مقاله پژوهشی

فصلنامه پژوهش‌های دانش انتظامی، سال بیست‌وهفتم، شماره ۲، تابستان ۱۴۰۴

صص ۶۹-۲۹

بررسی جرم‌شناختی زورگویی سایبری: تحلیل علل، پیامدها و راهکارهای مقابله (مطالعه موردی شهر تبریز)[۱]

بابک محبوب علیلو[۲]، دکتر حسین غلامی[۳]، دکتر حسنعلی موذن‌زادگان[۴]

تاریخ دریافت: ۱۴۰۳/۱۰/۲۳ تاریخ پذیرش: ۱۴۰۴/۰۴/۱۵

چکیده

زمینه و اهداف: گسترش تعاملات دیجیتالی، بزه‌دیدگی و بزهکاری سایبری را به‌شکل رایجی از رفتارهای مضر در فضای مجازی تبدیل کرده است که حقوق افراد را به‌شدت تهدید می‌کند. این پدیده‌ها در اشکال گوناگونی ظاهر می‌شوند و بر جنبه‌های متعددی از زندگی شخصی قربانیان تأثیر می‌گذارند. این پژوهش با تمرکز بر شهر تبریز، به بررسی علل و ارائه راهکارهای مقابله‌ای برای این پدیده می‌پردازد.

روش: این مطالعه با استفاده از رویکرد کیفی-کمی، جنبه‌های مؤثر بر بزه‌دیدگی و بزهکاری سایبری را بررسی می‌کند. داده‌ها از طریق مصاحبه جمع‌آوری شد، سپس عوامل مؤثر بر بزه‌دیدگی و بزهکاری سایبری از طریق تحلیل عامل اکتشافی و رگرسیون خطی چندگانه تحلیل شدند. در نهایت با همفکری متخصصان پیشنهادهای کاربردی ارائه شد. نمونه آماری پژوهش شامل ۹۵ نفر از مراجعه کنندگان (بزهکار-بزه‌دیده) با محوریت جرائم مرتبط با بزهکاری سایبری (۵۴ نفر از این افراد بزهکار و ۴۱ نفر بزه‌دیده) بودند. این افراد با روش نمونه‌گیری هدفمند انتخاب شدند. کلیه تحلیل‌های آماری، به‌وسیله SPSS25 انجام شد.

یافته‌ها: عوامل بزه‌دیدگی سایبری در تبریز را می‌توان به خودکنترلی پایین، استفاده گسترده از شبکه‌های اجتماعی، نظارت ضعیف والدین و افشای بیش از حد اطلاعات شخصی اشاره کرد. همچنین، عوامل مؤثر بر بزهکاری سایبری شامل ناشناسی، یادگیری اجتماعی، تغییر ارزش‌ها و عدم درگیری اخلاقی هستند.

نتایج: به‌منظور کاهش بزه‌دیدگی و بزهکاری سایبری باید از فناوری‌های پیشرفته مانند هوش مصنوعی و تحلیل داده‌ها برای پیش‌بینی و پیشگیری از جرائم سایبری و توسعه سامانه‌های برخط گزارش‌دهی برای تسهیل اطلاع‌رسانی جرائم سایبری توسط قربانیان، افزایش آگاهی از طریق برگزاری کارگاه‌های آموزشی، همکاری با مدارس و دانشگاه‌ها و برگزاری گروه‌های آگاهی‌بخشی در سطح شهر استفاده کرد.

کلیدواژه‌ها: زورگویی سایبری، جرائم سایبری، بزهکاری سایبری، راهکارهای مقابله و پیشگیری.

---

۱. مقاله برگرفته از رساله دکتری.

۲. دانشجوی دکترای حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران. رایانامه: shalchi.b@gmail.com

۳. استاد حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران. رایانامه: hossein.gholami@atu.ac.ir

۴. استاد حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران. رایانامه: ha.moazenzadegan@atu.ac.ir

مقدمه

از اواسط دهه ۱۹۹۰، پیشرفت‌های فناوری به‌طور چشمگیری پویایی ارتباطات را دگرگون کرده‌اند. ظهور فناوری‌های ارتباطی مقرون به صرفه و رایانه‌های شخصی، دسترسی گسترده به اینترنت و تلفن‌های همراه را در سطح خانوارها در سراسر جهان تسهیل کرده است (دوبی[1]،۱۹۹۱). این تحولات سبک‌زندگی افراد، عادات کاری و فعالیت‌های اوقات فراغت را متحول کرده و در عین حال ماهیت تعاملات و روابط انسانی را به‌طور اساسی تغییر داده است (باسو[2] و همکاران، ۲۰۰۲). با این حال، در کنار این تغییرات مثبت، پیامدهای منفی خاصی مانند بزه‌دیدگی سایبری[3] و بزهکاری سایبری[4] ظهور کرده‌اند که چالش‌های منحصر به فردی را در فضای دیجیتال ایجاد می‌کنند (کیم[5] و همکاران، ۲۰۲۳). بزهکاری سایبری، به‌عنوان یک رفتار پرخاشگرانه و آسیب‌زننده در فضای برخط، به یکی از مسائل فوری و نگران‌کننده در جامعه امروزی تبدیل شده است. این پدیده توجه گسترده‌ای را از سوی محققان، سیاست‌گذاران، مربیان و متخصصان حوزه سلامت روان به خود معطوف کرده است، چرا که تأثیرات عمیق و گسترده‌ای بر افراد و جامعه به‌همراه دارد.

در ابتدا، رفتارهای مشابه بزهکاری سایبری تحت یک اصطلاح واحد شناخته نمی‌شدند. این رفتارها با عباراتی مانند «فلمینگ[6]» که به‌معنای انفجارهای خشم در فضای مجازی بود، «فلودینگ[7]» که با ارسال پیام‌های تکراری برای تحت‌تأثیر قرار دادن گیرنده مشخص می‌شد، «کیکینگ[8]» که شامل حذف یک فرد از یک گروه برخط بود، و

---

[1] Duby
[2] Basu
[3] Cyber Victimization
[4] Cyber Offending
[5] Kim
[6] Flaming
[7] Flooding
[8] Kicking

«اسپمینگ[1]» که به ارسال پیام‌های ناخواسته اشاره داشت، شناخته می‌شدند (گارباس[2]، ۱۹۹۷؛ ترکل[3]، ۱۹۹۵؛ یانگ[4]، ۱۹۹۶). این رفتارها اغلب به‌عنوان مسائل مجزا در نظر گرفته می‌شدند و درک محدودی از پیامدهای گسترده‌تر آنها وجود داشت. با این حال، با رشد سریع برنامه‌های کاربردی دیجیتال و جوامع برخط، این اشکال سوءرفتار تکامل یافته و تحت چتر اصطلاح «بزهکاری سایبری» قرار گرفته‌اند. در زمینه‌های خاص، مانند جوامع بازی‌های برخط، این رفتارها به‌عنوان «گریفینگ» که شامل آزار عمدی دیگر بازیکنان است، و «ترولینگ» که شامل تحریک دیگران از طریق اظهارات توهین‌آمیز یا تحریک‌آمیز است، شناخته می‌شوند (وارنر و رایتر[5]، ۲۰۰۵).

علی‌رغم تحقیقات گسترده، یک تعریف جهانی پذیرفته‌شده از بزهکاری سایبری همچنان مورد توافق همگانی نیست (اسمیت[6] و همکاران، ۲۰۰۲). طبق یکی از تعاریف، بزهکاری سایبری به‌عنوان یک عمل تهاجمی و عمدی تعریف می‌کنند که به‌طور مکرر و در طول زمان با استفاده از ابزارهای الکترونیکی علیه قربانیانی که قادر به دفاع از خود نیستند، انجام‌می‌شود (شاجینگ سون[7]، ۲۰۱۶). این تعریف، اگرچه ریشه در مفهوم‌سازی سنتی بزهکاری دارد، نیاز به اصلاح بیشتر برای در نظر گرفتن ویژگی‌های منحصربه‌فرد تعاملات دیجیتالی دارد. بزهکاری سایبری در اشکال مختلفی بروز می‌کند، از جمله آزار و اذیت سایبری (ارسال پیام‌های تهدیدآمیز یا توهین‌آمیز)، بدنام‌سازی (پخش اطلاعات نادرست یا مضر درباره یک فرد)، جعل هویت (ایجاد حساب‌های جعلی برای تقلید یا آزار دیگران) و زورگیری جنسی سایبری (استفاده از

[1] Spamming
[2] Garbasz
[3] Turkle
[4] Young
[5] Warner & Raiter
[6] Smith
[7] Shaojing Sun

برنامه‌های کاربردی دیجیتال برای رفتارهای جنسی اجباری) (قاسم‌تبار و همکاران، ۲۰۲۱).

بزهکاری سایبری تنها یک مزاحمت اجتماعی نیست، بلکه یک نگرانی حقوقی و روان‌شناختی مهم است. از منظر حقوقی، این پدیده به‌عنوان یک رفتار ضداجتماعی در فضای مجازی طبقه‌بندی می‌شود که شامل نقض حریم خصوصی، آزار و اذیت و تهدید حقوق اساسی کاربران است. این رفتار خطرات روانی قابل توجهی را به ویژه برای گروه‌های آسیب‌پذیر مانند کودکان، زنان و نوجوانان ایجاد می‌کند. قربانیان بزهکاری سایبری اغلب پیامدهای منفی سلامت روانی از جمله افسردگی، اضطراب، کاهش اعتماد به نفس و در موارد شدید، افکار یا رفتارهای خودکشی را تجربه می‌کنند (تامپسن[1]، ۱۹۹۴؛ لی[2]، ۲۰۰۶). اثرات مخرب بزهکاری سایبری فراتر از افراد است و می‌تواند حس جمعی امنیت در فضای دیجیتال را تضعیف کرده و فضایی از بی‌اعتمادی و ترس ایجاد کند. مطالعه بزهکاری سایبری به چند دلیل حیاتی است. اولاً، گسترش استفاده از اینترنت و برنامه‌های کاربردی رسانه‌های اجتماعی به‌طور قابل توجهی شیوع و رؤیت‌پذیری حوادث بزهکاری سایبری را افزایش داده است. درک زاهکارهای و پیامدهای بزهکاری سایبری برای توسعه مداخلات و اقدامات پیشگیرانه هدفمند ضروری است. ثانیاً، پژوهش در این زمینه می‌تواند به تدوین سیاست‌ها و چارچوب‌های حقوقی مؤثر کمک کند و شکاف‌های موجود در سیستم‌های فعلی را برطرف کند. علاوه بر این، ماهیت پویای فناوری نیازمند تحقیقات مستمر برای همگام شدن با روندهای نوظهور در رفتارهای بزهکاری سایبری است.

فراتر از تأثیرات فوری، بزهکاری سایبری پیامدهای گسترده‌ای برای جامعه دارد. این پدیده می‌تواند اعتماد عمومی به برنامه‌های کاربردی دیجیتال را تضعیف کند، دسترسی و کارایی آنها (به‌ویژه برای گروه‌های آسیب‌پذیر) را کاهش دهد. علاوه بر این،

[1] Thompsen
[2] Li

بزهکاری سایبری محیطی از ناامنی و ترس ایجاد می‌کند که بر روابط بین فردی و خانوادگی تأثیر منفی می‌گذارد. همان‌طور که *لوپز - منزس*[1] و همکاران (۲۰۲۰) تأکید می‌کنند، پرداختن به این مسئله نه‌تنها از منظر حقوقی و جرم‌شناختی ضروری است، بلکه به‌عنوان یک ضرورت اجتماعی و روان‌شناختی نیز مطرح می‌شود. تلاش‌ها برای مقابله با بزهکاری سایبری باید بر افزایش آگاهی عمومی و آموزش کاربران در مورد ایمنی برخط و راهبردهای محافظت از خود متمرکز شود (هندوجا و پرچین[2]، ۲۰۱۵). ایجاد سازوکارهای گزارش‌دهی قوی و سامانه‌های حمایتی برای قربانیان نیز به همان اندازه حیاتی است. همکاری بین‌المللی و تبادل بهترین تجربیات بین کشورها می‌تواند راهبردهای کاهش بزهکاری سایبری را تقویت کند (یونیسف[3]، ۲۰۲۰).

