

تخلفات رایانه‌ای در میان دانشجویان دانشگاه مازندران: آزمون تجربی نظریه یادگیری اجتماعی ایکرز

اکبر علیوردی نیا،* اعظم ملک دار،** محمدرضا حسنی***

(تاریخ دریافت ۹۲/۰۸/۱۱، تاریخ پذیرش ۹۳/۰۷/۲۲)

چکیده: با توجه به گسترش روز افزون رفتارهای انحرافی مرتبط با رایانه و پدید آیی جرایم نوظهور، طیف وسیعی از تهدیدات متوجه افراد و جامعه می‌باشد. تحقیق حاضر با استفاده از نظریه یادگیری اجتماعی ایکرز، در صدد تبیین تخلفات رایانه‌ای دانشجویان دانشگاه مازندران می‌باشد. روش مورد استفاده در این پژوهش، پیمایش و ابزار جمع آوری داده‌ها، پرسش‌نامه می‌باشد. جمعیت این تحقیق شامل کلیه دانشجویان دختر و پسر دانشگاه مازندران در سال تحصیلی ۹۲-۹۱ می‌باشد که ۴۰۳ نفر به روش نمونه گیری طبقه‌ای متناسب با حجم به عنوان نمونه انتخاب شده و مورد مطالعه قرار گرفته‌اند. متغیر تخلفات رایانه‌ای از سه بعد «علیه داده و سیستم»، «جعل هویت» و «فرهنگی» تشکیل شده و متغیرهای مستقل عبارتند از: پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف که تأثیر آن‌ها بر تخلفات رایانه‌ای و ابعاد سه گانه آن بررسی شده است. تحلیل داده‌ها با استفاده از نرم افزار «Spss» و «lisrel» انجام گرفته است. بر اساس نتایج مدل معادلات ساختاری، از میان چهار متغیر یادگیری اجتماعی، متغیر پیوند افتراقی و تقویت افتراقی معنادار بوده و تقویت افتراقی با ضریب رگرسیونی $(\beta = 0/41)$ ، مهمترین تبیین کننده تخلفات رایانه‌ای است.

مفاهیم کلیدی: رفتارهای انحرافی، جرایم نوظهور، تخلفات رایانه‌ای، دانشجویان، نظریه یادگیری اجتماعی.

aliverdinia@umz.ac.ir

* دانشیار جامعه شناسی، دانشگاه مازندران (نویسنده مسئول)

** کارشناس ارشد مطالعات جوانان، دانشگاه مازندران

*** دانشجوی دکتری جامعه شناسی، دانشگاه مازندران

مجله جامعه‌شناسی ایران، دوره پانزدهم، شماره ۲، تابستان ۱۳۹۳، ص ۲۳-۵۶

مقدمه و طرح مسأله

نفوذ فناوری اطلاعات به تمام ابعاد زندگی انسان، رایانه‌ها را به ابزاری مهم در زندگی روزمره تبدیل کرده است و گسترش استفاده از رایانه و اینترنت، بر میزان رفتارهای انحرافی افزوده است (هیندوجا^۱، ۲۰۰۷). رایانه‌ها و شبکه‌های ارتباطی دارای صفات و خصوصیتی هستند که فرصت مناسبی برای انجام رفتارهای انحرافی فراهم می‌کنند. تخلفات و جرایمی که با استفاده از رایانه و تکنولوژی‌های ارتباطی انجام می‌شود، مستلزم استفاده از منابع نسبی کمتری است و افراد با انگیزه‌های مختلف بدون محدودیت سنی و مکانی قادر به انجام این رفتارها می‌باشند. همچنین این دسته از تخلفات و جرایم می‌تواند در فضایی صورت گیرد که افراد در آن حضور فیزیکی ندارند. ناشناس ماندن و گمنامی در فضایی که رایانه و اینترنت فراهم آورده، با کاهش احتمال شناسایی و دستگیری افراد، بر میزان این نوع جرایم و تخلفات افزوده است (وال^۲، ۲۰۰۵).

همزمان با پیشرفت فناوری اطلاعات و ارتباطات، تعداد قابل توجهی از جرایم سنتی به شدت متحول شده و در سطح وسیعی صورت می‌گیرند. از جمله این جرایم و تخلفات می‌توان به کلاهبرداری، سرقت (جوردان و تیلور^۳، ۱۹۹۸)، آزار و اذیت (بوسیج^۴، ۲۰۰۴؛ هالت و باسلر^۵، ۲۰۰۹) و پورنوگرافی (بازل^۶، ۲۰۰۵) اشاره نمود. در کنار تحول جرایم سنتی، جرایم و تخلفات جدیدی ظهور پیدا کرده‌اند که منحصراً با توسعه ارتباطات الکترونیک و اینترنت پدید آمده‌اند که از جمله آن‌ها می‌توان به هک کردن، انتقال ویروس، دسترسی غیرمجاز به اطلاعات دیگران، تکثیر غیر مجاز نرم افزارها (هیگینز^۷، ۲۰۰۵) و تجاوز به حقوق مالکیت معنوی اشاره نمود.

ماهیت پیچیده، متنوع و نوآورانه تخلفات رایانه‌ای سبب شده که اجماعی در یک تعریف واحد از آن وجود نداشته باشد. علاوه بر آن، تفکیک و تمایز میان تخلفات و جرایم رایانه‌ای وجود ندارد؛ بسیاری از رفتارهای انحرافی مرتبط با رایانه و اینترنت مانند انتقال ویروس به سیستم دیگران، دروغ گفتن در فضای مجازی و حدس زدن رمز عبور^۸ دیگران غیر اخلاقی و آسیب زا می‌باشند اما جرم تلقی نمی‌شوند و نمی‌توان آن‌ها را در زمره رفتارهای مجرمانه طبقه بندی کرد، بلکه تخلف محسوب می‌شوند (جوکز، ۲۰۱۰: ۵۲۶). همچنین با توجه به دشواری تفکیک جرایم رایانه‌ای و اینترنتی، این دوگونه از جرایم اغلب بصورت مترادف به کار برده می‌شوند. در نتیجه در توصیف رفتارهای انحرافی مرتبط با رایانه، اصطلاحات مختلفی از قبیل جرم رایانه‌ای، تخلفات رایانه‌ای، جرایم مجازی و جرایم سایبری به جای یکدیگر مورد استفاده قرار می‌گیرند (مک کواد^۹، کواد^۹، ۲۰۰۶). با توجه به این که اصطلاح «تخلفات» وسیع تر و عام تر از مفهوم «جرایم» می‌باشد،

1. Hinduja
2. Wall
3. Jordan & Taylor
4. Bocij
5. Bossler
6. Buzzell
7. Higgins
8. Pass word
9. Mcquade

بدین ترتیب، «تخلفات رایانه‌ای» طیف وسیعی از رفتارهای انحرافی مرتبط با رایانه اعم از جرم و تخلف را در بر می‌گیرد که عبارت است از «فعالیت‌های غیرقانونی و خلاف‌کارانه مبتنی بر رایانه که از طریق کاربرد شبکه جهانی آزاد، تکنولوژی اطلاعات و ارتباطات صورت می‌گیرد» (محسنی، ۱۳۸۶ : ۲۲۳). از جمله شایع‌ترین تخلفات رایانه‌ای می‌توان به استفاده از خدمات تلفنی و اینترنتی بدون پرداخت هزینه^۱، قماربازی^۲ اینترنتی، پول‌شویی، کلاهبرداری از طریق کارت اعتباری^۳، خرید آنلاین کاذب^۴، دسترسی غیرمجاز به اطلاعات شخصی و محرمانه دیگران^۵، دسترسی غیرمجاز به نام کاربری و رمز عبور دیگران، هک کردن^۶، پخش ویروس^۷، سرقت و جعل جعل هویت^۸، نوشته‌ها و عکس‌های مستهجن^۹، آزار و تهدید دیگران از طریق اینترنت، شایعه پراکنی علیه دیگران^{۱۰}، تهدید و ترساندن دیگران^{۱۱}، نقض مالکیت معنوی (کپی رایت): مانند کرک کردن^{۱۲} نرم افزار (شکستن قفل نرم افزار یا تغییر دادن نرم‌افزار به منظور حذف کردن روش‌های حفاظتی آن) و عدم رعایت قانون کپی رایت اشاره نمود.

