بزه‌دیدگی سایبری و رفتارهای پیشگیرانه کاربران در محیط‌های آنلاین

موردپژوهی: دانشگاه زابل، ایران

.

چکیده

بزه‌دیدگی سایبری در شبکه‌های اجتماعی می‌تواند پیامدهای رفتاری، روان‌شناختی و امنیتی گسترده‌ای برای کاربران به همراه داشته باشد و شناسایی سازوکارهای مؤثر بر شکل‌گیری آن، نقش مهمی در ارتقای سیاست‌های پیشگیرانه و توسعه راهبردهای حمایتی دارد. در این راستا، پژوهش حاضر با رویکرد کمی و روش توصیفی – تحلیلی، به بررسی رابطه میان بزه‌دیدگی سایبری و رفتارهای پیشگیرانه کاربران پرداخته است. جامعه آماری پژوهش شامل کلیه دانشجویان دانشگاه زابل در سال ۱۴۰۴ است. حجم نمونه با استفاده از فرمول کوکران ۳۸۴ محاسبه شد. نمونه نهایی۱۶۲ نفر با استفاده از روش نمونه‌گیری قضاوتی در دسترس انتخاب شده‌اند. ابزار گردآوری داده‌ها پرسش‌نامه محقق ساخته‌ای است که روایی محتوایی آن از طریق نظر خبرگان و پایایی آن با بهره‌گیری از آلفای کرونباخ تأیید شده است. داده‌ها پس از جمع‌آوری با استفاده از نرم‌افزار MATLAB و به‌کارگیری آزمون‌های آماری همبستگی پیرسون و رگرسیون چندگانه مورد تحلیل قرار گرفته‌اند تا روابط علّی و هم‌زمان میان متغیرهای پژوهش بررسی شود. یافته‌های تجربی نشان می‌دهد ٦/٥٥ درصد از شرکت‌کنندگان دست‌کم یک‌بار لینک فیشینگ دریافت کرده‌اند و ۷/۳۲ درصد آنان تجربه تلاش برای سرقت اطلاعات شخصی داشته‌اند که این امر بیانگر شیوع قابل‌توجه رفتارهای مجرمانه سایبری در میان کاربران جوان است. افزون بر این، تنها ۲/٦ درصد از موارد بزه‌دیدگی به پلیس فضای مجازی گزارش شده است که این عدد نشان می دهد یکی از علل عدم تمایل به گزارش‌دهی ناشی از پیامدهای ثانویه بزه‌دیدگی اولیه است.ابر این اساس،، بازنگری در سیاست‌های پیشگیری، ارتقای سواد سایبری و تقویت مکانیسم‌های رسمی حمایت از بزه‌دیدگان یک ضرورت اجتناب ناپذیر است.

کلیدواژه‌ها: بزه‌دیدگی سایبری، امنیت سایبری، کاربران آنلاین، رفتارهای پیشگیرانه، سواد سایبری.

مقدمه

امروزه، الگوی تعاملات کاربران دانشگاهی در سایه‌گسترش فناوری‌های اطلاعاتی و ارتباطی به‌خصوص در بستر توسعه شبکه‌های اجتماعی و اینترنت دچار تحولات بنیادین شده است. این تغییرات را در حوزه‌های مختلف از جمله تقویت کیفیت آموزش در میان

کاربران دانشگاهی قابل‌مشاهده است (Apuke & Iyendo,۲۰۱۸:۱). بااین‌وجود، به‌موازات توسعه الگوهای تعاملاتی در فضای مجازی، اشکال نوینی از جرایم سایبری و بزه‌دیدگی سایبری نیز به وجود آمده است. برای نمونه، می‌توان به شکل‌گیری رفتارهای خشونت‌آمیز در میان همسالان نظیر، قلدری، آزار و اذیت، پرخاشگری در روابط عاشقانه و جرایم مرتبط با باندهای تبهکاری در بستر فضای مجازی اشاره کرد (Patton et al,.۲۰۱٤:٥٤٨) که از آن به‌عنوان جرم و جنایت دیجیتالی یاد می‌شود (Borwell et al.,۲۰۲۱:۸٥). گسترش این جرائم، زمینه بزه‌دیدگی سایبری را درمیان کاربران فعال فضای مجازی افزایش داده است (جعفری و همکاران، ۱:۱٤۰٤). هرچند تعریف جامعی از بزه‌دیدگی سایبری وجود ندارد. بااین‌حال، برخی از تعاریف ارائه شده، این پدیده شامل عناصری از آسیب عمدی و مکرر وارده از طریق استفاده از فناوری دانسته‌اند (Brown et al,.۲۰۱۷:۱۲). ابهام در دستیابی به تعریف جامع برای این اصطلاح ریشه در ابعاد پیچیده و پنهان علل شکل‌گیری جرائم سایبری و به‌تبع آن بزه‌دیدگی سایبری دارد که نشان می‌دهد، شکاف دانشی و فنی میان کاربران محیط‌های آنلاین و مجرمان سایبری، در کنار محدودیت نهادهای نظارتی در کنترل و پیشگیری از جرائم اینترنتی سبب شکل‌گیری «بی‌دفاعی دیجیتال» در فضای مجازی شده است (Wall, ۲۰۰۸:۱).

اگرچه، ارتقای سواد و مهارت‌های استفاده از فناوری‌های اطلاعات در محیط‌های دانشگاهی به کاهش مخاطرات استفاده از فضای مجازی کمک شایانی می‌کند (Hashemi et al.,۲۰۲۲:۱). بااین‌وجود، به دلیل حضور گسترده کاربران آنلاین در شبکه‌های مجازی، عدم آگاهی و مهارت لازم در خصوص چگونگی حفاظت از خود در بستر فضای مجازی، تفاوت‌های فرهنگی در چگونگی استفاده از محیط‌های آنلاین و میزان دسترسی به شبکه اینترنت، کاربران را در معرض بزه‌دیدگی سایبری قرار داده است (Chudal.,۲۰۲۲:۱۳۹۱). بسیاری از کشورها تلاش‌هایی را باهدف بهبود زیرساخت‌های اینترنتی پیشرفته، توجه به‌نظام آماری دقیق و سیاست‌گذاری‌های پیشگیری از جرائم سایبری باهدف کاهش بزه‌دیدگی سایبری را صورت داده‌اند (Ho & Luong,۲۰۲۲:۱). این تلاش‌ها سبب افزایش آگاهی از شیوه‌های ارتکاب جرائم سایبری، شناخت الگوهای بزه‌دیدگی و واکنش‌های پیشگیرانه کاربران فضای آموزش و پژوهش را به دنبال داشته است. از رهگذر شناخت عوامل اثرگذار، دانش و مهارت‌های پیشگیرانه کاربران فضای مجازی را افزایش داده‌اند و در نتیجه آن شاهد کاهش بزه‌دیدگی سایبری بوده‌اند (Suzuki,۲۰۲٤:۳۷۳). این نتایج نشان می‌دهد که رابطه معناداری میان عدم آگاهی در مورد جرایم سایبری و اقدامات امنیت سایبری با بزه‌دیدگی سایبری وجود دارد (Ahmead et al.,۲۰۲٤:۱). در این میان، دانشگاه زابل به‌عنوان یکی از دانشگاه‌های بزرگ شمال شرق ایران، محیطی چندفرهنگی و در حال گذار از نظر دیجیتالی‌شدن خدمات آموزشی و ارتباطی است. رشد سریع استفاده از سامانه‌های برخط، شبکه‌های اجتماعی و تعاملات اینترنتی در میان دانشجویان، ضمن افزایش فرصت‌های علمی، خطر مواجهه آنان را با بزه‌دیدگی سایبری به جهت تفاوت در سطح آگاهی فناوری، جنسیت، رشته تحصیلی و وضعیت اقتصادی افزایش داده است. از این رو، توجه به اصول، رویکردها و الگوهای شناسایی شده در حوره پیشگیری از بزهکاری، می‌تواند اثر گذاری لازم را در مهار پدیده بزهکاری و (کاهش بزه دیدگی) ایفا نماید(خواجه نوری و نیاز پور،۱٤۰۳:۱٥۸). به همین دلیل، این تحقیق، نه‌تنها می‌تواند تصویری دقیق از وضعیت امنیت سایبری در محیط دانشگاهی ارائه دهد، بلکه به سیاست‌گذاران دانشگاهی و نهادهای انتظامی کمک می‌کند تا برنامه‌های آگاهی‌بخشی و

پیشگیرانه مؤثرتری را تدوین کنند. ازاین‌رو، پرسش اصلی این پژوهش این است که اشکال بزه‌دیدگی سایبری در میان دانشجویان دانشگاه زابل شامل چه رفتارهایی است؟ واکنش‌های پیشگیرانه کاربران این محیط‌ها از چه الگوهای رفتاری تبعیت می‌کند؟ مطالعه حاضر باهدف پر کردن این خلأ، به بررسی رابطه میان بزه‌دیدگی سایبری و رفتارهای پیشگیرانه کاربران دانشگاهی در محیط‌های آنلاین می‌پردازد و تلاش دارد تا ضمن شناسایی اشکال مختلف رفتارهای پیشگیرانه، رابطه میان تجربه بزه‌دیدگی و تمایل به رفتارهای پیشگیرانه را مورد تحلیل و بررسی قرار دهد. نتایج این مطالعه، ضمن پر کردن خلأ دانشی در زمینه بومی‌سازی مطالعات بزه‌دیدگی سایبری در فضای دانشگاه‌های ایران، می‌تواند مبنایی برای طراحی سیاست‌های پیشگیرانه محلی و بومی در زمینه بزه‌دیدگی سایبری باشد. زیرا، از رهگذر تقویت سواد سایبری و آموزش‌های لازم نظیر، مدیریت رمز عبور، استفاده از ایمیل، استفاده از اینترنت، استفاده از رسانه‌های اجتماعی، چگونگی استفاده از دستگاه‌های تلفن همراه، مدیریت اطلاعات و گزارش حوادث سایبری کاهش بزه‌دیدگی سایبری هدفی دست‌یافتن خواهد بود (Kont,۲۰۲٤:۱۳۵). به همین منظور، ابتدا، چارچوب مفهومی و پیشینه نظری پژوهش مرور می‌شود؛ سپس، به روش‌شناسی تحقیق، جامعه آماری، ابزار گردآوری داده‌ها و شیوه تحلیل پرداخته خواهد شد؛ پس از آن، یافته‌های توصیفی و تحلیلی ارائه می‌شود؛ همچنین، تلاش می‌شود تا بحث و تفسیر نتایج در پرتو نظریه‌های جرم‌شناسی مورد کنکاش قرار گیرد.

۱-پیشینه تحقیق

علیوردنیا و سیاهکل رودی (۱۳۹۸) در پژوهشی با عنوان «**بررسی جامعه‌شناختی بزه‌دیدگی ناشی آزاررسانی سایبری در میان دانشجویان دانشگاه مازندران**» به بررسی مشکلات ناشی از بزه‌دیدگی سایبری از منظر جامعه‌شناختی پرداخته‌اند. مطالعه آنان با روش پیمایشی بر روی نمونه ۳۷٤ نفری نشان داد که سه متغیر سبک زندگی منحرفان آنلاین، محافظت آنلاین (به طور مستقیم) و مجاورت آنلاین با متخلفان (به طور معکوس) تأثیر معناداری بر بزه‌دیدگی ناشی از آزاررسانی سایبری دارد. همچنین، یافته‌ها این پژوهش نشان داد که دختران بیش از پسرها قربانی بزه‌دیدگی مالی و جنسی می‌شوند.

مالمیر و زررخ (۱۳۸۹) در پژوهشی با عنوان «پیشگیری از بزه‌دیدگی سایبری» به این مسئله مهم پرداخته‌اند که بزه‌دیده‌شناسی سایبری پدیده‌ای پیچیده و نوین است؛ لذا، شناخت زمینه‌های بزه‌دیدگی و علل آن از مهم‌ترین مباحث جرم‌شناسانه امروز دررابطه‌با فضای مجازی است. مطالعه آنان در ابتدا به مبانی جرم‌شناسی در حوزه علل وقوع بزه‌دیدگی سایبری پرداخته است. یافته‌های تحقیق آنان نشان می‌دهد که پیشگیری وضعی و بهره‌گیری از نیروی حفاظتی خارجی یا همان پلیس سایبری، از مهم‌ترین راهکارهای پیشگیری از بزه‌دیدگی سایبری است.

دانش ناری و همکاران (۱۳۹۷) در تحقیق با عنوان «تحلیل بزه‌دیدگی جنسی زنان در شبکه‌های اجتماعی: نمونه پژوهی تانگو» به مقوله رشد اینترنت و افزایش روابط اجتماعی در بستر فضای مجازی پرداخته‌اند. آنان در این پژوهش تاکید کردند که اگرچه گسترش ارتباطات در فضای مجازی فرصت مناسبی جهت به اشتراک گذاشتن دانش، سوابق شغلی و حرفه‌ای را فراهم آورده است. با

این‌حال، عواملی چون نمایه عمومی کاربران در تنظیمات اولیه این برنامه، عدم رعایت حریم خصوصی توسط کاربران، امکان یافتن کاربران زن از طرق مختلف، عدم نظارت اولیه شبکه تانگو در ارسال تصاویر و ویدئوها و عدم سازوکارهای مناسب جهت شناسایی هویت واقعی کاربران، زمینه‌ی بزه دیدگی جنسی زنان را افزایش داده است.

