستان ۱۳۸۲): ۹-۵۲

۳. بن شاب، آلبرت، «عشق ورزی در فضای مجازی»، ماهنامه سیاحت غرب، هیئت مترجمین مرکز پژوهش‌های اسلامی صدا و سیما، شماره ۳۰ (۱۳۸۳) ، ۴۷-۵۸.

۴. جبلی طاهری، محسن، «جرم و رایانه»، مجله حقوقی و قضایی دادگستری، شماره۹ (۱۳۷۲)، ۱۰۱-۱۱۲.

۵. دزیانی، محمدحسن، «بررسی پیش نویس قانون مبارزه با جرایم رایانه‌ای در گفت و گو با کارشناسان حقوق و فن آوری»، مجله دنیای رایانه و ارتباطات، شماره ۲۶ (تابستان ۱۳۸۳)، ۷۱-۸۲.

۶. دزیانی، محمد حسن، «ابعاد جزائی کاربرد رایانه و جرایم رایانه‌ای»، خبرنامه انفورماتیک شورای عالی انفورماتیک کشور، شماره ۵۸ (اردیبهشت ۱۳۷۳)، ۸۷-۹۸

۷. دزیانی، محمدحسن، «شروع جرایم رایانه‌ای – سایبری»، خبرنامه انفورماتیک شورای عالی انفورماتیک کشور، شماره ۹۳ (دی ۱۳۸۴)، ۶۵-۷۳

۸. رجب‌پور کاشف، مهدی، «تقابل امنیت فناوری اطلاعات با جرایم سایبری»، ماهنامه تخصصی وب، شماره ۱۳۵(آبان ۱۳۹۰)، ۴۳-۵۱.

۳-۳- پایان نامه و رساله

۱. پاکزاد، بتول، جرایم رایانه‌ای، پایان نامه کارشناسی ارشد، دانشکده حقوق، دانشگاه شهید بهشتی، ۱۳۷۵.

۲. حسن‌بیگی، 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.

۳. حسینی خواه، نور الله، جرایم رایانه‌ای، پایان نامه کارشناسی ارشد، دانشکده حقوق، دانشگاه آزاد اسلامی واحد نراق، ۱۳۷۷.

۴. خرم آبادی، عبدالصمد، جرایم فناوری اطلاعات، رساله دکتری، دانشکده حقوق، دانشگاه تهران، ۱۳۸۴.

۵. شیرین بیگ‌پور، رؤیا، مطالعه تطبیقی جرایم رایانه‌ای و جرایم سنتی مشابه در نظام کیفری ایران، پایان نامه کارشناسی ارشد، دانشکده حقوق، دانشگاه تبریز، ۱۳۹۰.

۶. عبقری، آدینه، جرم رایانه‌ای جلوه‌ای نوین از بزه کاری، پایان نامه کارشناسی ارشد، دانشکده حقوق، دانشگاه تهران، ۱۳۷۷.

۳-٤- منابع لاتین

1. Brenner, Susan W, “Is There Such a Thing as virtual Crime”, California Criminal Law Review, 2001.
2. Göritz, A. S, “Incentives in web studies: Methodological issues and a review”, International Journal of Internet Science, 1(1), 2006, 58-70.
3. Hine, Christine, Systematics as cyberscience: computers, change, and continuity in science, The MIT Press, 2008.
4. Parker, Dann.B, Combattre la criminalite informatique ,ed oros, 1985.
5. scott.M.D, Internet and Technology Law Desk Refereace, Aspen law & Business, 2001.

منابع اینترنتی

آخرین مشاهده (۹۴/۴/۱۲) http://www.crime-research.org/library/Polivanjuk_mar.html

آخرین مشاهده (۹۴/۴/۱۸) http://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime

آخرین مشاهده (۹۴/۳/۱۰) http://www.alexa.com/topsites/countries/IR

آخرین مشاهده (۹۴/۱/۲۹) http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

آخرین مشاهده (۹۴/۲/۱۲) https://www.fbi.gov/news/stories/2012/october/cyber-division-focusing-on-hackers-and-intrusions

آخرین مشاهده (۹۴/۳/۵)

http://hashemirafsanjani.ir/fa/content/%C2%AB%D8%A7%D9%86%D8%AA%D8%AE%D8%A7%D8%A8-%D9%85%D8%B1%D8%AF%D9%85%C2%BB-%D8%A8%D8%A7%D8%A8-%D9%85%DB%8C%D9%84-%D8%B5%D8%AF%D8%A7%D9%88-%D8%B3%DB%8C%D9%85%D8%A7-%D9%86%D8%A8%D9%88%D8%AF

