کج‌روی‌های اینترنتی؛ لزوم نظارت و محدود کردن دسترسی به اطلاعات

مریم میرحسینی

فارغ التحصیل کارشناسی جامعه شناسی دانشکده علوم اجتماعی، و دانشجوی کارشناسی ارشد دانشکده مطالعات جهان دانشگاه تهران، mirhoseini.maryam@gmail.com

چکیده

در این مقاله ضمن مقایسه‌ی کج‌روی در فضای واقعی و فضای مجازی، کج‌روی در فضای مجازی مطالعه خواهد شد. پس از ارائه یک نوع‌شناسی ازکج‌روی‌هایی که از کانال اینترنت انجام می‌شود، ۴ مورد از آنها مورد مطالعه قرار خواهد گرفت. سپس مقاله حاضر به این سوالات پاسخ می‌دهد : چرا اینترنت ابزاری برای کج‌روی است؟ آیا باید بر اینترنت نظارت صورت گیرد؟ آیا باید پیامدهای منفی اینترنت کنترل شود؟ در بخش بعد لزوم نظارت دولتی و محدود شدن دسترسی به اطلاعات مطالعه خواهد شد. در پایان نیز راهکارهایی جهت کاهش آسیب‌های ناشی از اعمال انحرافی در اینترنت ارائه خواهد شد.

کلید واژه‌ها : کج‌روی در اینترنت، نظارت، محدودیت دسترسی، اطلاعات در حوزه عمومی.

مقدمه

شبکه‌ی جهانی اینترنت ارتباط انسان‌ها را بدون محدودیت های زمانی و مکانی امکان پذیر می‌سازد. تقریباً در اوایل دهه ۲۰۰۰ در ایالات متحده در هر خانه یک دستگاه کامپیوتر وجود داشت که امکان استفاده گسترده از اینترنت را فراهم می‌کرد. انسان‌ها برای برآوردن نیازهای گوناگون و متفاوتی به شبکه وصل می‌شوند. این نیازها اطلاع و خبرگیری، آموزش، تجارت، سرگرمی و غیره را در بر می‌گیرد و در این زمینه‌ها تعداد صفحات وب در دسترس کاربران اکنون به بیلیون و بیشتر می‌رسد. از زمانی‌که اینترنت تبدیل به یک وسیله‌ی ارتباطی در دسترس همگان شد به عنوان ابزاری برای کج‌روی هم مورد استفاده قرار گرفت. در همه‌ی ابعاد استفاده از اینترنت این امکان وجود دارد که ارتباط میان دو فردی برقرار شود که یکی عامل کج‌روی و دیگری قربانی است. افراد در فضای مجازی به خاطر داشتن ویژگی‌هایی که در ادامه ذکر خواهد شد بسیارسهل‌تر از فضای واقعی می‌توانند مرتکب اعمال انحرافی شوند.

همه‌ی کامپیوترهای خانگی می‌توانند از طریق یک خط تلفن به اینترنت متصل شوند و این زمینه‌ساز انواع مختلفی از کج‌روی‌ها در اینترنت است. این‌که همه افراد در همه سنین می‌توانند به اینترنت دسترسی داشته باشند نیز از دلایل افزایش کج‌روی‌هاست. انحرافات و کج‌روی‌هایی که در حوزه اینترنت صورت می‌گیرد را می‌توان به بخش‌های زیر تقسیم کرد :

- انحرافات جنسی در وب و گسترش پورنوگرافی در اینترنت
- کلاهبرداری و سواستفاده های مالی
- سرقت اطلاعات (هکرها)
- تقلب و جعل حقایق در سطح دیدگاه‌های سیاسی
- نقض کپی رایت از طریق وارد کردن آثار به اینترنت

که در این مقاله به سه مورد اول پرداخته خواهد شد.

واندنبرگ (۲۰۰۴) در یکی از فصل‌های کتاب خود به نام کج‌روی در فضای سایبر به طبقه‌بندی انواع کج‌روی‌هایی که در فضای سایبر اتفاق افتاده است می‌پردازد و همچنین مثال‌های فراوانی از قربانیان این نوع کج‌روی‌ها در ایالات متحده را در کتاب خود می‌آورد.