جامی‌پور و همکاران (۱۳۹۹) در مطالعه‌ی با عنوان «بررسی رابطه بین مهارت‌های سایبری و میزان بزه دیدگی سایبری» به بررسی رابطه مهارت‌های سایبری و میزان بزه‌دیدگی سایبری و در نهایت شناسایی راهکارهایی برای توسعه این مهارت‌ها پرداخته‌اند. یافته‌های پژوهش حاضر نشان می‌دهد که با گسترش ابزارهای دیجیتال و شبکه‌های اجتماعی، فرصت‌های تعامل و یادگیری مهارت‌های سایبری افزایش یافته است، اما ضعف در مهارت‌های امنیتی کاربران، رعایت ناکافی حریم خصوصی و نبود سازوکارهای حفاظتی مؤثر، زمینه بزه‌دیدگی سایبری را تشدید می‌کند. این نتایج، حاکی از آن است که مهارت‌های پایه‌ای، حل مسئله و ایمنی/قانونی نقش کاهش‌دهنده در حوزه بزه‌دیدگی دارند و توسعه این مهارت‌ها در خانواده، مدرسه و جامعه/دولت برای ایجاد فضای آنلاین امن ضروری است.

فارل و ام درو[۱] (۲۰۱۸) در پژوهشی با عنوان «خطر قربانی شدن آنلاین و استراتژی‌های خود حفاظتی: توسعه برنامه‌های پیشگیری از کلاهبرداری سایبری تحت هدایت پلیس» به بررسی نقش آگاهی، دانش و رفتارهای خود حفاظتی کاربران در مواجهه با کلاهبرداری‌های سایبری پرداخته شده است. یافته‌های پژوهش نشان می‌دهد که با افزایش تنوع و نوآوری در روش‌های کلاهبرداری، میزان بزه‌دیدگی سایبری نیز روندی صعودی یافته است. بااین‌حال، نتایج نشان داد افرادی که باوجود آگاهی از خطرات و دانش کافی درباره رفتارهای ایمن آنلاین، از استراتژی‌های پیشگیری به‌درستی استفاده نمی‌کنند، بیش از دیگران در معرض قربانی شدن قرار دارند. براین‌اساس، پژوهش مذکور بر ضرورت طراحی و اجرای برنامه‌های آموزشی مهارت‌محور از سوی نهادهای پلیسی و آموزشی برای ارتقای رفتارهای پیشگیرانه در فضای مجازی تأکید دارد.

میچل[۲] و همکاران (۲۰۱۱) در تحقیقی با عنوان« قربانی شدن جوانان در اینترنت در یک زمینه قربانی شدن گسترده‌تر» به تحلیل میزان قربانی شدن در فضای مجازی و واقعی و تأثیر آن بر سلامت روان و رفتارهای بزهکارانه پرداخته شده است. داده‌های این پژوهش از طریق مصاحبه تلفنی با ۲۰۵۱ نوجوان ۱۰ تا ۱۷ ساله در قالب بررسی ملی مواجهه کودکان با خشونت گردآوری شد. یافته‌ها نشان دادند که بین بزه‌دیدگی آنلاین و آفلاین ارتباطی قوی وجود دارد، به‌گونه‌ای که بیشتر قربانیان فضای مجازی، در محیط‌های آفلاین نیز مورد آزار قرار گرفته‌اند. قربانیان آنلاین سطوح بالاتری از آسیب‌های روانی، تجربه تروما و رفتارهای بزهکارانه را گزارش کردند. بر این اساس، پژوهش تأکید می‌کند که برنامه‌های پیشگیری و مداخله باید به‌صورت جامع و چندبعدی طراحی شوند و تنها بر آموزش ایمنی اینترنت تمرکز نداشته باشند.

[۱] Farrell &M. Drew
[۲] Mitchell

باسلر[۳] و همکاران (۲۰۱۲) در پژوهشی با عنوان «پیش‌بینی قربانی آزار و اذیت آنلاین شدن در میان جمعیت نوجوانان» به تحلیل تجارب بزه‌دیدگی سایبری در میان دانش‌آموزان مقطع راهنمایی و دبیرستان پرداخته شده است. در این پژوهش، داده‌ها از طریق نظرسنجی از ٤٣٤ دانش‌آموز در مدارس ایالت کنتاکی جمع‌آوری و با استفاده از مدل‌های رگرسیون لجستیک چندگانه تحلیل شدند. یافته‌ها نشان دادند که احتمال قربانی شدن در آزار و اذیت آنلاین در میان نوجوانانی بیشتر است که از شبکه‌های اجتماعی استفاده مکرر دارند، با همسالان مرتکب آزار آنلاین در ارتباط‌اند و اطلاعات شخصی یا حساس خود را به‌صورت عمومی منتشر می‌کنند. بر اساس نتایج، پژوهش بر ضرورت آموزش‌های آگاهی‌بخش درباره رفتار ایمن در فضای مجازی و تدوین سیاست‌های حمایتی برای کاهش بزه‌دیدگی نوجوانان در محیط‌های آنلاین تأکید می‌کند.

۲- مبانی نظری

۲-۱- نظریه مدیریت ریسک

نظریه مدیریت ریسک [٤]یکی از رویکردهای کلیدی در تحلیل رفتار کاربران در محیط‌های آنلاین به شمار می‌رود که بر چگونگی ادراک، ارزیابی و کنترل مخاطرات احتمالی توسط افراد در فضای مجازی تمرکز دارد. این دیدگاه معتقد است که واکنش افراد در مواجهه با ریسک‌های حوزه فناوری تابعی از آگاهی، ارزیابی ذهنی و توانایی کنترل ریسک‌ها تأثیر می‌پذیرد (Tsai,۲۰۲٤:۲). بااین‌حال، اکثر افرادی که از اینترنت استفاده می‌کنند، هنگام نظارت و افشای اطلاعات شخصی چه به‌صورت آنلاین و چه به‌صورت آفلاین هوشیاری لازم را مبنی بر اینکه در جزء آماج جرم هستند را ندارند (Qu et al., ۲۰۲٤:٥٤٥). درک خطر جرائم سایبری تابعی از سطح دانش سایبری کاربران، تجربه‌های پیشین، نوع استفاده از فناوری، و زمینه اجتماعی فرهنگی است؛ لذا، مداخلات پیشگیرانه برای تسهیل استفاده از اقدامات حفاظتی و مقابله‌ای باید باهدف تأثیرگذاری بر ادراک خطر در جهت کاهش خطر بزه‌دیدگی سایبری تمرکز داشته باشد (THES,۲۰۲٥:۱). به‌ویژه آنکه، در محیط های اجتماعی و فرهنگی که هنجارهای اجتماعی و شرایط شخصی نقش مهمی در شکل دهی تجربیات بزه دیدگی دارند(شاهپوری و بشیریه،۲۸۹:۱٤۰٤). بر پایه مبانی این نظریه، اقدامات پیشگیرانه کاربران تابعی از یک فرایند شناختی چندمرحله‌ای است؛ مانند شناسایی ریسک، ارزیابی شدت پیامدها، انتخاب راهبرد مناسب و اجرای اقدام حفاظتی است. در نتیجه، به جهت آنکه فضای دانشگاهی ترکیبی از تعاملات گسترده آنلاین، وابستگی شدید به شبکه‌های اجتماعی، و تبادل مداوم اطلاعات آموزشی و شخصی است، ضرورت دارد، دانشجویان به شکلی فعال ریسک‌های سایبری را مدیریت کنند تا از این رهگذر، خطر بزه‌دیدگی کمتر برخوردار شود.

۲-۲- نظریه فعالیت روز مره

[۳] Basler
[٤] Risk management theory

بر پایه این نظریه، افرادی که زمان بیشتری را در محیط‌های پر خطری مانند فضای مجازی سپری می‌کنند، احتمال بزه‌دیدگی آنان به دلیل الگوهای رفتار خاص در فضای مجازی افزایش می‌یابد. برای مثال، مطالعه موردی که بر روی نوجوانان کشور پرتغال صورت‌گرفته است، نشان می‌دهد، نوجوانانی که اطلاعات شخصی خود را در پروفایل شبکه‌های اجتماعی بارگذاری می‌کنند، بیشتر با افراد ناشناس قرار ملاقات حضوری می‌گذارند و والدینشان به دلیل عدم اطلاع از رفتارهای آنان، نظارتی کمتری بر روابط فرزندان خویش دارند و در نتیجه نوجوانان در معرض بزه‌دیدگی آنلاین بیشتری قرار می‌گیرند (Vale et al.,۲۰۲۲:٦٠٤). این یافته بع این دلیل است که وقوع جرم در شرایطی که بزهکار انگیزه‌مند، هدف مناسب و فقدان نگهبان مؤثر به‌صورت هم‌زمان تلاقی می‌کنند، افزایش می‌یابد (علیوردی نیا و علیمردانی،١٣٩٦:٤). برای مثال، بی‌احتیاطی در اشتراک‌گذاری اطلاعات شخصی، استفاده از رمزهای ساده، و کلیک بر پیوندهای ناشناس، مصداق بارزی از مناسب‌بودن هدف به شمار می‌رود. به‌ویژه آنکه بزه‌دیدگی سایبری تحت‌تأثیر مجموعه‌ای از عواملی مانند: سن، جنس، سطح سواد دیجیتال، میزان حضور در شبکه‌های اجتماعی به وجود می‌آید؛ لذا، توجه به نوع و سبک فعالیت کاربران در فضای مجازی، می‌تواند راهکارهایی مؤثر برای پیشگیری از بزه‌دیدگی سایبری در اختیار جامعه قرار دهد.

۲-۳-بزه‌دیدگی اولیه و ثانویه در بستر سایبری

بزه‌دیدگی یکی از مفاهیم اساسی در مطالعات جرم به شمار می‌رود که از قابلیت بررسی و تحلیل واکنش‌های پس از وقوع جرم و نحوه مواجهه بزه‌دیده در تداوم و تشدید پیامدهای بزه‌دیدگی برخوردار است. از این منظر، تمایز میان بزه‌دیدگی اولیه و ثانویه، چارچوب مناسبی برای تحلیل تجربه کاربران در محیط‌های آنلاین فراهم می‌کند؛ چرا که بزه‌دیدگی اولیه ناظر بر آسیب مستقیم ناشی از وقوع جرم است (آقایی،٧:١٤٠٠) ؛ در حالی که بزه‌دیدگی ثانویه به آسیب‌هایی اشاره دارد که بزه‌دیده در فرایند واکنش اجتماعی و نهادی پس از وقوع جرم تجربه می‌کند. این تفکیک در فضای سایبری اهمیت بیشتری می‌یابد؛ زیرا، بسیاری معتقدند که بزه دیدگان سایبری به علت شرایط خاص فضای سایبر نیازمند حمایت های بیشتری هستند (مالمیر و زررخ،۵۹:۱۳۸۹). ریشه این دیدگاه ناشی از ویژگی‌هایی همچون گستردگی مخاطبان، سرعت انتشار اطلاعات، ماندگاری محتوای دیجیتال و دشواری حذف کامل آثار جرم است که می‌تواند مرز میان آسیب اولیه و پیامدهای ثانویه را پیچیده‌تر کند. در تبیین و تحلیل این دوقسم از بزه دیدگی باید خاطر نشان ساخت که ، بزه‌دیدگی اولیه می‌تواند در نتیجه رفتارهایی مانند فیشینگ و کلاهبرداری اینترنتی، سرقت هویت و اطلاعات، نفوذ به حساب‌های کاربری، تهدید و اخاذی، آزار و مزاحمت آنلاین یا افشای غیرمجاز اطلاعات خصوصی ایجاد شود. در این وضعیت، کاربر به‌طور مستقیم متحمل خسارت مالی، نقض حریم خصوصی، آسیب به اعتبار، اضطراب و سایر پیامدهای ناشی از رفتار مجرمانه می‌شود. با وجود این، ماهیت شبکه‌ای فضای مجازی موجب می‌شود که آسیب واردشده در بسیاری از موارد پس از پایان رفتار مجرمانه نیز ادامه یابد. برای مثال، انتشار مجدد تصویر یا اطلاعات خصوصی، بازنشر محتوای مجرمانه یا واکنش‌های منفی سایر کاربران می‌تواند آسیب ناشی از بزه‌دیدگی اولیه را استمرار بخشیده و به تجربه‌ای ثانویه تبدیل کند.