یکی از نوآوری‌های کلیدی این پژوهش، توجه همزمان به بزهکار سایبری و بزه‌دیده سایبری است. این رویکرد دو وجهی از آن جهت مورد تأکید است که پدیده آزارگری سایبری تنها با بررسی یک‌طرفه (چه بزهکار و چه بزه‌دیده) به‌طور کامل قابل درک نیست. درک کامل این پدیده نیازمند تحلیل تعاملات و روابط بین این دو طرف است. آزارگری سایبری به‌عنوان یک پدیده اجتماعی-دیجیتالی، در فضای ارتباطی بین بزهکار و بزه‌دیده شکل می‌گیرد و گسترش می‌یابد. بنابراین، برای دستیابی به درکی جامع و همه‌جانبه از این پدیده، لازم است که هر دو بعد بزهکاری و بزه‌دیدگی به‌طور همزمان مورد بررسی قرار گیرند. همچنین، بسیاری از تحقیقات موجود در حوزه بزهکاری سایبری بر جوامع غربی متمرکز هستند و دیدگاه‌های محلی و بومی را نادیده می‌گیرند. این کمبود می‌تواند به ارائه راهکارهایی منجر شود که با شرایط فرهنگی و اجتماعی جوامع محلی سازگار نیستند. علاوه بر این، بزهکاری سایبری می‌تواند

[1] López-Meneses
[2] Hinduja & Patchin
[3] UNICEF

پیامدهای جرم‌شناختی و اجتماعی شدیدی از جمله آسیب‌های روانی به قربانیان، کاهش اعتماد به فضای دیجیتال، و تهدید امنیت‌ملی داشته باشد.

این پژوهش به‌عنوان یک ابزار راهبردی برای پلیس و نهادهای مسئول در حوزه امنیت سایبری عمل می‌کند و به طراحی راهبردهای پیشگیرانه و واکنشی مؤثر در مقابله با بزهکاری سایبری کمک می‌نماید. از طریق شناسایی الگوهای جرائم سایبری و تحلیل عوامل مؤثر بر آن در جامعه محلی تبریز، پلیس می‌تواند اقدامات هدفمندی برای رصد و مقابله با این جرائم طراحی کند. همچنین، یافته‌های این مطالعه زمینه‌ساز تقویت آموزش تخصصی کارکنان پلیس در زمینه فناوری‌های نوین، روش‌های تشخیص جرائم سایبری، و روش‌های تعامل با قربانیان است. علاوه بر این، پلیس می‌تواند از نتایج پژوهش برای ارتقای آگاهی عمومی از طریق گروه‌های آموزشی، بهبود زیرساخت‌های گزارش‌دهی جرائم سایبری، و تدوین سیاست‌های بومی متناسب با تفاوت‌های فرهنگی و اجتماعی استفاده کند. این پژوهش همچنین بر لزوم همکاری فراسازمانی پلیس با برنامه‌های کاربردی دیجیتال، نهادهای آموزشی، و سازمان‌های بین‌المللی تأکید دارد. در نهایت، این مطالعه به پلیس امکان می‌دهد با درک عمیق‌تری از ریشه‌ها و پیامدهای بزهکاری سایبری، نه‌تنها به مقابله قانونی با جرائم بپردازد، بلکه با اقدامات پیشگیرانه و آموزشی، به کاهش ناامنی در فضای دیجیتال کمک کرده و اعتماد عمومی به نهادهای انتظامی را افزایش دهد.

این مطالعه بر جامعه کاربران برخط در تبریز متمرکز است و هدف آن بررسی دلایل اصلی بزهکاری سایبری، پیامدهای جرم‌شناختی و اجتماعی آن، و اثربخشی اقدامات پیشگیرانه است. جامعه مورد مطالعه شامل کاربران فعال اینترنت در تبریز است که دیدگاهی محلی در مورد این مسئله جهانی ارائه می‌دهد. این رویکرد محلی به درک بهتر تفاوت‌های فرهنگی و اجتماعی در بروز و مقابله با بزهکاری سایبری کمک می‌کند. یافته‌های این تحقیق انتظار می‌رود که عوامل کلیدی مؤثر بر بزهکاری سایبری

را روشن کند، پیامدهای آن را برجسته کند و راهکارهای عملی پیشنهاد دهد. این بینش‌ها می‌توانند توسعه راهبردهای محلی و ملی برای مقابله مؤثر با بزهکاری سایبری را هدایت کنند.

در نتیجه، بزهکاری سایبری یک پدیده پیچیده و چندوجهی است که نیازمند بررسی و مداخله دقیق است. با تمرکز بر تبریز، این مطالعه به‌دنبال افزایش درک بزهکاری سایبری و توسعه راهکارهای عملی برای مقابله با آن است. یافته‌ها پتانسیل بهبود تجربه برخط کاربران در تبریز و الگویی برای ابتکارات مشابه در سایر شهرها و مناطق را دارند. تحقیقات مستمر و همکاری بین ذی‌نفعان برای ایجاد یک محیط دیجیتال امن‌تر و فراگیرتر ضروری است. از طریق تلاش‌های هماهنگ، می‌توان شیوع بزهکاری سایبری را کاهش داد و اطمینان حاصل کرد که فضاهای دیجیتال به تعاملات و تجربیات مثبت برای همه کاربران کمک می‌کنند. بنابراین، این مطالعه به‌دنبال پاسخ به این سؤال اساسی است که چه عواملی باعث بروز بزه‌دیدگی و بزهکاری سایبری در میان کاربران برخط شهر تبریز می‌شوند و چه راهکارهایی برای پیشگیری و مقابله مؤثر با این پدیده می‌توان ارائه داد؟

پیشینه و مبانی نظری

پیشینه داخلی

جباریان و همکاران (۲۰۲۴)، در پژوهشی باعنوان «رابطه بین نشانگان درونی‌سازی شده و کنجکاوی بیمارگونه و آزارگری سایبری در نوجوانان» انجام دادند، نتایج نشان داد، که نشانگان درونی‌سازی و آزارگری سایبری و همچنین بین کنجکاوی بیمارگونه و آزارگری سایبری رابطه ساختاری معناداری وجود دارد. با این حال، نشانگان درونی‌سازی و کنجکاوی بیمارگونه تنها ۴/۸ درصد از تهاجم سایبری را تبیین می‌کنند.

کامران و همکاران (۱۴۰۳)، در پژوهشی باعنوان «تدوین مدل ساختاری قربانی‌شدن سایبری بر اساس اعتیاد به اینترنت و حمایت اجتماعی ادراک شده با نقش واسطه‌ای

ویژگی‌های شخصیتی» انجام دادند، یافته‌ها نشان داد که اعتیاد به اینترنت رابطه معنادار و معکوس بر مسئولیت‌پذیری و رابطه معنادار و مستقیم بر روان‌آزرده‌گرایی دارد. حمایت اجتماعی ادراک شده نیز رابطه معنادار مستقیم بر مسئولیت‌پذیری و برون‌گرایی دارد. خرده مقیاس روان‌آزرده‌گرایی رابطه مستقیم و معنادار بر قربانی‌شدن سایبری دارد و در نهایت عامل مسئولیت‌پذیری و برون‌گرایی به‌عنوان عامل میانجی با اعتیاد به اینترنت و حمایت اجتماعی، بر قربانی‌شدن سایبری رابطه معنادار دارند و رابطه غیرمستقیم سایر خرده مقیاس‌ها معنی‌دار نبود.

پیکری و همکاران (۱۴۰۳)، در پژوهشی باعنوان «راهبردهای نیروی انتظامی در پیشگیری اجتماعی از بزه‌دیدگی در فضای مجازی»، نشان داد که موقعیت راهبردی پلیس در پیشگیری اجتماعی از بزه‌دیدگی سایبری شامل ۴۳ عامل محیط داخلی و ۱۹ عامل محیط بیرونی است و بر این اساس ۲۰ راهبرد پیشگیرانه در قالب راهبردهای تهاجمی، رقابتی، محافظه‌کارانه و تدافعی تدوین شده است که می‌تواند مبنای اقدامات پیشگیرانه پلیس قرار گیرد.

درویشی و همکاران (۱۴۰۲)، در پژوهشی باعنوان «راهبردهای پلیس در پیشگیری از بزه‌دیدگی اطفال و نوجوانان با تأکید بر وضعیت‌های مخاطره» نشان داد که راهبردهای حمایتی، مشارکتی و تعاملی پلیس تأثیر معناداری بر پیشگیری از بزه‌دیدگی اطفال و نوجوانان در وضعیت‌های مخاطره‌آمیز دارند و اجرای این مداخلات موجب کاهش آثار عوامل آسیب‌زا در بزه‌دیدگی این گروه می‌شود.

محمدی‌مقدم و همکاران (۱۴۰۱)، در پژوهشی باعنوان «واکاوی علل مؤثر وقوع جرم در فضای سایبری» نشان دادند که شانزده عامل به‌عنوان عوامل مؤثر و پیشران‌های اصلی وقوع جرم در فضای سایبری شناسایی شده‌اند و شناخت این عوامل می‌تواند نقش مهمی در پیشگیری از ارتکاب جرائم سایبری دارند.

فیروزچیان و همکاران (۱۴۰۱)، در پژوهشی باعنوان «تحلیل عوامل مؤثر بر قربانی شدن سایبری در میان شهروندان (مورد مطالعه: شهروندان شهر بابل)» نشان دادند که بین متغیرهای نظریه زندگی روزمره و تجربه قربانی شدن در فضای مجازی (تنوع استفاده از فضای مجازی، رفتارهای پرخطر در فضای مجازی، حفاظت فیزیکی، حفاظت شخصی، جذابیت، تجربه قربانی شدن اطرافیان و عدم امنیت و کنترل) رابطه وجود دارد.

عطادخت و احمدی (۱۴۰۰)، در پژوهشی باعنوان «طراحی الگوی روابط ساختاری پرخاشگری سایبری بر اساس الگوی ارتباطی خانواده با نقش میانجی اعتیاد به اینترنت» نشان دادند، جهت‌گیری گفت‌وشنود هم‌بستگی مستقیم با پرخاشگری سایبری دارد. همچنین جهت‌گیری گفت‌وشنود از مولفه‌های الگوی ارتباطی خانواده با میانجیگری اعتیاد به اینترنت هم‌بستگی غیرمستقیم با پرخاشگری سایبری دارد. شاخص‌های برازش الگو نیز، جهت‌گیری گفت‌وشنود به پرخاشگری سایبری را با میانجیگری اعتیاد به اینترنت تأیید کرد.

کریم‌زاده و همکاران (۱۴۰۰)، در پژوهشی باعنوان «بررسی رابطه بین سرمایه اجتماعی و فرهنگی با گرایش به بزهکاری سایبری، جامعه‌شناسی اقتصادی و توسعه» نشان داند، گرایش به بزهکاری سایبری در بین مردان بیشتر از زنان است. هم‌بستگی چندگانه معادل ۰/۲۵۶ و متغیرهای مستقل به‌طور همزمان ۰/۴۶۵ با گرایش به بزهکاری سایبری ارتباط دارند و ۰/۲۸ درصد از تغییرات گرایش به بزهکاری سایبری پاسخ‌گویان توسط متغیرهای اعتماد نهادی، انسجام اجتماعی، دینداری، سواد رسانه‌ای، فرسایش سرمایه اجتماعی خانوادگی و حمایت اجتماعی تبیین شده است. بنابراین تدابیر خانواده‌محور، نشاط ملی و رضایتمندی، شفافیت در عملکرد کارگزاران، درونی کردن باورهای دینی و... در کاهش بزهکاری سایبری ثمربخش خواهد شد.

شـــیرافکن و همکاران (۱۳۹۹)، در پژوهشـــی باعنوان «رابطه اعتیاد به اینترنت با بزهکاری سایبری و نوموفوبیا در میان دانش‌آموزان، بر نقش اعتیاد به دنیای مجازی به‌عنوان عاملی مهم در شیوع بزهکاری سایبری» تأکید کردند. این مطالعه تقاطع بین وابســـتگی‌های روانی، مانند اعتیاد به اینترنت و تظاهرات رفتاری پرخاشـــگری در فضای برخط را برجسته ساخت.