در بحث انحرافات جنسی و پورنوگرافی در اینترنت به طور خاص مارک لاسر که خود یکی از رها یافتگان از چنگال اعتیاد به مسائل انحرافی و همچنین مدیر اجرایی اتحادیه مسیحی بازپروی معتادان به مسائل انحرافی می‌باشد در مقاله‌ای با عنوان هرزه‌نگاری در اینترنت به مباحثی از قبیل شیوع استفاده از هرزه‌نگاری اینترنتی، اشکال متعدد انحطاط، اعتیاد به هرزه‌نگاری اینترنتی، غارتگران اتاق محاوره، منحصر به فرد بودن اینترنت و برخورد اتفاقی می‌پردازد. در بخش برخورد اتفاقی وی بیان می‌دارد که آنان که تلاش داشته‌اند از حقوق آزادی بیان برای هرزه‌نگاران دفاع کنند، دیری است که ادعا می‌کنند، همگی مختارند در مورد تماشای هرزه‌نگاری‌ها تصمیم بگیرند. در حالی‌که در اینترنت، این هرزه‌نگاری است که می‌تواند در جست و جوی شما باشد و نیز این‌که، همگی ما مطلع هستیم که گاهی ناخواسته و نطلبیده، مطالبی از طریق پست الکترونیک برای ما ارسال می‌شود که سایت‌های اینترنتی مختص به مسائل انحرافی را تبلیغ می‌کنند" (لاسر، ۲۰۰۶).

همه‌ی دولت‌های جهان معتقدند که باید با تبعات و آثار منفی شبکه مقابله کرد. اما به دلیل این‌که اینترنت به‌عنوان یک پروژه‌ی دولتی توسعه پیدا کرد و هزینه‌ای برای استفاده‌کنندگان نداشت بسیاری از افراد عقیده دارند که از ویژگی‌های خاص اینترنت باید ارتباطات رایگان و برقراری راحت روابط خاص باشد (واندنبرگ، ۲۰۰۴).

در مورد اینترنت این اندیشه وجود دارد که کنترل اجتماعی در آن، باید در پایین‌ترین حد باشد و باید اجازه داده شود که ارتباط در سرتاسر شبکه برقرار شود. مطابق نظر بسیاری از کاربران، همه‌ی اطلاعات باید آزاد و در دسترس باشد.

بر خلاف نظر این افراد، تمامی دولت‌ها در کشورهای مختلف تلاش کرده‌اند تا در زمینه‌ی قسمت‌های مختلف شبکه، ابزار کنترل اجتماعی و اهرم‌های نظارتی را به‌کار برند، اما انتقادها و اعتراض‌هایی وجود دارد که خواستار توقف نظارت‌هاست. برخی از گروه‌ها با هر نوع نظارت و کنترل مخالفند و آن را گامی در جهت سرکوب آزادی‌های دموکراتیک می‌دانند و ادعا می‌کنند این اقدامات مخالف آزادی بیان و اندیشه است. به نظر هکرها نیز هر کس باید بتواند به هر نقطه که می‌خواهد در شاهراه اطلاعاتی برود و محدود کردن دسترسی به اطلاعات در فضای سایبر در هیچ کجا قانونی نیست. اگر چه این درخواست آنان تا حدی درست است اما مسئله‌ی اصلی این است که ارتباطات بدون محدودیت در سرتاسر شبکه و همچنین رایگان بودن اینترنت، مشکلاتی نیز به دنبال دارد. کودکان و نوجوانان و افرادی که آگاهی اندکی دارند ممکن است توسط غارتگران جنسی که در کمین هستند آسیب و زیان‌های جبران ناپذیر ببینند.

در زمینه‌ی هزینه‌های مالی، بازرگانان و تاجران باید سهم سود مالی خود را بپردازند و در این حوزه، رایگان بودن همه‌ی خدمات اینترنت زیر سوال می‌رود.

بعضی از اطلاعات مربوط به حریم زندگی خصوصی و یا اطلاعات محرمانه تجارت، بازرگانی و امور مالی است، بنابراین بحث و صحبت از این‌که همه‌ی اطلاعات باید در حوزه عمومی باشد مجاز نیست.

همچنین هکرها که عقاید آزادی‌طلبانه در زمینه‌ی اطلاعات در اینترنت دارند جزء کاربران و بازدیدکنندگانی هستند که خسارت‌های مادی و معنوی فراوانی را در کامپیوترها سبب می‌شوند. همه‌ی این دلایل نشان می‌دهند که باید خطرات و تبعات اجتماعی اینترنت و گسترش مسایل غیر اخلاقی و پورنوگرافی کنترل شوند و استفاده از اینترنت قاعده‌مند شود.

