جامعهٔ اطلاعاتی و جرائم نوظهور:
تلاشی جامعه‌شناختی در تبیین قربانیان تعرض سایبری در شهر تهران[1]

محمد توکل[2]، محمدعلی فاطمی‌نیا[3]

تاریخ دریافت: ۱۳۹۸/۸/۱۸ تاریخ پذیرش: ۱۳۹۸/۱۲/۱٤

بررسی مسائل اجتماعی ایران، دوره دهم، شماره اول، بهار و تابستان ۱۳۹۸، ص ۳۷-۶۲

چکیده

توسعهٔ جامعهٔ اطلاعاتی با خود تحولات فراوانی را به‌دنبال داشته است که ازجمله می‌توان به گسترش فضای سایبری و شکل‌گیری انواع جدیدی از انحرافات و جرائم سایبری اشاره نمود. یکی از این جرائم، که دامنهٔ وسیعی دارد، تعرض سایبری است. سازمان‌ها و نهادهای رسمی درخصوص این نوع جرم داده‌های دقیقی ارائه نمی‌کنند. همچنین به دلیل نظام ارزشی حاکم بر کشور، بسیاری از این نوع جرائم به نهادهای مربوطه گزارش نمی‌شوند. بنابراین، برای غلبه بر این محدودیت، رویکرد نظری بزهدیده‌شناسی براساس نظریهٔ فعالیت روزمرهٔ فلسون مبنای تحقیق قرار گرفته است که برآوردی دقیق‌تر از این جرم ارائه دهد. این جرم به دلیل ماهیت تعاملی آن در میان افرادی که از دو جنس متفاوت هستند رخ می‌دهد. انواع تعرض سایبری که موضوع این پژوهش بوده است تهدید، سرقت اطلاعات و هویت، نشر اکاذیب و مزاحمت می‌باشد. روش تحقیق این پژوهش پیمایش بزهدیده‌شناسی است که باهدف کشف نرخ وقوع این جرم و تحلیل علل آن می‌باشد و در میان شهروندان بالای ۱۵ سال شهر تهران، که در هفته حداقل یک ساعت کاربر اینترنت هستند، انجام شده است. یافته‌های این پژوهش نشان می‌دهد که در حدود ۸,۹ درصد کاربران تهرانی حداقل یک بار مورد تعرض قرار گرفته‌اند. بنابراین، می‌توان گفت تعرض سایبری مسئله‌ای اجتماعی است که در فضای مجازی در حال رخ دادن است. تحلیل یافته‌ها بیانگر آن است که سبک زندگی آنلاین قربانیان بر میزان و کیفیت رخداد تعرض سایبری اثرگذاری معناداری دارد. ازجمله عوامل اثرگذار بر قربانی شدن تعرض سایبری تغییر ارزش‌ها در فضای سایبری و کاهش کنترل اجتماعی است که کناره‌گیری اخلاقی و کاهش خودکنترلی افراد را به‌دنبال دارد. این فرایند درنهایت، موجب افزایش رؤیت‌پذیری و رفتارهای ریسک‌پذیرانهٔ افراد می‌شود که شرایط قربانی شدن آنها را فراهم می‌کند.

واژگان کلیدی: جرائم سایبری، تعرض سایبری، تغییر ارزش‌ها، کنترل اجتماعی، رؤیت‌پذیری و ریسک‌پذیری

---

۱ این مقاله برگرفته از رساله دکتری آقای محمدعلی فاطمی نیا با راهنمایی دکتر محمد توکل است.

۲ استاد گروه جامعه‌شناسی دانشکده علوم اجتماعی دانشگاه تهران؛ پست الکترونیکی: mtavakol@ut.ac.ir

۳ دکتری جامعه شناسی دانشگاه تهران و مدرس دانشگاه (نویسندهٔ مسئول)؛ پست الکترونیکی: Fateminia.s@ut.ac.ir

مقدمه و بیان مسئله

اگر به اطراف خود دقت کنیم، به‌خوبی پی خواهیم برد که جهان بسیار متفاوت‌تر از آن چیزی است که در چند دههٔ گذشته از آن سراغ داریم. انجام فعالیت‌های اداری، بانکداری، آموزش، پژوهش و حتی شیوهٔ تعاملات بین انسان‌ها بسیار دگرگون شده است. رسانه‌های نوین ارتباطی و اطلاعاتی شکل جدیدی از جامعه را به‌وجود آورده است که تا پیش‌ازاین سابقه‌ای از آن وجود نداشته است. سرعت، دقت، فرازمانی و فرامکانی بودن این ارتباطات بر شکل‌گیری و وجود جامعهٔ اطلاعاتی صحه می‌گذارد. حتی عده‌ای به چارچوب زمانی امروز محدود نمی‌شوند و جامعهٔ اطلاعاتی را زمینه‌ساز عصر مجازی آینده می‌دانند. فارغ از آینده‌نگری، آن عصری که به‌صورت قاطع، در آن حضور داریم عصر اطلاعات است.

امروزه بخش اعظم عصر اطلاعات بر فضای سایبر استوار است. فضای سایبر[1] به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و ابزارهای مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. این فضا، علاوه‌بر کارکردهای مثبتی که دارد، شرایطی را برای ارتکاب جرم فراهم کرده است و چون چنین جرمی در فضای اینترنتی روی می‌دهد آن را جرم دیجیتال یا جرم سایبری[2] نام می‌نهند. به‌عبارت‌دیگر، همراه با توسعهٔ فناوری‌های نوین فرصت‌هایی برای ارتکاب جرم ایجاد شده که به‌نظر می‌رسد منبع پایان‌ناپذیری را برای جرائم فراهم کرده است (نیومن و کلارک، ۲۰۰۳؛ گرابوسکای، ۲۰۰۷؛ وال، ۲۰۰۸ ؛ رینز، ۲۰۱۰).

داده‌های جهانی درخصوص جرائم سایبری نشان می‌دهد که سالانه حدود ۵۵۶ میلیون نفر و در هر ثانیه ۱۸ نفر بزهدیده اینگونه جرائم می‌شوند. همچنین یک نفر از هر ۱۰ نفر استفاده‌کننده از شبکه‌های اجتماعی در وضعیت بزهدیده قرار می‌گیرند. در یک مطالعهٔ بین‌المللی، یافته‌ها نشان داده است که در سال ۲۰۱۳، سازمان‌هایی که در نمونه آماری تحقیق بوده‌اند سالانه ۱۱٫۶ میلیون دلار هزینه محافظت در برابر جرائم سایبری می‌کنند که این رقم در یک سال قبل از آن، در حدود ۸٫۹ میلیون دلار بوده است. درمجموع، سالانه نزدیک به ۴۰۰ میلیارد دلار خسارتی است که از جرائم سایبری به‌جا می‌ماند (مؤسسهٔ پانمان، [3]۲۰۱۴: ۱). این یافته‌ها در کنار رشد صعودی کاربران اینترنتی واقعیتی را به تصویر می‌کشد که لاجرم باید منتظر افزایش روزافزون جرائم اینترنتی بود. تعداد کاربران اینترنت در جهان در سال ۱۹۹۳، از حدود ۱۴ میلیون نفر به حدود ۳ میلیارد نفر در سال ۲۰۱۵، رسیده است (سایت آمار جهانی اینترنت[4]:

1 Cyberspace
2 Cybercrime
3 Ponemon Institute
4 WORLD INTERNET USAGE AND POPULATION STATISTICS (www.internetworldstats.com)

۲۰۱۵). در ایران نیز جرائم رایانه‌ای کشور رشد ۱۰۰ درصدی را تجربه کرده است (هادیانفر، ۱۳۹۴: سایت رسمی پلیس فتا).

طبقه‌بندی مختلفی از جرائم سایبری ارائه شده است. معروف‌ترین طبقه‌بندی جرائم سایبری را به چهار دسته جرائم علیه اموال، جرائم علیه سازمان‌ها، جرائم علیه جامعه و جرائم علیه اشخاص دسته‌بندی می‌کند (پونیا، ۲۰۱۴: ۱۲۰). در پژوهش حاضر، در بین چهار دستهٔ فوق، جرائم علیه اشخاص بررسی می‌شود که خود انواع مختلفی دارد. هدف این نوع جرم اثرگذاری بر فرد است. این جرم‌ها شامل هرزه‌نگاری، تعرض سایبری، تهمت و افترا سایبری، اخاذی اینترنتی، قاچاق موادّمخدر، تقلب در کارت اعتباری، جرائم مرتبط با چت روم‌ها، سرقت ادبی، و هر جرمی که آسیب آن به افراد به‌مراتب می‌تواند سخت‌تر و بیشتر باشد. در این میان، تعرض سایبری[1] ازجمله جرائم سایبری در حال گسترش است.

تعرض سایبری شامل استفاده از شبکهٔ اینترنت یا دیگر ابزار دیجیتال برای آزار و اذیت دیگران است (پتروسیلی، ۲۰۰۵؛ سومایا و همکاران، ۲۰۱۴: ۴). به‌طورکلی، تعرض به رفتارهای مزاحم و تکرار شونده‌ای اشاره دارد که پیامدهایی چون احساس ترس، آسیب فیزیکی، روانی و استرس‌های عاطفی را در پی دارد (فینچ، ۲۰۰۱). این جرم برخلاف بسیاری از جرائم سایبری، که علیه اموال انجام می‌شود، علیه افراد است (روبرتز، ۲۰۰۸: ۲۷۱). بوسیج[2](۲۰۰۲) در یک تعریف موسع «گروهی از رفتارها که در آن یک فرد، گروهی از افراد و/یا سازمان‌ها از فنّاوری اطلاعات و ارتباطات برای ایجاد مزاحمت برای دیگر افراد، گروه‌ها و/یا سازمان‌ها استفاده می‌کنند. این رفتارها شامل تهدید و هشدارهای کاذب، تخریب تجهیزات و داده‌ها، سرقت هویت، سرقت اطلاعات، پایش رایانه‌ای، درخواست‌های جنسی از افراد کم سن‌وسال و هر نوع خشونت دیگر است که با ابزار دیجیتال ،به‌ویژه شبکه اینترنت، انجام می‌شود».

این نوع از جرم به دلایل مختلف گرایش به مخفی شدن دارد. به‌ویژه در کشوری مانند ایران که از هنجارهای قوی دینی و عرفی برخوردار است؛ افراد از گزارش آن به مراکز پلیس و/یا قوه قضائیه جلوگیری می‌کنند. به همین دلیل، تخمین دامنهٔ شیوع این نوع جرم مشکل و نیازمند شیوه‌های مختلف گردآوری اطلاعات دربارهٔ آن و همچنین انجام پیمایش‌های بزهدیده‌شناسی است. این جرم از این حیث مهم است که در وهلهٔ اول، علیه افراد است. دوم، نیازمند طی یک فرایند اجتماعی است. سوم، بزهدیده در وقوع آن نقش ایفا می‌کند. چهارم، از سبک زندگی نوین افراد تأثیرپذیر است. پنجم، فضا در وقوع آن نقش فعالی دارد و نهایتاً اینکه پیامدهای وسیع اجتماعی دارد که می‌تواند اخلاق و عفت عمومی را از خود متأثر سازد.

---

1 Cyber stalking
2 Bocjj

بنابراین سؤال اصلی این تحقیق این است که دامنهٔ تعرض سایبری در شهر تهران چقدر است؟ و چه عواملی بر قربانی شدن در جرم تعرض سایبری اثرگذار است؟ این پژوهش در نظر دارد با انجام یک پیمایش قربانی شناختی به این سؤالات پاسخ دهد.