تخلفات و جرایم رایانه‌ای، طیف وسیعی از خسارات اقتصادی، روانی و احساسی را به همراه دارند. گزارش سازمان بازرسی اروپا^{۱۳} (۱۹۹۸)، حاکی از آن است که میزان جرایمی چون کلاهبرداری، سرقت و هک کردن افزایش قابل توجهی یافته است و این جرایم، خسارات مالی فراوانی را به بار آورده‌اند. سرقت دیجیتالی که شامل تکثیر غیرمجاز نرم افزار، فیلم و موسیقی می‌باشد، میلیاردها دلار خسارت به کمپانی‌ها وارد می‌کند (هیگنز و همکاران، ۲۰۱۲: ۴۱۳)، سالانه میلیون‌ها دلار پول در استفاده از کارت‌های اعتباری در معاملات گم می‌شود و هر روز شاهد افزایش آمار خرید و فروش ابزار جرایم سایبر مانند کدهای مخرب، حملات اینترنتی و حفره‌های امنیتی می‌باشیم (شعاع کاظمی و مؤمنی، ۱۳۹۱: ۷۴)، همچنین آزار و اذیت که به شکل تهدید یا فرستادن پیام‌های جنسی با ایمیل یا از طریق چت روم صورت می‌گیرد، علاوه بر اخاذی، کلاهبرداری و زیان مالی، ترس و اضطراب زیادی را موجب می‌گردد (بوسیچ، ۲۰۰۴؛ وال، ۲۰۰۱). علاوه بر این، محبوبیت شبکه‌های اجتماعی مختلف در فضای مجازی در میان جوانان به آن‌ها اجازه می‌دهد که چنین پیام‌هایی را در مورد دیگران روی صفحه در معرض دید عموم قرار

1. Phreaking
2. Gambling
3. Credit card fraud
4. False purchases online
5. Unauthorized access to information
6. Hacking
7. Purposely given a virus
8. Identity theft
9. Pornography
10. Spreading rumors about person
11. Intimidating fighting another person
12. Crack
13. Uk audit commission

دهند (هیندوجا و پاتچین^۱، ۲۰۰۹) که باعث بی‌آبرویی و خدشه دار شدن آبرو و محبوبیت فرد می‌گردد. هک کردن رایانه‌ها و شکل‌های ساده‌هک کردن شامل حدس زدن رمز عبور و دسترسی به حساب کاربری دیگران بدون اجازه آن‌ها (باسلر و باراس^۲، ۲۰۱۰) که اغلب به نوجوانان و جوانانی نسبت داده می‌شود که وقت خود را صرف جستجو در شبکه‌های رایانه‌ای بدون اجازه از صاحبان آن سیستم‌ها می‌کنند، خسارات مالی و آسیب‌های روانی به همراه می‌آورند (فارنل^۳، ۲۰۰۲؛ یار^۴، ۲۰۰۶). گسترش استفاده از شبکه‌های اجتماعی مجازی در میان جوانان، زمینه‌ساز سوء استفاده از اطلاعات شخصی افراد در پروفایل یا صفحه شخصی آنان توسط افرادی با انگیزه‌های جنسی را فراهم آورده است. تحقیقات حاکی از آن است که از هر سه نفر، یک نفر در معرض پورنوگرافی آنلاین قرار می‌گیرد (ولاک^۵ و همکاران، ۲۰۰۸: ۲۲) و رفتارهایی از قبیل تجربه نامناسب رابطه جنسی با افراد در فضای مجازی، درگیر شدن در تولید و توزیع غیرقانونی برنامه‌هایی با محتوای جنسی و درگیر شدن در یک رابطه فریبکارانه، فرصتی برای بهره‌کشی و سوء استفاده جنسی از افراد فراهم نموده است (برایس^۶، ۲۰۱۰: ۳۲۱). از دیگر آثار جرایم و تخلفات رایانه‌ای می‌توان به تشکیل خرده فرهنگ‌های منحرف، ناهنجاری، تعارض در نقش‌های اجتماعی و اخلال در سازگاری اجتماعی و بحران هویت اشاره نمود. همچنین جرایم و تخلفات رایانه‌ای با حمله به حریم شخصی و محرمانگی اطلاعات شخصی، منجر به کاهش امنیت می‌گردند. شخص ممکن است قربانی سرقت هویت شده و شهرت و آبروی خود را از دست داده و متحمل خسارات جبران ناپذیری از لحاظ مالی، روانی و عاطفی شود.

پژوهش حاضر با تکیه بر نظریه یادگیری اجتماعی ایکرز، در پی بررسی تخلفات رایانه‌ای در میان دانشجویان و عوامل مؤثر بر آن می‌باشد. بررسی این موضوع با رویکرد یادگیری اجتماعی از چند جهت ضروری می‌نماید: اول اینکه، این نظریه دارای مبنای تئوریک و تجربی بوده و مدعی است که نظریه‌ای عمومی و کاربردی در تبیین انواع رفتارهای انحرافی می‌باشد (ایکرز، ۱۹۸۵). در نتیجه برای تبیین و تحلیل رفتارهای انحرافی مرتبط با رایانه نیز مناسب است. دوم اینکه، تخلفات رایانه‌ای در کشور، عمدتاً با دیدگاه حقوقی و قانونی مورد بررسی قرار گرفته‌اند و بیشتر به قوانین موجود و کاستی‌های آن، قربانیان و پیامدهای این نوع تخلفات پرداخته شده است. همچنین، طبق بررسی‌های انجام شده، به نظر می‌رسد تاکنون در کشور، تحقیق تئوریکی به‌ویژه از دیدگاه نظریه یادگیری اجتماعی در این زمینه انجام نشده است، در نتیجه انجام این تحقیق با رویکرد یادگیری اجتماعی، می‌تواند علاوه بر آزمون اعتبار تجربی نظریه، گامی مؤثر در تبیین و تشریح علل تخلفات رایانه‌ای در میان دانشجویان باشد و این شناخت، می‌تواند زمینه‌ای مناسب در تنظیم راه‌کارهای پیشگیرانه از وقوع تخلفات رایانه‌ای فراهم نماید.