جاه‌بین و همکاران (۱۳۹۷)، در پژوهشی باعنوان «مطالعه کیفی عوامل پشت جرائم سایبری (تحلیل محتوای کیفی پرونده‌های جرائم سایبری)»، بزهکاری سایبری را به‌عنوان یکی از عوامل کلیدی مؤثر در ارتکاب برخی جرائم در فضـــای دیجیتال شـــناســـایی کردند. مطالعه آنها فهرســـتی از عناصـــری را ارائه داد که ناکارآمدی بزهکاری ســـایبری را تشـــدید می‌کنند و تأثیرات گســـترده آن را در زمینه‌های گسترده‌تر جرائم سایبری روشن می‌سازند.

شـــاه‌محمدی و رجبی (۱۳۹۷)، در پژوهشـــی باعنوان «تحلیل جرائم اخلاقی فضـــای سایبر با رویکرد داده‌کاوی» نشان داد که بهترین مدل برای تحلیل و استخراج قوانین حاکم بر داده‌های جرائم اخلاقی فضـــای ســـایبر، مدل درخت تصـــمیم اســـت و متغیرهای شـــغل، تحصـــیلات، جنســـیت، ســـن، وضـــعیت تأهل و نقش فرد به‌ترتیب بیشترین تأثیر را بر وقوع جرائم اخلاقی فضای سایبر دارند و با استخراج این قوانین می‌توان راهکارهای پیشگیرانه مؤثری ارائه داد.

رضـــوی‌فرد و کوره‌پز (۱۳۹۴)، در پژوهشـــی باعنوان «راهبردهای آگاهی‌بخش آموزشـــی پیشـــگیرانه: ضـــرورتی در برابر برنامه‌های کنترل انحرافات ســـایبری»، از پاسخ‌های کنشی به رفتارهای نادرست در دنیای مجازی حمایت کردند. راهبردهای آگاهی‌بخش آموزشـی پیشـنهادی آنها بر تجهیز کاربران جوان به دانش و ابزارهای لازم برای حرکت مسئولانه در فضای دیجیتال تأکید دارد.

مارک[1] و همکاران (۲۰۲۴)، در پژوهشی باعنوان «ریشه‌های آزارگری سایبری: کشف خشونت سایبری» که از طریق مرور سیستماتیک انجام دادند، نشان داند، عوامل مؤثر بر پرخاشگری سایبری را به دو دسته اصلی تقسیم می‌شوند: عوامل فردی و عوامل محیطی. عوامل فردی شامل ویژگی‌های شخصیتی (مانند پرخاشگری، خودشیفتگی)، انگیزه‌ها (مانند انتقام یا جلب توجه) و مهارت‌های فنی است. عوامل محیطی شامل دسترسی به فناوری، هنجارهای اجتماعی، فرهنگ دیجیتال و حمایت نهادی می‌شود. همچنین، نداشتن مدل‌های جامع که عوامل اقتصادی و اجتماعی را در نظر بگیرند، به‌عنوان یک چالش کلیدی شناسایی شده است. این عوامل در تعامل با یکدیگر، زمینه‌ساز بروز و گسترش خشونت سایبری هستند.

ژونگ[2] و همکاران (۲۰۲۱)، در پژوهشی باعنوان «مطالعه عوامل مؤثر در آزار و اذیت سایبری در میان دانشجویان کالج چینی» نشان دادند، که زورگیری سایبری در میان دانشجویان چینی در سطح پایینی است. جنسیت، زمان صرف‌شده برای فعالیت‌های غیردرسی، و ویژگی‌های شخصیتی مانند همدلی و استرس، تأثیر معناداری بر زورگیری سایبری و قربانی شدن دارند. همچنین، درک و رعایت آداب اینترنتی و قوانین دیجیتال تأثیر منفی بر زورگیری سایبری داشته، در حالی که اعتیاد به اینترنت و توانایی ارتباط برخط تأثیر مثبت نشان دادند. این یافته‌ها می‌توانند به طراحی راهکارهای مؤثر برای کاهش زورگیری سایبری کمک کنند.

سیمنزا[3] (۲۰۱۹)، در پژوهشی باعنوان «تفاوت‌های جنسیتی در روابط قربانی-مجرم مرتبط با خشونت نوجوانی برخط و غیربرخط، تأثیر دینامیک جنسیت را بر هر دو جنبه مجرمیت و قربانی‌شدن در چارچوب بزهکاری سایبری بررسی کرد. این

[1] Mukred
[2] Zhong
[3] Semenza

مطالعه ماهیت جنسیتی پرخاشگری برخط را روشن ساخت و بینش‌های مهمی در مورد چگونگی تفاوت روابط قربانی-مجرم بین نوجوانان دختر و پسر ارائه داد.

می‌تر و بومن[1] (۲۰۱۸)، در پژوهشی باعنوان «بی‌تعهدی اخلاقی در بزهکاری سایبری و نظارت والدین»، بر نقش حیاتی نظارت والدین و توسعه مهارت‌ها در پیشگیری از بزهکاری سایبری در میان کاربران کودک تأکید کردند. آنها این فرضیه را مطرح کردند که پرورش آگاهی اخلاقی و مشارکت والدین می‌تواند به‌طور قابل توجهی از بروز رفتارهای مضر برخط بکاهد.

آسانان[2] (۲۰۱۷)، در پژوهشی باعنوان «بزهکاری سایبری: اشکال، آگاهی و توجیهات اخلاقی در میان جوانان» توصیه‌های عملی برای پرداختن به ریشه‌های بزهکاری سایبری ارائه کرد. نتایج نشان داد، زورگیری سایبری در میان جوانان شایع است و ۸۷ درصد از نمونه‌ها با این پدیده آشنا هستند. آگاهی و استدلال اخلاقی رابطه مثبتی با کاهش زورگیری سایبری دارند، اما برخی جوانان از تأثیرات اخلاقی رفتار خود آگاه نیستند. قربانیان این پدیده اغلب دچار آسیب‌های روانی شدید مانند کاهش عزت نفس می‌شوند و آموزش و ترویج ارزش‌های اخلاقی برای مقابله با آن ضروری است.

ژانگ و همکاران (۲۰۱۶)، در پژوهشی باعنوان «دوست یا دشمن: بزهکاری سایبری در سایت‌های شبکه‌های اجتماعی»، به بررسی مهم‌ترین علل اجتماعی و فرهنگی بزهکاری سایبری، به ویژه از منظر جرم‌شناسی فرهنگی، پرداختند. کار آنها نقش سایت‌های شبکه‌های اجتماعی را به‌عنوان تسهیل‌کننده و تعدیل‌کننده رفتارهای بزهکاری سایبری برجسته ساخت.

همفیل و همکاران (۲۰۱۵)، در پژوهشی باعنوان «پیش‌بین‌های قربانی‌شدن در بزهکاری سایبری و سنتی: یک مطالعه طولی در میان دانش‌آموزان دبیرستانی

[1] Meter & Bauman
[2] Asanan

استرالیا»، شاخص‌های مختلف قربانی‌شدن را در میان دانش‌آموزان دبیرستانی در استرالیا بررسی کردند. یافته‌های آنها به درک عمیق‌تری از پیش‌بین‌های مشترک و منحصربه‌فرد قربانی‌شدن در بزهکاری در محیط‌های مختلف کمک کرد.

های[1] و همکاران (۲۰۱۰)، در پژوهشی باعنوان «بزهکاری سنتی، بزهکاری سایبری و انحراف: یک رویکرد مبتنی بر نظریه فشار عمومی»، نظریه فشار جرم‌شناختی را برای تحلیل انگیزه‌ها و فشارهای زیربنایی رفتارهای بزهکاری سنتی و مجازی به کار بردند. چارچوب نظری آنها لنزی جامع برای درک عوامل استرس‌زای اجتماعی و هیجانی گسترده‌تر که به بزهکاری منجر می‌شوند، فراهم کرد.

مبانی نظری

بزهکاری سایبری را می‌توان از طریق نظریه‌های مختلف جرم‌شناسی درک و تحلیل کرد که چارچوبی نظری برای توضیح علل ظهور و تداوم چنین رفتارهایی در محیط برخط ارائه می‌دهند. این نظریه‌ها نه‌تنها بینش‌ی درباره علل زیربنایی این رفتارها فراهم می‌کنند، بلکه راهکارهایی برای پیشگیری و مداخله نیز ارائه می‌دهند. در ادامه، چند نظریه جرم‌شناسی مرتبط با پدیده بزهکاری سایبری به تفصیل بررسی می‌شوند:

۱. نظریه هم‌نشینی افتراقی

این نظریه که توسط *ادوین ساترلند*[2] (۱۹۷۴)، مطرح شده است، تأکید می‌کند که رفتارهای مجرمانه، از جمله بزهکاری سایبری، از طریق تعامل مستقیم با دیگران آموخته می‌شوند. افراد، نگرش‌ها، روش‌ها و انگیزه‌های رفتارهای انحرافی را از محیط خود کسب می‌کنند. در فضای مجازی، تعامل طولانی‌مدت با گروه‌ها یا جوامعی که بزهکاری سایبری را تأیید یا عادی‌سازی می‌کنند، می‌تواند تأثیر قابل توجهی در گرایش افراد به چنین رفتارهایی داشته باشد. به‌عنوان مثال، مشارکت

[1] Hay
[2] Edwin Sutherland

در فروم‌ها یا گروه‌های شبکه‌های اجتماعی که بزهکاری در آنها رایج است، ممکن است به تقلید از این رفتارها منجر شود. *هندوژا* و *پاتچین*[1] (۲۰۰۸)، نقش شبکه‌های اجتماعی و رسانه‌ها را به‌عنوان بسترهایی که افراد، به ویژه جوانان، از طریق آنها رفتارهای بزهکاری را یاد گرفته و تکرار می‌کنند، برجسته کردند.

۲. نظریه بی‌هنجاری

این نظریه که توسط *رابرت مرتون*[2] (۱۹۳۸)، ارائه شده است، ناتوانی در دستیابی به اهداف مورد تأیید جامعه را با تمایل به انجام رفتارهای انحرافی مرتبط می‌داند. در محیط دیجیتال، افرادی که با ناکامی‌های اجتماعی یا اقتصادی مواجه هستند، ممکن است برای ابراز قدرت یا کسب احساس برتری، به بزهکاری سایبری روی آورند. دنیای مجازی، که با نظارت ضعیف و هنجارهای اجتماعی مبهم مشخص می‌شود، می‌تواند احساس بیگانگی و بی‌هنجاری را تشدید کرده و احتمال رفتارهای پرخاشگرانه را افزایش دهد. *پاتچین* و *هندوژا* (۲۰۱۳)، اشاره کردند که کمبود مقررات در فضای مجازی می‌تواند این تمایلات را تشدید کند و بستری مناسب برای بزهکاری سایبری ایجاد کند.

۳. نظریه کنترل اجتماعی

نظریه کنترل اجتماعی *تراویس هیرشی*[3] (۱۹۶۹)، بیان می‌کند که پیوندهای قوی اجتماعی با نهادهایی مانند خانواده، مدرسه و جامعه به‌عنوان عوامل محافظتی در برابر رفتارهای مجرمانه عمل می‌کنند. در حوزه بزهکاری سایبری، نبود چنین پیوندهایی می‌تواند خطر رفتارهای انحرافی را افزایش دهد. به‌عنوان مثال، کودکان و نوجوانانی که فاقد نظارت والدین بر فعالیت‌های برخط خود هستند، بیشتر در معرض خطر مشارکت در بزهکاری سایبری یا قربانی شدن قرار دارند.

---

[1] Hinduja & Patchin
[2] Robert Merton
[3] Travis Hirschi

علاوه بر این، کمبود قوانین مؤثر و بازدارنده‌های اجتماعی در فضای مجازی، وقوع چنین رفتارهایی را تسهیل می‌کند. *هالت* و *باسلر*[1] (۲۰۰۹)، بر نیاز به نظارت قوی والدین و جامعه برای کاهش این خطرات و ایجاد محیط‌های برخط امن‌تر تأکید کردند.