بزه‌دیدگی ثانویه در محیط‌های آنلاین همچنین می‌تواند در نتیجه واکنش نامناسب کاربران، خانواده، پلتفرم‌های آنلاین یا نهادهای مسئول شکل گیرد. سرزنش قربانی، بی‌اعتنایی به گزارش بزه‌دیدگی، مقصر دانستن کاربر به دلیل اعتماد یا سهل‌انگاری، بازنشر محتوای مرتبط با جرم و ایجاد احساس بی‌اعتمادی یا انزوای اجتماعی، از جمله واکنش‌هایی هستند که می‌توانند آسیب ناشی از بزه‌دیدگی را تشدید کنند. از این منظر، کاربر ممکن است نه‌تنها از رفتار مجرمانه اولیه، بلکه از نحوه واکنش دیگران به تجربه بزه‌دیدگی نیز متضرر شود؛ بنابراین، در محیط‌های آنلاین، بزه‌دیدگی را باید فرایندی دانست که از وقوع کنش مجرمانه آغاز شده و بسته به واکنش‌های پس از آن می‌تواند تداوم و دامنه متفاوتی پیدا کند. این چارچوب نظری از منظر تبیین رفتارهای پیشگیرانه کاربران نیز اهمیت دارد. تجربه بزه‌دیدگی اولیه می‌تواند ادراک کاربران از خطرات فضای آنلاین را افزایش داده و آنان را به اتخاذ تدابیر احتیاطی بیشتر سوق دهد. کاربری که باتجربه مستقیم یک حمله سایبری مواجه شده است، ممکن است در ادامه استفاده از محیط‌های آنلاین، در حفاظت از اطلاعات شخصی، انتخاب گذرواژه، احراز هویت، پذیرش درخواست‌های ناشناس، کلیک بر پیوندهای مشکوک و تعامل با حساب‌های ناشناس محتاط‌تر عمل کند. به همین ترتیب، تجربه بزه‌دیدگی ثانویه می‌تواند نگرش کاربر نسبت به گزارش جرم، استفاده از سازوکارهای حمایتی و نحوه مواجهه با موقعیت‌های پرخطر را تحت‌تأثیر قرار دهد. بااین‌حال، عمده علل عدم گزارشی دهی جرم متأثر از نوع جرم ارتکابی و نحوه انجام آن است (نورپو و همکاران،۱۹۹:۱٤۰۰)

۲-٤- نظریه فضاهای بی‌دفاع

نظریه فضاهای بی‌دفاع باتکیه‌بر مفهوم «قابلیت نظارت‌پذیری» و «قابلیت کنترل اجتماعی محیط»، به تحلیل شرایط و مکان‌هایی می‌پردازد که به دلیل ضعف ساختاری یا فقدان سازوکارهای کنترلی، زمینه‌ساز بزه‌دیدگی به شمار می‌روند (صمد دوست و قمی،۱:۱٤۰۲). بر پایه این نظریه، با گسترش فضای دیجیتال، محیط‌های آنلاین همانند محیط فیزیکی می‌تواند دارای فضاهای «ایمن» و «بیدفاع» باشد. توضیح آنکه در محیط‌های آنلاین، فضاهای بی دفاع به صورت پروفایل‌های عمومی، گروه‌های ناشناس، کانال‌های بدون مدیریت، پیام‌رسان‌های نمود خارجی پیدا می‌کند. به همین دلیل، کاربران دانشگاهی ممکن است در معرض جرایم سایبری قرار گیرند و بزه دیده مزاحمت سایبری، سرقت هویت، کلاهبرداری، دسترسی غیرمجاز به اطلاعات یا انتشار بدافزار قرار گیرند. کاربرد این نظریه در پژوهش حاضر، بر این محور استوار است که بخش قابل توجهی از کاربران بدون آگاهی یا با اعتماد بیش از حد در محیط‌های آنلاین فعالیت می‌کنند و به همین دلیل، از پتانسیل بالایی برای بزه‌دیدگی برخوردار هستند. برای رفع این مشکل جاکوبز[۵] معتقد است که اهمیت دادن به طراحی و برنامه ریزی مناسب محیط می‌تواند منجر به کاهش فرصت های وقوع جرم و بهبود زندگی مردم شود(فرهادی،۱:۱۳۹۹). برپایه این استدلال هرچه فضای آنلاین از نظر ساختاری مانند وجود تنظیمات حریم خصوصی، کنترل کاربران، امکان گزارش تخلف، شفافیت مالکیت محتوا و حضور ناظران قابل کنترل‌تر باشد، احتمال بروز بزه‌دیدگی کاهش می‌یابد. در این چارچوب، ضعف آگاهی دانشجویان از معیارهای انتخاب فضای امن، حضور در گروه‌های عمومی، و کمبود

[۵] Jacobs

سازوکارهای نظارتی بر شبکه‌های دانشجویی همگی می‌توانند باعث شکل‌گیری فضاهای بی دفاع دیجیتال شوند که در نتیجه آن، جامعه شاهد افزایش بزه‌دیدگان سایبری خواهد بود.

۳ .روش تحقیق

پژوهش حاضر با رویکرد کمی و در قالب مطالعه‌ای توصیفی – تحلیلی و همبستگی به بررسی رابطه میان بزه‌دیدگی سایبری و رفتارهای پیشگیرانه کاربران در شبکه‌های اجتماعی پرداخته است. انتخاب روش پیمایشی به دلیل ماهیت ادراکی متغیرها و ضرورت گردآوری داده‌های میدانی از تجربیات واقعی کاربران انجام گرفت؛ روشی که در تحقیقات پیشین حوزه جرم‌شناسی سایبری نیز کارآمدی خود را در سنجش رفتارها و نگرش‌های امنیتی کاربران نشان داده است(Reyns,۲۰۱۱:۲۱٦). جامعه آماری پژوهش حاضر شامل تمامی دانشجویان مقطع کارشناسی و تحصیلات تکمیلی دانشگاه زابل در سال تحصیلی ۱۴۰۴-۱۴۰۳ است که طبق آمار رسمی، تعداد آنان ۵۰۰۰ نفر است. باتوجه‌به ماهیت پژوهش و عدم دسترسی به لیست دقیق دانشجویان دارای تجربه بزه‌دیدگی سایبری، از روش نمونه‌گیری غیراحتمالی (در دسترس) استفاده شد. جهت تعیین حجم نمونه موردنیاز، از فرمول کوکران برای جوامع محدود با سطح اطمینان ۹۵ درصد (Z= ۱,۱۹٦)، نسبت برآورد ویژگی (P=۰,۵) و خطای مجاز ۵ درصد استفاده گردید. باتوجه‌به این پارامترها، حجم نمونه آماری موردنیاز ۳۸۴ محاسبه شد. نمونه نهایی شامل دانشجویان رشته‌های مختلف دانشگاه زابل بود و برای افزایش تنوع نمونه، رشته‌ها در شش حوزه اصلی شامل علوم‌انسانی (حقوق، زبان و ادبیات فارسی، جغرافیای روستایی، تربیت‌بدنی و زبان و ادبیات عربی)، فنی و مهندسی(عمران، برق و مکانیک)، کشاورزی (زراعت، باغبانی، صنایع غذایی، گیاه پزشکی و اصلاح نباتات)، علوم (فیزیک ، شیمی و ریاضی)، دامپزشکی(بهداشت و مواد غذایی) و هنر و معماری(باستان شناسی، شهرسازی و هنر های نمایشی) طبقه‌بندی شدند. با این حال، با توجه به محدودیت‌های موجود در دسترسی به پاسخ‌دهندگان، حجم نمونه نهایی شامل ۱۶۲ پرسشنامه که از طریق روش در دسترس تکمیل شده بود، مورد تحلیل قرار گرفت. حجم نمونه مناسب است؛ چراکه در نمونه‌گیری هدفمند، نمونه‌گیری و جمع‌آوری داده‌ها تا زمانی ادامه می یابد که محقق با بینش و مفهومی جدیدی مواجه نگردد(رستگار آگاه،۱٤۰٤:۱٤۳).

ابزار گردآوری داده‌ها، پرسش‌نامه‌ای محقق ساخته بود که بر اساس چارچوب نظری پژوهش، گستره‌ای نظریات علمی پیرامون بزه‌دیدگی سایبری و اقدامات پیشگیرانه و یافته‌های تجربی پیشین در زمینه بزه‌دیدگی سایبری طراحی شد. این پرسش‌نامه متشکل از سه بخش اصلی است که عبارت‌اند از: نخست، ویژگی‌های جمعیت‌شناختی پاسخ‌دهندگان مانند سن، جنسیت و میزان استفاده روزانه از شبکه‌های اجتماعی؛ دوم، شاخص‌های بزه‌دیدگی سایبری شامل فیشینگ، نفوذ به‌حساب کاربری، مهندسی اجتماعی، سرقت اطلاعات و نقض حریم خصوصی؛ و سوم، شاخص‌های رفتارهای پیشگیرانه و تغییر رفتار امنیتی کاربران. گویه‌ها در قالب طیف لیکرت پنج‌درجه‌ای از «کاملاً مخالفم» تا «کاملاً موافقم» طراحی شده است. سپس، پرسش‌نامه در میان یک گروه اولیه از شرکت‌کنندگان (۵ نفر) مورد آزمون مقدماتی قرار گرفت، نتایج ،بررسی بازخورد آنان در پاسخ دهی در رفع ابهام از گویه های مبهم و کلی بسیار اثر گذار بود. به منظور سنجش میزان روایی، ابتدا گویه ها به تایید برخی از اساتید رشته حقوق رسانده،شده است. علاوه بر این، پایایی ابزار تحقیق از طریق ضریب آلفای کرونباخ ارزیابی شد که مقدار کلی آن برابر با ۰،۸۷ و برای خرده‌مقیاس‌ها

بین ۰٫۷۱ تا ۰٫۹۱ بود که نشان‌دهنده همسانی درونی مطلوب ابزار است. تحلیل داده‌ها با استفاده از نرم‌افزار (MATLAB R۲۰۲۳b)صورت گرفت. در مرحله نخست، شاخص‌های آمار توصیفی شامل میانگین، انحراف معیار، فراوانی و درصد برای توصیف ویژگی‌های جمعیت‌شناختی و توزیع متغیرها محاسبه شد. در مرحله دوم، برای آزمون فرضیه‌ها و تحلیل روابط بین متغیرها از آزمون همبستگی پیرسون و مدل رگرسیون چندگانه خطی استفاده شد. یافته‌ها نشان داد میان بزه‌دیدگی سایبری و تغییر رفتار کاربران رابطه مثبت و معناداری وجود دارد($r = ۰٫۸۵۲, \beta = ۱٫۵۱۹, R^2 = ۰٫۷۲۵, p < ۰٫۰۰۱$) در حالی که بین بزه‌دیدگی و رفتارهای پیشگیرانه رابطه‌ای منفی و معنادار مشاهده شد ($r = -۰٫۶۱۳, \beta = -۰٫۶۵۵, R^2 = ۰٫۳۷۶, p < ۰٫۰۰۱$). این الگوی دوگانه، ضمن تأیید تأثیر تجربه بزه‌دیدگی بر افزایش آگاهی امنیتی، بر وجود شکاف میان آگاهی و کنش پیشگیرانه کاربران نیز دلالت دارد.

٤- یافته‌ها

٤-١-آمار توصیفی

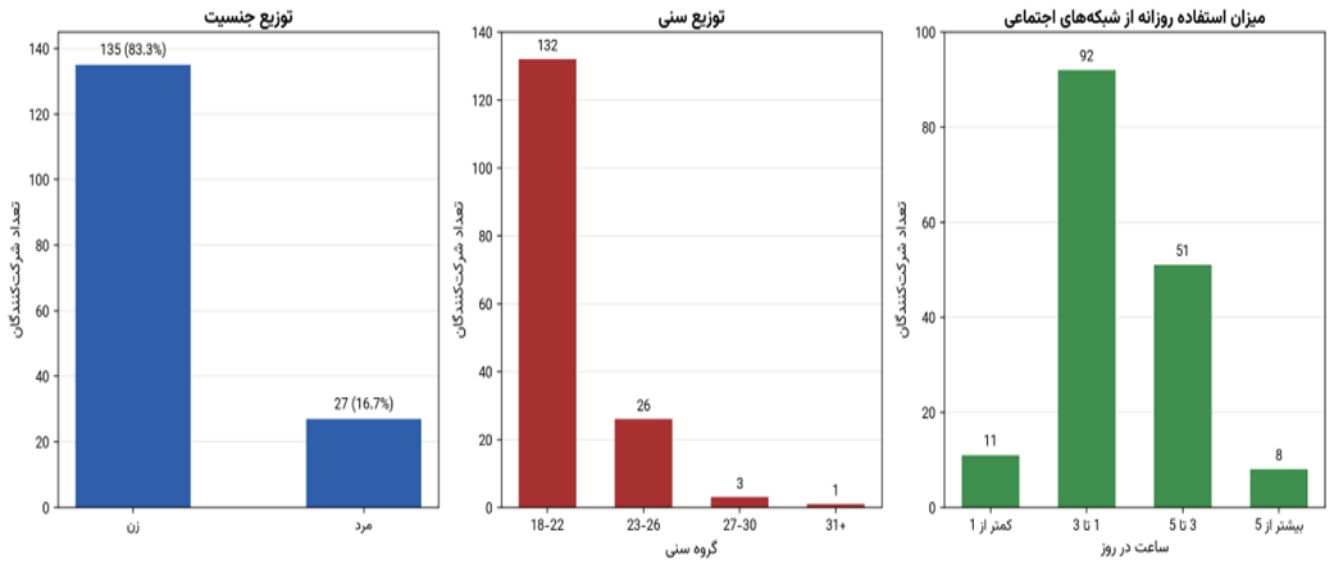
بر اساس داده‌های جدول (۱)، از میان ۱۶۲ نفر پاسخ‌دهنده، ۱۳۵ نفر (۸۳٫۳ درصد) زن و ۲۷ نفر (۱۶٫۳ درصد) مرد بوده‌اند. از نظر سنی، بیشترین فراوانی مربوط به گروه سنی ۱۸ تا ۲۲ سال با ۱۳۲نفر (۸۱٫۵ درصد) است که عمدتاً دانشجویان مقطع کارشناسی را شامل می‌شود. پس از آن، گروه سنی ۲۳ تا ۲۶ سال با ۶۱ نفر (۱۶ درصد) قرار دارد که غالباً در مقطع کارشناسی ارشد تحصیل می‌کنند. در نهایت، گروه‌های سنی ۲۷ تا ۳۰ سال و ۳۱ تا ۴۲ سال، به‌ترتیب با ۷ نفر (۱٫۹ درصد) و ۲ نفر (۰٫۶ درصد)، نمایانگر دانشجویان دکتری یا افرادی هستند که در مقاطع تحصیلات تکمیلی مشغول به فعالیت علمی یا آموزشی‌اند. این توزیع سنی و تحصیلی بیانگر آن است که اکثریت پاسخ‌دهندگان از قشر جوان و فعال دانشگاهی تشکیل شده‌اند؛ قشری که بیشترین حضور را در فضای مجازی دارد و از این رو، بررسی بزه‌دیدگی سایبری و رفتارهای پیشگیرانه در میان آنان از اهمیت ویژه‌ای برخوردار است.