1. Patchin
2. Bossler & Burruss
3. Furnell
4. Yar
5. Wolck
6. Bryce

تخلفات رایانه‌ای در ایران

رایانه از اوایل سال ۱۳۴۰ یعنی حدود ۲۲ سال پس از اختراع اولین رایانه، وارد ایران شد. با سیاست‌گذاری و فعالیت نهادهای متولی فناوری اطلاعات و تلاش و سرمایه‌گذاری بخش خصوصی، فناوری اطلاعات در سال‌های اخیر رشد نسبتاً خوبی داشته است. در حال حاضر تقریباً تمام وزارتخانه‌ها و مؤسسات دولتی خصوصاً دانشگاه‌ها و مراکز پژوهشی، بانک‌ها و مؤسسات خصوصی برای انجام بسیاری از امور خود از سیستم‌ها و شبکه‌های رایانه‌ای استفاده می‌کنند. علاوه بر آن، میزان استفاده از رایانه و اینترنت توسط خانواده‌های ایرانی افزایش چشم‌گیری داشته است. در سال‌های اخیر افزایش عضویت جوانان در شبکه‌های مجازی از قبیل کلوب، فیس بوک، توییتر و گوگل پلاس فرصتی برای حضور گسترده جوانان در اینترنت، تسهیل ارتباطات و به اشتراک گذاشتن علائق و تجربیات آنان فراهم آورده است. طبق آمار منتشر شده از سرشماری سال ۱۳۹۰، تعداد کاربران اینترنتی در کشور ۱۱ میلیون و ۲۲۱ هزار و ۸۱۰ نفر و با ضریب نفوذ^۱ ۶۳/۲ درصد است (مرکز آمار ایران، سرشماری عمومی نفوس و مسکن سال ۱۳۹۰) که ۴۰ درصد از کاربران را گروه سنی ۲۰-۲۹ سال تشکیل می‌دهند (خبرگزاری مهر، ۱۳۹۲).

آمار دقیقی در خصوص میزان تخلفات رایانه‌ای و اینترنتی در دست نیست، با این حال، گزارش‌های موجود از مرجع رسیدگی به جرایم رایانه‌ای و اینترنتی در ایران (پلیس فتا) و نیز گزارش‌های منتشر شده از منابع مختلف، نشانگر شیوع تخلفات رایانه‌ای در ایران می‌باشد. مسئولان پلیس فتا، جرایم اینترنتی در ایران را در حال افزایش دانسته است. به استناد گزارش این واحد پلیس، ۸۱ درصد از مجرمین با انگیزه مالی، ۱۳ درصد با انگیزه غیر اخلاقی، ۳ درصد با انگیزه انتقام‌جویی، ۲ درصد با انگیزه سرگرمی و یک درصد با انگیزه‌های دیگر مرتکب جرایم رایانه‌ای شده‌اند. ۹۵ درصد از مرتکبین جرایم رایانه‌ای مرد و در گروه سنی ۱۸ تا ۳۵ سال قرار دارند. برداشت از حساب‌های بانکی و هتک حیثیت مهمترین جرایم رایانه‌ای در ایران اعلام شده و بیشترین میزان جرایم رایانه‌ای به ترتیب در استان‌های تهران، خراسان، گیلان و مازندران بوده است (به نقل از سایت پویا سازان فتاوری اطلاعات، ۱۳۹۱).

در حالی که میزان دقیق تخلفات رایانه‌ای نامشخص و تخمین هزینه این دسته از انحرافات و جرایم در مطالعات مختلف، متفاوت است، اما پژوهش‌های صورت گرفته نشان می‌دهد که انحرافات رایانه‌ای پدیده‌ای مهم و جهانی است (مون و همکاران، ۲۰۱۰) که جامعه ایران نیز از آن مصون نمی‌باشد. با ورود ایران به مدرنیته، همزمان شاهد تحولات وسیعی در عرصه‌های گوناگون هستیم. یکی از تغییرات محسوس در ساختار جامعه، افزایش دانشگاه‌ها می‌باشد. دانشگاه به‌عنوان محیطی اجتماعی که شرایط جامعه‌پذیری را برای افراد فراهم می‌نماید، علاوه بر تسهیل دسترسی افراد به تکنولوژی اطلاعات از قبیل رایانه و اینترنت، شرایط مطلوبی نیز برای یادگیری و ارتکاب تخلفات و جرایم مختلف فراهم می‌نماید. علاوه بر آن، دانشگاه به‌عنوان ابزار کنترل اجتماعی رسمی با قواعد و چارچوب‌های خاص خود، می‌تواند زمینه بروز رفتار انحرافی را فراهم و یا از وقوع و شیوع آن جلوگیری نماید. تردیدی نیست که نسل جوان و نوجوان، بیشتر از دیگر افراد با رایانه و اینترنت سر

۱. درصد افرادی که حداقل یک بار از اینترنت استفاده کرده‌اند.

و کار دارد (جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۳). در نتیجه با توجه به رابطه تنگاتنگ رایانه و اینترنت با زندگی دانشجویی و استفاده بالای دانشجویان از تکنولوژی اطلاعات، این گروه بیشتر مرتکب تخلفات رایانه‌ای می‌شوند و آمارهای موجود، بر این ادعا صحت می‌گذارند. بدین ترتیب، تهدیدات جدی که طیف وسیع این تخلفات، متوجه افراد جامعه می‌دارد، لزوم توجه، بررسی و تبیین آن را ضروری می‌نماید.

مروری بر تحقیقات پیشین

با توجه به بررسی‌های انجام شده، اغلب پژوهش‌های داخلی موجود، با رویکردی حقوقی به جرایم و تخلفات رایانه‌ای پرداخته‌اند. خرم آبادی (۱۳۸۴) در پایان نامه مقطع دکترای خود با عنوان «جرایم فناوری اطلاعات»، طارمی (۱۳۸۷) در مقاله‌ای تحت عنوان «طبقه بندی و آسیب شناسی جرایم رایانه‌ای» با رویکردی حقوقی به انواع جرایم رایانه‌ای، خصوصیات و نیز چالش‌های مربوط به این جرایم می‌پردازند و راهکارهایی را جهت مقابله با این آسیب ارائه داده و به لوایح قانونی موجود در این زمینه و کاستی‌های آن تأکید کرده‌اند. رضوی (۱۳۸۷) در مقاله‌ای با عنوان «پیشگیری انتظامی از جرایم سایبری» و جلالی فراهانی (۱۳۸۳) در مقاله‌ای تحت عنوان «پیشگیری از جرایم رایانه‌ای» به بررسی روش‌های پیشگیری از جرایم رایانه‌ای پرداخته‌اند. صادقی فسائی و محمدی (۱۳۸۴) در مقاله‌ای تحت عنوان «نگاهی جرم‌شناسانه بر جرایم، امنیت و کنترل در اینترنت و آسیب‌های اجتماعی»، راورداد (۱۳۸۴) در مقاله‌اش با عنوان «مسائل اجتماعی زنان در اینترنت»، عبدالهیان (۱۳۸۴) در مقاله‌ای تحت عنوان «نوع شناسی و باز تعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران» و رازقی (۱۳۸۹) در تحقیقی با عنوان «شناخت آسیب‌ها و جرایم اجتماعی در فضای مجازی» از منظر جامعه‌شناختی به بررسی جرایم رایانه‌ای و پیامدهای آن و راهکارهای پیشگیرانه و مبارزه با این جرایم پرداخته‌اند. بررسی‌ها نشانگر آن است که تحقیقات انجام شده در حیطه جامعه‌شناسی محدود بوده و غالباً توصیفی می‌باشد. در میان این تحقیقات، میزان جرایم رایانه‌ای و علل ارتکاب به آن‌ها کمتر مورد بررسی واقع شده است. تحقیقات انجام شده غالباً به روش اسنادی و کتابخانه‌ای انجام شده و فاقد چارچوب نظری بوده‌اند و به نظر می‌رسد تا کنون تخلفات رایانه‌ای در ایران، به‌طور کافی از منظر جامعه‌شناختی و از دیدگاه یادگیری اجتماعی یک‌پارچه به‌طور کلی مورد بررسی واقع نشده است. همچنین در تحقیقات انجام شده تفکیکی میان جرایم و تخلفات رایانه‌ای دیده نشده و همه رفتارهای انحرافی مرتبط با رایانه تحت عنوان جرایم رایانه‌ای مورد بررسی قرار گرفته‌اند. در زمینه تخلفات و جرایم رایانه‌ای، تحقیقات زیادی در خارج از کشور صورت گرفته و مباحث و موضوعات متعددی از قبیل بررسی مجرمان و قربانیان جرایم رایانه‌ای، گرایش به جرایم رایانه‌ای، میزان و انواع جرایم رایانه‌ای مورد بررسی قرار گرفته است. همچنین تنوع دیدگاه‌های روان‌شناختی، حقوقی و جامعه‌شناختی نیز در این زمینه به چشم می‌خورد.