کج‌رفتاری

کج‌رفتاری شامل انواع بسیاری از رفتارهای نابهنجار است که اشکالی از آن در هر جامعه‌ای رخ می‌دهد. گفته شده که رفتار نرمال یا بهنجار، هر نوع رفتاری است که از هنجارها یا مقررات گروهی که رفتار مزبور در آن روی می‌دهد تبعیت کند. در مقابل، کج رفتاری هر نوع رفتاری است که با هنجارها یا مقررات گروه، همنوایی نداشته باشد و دامنه‌ی وسیعی از رفتارها، از تخلفات جزیی در رانندگی تا قتل را دربرمی‌گیرد (صدیق سروستانی، ۱۳۸۳). مجموعه‌ی صاحب نظرانی که تعریفی از کج‌رفتاری ارائه داده‌اند را می‌توان به دو گروه بزرگ تقسیم کرد. یک گروه آنان‌که کج رفتاری را پدیده‌ای واقعی و دارای صفاتی می‌دانند که از رفتارهای بهنجار قابل تشخیص و تفکیک است (نتلر، ۱۹۸۴ ؛ هرشی، ۱۹۷۳). دسته‌ی دوم آنان‌که مدعی‌اند کج‌رفتاری لزوماً واقعی نیست و چه بسیارند کسانی که به غیر حق، متهم به کاری می شوند و به اشتباه و از روی غرض برچسب می‌خورند. بنابراین از نظر این گروه اساساً این انگ است و نه نفس رفتار که کسی را کج‌رفتار می‌کند (ارمن و لاندمن، ۱۹۹۶؛ سیمون، ۱۹۹۶؛ بکر، ۱۹۷۳؛ اریکسون، ۱۹۶۲).

کج‌رفتاری‌ها از مجراها و کانال‌های مختلفی انجام می‌شوند. کج‌رفتاری را می‌توان به دو گروه کج‌رفتاری در فضای واقعی و فضای مجازی تقسیم کرد. در حوزه‌ی فضای مجازی از زمانی که اینترنت تبدیل به یک وسیله‌ی ارتباطی در دسترس همگان شد به عنوان ابزاری برای کج‌روی هم مورد استفاده قرار گرفت و مانند هر ابزار تکنولوژیکی دیگر هم جنبه‌های مثبت یافت و هم منفی.

انحراف جنسی روی وب

کج‌روی جنسی روی وب، ابعاد ویژه‌ای دارد. اینترنت به خاطر داشتن سه ویژگی، مهم‌ترین منبع اشاعه‌ی هرزه‌نگاری است. این سه ویژگی عبارتند از :

۱. قابلیت دسترسی آسان کاربران به آن
۲. توانایی پرداخت بهای آن در سایت‌هایی که استفاده از آنها مستلزم پرداخت پول است
۳. ناشناس ماندن مصرف‌کنندگان آن (لاسر، ۲۰۰۶)

هرکسی از هر جایی می‌تواند به موضوعات متنوع و گوناگونی در اینترنت دسترسی پیدا کند. افراد می‌توانند از خدمات بولتن بورد و وب سایت‌ها در جهت مناظره‌ی مجازی مسائل انحرافی استفاده کنند. همچنین افراد برای ملاقات دیگران برای مسائل انحرافی از وب سایت‌ها استفاده می‌کنند و گاهی کودکان و نوجوانان را هدف قرار می‌دهند. کودکان در هر سنی می‌توانند به سایت‌های مختلف مراجعه کنند و توسط مفسدان اینترنتی اغفال شوند و گاهی اوقات زمانی‌که کودکان در موتور جستجویی مثل گوگل دنبال مطلبی می‌گردند به‌طور اتفاقی با سایت‌های هرزه مواجه می‌شوند.

وب‌سایت‌ها سطح جدیدی از بده بستان‌ها را میان مشتریان موضوعات پورنوگرافی و افراد علاقه‌مند به فعالیت‌های بی‌بندوباری جنسی باب کرده‌اند. وب سایت‌ها همچنین میزان دسترسی متجاوزان جنسی به اشخاص آسیب‌پذیر را افزایش داده‌اند.

پورنوگرافی در اینترنت

یکی از جنبه‌های تاثیرات اجتماعی، اشاعه‌ی مسایل غیراخلاقی، تصاویر مستهجن و دیگر اطلاعات مضر و منحرف‌کننده است. در یک مطالعه کلی، می‌توان دریافت که موضوعات انحرافی و هرزه‌نگاری در اینترنت، فراوان و اغلب آزاد است. مطالعه‌ای که در سال ۱۹۹۹ انجام شد، نشان داد که ۳۱ درصد از کاربران متصل به اینترنت به سایت‌هایی اتصال داشته‌اند که مختص به مسائل انحرافی بوده است (بازرمن، ۲۰۰۶).

در مورد تمامی موتورهای جستجو از جمله یاهو و گوگل می‌توان با وارد کردن کلماتی که ارتباط اندکی با مسائل انحرافی دارند به هزاران سایت اینترنتی مختص به آن دست پیدا کرد. اگر چه استفاده از بسیاری از سایت‌های انحرافی نیازمند هزینه‌ی مالی است که معمولاً با کارت اعتباری پرداخت می‌شود، اما همه‌ی سایت‌ها، یک بخش برای فریفتن مخاطبان دارند که به‌صورت رایگان تصاویری جهت وسوسه کردن ارائه می‌دهند تا شخص برای مشاهده‌ی مطالب مفصل‌تر، مجبور به استفاده از کارت اعتباری خود شود. در ضمن مصرف‌کنندگانی که نمی‌خواهند مبلغی پرداخت کنند می‌توانند از این سایت به سایت دیگر بروند و بدون نیاز به شماره‌ی کارت اعتباری، فقط از بخش‌های رایگان استفاده کنند.