پیشینهٔ تجربی

موضوع تعرض سایبری در ایران کمتر موردتوجه بوده است به‌ویژه می‌توان گفت که یک تحقیق میدانی در این خصوص انجام نشده است. آثار معدودی هم که وجود دارد اغلب نظری و توصیه‌ای هستند. در خارج از کشور، تحقیقات نظری و کاربردی بسیاری دربارهٔ جرائم سایبری و ازجمله تعرض سایبری انجام شده است.

الیسون[1](۱۹۹۹) تعرض سایبری را در ارتباط با موضوعات سیاسی اجتماعی چون احترام به حریم خصوصی و آزادی بیان دانسته است. او معتقد است که تعرض سایبری موجب نادیده گرفته شدن حریم خصوصی و آزادی بیان می‌گردد این قضیه درخصوص زنان به‌مراتب اثرگذارتر است (الیسون و اکدنیز، ۱۹۹۸).

در تحقیقی نظری که در استرالیا و در سال ۲۰۰۰، به انجام رسیده است اوگلیو[2] ضمن مقایسهٔ تعرض سایبری با تعرض سنتی به گونه‌شناسی تعرض سایبری در سه وجه تعرض ایمیلی، کامپیوتری و اینترنتی می‌پردازد. او راهکار پیشگیری و مقابله با تعرض سایبری را در مراقبت‌های فردی، ترتیبات تکنیکی و ابزار قانون‌گذاری می‌داند (اوگلیو، ۲۰۰۰).

در پیمایشی که در کشور انگلستان انجام شده است حدود ۳۵۳ نفر به‌عنوان نمونه انتخاب شده‌اند که ۱۰۹ نفر آنها مرد و مابقی زن هستند. نتایج این پیمایش نشان داده است که بیشترین دامنهٔ سنی که در معرض تعرض سایبری بوده‌اند افراد ۲۰ تا ۳۹ سال هستند و در حدود ۸۰ درصد مردم از اینکه بزهدیده چنین جرمی شوند ترس دارند. ترس ۱۳ درصد افراد جریحه‌دار شدن احساسات، ۲۴ درصد صدمات فیزیکی و ۳۴ درصد نیز ترس از دست دادن آبرو بوده است. ۵۸ درصد افراد ۳ بار و/یا بیشتر تعرض سایبری را تجربه کرده‌اند. از بین زنان در حدود ۷۶ درصد بزهدیدگان دارای سابقهٔ آشنایی با بزهکار بوده‌اند (ماپل و همکاران، ۲۰۱۱). در کشور آمریکا نیز پیمایش ملی بزهدیدگان جرائم گزارش می‌دهد که در حدود ۴۶ درصد افراد تجربهٔ بزهدیده شدن به شکل سنتی آن را داشته‌اند که در حدود ۲۵ درصد آنها تعرض سایبری را نیز گزارش کرده‌اند که تقریباً ۸۰ درصد آن از طریق ایمیل رخ داده است (باوم و همکاران، ۲۰۰۹).

پژوهشی با عنوان «جوانان و تعرض سایبری در کشور آمریکا» در بین دانش‌آموزان کارولینای شمالی، دو نظریهٔ مهم خودکنترلی و نظریهٔ یادگیری اجتماعی به‌عنوان متغیرهای پیش‌بین به‌کار گرفته شده‌اند.

---

1 Louise Ellison
2 Emma Ogilvie

نمونهٔ تحقیق ۱۶۶۹ نفر بودند. نتایج نشان داد که سطح خودکنترلی پایین و یادگیری از همالان، موجب افزایش سطح جرم تعرض سایبری می‌شود (مارکوم و همکاران، ۲۰۱۴).

جدول شمارهٔ ۱: خلاصهٔ تحقیقات مربوط به موضوع تعرض سایبری

ردیف	نویسنده	سال	عنوان اثر	نوع اثر	زمینه تحقیق
۱	الیسون و اکدنیز	۱۹۹۸	تعرض سایبری: قوانین مرتبط با مزاحمت در اینترنت	نظری	حقوقی
۲	الیسون	۱۹۹۹	تعرض سایبری: مبارزه با مزاحمت در اینترنت	نظری	حقوقی
۳	اوگلیو	۲۰۰۰	تعرض سایبری: روندها و موضوعات	نظری	حقوقی
۴	برگس و همکاران	۲۰۰۵	درک از تعرض سایبری در میان دانش‌آموزان	کاربردی	علوم اجتماعی
۵	بوسیج	۲۰۰۴	تعرض سایبری: مزاحمت در عصر اینترنت و چگونگی محافظت از خانواده	نظری	علوم اجتماعی
۶	شریدان و گرنت	۲۰۰۷	آیا تعرض سایبری متفاوت است؟	کاربردی	علوم اجتماعی
۷	پاولت و همکاران	۲۰۰۹	تعرض سایبری: یک مطالعهٔ اکتشافی در بین دانشجویان دانشگاه آتلانتیک	نظری	علوم اجتماعی
۸	اسپتزبرگ و هولبر	۲۰۰۲	تعرض سایبری و فناوری تروریسم بین شخصی	نظری	علوم اجتماعی
۹	میشرا و میشرا	۲۰۰۸	تعرض سایبری: چالشی برای امنیت وب	نظری	علوم اجتماعی
۱۰	گودنو	۲۰۰۷	تعرض سایبری یک جرم جدید: ارزیابی کارایی قوانین فدرال و ایالتی	نظری	حقوقی
۱۱	فاین	۲۰۰۴	پیمایش مزاحمت آنلاین در دانشگاه	کاربردی	علوم اجتماعی
۱۲	مپل و همکاران	۲۰۱۱	پیامدهای تعرض سایبری	نظری	علوم اجتماعی
۱۳	استفانسن و والتر	۲۰۱۱	به‌سوی برآمد جرائم سایبری: تعرض سایبری	نظری	حقوقی
۱۴	جایشنکار و سنکاری	۲۰۰۶	تعرض سایبری: تهدیدی جهانی در بزرگ‌راههای اطلاعاتی	کاربردی	علوم اجتماعی
۱۵	باوم و همکاران	۲۰۰۹	بزهدیدگان تعرض در ایالات متحده آمریکا	کاربردی	علوم اجتماعی
۱۶	پیتارو	۲۰۰۷	تعرض سایبری: تحلیل ارعاب و مزاحمت آنلاین	نظری	علوم اجتماعی
۱۷	مکفارلن و بوسیج	۲۰۰۳	تبیین و پیش‌بینی رفتار در فضای سایبری: به‌سوی گونه‌شناسی متعرضان سایبری	کاربردی	علوم اجتماعی

ادامه جدول شمارهٔ ۱: خلاصهٔ تحقیقات مربوط به موضوع تعرض سایبری

ردیف	نویسنده	سال	عنوان اثر	نوع اثر	زمینه تحقیق
۱۸	بوسج	۲۰۰۳	تعرض سایبری: مطالعه‌ای اکتشافی	کاربردی	علوم اجتماعی
۱۹	رینز و همکاران	۲۰۱۱	مورد تعقیب بودن آنلاین: به‌کارگیری نظریه فعالیت روزمره در بزهدیده شدن سایبری	کاربردی	علوم اجتماعی
۲۰	بوسیچ و همکاران	۲۰۰۲	تعرض سایبری: چالشی جدید برای وکلا و قانون‌گذاران	نظری	حقوقی
۲۱	لیندنبرگ	۲۰۱۲	تعرض سایبری: مرور ادبیات	نظری	علوم اجتماعی
۲۲	هازلوود و ماگین	۲۰۱۳	تعرض سایبری و قوانین مربوطه در آمریکا	نظری	حقوقی
۲۳	مارکوم و همکاران	۲۰۱۴	جوانان و تعرض سایبری در آمریکا	کاربردی	علوم اجتماعی
۲۴	بک	۲۰۱۶	برآورد تجربی بزهدیدگان مزاحمت سایبری به‌وسیله نظریهٔ فعالیت روزمره	کاربردی	علوم اجتماعی

درجمع‌بندی پیشینهٔ تحقیق می‌توان گفت درحالی‌که در تحقیقات خارجی، موضوع جرائم و تعرض سایبری نزدیک به چند دهه، در کانون توجه اندیشمندان و صاحب‌نظران قرار گرفته است، اما این قبیل موضوعات در ایران عمر کوتاهی دارد و اغلب مقالات و پژوهش‌های تولیدشده کلی و در سطح مباحث نظری و گردآوری آثار پیشین بوده است. در اغلب آثار داخلی و خارجی که دربارهٔ تعرض سایبری بوده است تمرکز بر چند محور: ۱. بزهدیده و صدمات او، ۲. بزهکار و انگیزه‌های او، ۳. جرم و دیدگاه‌های حقوقی نسبت به آن و ۴. راهکارهای پیشگیرانه و مبارزه با آن بوده است. این تحقیق در نظر دارد با تمرکز بر موضوع تعرض سایبری این شکل از جرم را با تأکید بر فرد بزهدیده موردمطالعهٔ میدانی قرار دهد. از حیث روش‌شناختی در زمرهٔ پیمایش‌های بزهدیده‌شناسی قرار می‌گیرد. نوآوری این تحقیق ازاین‌جهت است که هم ازنظر موضوعی و هم ازنظر داده‌هایی که در فرایند پیمایش تولید می‌شود سابقه‌ای برای این تحقیق وجود ندارد.

مبانی و چارچوب نظری

تعرض سایبری[1] شامل استفاده از شبکهٔ اینترنت یا دیگر ابزار دیجیتال برای آزار و اذیت دیگران است (پتروسیلی، ۲۰۰۵؛ سومایا و همکاران، ۲۰۱۴: ۴). به‌طورکلی، تعرض به رفتارهای مزاحم و تکرار شونده‌ای

1 Cyber stalking

اشاره دارد که پیامدهایی چون احساس ترس، آسیب فیزیکی، روانی و استرس‌های عاطفی را در پی دارد (فینچ، ۲۰۰۱). این جرم برخلاف بسیاری از جرائم سایبری که علیه اموال انجام می‌شود علیه افراد است (روبرتز، ۲۰۰۸: ۲۷۱). البته در یک تعریف موسع بوسیج[1](۲۰۰۲) «گروهی از رفتارها که در آن یک فرد، جمعی از افراد و یا سازمان‌ها از فنّاوری اطلاعات و ارتباطات برای ایجاد مزاحمت برای دیگر افراد، گروه‌ها و یا سازمان‌ها استفاده می‌کنند. این رفتارها شامل تهدید و هشدارهای کاذب، تخریب تجهیزات و داده‌ها، سرقت هویت، سرقت اطلاعات، پایش رایانه‌ای، درخواست‌های جنسی از افراد کم سن‌وسال و هر نوع خشونت دیگر است که با ابزار دیجیتال و به‌ویژه شبکه اینترنت انجام می‌شود».