هلینگر^۱ (۱۹۹۲) در تحقیق خود با عنوان «جرم رایانه‌ای: ارتباط سرقت نرم افزاری^۲ و دست‌رسی غیر مجاز به رمز عبور دیگران» از منظر تئوری یادگیری اجتماعی به بررسی مجرمان

1. Hollinger
2. Software Piracy

رایانه‌ای پرداخته است. وی دو نوع از جرایم رایانه‌ای شامل (۱) دانلود، استفاده، تکثیر و پخش غیر مجاز نرم افزار (۲) دسترسی غیرمجاز به رمز عبور سیستم دیگران یا فایل‌ها و اطلاعاتشان را مورد بررسی قرار داده است. در این تحقیق، دو متغیر کلیدی که همبستگی قوی‌ای با جرم‌های رایانه‌ای داشته‌اند، ارتباط با دوستان متخلف و اطمینان از گرفتار شدن است.

اسکینر و فریام (۱۹۹۷) در مقاله‌ای با عنوان «تحلیل نظریه یادگیری اجتماعی از جرایم رایانه‌ای در میان دانشجویان دانشگاه» به بررسی پنج رفتار غیرقانونی رایانه‌ای شامل استفاده عمدی از نرم افزار کپی شده یا کپی کردن نرم افزار بدون اجازه، حدس زدن رمز عبور دیگران برای نفوذ به رایانه آن‌ها یا دسترسی به فایل‌هایشان، دسترسی به رمز ورود رایانه دیگران بدون اجازه یا اطلاع آن‌ها برای نگاه کردن به فایل‌ها یا اطلاعاتشان، اضافه کردن، حذف کردن، تغییر یا پخش هر اطلاعاتی از رایانه دیگران بدون اطلاع یا اجازه آن‌ها و نوشتن برنامه ویروس یا استفاده از برنامه‌ای که به اطلاعات دیگران صدمه بزند پرداخته است. نتایج این تحقیق، نشانگر رابطه معنادار بین میزان پیوند افتراقی، تقویت و تنبیه افتراقی، تعاریف و منابع تقلید با جرم رایانه‌ای بوده است. به عبارت دیگر، طبق یافته‌های این تحقیق، هر چه فرد با دوستانی که مرتکب جرایم رایانه‌ای می‌شوند بیشتر در ارتباط باشد و هرچه بیشتر از محیط اطراف خود از قبیل مدرسه و خانواده این جرایم را یاد بگیرد و نیز هرچه این قبیل رفتارها بیشتر مورد تأیید واقع شوند فرد بیشتر مرتکب این جرایم می‌شود. در این تحقیق، پیوند افتراقی، مهمترین عامل پیش بینی کننده در ارتکاب جرایم رایانه‌ای بوده است.

هیگینز و همکاران (۲۰۰۵) در تحقیقی با عنوان «کاربرد نظریه بازدارندگی^۱ در سرقت نرم افزار» به بررسی نقش تئوری بازدارندگی در کاهش سرقت نرم افزار پرداخته‌اند. متغیرهای مورد بررسی در این تحقیق عبارت است از: شدت و قطعیت مجازات، بازدارندگی اجتماعی شامل مخالفت خانواده و دوستان، بازدارندگی فردی شامل احساس شرم و گناه، قواعد اخلاقی مورد قبول، ارتکاب قبلی به سرقت نرم افزار و ارتباط با دوستان. طبق نتایج این تحقیق، قطعیت مجازات، احساس شرم، مخالفت خانواده و خودکنترلی پایین رابطه منفی و پیوند با دوستان و همسالان رابطه مثبتی با سرقت نرم افزار دارد.

هیگینز و همکاران (۲۰۰۶) در تحقیقی با عنوان «سرقت دیجیتال^۲: ارزیابی سهم نظریه کنترل اجتماعی و یادگیری اجتماعی» به بررسی یکی از انواع جرایم رایانه‌ای تحت عنوان سرقت دیجیتالی می‌پردازند. این تحقیق تأثیر دو نظریه یادگیری اجتماعی و کنترل اجتماعی را بر سرقت دیجیتالی مورد آزمون قرار داده است. طبق یافته‌های این تحقیق، پیوند افتراقی و تعاریف بطور غیرمستقیم با تأثیر بر خودکنترلی پایین، روی سرقت دیجیتالی تأثیر می‌گذارند. این تحقیق، مدلی سه عاملی را تحت عنوان "خودکنترلی پایین ← یادگیری اجتماعی ← سرقت اجتماعی" ارائه نموده است که برای فهم رفتار مجرمانه مدلی کاربردی است. در این مدل، یادگیری اجتماعی به‌عنوان واسطه بین خودکنترلی پایین و سرقت دیجیتال عمل می‌کند. نتایج این تحقیق نشان می‌دهند افرادی که

-
1. Deterrence Theory
 2. Digital Piracy

خودکنترلی پایین داشته باشند و به‌طور اجتماعی سرقت دیجیتال را فراگرفته باشند، بیشتر مرتکب این رفتار مجرمانه می‌شوند.

موریس^۱ و هیگینز (۲۰۰۹) در تحقیق خود با عنوان «تکنیک خنثی سازی^۲ و گزارش سرقت دیجیتال؛ بررسی رویکرد نظری چندگانه میان دانشجویان کارشناسی» به بررسی سرقت دیجیتال پرداخته‌اند. تئوری‌های مورد استفاده در این تحقیق شامل نظریه یادگیری اجتماعی، خودکنترلی، انومی در سطح خرد و تکنیک‌های خنثی سازی است. متغیر ارتکاب سرقت دیجیتال که با دانلود غیرقانونی فیلم، موسیقی و نرم افزار سنجیده شده و تمایل به ارتکاب سرقت دیجیتال که با تمایل به دانلود غیرقانونی فیلم و موسیقی مورد سنجش قرار گرفته است، متغیرهای وابسته این پژوهش هستند. به‌طور کلی نتایج نشانگر آن است که مهم‌ترین و قوی‌ترین پیش‌بینی‌کننده سرقت دیجیتال (دانلود غیرمجاز فیلم، آهنگ و نرم افزار)، پیوند افتراقی و ارتباط با دوستان است که این عامل در توسعه تکنیک‌های خنثی سازی نقش مهمی را بازی می‌کند.

