دوفصلنامه علمی- پژوهشی دین و ارتباطات، سال بیست و چهارم، شمارهٔ دوم (پیاپی ۵۲)، پاییز و زمستان ۱۳۹۶ صص ۹۹-۱۲۸

چالش‌های اعاده حیثیت در فضای مجازی

علی غلامی *

مسعود پیرهادی **

تاریخ دریافت: ۱۳۹۵/۰۷/۰۴

تاریخ پذیرش: ۱۳۹۶/۰۲/۲۸

چکیده

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

یکی از مصادیق مهم فناوری پیشرفته، فضای سایبر، 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 آن¬ها، 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 آن-طور که می‌توان در فضای حقیقی، اعاده حیثیت نموده و خسارت معنوی وارد آمده به اشخاص را جبران کرد، در فضای مجازی چنین امکانی وجود ندارد. در واقع قوانین فعلی، امکان اعاده حیثیت اشخاص را از جرایم سایبری ایجاد نمی‌کند و می‌بایست با اتخاذ روش‌های پیشگیرانه و آموزش‌های شهروندی، مانع ارتکاب جرایم علیه حیثیت معنوی اشخاص در فضای سایبر شد.

واژگان کلیدی: *جرم علیه حیثیت معنوی، جرم رایانه‌ای، جرایم سایبری، فضای سایبر، اعاده حیثیت.*

* دانشیار دانشکده معارف اسلامی و حقوق دانشگاه امام صادق (علیه‌السلام) (نویسنده مسئول) gholami@isu.ac.ir

** کارشناسی ارشد معارف اسلامی و حقوق جزا و جرم‌شناسی دانشگاه امام صادق (علیه‌السلام) Masoud.pirhadi@gmail.com

مقدمه

فضای مجازی در سال‌های اخیر به صورت حیرت‌آوری وارد زندگی انسان‌ها شده است؛ به نحوی‌که زندگی بدون امکانات آن، دشوار به نظر می‌آید. فضای مجازی[1] از آن‌جا که محیطی، مخفی، آزاد و نامحدود است، احتیاج به نظم دارد و اگر خلاف این باشد، هر «صفحه» از این محیط می‌تواند صحنه جرم باشد. امروزه مجرمان حیطه سایبر، از فضای مجازی به‌عنوان 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 نمی ماند، 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).

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 بار آورده و درعین‌حال ناشناخته باقی بمانند. هتاکی و اهانت، نشر اکاذیب، 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.

ارائه تعریف مشخص و مختار از جرم رایانه‌ای نیز دشوار است، لیکن 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 ٤).

در این مقاله ابتدا به مفهوم و شیوه‌های اعاده حیثیت پرداخته شده و سپس چالش‌های اعاده حیثیت در فضای سایبر ناظر به جرم و مجرم که مشتمل بر شش قسمت: سختی یافتن مجرم، گمنامی عامل، پیچیدگی احراز اصالت، سادگی انجام جرایم سایبری، رشد فزاینده کاربران فضای سایبر و اثر اولیه خبر کذب یا هتک حرمت بررسی و معرفی شده است و در قسمت بعد به چالش‌های اعاده حیثیت در فضای سایبر ناظر به بستر ارتکاب مشتمل بر هفت عنوان: گستره انتشار، سرعت و بلادرنگی، مانایی محتوا در فضای سایبر، عدم امکان پیشگیری، تعدد وبسایت‌ها و خبرگزاری‌های مجازی، نرخ بازدید یک باره و ترافیک بالای شبکه‌ها از دریچه فنی و علمی نگریسته شد و در پایان با نتیجه‌گیری و پیشنهادها سعی بر کاربردی شدن این مقاله شده است.

۱. مفهوم و شیوه‌های اعاده حیثیت

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

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 ٦١).

اعاده حیثیت به لحاظ لغوی از دو کلمه عربی «اعاده» و «حیثیت» ترکیب یافته است که اعاده به معنای بازگردانیدن (معین، ۱۳۸۲، ص١٣٤) و حیثیت به معنای اعتبار و آبرو (معین، ۱۳۸۲، ص٣٩٤) است و گفته شده اعاده حیثیت «بازگشت به اهلیتی است که شخص به علتی آن را از دست داده است» (جعفری لنگرودی، ١٣٦٣، ص٧٨).

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 (جعفری لنگرودی، ۱۳۸۸، ص۵۹).

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 بین رفته مجنی‌علیه به شمار می‌رود. حفظ حرمت و حیثیت اشخاص از چنان درجه‌ای از اهمیت برخوردار است که در اصل بیست و دوم 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».

دکتر سیدحسن امامی در تعریف خسارات معنوی می‌نویسد: «ضرر معنوی عبارت است از صدمات روحی و کسر حیثیت و اعتبار شخص که در اثر عمل بدون مجوز قانونی، دیگری باعث آن شده است». تعریف دیگری که در برخی قوانین آمده، می‌گوید: «ضرر معنوی عبارت است از کسر حیثیت یا اعتبار اشخاص یا صدمات روحی». همچنین ماده یک قانون مسئولیت مدنی مصوب ۱۳۳۹ با یک عبارت عام و کلی این تعریف را کامل کرد که «هر حق دیگری که به موجب قانون برای افراد ایجاد گردیده است». بنابراین ضررهای معنوی ممکن است ناشی از لطمه زدن به یکی از حقوق مربوط به شخصیت، حیثیت و شرافت افراد و یا در نتیجه صدمات روحی باشد. بنابر تعاریف ارائه شده می‌توان خسارات معنوی را به دو دسته کلی تقسیم کرد: دسته اول صدمات وارده به یکی از حقوق مربوط به شخصیت، شرافت و آزادی‌های فردی و دسته دوم، صدمات روحی و به‌طور کلی زیانی که به عواطف افراد وارد می‌شود.