به‌طورکلی، متعرضان سایبری از شیوه‌های مختلف و متعددی برای آزار بزهدیدهٔ خود استفاده می‌کنند که شامل چهار نوع رفتار است که عبارت‌اند از: تهدید، سرقت اطلاعات و هویت، نشر اکاذیب و افترا و درنهایت آزار و مزاحمت. مبتنی بر آنچه پیش‌ازاین گفته شد، تعرض سایبری دارای ویژگی‌هایی است که آن را از دیگر جرائم متمایز می‌سازد:

۱. تعرض سایبری یک فرایند اجتماعی وقوع دارد که ممکن است از چند روز تا چند ماه به طول بیانجامد.
۲. بزهکار در ارتکاب جرم خود انگیزهٔ زیادی دارد و حاضر است وقت و فرصت زیادی را برای رسیدن به هدف صرف کند.
۳. نوعی حسابگری و هدفمندی در رفتار بزهکار و انتخاب بزهدیده وجود دارد.
۴. انگیزه و هدف بزهکار تنوع‌پذیر است؛ یعنی ممکن است انگیزهٔ مادی، جنسی، انتقام، هتک حرمت و... وجود داشته باشد.
۵. اقدامات بزهکار تکرارپذیر است؛ یعنی ممکن است یک بزهدیده را برای مدت طولانی طعمه خود سازد.
۶. رابطهٔ بزهکار و بزهدیده مبتنی بر تعامل متقابل کوتاه‌مدت و/یا بلندمدت است.
۷. بزهدیده در وقوع جرم نقش ایفا می‌کند.
۸. ترس و ناراحتی بزهدیده؛ به این معنا که بزهدیده در فرایندی حضور دارد که دائماً در آن مورد تهدید، تحقیر و آزار قرار می‌گیرد.

این ویژگی‌ها، به‌طور ضمنی، بر این نکته صحه می‌گذارد که تعرض سایبری موضوعی است که بیش از جرائم دیگر به تحلیل‌های جامعه‌شناسانه و جرم‌شناسانه تن می‌دهد. برای مثال، کسی که مرتکب جرم

1 Bocij

فیشینگ می‌شود، انگیزهٔ اصلی او مادی و کسب مال دیگران است و اصلاً توجهی ندارد که بزهدیده او چه کسی خواهد بود. علاوه‌براین، این جرم به‌صورت آنی رخ می‌دهد و نیازمند تعامل با بزهدیده نمی‌باشد.

هیدلانگ و همکاران (۱۹۷۸) نظریهٔ مواجه‌ای سبک زندگی را برای تبیین جرائم ارائه کرده‌اند. این تبیین بیشتر ناظر به رفتار بزهدیده است، اگرچه برخی معتقدند که امروزه می‌توان از آن در تبیین رفتار بزهکار استفاده کرد. این نظریه در بسیاری از تحقیقاتی که درباره جرائم سایبری بوده به‌کار گرفته شده است. این نظریه بر سبک زندگی به‌عنوان عاملی مؤثر بر وقوع جرم تأکید دارد. درواقع، از دیدگاه این نظریه وقوع جرم تابع همگرایی و شباهت سبک و شیوهٔ زندگی بزهکار و بزهدیده است. سبک زندگی امکان دسترسی بزهکار به بزهدیده را فراهم می‌کند و مادامی‌که ارتباطی بین این دو وجود نداشته باشد، تصور وقع جرم امری بعید و دور از ذهن است. تعرض سایبری از این حیث که ماهیتی تعاملی دارد با این نظریه بیشتر تبیین‌پذیر خواهد بود. تحولات فناوری شرایط جدیدی در زندگی فراهم کرده است که اغلب افراد دارای زندگی دومی شده‌اند که همان فضای سایبری است. در همین رابطه، تحقیقات نشان داده است که هرچه افراد حضور بیشتر و ناآگاهانه‌ای در اینترنت پیدا می‌کنند، احتمال بیشتری وجود دارد که در دام از پیش پهن‌شدهٔ بزهکاران قرار گیرند (جشنیکار، ۲۰۱۱: ۲۳۴). این نظریه بر عواملی چون سن، جنسیت، آموزش و سطح مهارت تأکید و آن را به‌عنوان عناصر تعیین‌کنندهٔ سبک زندگی، که در وقوع جرم مؤثر هستند، معرفی می‌کند. بنابراین، فرضیهٔ زیر که «هرچه میزان حضور افراد در فضای سایبری و شبکه‌های اجتماعی بیشتر می‌شود، احتمال مورد تعرض قرار گرفتن فزونی می‌گیرد» از آن قابل استخراج است.

درحالی‌که نظریهٔ سبک زندگی بر عناصر و عوامل فردی و جمعیت‌شناختی محوریت یافته است، فلسون و کوهن (۱۹۷۹) نظریه‌ای را پروراندند که بر عوامل اجتماعی تمرکز دارد. این نظریه بر سه رکن مفهومی، بزهکار با انگیزه، بزهدیدهٔ مناسب و فقدان نظارت و ایمنی محیطی استوار است. بزهکار با انگیزه کسی است که دارای شرایط اجتماعی نامناسب است و به‌اصطلاح جرم‌شناسی، ریسک‌فاکتورهای زیادی در زندگی او مشاهده می‌شود. برای مثال، فرد بزهکار پایگاه اجتماعی اقتصادی پایینی دارد، مهاجر است، خانواده او از هم گسیخته است و... (میث و میر، ۱۹۹۴: ۸۴). بزهدیدهٔ مناسب به فردی اشاره دارد که از ویژگی‌هایی برخوردار است که او را آماج بزهکار قرا می‌دهد. در فضای سایبری، بزهدیدهٔ مناسب شخصی است که از رؤیت‌پذیری بالایی برخوردار است، به این معنا که اطلاعات شخصی بیشتری از خود بروز می‌دهد. بنابراین «هر چه افراد رؤیت‌پذیری (اطلاعات بیشتری) از خود ارائه می‌دهد به همان میزان احتمال بیشتری وجود دارد که بزهدیدهٔ تعرض سایبری شوند».

فقدان محیط امن بر موضوع کنترل و نظارت متمرکز است که چه‌بسا بسیاری از جرائم به دلیل وجود آن می‌تواند رخ ندهد. در فضای سایبری، بعد نظارت امری ضروری است که به دلایل مختلف خارج از

کنترل سیاست‌گذاران قرار گرفته است. نظارت در فضای سایبری، بر دو گونه کنترل دیجیتال و کنترل اجتماعی است. بعد دیجیتال شامل نسب فایروال‌ها، آنتی‌ویروس و گذرواژه‌های پیچیده بر سیستم رایانه‌ای و پروفایل‌های شخصی است. بعد اجتماعی شامل میزان کنترل و نظارت مدیران فضای شبکه‌هاست مانند مشخص شدن آی‌پی و هویت کاربران و اعضای شبکهٔ اجتماعی (یار، ۲۰۰۵؛ هالت و بوسلر، ۲۰۰۹). بنابراین «هرچه افراد تصور نمایند که در فضای سایبری کنترل اجتماعی کمتری وجود دارد، احتمال بیشتری وجود دارد که بزهدیده تعرض سایبری شوند». درواقع، وجود نظارت از بین برندهٔ فرصت وقوع جرم است. به همین دلیل، نظریهٔ فرصت جرم اگرچه با نظریات فوق هم‌پوشانی دارد، اما از این لحاظ که مفهوم فرصت در کانون مباحث آن قرار دارد متفاوت است.

نظریهٔ عمومی جرم، که در آغاز از سوی گاتفردسون هر شی در تبیین رفتار بزهکار به‌کار گرفته می‌شد، امروزه در توضیح رفتار بزهدیده نیز کاربرد پیدا کرده است. این توسعه در تبیین، عامیّت مفهوم «عمومی» را در این نظریهٔ وسعت بخشید (هیرشی، ۲۰۰۴: ۵۴۱). از دیدگاه این نظریه، مهم‌ترین عامل وقوع جرم خودکنترلی است، یعنی توانایی خویشتن‌داری افراد در موقعیت‌های وسوسه‌انگیز. متعرضان سایبری موقعیت‌های فریب‌دهنده‌ای را فراهم می‌کنند که بزهدیده قدرت خویشتن‌داری خود را از دست می‌دهد و در دام او گرفتار می‌شود. بنابراین این فرضیه که «هرچه افراد خودکنترلی بیشتری داشته باشند، احتمال بزهدیده شدن آنها کاهش پیدا می‌کند» در این تحقیق مورد آزمون قرار خواهد گرفت.

در نگاه جامعه‌شناختی، هنجارها و ارزش‌ها محصول تعاملات اجتماعی است و ازسوی‌دیگر، در همین تعاملات بازآفرینی می‌شود. در فضای سایبری، که تعاملات اجتماعی از نقصی ذاتی برخوردار است، افراد از طریق میانجی با هم در ارتباط‌اند و حضور فیزیکی ندارند. در چنین شرایطی، هرگونه انحرافی قابل رخ دادن است زیراکه آنها ممکن است هویت‌های کاذبی برای خود برگزینند که هیچ ارتباطی با زندگی واقعی آنها ندارد. لذا آنها از زندگی خود به‌نوعی هنجار زدایی و ارزش‌زدایی می‌کنند. برای مثال، وقتی کسی در فضای سایبری برای خود هویت یک پزشک را جعل می‌کند و قصد فریب دیگران را دارد به‌هیچ‌وجه، با نظام اخلاقی و صنفی این حرفه آشنا نیست و به همین دلیل هیچ‌گونه فشار هنجاری و ارزشی را بر خود احساس نمی‌کند، لذا در عبور از مرزهای اخلاقی کمتر دچار چالش و تضاد شناختی می‌شود.

این موضوع اهمیت نظریهٔ کناره‌گیری اخلاقی را برجسته می‌سازد. که باندورا (۱۹۹۶) آن را نظریهٔ شناختی_اجتماعی معرفی می‌کند. نظریهٔ مذکور بر این اصل استوار است که افراد در طول زندگی خود، متناسب با پایگاه اجتماعی‌شان به اصول و ارزش‌هایی مجهز می‌شوند که راهنمای رفتار آنها در موقعیت‌های اجتماعی است. باندورا می‌گوید گاهی در زندگی موقعیت‌هایی پیش می‌آید که مجبور به نادیده گرفتن این اصول و ارزش‌ها می‌شوند. این موقعیت‌ها چیزی جز کاهش فشار محیطی نیست (ابوذری،

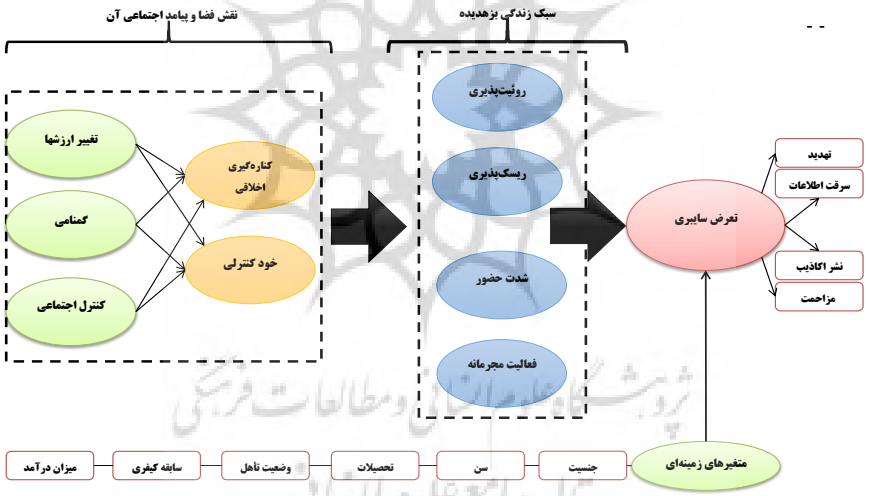
۱۳۹۱: ۷۶). فقدان نظارت‌های فنی و حقوقی و اجتماعی در فضای سایبر، ارتباط ناقص و همراه با میانجی، عدم مشاهده درد و رنج بزهدیده‌گان ازسوی بزهکار و هویت‌های سیال، چندگانه و مخدوش همه و همه از میزان فشار محیطی فضای سایبری کاسته است و به‌همین‌خاطر، زمینه‌های کناره‌گیری اخلاقی کاربران بیشتر فراهم است. لازم به ذکر است فشار محیطی همان چیزی است که از طریق فرایندهای کنترل درونی و اجتماعی بر افراد اعمال می‌شود. بنابراین «هرچه از فشار محیطی کاسته می‌شود، بر میزان کناره‌گیری اخلاقی افزوده می‌شود و درنهایت میزان تعرض سایبری فزونی می‌گیرد». البته تعرض سایبری می‌تواند به دو صورت فعل بزهکارانه و/یا بزهدیده شدن صورت پذیرد.