کسانی که از حقوق آزادی بیان برای ایجاد کنندگان سایت‌های هرزه‌نگاری دفاع می‌کنند، ادعا دارند که هر کس می‌تواند تصمیم بگیرد که این صفحات را ببیند یا نه، اما برخورد اتفاقی با این سایت‌ها را نیز باید در نظر گرفت. بعضی از سایت‌های پورنو، برنامه‌هایی را بدون اختیار و اجازه‌ی کاربر روی کامپیوترهای خانگی نصب می‌کنند و کاربر را به‌طور اتوماتیک به سایت‌های دیگر در این زمینه، هدایت می‌کنند و گاهی نیز ناخواسته مطالبی از طریق پست الکترونیک برای افراد ارسال می‌شود که سایت‌های پورنو را تبلیغ می‌کنند و یا حاوی تصاویر غیر اخلاقی هستند.

پورنوگرافی کودکان نیز بحث مهمی است که لزوم نظارت بر اینترنت را متذکر می‌شود. امروزه با پیدایش تابلوی اعلانات شبکه‌های داخلی و شبکه‌ی جهانی اینترنت و امکانات گرافیکی پیشرفته‌ی آن، صنعت پورنوگرافی کودکان امکان یافته است تا از طریق کامپیوتر احیا شود. قبل از توسعه‌ی شبکه‌ی جهانی اینترنت صنعت پورنوگرافی کودکان از طریق مجلات و نشریات واقعی (نه مجازی) و در مکان‌های خاصی انجام می‌شد که رسیدن به این مکان‌ها و رفتن به آنها مستلزم سختی‌ها و مرارت‌هایی بود، اما اکنون با وجود اینترنت و سه دلیلی که قبلاً ذکر شد پورنوگرافی کودکان در اینترنت راحت‌تر و درآمدزاتر شده است. مطابق قانون فدرال آمریکا صرف گرفتن تصویری مستهجن از یک کودک یا نوجوان به منظور مشاهده بر روی صفحه مانیتور، بدون در نظر گرفتن این‌که تصویر، ذخیره شده، یا به دیگران منتقل شود، ممنوع است. (www. findarticles. com)

اگر یک کاربر به‌طور اتفاقی و بدون اطلاع به پورنوگرافی‌های کودک دسترسی پیدا کند، دچار مشکلات حقوقی و اساسی می‌شود حتی اگر به یاد نیاورد که به این تصاویر نگاه کرده است یا نه زیرا آنها در حافظه‌ی وب ثبت و ذخیره می‌شوند. توصیه‌ی کارشناسان برای کنترل گروه‌های منتشرکننده‌ی پورنوگرافی کودکان، همکاری با ارائه‌دهندگان خدمات اینترنتی برای کاهش چشمگیر مبادلات این گروه‌هاست (جنکینز،۲۰۰۱).

وب سایت‌ها به‌عنوان مجرایی برای تجاوز به حریم انسانها

چون کامپیوترها یک سرگرمی محبوب برای کودکان و نوجوانان هستند، گاهی اوقات زمانی که بچه‌ها به وب سایت‌ها دسترسی پیدا می‌کنند، خطرهای جدیدی را پیش روی‌شان قرار می‌دهند (آفتاب، ۱۹۹۹).

نوجوانانی که در سن بلوغ هستند به طور طبیعی علاقه‌مند به مسائل جنسی و صحبت کردن در مورد آن هستند بنابراین آنها در چت‌روم‌هایی که در دسترس‌شان هست با غارتگران جنسی و متجاوزان جنسی که آنها را نمی‌شناسند هم‌صحبت می‌شوند. در چت‌روم، متجاوز جنسی هویتش را جعل می‌کند و برای بچه‌ها نقش بازی می‌کند تا به‌تدریج و آرام آرام، اعتمادشان را جلب کند و با آنها صمیمی شود. متجاوزان، اغلب فریبکارند و می‌دانند که برای جلب وابستگی کودکان چگونه با آنها رفتار کنند. یک متجاوز جنسی برای گسترش وابستگی با یک قربانی، زمان زیادی را صرف می‌کند، و ممکن است به مسائل انحرافی، بچه دزدی، تجاوز جنسی و حتی قتل منجر می‌شود.