البته جبران خسارت معنوی در مقایسه با اعاده حیثیت معنوی مفهوم عام‌تری دارد، بدین معنی که یکی از راهکارهای جبران خسارت معنوی، اعاده حیثیت است. در بیان

این‌که نحوه جبران صدمات معنوی چگونه است باید قائل به تفکیک شد. در برخی از خسارات معنوی پرداخت جریمه الزامی است، ولی در برخی دیگر از آن‌ها، اعاده حیثیت شخص، مورد حکم قرار می‌گیرد و در برخی موارد هر دو مجازات یعنی هم پرداخت جریمه و هم اعاده حیثیت، مقرر می‌گردد. به‌عنوان مثال، افترا علیه یک شرکت تجاری موجب وارد شدن خسارت معنوی به شرکت شده و به همین دلیل، شرکت ضرر مالی می‌کند. در اینجا می‌توان خسارت وارد شده را با پرداخت جریمه نقدی جبران کرد. اما فرض کنید به فردی نسبت ناروای قذف داده شود. در چنین شرایطی، خسارت معنوی وارد شده به فرد با پرداخت جریمه نقدی جبران نمی‌شود و علاوه بر اعمال جرایم مالی، حتماً باید اعاده حیثیت معنوی صورت گیرد.

۲-۱. شیوه‌های اعاده حیثیت

روش‌های متداول جبران خسارت معنوی بر اساس متون قانونی شامل موقوف کردن یا از بین بردن منبع ضرر، عذرخواهی شفاهی از خسارت دیده، عذرخواهی عملی یا کتبی یا درج مراتب اعتذار در جراید، اعاده حیثیت از خسارت دیده به هر نحو دیگر و پرداخت مال یا مابه‌ازای مادی به خسارت دیده می‌شود (بایگان، بانک جامع قوانین و مقررات کشور، ۱۳۹۲). [۲]

خسارت معنوی در قلمرو حقوق مدنی به‌ویژه در عرصه مسئولیت مدنی جایگاهی مهم و اساسی دارد. این خسارات، مصادیق بسیار متنوع و متعددی دارد و محدود به حد هتک حیثیت و صدمه به اعتبارات شخصی و اجتماعی نمی‌شود. البته دعاوی راجع به خسارات معنوی در محاکم قضایی ایران بسیار مهجور مانده است و برخی قضات، توجه چندانی به این‌گونه دعاوی ندارند یا حداکثر موضوع را از طریق صلح و سازش فیصله می‌دهند. در قوانین کیفری نیز خسارات معنوی مطرح و موضوع حکم قرار گرفته است. در ماده ۹ قانون آیین دادرسی کیفری از ضرر و زیانی که قابل مطالبه است و ضرر و زیان معنوی که شامل کسر حیثیت یا اعتبار اشخاص یا صدمات روحی می‌شود و باید جبران شود، اشاره شده است. همچنین در ماده ۱۴۱ قانون تعزیرات مصوب سال ۱۳۶۲ نیز خسارت معنوی در کنار خسارات مادی مورد توجه قرار گرفته

است. در متون قوانین کیفری سابق که بعضی از آن‌ها هنوز منسوخ نشده بیش از متـون موجود، بر این مهم تأکید شـده اسـت. از جملـه در مـواد ۲۱۲ مکـرر قـانون مجـازات عمومی سابق و تبصره ۱ ماده ۲۰ قانون مطبوعات سابق، قانون‌گذار با صراحت ترتیـب تعیین مابه‌ازاء مالی در قبال خسارت معنوی را مقرر کرده است.

ماده ٦۹۸ (۹۲۲) قانون مجازات اسلامی نیز مقرر می‌دارد «هرکسی به قصـد اضـرار 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 خطـی بـا امضـا یـا بـدون امضـا اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را برخلاف حقیقت رأساً یـا بـه‌عنـوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی تصریحاً یا تلویحاً نسبت دهـد، اعم از این‌که از طریق مزبور به نحوی از انحا ضرر مادی یا معنوی به غیر وارد شود یـا نه، علاوه بر اعاده حیثیت در صورت امکان، باید به حبس از دو مـاه تـا دو سـال و یـا شلاق تا ٧٤ ضربه محکوم شود». طرقی که در موارد مزبور برای اعاده حیثیت انتخـاب می شود 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 مـاده ۲۷ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مصوب ۱۳٤۸، ذیل مـاده ۱۷ قـانون اقدامات تأمینی و ماده ۲۹۸ قانون آیین دادرسی در امور کیفری به این شیوه اشاره دارد. در این ماده آمده است: «شاکی خصوصی می‌تواند از دادگاه صـادرکننـده حکـم نهـایی درخواست کند که مفاد حکم در یکی از روزنامه‌ها به انتخاب و هزینه او آگهی شـود». از آن‌جا که اعاده حیثیت با آبروی افراد در ارتباط است، مستلزم اطلاع‌رسانی به دیگران پس از صدور حکم است و به همین دلیل در مواردی قانون‌گذار این امکان را در اختیار افراد قرار می‌دهد. ماده ۱۰ قانون مسؤلیت مـدنی مصـوب ۱۳۳۹ نیـز همـین راه‌حـل را تجویز کرده است.

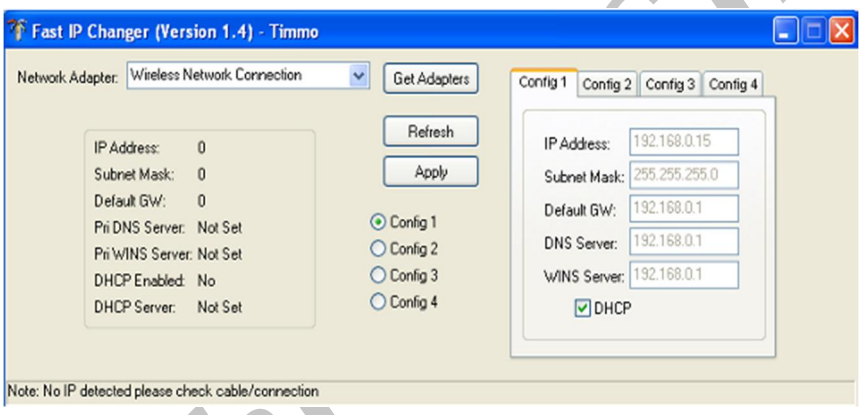
۲. چالش‌های اعاده حیثیت در فضای سایبر ناظر به جرم و مجرم

۲-۱. سختی یافتن مجرم

گاهی اوقات عامل انتشار یک خبر، رویداد، عکس و یا فیلم، مشخص است، اما یـافتن

او کار آسانی نیست. شاید بتوان این مطلب را این‌طور 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.