جدول شماره ۱-توزیع ویژگی‌های جمعیت‌شناختی پاسخ‌دهندگان

متغیر	فراوانی	درصد
جنسیت		
زن	۱۳۵	%۸۳٫۳
مرد	۲۷	%۱۶٫۳
گروه سنی		

۲۲-۱۸ سال	۱۳۲	%۸۱/۱
۲۶-۲۳ سال	۲۶	%۱۶/۰
۳۰-۲۷ سال	۳	%۱,۹
۳۰+ سال	۱	%۰,۶
جمع	۱۶۲	%۱۰۰

مان‌طور که در شکل ۱ نشان داده شده است، توزیع سنی پاسخ‌دهندگان نیز تمرکز قابل توجهی در گروه سنی هجده تا بیست و دو سال دارد که سیصد و سیزده نفر معادل هشتاد و یک درصد و پنج دهم از کل نمونه را تشکیل می‌دهند. این یافته قابل انتظار است، زیرا اکثریت دانشجویان در مقاطع کارشناسی در این بازه سنی قرار دارند.

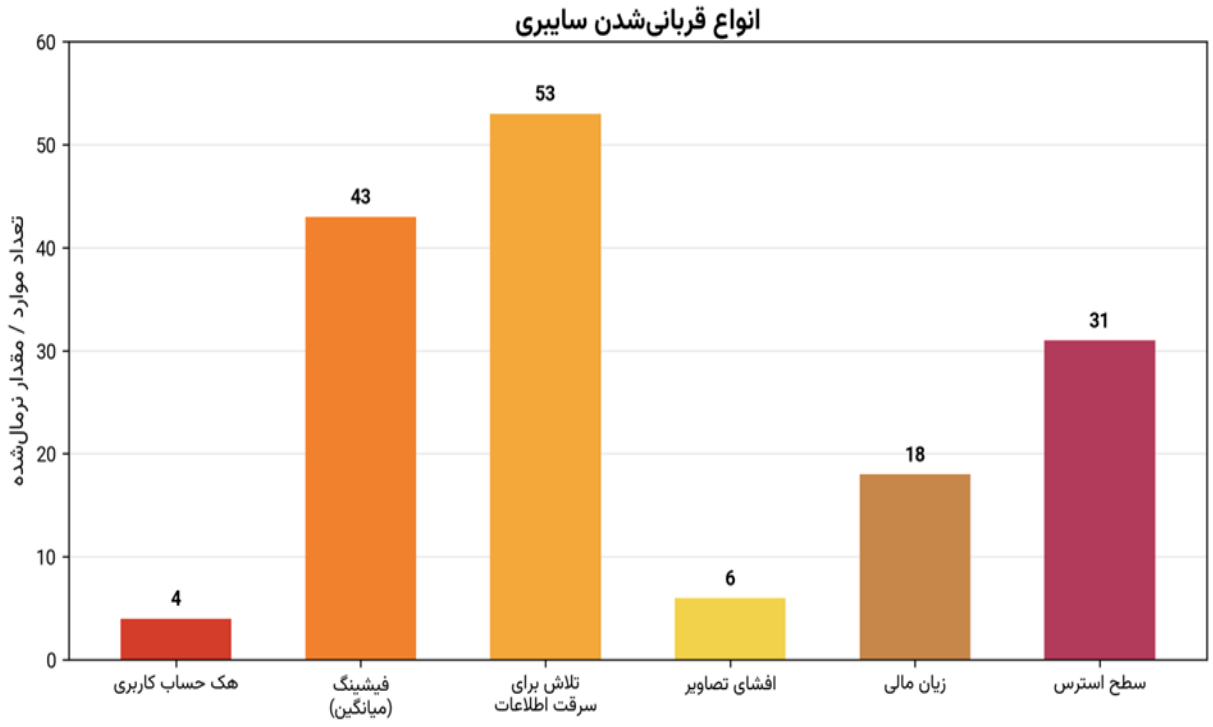


شکل ۱. توزیع فراوانی ویژگی‌های جمعیت‌شناختی پاسخ‌دهندگان: (الف) جنسیت؛ (ب) گروه‌های سنی؛ (ج) میزان استفاده روزانه از شبکه‌های اجتماعی (n=۱۶۲)

٤-۱-۱-فراوانی و اشکال بزه‌دیدگی سایبری

داده‌های منعکس شده در جدول شماره (۲) بیانگر آن است که بزه‌دیدگی سایبری در میان کاربران با شدت‌ها و الگوهای متفاوتی بروز یافته است.

اشکال بزه‌دیدگی	بله (نفر)	خیر (نفر)	درصد بزه‌دیدگی
نفوذ به‌حساب کاربری	٤	١٥٨	٪٢,٥
سرقت اطلاعات شخصی	٥٣	١٠٩	٪٣٢,٧
انتشار عکس خصوصی	٦	١٥٦	٪٣,٧
دریافت فیشینگ (حداقل ۱ بار)	٩٠	٧٢	٪٥٥,٦
خسارت مالی	١٦	١٤٦	٪٩,٩



شکل ۲. مقایسه فراوانی انواع بزه‌دیدگی سایبری در میان دانشجویان

شکل شماره (۲) مقایسه‌ی فراوانی انواع بزه‌دیدگی سایبری در میان دانشجویان را نشان می‌دهد. نتایج بیانگر آن است که دریافت فیشینگ (٪۵۵,۶) و سرقت اطلاعات شخصی (٪۳۲,۷) بیشترین شیوع را دارند، در حالی‌که نفوذ به حساب کاربری (٪۲,۵) و انتشار عکس خصوصی (٪۳,۷) کمترین میزان را نشان می‌دهند. این یافته‌ها حاکی از آن است که الگوی بزه‌دیدگی سایبری در میان دانشجویان بیشتر متکی بر فریب و مهندسی اجتماعی است تا نفوذ فنی مستقیم؛ موضوعی که اهمیت تقویت سواد دیجیتال و پیشگیری وضعی را در محیط‌های دانشگاهی برجسته می‌کند.

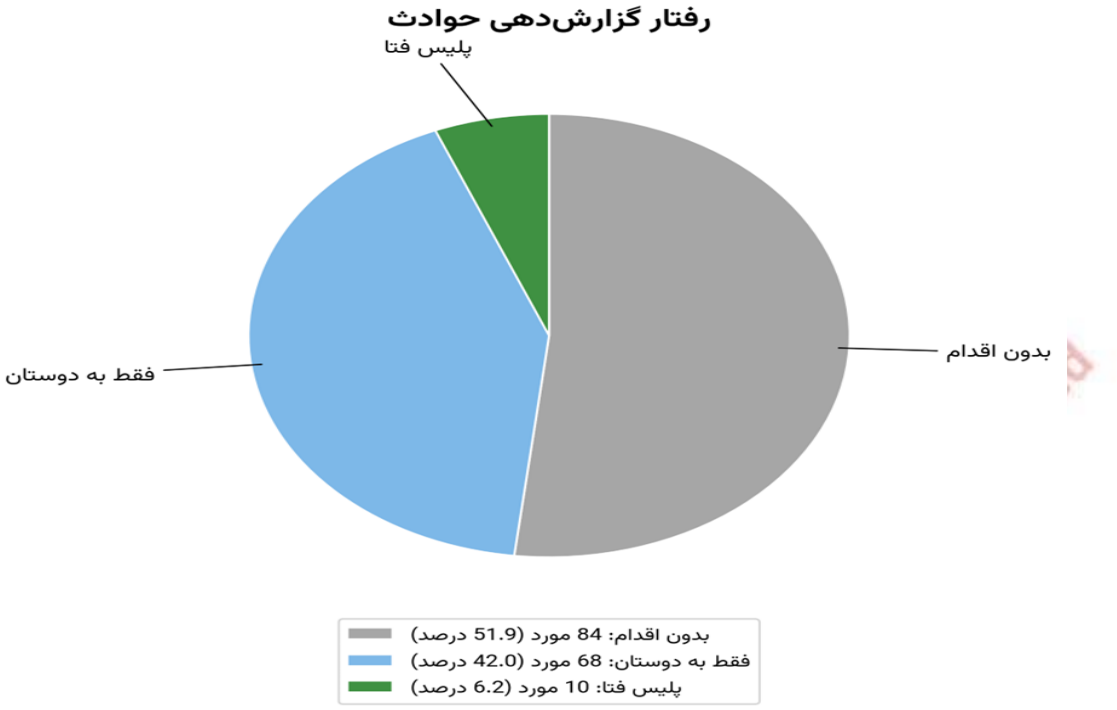
٤-١-٢- الگوهای واکنشی بزه‌دیدگان سایبری

یافته‌ها نشان می‌دهد که پس از بزه‌دیدگی سایبری، اکثریت پاسخ‌گویان (٪۵۱,۹) هیچ اقدامی برای پیگیری انجام نداده‌اند. ٪٤٢ تنها موضوع را با دوستان یا آشنایان در میان گذاشته‌اند و فقط ٪٦,٢ بزه‌دیدگی خود را به پلیس فضای مجازی گزارش کرده‌اند.

نوع واکنش بزه‌دیدگان سایبری	تعداد	درصد
هیچ اقدامی انجام نداده‌اند	٨٤	٪۵۱,۹
فقط به دوستان گفته‌اند	٦٨	٪٤٢
گزارش به پلیس فضای مجازی	١٠	٪٦,٢
جمع	١٦٢	٪١٠٠

جدول شماره (۳):توزیع فراوانی تعدیل کننده حمایتی از بزه دیدگان سایبری

این الگو نشان داد، تمایل به گزارش رسمی و پیگیری قانونی پایین است و بیشتر واکنش‌ها در سطح غیررسمی و شخصی باقی می‌ماند. چنین وضعیتی می‌تواند ناشی از بی‌اعتمادی به نهادهای رسمی، ترس از انگ اجتماعی یا ناآگاهی نسبت به مسیرهای قانونی پیگیری باشد و بر ضرورت ارتقای آگاهی کاربران و حمایت نهادی از بزه‌دیدگان سایبری تأکید می‌کند.



شکل ٦. نمودار دایره‌ای الگوی تعدیل کننده حمایتی از بزه دیدگان سایبری

همان‌طور که در شکل ٦ نمایش داده شده است، الگوی گزارش‌دهی پاسخ‌دهندگان نشان می‌دهد که اکثریت قابل توجه آنها اصلاً اقدامی برای گزارش رسمی واقعه انجام نداده‌اند یا تنها به دوستان و آشنایان خود در این باره سخن گفته‌اند.از میان یکصد و شصت و دو پاسخ‌دهنده، هشتاد و چهار نفر معادل (٥١,٩٪)به دلیل بی‌فایده دانستن گزارش‌دهی، هیچ اقدامی انجام نداده‌اند. این گروه معتقد بودند که گزارش‌دهی واقعه منجر به نتیجه مثبتی نخواهد شد یا اصلاً نمی‌دانستند چگونه و به کجا باید گزارش دهند.

٤-١-٣-توزیع فراوانی رشته تحصیلی با بزه‌دیدگی سایبری

به‌منظور بررسی ارتباط حوزه تحصیلی با بزه‌دیدگی، فراوانی دانشجویان بزه‌دیده در هر یک از شش حوزه تحصیلی نیز محاسبه شد.