٤. نظریه فعالیت روزمره

نظریه فعالیت روزمره *کوهن* و *فلسون*[2] (۱۹۷۹)، سه عنصر اساسی برای وقوع جرم را شناسایی می‌کند: (۱) مجرم مستعد، (۲) قربانی مناسب، و (۳) نبود نگهبان قادر. در دنیای دیجیتال، این عناصر به شیوه‌های منحصر به فردی با هم ترکیب می‌شوند. مجرمان مستعد می‌توانند افرادی را هدف قرار دهند که به‌راحتی اطلاعات شخصی خود را در فضای برخط به اشتراک می‌گذارند و آنها را در معرض آزار و اذیت قرار می‌دهند. عدم وجود سازوکارهای نظارتی یا بازدارنده مؤثر در فضای مجازی - مانند ناشناس بودن و نظارت ناکافی - فرصت‌هایی را برای گسترش بزهکاری سایبری ایجاد می‌کند. *ناوارو* و *جاسینسکی*[3] (۲۰۱۲)، خاطرنشان کردند که ناشناس بودن کاربران به‌عنوان یک عامل مهم، مجرمان را تشویق می‌کند تا بدون ترس از شناسایی یا پیامدهای قانونی، به بزهکاری بپردازند.

۵. نظریه خنثی‌سازی

نظریه خنثی‌سازی که توسط *سایکز* و *ماتزا*[4] (۱۹۵۷)، معرفی شد، توضیح می‌دهد که افراد چگونه قبل از ارتکاب رفتارهای انحرافی، آنها را توجیه می‌کنند. در زمینه بزهکاری سایبری، مجرمان ممکن است اقدامات خود را با عباراتی مانند «این فقط یک شوخی بود» یا «همه این کار را می‌کنند» توجیه کنند. این توجیهات به آنها اجازه می‌دهد تا مسئولیت شخصی خود را به حداقل رسانده و به اقدامات

[1] Holt & Bossler
[2] Cohen & Felson
[3] Navarro & Jasinski
[4] Sykes & Matza

مضـــر خود ادامه دهند. علاوه بر این، مقصـــر دانســـتن قربانی - مانند این ادعا که «آنها اطلاعات خود را به‌صـــورت عمومی به اشـــتراک گذاشـــتند» - یکی دیگر از روش‌های رایج خنثی‌سازی است که توسط *هندوژا* و *پاتچین* (۲۰۱۳)، شناسایی شـده اسـت. چنین توجیهاتی نقش مهمی در تداوم و گسـترش رفتارهای بزهکاری سایبری دارند.

٦. نظریه فشار عمومی

نظریه فشـــار عمومی که توســـط *رابرت اگنیو*[1] (۱۹۹۲)، توســـعه یافت، اســـتدلال می‌کند افرادی که تحت فشـــارهای روانی یا اجتماعی قرار دارند، بیشـــتر احتمال دارد به رفتارهای انحرافی روی آورند. در مورد بزهکاری ســـایبری، فشـــارهایی مانند طرد اجتماعی، شـــکســـت تحصـــیلی یا تعارضـــات بین‌فردی در دنیای واقعی می‌توانند افراد را به بیان ناامیدی یا خشـــم خود در فضـــای مجازی ســـوق دهند. *پاتچین* و *هندوژا* (۲۰۱۱)، مشـــاهده کردند که بزهکاری ســـایبری اغلب به‌عنوان راهی برای تخلیه احساسات جابه‌جا شده عمل می‌کند، به ویژه در میان نوجوانانی که در مقابله با استرس‌های زندگی غیربرخط خود مشکل دارند.

۷. نظریه فرصت

نظریه فرصـت که توسـط *کلاورد* و *اوهلین*[2] (۱۹۶۰)، مطرح شـد، پیشـنهاد می‌کند که وجود فرصـــت‌ها، ارتکاب جرائم را تســـهیل می‌کند. فضـــای مجازی، با ویژگی‌های منحصر به فردی مانند ناشناس بودن، دسترسی آسان ونبود لحظه‌ای، فرصـت‌های زیادی را برای وقوع بزهکاری سـایبری فراهم می‌کند. *یار*[3] (۲۰۰۵)، تأکید کرد که محیط دیجیتال، خطرات مرتبط با رفتارهای انحرافی را کاهش

[1] Robert Agnew
[2] Cloward & Ohlin
[3] Yar

می‌دهد و بزهکاری سایبری را به گزینه‌ای جذاب برای افرادی تبدیل می‌کند که ممکن است در محیط‌های غیربرخط به چنین رفتارهایی دست نزنند.

۸. نظریه هویت اجتماعی

نظریه هویت اجتماعی که توسط *تاژفل و ترنر*[1] (۱۹۷۹)، توسعه یافت، بررسی می‌کند که افراد چگونه احساس ارزشمندی خود را از عضویت در گروه‌ها به‌دست می‌آورند. در زمینه بزهکاری سایبری، افراد ممکن است برای ارتقای جایگاه گروه خود یا تضعیف یک گروه دیگر، به رفتارهای پرخاشگرانه برخط روی آورند. به‌عنوان مثال، بزهکاری برخط ممکن است با هدف دفاع از یک نظریه و بینش خاص یا تقویت سلطه یک گروه اجتماعی خاص انجام شود. *تالوار*[2] و همکاران (۲۰۲۰) بررسی کردند که چگونه چنین پویایی‌های گروهی در شکل‌دهی به رفتارهای بزهکاری سایبری (به‌ویژه در محیط‌های برخط قطبی یا فکری) نقش دارند.

روش

این پژوهش از روش‌شناسی کیفی-کمی و تحلیل محتوا برای بررسی عوامل مؤثر بر بزهکاری سایبری استفاده می‌کند. با انجام این مطالعه، تلاش شده است، مفاهیم و الگوهای مرتبط با بزهکاری سایبری را بهتر درک شوند و راهکارهای مؤثرتری برای پیشگیری و کاهش آن ارائه داده شود. این پژوهش بر روی شهر تبریز، یکی از پرجمعیت‌ترین شهرهای ایران، متمرکز شده است تا این مسئله را بررسی کند. انتخاب این شهر برای مطالعه به‌دلیل تنوع جمعیتی و فرهنگی آن و همچنین تأثیرات متفاوت فناوری اطلاعات بر زندگی روزمره ساکنان آن است. روش نمونه‌گیری هدفمند برای انتخاب مجرمان و قربانیان بزهکاری سایبری استفاده شد. استفاده از نمونه‌گیری هدفمند به‌دلیل در دسترس نبودن به لیست کامل

[1] Tajfel & Turner
[2] Talwar

مجرمان و قربانیان و عدم امکان تعیین احتمال انتخاب هر فرد به‌طور مستقل اجتناب‌ناپذیر بود. این روش نمونه‌گیری امکان انتخاب نمونه‌هایی را فراهم می‌کند که درگیر زورگیری سایبری بوده‌اند، انتخاب شده‌اند.

برای این منظور پرسش‌نامه‌های نیمه‌ساختاریافته طراحی شدند، به این معنی که سؤالات و موضوعات خاصی از پیش تعیین شده بودند، اما به پاسخ‌دهندگان اجازه داده شد تا در طول فرآیند تکمیل پرسش‌نامه به موضوعات دیگر نیز آزادانه بپردازند. این رویکرد اطمینان می‌دهد که داده‌های جمع‌آوری‌شده حاوی اطلاعات غنی و جامعی از تجربیات و دیدگاه‌های پاسخ‌دهندگان باشند. پایایی پرسش‌نامه‌ها با استفاده از آلفای کرونباخ برای کل پرسش‌نامه و برای هر بخش به‌طور جداگانه ارزیابی شد. روایی محتوا و سازه نیز بررسی شدند تا اطمینان حاصل شود که پرسش‌نامه‌ها مفاهیم مورد نظر را به‌درستی اندازه‌گیری می‌کنند. پایایی و روایی بالای پرسش‌نامه‌ها نشان‌می‌دهد که ابزارهای اندازه‌گیری استفاده‌شده در این مطالعه از کیفیت مناسبی برخوردار هستند. ضریب آلفای کرونباخ ۰/۷۳ نشان‌دهنده همسانی درونی بالای پرسش‌نامه است که به اعتبار نتایج کمک می‌کند. علاوه بر این، بررسی روایی محتوا و سازه اطمینان می‌دهد که پرسش‌نامه‌ها به‌طور مناسب مفاهیم مورد نظر را پوشش داده و اندازه‌گیری می‌کنند.

پس از جمع‌آوری داده‌ها، مراحل شامل کدگذاری داده‌ها، تفسیر و استخراج الگوها بود که با هدف شناسایی جنبه‌های کلیدی و مهم مؤلفه‌های جرم‌شناختی بزهکاری سایبری انجام شد. هدف از این مرحله دستیابی به نتایج قابل‌اعتماد و مؤثر است که می‌تواند به نظریه‌پردازی و درک بهتر مفاهیم جرم‌شناختی بزهکاری سایبری کمک کند. در این مطالعه، داده‌های جمع‌آوری‌شده از طریق پرسش‌نامه‌ها از مجرمان و قربانیان بزهکاری سایبری با استفاده از نرم‌افزار SPSS

و تحلیل عاملی مورد بررسی قرار گرفتند. تحلیل عاملی امکان شناسایی و محاسبه الگوها یا ساختارهای پنهان در داده‌ها را فراهم می‌کند و به تحلیل روابط پیچیده بین متغیرها، شناسایی ابعاد گوناگون موضوع یا کشف عوامل مهم پشت داده‌ها کمک می‌کند. کلیه محاسبات آماری این پژوهش با نرم‌افزار SPSS نسخه ۲۵ انجام شده است.

ویژگی‌های جمعیت‌شناختی

در مجموع، ۹۵ فرد (مجرمان و قربانیان) مصاحبه شدند که بر روی جرائم مرتبط با بزهکاری سایبری متمرکز بود، شامل ۵۴ مجرم و ۴۱ قربانی. از میان ۴۱ قربانی، ۱۹ زن و ۲۲ مرد بودند، در حالی که از میان ۵۴ مجرم، ۴۵ مرد و ۹ زن بودند. این یافته نشان می‌دهند که تفاوت معناداری در قربانی‌شدن بین مردان و زنان وجود ندارد، اما در مورد مجرمان تفاوت معناداری وجود دارد، به‌طوری که مردان بیشتر احتمال دارد مرتکب بزهکاری سایبری شوند.

تعداد مردان در نمونه ۲۲ نفر (۵۳/۶۶ درصد) و تعداد زنان ۱۹ نفر (۴۶/۳۴ درصد) بود. حداقل سن برای هر دو جنسیت ۱۹ سال بود، اما حداکثر سن برای مردان ۷۱ سال و برای زنان ۵۶ سال بود که نشان‌می‌دهد مردان مسن‌تری در مطالعه حضور داشتند. میانگین سن مردان ۳۶/۲۳ سال و میانگین سن زنان ۳۶/۱۶ سال بود که توزیع سنی مشابهی بین دو جنسیت را نشان‌می‌دهد. انحراف معیار سن مردان ۱۱/۳۹ و انحراف معیار سن زنان ۱۰/۶۶ بود که نشان‌دهنده پراکندگی سنی بیشتر در میان مردان است.

بررسی وضعیت تحصیلی قربانیان و مجرمان بزهکاری سایبری تفاوت‌هایی در سطح تحصیلات بین دو گروه را نشان‌می‌دهد. از میان موارد بررسی‌شده، حدود ۳۹ درصد از قربانیان دارای تحصیلات دانشگاهی بودند، در حالی که ۶۱ درصد دیپلم یا کمتر داشتند. برای مجرمان، ۶۸/۵ درصد دارای تحصیلات دانشگاهی و ۳۱/۵ درصد دیپلم یا کمتر داشتند. سطح تحصیلات بالاتر در میان مجرمان بزهکاری سایبری در مقایسه با

جرائم سنتی، که اغلب توسط افراد با سطح تحصیلات پایین‌تر انجام می‌شد، قابل توجه است.