در فضای سایبر هر دستگاهی که به اینترنت متصل می‌شود دارای یک شناسه عددی یا همان IP [۳] است. این شناسه همانند کد ملی افراد، یکتاست و هیچ دو دستگاهی که به اینترنت متصل می‌شوند، IP یکسان ندارند. ازاین‌رو مانند اثر انگشت عمل می‌کند و در واقع کمکی برای یافتن مجرم است.



تصویر شماره ۱، تصویر نرم‌افزار 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 شناسه یک دستگاه می‌توانند کشور، شهر و حتی حدود منطقه آن را بفهمند اما این کار با چالش‌هایی روبروست:

الف) معمولاً 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، روزانه ده‌ها نفر از آن استفاده می‌کنند و

مشخص نیست اگر از طریق آن جرمی صورت پذیرفت، باید به سراغ چه کسی رفت.

ج) مسئله دیگر آن است که در هر ساعت، صدها جرم در فضای سایبر صورت می‌گیرد که بالقوه قابل تعقیبند اما در عمل به دلیل هزینه بالا، همه جرایم تعقیب نمی‌شوند. به همین دلیل است که پلیس‌های سایبری دنیا ـ در ایران پلیس فتا[۴] ـ 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[۵] انجام‌دهنده یک کار یا منتشرکننده 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.

۲-۲. گمنامی عامل[۶]

گمنامی در اصطلاح فضای سایبر، به معنای عدم امکان دسترسی به هویت و مشخصات تولیدکننده و یا نشردهنده یک محتوا، اعم از متن، فیلم و یا عکس است (Kabay, 1998, p12). معنای این مطلب آن نیست که عامل انتشار اولیه 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.

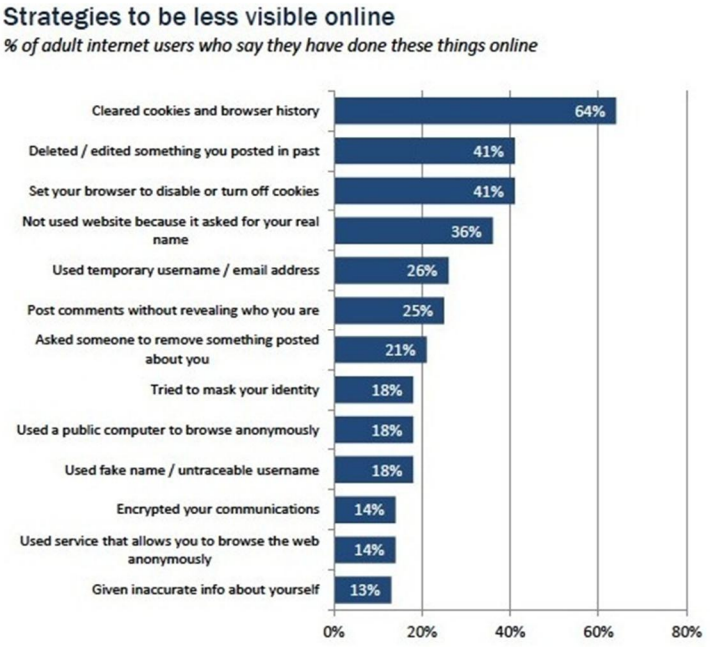
یکی از راه‌های ایجاد گمنانی استفاده از پراکسی‌ها[۷] است. پراکسی‌ها به‌گونه‌ای عمل می‌کنند که کاربر پس از اتصال به آن، ردی از خود به‌جا نمی‌گذارد و دیگران آثار کار او را، آثار پراکسی می‌بینند. در واقع پراکسی دیواری است که عامل، از پشت آن اقدام به فعالیت در فضای سایبر می‌نماید و دیگران فقط دیوار را می‌بینند. وی‌پی‌ان[۸] نوع دیگری از اتصال به اینترنت است که کاربرد مشابهی دارد. انواعی از پروتکل‌های اینترنتی وجود دارند که موجب گمنامی عامل را فراهم می‌سازد. تأمین گمنامی عامل یکی از شاخه‌های علم امنیت اطلاعات[۹] است و ذاتاً مذموم نیست، بلکه استفاده‌هایی از این ویژگی فضای سایبر می‌شود که می‌تواند مخرب و مجرمانه باشد (Ferguson, 1998, p.9)

در چند گزارش که پس از کشف حمله ویروس استاکس نت[۱۰] به تأسیسات اتمی ایران منتشر شده بود، در بخش‌هایی از حمله به اطلاعات و داده‌های حساس، تلاش شده بود تا پس از آن، سابقه کار[۱۱] از سامانه‌های اطلاعاتی ایران پاک شود و به همین دلیل شناسایی این فعالیت مخرب، ماه‌ها به تأخیر افتاد. این در واقع یک نمونه عینی تلاش برای گمنامی عامل در یک حمله مخرب سایبری است.[۱۲] نمونه‌های فراوانی از جرم علیه حیثیت معنوی در فضای سایبر وجود دارند که پایه اصلی آن‌ها گمنامی عامل بوده است. انتشار تصاویر خصوصی زندگی اشخاص مشهور در وب‌سایت‌های ثبت نشده و بی‌شناسنامه 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 به‌دست 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 معتبر در سامانه (pew research center) است، حدود ۸۶ درصد از کاربران اینترنت، علاقه‌ای به رصد[۱۳] و دنبال شدن در این فضا ندارند و دوست دارند به‌عنوان یک شخصیت گمنام در

فضای اینترنت حضور داشته باشند. بدین منظور، این افراد از پاک کردن کوکی‌ها[۱۴] و تاریخچه[۱۵] تا تغییرات تنظیمات پیش‌فرض رایانه خود، ساختن ایمیل با نام جعلی و ... انجام می‌دهند.



نمودار شماره ۱، اقدامات برای گمنام ماندن در فضای اینترنت[۱۶]

۳-۲. پیچیدگی احراز اصالت[۱۷]

احراز اصالت به معنی تعیین و اثبات عامل حقیقی انجام یک عمل است. گاهی اوقات این مفهوم با گمنامی عامل اشتباه گرفته می‌شود درحالی‌که تقریباً این دو مفهوم عکس یکدیگرند. ویژگی گمنامی عامل یعنی در یک تراکنش[۱۸]، عامل انجام یک کار می‌تواند اگر بخواهد هویت خود را مخفی نگه دارد. احراز اصالت یعنی آن که عامل انجام یک کار یعنی فرستنده 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

آمریکایی یا اروپایی هستند. به‌عنوان 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 به‌عنوان 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.