دانشکده	رشته تحصیلی	کل دانشجویان	بزه‌دیده	درصد
ادبیات و علوم‌انسانی	حقوق، زبان و ادبیات فارسی، جغرافیای روستایی، تربیت‌بدنی و زبان و ادبیات عربی	۳۸	۱۹	٪۵۰
فنی و مهندسی	عمران، برق و مکانیک	۳۱	۱۳	٪٤١/٩

کشاورزی	زراعت، باغبانی، صنایع غذایی، گیاه‌پزشکی و اصلاح نباتات	۳۵	۱۶	٪۴۵/۷
علوم	فیزیک، شیمی و ریاضی	۲۵	۱۰	٪۴۰
دامپزشکی	بهداشت و مواد غذایی	۱۸	۷	٪۳۸/۹
هنر و معماری	باستان‌شناسی، شهرسازی و هنرهای نمایشی	۱۵	۶	٪۴۰
	جمع	۱۶۲	٪۴۳/۸	

جدول شماره: توزیع فراوانی رشته تحصیلی با بزه‌دیدگی سایبری

بر اساس یافته‌های توصیفی، بیشترین میزان بزه‌دیدگی در میان دانشجویان علوم‌انسانی با ۵۰ درصد مشاهده شد. پس از آن، دانشجویان رشته‌های کشاورزی با ۷/۴۵ درصد و رشته‌های فنی و مهندسی با ۴۱/۹ درصد قرار داشتند. کمترین میزان بزه‌دیدگی مربوط به دانشجویان دامپزشکی با ۳۸/۹ درصد بود.

۴-۲- یافته های استنباطی

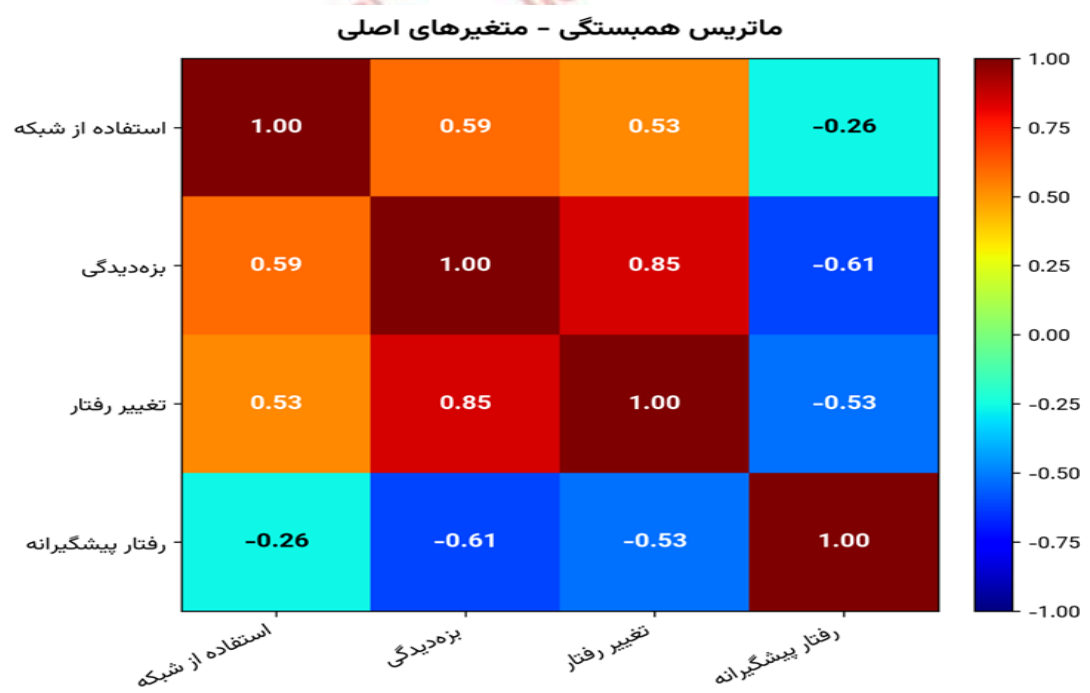
۴-۲-۱-ماتریس همبستگی

همان‌طور که در جدول شماره (۵)،یافته‌های همبستگی پیرسون مشاهده می شود؛ بین بزه‌دیدگی سایبری و استفاده از شبکه رابطه مثبت و معناداری وجود دارد ($r = ۰,۵۸۶, p < ۰,۰۱$)، به‌طوری که افزایش میزان استفاده از شبکه با افزایش احتمال بزه‌دیدگی همراه است. علاوه بر این، بزه‌دیدگی سایبری با تغییر رفتار نیز رابطه مثبت و قوی دارد ($r = ۰,۸۵۲, p < ۰,۰۱$)، که نشان می‌دهد افرادی که تجربه بزه‌دیدگی بیشتری دارند، تمایل بیشتری به تغییر رفتار از خود نشان می‌دهند. در مقابل، روابط بزه‌دیدگی سایبری با رفتارهای پیشگیرانه ($r = -۰,۶۱۳, p < ۰,۰۱$) و تغییر رفتار با رفتارهای پیشگیرانه ($r = -۰,۵۳۲, p < ۰,۰۱$) منفی و معنادار بود؛ این امر بیانگر آن است که افزایش بزه‌دیدگی و تغییر رفتار با کاهش سطح رفتارهای پیشگیرانه همراه است. همچنین، استفاده از شبکه نیز با رفتارهای پیشگیرانه رابطه منفی و معناداری نشان داد ($r = -۰,۲۵۶, p < ۰,۰۱$). نتایج کلی حاکی از آن است که بزه‌دیدگی سایبری نه تنها با افزایش تغییر رفتار مرتبط است، بلکه با کاهش رفتارهای پیشگیرانه کاربران در مواجهه با تهدیدات سایبری نیز همراه می‌باشد، و افزایش میزان استفاده از شبکه می‌تواند خطر بزه‌دیدگی سایبری را تشدید کند و به کاهش اقدامات پیشگیرانه کاربران منجر شود.

جدول ۵. ماتریس همبستگی پیرسون بین متغیرهای اصلی پژوهش

متغیر	استفاده از شبکه	بزه‌دیدگی	تغییر رفتار	رفتار پیشگیرانه
استفاده از شبکه	۱,۰۰۰	۰,۵۶۸	۰,۵۳۳	−۰,۲۵۶
بزه‌دیدگی	۰,۵۶۸	۱,۰۰۰	۰,۵۸۲	−۰,۶۱۳
تغییر رفتار	۰,۵۳۳	۰,۵۸۲	۱,۰۰۰	−۰,۵۳۲
رفتار پیشگیرانه	−۰,۲۵۶	−۰,۶۱۳	−۰,۵۳۲	۱,۰۰۰

همان‌طور که در شکل (٤) مشاهده می شود:رنگ قرمز نشان‌دهنده همبستگی مثبت و رنگ آبی نشان‌دهنده همبستگی منفی است.



شکل ٤. نقشه حرارتی ماتریس همبستگی پیرسون بین متغیرهای اصلی پژوهش

همان‌طور که مشاهده می‌شود، نتایج ماتریس همبستگی متغیرهای اصلی پژوهش تصویری روشن از نحوه تعامل سازه‌های مرتبط با بزه‌دیدگی سایبری و رفتار کاربران در محیط‌های آنلاین ارائه می‌دهد. در این ماتریس، شدت و جهت روابط از طریق تلفیقی از ضرایب همبستگی و طیف‌های رنگی نمایش‌داده‌شده است؛ به‌گونه‌ای که رنگ‌های قرمز تیره بیانگر همبستگی‌های قوی و مثبت، رنگ‌های نارنجی تا قرمز روشن نشان‌دهنده همبستگی‌های متوسط و مثبت و طیف‌های آبی روشن تا آبی تیره معرف همبستگی‌های منفی میان متغیرها هستند. بر اساس داده‌ها، قوی‌ترین همبستگی مثبت میان متغیر بزه‌دیدگی سایبری و تغییر رفتار کاربران با مقدار ۰,۸۵ مشاهده شد که با رنگ قرمز تیره مشخص شده است. این نتیجه بیانگر آن است که افزایش تجربه بزه‌دیدگی سایبری، با احتمال بالاتری به بروز تغییرات رفتاری در کاربران منجر می‌شود. علاوه بر این، متغیر استفاده از شبکه با بزه‌دیدگی سایبری (۰,۵۹) و با تغییر رفتار (۰,۵۳) دارای همبستگی مثبت متوسط بوده و در نمودار با رنگ‌های نارنجی و نارنجی متمایل به قرمزنمایش یافته است. این یافته‌ها نشان می‌دهد افزایش میزان حضور در شبکه‌های اجتماعی، افراد را در معرض خطرات بیشتر قرار می‌دهد و به تبع آن احتمال تغییر در الگوهای رفتاری آنان نیز افزایش می‌یابد.در مقابل، متغیر رفتارهای پیشگیرانه با سایر متغیرها دارای همبستگی منفی است؛ موضوعی که با طیف‌های آبی روشن تا آبی تیره مشخص شده است. همبستگی منفی نسبتاً قوی این متغیر با بزه‌دیدگی سایبری (۰,٦۱–) و با تغییر رفتار (۰,۵۳–) نشان می‌دهد که اتخاذ رفتارهای پیشگیرانه می‌تواند نقش مؤثری در کاهش بزه‌دیدگی و پیامدهای رفتاری آن داشته باشد. همچنین رابطه منفی ضعیف‌تر میان استفاده از شبکه و رفتارهای پیشگیرانه (۰,۲٦–) که با رنگ آبی روشن نمایش یافت، بیانگر آن است که کاربرانی که زمان بیشتری را صرف فعالیت آنلاین می‌کنند، کمتر به رفتارهای پیشگیرانه توجه نشان می‌دهند.

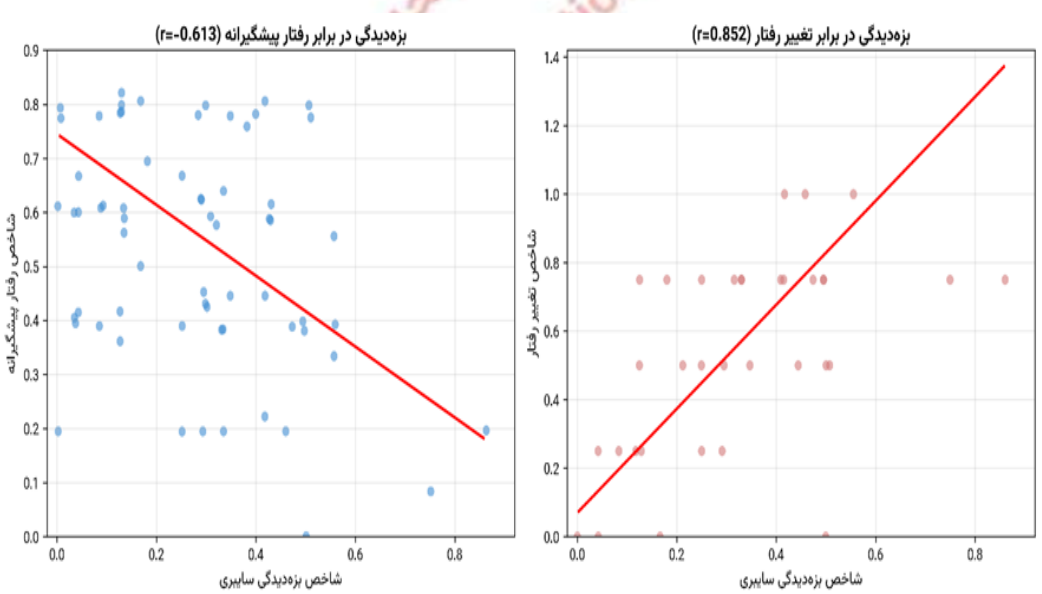
٤-۲-۲- تحلیل رگرسیون خطی

به‌منظور بررسی تأثیر بزه‌دیدگی سایبری و تغییر رفتار بر رفتارهای پیشگیرانه کاربران و نیز تحلیل نقش بزه‌دیدگی در تغییر رفتار، سه مدل رگرسیونی اجرا شد. نتایج این مدل‌ها در جدول مربوطه ارائه شده است.