بررسی وضعیت تحصیلی والدین قربانیان و مجرمان بزهکاری سایبری نشان‌می‌دهد که ۱۷/۱ درصد از پدران قربانیان بی‌سواد، ۷/۳ درصد دارای مدرک لیسانس، ۲۹/۳ درصد دیپلم و ۴۶/۳ درصد کمتر از دیپلم داشتند. برای مادران قربانیان، ۳۴/۱ درصد بی‌سواد، ۷/۳ درصد دارای مدرک لیسانس، ۱۹/۵ درصد دیپلم و ۳۹ درصد کمتر از دیپلم داشتند. تحلیل جنسیت و تحصیلات پدران قربانیان نشان‌می‌دهد که پدران هر دو جنس قربانیان عمدتاً کمتر از دیپلم داشتند. این موضوع نشان‌می‌دهد که سطح تحصیلات پدر تأثیر مستقیم کمتری بر قربانی‌شدن فرزندان دارد. تحلیل جنسیت و تحصیلات مادران قربانیان نشان‌می‌دهد که اکثریت مادران هر دو جنس قربانیان کمتر از دیپلم داشتند. با این حال، زنان بیشتر مادرانی با تحصیلات بی‌سواد داشتند. این موضوع نشان‌می‌دهد که دسترسی به تحصیلات برای مادران زنان کمتر است و ممکن است تأثیر منفی بر تجربه قربانی‌شدن آن‌ها داشته باشد.

وضعیت اقتصادی تأثیر قابل توجهی بر تجربه قربانی‌شدن دارد. ارزیابی وضعیت اقتصادی قربانیان نشان‌می‌دهد که ۶۳/۴ درصد از قربانیان بزهکاری سایبری در شرایط اقتصادی بدی قرار دارند. در میان مجرمان، ۲۷/۸ درصد در شرایط اقتصادی متوسط و ۲۹/۶ درصد در شرایط بد قرار داشتند. در واقع، مجرمان از طبقات متوسط و پایین جامعه هستند.

بررسی وضعیت تأهل در میان قربانیان نشان‌می‌دهد که ۶۳/۴ درصد از قربانیان متأهل و ۳۶/۶ درصد مجرد بودند. در میان مجرمان، ۷۰/۴ درصد متأهل و ۳۹/۶ درصد مجرد بودند. در مورد وضعیت تأهل، مشاهده می‌شود که نسبت افراد متأهل در هر دو گروه بیشتر از افراد مجرد است. این یافته ممکن است نشان‌دهنده این باشد که مجرمان از

موقعیت اجتماعی افراد متأهل سوء استفاده می‌کنند و موقعیت اجتماعی افراد متأهل می‌تواند برای آن‌ها هزینه‌بر باشد.

کیفیت رابطه بین بزهکار و بزه‌دیده می‌تواند نقش مهمی در وقوع بزهکاری سایبری ایفا کند. یافته‌های این تحقیق نشان‌می‌دهد که در ۸۷ درصد موارد، بزهکاران پیشینه آشنایی با بزه‌دیده داشته‌اند، در حالی که تنها در ۱۳ درصد موارد، هیچ‌گونه ارتباط قبلی بین بزهکار و بزه‌دیده مشاهده نشده است. این نتایج حاکی از آن است که آشنایی قبلی بین بزهکار و بزه‌دیده ممکن است به‌عنوان یک عامل تسهیل‌کننده در بروز بزهکاری سایبری عمل کند.

یافته‌ها

تحلیل کیفی مصاحبه‌ها با بزه‌دیدگان سایبری

با کدگذاری مصاحبه‌ها عوامل بزه‌دیدگی سایبری شناسایی شد. این عوامل عبارتند از: ضعف خودکنترلی، وابستگی به شبکه‌های اجتماعی، فشار همسالان، نداشتن مهارت‌های ارتباطی مؤثر، تمایل به تأیید اجتماعی، نداشتن مهارت‌های حل تعارض، تقلید از رفتارهای پرخطر، نداشتن مهارت‌های تصمیم‌گیری، نداشتن مهارت‌های مدیریت زمان، نداشتن مهارت‌های انتقادی، نداشتن مهارت‌های همدلی، نداشتن مهارت‌های مدیریت استرس، نداشتن مهارت‌های خودمراقبتی، نداشتن مهارت‌های تنظیم هیجانات، نداشتن مهارت‌های کار تیمی، نداشتن مهارت‌های مدیریت حریم خصوصی، نداشتن مهارت‌های مدیریت اطلاعات، نداشتن مهارت‌های مدیریت هویت دیجیتال، نداشتن مهارت‌های مدیریت تعاملات اجتماعی، نداشتن مهارت‌های مدیریت ریسک، نداشتن مهارت‌های مدیریت اعتبار دیجیتال، نداشتن مهارت‌های مدیریت تعارضات دیجیتال، نداشتن مهارت‌های مدیریت زمان برخط، نداشتن مهارت‌های مدیریت محتوای دیجیتال و نداشتن مهارت‌های مدیریت ارتباطات دیجیتال، تنش‌های خانوادگی، مشغله والدین.

تحلیل عامل اکتشافی عوامل مرتبط با بزه‌دیدگی سایبری

در ادامه به‌منظور بررسی تعداد عامل‌های سازنده مقیاس، از تحلیل عامل اکتشافی به شیوه تحلیل مؤلفه‌های اصلی استفاده شد. مقدار شاخص کفایت نمونه‌گیری (KMO) برابر با ۰/۹۱ بود که این مقدار نشان داد که نمونه حاضر از کفایت و بسندگی مطلوبی برای تحلیل برخوردار است. همچنین، آزمون کرویت بارتلت از لحاظ آماری معنی‌دار بود (χ^2=۲۸۲۲/۲۸، p=۰/۰۰۱) که این مقدار نشان‌دهنده آن است امکان انجام تحلیل عاملی اکتشافی روی داده‌های پژوهش وجود دارد. به‌منظور چرخش عامل‌ها از روش متعامد واریماکس استفاده شد و گویه‌هایی زیر عنوان یک عامل حفظ شدند که وزن عاملی آنها از ۰/۴ بیشتر بود. درمجموع، شش مؤلفه، ارزش ویژه بالاتر از یک داشت که در مجموع ۶۹/۹۹ درصد از واریانس کل را تبیین می‌کرد. در ادامه در جدول شماره (۱)، میزان واریانس تبیین شده توسط عوامل استخراج‌شده در تحلیل عامل اکتشافی آورده شده است.

جدول (۱): واریانس تبیین شده توسط عوامل استخراج‌شده

عامل	واریانس توضیح داده شده	نسبت واریانس توضیح داده شده
عامل ۱	۲/۱۷	۱۸/۲۴
عامل ۲	۱/۸۲	۱۵/۲۹
عامل ۳	۱/۵۳	۱۲/۸۷
عامل ۴	۱/۲۲	۹/۶۸
عامل ۵	۱/۰۷	۷/۲۳
عامل ۶	۱/۰۱	۶/۸۶

این جدول نتایج تحلیل عاملی را نشان‌می‌دهد که در آن سهم هر عامل از واریانس کل داده‌ها بررسی شده است. عامل ۱ با واریانس توضیح‌داده‌شده‌ی ۲/۱۷ و سهم ۱۸/۲۴ بیشترین تأثیر را دارد. به‌ترتیب عوامل ۲ تا ۶ سهم کم‌تری از واریانس را توضیح

می‌دهند، به‌طوری که عامل ۶ با واریانس ۱/۰۱ و سهم ۶/۸۶ درصد کم‌ترین تأثیر را دارد.

با تحلیل و بررسی گویه‌ها، عامل اول، خودکنترلی، عامل دوم، میزان و چگونگی استفاده از شبکه‌های اجتماعی و اینترنت، عامل سوم، روابط و تعاملات اجتماعی برخط، عامل چهارم، تجربه و پاسخ به بزهکاری سایبری، عامل پنجم، نظارت و کنترل والدین و عامل ششم، پوشش و ارائه اطلاعات شخصی نام گرفت.

میزان پیش‌بینی‌پذیری بزه‌دیدگی سایبری براساس عوامل استخراج‌شده

در ادامه، به‌منظور پیش بینی بزه‌دیدگی توسط عوامل استخراج‌شده (خودکنترلی، میزان و چگونگی استفاده از شبکه‌های اجتماعی و اینترنت، روابط و تعاملات اجتماعی برخط، تجربه و پاسخ به بزهکاری سایبری، نظارت و کنترل والدین و پوشش و ارائه اطلاعات شخصی) از رگرسیون خطی چندگانه استفاده شد در جدول شماره (۲)، نتایج رگرسیون خطی چندگانه به‌منظور پیش‌بینی بزه‌دیدگی سایبری آورده شده است.

جدول (۲): نتایج رگرسیون خطی چندگانه به‌منظور پیش‌بینی بزه‌دیدگی سایبری

متغیر	ضریب رگرسیون(β)	خطای استاندارد (SE)	مقدارt	سطح معناداری(p-value)
خودکنترلی	۰/۴۵۲	۰/۰۸۷	۵/۱۹	۰/۰۰۰
میزان و چگونگی استفاده از شبکه‌های اجتماعی و اینترنت	۰/۳۲۱	۰/۰۹۵	۳/۳۸	۰/۰۰۱
روابط و تعاملات اجتماعی برخط	۰/۲۸۷	۰/۱۰۲	۲/۸۱	۰/۰۰۵
تجربه و پاسخ به بزهکاری سایبری	۰/۱۵۶	۰/۰۷۶	۲/۰۵	۰/۰۳۵
نظارت و کنترل والدین	۰/۱۲۳	۰/۰۵۵	۲/۲۴	۰/۰۲۶

متغیر	ضریب رگرسیون(β)	خطای استاندارد (SE)	مقدارt	سطح معناداری(p-value)
پوشش و ارائه اطلاعات شخصی	۰/۰۸۹	۰/۰۴۲	۲/۱۲	۰/۰۳۴
ثابت	۱/۲۳۴	۰/۲۱۲	۵/۸۲	۰/۰۰۰

همان‌طور که در جدول شماره (۲)، دیده می‌شود، سطح معنادار همه متغیرها کمتر از ۰/۰۵ است بنابراین هر شش متغیر به‌طور معناداری بزه‌دیدگی سایبری را پیش‌بینی می‌کنند.

تحلیل کیفی مصاحبه‌ها با بزهکاران سایبری

با کدگذاری مصاحبه‌ها عوامل بزهکاری سایبری شناسایی شد. این عوامل عبارتند از: عدم درگیری اخلاقی، تغییر ارزش‌ها، فشار عمومی، میزان بازدارندگی پایین، گمنامی، یادگیری اجتماعی، ضعف خودکنترلی، وابستگی به شبکه‌های اجتماعی، فشار همسالان، نداشتن مهارت‌های ارتباطی مؤثر، تمایل به تأیید اجتماعی، نداشتن مهارت‌های حل تعارض، تقلید از رفتارهای پرخطر، نداشتن مهارت‌های تصمیم‌گیری، نداشتن مهارت‌های مدیریت زمان، نداشتن مهارت‌های انتقادی، نداشتن مهارت‌های همدلی، نداشتن مهارت‌های مدیریت استرس، نداشتن مهارت‌های خودمراقبتی و نداشتن مهارت‌های تنظیم هیجانات.

تحلیل عامل اکتشافی عوامل مرتبط با بزهکاری سایبری

در ادامه به‌منظور بررسی تعداد عامل‌های سازنده مقیاس، از تحلیل عامل اکتشافی به شیوه تحلیل مؤلفه‌های اصلی استفاده شد. مقدار شاخص کفایت نمونه‌گیری (KMO) برابر با ۰/۸۸ بود که این مقدار نشان داد که نمونه حاضر از کفایت و بسندگی مطلوبی برای تحلیل برخوردار است. همچنین، آزمون کرویت بارتلت از لحاظ آماری معنی‌دار بود (χ^2=۲۵۸۹/۲۲، p=۰/۰۰۱) که این مقدار نشان‌دهنده آن است امکان انجام تحلیل

عاملی اکتشـــافی روی داده‌های پژوهش وجود دارد. به‌منظور چرخش عامل‌ها از روش متعامد واریماکس استفاده شـد و گویه‌هایی زیر عنوان یک عامل حفظ شـدند که وزن عاملی آنها از ۰/۴ بیشـتر بود. درمجموع، شـش مؤلفه، ارزش ویژه بالاتر از یک داشـت که درمجموع ۶۶/۵۲ درصد از واریانس کل را تبیین می‌کرد. در ادامه در جدول شماره (۳)، میزان واریانس تبیین شـده توسـط عوامل اسـتخراج‌شـده در تحلیل عامل اکتشـافی آورده شده است.