٤-۲. سادگی انجام جرایم سایبری

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 نامه الکترونیکی دان پارکر[۱۹] به پروفسور سوزان برنر[۲۰] 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» (Brenner, 2001, p.48)

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 وجود دارد. 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 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 محتوا در فضای سایبر ماناست و با حذف از یک سایت و دو سایت اعاده به وضع سابق اتفاق نمی‌افتد.

۵-۲. رشد فزاینده کاربران فضای سایبر

الف) میزان رشد کاربران فضای سایبر در ایران

در سال‌های اخیر، نفوذ روزافزون فضای سایبر در زندگی تمام مردم به دلایلی همچون پایین بودن هزینه استفاده از آن، افزایش چشم‌گیر بهره‌وری، بی‌انتها بودن در بسیاری از سطوح اجتماعی و نامتقارن بودن در آسیب‌پذیری موجب شده دول مختلف در دوران کنونی، این فضای قدرتمند را به‌عنوان 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.

جدول شماره ۱، میزان رشد کاربران فضای مجازی در ایران

ب) میزان رشد کاربران فضای سایبر در جهان

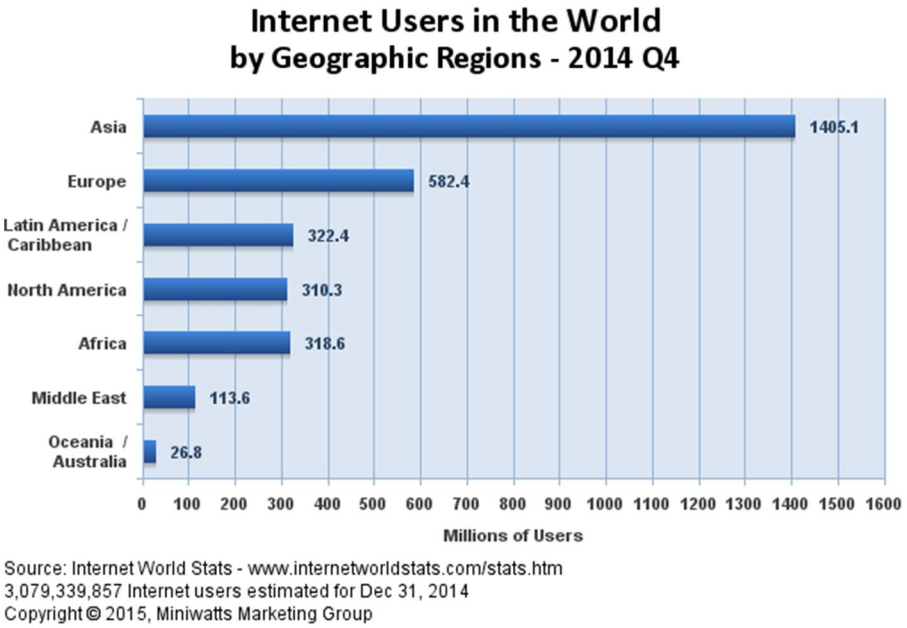
منبع	درصد	جمعیت	تعداد کاربران	سال
www.itu.int	۳.۸	٦۹.٤٤۲.۹۰٥	۲٥۰.۰۰۰	۲۰۰۰
www.itu.int	۷.٥	٦۹.٤٤۲.۹۰٥	٥.٥۰۰.۰۰۰	۲۰۰۲
www.itu.int	۱۰.۸	٦۹.٤٤۲.۹۰٥	۷.٥۰۰.۰۰۰	۲۰۰٥
www.itu.int	۳٤.۹	٦٥.۸۷٥.۲۲۳	۲۳.۰۰۰.۰۰۰	۲۰۰۸
Internetworldstats	٤۸.٥	٦٦.٤۲۹.۲۸٤	۳۲.۲۰۰.۰۰۰	۲۰۰۹
Internetworldstats	٤۳.۲	۷٦.۹۲۳.۳۰۰	۳۳.۲۰۰.۰۰۰	۲۰۱۰
Internetworldstats	٥۳.۳	۷۸.۸٦۸.۷۳۱	٤۲.۰۰۰.۰۰۰	۲۰۱۲
Internetworldstats	٥۷.۲	۸۱.۸۲٤.۲۷۰	٤٦.۸۰۰.۰۰۰	۲۰۱٥

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

جدول شماره ۲، تعداد کاربران فضای سایبر در جهان

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 %**

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



نمودار شماره ۲، درصد کاربران فضای مجازی و اینترنت در قاره‌های مختلف

٦-۲. اثر اولیه خبر کذب یا هتک حرمت

در فضای اطلاع‌رسانی و خبر، در شرایط برابر از حیث اعتبار معمولاً خبر آن رسانه‌ای در ذهن مردم می‌نشیند و از سوی آن‌ها مقبول می‌افتد که 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.

این‌که حیثیت چگونه و در چه شرایطی هتک شود، تابعی از چند عامل است که یکی از آن‌ها بستر وقوع جرم است. در فضای مجازی به‌عنوان بستر جرمی که در این مقاله مورد بررسی قرار گرفته، به دلیل ویژگی‌هایی از جمله سرعت و گستره انتشار بالای مطالب، آن فردی که در یک موضوع اولین خبر را منتشر می‌کند، بیش از دیگران می‌تواند ذهن‌ها را در تصرف خبر خود درآورد. حال آن‌که در مطبوعات و رسانه‌های

مکتوب عموماً چنین اتفاقی یا رخ نمی‌دهد و یا شدت آن به مراتب کمتر است.

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. به‌عنوان 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 می‌کند. به‌عنوان مثال این خبر از طریق چند سایت نامعتبر منتشر می‌شود که علت صدا، انفجار یک بمب توسط داعش بوده و در اثر آن یک مسئول بلندپایه دولتی جان باخته است. در چنین شرایطی اگر خبر درست با تأخیر به‌دست مردم برسد، دیگر خیلی کسی شنوای آن نیست. همان‌طور که از مثال برمی‌آید، سرعت در اطلاع‌رسانی موضوعیت دارد و این بار معمولاً به دوش رسانه‌های مجازی است. چه آنکه بلافاصله پس از وقوع یک پدیده، ذهن‌های کنجکاو، عطشی برای دانستن علت پدیده دارند که در صورتی که این عطش با شنیدن خبر غلط فروکش کند، دیگر جویای علت اصلی پدیده نخواهد بود و در صورتی که خبر صحیح به افراد برسد، در صحت آن تشکیک خواهند کرد.