آخرین مشاهده (۹۴/۵/۲۵) http://edition.cnn.com/2010/US/11/28/us.wikileaks.iran/

آخرین مشاهده (۹۴/۵/۱۸) http://www.khabaronline.ir/detail/441464/Politics/parties

آخرین مشاهده (۹۴/۵/۲۱) http://www.farsnews.com/newstext.php?nn=13940512001327

آخرین مشاهده (۹۴/۶/۲) http://farsi.alarabiya.net/fa/iran/2015/06/10/%D8%B3%D9%BE%D8%A7%D9%87-%D9%BE%D8%A7%D8%B3%D8%AF%D8%A7%D8%B1%D8%A7%D9%86-%D8%A7%D8%B5%D9%81%D9%87%D8%A7%D9%86-%D8%B4%D9%87%D8%B1-%D8%B1%D8%A7-%D8%A8%D9%87-%D8%AA%D9%88%D9%BE-%D8%A8%D8%B3%D8%AA-.html

آخرین مشاهده (۹۴/۳/۱) http://aftabnews.ir/vdcepp8zwjh8xoi.b9bj.html

العنوان: الجرم ضد كرامة الأشخاص النفسية في الفضاء السيبراني و استعادة كرامتهم

الأستاذ المشرف: الدكتور علي غلامي

الأستاذ المساعد: الدكتور سلمان عمراني

الباحث: مسعود پيرهادي

الفرع الدراسي: الدراسات الإسلامية و القانون

الملخّص:

لقد تعددت الجرائم و تنوعت إثر التوسع في التقنيّات المتقدمة، فالعديد من القوانين والإجراءات السابقة للتصدي لها باتت دون جدوى.

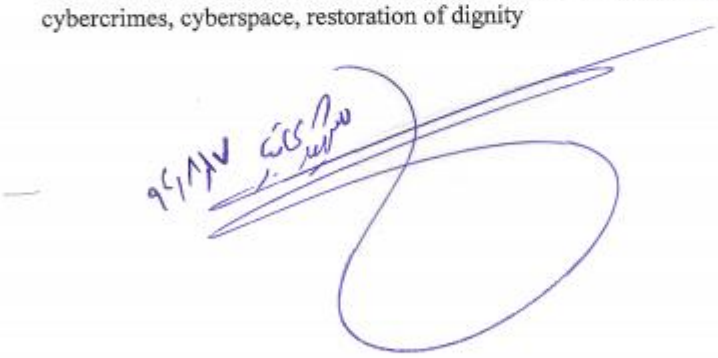
فالفضاءات الافتراضية و الوسائل و الأدوات المتعلقة بها كالحاسوب و الهواتف الذكية و الشبكات الاجتماعية تُعدُّ إحدى هذه المصاديق الهامة للتقنيات المتقدمة. تحدث العديد من الجرائم بشكل متزايد كُلَّ يوم في الفضاء الافتراضي فمنها مايُرتكب ضد الكرامة النفسية للأشخاص. جرائم كالإهانة و التشهير و نشر معلومات رقمية كاذبة تدمر أحيانا الكرامة الروحية للأشخاص أكثر من الجرائم في الأجواء الحقيقية بسبب تحديات الفضاء الافتراضي مثل النطاق وسرعة النشر فيها و كما يمكن استعادة الكرامة و تعويض الخسارة الروحية للأشخاص في الأجواء الحقيقية، لا يوجد مثل هذة الإمكانية في الفضاءات الافتراضية. في الواقع، القوانين الحالية لا تسمح استعادة كرامة الأشخاص من الجرائم السيبرانية و يجب الوقاية من ارتكاب الجرائم ضد الكرامة النفسية للأشخاص في الأجواء الافتراضية عن طريق اعتماد نهج وقائي والدورات التدريبية لرفع مستوى المواطنة.

الكلمات الدليلة:الكرامة الروحية، الجرم ضد الكرامة النفسية، الجرم الكمبيوتري، الجرائم السيبرانية ، الفضاء السيبراني ، استعادة الكرامة

Abstract:

With the expansion of advanced technologies, the crime becomes various and diverse. Many of the previous laws and procedures for dealing with the crime seem inefficient. One of the most important instances of advanced technology is cyberspace and its related tools and items such as computers, smart phones and social networks. Every day in cyberspace, much crime happens that a great number of it is committed against spiritual dignity of individuals. Some instances of crime such as insult, defamation and dissemination of cyber false information occasionally destroy spiritual dignity of individuals more in comparison with crime in real life, since in cyberspace the speed and scope of spreading any news is extremely high. Also dignity can be resorted and spiritual damage inflicted to individuals can be compensated in real atmosphere, while, such a possibility does not exist in cyberspace. In fact, the current laws don't allow resorting dignity of individuals from cybercrimes and commitment of any crime against spiritual dignity of individuals should be prevented by taking a proactive approach and citizenship trainings.

Keywords: spiritual dignity, crimes against spiritual dignity, computer crimes, cybercrimes, cyberspace, restoration of dignity



Imam Sadiq University (ISU)

Faculty of Islamic Studies and Law

Continuous M.A. Islamic Studies and Law

LLM in Criminal Law

Crimes against Spiritual Dignity of Individuals in Cyberspace and Restoration of Dignity

Supervisor

Dr. Ali Gholami

Student

Masoud Pirhadi

September 2015