جدول (۳): واریانس تبیین شده توسط عوامل استخراج‌شده

عامل	واریانس توضیح داده شده	نسبت واریانس توضیح داده شده
عامل ۱	۱/۹۱	۱۶/۲۹
عامل ۲	۱/۶۲	۱۴/۲۹
عامل ۳	۱/۲۷	۱۱/۸۷
عامل ۴	۱/۱۲	۹/۶۸
عامل ۵	۱/۰۷	۷/۷۳
عامل ۶	۱/۰۲	۶/۶۶

این جدول نتایج تحلیل عاملی را نشان‌می‌دهد که در آن سـهم هر عامل از واریانس کل داده‌ها بررسـی شـده اسـت. عامل ۱ با واریانس توضیح‌داده‌شـده‌ی ۱/۹۱ و سـهم ۱۶/۲۹ بیشـــترین تأثیر را دارد. به‌ترتیب عوامل ۲ تا ۶ ســـهم کم‌تری از واریانس را توضـــیح می‌دهند، به‌طوری که عامل ۶ با واریانس ۱/۰۲ و ســـهم ۶/۶۶ درصـــد کم‌ترین تأثیر را دارد.

با تحلیل و بررسی گویه‌ها، عامل اول، عدم درگیری اخلاقی، عامل دوم، تغییر ارزش‌ها، عامل سوم، فشار عمومی، عامل چهارم، میزان بازدارندگی، عامل پنجم، گمنامی و عامل ششم، یادگیری اجتماعی نام گرفت.

میزان پیش‌بینی‌پذیری بزهکاری سایبری براساس عوامل استخراج‌شده

در ادامه، به‌منظور پیش بینی بزهکاری توسط عوامل استخراج‌شده (عدم درگیری اخلاقی، تغییر ارزش‌ها، فشار عمومی، میزان بازدارندگی، گمنامی و یادگیری اجتماعی) از رگرسیون خطی چندگانه استفاده شد در جدول شماره (۴)، نتایج رگرسیون خطی چندگانه به‌منظور پیش‌بینی بزهکاری سایبری آورده شده است.

جدول (٤): نتایج رگرسیون خطی چندگانه به‌منظور پیش‌بینی بزهکاری سایبری

متغیر	ضریب رگرسیون (β)	خطای استاندارد (SE)	مقدار t	سطح معناداری (p-value)
عدم درگیری اخلاقی	۰/۵۶۷	۰/۱۲۳	۳/۴۵	۰/۰۰۲
تغییر ارزش‌ها	۰/۴۳۲	۰/۱۵۶	۴/۲۲	۰/۰۰۳
فشار عمومی	۰/۳۲۱	۰/۰۸۹	۱/۹۸	۰/۰۰۴
میزان بازدارندگی	۰/۲۳۴	۰/۰۴۵	۲/۷۶	۰/۰۱۵
گمنامی	۰/۱۹۸	۰/۰۶۷	۲/۳۳	۰/۰۲۸
یادگیری اجتماعی	۰/۱۷۶	۰/۰۷۸	۲/۱۱	۰/۰۳۹

همان‌طور که در جدول (۴)، دیده می‌شود، سطح معنادار همه متغیرها کمتر از ۰/۰۵ است، بنابراین هر شش متغیر به‌طور معناداری بزهکاری سایبری را پیش‌بینی می‌کنند.

بحث و نتیجه‌گیری

اینترنت به بخشی جدایی‌ناپذیر از زندگی مدرن تبدیل شده و نحوه تعامل، کار و دسترسی افراد به اطلاعات را دگرگون کرده است (جوشی[1] و همکاران، ۲۰۲۲). با وجود مزایای فراوان، اینترنت کاربران را در معرض خطرات قابل توجهی مانند بزهکاری سایبری قرار می‌دهد (کیم و همکاران، ۲۰۲۳)؛ این مسئله پیامدهای روانی و

[1] Joshi

اجتماعی عمیقی دارد. این پژوهش به بررسی ابعاد جرم‌شناختی بزهکاری سایبری در شهر تبریز می‌پردازد و بر علل، پیامدها و راهکارهای مقابله با آن تمرکز دارد. با تلفیق چارچوب‌های نظری و داده‌های تجربی، این مطالعه در پی دستیابی به درک عمیق‌تری از بزه‌دیدگی و بزهکاری سایبری و ارائه راهکارهای پیشگیری مؤثر است.

در بخش اول بزه‌دیدگی سایبری بررسی شد. یافته‌های این مطالعه نشان‌می‌دهد که بزه‌دیدگی سایبری تحت‌تأثیر تعامل پیچیده‌ای از عوامل فردی، اجتماعی و محیطی قرار دارد. عوامل اصلی مؤثر بر بزه‌دیدگی سایبری شامل خودکنترلی، میزان و چگونگی استفاده از شبکه‌های اجتماعی و اینترنت، روابط و تعاملات اجتماعی برخط، تجربه و پاسخ به بزهکاری سایبری، نظارت و کنترل والدین و پوشش و ارائه اطلاعات شخصی است. این یافته‌ها با پژوهش *همفیل* و همکاران (۲۰۱۵) و فیروزچیان و همکاران (۱۴۰۱) همسو است. در تبیین این یافته‌ها می‌توان گفت، تعاملات اجتماعی در فضای برخط، در صورت عدم آگاهی یا اتخاذ تدابیر حفاظتی، آسیب‌پذیری افراد نسبت به جرائم سایبری را افزایش می‌دهد. علاوه بر این، عواملی مانند ناشناس بودن در فضای سایبری، کاهش مسئولیت‌پذیری اخلاقی و تغییر ارزش‌های اجتماعی، افراد بزهکار را به سوءاستفاده از قربانیان ترغیب می‌کند. ناشناس بودن، خطر شناسایی و مجازات را کاهش داده و محیطی مناسب برای رفتارهای آسیب‌رسان ایجاد می‌کند. یادگیری اجتماعی و تقلید از رفتارهای مشاهده‌شده در فضای برخط نیز به‌طور قابل‌توجهی در بزه‌دیدگی و ارتکاب جرائم سایبری نقش دارند.

نتایج این مطالعه بر اهمیت راهبردهای پیشگیری هدفمند برای کاهش خطرات مرتبط با بزه‌دیدگی سایبری تأکید می‌کند. آموزش سواد دیجیتال، ترویج رفتار مسئولانه در فضای برخط و افزایش آگاهی در مورد تنظیمات حریم خصوصی و شیوه‌های ایمن برخط، گام‌های حیاتی هستند. علاوه بر این، نظارت و راهنمایی والدین نقش مهمی در حفاظت از افراد آسیب‌پذیر، به‌ویژه نوجوانان، در برابر تهدیدات سایبری ایفا می‌کند. از

منظر سیاست‌گذاری، وضع قوانین سخت‌گیرانه‌تر، افزایش مجازات برای جرائم سایبری و تقویت سازوکارهای اجرایی برای بازدارندگی مجرمان ضروری است. همچنین، باید ابتکاراتی برای ترویج رفتار اخلاقی در فضای مجازی و اصلاح نگرش‌های اجتماعی نسبت به تعاملات دیجیتال در اولویت قرار گیرند. به‌طور کلی، این مطالعه بر ضرورت رویکردی چندبعدی شامل مداخلات فردی، اجتماعی و قانونی برای مقابله با مسئله فزاینده بزه‌دیدگی سایبری تأکید دارد. تحقیقات آینده باید برنامه‌های پیشگیری اختصاصی را بررسی کرده و اثربخشی آن‌ها را در زمینه‌های مختلف ارزیابی کنند. این تلاش‌ها می‌تواند به ایجاد محیط‌های دیجیتال امن‌تر و کاهش شیوع بزه‌دیدگی سایبری در جامعه کمک کند.

در بخش دوم به بزهکاری سایبری پرداخته شد. بزهکاری سایبری در چارچوب نظریه‌های جرم‌شناختی مانند نظریه هم‌نشینی افتراقی (ساترلند، ۱۹۷۴)، نظریه فعالیت روزمره (کوهن و فلسون، ۱۹۷۹) و نظریه فرصت (کلاورد و اوهلین، ۱۹۶۰) به‌طور گسترده‌ای مطالعه شده است. نظریه هم‌نشینی افتراقی بیان می‌کند که افراد از طریق مشاهده و تقلید، رفتارهای مجرمانه را یاد می‌گیرند (ساترلند، ۱۹۷۴)، در حالی که نظریه فعالیت روزمره بر همگرایی بزهکاران دارای انگیزه، اهداف مناسب و عدم وجود محافظان توانمند در فضای سایبر تأکید می‌کند (کوهن و فلسون، ۱۹۷۹). از سوی دیگر، نظریه فرصت نشان‌می‌دهد که افراد به‌دلیل ناشناس بودن و کاهش کنترل‌های اجتماعی در فضای سایبری، رفتار متفاوتی از خود نشان می‌دهند (کلاورد و اوهلین، ۱۹۶۰). یافته‌های این پژوهش با پژوهش‌های *ژانگ* و همکاران (۲۰۱۶) و جاه‌بین و همکاران (۱۳۹۷) همسو است. این پژوهش با یافته‌های تحقیقات پیشین نقش عواملی مانند ناشناس بودن، کنترل پایین خود و عدم درگیری اخلاقی را در افزایش

بزهکاری سایبری برجسته کرده‌اند (کوالسکی[1] و همکاران، ۲۰۱۲؛ لی[2] و همکاران، ۲۰۲۳) نیز همسو است.

مطالعات کمی به بررسی این عوامل در زمینه‌های غیرغربی، به‌ویژه در ایران، پرداخته‌اند. در این مطالعه با بررسی بزهکاری سایبری در تبریز، سعی شده است، این شکاف پژوهشی را پر شود. یافته‌ها بینش‌های مهمی در مورد پویایی‌های بزهکاری سایبری در تبریز ارائه می‌دهند. اولاً، ویژگی‌های جمعیت‌شناختی نقش مهمی در شکل‌دهی آسیب‌پذیری و رفتار بزهکارانه ایفا می‌کنند. اگرچه رابطه معناداری بین جنسیت و قربانی‌شدن یافت نشد، مردان بیشتر از زنان مرتکب رفتارهای بزهکاری سایبری می‌شدند. قربانیان معمولاً سطح تحصیلات پایین‌تری داشتند، در حالی که بزهکاران اغلب از سطح تحصیلات بالاتری برخوردار بودند که نشان‌دهنده نقش سواد دیجیتال در تسهیل بزهکاری سایبری است. علاوه بر این، قربانیان عمدتاً از خانواده‌های کم‌درآمد بودند که نشان‌می‌دهد آسیب‌پذیری اقتصادی ممکن است حساسیت به بزهکاری سایبری را افزایش دهد. عوامل رفتاری و روان‌شناختی نیز به‌عنوان پیش‌بین‌های مهم شناسایی شدند. به‌عنوان مثال، ناشناس بودن به‌عنوان محرک اصلی بزهکاری سایبری عمل می‌کند، زیرا پاسخ‌گویی را کاهش داده و احتمال رفتارهای پرخاشگرانه را افزایش می‌دهد. کنترل پایین خود، که با نظریه عمومی جرم *گاتفریدسون و هیرشی*[3] (۱۹۹۰)، همسو است، ارتباط قوی با بزهکاری سایبری داشت، در حالی که جدایی اخلاقی به بزهکاران اجازه می‌داد با کم‌اهمیت‌کردن آسیب یا سرزنش قربانی، اقدامات خود را توجیه کنند. عوامل اجتماعی و محیطی، مانند یادگیری اجتماعی و انتخاب سبک‌زندگی، نیز بر پویایی‌های بزهکاری سایبری تأثیرگذار بودند. بسیاری از بزهکاران گزارش دادند که رفتارهای بزهکاری سایبری را از همسالان یا

[1] Kowalski
[2] Li
[3] Gottfredson & Hirschi

جوامع برخط یاد گرفته‌اند، در حالی که قربانیانی با سبک‌زندگی برخط ماجراجویانه‌تر و کنجکاوتر – مانند استفاده مکرر از شبکه‌های اجتماعی و تعامل با غریبه‌ها – در معرض خطر بیشتری برای قربانی‌شدن بودند (قائمی و همکاران، ۱۴۰۳).