برای شناسایی و توقیف و بازداشت متجاوزان جنسی که تحت وب کار می‌کنند، پلیس از شیوه‌ی کمین استفاده می‌کند و نقش کودکان را بازی می‌کند. وقتی ملاقات حضوری ترتیب داده شد یک کودک به عنوان طعمه حاضر می‌شود و پلیس‌ها منتظر متجاوز می‌مانند تا او را توقیف کنند.

کلاهبرداری روی وب

یکی از جدی‌ترین مشکلات در مورد وب سایت‌ها این است که از کانال‌های اصلی کلاهبرداری اینترنتی محسوب می‌شوند. درست همان‌طور که تلفن، شکل‌های جدیدی از کلاهبرداری به صورت تقاضای مستقیم را به‌وجود آورد، وب هم فرصت‌هایی را برای بهره‌برداری از قربانیان از راه فریب و نیرنگ به‌وجود آورده است. قربانیان واقعاً نمی‌توانند کالاها یا خدماتی که مایل به خرید آنها هستند را ببینند. به همین دلیل ممکن است آنها سفارش خرید کالاهایی را بدهند که بی‌ارزش هستند. بازرگانان وبی لزوماً در یک نشانی مشخص فعالیت نمی‌کنند و این باعث می‌شود که مشتریانی که از کالای دریافتی خود ناراضی هستند نتوانند محلشان را پیدا کنند.

به دنبال وقایع ۱۱ سپتامبر۲۰۰۱ و بعد از آن حملات سیاه زخم روی افراد مختلف، شرکت‌ها شروع به فروش کیت‌های کشف و ردیابی سیاه زخم در وب سایت‌ها کردند. این کیت‌ها با توجه به میزان ترس از سیاه زخم به‌طور فوق العاده ای به فروش رسیدند. وکلا و نمایندگان شرکت‌ها سعی کردند تا فعالیت‌های این شرکت‌های تولید کننده را متوقف کنند (واندنبرگ،۲۰۰۴).

حراج اینترنتی

حراج‌های اینترنتی از سایت‌های رایج کلاهبرداری محسوب می‌شوند. در این نوع حراج، فروشندگان، اجناسی را که می‌خواهند به فروش برسانند پست می‌کنند و خریداران ناشناس نیز روی اجناس قیمت‌گذاری می‌کنند. با وجود قانونی بودن اکثر این حراج‌ها، محصولات بی‌ارزش نیز غالباً با این روش فروخته می‌شوند (تومس،۲۰۰۰). این نوع کلاهبرداری‌ها اغلب توسط افرادی که این محصولات را ارائه می‌دهند، صورت می‌گیرد و سرویس‌های خدماتی که معرفی این کالاها را بر عهده دارند مسئولیتی متوجه‌شان نیست. این سرویس‌های خدماتی معمولاً در قبال کیفیت یا حتی تحویل اجناس نیز مسئولیتی نمی‌پذیرند. در برخی موارد، مشاهده شده است که افراد، اجناسی را که اصلاً وجود خارجی ندارند به فروش رسانده‌اند.

فریبکاری

اینترنت برای مقاصد فریبکارانه‌ای که سوءاستفاده از احساسات و عواطف مردم است، استفاده می‌شود. نمونه‌ای از آنها، انتخاب آژانس‌هایی است که نقشه‌های کلاهبرداری را طراحی می‌کنند. طراحان این برنامه‌ها، وب‌سایتی را در اینترنت ارائه می‌دهند. این سایت شامل عکس‌های کودکان و صحنه‌های احساسی و عاطفی است. به‌طور مثال در صفحه‌ی اصلی، معمولاً زنی به‌عنوان یک

مددکار اجتماعی ظاهر می‌شود که پیشنهاد می‌دهد تا والدین برگزیده‌ای را با مادران جوانی که قادر به نگهداری از فرزندان خویش نیستند، آشنا سازد. این مددکار حدود پنج هزار تا پانزده هزار دلار دریافت می‌کند که بلافاصله باید پرداخت شود و قابل برگشت نیست. پس از طی زمان زیادی که در طول آن مددکار با متقاضیان در ارتباط است و در مراحل مختلف، مبالغ دیگری نیز دریافت می‌کند تا بتواند کودک را از مادرش بگیرد (در حالی‌که اصلاً مادر و کودک وجود خارجی ندارند)، در پایان می‌بینیم که اکثر متقاضیان در رسیدن به خواسته‌های خود، ناکام مانده‌اند. به دلیل دشواری‌های روند فرزندخواندگی به‌طور قانونی این نوع فریبکاری‌ها مورد توجه متقاضیان قرار می‌گیرد. ممکن است گرفتن سرپرستی یک کودک سال‌ها طول بکشد اما به طور غیرقانونی انتظار می‌رود مدت زمان کوتاه‌تری برای این کار لازم باشد(واندنبرگ، ۲۰۰۴).