با توجه به نکات پیش‌گفته اعاده حیثیت یا جبران خسارت معنوی با عنایت به اثر مخرب اولیه در انتشار خبر کذب یا هتک حرمت علیه اشخاص با صعوبت یا عدم امکان همراه خواهد بود.

۳. چالش‌های اعاده حیثیت در فضای سایبر ناظر به بستر ارتکاب

۱-۳. گستره انتشار[۲۱]

اگرچه فضای سایبر و شبکه جهانی وب دو تعریف مجزا اما نزدیک به هم دارند، در یک نگاه کل به جزء می‌توان آن‌ها را نزدیک به هم درنظر گرفت. شبکه جهانی وب (www)[۲۲] آن‌طور که از نام آن برمی‌آید، همچون یک تار عنکبوت گسترده است که در

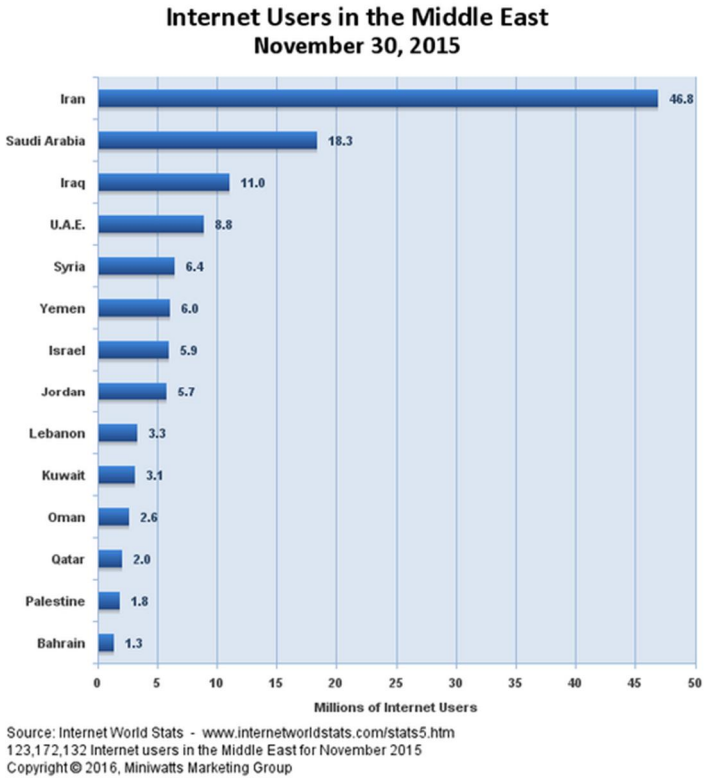
سرتاسر کره زمین تنیده شده و از همین رو شاید نتوان رسانه‌ای یافت که گستره‌ای وسیع‌تر از آن داشته باشد.

این گستردگی در بسیاری از موارد، مستقل از شرایط است. این بدان‌معناست که تولیدکننده و یا انتشاردهنده یک مطلب در فضای سایبر هرچقدر هم که خرد باشد، از گستره انتشاری، معادل با یک تولیدکننده و یا انتشاردهنده کلان برخوردار است. این خود، یکی از وجوه قابل تأمل در ارتباط با ارتکاب جرایم در فضای سایبر است. چه این‌که رسانه‌های کلان به جهت حیثیت و اعتباری که دارند، برای ارتکاب جرایم، انگیزه 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. پیام‌های اینترنتی می‌توانند از نوع تک‌فرستنده ـ تک‌گیرنده[۲۳] 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 ازآن‌رو استفاده شده که سرویس‌دهنده ابزار چت و احیاناً شنودکننده‌ها[۲٤] 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.

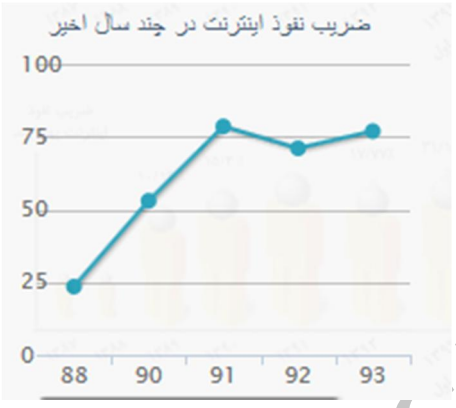
از آن‌جا که جرایم مورد نظر در این مقاله، «جرایم علیه حیثیت معنوی اشخاص» می‌باشد، علی‌القاعده مجرم یا مجرمین، بیشتر مایلند از پیام‌های نوع دوم، یعنی پیام‌هایی که توسط یک فرستنده (خود مجرم) روی شبکه جهانی وب قرار گرفته و برای تمام کاربران اینترنت قابل رؤیت باشد، استفاده کنند. نکته قابل ملاحظه دیگر آن است که ضریب نفوذ اینترنت در تمام دنیا و همچنین در کشور ما در حال رشد است. این بدان معناست که گستره انتشار فضای سایبر اگرچه بسیار وسیع است، اما در همین حد هم

نخواهد ماند و روزبه‌روز گسترده‌تر خواهد شد. این مسئله بر پیچیدگی بررسی وقوع جرم در این فضا می‌افزاید. آمارها نشان می‌دهد که ایران در آذرماه ۱۳۹٤ با ٤٦/۸ بیشترین درصد استفاده‌کنندگان از اینترنت را در منطقه غرب آسیا داشته است.