جدول ٦. خلاصه نتایج مدل‌های رگرسیون

مدل	متغیر وابسته	متغیر مستقل	ضریب β	R^2	p-value
۱	رفتار پیشگیرانه	بزه‌دیدگی	-۰,٦۵۵	۰,۳۷٦	<۰,۰۰۱
۲	تغیر رفتار	بزه‌دیدگی	۱,۵۱۹	۰,۷۲۵	<۰,۰۰۱
۳	رفتار پیشگیرانه	بزه‌دیدگی + تغیر رفتار	-۰,٦۲۲ -۰,۰۲۲	۰,۳۷٦	<۰,۰۰۱

در مدل اول، اثر بزه‌دیدگی سایبری بر رفتارهای پیشگیرانه مورد بررسی قرار گرفت. ضریب بتای استانداردشده برابر $\beta = -۰,۶۵۵$ به‌دست آمد که نشان‌دهنده رابطه منفی میان دو متغیر است. مقدار $R^2 = ۰,۳۷۶$ بیانگر آن است که بزه‌دیدگی حدود ۳۷,۶ درصد از واریانس رفتارهای پیشگیرانه را تبیین می‌کند. مقدار $p < ۰,۰۰۱$ نیز معناداری این مدل را تأیید می‌کند. در مدل دوم، تأثیر بزه‌دیدگی سایبری بر تغییر رفتار کاربران بررسی شد. ضریب بتای استانداردشده $\beta = ۱,۵۱۹$ حاکی از وجود رابطه مثبت و عمده میان بزه‌دیدگی و تغییر رفتار است. مقدار $R^2 = ۰,۷۲۵$ نشان می‌دهد که بزه‌دیدگی ۷۲,۵ درصد از تغییر رفتار کاربران را تبیین می‌کند. این مدل نیز از نظر آماری معنادار بوده و مقدار $p < ۰,۰۰۱$ این موضوع را تأیید می‌کند. در مدل سوم، متغیرهای بزه‌دیدگی سایبری و تغییر رفتار به‌صورت همزمان برای پیش‌بینی رفتارهای پیشگیرانه وارد مدل شدند. ضرایب بتای استانداردشده برای بزه‌دیدگی $\beta = -۰,۶۲۲$ و برای تغییر رفتار $\beta = -۰,۰۲۲$ گزارش شد. هرچند هر دو ضریب منفی هستند، اما مقدار $R^2 = ۰,۳۷۶$ نشان می‌دهد که این مدل، مشابه مدل اول، ۳۷,۶ درصد از واریانس رفتارهای پیشگیرانه را تبیین می‌کند. معناداری کلی مدل نیز با $p < ۰,۰۰۱$ تأیید می‌شود. در ادامه شکل ۵ رابطه میان بزه‌دیدگی سایبری و دو متغیر رفتارهای پیشگیرانه و تغییر رفتار کاربران را به‌صورت نمودار پراکنش به همراه خط رگرسیون نمایش می‌دهد. این نمودارها امکان مشاهده الگوی کلی داده‌ها و جهت و شدت ارتباط بین متغیرها را فراهم می‌سازند



شکل ۵. نمودارهای پراکنش و خطوط رگرسیون

همان‌طور که در شکل شماره (۵) مشاهده می شود، در قسمت (الف) شکل ۵، رابطه میان بزه‌دیدگی سایبری و رفتارهای پیشگیرانه ترسیم شده است. همان‌گونه که مشاهده می‌شود، نقاط پراکنش الگوی نزولی دارند و خط رگرسیون نیز شیب منفی را نشان می‌دهد.

مقدار همبستگی (r=-۰,٦۱۳) مؤید وجود یک رابطه منفی و نسبتاً قوی میان دو متغیر است؛ به‌طوری‌که با افزایش بزه‌دیدگی سایبری، میزان رفتارهای پیشگیرانه کاهش می‌یابد. این الگو با نتایج رگرسیون گزارش‌شده در جدول نیز همخوانی دارد.در قسمت (ب) شکل ۵، رابطه میان بزه‌دیدگی سایبری و تغییر رفتار کاربران نمایش داده شده است. در این نمودار، پراکنش داده‌ها روندی صعودی را نشان می‌دهد و خط رگرسیون نیز دارای شیب مثبت است. همبستگی (r=۰,۸۵۲) بیانگر وجود رابطه مثبت و بسیار قوی میان دو متغیر است؛ بدین معنا که افزایش بزه‌دیدگی با افزایش تغییر رفتار همراه بوده است. این رابطه نیز با نتایج تحلیل رگرسیون ارائه‌شده در بخش قبلی مطابقت دارد.

۵- بحث

این پژوهش به بررسی رابطه بزه‌دیدگی سایبری و رفتارهای پیشگیرانه کاربران در محیط‌های آنلاین در میان دانشجویان دانشگاه زابل پرداخته است. بر اساس یافته‌های حاصل از این پژوهش، جامعه هدف سطوح مختلفی از بزه‌دیدگی سایبری را گزارش کرده‌اند. در ادامه، سطوح بزه‌دیدگی و واکنش‌های صورت‌گرفته از منظر دانش پیشگیری از جرم مورد بحث قرار می‌گیرد.

۵-۱- فضای آنلاین و سطوح بزه دیدگی

یافته‌های پژوهش حاضر نشان می‌دهد که دانشجویان دانشگاه زابل در معرض سطوح مختلفی از بزه‌دیدگی سایبری قرار دارند، به‌ویژه در حوزه فیشینگ و سرقت اطلاعات شخصی. بروز ۵۵,٦ درصدی فیشینگ و ۳۲,۷ درصدی سرقت اطلاعات نشان می‌دهد که پرخطرترین تهدیدهای سایبری، تهدیدهایی‌اند که از طریق پیام‌ها، لینک‌ها و تعاملات روزمره در شبکه‌های اجتماعی رخ می‌دهند. این نتیجه با یافته‌های فارل و امدرو (۲۰۱۸) هم‌خوان است؛ آنان نیز گزارش کرده‌اند که افزایش روش‌های فریب آنلاین و پیام‌های جعلی، رایج‌ترین شکل بزه‌دیدگی کاربران است و بخش بزرگی از مخاطبان حداقل یک‌بار تجربه فیشینگ داشته‌اند. ازسوی‌دیگر درصد پایین نفوذ به‌حساب کاربری (۲,۵ درصد) و انتشار تصاویر خصوصی (۳,۷ درصد) با یافته‌های علیوردنیا و سیاهکل رودی (۱۳۹۸) تفاوت‌هایی دارد. آنان گزارش کرده‌اند که آزاررسانی تصویری و تعرض به حریم خصوصی در میان دانشجویان مازندران به‌ویژه برای دختران شایع‌تر است. این تفاوت می‌تواند ناشی از تفاوت‌های فرهنگی و الگوهای استفاده از شبکه‌های اجتماعی در دو استان باشد یا اینکه دانشجویان زابل در انتشار تصاویر شخصی محتاط‌تر عمل می‌کنند.

۵-۱- پیوند حضور در محیط های آنلاین با بزه‌دیدگی

یافته‌های پژوهش نشان داد که رابطه‌ای مثبت و نسبتاً قوی میان میزان استفاده از شبکه‌های اجتماعی و بزه‌دیدگی سایبری وجود دارد (r = ۰,٥٦۸). در تبیین چرایی ایجاد این رابطه بر پایه نظریات جرم‌شناسی به نظر می‌رسد، از منظر نظریه فعالیت روزمره، افزایش حضور کاربران در فضای آنلاین، آنان را به هدف مناسبی برای بزهکاران فضای سایبری در غیاب مراقب و ناظر مؤثر مبدل می‌سازد. این یافته ها همسو با مطالعات باسلر و همکاران (۲۰۱۲) و میچل و همکاران (۲۰۱۱) است که نشان می‌دهد، حضور بیشتر در فضای

آنلاین می‌تواند خطر بزه‌دیدگی سایبری را افزایش دهد. علاوه بر این، به نظر می‌رسد از منظر نظریه یادگیری اجتماعی، محیط‌های آنلاینی که در آن رفتارهای بزهکارانه (مانند فریب، آزار سایبری یا سرقت داده) صورت می‌گیرد، بستر را برای تشویق و عادی‌سازی تکرار الگوهای مجرمانه را فراهم می‌آورد. براین‌اساس، با افزایش حضور در بستر فضای مجازی، خطر بزه‌دیدگی نیز افزایش می‌یابد(فرامرزیانی و همکاران،۹:۱٤۰۳). زیرا، کاربران پرمصرف بیش از دیگران در معرض گروه‌ها یا الگوهای مجرمانه قرار می‌گیرند و در نتیجه احتمال بزه‌دیدگی‌شان افزایش می‌یابد. بعلاوه، از منظر نظریه انتخاب عقلانی جرم، تلفیق و ترکیب منافع و فرصت های جرم که مانند پیچ و مهره عمل می‌کنند(علیوردی نیا و صالح نژاد،۱۲:۱۳۹۲)، باعث می شود مجرمان فضای سایبری به‌طور منطقی اهدافی را انتخاب کنند که بیشترین حضور، بیشترین اطلاعات قابل دسترس و کمترین سطح محافظت را دارند. بنابراین، سبک زندگی دیجیتال و نحوه استفاده از شبکه‌های اجتماعی نه‌تنها یک متغیر فردی بلکه یک عامل جرم‌شناختی ساختاری است که به‌صورت مستقیم احتمال بزه‌دیدگی سایبری را افزایش می‌دهد.

۵-۲- بزه‌دیدگی سایبری و الگوهای رفتاری پیشگیرانه

از منظر پیشگیری از جرم، تحلیل الگوهای رفتار و روانی بزه‌دیدگان یکی از متغیرهای مهم جهت سنجش و اتخاذ سیاست‌گذاری‌های مناسب برای تدوین برنامه‌های پیشگیرانه از جرم به شمار می‌رود. در همین راستا، نوع واکنش و ایجاد حساسیت بزه‌دیدگان در جرائم سایبری می‌تواند، جهت‌دهی مناسبی برای تدابیر پیشگیرانه از جرم فراهم سازد. در این مطالعه، نتایج رگرسیون نشان داد که به دنبال بزه‌دیدگی سایبری، کاربران آنلاین الگوهای رفتاری خود را در این محیط‌های تغییر داده‌اند (β = ۱,۵۱۹, R^2 = ۰,۷۲۵). توضیح آنکه بر اساس، تحلیل آماری گویه‌های پاسخ داده شده توسط مشارکت‌کنندگان، کاربران پس از تجربه تهدید یا خسارت، الگوی استفاده خود را تغییر می‌دهند و در استفاده از فضای مجازی تلاش می‌کنند تا اقدامات احتیاطی بیشتری را صورت دهند. برای نمونه، یافته‌ها نشان داد که کاربران نسبت به لینک‌ها یا پیام‌های مشکوک پس از تجربه بزه‌دیدگی حساسیت بیشتری از خود نشان داده‌اند. این یافته کاملاً با نتایج فارل و امدرو (۲۰۱۸) همسو است؛ آنان نیز گزارش کردند که تجربه شخصی بزه‌دیدگی قوی‌ترین محرک برای تغییر سبک استفاده و افزایش رفتارهای محافظتی است. باتوجه‌به تغییر الگوهای رفتاری که بزه‌دیدگان سایبری از خود نشان می‌دهند، به نظر می‌رسد، نقش و تأثیر آموزش در حوزه پیشگیری از جرم از اهمیت فراوان برخوردار است. چرا که جلوگیری از تکرار بزه‌دیدگی سایبری، از رهگذر توانمندسازی مبتنی بر آموزش امنیت سایبری و آموزش سواد دیجیتال می‌تواند، اثری چشمگیری در پیشگیری از تکرار این جرائم به دنبال داشته باشد (کمارعلیا و همکاران،۷۳:۱٤۰٤). باوجود این، نتایج پژوهش حاضر حاکی از آن بود که بزه‌دیدگی به‌تنهایی تأثیری منفی بر رفتارهای پیشگیرانه دارد (β = -۰,٦٥٥). این مهم همسو با نتایج مطالعات جامی‌پور و همکاران (۱۳۸۹) است که نشان می‌دهند بخش قابل‌توجهی از قربانیان، به دلیل ضعف آگاهی و مهارت‌های سایبری، حتی پس از تجربه بزه نیز قادر به اتخاذ اقدامات حفاظتی مؤثر نیستند. ازاین‌رو، می‌توان استنباط کرد که دانش امنیتی ناکافی در میان کاربران دانشگاه زابل مانع از تبدیل تجربه بزه‌دیدگی به رفتارهای پیشگیرانهٔ مؤثر شده است.