همچنین، تحلیل نقش ساختارهای فرهنگی و اجتماعی در بروز و پیشگیری از بزهکاری سایبری می‌تواند درک بهتری از این پدیده فراهم آورد. هنجارهای فرهنگی، ارزش‌های اجتماعی و سطح اعتماد عمومی در یک جامعه می‌توانند تأثیر مستقیمی بر میزان پذیرش یا طرد رفتارهای بزهکارانه در فضای مجازی داشته باشند. در جوامعی که پیوندهای اجتماعی قوی‌تر و نظارت اجتماعی بیشتری وجود دارد، افراد کمتر به رفتارهای پرخطر سایبری روی می‌آورند (کریس[1] و همکاران، ۲۰۲۱). از سوی دیگر، در جوامعی با ساختارهای اجتماعی شکننده و سطوح پایین سرمایه اجتماعی، احتمال وقوع بزهکاری سایبری افزایش می‌یابد (بویانیچ[2] و همکاران، ۲۰۲۲). این موضوع نشان‌می‌دهد که برای مقابله مؤثر با بزهکاری سایبری، باید علاوه بر اقدامات قانونی و فناورانه، به تقویت سرمایه اجتماعی، آموزش‌های فرهنگی و ارتقای آگاهی عمومی نیز توجه ویژه‌ای شود. در کنار عوامل فردی و اجتماعی، نقش نهادهای آموزشی و رسانه‌ها در پیشگیری از بزهکاری سایبری غیرقابل‌انکار است. مدارس و دانشگاه‌ها می‌توانند با گنجاندن آموزش‌های مرتبط با سواد دیجیتال، ایمنی در فضای مجازی و حقوق سایبری در برنامه‌های درسی، آگاهی نسل جوان را نسبت به تهدیدات سایبری افزایش دهند (الثبیانی و الزهرانی[3]، ۲۰۲۳). این آموزش‌ها باید فراتر از مهارت‌های فنی بوده و شامل پرورش تفکر انتقادی، مسئولیت‌پذیری برخط و مدیریت رفتارهای پرخطر در فضای مجازی باشد. علاوه بر این، رسانه‌های جمعی با تولید و پخش محتواهای آموزشی و آگاهی‌بخش می‌توانند نقش مؤثری در تغییر نگرش عمومی نسبت به خطرات بزهکاری

[1] Creese
[2] Bojanić
[3] Althibyani & Al-Zahrani

سایبری ایفا کنند (بله و همکاران، ۲۰۱۴). بهره‌گیری از ظرفیت رسانه‌های اجتماعی برای اجرای کمپین‌های اطلاع‌رسانی، به‌ویژه در میان گروه‌های سنی جوان، می‌تواند به کاهش آسیب‌پذیری کاربران و ترویج رفتارهای مسئولانه در فضای برخط کمک کند. کاربردهای عملی این یافته‌ها گسترده و چندوجهی هستند. برنامه‌های آموزشی و ابتکارات سواد دیجیتال برای تجهیز افراد به مهارت‌های لازم برای استفاده ایمن از فضای سایبر ضروری هستند. برنامه‌های درسی مدارس باید شامل درس‌هایی درباره شناسایی و پاسخ به بزهکاری سایبری باشد، در حالی که گروه‌های آگاهی‌رسانی عمومی می‌توانند جامعه را درباره خطرات و پیامدهای آزار و اذیت برخط آموزش دهند. برنامه‌های آموزشی برای معلمان و والدین نیز حیاتی هستند، زیرا آن‌ها نقش محوری در شناسایی علائم بزهکاری سایبری و حمایت از قربانیان دارند. اقدامات حقوقی و فنی باید تقویت شوند تا اطمینان حاصل شود که مجازات‌های قطعی و شدید برای جرائم بزهکاری سایبری اعمال می‌شود. این شامل به‌روزرسانی قوانین سایبری برای مقابله با اشکال نوظهور آزار و اذیت برخط و تقویت قابلیت‌های پلیس فتا از طریق ابزارهای نظارتی پیشرفته و سیستم‌های شناسایی کاربران است. مداخلات جامعه‌محور، مانند شبکه‌های حمایتی و همکاری بین مدارس، خانواده‌ها و سازمان‌های محلی، برای ایجاد محیطی حمایتی برای قربانیان و تقویت تاب‌آوری در میان جوانان حیاتی هستند. راه‌حل‌های فناورانه، از جمله ابزارهای نظارتی مبتنی بر هوش مصنوعی و نرم‌افزارهای کنترل والدین، می‌توانند با تشخیص محتوای مضر و امکان نظارت والدین بر فعالیت‌های برخط فرزندان، خطرات بزهکاری سایبری را کاهش دهند.

این یافته‌ها با نظریه‌های جرم‌شناختی موجود همسو هستند و در عین حال عوامل زمینه‌ای منحصربه‌فرد در تبریز را برجسته می‌کنند. به‌عنوان نمونه نقش ناشناس بودن و کنترل پایین خود با تحقیقات پیشین مطابقت دارد، اما تأکید بر سواد دیجیتال به‌عنوان پیش‌بین رفتار بزهکارانه، یک یافته نوآورانه است. نبود وجود رابطه معنادار بین جنسیت و

قربانی‌شدن، برخی مطالعات غربی را به چالش می‌کشد و نشان‌می‌دهد که هنجارهای فرهنگی در ایران ممکن است پویایی‌های بزهکاری سایبری را به‌گونه‌ای متفاوت تحت‌تأثیر قرار دهند. با این حال، این مطالعه بدون محدودیت نیست. اتکا به داده‌های خوداظهاری ممکن است باعث ایجاد سوگیری شود، زیرا شرکت‌کنندگان ممکن است رفتارهای نامطلوب اجتماعی را کمتر گزارش کنند. علاوه بر این، نمونه‌گیری محدود به تبریز ممکن است تعمیم‌پذیری یافته‌ها را تحت‌تأثیر قرار دهد. تحقیقات آینده باید دامنه جغرافیایی را گسترش داده و از داده‌های طولی برای بررسی تغییرات روند بزهکاری سایبری در طول زمان استفاده کنند.

با نگاه به آینده، تحقیقات و تلاش‌های سیاستی باید بر گسترش دامنه جغرافیایی مطالعات برای مقایسه پویایی‌های بزهکاری سایبری در زمینه‌های فرهنگی و اقتصادی مختلف متمرکز شوند. مطالعات طولی برای ردیابی تغییرات روند بزهکاری سایبری در طول زمان و ارزیابی اثربخشی بلندمدت راهبردهای پیشگیری ضروری هستند. تحقیقات بین‌رشته‌ای که بینش‌های جرم‌شناسی، روان‌شناسی، جامعه‌شناسی و علوم رایانه را ترکیب می‌کند، می‌تواند به درک جامع‌تری از بزهکاری سایبری و راه‌حل‌های نوآورانه منجر شود. ارزیابی سیاست‌ها نیز برای شناسایی بهترین روش‌ها و زمینه‌های بهبود در مداخلات موجود حیاتی است. در نهایت، همکاری جهانی بین دولت‌ها، سازمان‌های غیردولتی و شرکت‌های فناوری می‌تواند توسعه استانداردها و ابتکارات بین‌المللی برای مقابله با بزهکاری سایبری در مقیاس بزرگ‌تر را تسهیل کند.

در نتیجه، این مطالعه بینش‌های ارزشمندی در مورد ابعاد جرم‌شناختی بزهکاری سایبری در تبریز ارائه می‌دهد و نقش ناشناس بودن، کنترل خود و یادگیری اجتماعی را در تسهیل چنین رفتارهایی برجسته می‌کند. با تلفیق چارچوب‌های نظری و داده‌های تجربی، این پژوهش به درک عمیق‌تری از بزهکاری سایبری کمک کرده و توصیه‌های عملی برای پیشگیری و مداخله ارائه می‌دهد. با این حال، مقابله با این مسئله پیچیده

نیازمند رویکردی چندوجهی است که آموزش، اقدامات حقوقی، مشارکت جامعه و راه‌حل‌های فناورانه را ترکیب کند. از طریق تلاش‌های مشترک و راهکارهای نوآورانه، ایجاد محیط دیجیتالی امن‌تر و فراگیرتر برای همه امکان‌پذیر است.

پیشنهادهای کاربردی

برای مقابله مؤثر با مسئله بزهکاری سایبری در تبریز، پژوهش ضرورت دارد یافته‌های پژوهشی به راه‌حل‌های عملی و کاربردی تبدیل شوند. بدین‌منظور با همفکری و بحث گروهی با کارشناسان این حوزه که شامل چهار عضو هیئت علمی جامعه‌شناس، سه عضو هیئت علمی روانشناس و دو متخصص جرم شناسی پیشنهادهای زیر رویکردی چندوجهی برای مقابله با بزهکاری سایبری ارائه می‌دهد که بر پیشگیری، مداخله و بهبود سیستم‌ها متناسب با شرایط تبریز متمرکز است.

۱. استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و تحلیل داده‌ها برای پیش‌بینی و پیشگیری از جرائم سایبری

فراجا می‌تواند با به‌کارگیری هوش مصنوعی و تحلیل داده‌های بزرگ، الگوهای جرائم سایبری را شناسایی و رفتارهای مشکوک را پیش‌بینی کند. این فناوری‌ها می‌توانند با ایجاد سیستم‌های هشدار زودهنگام و ردیابی مجرمان، به کاهش جرائم سایبری و افزایش امنیت فضای مجازی کمک کنند.

۲. توسعه سامانه‌های برخط گزارش‌دهی برای تسهیل اطلاع‌رسانی جرائم سایبری توسط قربانیان

ایجاد سامانه‌های برخط برای گزارش جرائم سایبری می‌تواند به شهروندان امکان دهد تا به‌سرعت و بدون نیاز به مراجعه حضوری، جرائم را گزارش کنند. این سامانه‌ها باید کاربرپسند و قابل دسترس باشند و امکان پیگیری وضعیت گزارش‌ها را برای شهروندان فراهم کنند. این اقدام می‌تواند سرعت پاسخ‌گویی به جرائم سایبری را افزایش دهد.

۳. برگزاری کارگاه‌های آموزشی برای شهروندان

فراجا می‌تواند با همکاری سازمان‌های آموزشی و فرهنگی، کارگاه‌های آموزشی درباره امنیت سایبری برای شهروندان تبریز برگزار کند. این کارگاه‌ها باید شامل آموزش‌هایی درباره روش‌های محافظت از اطلاعات شخصی، شناسایی کلاهبرداری‌های اینترنتی و استفاده ایمن از شبکه‌های اجتماعی باشد. این اقدام می‌تواند آگاهی عمومی را افزایش داده و از بزه‌دیدگی سایبری جلوگیری کند.

٤. همکاری با مدارس و دانشگاه‌ها برای آموزش دانش‌آموزان و دانشجویان

فراجا می‌تواند با مدارس و دانشگاه‌های شهر تبریز همکاری کند تا برنامه‌های آموزشی درباره امنیت سایبری را برای دانش‌آموزان و دانشجویان اجرا کند. این برنامه‌ها باید شامل آموزش‌هایی درباره خطرات فضای مجازی، روش‌های محافظت از خود، و پیامدهای بزهکاری سایبری باشد. این اقدام می‌تواند از بزهکاری سایبری در میان جوانان جلوگیری کند.

٥. آگاهی‌بخشی در سطح شهر

فراجا می‌تواند با اجرای تبلیغاتی در سطح شهر تبریز، آگاهی عمومی درباره جرائم سایبری را افزایش دهد. این موارد می‌توانند شامل پوسترها، بنرها، و تبلیغات در شبکه‌های اجتماعی باشند که به شهروندان درباره خطرات فضای مجازی و روش‌های مقابله با آن هشدار می‌دهند. این اقدام می‌تواند به کاهش بزه‌دیدگی و بزهکاری سایبری کمک کند.

در نتیجه، پیشنهادهای عملی ارائه‌شده در بالا نقشه‌ای جامع برای مقابله با بزهکاری سایبری در تبریز فراهم می‌کند. با تمرکز بر آگاهی‌بخشی، اصلاحات قانونی، حمایت از قربانیان، همکاری و بهبود مستمر، این پژوهش می‌تواند به ایجاد محیط دیجیتالی امن‌تر و فراگیرتر برای همه ساکنان کمک کند. این تلاش‌ها نه‌تنها تأثیرات فوری بزهکاری سایبری را کاهش می‌دهد، بلکه تاب‌آوری و رفاه بلندمدت جامعه را نیز تقویت می‌کند.