نمودار شماره ۳، درصد کاربران اینترنت در خاورمیانه (غرب آسیا) ۳۰ نوامبر ۲۰۱۵ (۹٤/۹/۹ شمسی)[۲۵]

غیر از درصد کاربران، ضریب نفوذ اینترنت[۲٦]، 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 دست‌کم در یک سال گذشته یک بار به اینترنت متصل شده و از آن استفاده کرده باشد».[۲۷]



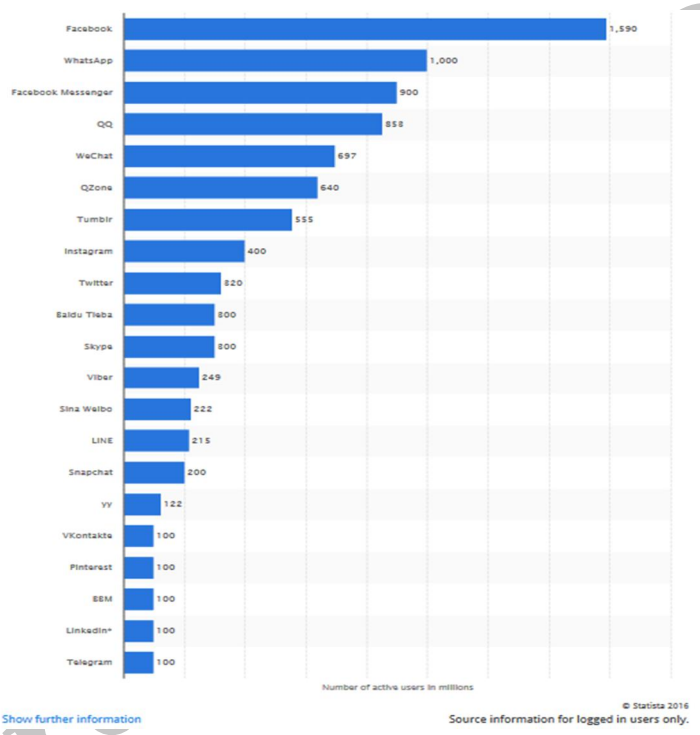
نمودار شماره ٤، میزان ضریب نفوذ اینترنت در سال‌های اخیر

علاوه بر موضوع افزایش ضریب نفوذ اینترنت، امروزه ابزارها، سایت‌ها و امکاناتی برای کمک به انتشار قوی‌تر و گسترده‌تر پیام‌ها به وجود آمده است که شبکه‌های اجتماعی، پایگاه‌های بارگذاری فیلم و عکس و خبرخوان‌ها از این‌دسته‌اند. به‌عنوان مثال 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 این‌که آن‌ها بیشتر در معرض استفاده عموم هستند و ممکن است تعداد کاربرانی که به آن‌ها رجوع می‌کند، چند برابر یک تولیدکننده یا انتشاردهنده معمولی باشد.

در حال حاضر شبکه‌های اجتماعی متعددی به زبان‌ها و با کارکردهای مختلف وجود دارند که از مهم‌ترین آن‌ها می‌توان به فیسبوک[۲۸]، توییتر[۲۹] و اینستاگرام[۳۰] اشاره کرد. برخی از این شبکه‌های اجتماعی گستره کاربران توزیع‌شده‌تری[۳۱] دارند، مانند

فیسبوک و برخی اغلب کاربرانشان در یک یا دو کشورند، مانند شبکه اجتماعی کیوکیو[۳۲] که اغلب کاربرانش چینی هستند. جدول زیر نام و تعداد کاربران ۲۱ شبکه اجتماعی پر مخاطب دنیا را نشان داده است. لازم به ذکر است اعداد درون جدول بر حسب میلیون هستند، به‌عنوان مثال، وایبر[۳۳] در دنیا ۲۴۹ میلیون کاربر دارد.



نمودار شماره ۵، پربیننده‌ترین شبکه‌های اجتماعی دنیا، سال ۲۰۱۶

۲-۳. سرعت و بلادرنگی[۳۴]

یکی از ویژگی‌های اختصاصی فضای سایبر به‌عنوان 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 فاصله تولید تا انتشار یک پیام اعم از متن، فیلم و یا

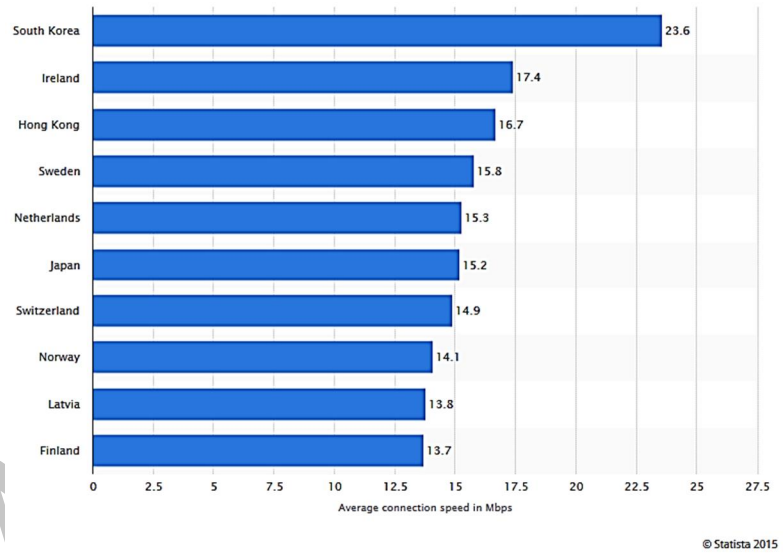
عکس کمتر باشد، فرصت کمتری برای پیشگیری از وقوع جرم وجود خواهد داشت. در مورد رسانه‌های برخط[۳۵] این امکان تقریباً به صفر می‌رسد و شاید بتوان گفت پیشگیری نشدنی است.

غیر از این نکته، می‌توان به افزایش انگیزه مجرم در ارتکاب جرم به جهت سرعت بالا در انجام جرم اشاره کرد. وقتی مقدمات وقوع جرم مفصل و زمان‌بر باشد، انگیزه 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 ـ مثلاً در حد اتصال اینترنت ـ و تنها وسیله 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، ازآن‌رو 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 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 نه‌تنها 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. به‌عنوان مثال، اگر روزنامه‌ای جرمی مرتکب شود که حیثیت معنوی شخص 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، مسئله 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 پیش‌رو کشورهای با بیشترین سرعت اینترنت در دنیا به ترتیب مشخص شده‌اند.



نمودار شماره ٦، کشورهای دارای پرسرعت‌ترین اینترنت دنیا

کره‌جنوبی با میانگین سرعت ۲۳.٦ مگابیت در ثانیه دارای پرسرعت‌ترین اینترنت دنیاست.