هالت و همکاران (۲۰۱۰) در تحقیقی با عنوان «خودکنترلی پایین، ارتباط با دوستان منحرف و انحراف اینترنتی نوجوانان» در پی بررسی تأثیر خودکنترلی پایین و پیوند با همسالان منحرف بر انواع انحرافات سایبری بوده‌اند. نتایج تحقیق حاکی از ارتباط مثبت و معنادار خودکنترلی پایین و پیوند با همسالان منحرف با انحرافات سایبری است، اگرچه پیوند با همسالان منحرف نسبت به خودکنترلی پایین تأثیر بیشتر و شدیدتری بر انحرافات سایبری داشته است. همچنین طبق نتایج، پیوند با همسالان منحرف و خودکنترلی پایین با یکدیگر همبستگی دارند. این تحقیق همچنین به بررسی رابطه ارتکاب نوجوانان به تخلفات سایبری با بزهکاری در دنیای واقعی پرداخته است. یافته‌ها نشانگر رابطه روشنی بین این دو نبوده است.

هیگینز و همکاران (۲۰۱۲) در تحقیقی با عنوان «تبیین نقش همسالان و خودکنترلی بر رفتارهای دانلودی» در پی بررسی رابطه بین دوستان مجازی و واقعی با دانلود غیر مجاز و رابطه بین خودکنترلی و پیوند با دوستان (مجازی و واقعی) در ارتباط با دانلود غیر مجاز بوده‌اند. دو تئوری مورد استفاده در این تحقیق، خودکنترلی و یادگیری اجتماعی است. نتایج تحقیق نشان می‌دهد که ۴۷ درصد از نمونه مورد مطالعه به شیوه غیر مجاز، آهنگ‌هایی را دانلود می‌کنند. طبق یافته‌های این پژوهش، بین خودکنترلی، پیوند با دوستان واقعی و مجازی و مدت رابطه با آن‌ها با دانلود غیر مجاز آثار موسیقیایی رابطه معناداری وجود دارد. به‌گونه‌ای که خودکنترلی پایین و پیوند طولانی با همسالانی (مجازی و واقعی) که به‌طور غیر قانونی آهنگ دانلود می‌کنند، احتمال دانلود غیر مجاز را افزایش می‌دهد. اگرچه یافته‌ها به‌طور کلی از نظریه خودکنترلی حمایت می‌کند اما سهم پیوند با همسالان در افزایش احتمال به دانلود غیر مجاز بیشتر از خودکنترلی پایین بوده است. نتایج این تحقیق وجود رابطه بین پیوند با دوستان و خودکنترلی پایین را تأیید نمی‌کند به عبارت دیگر خودکنترلی پایین و پیوند با دوستان در دانلود غیر مجاز، مشروط به یکدیگر نیستند.

-
1. Morris
 2. Neutralization Techniques

عمده تحقیقات بررسی شده دیگر شامل دانیل^۱ (۲۰۰۰)، فیسک^۲ (۲۰۰۶)، گانتز^۳ (۲۰۰۸)، هیندوجا و اینگرام^۴ (۲۰۰۹) از نظریه یادگیری اجتماعی استفاده کرده‌اند. در این دسته از تحقیقات، پیوند افتراقی و متغیر ارتباط با دوستان متخلف، مهمترین پیش بینی کننده مصادیق مختلف جرایم رایانه‌ای بوده است. چهار مورد از تحقیقات شامل دولاند^۵ (۱۹۹۹)، چئون^۶ و همکاران (۲۰۰۹)، لیانگ و لو^۷ (۲۰۱۰)، وارنر^۸ (۲۰۱۱)، هیچ چارچوب نظری را در کار خود عنوان نکرده‌اند. در میان تحقیقات بررسی شده، تنها دو مورد از آن‌ها، دولاند (۱۹۹۹) و دانیل (۲۰۰۰) به بررسی نگرش به تخلفات رایانه‌ای پرداخته است و بقیه تحقیقات به میزان گرایش و ارتکاب تخلفات رایانه‌ای پرداخته‌اند. اغلب تحقیقات بررسی شده حاوی تبیین‌های جنسیتی بوده‌اند و سهم تخلفات رایانه‌ای مردان را بیشتر از زنان برآورد نموده‌اند. در میان پژوهش‌های مورد بررسی، تنوع بررسی مصادیق جرایم و تخلفات رایانه‌ای به چشم می‌خورد که شامل مصادیقی از قبیل سرقت دیجیتال، دسترسی غیر مجاز به اطلاعات دیگران، دسترسی غیر مجاز به رمز عبور و نام کاربری دیگران، جعل هویت، پورنوگرافی، ویروس و هک کردن بوده که سرقت دیجیتال (شامل دانلود، استفاده و تکثیر غیر مجاز نرم افزار، آهنگ و فیلم) بیشترین سهم را در میان انواع تخلفات مورد بررسی داشته است. مهمترین عوامل مؤثر بر تخلفات رایانه‌ای و اینترنتی در تحقیقات انجام شده عبارت بوده‌اند از: پیوند با دوستان متخلف، تقویت افتراقی، خود کنترلی پایین، استفاده از تکنیک‌های خنثی سازی و میزان مهارت‌های رایانه‌ای که پیوند با دوستان متخلف و خود کنترلی پایین به عنوان مهمترین و تأثیرگذارترین عوامل بر تخلفات و جرایم رایانه‌ای شناسایی شده‌اند.

چارچوب نظری

چارچوب نظری این تحقیق، مبتنی بر نظریه یادگیری اجتماعی^۹ ایگرز^{۱۰} است. این تئوری یکی از قابل آزمون ترین تئوری‌های معاصر جرم و انحرافات بوده که فرض اساسی آن بر این ایده استوار است که فرایند یادگیری، در متن ساختار اجتماعی و از طریق کنش متقابل، رفتار سازگاران و انحرافی را تولید می‌کند (ایگرز و سلرز^{۱۱}، ۲۰۰۴: ۸۵) و بروز رفتارهای مجرمانه یا سازگاران وابسته به عملکرد متغیرهای فرایند یادگیری اجتماعی است (ایگرز، ۱۹۷۷؛ ایگرز، ۱۹۹۸). این نظریه هم عامل محرک و کنترل رفتارهای مجرمانه و منحرفانه را توضیح می‌دهد و هم به تبیین عوامل افزایش

1. Daniel
2. Fisk
3. Gunter
4. Ingram
5. Dowland
6. Cheon
7. Liang & Lu
8. Warner
9. Social learning theory
10. Akers
11. Sellers

سازگاری و تضعیف سازگاری می‌پردازد (ایکرز و جنسن^۱، ۲۰۰۶). بنابراین این تئوری صرفاً یک نظریه پوزیتویستی از علل جرم و جنایت نیست بلکه علاوه بر عوامل تسهیل کننده جرم، شامل عوامل بازدارنده جرم نیز می‌باشد (ایکرز، ۱۹۹۸). نظریه یادگیری اجتماعی ایکرز، پیرامون چهار مفهوم اساسی سازماندهی شده است که این مفاهیم خود متأثر از فرهنگ عمومی، ساختار جامعه، گروه‌ها و زمینه‌های تعامل اجتماعی در محیط - حجم و اندازه جامعه - است (ایکرز، ۱۹۹۹؛ ایکرز و جنسن، ۲۰۰۶). متغیرهای اصلی یادگیری اجتماعی عبارت است از: پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف.