۵-٤- تعدیل کننده حمایتی و بزه‌دیدگی سایبری

تعدیل‌کننده حمایتی، یکی از رویکردهای نوین و مؤثر در مقابله با بزه‌دیدگی سایبری به شمار می‌رود. به‌واقع، تعدیل‌کننده حمایتی فرایندی است که در آن نهادهای حمایتی مانند همسالان، خانواده، مدرسه، دانشگاه و نظایر آن از طریق گفتگو و تعامل سازنده به بزه‌دیده سایبری کمک می‌کند تا آسیب روانی و اجتماعی ناشی از بزه‌دیدگی را کاهش دهد. این فرایند مبتنی بر ایجاد فضایی امن برای بیان تجربه‌ها و احساسات، تقویت توانمندی‌های فردی قربانی و یافتن راهکارهای عملی برای مدیریت پیامدهای بزه‌دیدگی سایبری است. در همین راستا، یافته‌های پژوهش نشان می‌دهد که بیشتر قربانیان جرائم سایبری از نقش‌های واسطه‌ای و تعدیل‌کننده حمایت اجتماعی برای کاهش پیامدهای بزه‌دیدگی سایبری استفاده نمی‌کنند. به‌طوری که تنها، ٤٢٪ تجربه خود را به دوستان اطلاع داده‌اند و تنها ٦,٢٪ اقدام به گزارش رسمی به پلیس فضای مجازی کرده‌اند. این امر می‌تواند ناشی از شرم، ترس، بی‌اطلاعی و فقدان اعتماد باشد که در نتیجه آن درصد کمی از قربانیان از حمایت اجتماعی یا کانال‌های رسمی استفاده می‌کنند. این رفتار بازتاب نوعی از بزه‌دیدگی ثانویه است که بزه‌دیده برای پیشگیری از پیامدهای ثانویه، رفتار منفعلانه از خود نشان می‌دهد؛ بنابراین، باتوجه‌به پیچیدگی و ویژگی‌های منحصربه‌فرد بزه‌دیدگی سایبری، توجه به نقش تعدیل‌کننده‌های حمایتی نیازمند رویکردی چندبعدی شامل حمایت روان‌شناختی، مشاوره حقوقی و آموزش مهارت‌های دیجیتال است. مطالعات نشان می‌دهد که نقش‌های واسطه‌ای و تعدیل‌کننده حمایت اجتماعی (همسالان، خانواده) و تجربیات جو مدرسه (احساس امنیت و مراقبت دانش‌آموزان در محیط مدرسه) از اهمیت بسزایی در کاهش پیامدهای منفی بزه‌دیدگی سایبری برخوردار است (Holfeld, & Baitz,۲۰۲۰:۲۲۱٤)؛ بنابراین، توجه به نقش تعدیل‌کننده‌های حمایتی می‌تواند در کاهش استرس و اضطراب قربانی، ارتقای آگاهی و دانش حقوقی و دیجیتال، و بازسازی اعتماد اجتماعی آنان به‌ویژه در محیط‌های دانشگاهی نقش مؤثری ایفا نماید. بااین‌حال، تحقق این رویکرد، مستلزم فراهم‌کردن آموزش‌های لازم و حمایت روان‌شناختی، توانمندسازی آنان در مواجهه با تهدیدات سایبری است.

۵-۵-مهارت کم سایبری

نتایج پژوهش نشان می‌دهد که ضعف در رفتارهای پیشگیرانه و تمایل غالب کاربران به «واکنش پس از آسیب»، بیانگر کمبود آمادگی در حوزه شناخت تهدیدها و اتخاذ اقدامات حفاظتی است. به عبارتی دیگر، دانشجویان موردمطالعه به دلیل سواد سایبری محدود در حوزه امنیت دیجیتال، قادر به پیش‌بینی و مدیریت تهدیدهای سایبری نیستند. این یافته با شواهد تحقیقات، جامی‌پور و همکاران (۱۳۹۹) که نشان داده‌اند، فقدان مهارت‌های سایبری در نوجوانان و جوانان، یکی از مهم‌ترین عوامل افزایش بزه‌دیدگی سایبری است، همخوانی دارد. همچنین، باسلر و همکاران (۲۰۱۲) نیز تأکید کرده‌اند که افشای اطلاعات شخصی و ناآگاهی امنیتی از مهم‌ترین عوامل قربانی شدن کاربران جوان در فضای مجازی محسوب می‌شود. باتوجه‌به این شواهد، می‌توان گفت وضعیت دانشجویان دانشگاه زابل در واقع بخشی از یک الگوی جهانی است که در آن کاربران جوان به دلیل کمبود مهارت‌های حفاظتی و دانش امنیتی، آسیب‌پذیرتر از سایر گروه‌ها هستند. این مسئله نشان می‌دهد که فقدان سواد سایبری نه‌تنها شانس قربانی شدن را افزایش می‌دهد،

بلکه مانع بهره‌برداری ایمن از فرصت‌های فضای مجازی نیز می‌شود؛ بنابراین، نتایج این پژوهش اهمیت توسعه و تقویت سواد سایبری در حوزه امنیت دیجیتال را برجسته می‌کند. آموزش مهارت‌هایی مانند شناسایی تهدیدات، حفاظت از اطلاعات شخصی، و استفاده ایمن از ابزارهای دیجیتال می‌تواند به کاهش آسیب‌پذیری و افزایش توانمندی کاربران جوان در مقابله با جرائم سایبری کمک کند.

نتیجه‌گیری

یافته‌های پژوهش نشان داد که بزه‌دیدگی سایبری در میان دانشجویان، پدیده‌ای چندوجهی است که هم در سطح مواجهه مستقیم با کنش مجرمانه و هم در سطح پیامدهای پس از آن قابل‌تحلیل است. غلبه مواردی همچون دریافت پیام‌ها و لینک‌های تقلبی (۶/۵۵ درصد) و سرقت داده‌های شخصی (۷/۳۲ درصد) بیانگر آن است که بخش مهمی از بزه‌دیدگی تجربه‌شده توسط کاربران، در قالب بزه‌دیدگی اولیه تحقق می‌یابد؛ یعنی کاربر مستقیماً در معرض رفتار مجرمانه قرار گرفته و از آن متحمل آسیب می‌شود. در این سطح، یافته مربوط به رابطه معنادار میان میزان حضور در شبکه‌های اجتماعی و بزه‌دیدگی سایبری اهمیت ویژه‌ای دارد. افزایش حضور در شبکه‌های اجتماعی، فرصت مواجهه با پیام‌های جعلی، پیوندهای آلوده، حساب‌های ناشناس و سایر موقعیت‌های جرم‌زا را افزایش می‌دهد و در نتیجه، احتمال قرارگرفتن کاربر در موقعیت بزه‌دیدگی اولیه بیشتر می‌شود؛ بنابراین، یافته‌های پژوهش از این برداشت حمایت می‌کند که در محیط آنلاین، میزان و الگوی حضور کاربر می‌تواند در ایجاد فرصت بزه‌دیدگی نقش داشته باشد. بااین‌حال، بزه‌دیدگی سایبری در سطح آسیب مستقیم متوقف نمی‌شود. ویژگی محیط آنلاین موجب می‌شود آثار و تبعات جرم بتواند پس از وقوع کنش مجرمانه نیز استمرار یابد. در اینجا مفهوم بزه‌دیدگی ثانویه برای تبیین بخش دیگری از تجربه کاربران اهمیت پیدا می‌کند. هنگامی که کاربر پس از وقوع جرم با پیامدهایی نظیر تداوم انتشار یا سوءاستفاده از اطلاعات، خدشه به حریم خصوصی، احساس ناامنی، بی‌اعتمادی به محیط آنلاین، دشواری در گزارش جرم یا واکنش نامناسب دیگران مواجه می‌شود، آسیب تجربه‌شده دیگر صرفاً ناشی از کنش اولیه مجرم نیست، بلکه به فرایند پس از بزه‌دیدگی نیز مربوط می‌شود. از این منظر، فضای سایبری به دلیل قابلیت بازتولید و انتشار مجدد اطلاعات، امکان امتدادیافتن آسیب اولیه و تبدیل آن به تجربه‌ای مستمر را فراهم می‌کند؛ بنابراین، تحلیل بزه‌دیدگی سایبری بدون توجه به پیامدهای ثانویه آن، تصویر کاملی از تجربه کاربران ارائه نمی‌دهد.

یافته مهم دیگر پژوهش، رابطه میان تجربه بزه‌دیدگی و رفتارهای پیشگیرانه کاربران است. نتایج نشان داد که بزه‌دیدگی می‌تواند رفتار کاربران را تغییر دهد، اما این تغییر الزاماً به افزایش پایدار رفتارهای پیشگیرانه منجر نمی‌شود. این یافته را می‌توان با تفکیک بزه‌دیدگی اولیه و ثانویه تبیین کرد. تجربه بزه‌دیدگی اولیه، از طریق ایجاد آگاهی عینی از خطر، می‌تواند موجب افزایش حساسیت کاربر و بازنگری در شیوه استفاده از محیط‌های آنلاین شود. در چنین شرایطی، فرد ممکن است کنترل بیشتری بر اطلاعات شخصی اعمال کند، نسبت به پیام‌ها و لینک‌های ناشناس محتاط‌تر شود و اقدامات امنیتی بیشتری انجام دهد. در مقابل، زمانی که تجربه بزه‌دیدگی با پیامدهای ثانویه و احساس فقدان کنترل یا حمایت همراه می‌شود، الزاماً به رفتار پیشگیرانه فعال منتهی نخواهد شد و

حتی می‌تواند زمینه شکل‌گیری واکنش‌های منفعلانه را فراهم کند. براین‌اساس، یافته‌های پژوهش نشان می‌دهد که بزه‌دیدگی اولیه بیشتر نقش «هشداردهنده» و بزه‌دیدگی ثانویه نقش «تعدیل‌کننده» در رابطه میان تجربه جرم و رفتار پیشگیرانه دارد. به‌عبارت‌دیگر، مواجهه مستقیم با جرم می‌تواند ادراک خطر را افزایش دهد، اما چگونگی تجربه و مدیریت پیامدهای پس از جرم تعیین می‌کند که این ادراک خطر به رفتار پیشگیرانه تبدیل شود یا به احساس ناامنی، بی‌اعتمادی و انفعال بینجامد. از این منظر، صرف تجربه بزه‌دیدگی برای ایجاد رفتار ایمن کافی نیست؛ بلکه برخورداری کاربر از دانش، مهارت و حمایت مناسب پس از بزه‌دیدگی شرط مهمی برای تبدیل تجربه جرم به رفتار پیشگیرانه است. این تبیین همچنین نشان می‌دهد که یافته‌های پژوهش با نظریه فعالیت‌های روزمره در سطح وقوع بزه‌دیدگی اولیه همخوانی دارد. حضور بیشتر در شبکه‌های اجتماعی، فرصت تماس با بزهکاران بالقوه و موقعیت‌های جرم‌زا را افزایش می‌دهد و در صورت ضعف مراقبت و کنترل، احتمال بزه‌دیدگی بیشتر می‌شود. باوجوداین، نظریه فعالیت‌های روزمره به‌تنهایی برای توضیح پیامدهای پس از بزه‌دیدگی و تغییر رفتار قربانی کفایت نمی‌کند؛ زیرا بخش مهمی از تجربه کاربر پس از وقوع جرم، به نحوه مواجهه وی با آسیب، واکنش دیگران و میزان حمایت موجود مربوط است.

در مجموع، نتایج نشان می‌دهد که پیشگیری از بزه‌دیدگی سایبری در محیط دانشگاهی نباید تنها به کاهش فرصت وقوع جرم محدود شود. پیشگیری مؤثر باید دو مرحله را هم‌زمان موردتوجه قرار دهد: نخست، کاهش احتمال بزه‌دیدگی اولیه از طریق کاهش مواجهه پرخطر، ارتقای سواد و مهارت‌های امنیتی و افزایش مراقبت در تعاملات آنلاین؛ و دوم، جلوگیری از تشدید آسیب و شکل‌گیری بزه‌دیدگی ثانویه از طریق ایجاد سازوکارهای قابل‌اعتماد، محرمانه و در دسترس برای گزارش‌دهی، حمایت از بزه‌دیدگان و مدیریت پیامدهای جرم. در چنین رویکردی، هدف پیشگیری صرفاً جلوگیری از وقوع نخستین آسیب نیست، بلکه تبدیل تجربه بزه‌دیدگی به فرصتی برای افزایش توانمندی و رفتار ایمن کاربر نیز موردتوجه قرار می‌گیرد؛ بنابراین، مقابله مؤثر با بزه‌دیدگی سایبری مستلزم گذار از رویکرد صرفاً فنی به رویکردی چندسطحی است که در آن کاهش فرصت بزه‌دیدگی اولیه، جلوگیری از تداوم و تشدید بزه‌دیدگی ثانویه و تقویت رفتارهای پیشگیرانه کاربران به‌صورت هم‌زمان دنبال شود. این نسخه یک تفاوت اساسی با قبلی دارد: بزه‌دیدگی اولیه و ثانویه را به‌عنوان دو مرحله در فرایند بزه‌دیدگی و تغییر رفتار کاربر تحلیل می‌کند، نه اینکه صرفاً تعریف آنها را در نتیجه‌گیری تکرار کند.

منابع و مآخذ

الف- فارسی

آل رسول کمارعلیا,میرالتفات و مرشدی,مسعود . (۱٤۰٤). نقش آموزش در پیشگیری از بزه‌دیدگی سایبری. پژوهش های جرم شناسی کاربردی, ۲(۵), ۷۳-۹۹.

آقایی,مجید . (۱٤۰۰). واکاوی انسان‌شناسی جنایی از منظر بزه‌دیده شناسی اولیه درکیفر قصاص با تکیه‌بر اندیشه‌های امام خمینی (س). پژوهشنامه متین, ۲۳(۹۱), ۱-۲۷.

جامی پور, مونا , فرازپور, مهدی و اسدی, محسن . (۱۳۹۹). بررسی رابطهٔ بین مهارت‌های سایبری و میزان بزه‌دیدگی سایبری. فصلنامه علمی پژوهش‌های اطلاعاتی و جنایی, ۱۵(۵۹), ۱۰۷-۱۳٤ .