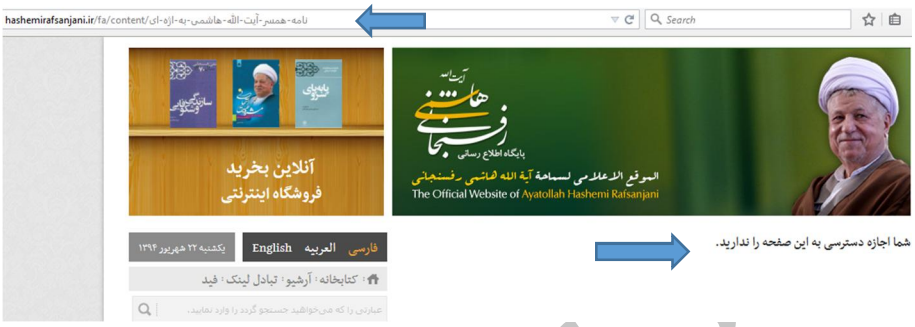
در کشور ما نیز رشد سرعت اینترنت، بسیار بالا بوده ولی همچنان در رده کم سرعت‌ترین اینترنت‌های جهان به سر می‌برد.

۳-۳. 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.

به‌عنوان 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 اطلاع‌رسانی حجت‌الاسلام 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 ۲، تصویر خبر پایگاه اطلاع‌رسانی حجت‌الاسلام هاشمی رفسنجانی لیکن مانایی محتوا در این فضا باعث شد، این خبر در فضای مجازی باقی بماند.



تصویر شماره ۳، صفحه خبر حذف شده از پایگاه اطلاع‌رسانی حجت‌الاسلام هاشمی رفسنجانی

یک مثال روشن دیگر از این موضوع RSS-R[۳۶] 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-Rها قابل مشاهده‌اند. برخی RSS-Rها 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 مجموعه خود نگهداری می‌کنند.[۳۷]

بارها اتفاق افتاده که دولت‌های مقتدر دنیا در عرصه فضای مجازی تصمیم به حذف کامل یک محتوا از اینترنت گرفته‌اند و موفق نشده‌اند. به‌عنوان نمونه، دولت آمریکا بارها تلاش کرده که از انتشار تصاویر قربانیان بلایای طبیعی جلوگیری کند. در طوفان نیواورلئان[۳۸] 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.[۳۹] از آن پس، در بحران‌های متعددی که در ایالات متحده آمریکا روی داده، می‌توان گفت

که با جستجو در اینترنت به ندرت شاهد تصویر ناراحت‌کننده‌ای از قربانیان خواهیم بود که مثالی از کار این کمیته ویژه، نظارت بر انتشار اخبار و تصاویر طوفان کاترینا‌ست.[۴۰]

٤-۳. عدم امکان پیشگیری

ماهیت فضای سایبر به گونه‌ای است که پیشگیری، یکی از تدابیر ناگریز و لازم‌الاجرا محسوب می‌شود. حتی در دنیای فیزیکی نیز این سخن، صادق است، زیرا تنها گزینه‌ای است که می‌تواند فرصت و ابزار ارتکاب جرم را هدف قرار دهد (جلالی فراهانی، ۱۳۸٤،ص ۱۳). لیکن 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. به‌عنوان مثال مجرمی 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 حافظه 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 ۹٤ در سایت خبری «الف» رخ داد. در بخش نظرات،[۴۱] 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 غیرکیفری که مبتنی بر اتخاذ تدابیری با ماهیت غیرکیفری 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 آنچان‌که شایسته است نه موجبات تأدیب بزه‌کاران را فراهم می‌کند و نه دردی از دردهای بزه‌دیده تسکین می‌یابد. فلذا می‌بایست برای این چالش مهم فضای مجازی که سختی و صعوبت پیشگیری است، اقدامات اساسی اجتماعی و فرهنگی انجام داد.

۵-۳. تعدد وب‌سایت‌ها و خبرگزاری‌های مجازی

طبق آمار منتشره سازمان تنظیم مقررات رادیویی که به ساماندهی موضوع اینترنت در کشور می‌پردازد، حدود ۸۰۰ هزار 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.[۴۲] درحالی‌که 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.

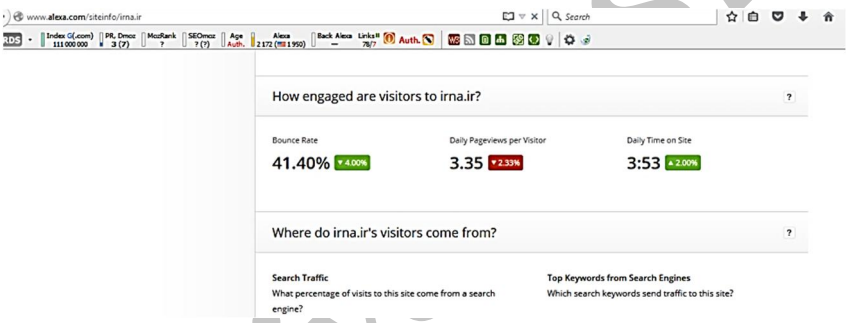
بالا بودن این تعداد، علاوه بر دشوار ساختن امکان پیشگیری از وقوع جرم، نظارت بر عملکرد این پایگاه‌ها و در نتیجه اعاده حیثیت را با سختی زیاد همراه می‌کند؛ چه اینکه گاهی ممکن است جرم علیه حیثیت معنوی یک شخص در فضای مجازی صورت بگیرد و مجنی‌علیه از تبعات آن متضرر شود لیکن از وقوع جرم علیه خود مطلع نشود.

۶-۳. نرخ بازدید یک باره[۴۳]

یکی از ویژگی‌های وب‌سایت‌ها و خبرگزاری‌های مجازی، درصد بازدیدکنندگانی است که فقط یک‌بار 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

می‌خوانند 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 بعداً تکذیب شود، بیننده خبر، تکذیبیه آن را نخواهد دید.