سرقت اوراق هویت

شبکه می‌تواند به‌عنوان ابزاری برای سرقت اوراق هویتی مورد استفاده قرار گیرد. برای دزدیدن هویت یک قربانی، شخص با بهره‌گیری از شبکه به دنبال جزئیات مربوط به مسایل مالی و شخصی فرد مورد نظر می‌گردد. با وجود محرمانه بودن این اطلاعات، کلاهبرداران از انواع خدمات شبکه با هزینه اندک، استفاده می‌کنند تا از طریق سرویس‌های تجاری که چنین اطلاعاتی را به آسانی منتقل می‌کنند به این اطلاعات محرمانه دست یابند. بارها مشاهده شده است که جاعلین به شماره کارت امنیتی شخص مورد نظر دست یافته‌اند و بدین ترتیب هویت شخص را به آسانی از آن خود ساخته‌اند. به این معنا که شخص جاعل، کارت اعتباری جعلی به نام شخص تهیه می‌کند و مبلغ بالایی را از حساب خارج کرده، سپس کارت را رها می‌کند.

سرقت‌های کلانی از کارت‌های اعتباری نیز انجام گرفته است. کلاهبرداران با کارت‌های اعتباری جعلی به خرید خانه و ماشین پرداخته‌اند. در مواردی کارت بیمه عمر شخصی مورد سوء استفاده قرار گرفته که برخی از آنها، بعدها برملا شده است.

تلاش‌های بسیاری شده تا اینترنت به‌عنوان منبع امنی برای مبادلات تجاری محسوب شود، اما هنوز مشکلات بسیاری بر سر راه است. هر زمان که یک فنآوری پیشرفته در دسترس قرار می‌گیرد، خطراتی نیز آن را تهدید می‌کند. سارقان اوراق هویت قادرند به کارت‌های اعتباری رمزدار یا دیگر اطلاعات فردی شخص، دست یابند. مهارت‌های این افراد سبب می‌شود تا هر روز روش‌های پیچیده‌تری را در دستیابی به اطلاعات شخصی افراد به کار برند. از آزادی‌های بیشتری که به وسیله‌ی اینترنت حاصل می‌شود، می‌توان به عنوان ظرفیت بالای آن برای تسهیل میلیون‌ها معامله‌ای که خارج از نظارت مستقیم دولت انجام می‌شود، اشاره کرد.

استفاده‌ی غیر قانونی از کامپیوترها

بسیاری از مشکلات مطرحی که با ورود کامپیوترها گسترش یافته‌اند، به استفاده‌ی غیر قانونی از کامپیوترهای دیگران مربوط است. بسیاری از هکرهای کامپیوتری تصور می‌کنند که اجازه دارند تا از طریق ارتباطات شبکه‌ای به کامپیوترهای دیگران وارد شوند و به اطلاعات آنها دست یابند. تعداد کمی از آنها بر این باورند که دستیابی به اطلاعات کامپیوتری افراد، برای نابود کردن مقاصد شوم، قانونی و اخلاقی است. اعمال مخرب کامپیوتری، اغلب خسارت‌های میلیارد دلاری را به دنبال خواهد داشت.

هک‌کردن

هک‌کردن، یک استفاده‌ی غیرقانونی ساده از کامپیوتر اشخاص دیگر، بدون اجازه یا اطلاع آنهاست. هکرها از طریق مودم‌ها (ارتباطات تلفنی) یا خطوط شبکه به ماشین‌ها وارد می‌شوند. امروزه، اینترنت می‌تواند به‌عنوان مجرایی برای هک‌کردن به‌کار رود. یک هکر، شگردهای گوناگونی برای دسترسی به یک دستگاه به‌کار می‌برد. یک روش، عبارت است از به‌دست آوردن رمز(password) های ثبت شده‌ی داخلی. در این روش، شخص از طریق هک‌کردن ماشین‌ها، یک لیست به‌دست می‌آورد و یک یا تعداد بیشتری از رمزها را برای استفاده به‌کار می‌گیرد. همچنین شخص می‌تواند روش‌های احتمالی (تلاش‌هایی که قبلاً انجام شده است) را با رمزهای محتمل برای دسترسی به دستگاه به‌کار برد، اگر چه بسیاری از ماشین‌ها بعد از تعداد معینی از رمزهای