پیوند افتراقی^۲: پیوند افتراقی، اولین اصل نظریه یادگیری اجتماعی بوده که بر مبنای نظریه پیوند افتراقی ساترلند است. این فرآیند معمولاً شامل ارتباط مستقیم با افرادی که رفتارهای متخلفانه یا مجرمانه مرتکب می‌شوند و نیز ارتباط غیر مستقیم با گروه‌های مرجع می‌باشد. گروه‌هایی که فرد با آن‌ها پیوند افتراقی دارد، زمینه اجتماعی عمده‌ای را فراهم می‌کنند که در آن، انگیزه‌ها، محرک‌ها، عقلانیت‌ها و روش‌های رفتار کردن به شیوه‌هایی خاص یاد گرفته شده و درونی می‌گردند. به اعتقاد ایکرز، خانواده و دوستان، مهمترین منابع پیوند افتراقی هستند ولی گروه‌های ثانویه از قبیل رسانه جمعی، اینترنت و گروه‌های مجازی نیز به فرایند یادگیری کمک می‌نمایند (وار^۳، ۲۰۰۲). همچنین ایکرز بیان می‌دارد پیوندها و ارتباطاتی که زودتر اتفاق می‌افتند (تقدم^۴)، مدت زمان زیادی طول می‌کشند (طول مدت^۵)، اغلب اوقات اتفاق می‌افتند (فراوانی^۶) و شامل دیگرانی می‌شوند که خیلی مهم‌اند یا رابطه نزدیکی با آن‌ها وجود دارد (شدت^۷) تأثیر بیشتری روی رفتار فرد دارند (ایکرز و جنسن، ۲۰۰۶). پیوند افتراقی از دو بعد مهم تشکیل شده است. بعد اول، رفتاری-تعاملی^۸ است و انحراف را به‌عنوان چیزی که از طریق «ارتباط مستقیم و متقابل با دیگرانی دیگرانی که انواع خاصی از رفتارها را مرتکب می‌شوند و نیز ارتباط غیرمستقیم و هویت یابانه با گروه‌های مرجع» به‌وجود می‌آید، در نظر می‌گیرد. بعد دوم کیفیت هنجاری^۹ بوده که در قالب موافقت یا مخالفت اخلاقی با رفتارهای منحرفانه یا مجرمانه، بخشی از فرآیند پیوند افتراقی است. به زعم ایکرز، دوستان، دیگران مهم و اعضای خانواده به‌عنوان گروه‌هایی هستند که زمینه اجتماعی را فراهم می‌کنند که در آن فرد، در معرض تعاریف، الگوهای تقلید و تقویت افتراقی قرار می‌گیرد (وینفری^{۱۰} و همکاران، ۱۹۹۴).

- 1.Jensen
- 2.Differential association
- 3.Warr
- 4.Priority
- 5.Duration
- 6.Frequency
- 5.Intensity
- 8.Behavioural-interactional
- 9.Norm qualities
- 10.Winfree

تقویت افتراقی^۱: تقویت و تنبیه افتراقی مفهومی است که پیامدهای مورد انتظار^۲ و واقعی^۳ یک یک رفتار خاص را نشان می‌دهد. این مفهوم به توازن پاداش‌ها^۴ و تنبیهاتی^۵ که با یک رفتار همراه است اشاره دارد. این مفهوم در واقع شبیه به مفهوم «بازدارندگی^۶» خصوصاً در نظریه‌های کلاسیک انتخاب عقلانی است که به تأثیر مجازات‌های خاص و شدید در جلوگیری از ارتکاب فرد به رفتار مجرمانه تأکید دارد (گانتر، ۲۰۰۸: ۵۷). ایگرز بین دو نوع از تقویت کننده‌های اجتماعی و غیر اجتماعی تمایز قائل شده و تقویت کننده‌های اجتماعی را در بروز یک رفتار مهم‌تر قلمداد می‌کند. تقویت کننده‌های اجتماعی مجموعه‌ای از پاداش‌های با ارزش واقعی و مورد انتظار، ملموس و غیر ملموس، مادی و نمادین هستند که شامل کلمات، واکنش‌ها، حضور و رفتار افرادی است که بطور مستقیم موجب تقویت رفتار شده و یا زمینه‌ای را برای تقویت رفتار فراهم می‌نمایند. تقویت غیر اجتماعی نیز شامل تأثیرات مستقیم فیزیکی مانند تأثیرات فیزیکی مواد مخدر و الکل است (ایگرز و جنسن، ۲۰۰۶).

تقلید^۷: تقلید به الگوبرداری از یک رفتار بعد از مشاهده مستقیم یا غیر مستقیم آن رفتار (مثلاً در رسانه‌ها) اشاره دارد. این که یک الگوی رفتاری تقلید شود یا نشود، متأثر از ویژگی الگوها، رفتار مشاهده شده و پیامدهای مشاهده شده از رفتار (تقویت کننده‌های جانشین) است (باندورا، ۱۹۷۷). گروه‌های اجتماعی مهم (والدین، دوستان، معلمان) و نیز منابعی نظیر رسانه‌ها از مهمترین منابع تقلید یا الگوبرداری هستند. تقلید در مراحل اول یادگیری رفتار انحرافی اهمیت زیادی دارد اما سپس اهمیت آن کم می‌شود، اگرچه کماکان تأثیر اندکی در استمرار و توقف رفتار دارد (اسکینر و فریام، ۱۹۹۷: ۴۹۹).

تعاریف^۸: تعاریف فرآیندی است که از طریق آن افراد رفتارشان را توجیه، تفسیر و ارزیابی کرده و غلط و درست را تعیین می‌کنند (ایگرز و سلرز، ۲۰۰۴). تعاریف نگرش‌هایی است درباره رفتارهایی خاص که به وسیله فرایند پیوند افتراقی، تقلید و کنش متقابل با منابع متنوعی از یادگیری که در محیط اجتماعی یک شخص واقع شده است، یاد گرفته می‌شوند و موقعیتی را به عنوان فرصت یا فقدان فرصت برای اعمال مجرمانه فراهم می‌کنند (ایگرز و جنسن، ۲۰۰۶). یادگیری اجتماعی، بین تعاریف مثبت، منفی و خنثی کننده^۹ تمایز قائل می‌شود. تعاریف مثبت، رفتار غیر قانونی را مطلوب، قابل پذیرش و مجاز مجاز می‌دانند. تعاریف منفی، رفتار غیر قانونی را نامطلوب، غیرقابل پذیرش، غیرمجاز و اشتباه می‌دانند و تعاریف خنثی کننده، رفتار غیر قانونی را بخشودنی، قابل توجیه و قابل تحمل ارزیابی می‌کنند. این تعاریف در جریان اصلی جامعه و بیرون از هر خرده فرهنگی یاد گرفته می‌شوند. هدف تعاریف خنثی

1. Differential reinforcement
2. Anticipated
3. Actual
4. Rewards
5. Punishments
6. Deterrence
7. Imitation
8. Definition
9. Positive, Negative & Neutralizing Definitions

کننده، کاهش احساس گناه و جلوگیری از سرزنش خود بعد از ارتکاب رفتار منحرفانه یا مجرمانه می‌باشد (ایکرز، ۱۹۹۸؛ اسکینر و فریام، ۱۹۹۷).