فرضیهٔ فوق یکی از ارکان و اصول پیشینی نظریهٔ انتقال موقعیت جشنیکار (۲۰۰۸) است. او در نظریهٔ خود، هشت پیش‌فرض به‌هم مرتبط ارائه می‌کند و در پیش‌فرض اول، خود مطرح می‌کند که افراد در فضای فیزیکی تحت‌تأثیر پایگاه اجتماعی‌شان تمایلات سرکوب‌شده‌ای به جرم دارند که ممکن است در فضای سایبری این تمایلات فعال شده و مرتکب جرم شوند. این پیش‌فرض به‌طور ضمنی، وجود برخی بزهکاران، که برای اولین‌بار مرتکب جرم می‌شوند، را تأیید می‌کند. علاوه‌براین، می‌توان گفت که «هرچه میزان کنترل اجتماعی کاهش پیدا می‌کند، ریسک‌پذیری افراد برای نادیده گرفتن قواعد هنجاری و ارزشی جامعه نیز افزایش پیدا می‌کند». همچنین او در پیش فرض دوم خود بر «گمنامی و فقدان عوامل بازدارنده» اشاره می‌کند که می‌توان آن را مرتبط با موضوع کنترل و نظارت اجتماعی در معنای عام آن دانست. علاوه‌براین، او در پیش فرض نهایی خود، وجود تضاد بین ارزش‌ها و هنجارهای جهان فیزیکی و سایبری را برجسته می‌سازد. به‌عبارت‌دیگر، «هرچه افراد در فضای سایبری تعامل و حضور بیشتری داشته باشند، زمینهٔ تغییر نگرش‌ها و ارزش‌های آن بیشتر فراهم می‌شود». مبتنی بر تمام مباحث نظری که در ادبیات و چارچوب نظری تحقیق مورد بحث قرار گرفت مدل نهایی تحقیق به‌صورت نمودار ارائه شده است.

همان‌طور که از مدل پیداست، متغیرهایی چون تغییر ارزش‌ها و کنترل اجتماعی ناظر به تصوراتی است که افراد از فضای سایبری دارند. یعنی فضایی که در آن کنترل اجتماعی پایین است و ارزش‌های آن نسبت به جهان فیزیکی متفاوت‌تر و کمتر سخت‌گیرانه است. چنین تصوراتی زمینه را برای افراد فراهم می‌کند که نسبت به ارزش‌ها و هنجارهای مستقر در جامعه احساس آزادی و رهایی بیشتری داشته باشند. به همین دلیل، افراد در این فضا تمایلات، آرزوها و خواسته‌های خود را بیشتر بروز می‌دهند و رؤیت‌پذیری بیشتری از خود نشان می‌دهند. علاوه‌براین، احساس کناره‌گیری اخلاقی، ریسک‌پذیری افراد را در ندیده گرفتن ارزش‌های و هنجارهای اجتماعی افزایش می‌دهد. رؤیت‌پذیری، کناره‌گیری اخلاقی و ریسک‌پذیری

سه ویژگی مهمی است که در چارچوب نظری فعالیت روزمره، بیانگر ویژگی‌ای بزهدیدهٔ مناسب است. بزهدیده که با رفتارهای مخاطره‌آفرین خود بیشتر خود را در معرض تعرض قرار می‌دهد.

به‌طورکلی، افراد نسبت به آنچه در فضای واقعی با آن مواجه هستند، کمتر احساس محدودیت می‌کنند و در فعالیت‌های بزهکارانه‌ای درگیر می‌شوند که پیش‌ازاین نیز در زندگی‌شان سابقه نداشته است. شاید به همین دلیل در مطالعات میدانی، مشخص شد که بسیاری از افرادی که مورد تعرض قرار گرفته‌اند و/یا فعالیت متعرضانه داشته‌اند فاقد سابقهٔ کیفری بوده‌اند. درگیر شدن در فعالیت بزهکارانه همان چیزی است که در چارچوب نظریهٔ فعالیت روزمره از آن به‌عنوان بزهکار با انگیزه یاد شده است. درمجموع، تمامی متغیرها با اثرات مستقیم و غیرمستقیمی که با هم داشته‌اند در آفرینش تعرض سایبری نقش داشته‌اند و به شکلی که در نمودار آمده وقوع تعرض سایبری را می‌توان از طریق آنها پیش‌بینی نمود. متغیرهایی که در مدل به‌کار گرفته شده‌اند در طراحی پرسش‌نامه به‌کار گرفته شده و مورد سنجش قرار خواهند گرفت.



نمودار شمارهٔ ۱: مدل نهایی تحقیق

در جهت توضیح بیشتر مدل فوق تعاریف عملیاتی هرکدام از متغیرهای ارائه می‌شود. تعرض سایبری به رفتارهای تهدید، سرقت اطلاعات، نشر اکاذیب و آزار و مزاحمت گفته می‌شود که در فضای سایبری از سوی کسی بر کس دیگر اعمال می‌گردد. این متغیر به استفاده از طیف لیکرت سنجش قرار گرفته شده است.

سبک زندگی آنلاین، یعنی شیوهٔ حضور و بروز افراد در فضای سایبری، که براساس دو مؤلفهٔ شدت حضور و کیفیت حضور مورد بررسی قرار گرفته است، این متغیر نیز در قالب چارچوب نظری پوشش‌دهندهٔ ویژگی بزهدیده است.

شدت حضور یعنی میزان ساعات حضور فرد در اینترنت در طول شبانه‌روز که در سطح سنجش نسبی اندازه‌گیری شده است. متغیر کیفیت حضور نیز براساس دو بعد نوع حضور، میزان رؤیت‌پذیری و ریسک‌پذیری سنجیده شده است.

الف) **رؤیت‌پذیری:** یعنی تعداد عضویت فرد در گروه‌ها و همچنین میزان ارائهٔ عکس و فیلم شخصی در این فضا که در سطح سنجش نسبی اندازه‌گیری شده است.

ب) **ریسک‌پذیری**: یعنی میزان ارتباط‌گیری فرد با افراد غریبه در فضای سایبری و کشاندن رابطه به فضای واقعی.

خودکنترلی یعنی اینکه فرد تا چه حد در مقابل خواسته‌های دیگران توان مخالف و ابراز عقیده دارد و علاوه‌برآن، در شرایط مختلف بر تغییرات رفتاری خود کنترل دارد. این متغیر نیز در جهت ویژگی قربانی موردتوجه قرار گرفته است. کناره‌گیری اخلاقی حالتی رفتاری که فرد نسبت به قواعد اخلاقی بی‌تفاوت می‌شود و نسبت به محرک‌های محیطی منفعلانه رفتار می‌کند. این متغیر با طیف لیکرت و در جهت شناخت ویژگی‌های بزهدیده سنجیده شده است.

با توجه به اینکه تعرض سایبری یک جرم میان جنسیتی است، تغییر ارزش‌ها براساس این مؤلفه، به معنای از دست دادن حساسیت نسبت به ارتباط با جنس مخالف و نمایش عکس و فیلم شخصی تعریف شده است. نام دیگر تغییر ارزش‌ها همان ارزش‌های نوگرایانه است. این متغیر در چارچوب نظری تحقیق ناظر به نقش فضا در وقوع جرم است. گمنامی به این معناست که کاربران تا چه حد احساس می‌کنند که رفتارهای و عملکرد آنها در اینترنت قابل ردیابی و پیگیری است که براساس طیف لیکرت مورد سنجش قرار گرفته شده است. کنترل اجتماعی یعنی اینکه فرد در فضای سایبری، به چه میزان احساس می‌کند که مورد کنترل و نظارت دیگران است.

روش تحقیق

روش تحقیق در این پژوهش پیمایش بزهدیده‌شناسی شناختی است که به‌دنبال بررسی میزان وقوع تعرض سایبری در سطح جامعه و عوامل احتمالی مؤثر بر قربانی شدن در این نوع جرم است. در نیمهٔ دوم قرن بیستم، به‌ویژه در دهه‌ها ۱۹۶۰ و ۷۰، بزهدیده و شناخت آن در کانون توجه نظریه‌پردازان قرار گرفت. شکل‌گیری این کانون فکری ازیک‌سو، ناشی از ناکارآمدی نظریاتی است که تنها به بزهکاران تأکید دارند

و ازسوی‌دیگر، یک رویکرد ترکیبی در عرصهٔ علم، به‌ویژه جامعه‌شناسی و جرم‌شناسی، شکل گرفته بود که قصد داشت پدیدهٔ جرم را هم از منظر بزهکار و هم بزهدیده موردمطالعه قرار دهد. علاوه‌براین، داده‌های جرائم که اغلب توسط پلیس و دستگاه‌های نظارتی تهیه می‌شود بازنمایی واقع‌گرایانه‌ای از جامعه نداشت (بالا بودن ارقام سیاه)، لذا اندیشمندان تلاش کردند با طراحی پیمایش‌های بزهدیده محور، شناخت دقیق‌تر و معتبری را از کم و کیف جرائم در سطح محلی و کلان جامعه ارائه دهند (ویلکاکس، ۲۰۱۰ به نقل از فیشر و لاب ۲۰۱۰: ۹۸۲).

جامعهٔ آماری تحقیق شهروندان بالای ۱۵ سال شهر تهران هستند که حداقل در هفته ۱ ساعت را در اینترنت سپری می‌کنند. شیوهٔ نمونه‌گیری پیمایش براساس اصل بازنمایی و از نوع نمونه‌گیری احتمالی است؛ یعنی اینکه هر شهروند بالای پانزده سال تهرانی که کاربر اینترنت است، شانس برابری برای انتخاب شدن در نمونهٔ تحقیق دارد. بنابراین برای انتخاب نمونه از شیوهٔ ترکیبی خوشه‌ای چندمرحله‌ای و تصادفی ساده استفاده شد. به این ترتیب که تهران به پنج پهنهٔ جغرافیایی تقسیم شد، سپس در هر پهنه چند منطقه، چند ناحیه و درنهایت، چند بلوک انتخاب شد که پرسشگر با مراجعه به در منزل و با اولین شهروند مشمول جامعهٔ آماری داده‌ها را گردآوری نموده است. میزان حجم نمونه براساس فرمول کوکران، ۴۰۰ نفر بوده است. درمجموع، متغیرهای تحقیق از روایی بالایی برخوردار بوده و میانگین آلفای کرونباخ متغیرهای اصلی تحقیق در حدود ۸۶ درصد بوده است.