پذیرفته نشده اجازه دسترسی را نمی‌دهند. هکرها می‌دانند که بسیاری از کامپیوترهای تجاری بزرگ درهای عقبی (backdoors) (راه‌هایی برای برنامه نویسان کامپیوتر یا تعمیرکاران برای دسترسی سریع‌تر) دارند و اغلب امتیازاتی از این درها برای دسترسی می‌گیرند. گروه‌های هکر که اغلب از طریق یک بولتن بورد یا لیست کاربران عمل می‌کنند، غالباً کیت‌هایی را تهیه می‌کنند که اعضایشان بتوانند دسترسی سریع‌تری پیدا کنند. این کیت‌ها عبارتند از برنامه‌هایی که شامل کدهای احتمالی برای دسترسی به سیستم‌های کامپیوترهای تجاری بزرگ هستند. این برنامه‌ها برای خرید یا مبادله ارائه می‌شوند و ممکن است توسط آخرین کاربران اصلاح شده و تغییر کنند. گاهی اوقات، هکرها درون یک سیستم برای مواجهه‌ی شخصی عمل می‌کنند، به این ترتیب که وقتی با یک‌سری موضوعات که رمز حفاظت شده دارند، روبرو می‌شوند، هر تلاشی برای دسترسی آنها انجام می‌دهند. می‌شود گفت که این رمزهای حفاظت شده برای هکر یک دعوت به مبارزه هستند. حتی اگر موضوعات آن کاملاً خارج از علاقه‌ی او باشند.
هکرها در اینترنت یک خرده فرهنگ معین تشکیل داده‌اند که در آن هکرها در مورد توانایی‌هایشان اغراق می‌کنند و با هم رقابت می‌کنند. آنها سعی می‌کنند در بین اعضای این خرده فرهنگ پایگاه بهتری کسب کنند.
باوجود رقابت‌هایی که گاه و بیگاه صورت می‌گیرد هکرهای واقعی بر این باورند که آنچه در فکر آنها می‌گذرد، به‌عنوان رفتار یا تفکری مناسب است. بر طبق اصول اخلاقی هکرها که در وب‌سایت دانشگاه کالیفرنیا ارائه شده است :

۱. دسترسی به منابع کامپیوتری باید نامحدود و کامل باشد.
۲. همه‌ی اطلاعات باید به‌طور رایگان در دسترس قرار گیرد.
۳. تو نباید ویران کنی (دانشگاه کالیفرنیا، ۲۰۰۲).

بدینسان ما می‌بینیم که آنها علاقه‌مند به آزادی کامل و دسترسی هستند، نه تخریب و نابودی.
برخلاف این حقیقت که هکرها مسئول هزینه شدن درآمد حاصل از شرکت‌های بزرگ و درآمد دولت هستند، که برای امنیت سیستم‌هایشان در برابر هکرها هزینه می‌کنند، از نظر آنها، این کار اخلاقی محسوب می‌شود. واضح است که با وجود اقداماتی که انجام می‌شود، سازمان‌ها نمی‌توانند اجازه‌ی دسترسی‌های نامحدود به فایل‌های امنیتی‌شان را بدهند. به همین دلیل صرف‌نظر از اهدافی که راجع‌به آنها بحث شد، هک کردن، یک اقدام مخرب محسوب می‌شود.

نتیجه گیری

با مطالعه کج‌روی‌ها در فضای مجازی و مقایسه‌ی آنها با انواع کج‌روی در فضای واقعی می‌توان به این نکته رسید که اعمال انحرافی در اینترنت و فضای مجازی به مراتب راحت‌تر انجام می‌شوند و در مقابل، پی‌گیری و شناسایی عاملان کج‌روی در این فضا، به خاطر ویژگی‌های خاص آن دشوارتر است. نمی‌توان در اینترنت، در همه‌ی زمینه‌های کج‌روی مانند فضای واقعی، نقش زیادی برای نیروهای امنیتی و پلیس و غیره قایل شد و در حوزه‌هایی هم که پلیس نقش دارد، لازم است قوای فکری و ابزار تکنولوژیکی پلیس، همیشه یک گام از متخلفان اینترت جلوتر باشد.
در بسیاری از جاها، به‌دلیل جدید بودن فنآوری، هنوز پلیس آموزش‌دیده و همین‌طور امکانات تکنولوژیکی مناسب برای مبارزه با جرایم اینترنتی وجود ندارد (راودراد، ۱۳۸۴).
بنابراین آنچه در فضای مجازی مفیدتر و کارآمدتر است، آموزش و هوشیاری کاربران اینترنت است. مفید است در کنار یادگیری اولیه استفاده از کامپیوتر و اینترنت، کودکان و کسانی که در آغاز راه ورود به فضای مجازی هستند مهارت‌هایی را نیز در زمینه‌ی برخورد با موارد کج‌روی در اینترنت کسب کنند. در این میان، نظارت والدین و مربیان در مدارس و نهادهای آموزشی نیز می‌تواند کارساز باشد. نظارت نهادهای مسئول، مواقعی که کاربران حقیقی و حقوقی در معرض آسیب قرار دارند در زمینه‌هایی مانند کاهش فعالیت هکرها، غارتگران جنسی و کلاهبرداران اینترنتی، نقش ایفا می‌کند. اما آن‌چه مهم است، تفاوت قایل شدن میان سانسور و فیلتر کردن بی‌مورد و سلیقه‌ای، و نظارت بر موارد انحراف است. این امر با کنترل عملکرد سایت‌های مختلف در زمینه‌ی کج‌روی امکان‌پذیر است تا با سوء استفاده از افراد آسیب‌پذیر باعث صدمات اجتماعی نشوند.