نظریه یادگیری اجتماعی، یکی از اصلی‌ترین تئوری‌های جرم و انحرافات است که دارای ارزش ذاتی قابل توجهی برای فهم مجموعه‌ای از رفتارهای انحرافی مرتبط با رایانه است. این نظریه در بین مطالعات فراوانی که وجود دارد، دارای مبنای تئوریک و تجربی بوده و مدعی است که نظریه‌ای عمومی و کاربردی در تبیین انواع رفتارهای انحرافی می‌باشد (ایکرز، ۱۹۸۵). در نتیجه برای تبیین و تحلیل رفتارهای انحرافی مرتبط با رایانه نیز مناسب است. همچنین طبق گفته ساترلند و کرسی (۱۹۷۴) «افراد نه فقط انگیزه‌های خاص، محرک‌ها، عقلانیت و نگرش‌ها را فرا می‌گیرند بلکه تکنیک‌های ارتکاب جرم را نیز یاد می‌گیرند؛ چه ساده چه پیچیده باشد». بدین ترتیب، افراد نه فقط چگونگی بهره برداری از تجهیزات و تکنولوژی را یاد می‌گیرند، بلکه همچنین روش‌های خاص، برنامه‌ها و تکنیک‌های استفاده غیرقانونی از آن‌ها را نیز می‌آموزند. علاوه بر آن، مطالعات متعددی که در زمینه تخلفات رایانه‌ای صورت گرفته است، با آزمون تجربی ابعاد مختلف نظریه یادگیری، سودمندی و کارایی این نظریه و ابعاد آن را در فهم تخلفات و جرایم رایانه‌ای نشان داده‌اند (هلینگر، ۱۹۹۲؛ اسکینر و فریام، ۱۹۹۷؛ هیگینز و همکاران، ۲۰۰۶؛ ۲۰۰۷؛ گانتر، ۲۰۰۸؛ هالت و همکاران، ۲۰۱۰؛ کانگ و لیام، ۲۰۱۲).

نظریه یادگیری اجتماعی، یک نظریه فرآیندی است که در آن متغیرهای پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف با یکدیگر تعامل متقابل دارند. فرایند یادگیری اجتماعی یک فرایند پویاست و شامل بازخورد و اثرات متقابل بین این متغیرها می‌باشد که بر یادگیری رفتارهای مجرمانه و سازگارانه اثر می‌گذارد. پیوند افتراقی با دیگرانی که موافق رفتارهای منحرفانه هستند، نوعاً مقدم بر ارتکاب به یک عمل می‌باشد. بدیهی است که ارتباط، تقویت رفتار انحرافی، الگوهای منحرفانه و قرارگیری در معرض تعاریف مطلوب و نامطلوب انحراف، ابتدا در خانواده و گروه دوستان اتفاق می‌افتد. نظریه یادگیری اجتماعی معتقد است که افراد از طریق تقویت افتراقی در فرایند پویای یادگیری اجتماعی، منحرف می‌شوند و یا موقعیت‌های مجرمانه را حفظ می‌کنند. در نتیجه تقویت مورد انتظار، موجب ارتکاب اولیه رفتار، تداوم یا توقف آن می‌گردد. علاوه بر این، مردم در تعامل با گروه‌های مهم در زندگیشان، ارزیابی از رفتارهایشان به عنوان خوب یا بد را یاد می‌گیرند. این تعاریف، رفتارهای کلامی و شناختی هستند که به‌طور مستقیم می‌توانند تقویت شوند و همچنین به‌عنوان محرک برای رفتار عمل کنند. افرادی که رفتارهای انحرافی را خوب (تعریف مثبت) یا حداقل موجه (تعریف خنثی کننده) تعریف می‌کنند، احتمال بیشتری دارد که مرتکب آن رفتارها شوند. تعاریف مطلوب رفتار انحرافی شامل نگرش‌ها، تصورات و توجیهات فرد از آن رفتار می‌باشد که طیف وسیعی از جرم و جنایت و دیگر رفتارهای انحرافی را تحت تاثیر قرار می‌دهد (ایکرز و جنسن، ۲۰۰۶). تعاریف از طریق تقلید یاد گرفته می‌شوند و به‌وسیله اعضای گروه‌هایی که با آن‌ها همراه هستند، تقویت می‌شوند و به محض یادگیری، این تعاریف به عنوان محرک و انگیزه‌ای برای انجام یا عدم انجام رفتار انحرافی به کار گرفته می‌شوند. در نتیجه تعاریف با الگوهای تقلید در تعامل اند (ایکرز و لی، ۱۹۹۶؛ کرون، ۱۹۹۹). نکته مهم در این فرایند این است که بعد از اینکه یک

عمل اتفاق افتاد، تقویت کننده‌ها و بازدارنده‌های واقعی (اجتماعی و غیر اجتماعی) وارد بازی شده و بر احتمال تکرار شدن آن عمل و فراوانی آن تأثیر می‌گذارند.

دانشگاه به عنوان ساختار اجتماعی، شرایط و بستری را فراهم می‌کند که افراد در معرض فرایندها و مکانیسم‌های یادگیری قرار بگیرند. ارتباط با دوستان، علاوه بر مواجه کردن فرد با الگوهای رفتارهای انحرافی رایانه‌ای، عاملی در یادگیری تعاریف مطلوب و نامطلوب مربوط به این رفتارها می‌باشد. فرد در معرض هنجارهای مطلوب تخلفات رایانه‌ای دوستان خود قرار گرفته و بدین ترتیب، باورها و اعتقادات خود در این زمینه را شکل داده و درونی می‌کند. علاوه بر این که دوستان نقش مهمی در یادگیری الگوهای متخلفانه رایانه‌ای و تعاریف مطلوب آن دارند، واکنش و عکس‌العمل آنان و نیز حمایت و تشویق آنان در ارتکاب به تخلفات رایانه‌ای می‌تواند در جهت تداوم و یا توقف رفتارهای انحرافی رایانه‌ای نقش مهمی داشته باشد. در نتیجه گروه همسالان مهمترین زمینه اجتماعی در روابط دوستانه است که بی‌شک تأثیر زیادی روی یادگیری تخلفات رایانه‌ای دارد. علاوه بر دوستان، دیگران مهمی مانند اعضای خانواده، استادان و معلمان نیز نقش مهمی در یادگیری رفتارهای انحرافی رایانه‌ای دارند. بدین ترتیب که هم منبعی برای تقلید رفتارهای انحرافی محسوب می‌شوند و هم واکنش‌های مورد انتظار و واقعی آنان در زمینه ارتکاب تخلفات رایانه‌ای، عاملی در تقویت این رفتارها است. با توجه به آن که وضعیت‌های قانونی منبعی برای تعریف منفی از جرم رایانه‌ای فراهم می‌کنند، در نتیجه انتظار می‌رود که تأیید و حمایت از قوانین ضد جرایم رایانه‌ای توسط دانشجویان، فراوانی این رفتارها را کاهش دهد. همچنین کنترل رسمی در دانشگاه که از طریق مراجعی مانند کمیته انضباطی اعمال می‌گردد به عنوان عاملی بازدارنده در رفتارهای انحرافی رایانه‌ای عمل می‌کند. نتیجه اینکه نظریه یادگیری اجتماعی ایگز و ابعاد مختلف آن، قابلیت استفاده در بررسی تخلفات رایانه‌ای را داشته و می‌تواند تبیین مناسبی در جهت فهم تخلفات رایانه‌ای در میان دانشجویان ارائه نماید.

فرضیه اصلی

بین یادگیری اجتماعی و تخلفات رایانه‌ای رابطه مستقیم وجود دارد.

فرضیات فرعی

۱- بین پیوند افتراقی و تخلفات رایانه‌ای رابطه مستقیم وجود دارد.

۲- بین تقویت افتراقی و تخلفات رایانه‌ای رابطه مستقیم وجود دارد.

۳- بین تقلید و تخلفات رایانه‌ای رابطه مستقیم وجود دارد.

۴- بین تعاریف و تخلفات رایانه‌ای رابطه مستقیم وجود دارد.