یافته‌ها

یافته‌های تحقیق نشان می‌دهد که درمجموع ۴۱۸ پرسش‌نامهٔ گردآوری شده، در حدود ۵۲,۹ درصد پاسخگویان مرد و در حدود ۴۷,۱ درصد نیز زن هستند. از این میان، ۵۴,۵ درصد متأهل، ۴۱,۳ درصد مجرد، و در حدود ۳,۴ درصد نیز مجرد براثر فوت یا طلاق می‌باشند. همچنین ۸۸,۵ درصد این افراد با افراد خانواده زندگی می‌کند و ۶,۱ درصد تنها و در حدود ۱,۵ درصد نیز با دوستان و/یا اقوام خود می‌باشند. وضعیت تحصیلی پاسخگویان نشان می‌دهد که در حدود ۱۶ درصد پاسخگویان زیر دیپلم، ۳۸,۴ درصد دیپلم و مابقی یعنی در حدود ۵۵,۶ درصد نیز دارای تحصیلات دانشگاهی می‌باشند. ازلحاظ وضعیت شغلی نیز در حدود ۴۵,۹ درصد دارای شغل آزاد، ۲۰,۱ درصد خانه‌دار، ۱۹,۹ درصد دانشجو و محصل، ۶,۱ درصد بازنشسته، ۳,۹ درصد شغل دولتی و در حدود ۴,۲ درصد نیز بیکار می‌باشند.

ازلحاظ تعلقات دینی نیز ۹۵,۱ درصد شیعه، ۱,۷ درصد سنی و مابقی از سایر ادیان هستند. وضعیت قومیتی پاسخگویان، ۷۷,۱ درصد فارس، ۱۴,۵ درصد، ترک، ۳,۲ درصد کرد و بقیه را از سایر اقوام گزارش می‌کند. حداقل سن پاسخگویان ۱۵ سال و حداکثر ۷۲ سال می‌باشد. علاوه‌براین، میانگین سنی در حدود

۳۵,۵۴ سال می‌باشد. همچنین حداقل درآمد ۸۰۰ هزار تومان، حداکثر ۷ میلیون تومان و میانگین درآمد در حدود ۱ میلیون و ۷۰۰ هزار تومان بوده است.

نرخ وقوع تعرض سایبری

تعرض سایبری از چهار بعد تهدید، سرقت اطلاعات، نشر اکاذیب و آزار و مزاحمت تشکیل شده است. این چهار بعد در قالب چهار سؤال اصلی و ۱۶ سؤال فرعی مورد بررسی قرار گرفته است.

جدول شمارهٔ ۲: توزیع ابعاد تعرض سایبری براساس درصد

ابعاد	خیر	۱ تا ۲بار	۳ تا ۵ بار	۶ تا ۷ بار	۸ تا ۹ بار	۱۰ بار و بیشتر
تهدید	۸۹,۲	۶,۵	۲,۴	۰	۱	۱
سرقت اطلاعات و هویت	۹۱,۱	۷,۹	۰,۵	۰	۰	۰,۵
نشر اکاذیب و افترا	۹۴,۲	۳,۸	۰,۵	۰	۰	۱,۴
آزار و مزاحمت	۸۹,۷	۷,۴	۱,۲	۰,۷	۰,۵	۰,۵
تعرض سایبری	۹۱,۰۵	۶,۴	۱,۱۵	۰,۱۷	۰,۳۷	۰,۸۵

همان‌طور که از جدول فوق پیداست، یافته‌های تعرض سایبری نشان می‌دهد که در حدود ۱۱,۹ درصد شهروندان حداقل یک بار مورد تهدید قرارگرفته‌اند. این میزان برای سرقت اطلاعات، نشر اکاذیب و مزاحمت سایبری به‌ترتیب برابر با ۹,۹، ۵,۲، و ۷,۶ درصد می‌باشد. لازم به ذکر است که اگرچه هرکدام از این ارقام بسیار کوچک می‌نماید اما چنانچه این درصد در جمعیت ۸ میلیون نفری شهر تهران ضرب شود، رقم بسیار بزرگی خواهد بود. برای مثال، نرخ تهدید سایبری که در حدود ۱۱ درصد شهروندان تهرانی برابر با ۸۰۰ هزار نفر خواهد بود. که اگر این افراد بخواهند در دادسرای جرائم رایانه‌ای پرونده تشکیل دهند، آن‌وقت میزان هزینه‌های واقعی این جرم خود را نشان خواهد داد. به‌طورکلی، نرخ وقوع تعرض سایبری با توجه به جمع هر چهار بعد به میزان ۸,۹۵ درصد می‌باشد. یعنی اینکه به این میزان حداقل یک بار مورد تعرض سایبری قرار گرفته‌اند.

ازمجموع بزهدیدگان تعرض سایبری تنها ۱۱,۴ درصد اظهار داشته‌اند که به مراجع ذی‌صلاح برای شکایت از بزهکار مراجعه نموده‌اند. از میان ۸۸,۶ درصد افراد باقی‌مانده درخصوص علت عدم شکایت خود دلایلی چون ۳۱,۹ درصد «خودم مقصر بودم»، ۲۷,۸ درصد «قانون در برخورد با این موارد سخت‌گیر نیست»، ۲۶,۴ درصد «عدم شناخت بزهکار» ۸,۳ درصد «ترسیدن از اتفاقات بدتر» و ۵,۶ درصد نیز «ترس از آبروریزی» را بیان کرده‌اند. این یافته‌ها نشان می‌دهد که در درجهٔ اول، تعرض سایبری حاصل تعامل

بین بزهکار و بزهدیده است و در درجهٔ دوم، تصور منفی به دستگاه قضا دارند و علاوه‌برآن، بخشی از بزهکاران از فنون گمنامی برای تعرض به دیگران استفاده می‌کنند. نرخ پایین ترس از آبروریزی نیز نشان می‌دهد که جامعه از شکل‌های سنتی خود خارج‌شده و توبیخ‌های اطرافیان یا وجود ندارد و/یا اینکه اثرگذاری خود را از دست داده است. به‌عبارت‌دیگر، افراد بیشتر به عملکردهای فردی خود توجه دارند و نه رفتارهای جمعی.

از میان کسانی که مورد تعرض تهدید قرار گرفته‌اند در حدود ۶۰ درصد زنان و ۴۰ درصد نیز مردان بوده‌اند. در حدود ۴۵,۵ درصد انگیزهٔ اصلی متعرض را برقراری یا ادامهٔ رابطه، ۴۰,۹ درصد آزار و اذیت، ۹,۱ درصد انتقام و ۴,۵ درصد اخاذی مالی ذکر نموده‌اند. ۵۰ درصد افراد بزهدیده رابطهٔ خود با بزهکار را دوست، ۴,۵ درصد همکلاسی و ۴۵,۵ درصد نیز غریبه گزارش کرده‌اند. ۷۳,۳ درصد متعرضان تهدیدگر مرد، ۱۳,۳ درصد زن و مابقی نیز نامعلوم بوده است. ۴۸,۹ درصد زنان از سوی مردان، ۱۳,۳ درصد مردان نیز از سوی زنان تهدید شده‌اند. صفر درصد از زنان و ۲۴,۴ درصد زنان افرادی از جنس خود را مورد تهدید قرار داده‌اند.

بزهدیده‌گانی که مورد تعرض سرقت اطلاعات قرار گرفته‌اند در حدود ۴۳ درصد زنان و ۴۷ درصد نیز مردان می‌باشند. انگیزهٔ اصلی بزهکاران را ۵۴,۱ درصد آزار و اذیت، ۲۱,۶ درصد برقراری رابطه، ۱۳,۵ درصد انتقام و ۱۰,۸ درصد نیز اخاذی گزارش کرده‌اند. در این نوع تعرض ۷۲,۲ درصد افراد بزهکار غریبه بوده‌اند. ۲۲,۵ درصد دوست و ۵,۶ درصد نیز همکلاسی می‌باشند. همچنین در حدود ۵۸,۸ درصد جنسیت بزهکار را مرد، ۵,۹ درصد زن و ۳۵,۳ درصد دارای جنسیت نامعلوم بوده‌اند. در حدود ۲۹,۴ درصد زنان از سوی مردان مورد سرقت اطلاعات قرار گرفته‌اند درحالی‌که عکس این مورد اصلاً گزارش نشده است؛ یعنی اینکه هیچ زنی اقدام به سرقت اطلاعات مردان ننموده است. ۵,۹ درصد زنان و ۲۹,۴ درصد مردان افراد همجنس خود را مورد تعرض سرقت اطلاعات و هویت قرار داده‌اند.

این آماره‌ها درخصوص متعرضان نشر اکاذیب به این صورت بوده است که ۳۳,۳ درصد افراد بزهدیده زنان و در حدود ۶۶ درصد نیز مردان بوده‌اند. انگیزهٔ اصلی افراد بزهکار در حدود ۷۲,۷ درصد آزار و اذیت، ۱۸,۲ درصد انتقام و ۹,۱ درصد نیز برقراری رابطه بوده است. در این نوع تعرض، در ۴۱,۷ درصد رابطهٔ بزهکار و بزهدیده از نوع دوستی، ۲۵ درصد همکلاسی، ۲۵ درصد غریبه و ۸,۳ درصد نیز همکار بوده‌اند. ۵۰ درصد بزهکاران مرد، ۲۵ درصد زن و ۲۵ درصد نیز نامعلوم می‌باشد. جنسیت بین بزهکار و بزهدیده نشان می‌دهد که ۸,۳ درصد موارد زنان از سوی مردان سرقت اطلاعات شده‌اند و به همین میزان نیز زنان مردان را مورد تعرض قرار داده‌اند. اما ۴۱,۷ درصد مردان و ۱۶,۷ درصد زنان نسبت به افراد همجنس خود اقدام به نشر اکاذیب کرده‌اند. این آماره‌ها بیانگر مردانه بودن تعرض نشر

اکاذیب است. درواقع، در نشر اکاذیب در درجهٔ اول، بزهدیدگان اغلب مرد هستند و در درجهٔ دوم، مردان اغلب مردان را مورد تعرض قرار داده‌اند.

در حدود ۶۱ درصد بزه‌دیدگان تعرض آزار و اذیت سایبری زنان و ۳۹ درصد نیز مردان بوده‌اند. اما درخصوص متعرضان مزاحمت، انگیزه اصلی بزهکاران با میزان ۵۷٫۱ درصد همان آزار و اذیت بوده، ۳۳٫۳ درصد نیز برقرار رابطه و تنها ۹٫۶ درصد انتقام و اخاذی می‌باشد. نوع رابطه در حدود ۶۰ درصد موارد دوستی، ۳۱٫۱ درصد غریبه و ۸٫۸ درصد نیز همکلاسی و همکار گزارش شده است. از لحاظ جنسیت، ۵۷٫۸ درصد بزهکاران مرد، ۲۲٫۲ درصد زن و در حدود ۲۰ درصد نیز گزارش نشده است. اما درخصوص تفاوت جنسیت بین بزهکار و بزهدیده باید گفت که ۳۳٫۳ درصد زنان از سوی مردان مورد آزار قرار گرفته‌اند و ۴٫۴ درصد مردان نیز از سوی زنان مورد آزار بوده‌اند. در این میان، ۲۴٫۴ درصد مردان و ۱۷٫۸ درصد زنان نیز افراد همجنس خود را مورد آزار قرار داده‌اند. براساس یافته‌های این بخش می‌توان چنین نتیجه گرفت:

۱. تعرض سایبری در شهر تهران نیز یک تعرض بینا جنسیتی است به این معنا که میان بزهکار و بزهدیده از حیث جنسیت تفاوت وجود دارد.
۲. برخلاف تحقیقات خارجی، که اغلب بزهدیدگان را (بالای۷۰ درصد) جمعیت زنان تشکیل می‌دهد شهروندان تهرانی دارای چنین اختلاف جنسیتی نمی‌باشند.
۳. غیر از تعرض تهدید ۵۶ درصد و سرقت هویت و اطلاعات که ۷۲ درصد بزهکاران را افراد غریبه تشکیل می‌دهند در بقیهٔ تعرض‌های افراد آشنا (دوست، همکار و همکلاسی) نقش پررنگی داشته‌اند.
۴. بیشترین نوع تعرض‌ها را تهدید و مزاحمت تشکیل می‌دهند و کمترین آنها را نشر اکاذیب.
۵. بنابراین می‌توان الگوی غالب تعرض سایبری را تعرض واکنشی دانست. زیراکه اولاً، بین بزهکار و بزهدیده رابطهٔ آشنایی وجود دارد و در ثانی، انگیزهٔ اصلی بزهکاران را ادامه و/یا برقراری رابطه تشکیل می‌دهد؛ یعنی نوعی تعرض که افراد در قبال کنش‌ها و واکنش‌هایی که در روابط خود داشته‌اند به آن اقدام کرده‌اند.