در نقش عمیقی که هم‌اکنون اینترنت در زندگی ما ایفا می‌کند و تاثیر بسیار زیادی که در تعاملات ما دارد، شکی نیست و همه کاربران اینترنتی ممکن است زمانی هدف هر یک از اعمال انحرافی از سرقت اوراق هویت گرفته تا انحراف جنسی قرار گیرند. پس نادیده گرفتن آن و توصیه به عدم استفاده و یا کاهش استفاده کاربران، راهکار غیر منطقی به نظر می رسد.

با توجه به توضیحاتی که دادیم نمی‌توان همه‌ی اطلاعات از جمله اسرار تجاری معاملات و مبادلات بزرگ، مشخصات هویتی وشخصی افراد، تصاویر مستهجن و اطلاعاتی که افراد تمایل ندارند در اختیار دیگران قرار گیرند را به‌طور آزاد در دسترس همه قرار داد. با توجه به این‌که کودکان و نوجوانان و افراد ناآگاه در معرض غارتگران اینترنتی هستند باید با پیامدهای منفی اینترنت مقابله کرد و از آسیب‌های ناشی از آن کاست.

منابع

منابع فارسی

بازرمن، ر (۲۰۰۶)، **مستهجن‌نگاری‌کودکان در اینترنت: اسطوره، حقیقت و نظارت اجتماعی**، در
http://www. iranculture. org/pdf/research/internet/۱/. pdf

راودراد، ا (۱۳۸۴)، **مسایل اجتماعی زنان در اینترنت**، فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، شماره ۲ و ۳، ص ص ۷۳ تا ۹۲.

صدیق سروستانی، ر (۱۳۸۳)، **آسیب شناسی اجتماعی**، تهران، انتشارات آن.

عبداللهیان، ح (۱۳۸۴)، **نوع شناسی و باز تعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران**، فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، شماره ۲ و ۳، ص ص ۱۳۵تا ۱۵۴.

کستلز، م (۱۳۸۰) **عصراطلاعات : اقتصاد،جامعه و فرهنگ ظهورجامعه شبکه ای**، ترجمه احمد علیقلیان و افشین خاکباز و حسن چاوشیان، ویراستارعلی پایا، تهران، انتشارات طرح نو.

کیا، ع، ا (۱۳۷۸)، **اینترنت و تاثیرات اجتماعی آن**، روزنامه ایران، ۲ خرداد.
لاسر، م (۲۰۰۶) در
http://www. iranculture. org/research/internet/viewpajohesh. php?id=۳۰

منابع انگلیسی

Aftab, P. (۱۹۹۹) **The Parent`s Guide to Protecting Your Children in Cyber space**. New York : McGraw-Hill.

Hunter , R. (۲۰۰۲) **World Without Secrets : Business , Crime , and Privacy in the Age of Ubiquitous Computing**. New York : John Wiley.

Jenkinz , P. (۲۰۰۱) **Beyond Tolerance : Child Pornography Online**. New York : NYU Press.

Mcbain, M. A. (۲۰۰۲) **Internet Pornography**. New York: i Universe.

Mccaghy ,C. H. & Capron , T. A. & Jamieson , J. (۱۹۹۹) **Deviant Behavior : Crime , Conflict , and Internet Groups**. Boston:Allyn and Bacon.

Rand Corporation , (۱۹۹۵) **Universal Access to E-Mail : Feasibility and social Implication**,Word Wide Web, http://www. rand. org/publications/MR/MR۶۵۰

Thomes , J. T. (۲۰۰۰). **Dotcons : Con Games, Fraud , and Deceit on the Internet**. New York : i Universe.

Vandenburgh ,H. (۲۰۰۴) **Deviance,the Essentials**. Upper Saddle River, NJ : Pearson :Allyn and Bacon.

Williams, J. (۱۹۹۷) **Cellular and Cordless Phone Phreaking**. New York: consumertronics.

منابع اینترنتی

www. securityfocus. com/news
www. irna. ir/schooolMediaStudies/NewsRoom
http://galent. galegroup. com
www. obscenitycrimes. org
www. hamshahri. org
www. findarticles. com
www. looksmart. com
www. rashtmarket. com