شاهپوری, تهمینه, و بشیریه, تهمورث. (۱٤۰٤). بررسی پیش‌بینی‌های بزه‌دیدگی جنسی از منظر مدل تلفیقی. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, ۲(۳), ۲۷۷-۳۰۷. Doi: ۱۰,۲۲۰۳٤/jclc.۲۰۲۵,۲۰٤۷۳۳٦,۱۱۲۸

جعفری، علیرضا و شهابی، سکینه و خنیاگر، طیبه و علی محمد حسینی، مرضیه (۱٤۰٤)،تحلیل جرم شناسی جرایم سایبری با تمرکز بر بزه دیدگان نوجوان،پنجمین همایش بین المللی وکالت، حقوق و علوم انسانی،همدان،۸-۱.

خواجه نوری, یاسمن, و نیازپور, امیرحسن. (۱٤۰۳). کنشگری پیشگیرانه پلیس در «قانون حمایت از اطفال و نوجوانان» ۱۳۹۹. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, ۱(۲), ۱۵۱-۱۸٤. Doi: ۱۰,۲۲۰۳٤/jclc.۲۰۲۵,۲۰٤۸٦۷٤,۱۱۳۲

دانش ناری, حمیدرضا , شیخ الاسلامی, عباس و محمدکوره پز, حسین . (۱۳۹۷). تحلیل بزه دیدگی جنسی زنان در شبکه‌های اجتماعی: نمونه‌پژوهی تانگو. فصلنامه پژوهش حقوق کیفری, ٦(۲۲), ٦۵-۱۰ .

رستگار آگاه, مصطفی . (۱٤۰٤). راهبردهای آماری برای عینی‌سازی اشباع نظری در مطالعات کیفی. فصلنامه اندازه گیری تربیتی, ۱٦(٦۰), ۱٤۳-۱٦۷.

رضازاده سلطان آباد، محمد و آقایی، مجید(۱۳۹۷) تحلیل جرمشناختی –جامعه شناختی جرایم در نقاط مرزی در پرتو تئوریهای فشار در بزهکاری با نگاهی به آیات و روایات. تحقیقات حقوقی تطبیقی ایران و بین الملل، ۱۱(٤۱). ٤۰٤-۳۷۳.

صمددوست، نسترن و قمی، صفا،(۱٤۰۲)،فضاهای بی دفاع شهری و پیشگیری از وقوع جرم با رویکرد طراحی محیطی،سومین کنفرانس بین المللی معماری،عمران،شهرسازی،محیط زیست و افق های هنر اسلامی در بیانیه گام دوم انقلاب،تبریز.

علیوردی نیا, اکبر و علیمردانی, منا . (۱۳۹٦). کاربست تجربی نظریهٔ فعالیت‌های روزمره در بررسی رفتارهای انحرافی دانشجویان. جامعه شناسی کاربردی, ۲۸(۳), ۱-۲٤.

علیوردی نیا, اکبر و صالح نژاد, صالح . (۱۳۹۲). کاربست های نظریه‌ی گزینش عقلانی در تبیین جرائم و ارائه دلالت های سیاستی برای پیشگیری از جرم. فصلنامه علمی کارآگاه, ۰۷(۲۵), ۹-۲٦.

علیوردی نیا اکبر، قربانزاده فایزه.(۱۳۹۸). بررسی جامعه‌شناختی بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان دانشگاه مازندران مسائل اجتماعی ایران ۱۰ (۱) :۱٦۹-۱٤۵ .

فرهادی، تورج(۱۳۹۹). نقش فضاهای بی دفاع در اجتماع و مدیریت شهری. فصلنامه علمی تخصصی مطالعات نوین برنامه ریزی شهری در جهان .۱(۲). ۲۲-۱.

فرامرزیانی, سعید . (۱٤۰۳). مطالعه نقش دوگانه شبکه های اجتماعی در بزهکاری (مطالعه موردی شهر ارومیه). فصلنامه مطالعات و پژوهش های امنیت داخلی, ۲(۳), ۱۰۹-۱۳۱.

مالمیر, محمود و زررخ, احسان . (۱۳۸۹). پیشگیری از بزه دیدگی سایبری. مطالعات پیشگیری از جرم, (۱۷), ۵۹-۸٦.

نورپور, محسن , سیدزاده ثانی, سید مهدی و ناصری فورگ, محمد یوسف . (۱٤۰۰). تحلیل عوامل مؤثر بر عدم گزارش بزه دیدگی (مطالعه موردی: دانشجویان پسر دانشگاه فردوسی مشهد). پژوهشنامه حقوق کیفری, ۱۲(۱), ۱۹۳-۲۱۸.

References

Apuke, O. D., & Iyendo, T. O. (2018). **University students' usage of the internet resources for research and learning: forms of access and perceptions of utility**. Heliyon, 4(12).Pp:1-20.

Aliverdinia, A. and Alimardini, M. (2017**). An Emprical Application of Routin Activities Theory in the Study of Studentsâ Deviant Behaviors**. Journal of Applied Sociology, 28(3), 1-24. (in Persian)

Alivardinia, Akbar, & Salehnejad, Saleh. (2013). **Applications of Rational Choice Theory in Explaining Crimes and Presenting Policy Implications for Crime Prevention**. Kargah Scientific Quarterly, ۷(۲۵), ۹–۲٦. (in Persian)

Alivardinia, Akbar, & Ghorbanzadeh, Faezeh. (2019). **A Sociological Study of Cyber-Harassment Victimization among Students at the University of Mazandaran.** *Social Issues of Iran*, ۱۰(۱), ۱٤۵–۱٦۹. (in Persian)

A. (2022). **Victimization by traditional bullying and cyberbullying and the combination of these among adolescents in ۱۳ European and Asian countries**. European child & adolescent psychiatry, ۳۱(۹),Pp: ۱۳۹۱-۱٤۰٤.

Ale Rasool Komarolia, M., & morshedy, M. (2024). **The role of education in preventing cyber victimization**. Applied criminology research, 2(5), 73-99. (in Persian)

Aghaei, M. (۲۰۲۱). **An Analysis of Anthropological Criminology from the Viewpoint of Initial Victimology in Qisas (Retaliation) Punishment with an Emphasis on Imam Khomeini's** Views. Matin Research Journal, ۲۳(۹۱), 1-27. (in Persian)

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). **Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study**. Crime Science, 13(1), 29.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). **Predicting online harassment victimization among a juvenile population**. Youth & Society, 44(4), Pp:500-523

Brown, C. F., Demaray, M. K., & Secord, S. M. (2014**). Cyber victimization in middle school and relations to social emotional outcomes.** Computers in human behavior, 35,Pp: 12-21.

Borwell, J., Jansen, J., & Stol, W. (2021). **Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions**. Journal of Digital Social Research, 3(3), Pp:85-110.

Chudal, R., Tiiri, E., Brunstein Klomek, A., Ong, S. H., Fossum, S., Kaneko, H., &Sourander, Wall, D. S(2011). **CYBERCRIME AND THE CULTURE OF FEAR: Social science fiction (s) and the production of knowledge about cybercrime** .

Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). **Cyberbullying in higher education: A literature review.** Computers in human behavior, 69,Pp: 268-274.

Drew, J. M., & Farrell, L. (2018). **Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs**. Police Practice and Research, 19(6).Pp:, 537-549.

Danesh-Nari, Hamidreza; Sheikh-Eslami, Abbas; and Koreh-Paz, Hossein (2018). **the analysis of Sexual victimization of women in social networks: The case study of Tango.** Journal of Criminal Law Research, 6(22), 65-101. (in Persian).

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017**). Defining cyberbullying**. Pediatrics, 140(2), Pp:148-151.

Farhadi, Touraj (۲۰۲۰). **The Role of Defenseless Spaces in Society and Urban Management.** Journal of Modern Urban Planning Studies Worldwide, ۱(۲), ۱–۲۲. (in Persian).

Faramarziani, Saeed. (2024). **A Study of the Dual Role of Social Networks in Delinquency (A Case Study of Urmia)**. Quarterly Journal of Internal Security Studies and Research, 2(3), 109-131. (in Persian).

Ho, H. T. N., & Luong, H. T. (۲۰۲۲). **Research trends in cybercrime victimization during ۲۰۱۰–۲۰۲۰: a bibliometric analysis**. SN Social Sciences, 2(1),4.

Hashemi, Y., Zarani, F., Heidari, M., & Borhani, K. (2022**). Purposes of internet use among Iranian university students: exploring its relationship with social networking site (SNS) addiction**. BMC psychology, 10(1), 80.

Holfeld, B., & Baitz, R. (2020). **The mediating and moderating effects of social support and school climate on the association between cyber victimization and internalizing symptoms**. Journal of Youth and Adolescence, 49(11),Pp: 2214-2228.

Jami Pour, M. , Faraz Pour, M. and Asadi, M. (2020). **Investigating the Relationship between Cyber Skills and Cyber Victim Rate.** Intelligence and criminal research journal, 15(59), 107-134. (in Persian).

Jafari, Alireza, Shahabi, Sakineh, Khonyagar, Tayebeh, & Ali Mohammad Hosseini, Marzieh (2026**), Criminological Analysis of Cybercrimes with a Focus on Adolescent Victims**, 5th International Conference on Advocacy, Law, and Humanities, Hamedan.1-8. (in Persian).

Kont, K. R. (2024). **The Role of Libraries in Creating a Safer Cyberspace: Awareness of Estonian Library Employees in Information Security**. The International Information & Library Review, ٥٦(٢), Pp:١٣٥–١٤٩.

Khajeh Nouri, Y., & Niazpour, A. (2025). **Preventive Police Actions in the Protection of Children and Adolescents under the 2019 Law.** Research and development in criminal law and criminology, 1(2), 151-184. Doi: 10.22034/jclc.2025.2048674.1132 (in Persian).

Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). **Youth internet victimization in a broader victimization context**. Journal of Adolescent Health, 48(2),Pp: 128-134.

Malmir, Mahmoud, & Zarrokh, Ehsan. (2010**). Prevention of cyber-victimization**. Crime Prevention Studies, (17), 59-86. (in Persian).

Nourpour, M. , Seyyed Zadeh Sani, S. M. and Naseri Fourg, M. Y. (2021). **Analysis of Factors Affecting Non-reporting of Victimization (Case Study: Male Students of Ferdowsi University of Mashhad**). Criminal Law Research, 12(1), 193-218. (in Persian).

Olweus, D., & Limber, S. P. (2018**). Some problems with cyberbullying research**. Currentopinion in psychology, 19, 139-143.

Olweus, D. (2012**). Cyberbullying: An overrated phenomenon?.** European journal of developmental psychology, 9(5),Pp: 520-538.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014**). Social media as a vector for youth violence: A review of the literature**. Computers in human behavior, 35,Pp: 548-553.

Qu, J., Lin, K., Wu, Y., & Sun, I. Y. (2024). **Fear and perceived risk of cyber fraud victimization among Chinese University students.** Crime, Law and Social Change, 82(3), Pp:543-562.

Reyns, B. W. (2011). **Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses**. Journal of Research in Crime and Delinquency, 50(2), Pp:216-238.

Rastgar Agah, M. (2025**). Statistical Strategies for Objectifying Theoretical Saturation in Qualitative** Studies. Quarterly of Educational Measurement, 16(60), 143-167. (in Persian).

Rezazadeh Soltan-Abad, Mohammad, & Aghaei, Majid (2018**). A Criminological-Sociological Analysis of Crimes in Border Areas in Light of Strain Theories of Delinquency: A Perspective Based on Quranic Verses and Narrations**. (Comparative Law Research (Iran and International), ۱۱(٤۱), ۳۷۳–٤۰٤. (in Persian).

Suzuki, A. (2024). **Routine activities and consumer fraud victimization: findings from a social survey in Chiba Prefecture, Japan**. Crime Prevention and Community Safety, 26(4),Pp: 373-384.

Samad-Doost, Nastaran, and Ghomi, Safa (2023), **"Vulnerable Urban Spaces and Crime Prevention through Environmental Design,"** 3rd International Conference on Architecture, Civil Engineering, Urban Planning, Environment, and Horizons of Islamic Art in the 'Second Step of the Revolution' Statement, Tabriz. (in Persian).

Shahpouri, T., & Bashirieh, T. (2025). **Examining Predictors of Sexual Victimization from the Perspective of an Integrated Model**. Research and development in criminal law and criminology, 2(3), 277-307. Doi: 10.22034/jclc.2025.2047336.1128 (in Persian).

Slonje, R., Smith, P. K., & Frisén, A. (2013). **The nature of cyberbullying, and strategies for prevention**. Computers in human behavior, 29(1), Pp:26-32.

Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013**). Cyberbullying myths and realities**. Computers in Human behavior, 29(6),Pp: 2703-2711.

Tsai, C. Y. (۲۰۲٤). Is undergraduates' adoption of the Internet of Things rational? The role of risk perception. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18(4).

THES Majid, T.(2025) Effect of changes in Interest rate on S&P500: A Literature Review. Bachelor International Business Administration

Vale, M., Pereira, F., Spitzberg, B. H., & Matos, M. (۲۰۲۲). **Cyber-harassment victimization of Portuguese adolescents: A lifestyle-routine activities theory approach.** Behavioral sciences & the law, ٤۰(٥),Pp: ٦۰٤-٦۱۸.