تحلیل رگرسیون

در تحلیل رگرسیون، با استفاده از ضرایب بتا سهم یا میزان اثرگذاری هر متغیر بر متغیر وابسته در مقایسه با سایر متغیرها مشخص می‌شود. در مدل رگرسیون چندگانه، ضریب رگرسیون برای یک متغیر به ما می‌گوید که با افزایش یک واحد در مقدار آن متغیر مستقل، چقدر متغیر وابسته تغییر می‌کند (وقتی‌که سایر متغیرهای مستقل ثابت باشند). یک ضریب مثبت به این معناست که با افزایش مقدار

متغیر مستقل، مقدار پیش‌بینی‌شده متغیر وابسته نیز افزایش می‌یابد. یک ضریب منفی به این معناست که با کاهش مقدار متغیر مستقل، مقدار پیش‌بینی متغیر وابسته افزایش می‌یابد. با توجه به موارد فوق، در پژوهش حاضر مشارکت نسبی متغیرهای مستقل در تبیین متغیر وابسته با استفاده از روش پیش‌رونده به شرح زیر موردبررسی قرار می‌گیرد.

در جدول زیر نتایج تحلیل رگرسیونی متغیرهای مستقل و تعرض سایبری تهدید گزارش شده است. همان‌طور که پیداست، ریسک‌پذیری با بیشتر میزان بتا، یعنی ۶۰۳/. دارای بالاترین ارتباط معنادار با تعرض تهدید بوده است. به‌این‌معنا که به‌ازای هر واحد افزایش در ریسک‌پذیری افراد به میزان بتا در بزهدیده شدن در تعرض تهدید افزایش خواهیم داشت.

جدول شمارهٔ ۳: نتایج تحلیل رگرسیونی متغیر وابسته بزهدیده شدن تعرض سایبری(تهدید)

ردیف	متغیرهای پیش‌بینی	ضرایب Beta	آزمون T	معناداری sig	ضریب تبیین R^2	آزمون F	معناداری sig
۱	**ریسک‌پذیری**	/۶۰۳	۸,۱۸۷	/۰۰۰	/۵۸۰	۴۸,۰۳۰	/۰۰۰
۲	**گمنامی**	-/۲۱۹	-۳,۳۳۵	/۰۰۰			
۳	**رؤیت‌پذیری**	-/۲۸۷	-۳,۳۱۰	/۰۰۱			
۴	**جنسیت**	/۲۲۴	۲,۵۳۱	/۰۱۲			
۵	**میزان درآمد**	-/۰۷۹	-۱,۴۰۷	/۱۶۲			

در این معادله، گمنامی و رؤیت‌پذیری افراد دارای رابطهٔ منفی و معناداری با تعرض تهدید بوده‌اند. به‌این‌معنا که به‌ازای هر واحد افزایش در گمنامی و رؤیت‌پذیری افراد به میزان بتای آنها بر بزهدیده شدن تعرض تهدیدی کاهش وجود خواهد داشت. در این معادله، جنسیت اگرچه یک متغیر مقوله‌ای است و سطح سنجش آن نسبی یا فاصله‌ای نیست، اما به‌عنوان یک متغیر تصنعی[1] وارد معادله شده است. متغیر تصنعی برداری است که در آن به اعضا طبقهٔ معین یک عدد دلخواه و به بقیهٔ آزمودنی‌هایی که عضو آن طبقه نیستند، عدد دلخواه دیگر نسبت داده که با توجه به کدگذاری این متغیر (مرد=۱ و زن=۲) می‌توان گفت که رابطهٔ مثبت به‌این‌معناست که هرچه از طرف مردان (۱) به‌طرف زنان (۲) حرکت می‌کنیم، احتمال بیشتری وجود دارد که بزهکارانه تهدید کردیم. بنابراین، زنان بیش از مردن بزهدیده تعرض تهدید قرار می‌گیرند. درمجموع، می‌توان گفت که متغیرهای حاضر در معادله در حدود ۵۸ درصد واریانس تعرض تهدید را تبیین کرده‌اند.

1 Dummy Variable

در مدل دوم، متغیرهای اصلی تحقیق با تعرض سایبری سرقت اطلاعات در معادلهٔ قرار گرفته است. میزان واریانس تبیین‌شده در حدود ۴۳ درصد است. در این مدل، رؤیت‌پذیری دارای بتای معناداری و مثبتی بوده است. این نتیجه برای ریسک‌پذیری نیز وجود داشته است. به این معنا که هرچه افراد رؤیت‌پذیری بیشتری در اینترنت دارند و ازسوی‌دیگر، در روابط خود ریسک بالاتری دارند به میزان بتای مندرج در جدول بر میزان احتمال بزهدیده شدن آنها افزوده می‌شود.

جدول شمارهٔ ٤: نتایج تحلیل رگرسیونی متغیر وابسته بزهدیده شدن تعرض سایبری (سرقت اطلاعات)

ردیف	متغیرهای پیش‌بینی	ضرایب Beta	آزمون T	معناداری sig	ضریب تبیین R^2	آزمون F	معناداری sig
۱	**رؤیت‌پذیری**	./۶۰۳	۸,۱۸۷	./۰۰۰	./۴۲۷	۲۵,۷۴۲	./۰۰۰
۲	**سواد دیجیتال**	-./۲۱۹	-۳,۳۳۵	./۰۰۱			
۳	**فعالیت بزهکارانه**	./۲۸۷	۳,۳۱۰	./۰۰۱			
۴	**ریسک‌پذیری**	./۲۲۴	۲,۵۳۱	./۰۱۲			
۵	**میزان درآمد**	-./۰۷۹	-۱,۴۰۷	./۱۶۲			

همان‌طور که قابل‌مشاهده است در جدول فوق، سواد دیجیتال دارای رابطهٔ منفی و معناداری با تعرض از نوع سرقت و اطلاعات بوده است؛ یعنی افزایش سواد دیجیتال کاهش بزهدیده شدن تعرض را در پی خواهد داشت.

در مدل سوم، متغیرهای اصلی تحقیق با تعرض نشر اکاذیب در ارتباط گذاشته شده است. این مدل نیز براساس نتایج آزمون F معنادار بوده است. واریانس تبیین شده از تعرض نشر اکاذیب توسط متغیرهای مستقل حاضر در معادله به میزان ۵۷ درصد بوده است. و مابقی این واریانس توسط متغیرهای دیگر قابل تبیین است که در این پژوهش موردمطالعه نبوده است.

جدول شمارهٔ ۵: نتایج تحلیل رگرسیونی متغیر وابسته بزهدیده شدن تعرض سایبری (نشر اکاذیب)

ردیف	متغیرهای پیش‌بینی	ضرایب Beta	آزمون T	معناداری sig	ضریب تبیین R^2	آزمون F	معناداری sig
۱	**رؤیت‌پذیری**	./۷۶۸	۱۱,۶۹۷	./۰۰۰	./۵۷۷	۳۵,۶۷۰	./۰۰۰
۲	**خودکنترلی**	-./۱۴۳	-۲,۴۰۶	./۰۱۸			
۳	**فعالیت بزهکارانه**	./۱۵۶	۲,۴۲۷	./۰۱۷			
۴	**سواد دیجیتال**	./۱۴۲	۲,۳۸۵	./۰۱۹			
۵	**میزان درآمد**	./۰۲۶	.۴۴۶	./۶۵۷			

همان‌طور که از جدول فوق پیداست، به‌ترتیب رؤیت‌پذیری، خودکنترلی، فعالیت بزهکارانه و سواد دیجیتال دارای رابطهٔ معناداری با تعرض نشر اکاذیب بوده‌اند. در این میان، خودکنترلی ارتباط منفی و معناداری به میزان ۱۴۳/.- می‌باشد. یعنی به‌ازای هر واحد افزایش در خودکنترلی افراد به میزان بتای مذکور در تعرض سایبری نشر اکاذیب کاهش خواهیم داشت.

اما در مدل چهارم، رگرسیون متغیر وابسته تعرض مزاحمتی اجراشده است. یافته‌های مندرج در جدول نشان می‌دهد که به ترتیب رؤیت‌پذیری با بتای ۳۲۶/.، کنترل اجتماعی با بتای ۳۳۸/.-، ریسک‌پذیری با بتای ۲۵۰/.-، وضعیت تحصیلی با بتای ۲۳۲/.، میزان درآمد با بتای ۱۸۰/. و جنسیت با بتای ۱۳۹/. دارای ارتباط معنادار با تعرض مزاحمتی بوده‌اند.

جدول شمارهٔ ٦: نتایج تحلیل رگرسیونی متغیر وابسته بزهدیده شدن تعرض سایبری (مزاحمت و آزار)

ردیف	متغیرهای پیش‌بینی	ضرایب Beta	آزمون T	معناداری sig	ضریب تبیین R^2	آزمون F	معناداری sig
۱	**رؤیت‌پذیری**	۳۲۶/.	۴,۶۶۲	۰۰۰/.	۲۵۵/.	۱۱,۲۵۳	۰۰۰/.
۲	**کنترل اجتماعی**	-۳۳۸/.	-۳,۳۷۴	۰۰۰/.			
۳	**ریسک‌پذیری**	-۲۵۰/.	-۳,۲۲۵	۰۰۱/.			
۴	**وضعیت تحصیلی**	-۲۳۲/.	-۳,۵۸۵	۰۰۰/.			
۵	**میزان درآمد**	۱۸۰/.	۲,۷۶۶	۰۰۶/.			
۶	**جنسیت**	۱۳۹.	۲,۱۹۶	۰۲۹/.			