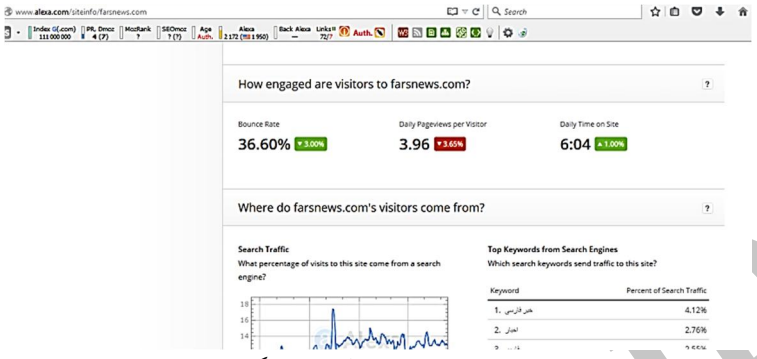
با توجه به این ویژگی، اگر در سایتی خبری قرار بگیرد که هتک حیثیت معنوی شخص یا اشخاصی محسوب شود، عملاً امکان اعاده حیثیت وجود ندارد، حتی اگر خبر اصلاح و یا تکذیب شود. برای نمونه نرخ بازدید یک باره چند خبرگزاری معتبر کشور طبق آمار جهانی الکسا[٤٤] در خرداد ۹٤ به این شرح است:



تصویر شماره ٦، نرخ بازدید یکباره خبرگزاری ایرنا

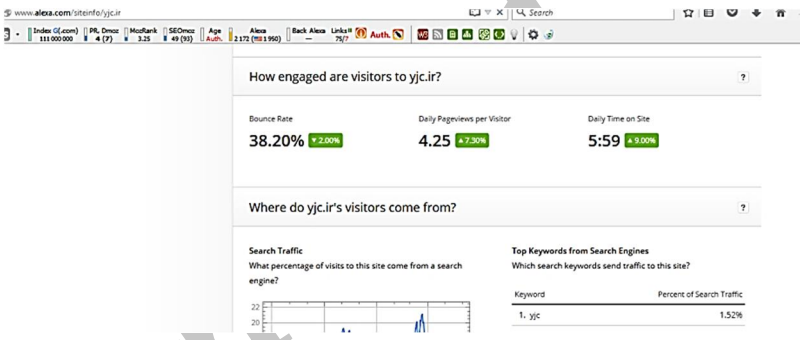
طبق تصویر شماره ۷، نرخ بازدید یک‌باره سایت خبرگزاری جمهوری اسلامی ایران (ایرنا)، ٤١/٤٠ درصد است. این یعنی از هر ۱۰۰ نفر بازدیدکننده سایت ایرنا، ٤١ نفر فقط یک‌بار به سایت رجوع می‌کنند.

نمونه دیگر وب‌سایت خبرگزاری فارس به‌عنوان پربازدیدترین خبرگزاری رسمی فارسی زبان است.



تصویر شماره ۷، نرخ بازدید یکباره خبرگزاری فارس

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



تصویر شماره ۸، نرخ بازدید یکباره خبرگزاری باشگاه خبرنگاران

طبق تصویر بالا، از هر ۱۰۰ نفر بازدیدکننده خبرگزاری باشگاه خبرنگاران صدا و سیما، حدود ۳۸ نفر بازدیدکننده یک‌باره محسوب می‌شوند.

۷-۳. 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 به‌عنوان یک شخص حقوقی مورد خدشه قرار دهند.

به‌عنوان مثال، تاکنون 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[٤٥] 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، لطفاً تلاش خود را چند دقیقه بعد تکرار کنید»، مواجه می‌شود. حال فرض کنید این سایت، یک پایگاه فروش اینترنتی باشد. اگر مشتریان چندبار 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 بیاندازند، در واقع نوعی حمله سازمان‌یافته به سایت انجام دادند که به آن حمله داس[٤٦] 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[٤٧] مورد چنین حمله‌هایی قرار گرفتند. همچنین از سایت‌های خبری پربازدید داخلی، سایت خبرگزاری فارس مورد چنین حمله‌ای قرار گرفته است.

یادداشت‌ها

1. Cyber space
2 http://hvm.ir/print.asp?id=38373 بانک جامع قوانین و مقررات کشور/ معاونت حقوقی و امور مجلس
3 Internet Protocol
٤. فتا مخفف فضای تبادل اطلاعات است.
5. Agent

6. Annonymity
7. Proxy
8. VPN
9. Information Security
10. Stuxnet
11. log
12. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
13. track
14. cookies
15. history
16. https://www.statista.com/chart/1447/strategies-people-use-to-be-less-visible-online
17. Authentication
18. transaction
19. Dann Parker
20. Susan Brenner
21. propagation range
22. World Wide Web
23. end to end
24. Sneefer

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

26. Internet Penetration Rate

۲۷. وزارت بازرگانی ایالات متحده آمریکا کاربر اینترنت را کسی می‌داند که دست‌کم سه سال سن دارد و در حال حاضر از اینترنت استفاده می‌کند.

28. Facebook
29. Twitter
30. Instagram
31. distributed
32. QQ
33. Viber
34. Real-time
35. Online
36. Rich Site Summary-Reader
37. Crawl
38. New Orlean
39. http://www.rajanews.com/news/128645
40. Katrina
41. Comment
42. http://www.nic.ir/Statistics
43. Bounce rate
44. www.alexa.com
45. request
46. Denial of service
47. Ebay

کتابنامه

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

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

جعفریی لنگرودی، محمد جعفر (۱۳۶۳)، ترمینولوژی حقوق، تهران: نشر گنج.

جلالی فراهانی، امیرحسین (۱۳۸۴)، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، مجله فقه و حقوق، شماره ۶ (پاییز): صص ۱۳۳-۱۶۲.

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

شاملو احمدی، محمدحسین (۱۳۸۰)، فرهنگ اصطلاحات و عناوین جزایی، تهران: نشر دادیار.

شیرزاد، کامران (۱۳۸۸)، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، تهران: نشر بهینه فراگیر.

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

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

Brenner, Susan W (2001), "Is There Such a Thing as virtual Crime", California Criminal Law Review.

Kabay, Me (1998), Anonymity and Pseudonymity in Cyberspace: Deindividuation incivility and lawlessness versus freedom and privacy.

Ferguson, Paul (1998), "What Is a VPN? - Part I", The Internet Protocol Journal - Volume 1, No. 1.

www.itu.int

www.Internetworldstats.com

www.Alexa.com

http://hvm.ir/print.asp?id=38373

https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

https://www.statista.com/chart/1447/strategies-people-use-to-be-less-visible-online

http://www.rajanews.com/news/128645

http://www.nic.ir/Statistics