منابع

۱) بطیاری، عاطفه و شیری ورنامخواستی، عباس. (۱۳۹۷). پیشگیری از بزه‌دیدگی بزهکاری کودکان و نوجوانان از مسیر مداخلات مدرسه‌محور (نگاهی به برنامه SEL). *مطالعات حقوق کیفری و جرم‌شناسی*، ۴۸(۲)، ۳۳۵-۳۵۶.

۲) پیکری، ناصر؛ هزارجریبی، جعفر؛ لک، بهزاد و استرکی، اکبر. (۱۴۰۳). راهبردهای نیروی انتظامی در پیشگیری اجتماعی از بزه‌دیدگی در فضای مجازی. *پژوهش‌های دانش انتظامی*، ۲۶(۲)، ۱—۳۰.

۳) جاه‌بین، زهرا؛ مظفری، افسانه؛ هاشم‌زهی، نوروز و دادگران، سید محمد. (۱۳۹۷). مطالعه کیفی عوامل ارتکاب جرائم در فضای مجازی (تحلیل محتوای کیفی پرونده‌های جرائم سایبری). *مطالعات علوم اجتماعی ایران*، ۱۵(۵۹).

۴) درویشی، صیاد؛ اسداللهی، بهروز و خوش‌نشان، محمود. (۱۴۰۲). راهبردهای پلیس در پیشگیری از بزه‌دیدگی اطفال و نوجوانان با تأکید بر وضعیت‌های مخاطره. *پژوهش‌های دانش انتظامی*، ۲۵(۳)، ۳۶۹—۳۹۷.

۵) رضوی‌فرد، بهزاد و کوره‌پز، حسین‌محمد. (۱۳۹۴). راهبردهای پیش‌گیرانه آموزشی آگاهی‌ساز: ضرورتی پیش روی برنامه‌های کنترل انحرافات سایبری. *کارآگاه*، ۳۲، ۸۴-۱۰۲.

۶) شاه‌محمدی، غلامرضا و رجبی، مصطفی. (۱۳۹۷). تحلیل جرائم اخلاقی فضای سایبر با رویکرد داده‌کاوی. *پژوهش‌های دانش انتظامی*، ۲۰(۴)، ۶۳—۹۱.

۷) شیرافکن، نسرین؛ نصراللهی، حمید؛ حسن‌زاده، رضا و رمضان، مریم. (۱۳۹۹). رابطه اعتیاد به فضای مجازی با بزهکاری سایبری و بی‌موبایل هراسی در

دانشجویان. *فصلنامه فناوری اطلاعات و ارتباطات در علوم‌تربیتی*، ۱۰(۳)، ۱۰۵-۱۲۴.

۸) عطادخت، اکبر و احمدی، شیرین. (۱۴۰۰). طراحی الگوی روابط ساختاری پرخاشگری سایبری بر اساس الگوی ارتباطی خانواده با نقش میانجی اعتیاد به اینترنت. *فصلنامه مدیریت ارتقای سلامت*، ۱۰ (۶)، ۶۶-۵۴.

۹) فیروزجائیان، علی اصغر؛ مؤمنی، فاطمه و نصیری، سپیده. (۱۴۰۱). تحلیل عوامل مؤثر بر قربانی شدن سایبری در میان شهروندان (مورد مطالعه: شهروندان شهر بابل). *راهبرد اجتماعی فرهنگی*، ۱۱ (۳)، ۷۳-۴۰.

۱۰) قاسم تبار، سید امیر؛ قاسم تبار، سید عبدالله و سهرابی، عاطفه. (۱۴۰۰). بزهکاری سایبری: تعریف، تاریخچه و گونه‌شناسی. *جامعه فرهنگ رسانه*، ۱۰(۴۱)، ۱۴۹-۱۷۲.

۱۱) قائمی، علی، واقف، لادن، و شالچی، بهزاد (۱۴۰۲). درستی‌آزمایی و قابلیت اعتماد نسخه فارسی مقیاس کنجکاوی بیمارگونه در دانشجویان. *مجله پزشکی دانشگاه علوم پزشکی تبریز*، ۴۵ (۶)، ۴۸۵-۴۹۴.

۱۲) کامران، اصغر؛ میرمهدی، سید رضا و قاضی سعیدی، زهرا. (۱۴۰۳). تدوین مدل ساختاری قربانی شدن سایبری بر اساس اعتیاد به اینترنت و حمایت اجتماعی ادراک شده با نقش واسطه‌ای ویژگی‌های شخصیتی. *پژوهش‌های روانشناسی اجتماعی*، ۱۴ (۵۵)، ۷۱-۸۶

۱۳) کریم‌زاده، بیاض؛ پورقهرمانی، بابک؛ و بیگی، جمال. (۱۴۰۰). بررسی رابطه بین سرمایه اجتماعی و فرهنگی با گرایش به بزهکاری سایبری. *جامعه‌شناسی*

اقتصادی و توسعه، ۱۰(۱)، ۲۷۱-۲۹۵.

۱۴) محمدی‌مقدم، یوسف، محسنی، فرید و ساعدی، عبدالله. (۱۴۰۱). واکاوی علل مؤثر وقوع جرم در فضای سایبری. *پژوهش‌های دانش انتظامی*، ۲۴(۴)، ۱۷۲-۲۰۳.

15) Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47-88.

16) Asanan, Z. (2017). A Study on Cyberbullying: Its Forms, Awareness, and Moral Reasoning Among Youth. *International Journal of Information and Communication Sciences*, 2, 54.

17) Basu, S., Fernald, J. G., & Shapiro, M. D. (2001). Productivity growth in the 1990s: Technology, utilization, or adjustment? *Carnegie-Rochester Conference Series on Public Policy*, *55*(1), 117–165.

18) Cloward, R. A., & Ohlin, L. E. (1960). Delinquency and Opportunity: A theory of delinquent gangs. Free Press.

19) Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44, 588-608

20) Duby, J.-J. (1991). The evolution of information technologies in the 90s and its impact on applications. *Future Generation Computer Systems*, *7*(1), 15–21.

21) Garbasz, Y. (1997). Flame, wars, flooding, kicking and spamming: Expressions of aggression in the virtual community. Retrieved June, 4, 2002.

22) Gottfredson, M. R., Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

23) Hay, C., Meldrum, R., & Mann, K. (2010). Traditional Bullying, Cyber Bullying, and Deviance: A General

Strain Theory Approach. *Journal of Contemporary Criminal Justice*, 26, 130-147.

24) Hemphill, S. A., Tollit, M., Kotevski, A., & Heerde, J. A. (2015). Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of Australian Secondary School Students. *Journal of interpersonal violence*, 30(15), 2567–2590.

25) Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, 29(2), 129-156.

26) Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of youth and adolescence*, 42(5), 711,722.

27) Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin Press.

28) Hirschi, T. (1969). *Causes of Delinquency*. *United Kingdom:* University of California Press.

29) Holt, Thomas & Bossler, Adam. (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*. 30. 1-25.

30) Jabarian, M., Ghoreyshi Rad, F., & Shalchi, B. (2024). The Relationship Between Internalizing Syndromes and Morbid Curiosity and Cyber Aggression in Adolescents: Cyber Aggression in Adolescents. International Journal of Medical Toxicology and Forensic Medicine, 14(03). https://doi.org/10.32598/ijmtfm.v14i03.44583

31) Joshi, Renu & Nagarajan, Pavithra & Singh, Chintu. (2022). Internet an Integral Part of Human Life in 21 st Century: A Review. *Current Journal of Applied Science and Technology*. 41. 12-18.

32) Kim, M., Ellithorpe, M., & Burt, S. A. (2023). Anonymity and its role in digital aggression: A

systematic review. *Aggression and Violent Behavior*, 72, 101856.

33) Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: A review of the literature on harassment through the internet and other electronic means. *Family Community Health*, 35(2), 107–117.

34) Li, H., Guo, Q., & Hu, P. (2023). Moral disengagement, self-control and callous-unemotional traits as predictors of cyberbullying: A moderated mediation model. *BMC Psychology*, 11(1), 247.

35) Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School psychology international*, 27(2), 157-170.

36) López-Meneses, E., Vázquez-Cano, E., González-Zamar, M. D., & Abad-Segura, E. (2020). Socioeconomic Effects in Cyberbullying: Global Research Trends in the Educational Context. *International journal of environmental research and public health*, 17(12), 4369.

37) Merton, R. K. (1938). Science and the social order. Philosophy of science, 5(3), 321-337.

38) Meter, D. J., & Bauman, S. (2018). Moral disengagement about cyberbullying and parental monitoring: Effects on traditional bullying and victimization via cyberbullying involvement. *The Journal of Early Adolescence*, 38(3), 303-326.

39) Mukred, M., Mokhtar, U. A., Moafa, F., Gumaei, A., Sadiq, A., & Al-Othmani, A. (2024). The roots of digital aggression: Exploring cyber-violence through a systematic literature review. *International Journal of Information Management Data Insights*, 4, 100281. https://doi.org/10.1016/j.jjimei.2024.100281

40) Navarro, Jordana & Jasinski, Jana. (2012). Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum*. 32. 81-94.
41) Semenza D. C. (2021). Gender Differences in the Victim-Offender Relationship for On- and Offline Youth Violence. *Journal of interpersonal violence*, 36(19-20), 9255–9276.
42) Shaojing Sun. Xitaofan, Jianxia D, "Cyberbullying perpetration a meta analysis of gender difference, " *Internatinal Journal of Internet Science*, no. 11 (2016): 62-63.
43) Smith, P. K., Cowie, H., Olafsson, R. F., & Liefooghe, A. P. (2002). Definitions of bullying: A comparison of terms used, and age and gender differences, in a Fourteen–Country international comparison. *Child development*, 73(4), 1119-1133.
44) Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), 664–670.
45) Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), 664–670.
46) Tajfel, H., & Turner, J. C. (1979). *An integrative theory of intergroup conflict.* In W. G. Austin & S. Worchel (Eds.), The social psychology of intergroup relations (pp. 33-37). Monterey, CA: Brooks/Cole.
47) Talwar, P., Gómez-García, G., & Romero-Rodríguez, L. M. (2020). The role of social identity in cyberbullying. *Journal of Social Media in Society*, 9(1), 1-14.
48) Thompsen, P. A. (1994). An episode of flaming: A creative narrative. ETC: *A Review of General Semantics*, 51-72.

49) Turkle, S. (1997). Life on the screen: Identity in the age of the internet. Literature and history, 6, 117-118.
50) UNICEF. (2020). *Cyberbullying: What is it and how to stop it*. Retrieved from https://www.unicef.org/end-violence/cyberbullying-what-is-it-and-how-to-stop-it
51) Warner, D. E., & Raiter, M. (2005). Social Context in Massively-Multiplayer Online Games (MMOGs):: Ethical Questions in Shared Space. *The International Review of Information Ethics*, 4, 46-52.
52) Yar, Majid. (2005). The Novelty of 'Cybercrime'An Assessment in Light of Routine Activity Theory. *European Journal of Criminology - Eurj Criminol.* 2. 407-427.
53) Young, R. M. (1996). NETDYNAM: Some parameters of virtual reality. Online Dokument:: www. shef. ac. uk/-psysc/staff/rmyoung/papers/paper17h. html.
54) Zhang, S., Yu, L., Wakefield, R.L., & Leidner, D.E. (2016). Friend or Foe: *Cyberbullying in Social Network Sites*. Data Base, 47, 51-71.
55) Zhong, J., Zheng, Y., Huang, X., Mo, D., Gong, J., Li, M., & Huang, J. (2021). *Study of the Influencing Factors of Cyberbullying Among Chinese College Students Incorporated With Digital Citizenship*: From the Perspective of Individual Students. Frontiers in psychology, 12, 621418. https://doi.org/10.3389/fpsyg.2021.621418
56) Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capac*ity* building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, *25*(4), 941,955.
57) Bojanić, S., Jonsson, S., Neergaard, A., & Sauer, B. (2022). Challenging cultures of rejection. *Patterns of Prejudice*, 56(4–5), 315–335.

58) Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*, *15*(15), 11512.

59) Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). *Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection*. International Association for the Development of the Information Society.