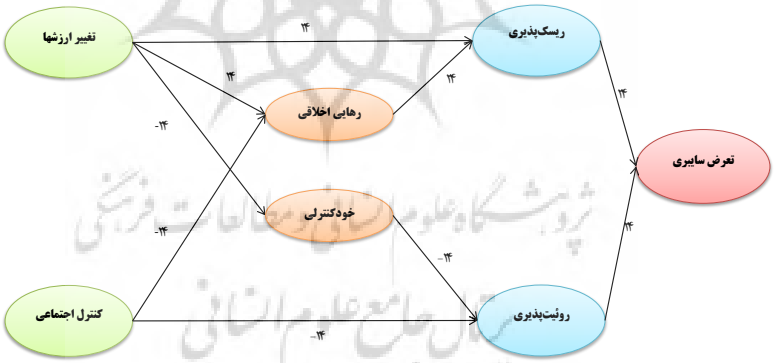
از نکات قابل‌توجه این جدول ارتباط معناداری بین درآمد و تعرض سایبری مزاحمتی است. به‌این‌معنا که افزایش درآمد احتمالی بزهدیده شدن را افزایش می‌دهد. همچنین در این مدل، زنان بیشتر از مردان در معرض تعرض مزاحمتی قرار می‌گیرند. درمجموع، متغیرهای فوق ۲۶ درصد واریانس این تعرض را تبیین نموده‌اند و مقدار F گزارش می‌کند که کل معادله رگرسیون ازلحاظ آماری معنادار می‌باشد.

تحلیل مسیر

همچنان‌که مدل ۲ نشان می‌دهد، متغیرهای مستقل اصلی (بدون زمینه‌ای) اثرات معنادار و همچنین مستقیم و غیرمستقیم بر بزهدیده شدن تعرض سایبری دارند. پیش از تحلیل، دو نکته لازم به ذکر است اول اینکه دو شیوه برای ترسیم یا حذف اثرات مستقیم یا غیرمستقیم وجود دارد. یکی نظریه و چارچوب

نظری است که به‌کار گرفته‌شده و دیگری، پیراستن نظری است که براساس دو ملاک معناداری نظری و آماری صورت می‌پذیرد. دوم اینکه، میان متغیرهای وابسته درونی ریسک‌پذیری و رؤیت‌پذیری روابط معنادار علی وجود دارد، ولی به دلیل اینکه ترسیم آن مدل تحلیل مسیر را نسبت به پیش‌فرض‌های آن دچار مشکل می‌سازد و علاوه‌برآن، بر پیچیدگی‌های آن _که خلاف اصل ساده بودن مدل‌ها است_ می‌افزاید بنابراین این مسیر علی حذف شده است. همان‌طور که از مدل پیداست، تغییر ارزش‌ها اثرات مستقیمی بر متغیرهایی چون ریسک‌پذیری به میزان ۶۶۵/.، بر کناره‌گیری اخلاقی به میزان ۲۸۶/. و بر خودکنترلی به میزان ۲۶۸/.-گذاشته است. همان‌طور که پیش‌ازاین اشاره شد، این اعداد ضرایب مسیر بتا هستند. و به‌این‌صورت تفسیر می‌شوند که به‌طورمثال، به‌ازای هر واحد افزایش در تغییر ارزش‌ها به مقدار ۶۶۵/. بر ریسک‌پذیری افزوده می‌شود.

همچنین کنترل اجتماعی دارای اثر مستقیمی بر کناره‌گیری اخلاقی و به میزان ۵۹۱/.- داشته است. اثر این متغیر بر رؤیت‌پذیری ۱۴۴/.- می‌باشد. اثرات غیرمستقیم کنترل اجتماعی بر بزهدیده شدن تعرض سایبری از طریق متغیر کناره‌گیری اخلاقی انجام می‌پذیرد. همچنین تغییر ارزش‌ها نیز از طریق خودکنترلی اثر غیرمستقیم بر بزهدیده‌شدن تعرض سایبری دارد.



نمودار شمارهٔ ۲: مدل تحلیل مسیر

به‌طورکلی، این مدل نشان می‌دهد که شهروندان تهرانی با توجه به نگرشی که به فضای مجازی دارند، در معرض بزهدیده شدن قرار می‌گیرند. یکی تغییر ارزش‌ها و دیگری کاهش کنترل اجتماعی در فضای مجازی است. به‌این‌معنا که افراد احساس می‌کنند در فضای مجازی، روابطشان کمتر کنترل می‌شود. علاوه‌براین نسبت به روابط بین دو جنس ارزش‌ها و نگرش‌های تغییریافته‌ای دارند که با جریان

زندگی واقعی آنها متفاوت است. چنین احساس و نگرشی شرایط را برای نوعی کناره‌گیری اخلاقی فراهم می‌کند. به‌این‌معنا که افراد بر این تصورند که در فضای مجازی، هرطور بخواهند، رفتار می‌کنند و نسبت به رفتارهای خود پاسخگو نیستند. این کناره‌گیری اخلاقی موجب افزایش ریسک‌پذیری افراد در ارتباط‌گیری با افراد غریبه می‌شود. همچنین تغییر ارزش‌ها موجب می‌شود که افراد از خودکنترلی کمتری در رفتارهای خود داشته باشند و در مقابل، درخواست‌های دیگران منفعلانه عمل کنند. بنابراین کاهش خودکنترلی، موجب رؤیت‌پذیری بیشتر افراد می‌شود و در ارائهٔ اطلاعات فردی و تصویری مقاومت کمتری از خود نشان می‌دهند. چنین فرایندی درنهایت، موجب افزایش ضریب بزهدیده شدن افراد در فضای سایبری می‌شود.

مدل تحلیل مسیر بیانگر دو سطح از عوامل در فرایند وقوع تعرض سایبری است؛ یکی نگرش و ارزش‌های شکل‌گرفته افراد نسبت به فضای سایبری است و دیگر رفتار و کیفیت عملکرد بزهدیده در این فضاست. بنابراین، می‌توان گفت که افراد بزهدیده تعرض سایبری تحت تأثیر نگرش‌های خود رفتارهای از خود بروز می‌دهند که نقش آنها را در وقوع جرم پررنگ می‌کند. به‌عبارت‌دیگر، آنها را به اهداف مناسبی برای بزهکاران باانگیزه تبدیل می‌کند. لازم به ذکر است که تمامی متغیرهای زمینه‌ای تحقیق مانند تحصیلات، درآمد، وضعیت شغلی، قومیت و مذهب فاقد ارتباط معنادار با متغیر وابسته تحقیق بوده‌اند و در مدل‌های مختلف، رگرسیون ناپایدار بوده و از مدل نهایی حذف شدند.

بحث و نتیجه‌گیری

یافته‌های این پژوهش نشان می‌دهد که اینترنت در میان اقشار مختلف جامعه، توسعه پیدا کرده است و زندگی بدون آن به امری غیرممکن تبدیل شده است. کاربران تهرانی به‌طور متوسط، ۴ ساعت و ۱۶ دقیقه در فضای سایبری سپری می‌کنند که اگر زمان خواب و استراحت را از ۲۴ ساعت شبانه‌روز کم کنیم، می‌توان گفت که در حدود یک‌چهارم وقت شهروندان در فضای اینترنت می‌گذرد. این مقدار در شرایطی است که هنوز تا الکترونیک شدن بسیاری از خدمات بخش دولتی و خصوصی فاصله زیادی وجود دارد.

دوم اینکه، پراستفاده‌ترین وسیلهٔ ارتباطی شهروندان به اینترنت تلفن همراه (۸۷/۵ درصد) آنهاست؛ یعنی ابزاری که هر لحظه افراد را در معرض کیفیات مثبت و منفی فضای سایبری قرار می‌دهد. بنابراین، اگر از منظر جامعه‌شناسی جرم به این موضوع نگریسته شود، می‌توان ادعا نمود که شهروندان امروزی در معرض فضاهای بی‌دفاع خودساخته‌ای قرار دارند که همیشه با آنها همراه است.

سوم اینکه، یافته‌های پیمایش بزهدیده‌شناسی این پژوهش، نرخ وقوع تعرض سایبری را در حدود ۸/۹ درصد گزارش می‌کند. این میزان اگرچه در ظاهر بسیار کوچک می‌نماید، اما چنانچه در جمعیت‌های بزرگی همچون پایتخت و/یا در سطح ملی محاسبه شود، رقم‌های بالای از وقوع تعرض سایبری را بیان می‌نماید

که از دید و رصد بسیاری از نهادهای ذی‌ربط مغفول مانده است. برای مثال، با احتساب ۴۰ میلیون نفر کاربر اینترنت در کشور و ضرب آن در ۸/۹ درصد (نرخ تعرض سایبری) عدد ۳ میلیون و پانصد و شصت هزار نفر به‌دست می‌آید. بنابراین یافته‌ها می‌توان ادعا نمود که تعرض سایبری یک مسئلهٔ اجتماعی است که نیازمند توجه صاحب‌نظران دانشگاهی و سیاست‌گذاران اجتماعی است.

از مهم‌ترین یافته‌های این پژوهش موضوع سبک زندگی آنلاین افراد بزهدیده و بزهکار است. یافته‌های این تحقیق نشان می‌دهد که اگرچه شدت حضور در فضای سایبری ارتباط معناداری با تعرض سایبری دارد، اما این معناداری در تحلیل‌های چند متغیری، به‌ویژه تحلیل رگرسیون، معناداری خود را از دست می‌دهد. و به‌جای شدت حضور، این کیفیت حضور در این فضاست که نقش تعیین‌کننده‌ای دارد. رؤیت‌پذیری و ریسک‌پذیری دو کیفیت مهمی هستند که در تبیین تعرض سایبری روابط معنادار و پایداری را از خود نشان داده‌اند. براساس این دو مفهوم، هرچه که افراد از خود اطلاعات (فردی، خانوادگی، عکس، فیلم و...) بیشتری منتشر می‌کنند، احتمال زیادتری وجود دارد که قربانی تعرض سایبری قرار گیرند. همچنین هرچه افراد در ارتباط گرفتن با افراد غریبه ریسک بیشتری را متحمل می‌شوند، احتمال بیشتری نیز برای درگیر شدن آنها در تعرض سایبری، چه به‌عنوان بزهکار و چه بزهدیده، فراهم می‌نماید.

تحلیل‌های رفتارشناسانهٔ فوق زمانی توضیح‌دهندگی بیشتری پیدا می‌کنند که بتوان آنها را در بسترهای اجتماعی‌شان تبیین نمود چیزی که می‌توان از آن به‌عنوان جامعه‌شناسی تعرض سایبری یاد نمود. دراین‌راستا، برخی از یافته‌های این پژوهش نشان می‌دهد که نظام ارزشی افراد ازیک‌سو و نگرش‌های آنها به فضای سایبری ازسوی‌دیگر، عوامل مهمی در بروز رفتارهایی است که در فوق به آنها اشاره شد.

جامعهٔ اطلاعاتی و در رأس آن، فضای سایبر بسترهای رشد فردیت را بیش از پیش میسر نموده است. افراد در فضاهای واقعی زندگی با انبوهی از ارزش‌ها، هنجارها و قواعد جمعی روبرو هستند که به‌طور دائمی، آنها را در فعالیت‌های و تعاملات روزانه خود بازآفرینی می‌کنند. این قواعد جمعی به نیروی اجتماعی تبدیل شده است که چیزی جز هم‌نوایی افراد را نمی‌طلبد. در عالم واقع، افرادی که از خود هم‌نوایی نشان نمی‌دهند، با توبیخ‌های اجتماعی مواجه می‌شوند که در برخی مواقع، به انزوا اجتماعی و طرد آنها از جمع منجر می‌شود؛ انزوایی که برای انسان ذاتاً اجتماعی بار سنگینی است که هر کس تاب تحمل آن را ندارد. شیوهٔ زندگی انسان امروزی چیزی است که در این مقام از تحلیل می‌تواند توضیح‌دهنده باشد.

انسان مصرف‌زدهٔ امروزی کسی است که بیش از هرچیزی برای توسعهٔ انتخاب‌های خود ارزش قائل است و مادامی‌که این انتخاب‌ها از سوی قواعد جمعی تحدید می‌شوند، لذت و نشاط انتخاب و گزینش برای او محقق نمی‌شود. به همین دلیل می‌توان گفت که در فضای واقعی، فردیت افراد در معرض

محدودیت‌های جمعی قرار می‌گیرد. فضای سایبری با توجه به شرایط حاکمیتی که بر آن وجود دارد و همچنین قابلیت‌های فنّاورانه آن برای گمنامی و ایجاد ارتباط با میانجی، شرایط را فراهم نموده که افراد بتوانند فردیت‌های خود را با تنوع بالایی بروز دهند.

افراد در این فضا، بسیار راحت‌تر از فضای واقعی ارزش‌های جمعی را زیر سؤال می‌برند و/یا حتی علیه آن قیام می‌کنند، زیرا که می‌دانند ارتباط آنها با دیگران ارتباطی با میانجی است که یک لایهٔ مصونیتی برای آنها می‌آفریند. افراد در این شرایط مکنونات درونی و پنهان خود را بیشتر به نمایش می‌گذارند، زیراکه دیگر خبری از قضاوت‌ها و توبیخ‌های اجتماعی، که در ارتباط ناب و چهره‌به‌چهره شکل می‌گیرد، نیست. به‌عبارت‌دیگر، رشد فردیت در فضای سایبری زمینه‌ساز کناره‌گیری اخلاقی افراد را میسر می‌سازد. آنها می‌دانند که در این فضا، واپایش‌های اجتماعی زندگی واقعی وجود ندارد و آزادانه‌تر از قبل به خواسته‌های و تمایلات فردی خود جامهٔ عمل می‌پوشانند. برای مثال، شخصی که در زندگی واقعی، از ترس نگاه‌ها و قضاوت‌های مردم از ارتباط با جنس مخالف خود می‌پرهیزد در این فضا، فارغ از آن نگاه‌ها ارتباط خود را مستقر می‌نماید و این همان چیزی است که می‌توان از آن به‌عنوان ارزش‌زدایی یا کناره‌گیری اخلاقی نام برد.

ازلحاظ نظری و عملی، ارزش‌ها و نگرش‌های افراد ازیک‌سو و واپایش‌های اجتماعی ازسوی‌دیگر، عوامل مهمی در عدم رخداد یک جرم محسوب می‌شوند. بنابراین، افرادی که ارزش‌های اجتماعی را نادیده می‌انگارند بیشتر در فعالیت‌های مجرمانه درگیر می‌شوند و ریسک‌پذیری آنها در تعاملات اجتماعی و خلق موقعیت‌های جدید در زندگی بالاتر است. در موضوع تعرض سایبری، افرادی که ارزش‌های اجتماعی را به کناری می‌گذارند و واپایش‌های اجتماعی در این فضا را تقلیل یافته می‌پندارند، دچار نوعی کناره‌گیری اخلاقی می‌شوند. این کناره‌گیری اخلاقی آنها را به‌جایی می‌رساند که از خود اطلاعات خصوصی بیشتری عرضه می‌کنند و علاوه‌برآن در ارتباط‌گیری با افراد غریبه جهت‌گیری‌های عامگرایانه و همراه با ریسک‌پذیری بیشتری از خود نشان می‌دهند. به همین دلیل به شکلی ناخواسته در فعالیت‌های مجرمانه درگیر می‌شوند. شاید به همین دلیل باشد که بسیاری از بزهکاران تعرض سایبری فاقد سابقه کیفری می‌باشند. بنابراین، می‌توان گفت که جامعه‌شناسی تعرض سایبری به بسترهای تغییر ارزش‌ها و نگرش‌هایی می‌پردازد که زمینه‌ساز فردگرایی مضاعف افراد را در پرتو جامعهٔ اطلاعاتی است.

علاوه‌بر آنچه درخصوص رؤیت‌پذیری و ریسک‌پذیری افراد در فضای سایبری گفته شد، یافته‌های تحلیل عاملی گزارش می‌کند که درمجموع می‌توان دو نوع سبک زندگی آنلاین را در فضای سایبری از یکدیگر بازشناخت یکی سبک زندگی هدفمند و کاربردی و دیگری سبک زندگی ماجراجویانه است. در سبک زندگی هدفمند، اغلب فعالیت‌های خود در اینترنت را در جهت انجام فعالیت‌های کاری و به‌صورت

مشخص برنامه‌ریزی می‌کنند که از آن جمله می‌توان به فعالیت تجاری، اداری و علمی آموزشی اشاره نمود. درحالی‌که سبک زندگی ماجراجویانه با ویژگی‌هایی چون تفریحی بودن و رابطه‌جویی (مانند حضور در شبکه‌های اجتماعی، ایمیل، بازی، فیلم و ...) قابل تعریف است. همچنین یافته‌های این پیمایش نشان داده است که افراد قربانی به‌طور متفاوت و معناداری، حضور بیشتری در فعالیت‌های تفریحی و ارتباط‌جویانه دارند. بنابراین، می‌توان گفت که سبک زندگی ماجراجویانه در فضای سایبری عامل مهمی در تبیین چرایی مورد تعرض واقع شدن افراد می‌باشد.

منابع

- ابوذری، مهرنوش (۱۳۹۱). *جرم‌شناسی جرائم سایبری*. پایان‌نامهٔ کارشناسی ارشد به راهنمایی عباس شیری، دانشگاه تهران، دانشکده حقوق و علوم‌سیاسی، گروه حقوق جزا و جرم‌شناسی.
- نجفی ابرندآبادی، علی‌حسین (۱۳۸۳). *تقریرات درس جرم‌شناسی*. مجموعه دو جلدی به کوشش شهرام ابراهیمی.
- نجفی ابرندآبادی، علی‌حسین (۱۳۸۸). دربارهٔ بزهکاری و جرم‌شناسی سایبری (گفتگو)، *مجله تعالی حقوق*، شماره ۳۶، ص ۱-۷.
- نجفی ابرندآبادی، علی‌حسین (۱۳۷۴). *تقریرات بزه‌دیده‌شناسی*. دورهٔ کارشناسی دانشگاه شهیدبهشتی. تنظیم فاطمه قناد.
- Back, Sinchul. (2016). Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory. In BSU Master's Theses and Projects. Item 30. Available at http://vc.bridgew.edu/theses/30.
- Baum, K.; Catalano, S.; Rand, M.; Rose, K. (2009). Stalking victimization in the United States. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.
- Bocij, P. & McFarlane, L. (2003a). Cyberstalking: The technology of hate. *The Police Journal*, 76: 204-221.
- Bocij, P.; McFarlane, L. (2003b). Seven fallacies about cyberstalking. *Prison Service Journal*, 149: 37-42.
- Bocij, P. (2004). Cyber stalking: Harassment in the Internet age and how to protect your family.Westport, CT: Praeger Publishers.
- Bocij, P., & McFarlane, L. (2003). Seven fallacies about cyberstalking. *Prison Service Journal*, 149: 37-42.
- Bocij, P., Griffiths, M., and McFarlane, L. (2002). Cyberstalking a new challenge for criminal law Criminal Lawyer, 122, 3-5.
- Bossler, A. M., & Holt, T. J. (2010). The Effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38: 227-236.
- Burgess Alexy, E., , A., Baker, T., & Smoyak, S. (2005). Perceptions of cyber stalking among college students. Brief Treatment and Crisis Intervention, 5, 279–289.

0 Clarke, R. V., & Felson, M. (1993). *Routine activity and rational choice*. New Brunswick, NJ: Transaction Publishers.

0 D'Ovidio, R. & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. FBI Law Enforcement Bulletin, 72(3): 10-17.

0 Dignan, J. (2005), Understanding Victims and Restorative Justice, Maidenhead: Open.

0 Finch, E. (2001). The criminalization of stalking: Constructing the problem and evaluating the solution. London: Cavendish.

0 Fisher B., & S. Lab(2010) (Eds.), *Encyclopedia of victimology and crime prevention*. Thousand Oaks: SAGE Publications, Inc. doi: 10.4135/9781412979993.n334.

0 Fukuchi, A. (2011). A balance of convenience: The use of burden-shifting devices in criminal cyberharassment law. Boston College Law Review, 52, 289-338.

0 Goodno, Naomi Harlin(2007) Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws, Missouri Law Review, Available at: http://scholarship.law.missouri.edu/mlr/vol72/iss1/7.

0 Grabosky, P.N. (2001). Virtual criminology: Old wine in new bottles? Social and Legal Studies, 10, 243-249.

0 Grabosky, P.N. (2007). Electronic Crime. Upper Saddle River, NJ: Pearson.

0 Hazelwood, Steven D.& Magnin, Sarah Koon(2013) Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis, International Journal of Cyber Criminology (IJCC) ISSN: 0974 –Vol 7 (2): 155–168.

0 Hirschi, T. (2004). Self-control and crime. In R. F. Baumeister & K. D. Vohs (Eds.), *Handbook of self-regulation: Research, theory and applications* (pp. 537-552). New York:Guilford Press.

0 Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.

0 Jaishankar, K. and Sankary, U.V. (2006). Cyberstalking: A global menace in the information super highway. All India Criminology Conference. 16-18. Madurai: India Madurai Kamaraj University.

0 Jaishankar. K (2011). Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.

0 Lindberg, D. (2012). Prevention of cyberstalking: A review of the literature. In Portland State University. Retrieved October 18, 2015.

0 Maple, Carsten & etal(2011) The Impact of Cyberstalking: review and analysis of the ECHO Pilot Project, National Centre for Cyberstalking Research.

0 Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

0 Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. International Journal of Cyber Criminology, 8, 47-56.

0 McFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. First Monday, 8(9).

0 Miethe, T. (1991). Citizen-Based Crime Control Activity and Victimization Risks: An Examination of Displacement and the Free-Rider Effect, *Criminology*, *29*, 419-441.

0 Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context : toward an integrated theory of offenders, victims, and situations*. Albany: State University of New York Press.

0 Mishra, Alok & Mishra, Deepti(2008) Cyber Stalking: A Challenge for Web Security, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/259148587.

0 Newman, G., & Clarke, R.V. (2003). Superhighway Robbery: Preventing E-commerce Crime. Portland, OR: Willan Publishing.

0 Ogilvie, E. (2000). Cyberstalking. Trends & Issues in Crime and Criminal Justice, No 166. Canberra: Australian Institute of Criminology.1-6.

0 Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58.

0 Pittaro, Michael L (2007) Cyber stalking: An Analysis of Online Harassment and Intimidation, International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 Vol 1 (2): 180–197.

0 Poonia,Ajeet Singh(2014) Cyber Crime: Challenges and its Classification, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Issue 6, 3(6), 119-121.

0 Reyns, B.W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention & Community Safety, 12, 99-118.

0 Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238.

0 Roberts, Lynne (2008) Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking, International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891, Vol 2 (1): 271–285.

0 SPITZBERG, B. H. (2002). The Tactical Topography of Stalking Victimization and Management. Trauma, Violence, & Abuse, 3(4), 261–288.

0 Stephenson, Peter R., and Walter, Richard D.(2011) Toward Cyber Crime Assessment: Cyberstalking, Annual Symposium on Information Assurance (ASIA), JUNE 7-8, ALBANY, NY.

0 Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information Communication and Society*, *11*(6), 861–884.

0 Somaiya,Jheel & etal(2014) A Survey: Web based Cyber Crimes and Prevention Techniques. International Journal of Computer Applications 105(17):6-9.

0 Yar, M. (2005). The Novelty of 'Cybercrime:' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.