روش تحقیق

روش پژوهش حاضر، پیمایشی و طرح تحقیق از نوع مقطعی می‌باشد. واحد تحلیل این تحقیق، در سطح فرد (دانشجو) بوده است. جمعیت تحقیق این پژوهش، کلیه دانشجویان دختر و پسر دانشگاه مازندران که در سال ۹۲-۱۳۹۱ مشغول به تحصیل بوده‌اند، می‌باشد که تعداد آن‌ها ۹۹۴۰ نفر (۳۲۸۶ پسر و ۶۶۵۴ دختر) بوده است که طبق نتایج به‌دست آمده از فرمول کوکران، حجم کل نمونه لازم برای تعمیم به جمعیت تحقیق، با احتمال ۹۵ درصد اطمینان، ۳۷۰ دانشجو برآورد گردید. با توجه به احتمال مخدوش شدن پرسش‌نامه‌ها در اثر پاسخ ندادن، الگوی یکنواختی در پاسخ دهی، پاسخ‌های نامربوط، مفقود شدن

پرسش‌نامه و غیره و برای جلوگیری از کاهش حجم نمونه، در مجموع ۴۳۰ پرسش‌نامه تکثیر و توزیع گردید. پس از کنار گذاشتن پرسش‌نامه‌های مخدوش، در نهایت ۴۰۳ پرسش‌نامه مورد تجزیه و تحلیل قرار گرفت. نمونه مورد بررسی به روش نمونه‌گیری طبقه‌ای^۱ متناسب با حجم به‌عنوان نمونه انتخاب شده‌اند. داده‌های تحقیق با ابزار پرسش‌نامه و به شیوه جمع‌اجرا گردآوری شده است. برای حصول اطمینان از اعتبار ابزار مورد استفاده، از اعتبار محتوایی^۲ و اعتبار سازه^۳ استفاده شده است. در اعتبار سازه، مفهوم و مقیاس یا سازه تحقیق باید با روابط مدنظر در نظریه‌ها یا تحقیقات انجام گرفته قبلی هماهنگی داشته باشد. اگر مفهوم، مقیاس یا سازه تحقیق روابط یا جهت‌های پیش‌بینی شده در تحقیقات انجام گرفته قبلی را نشان دهد، بر اساس اعتبار سازه، مفهوم و مقیاس مورد نظر از اعتبار برخوردار است (دواس، ۱۳۸۸: ۶۴). در این تحقیق، بر اساس آزمون مقایسه میانگین دو گروه (آزمون T)، مشاهده شده است که میزان تخلفات رایانه‌ای در پسران بیشتر از دختران بوده است. این یافته با نتایج تحقیقات (اسکینر و فریام، ۱۹۹۷؛ مون و همکاران، ۲۰۱۲؛ هیگینز، ۲۰۰۵، ۲۰۰۶؛ هیندوجا و پاتچین^۴، ۲۰۰۹؛ حالت و همکاران، ۲۰۱۰) مطابقت دارد. در نتیجه مقیاس متغیر وابسته (تخلفات رایانه‌ای) از اعتبار سازه نظری برخوردار می‌باشد. همچنین برای سنجش اعتبار سازه تجربی مقیاس متغیر مستقل، از تحلیل عاملی تأییدی استفاده شده که در مدل اندازه‌گیری لیزرل مورد تحلیل قرار گرفته و نشان داده است که متغیرهای مستقل از اعتبار سازه تجربی برخوردار می‌باشند. شاخص‌های برازش مدل نیز حاکی از آن است که مدل‌های اندازه‌گیری از برازش مطلوبی برخوردارند. نتایج تحلیل عاملی تأییدی متغیرهای مستقل در جدول (۱) نشان داده شده است.

جدول ۱: مقادیر استاندارد بارهای عاملی و شاخص‌های برازندگی

متغیرهای تحقیق	مؤلفه‌ها	بار عاملی	Chi-Square	p-value	Chi-Square/df	RMSEA	GFI
پیوند افتراقی	نگرش دوستان	۰/۶۷	۰/۰۰	۱/۰۰	-	-	-
	تعداد دوستان	۰/۷۸					
	شدت رابطه با دوستان	۰/۹۱					
تقویت افتراقی	عکس‌العمل	۰/۴۷	۰/۲۷	۰/۶۰	۰/۲۷	۰/۰۰۰	۱/۰۰
	بازدارندگی	۰/۳۸					
	پاداش	۰/۴۷					
	تشویق	۰/۸۹					
تعاریف	انکار مسئولیت	۰/۸۴	۵/۵۱	۰/۲۳۸	۱/۳۷	۰/۰۳۱	۰/۹۹
	انکار خسارت	۰/۶۶					

- 1.Stratified sampling
- 2.Content validity
- 3.Construct validity
- 4.Patchin

					۰/۶۸	محکوم کردن محکوم کنندگان	
					۰/۳۴	سرزنش قربانی	
					۰/۷۱	توسل به وفاداری‌های بالاتر	
					۰/۶۹	گویه (۱)	تقلید
					۰/۷۲	گویه (۲)	
					۰/۷۹	گویه (۳)	
					۰/۶۳	گویه (۴)	
					۰/۶۹	گویه (۵)	
					۰/۶۷	گویه (۶)	
					۰/۶۴	گویه (۷)	
					۰/۵۷	گویه (۸)	
۰/۹۹	۰/۰۴۲	۱/۷۱	۰/۰۴۵	۲۳/۹۹			

برای سنجش پایایی ابزار تحقیق نیز از ضریب آلفای کرونباخ استفاده شده است که نتایج سنجش پایایی مقیاس‌های تحقیق، نشانگر آن است که ضریب آلفا برای بعد علیه داده و سیستم (۵ گویه) ۰/۷۲، برای بعد جعل هویت (۳ گویه) ۰/۶۶، بعد فرهنگی (۶ گویه) ۰/۸۴، بعد رفتاری-تعاملی (۱۶ گویه) ۰/۹۱، بعد هنجاری (۸ گویه) ۰/۸۸، بعد عکس العمل (۸ گویه) ۰/۸۵، بعد بازدارندگی (۱۶ گویه) ۰/۹۱، بعد پاداش (۸ گویه) ۰/۸۷، بعد تشویق (۸ گویه) ۰/۸۹، بعد تقلید (۸ گویه) ۰/۸۷ و بعد تعریف (۹ گویه) ۰/۷۹ است. داده‌های تحقیق با استفاده از نرم افزار آماری علوم اجتماعی^۱ و لیزرل^۲ و با استفاده از مدل‌های رگرسیونی و مدل معادلات ساختاری مورد تحلیل قرار گرفته است.

تصریح مفاهیم و سنجش متغیرها

تخلفات رایانه‌ای:^۳ برای سنجش متغیر تخلفات رایانه‌ای به کمک مطالعه اکتشافی، چهارده نوع از مصادیق تخلفات رایانه‌ای شناسایی شده که در قالب سه بعد «علیه داده و سیستم»، «جعل هویت» و «فرهنگی» مورد سنجش قرار گرفته است.

بعد علیه داده و سیستم: به تخلفات و جرایمی اشاره دارد که از طریق هک کردن، انتقال ویروس یا روش‌های دیگر به صورت غیر مجاز به سیستم یا اطلاعات اشخاص و سازمان‌ها دسترسی پیدا کرده و موجب هر نوع تغییر یا صدمه زدن به آن‌ها شده و یا اطلاعات و داده‌ها را بدون اجازه در اختیار دیگران قرار دهد. برای سنجش این بعد، مؤلفه‌ها و معرف‌هایی تعریف شده و در نهایت پنج سؤال به آن اختصاص داده شد.

بعد جعل هویت: به فعالیتهای و تخلفاتی اشاره می‌کند که در آن فرد از یک هویت ساختگی، دستکاری شده و یا جعلی برای تسهیل ارتکاب جرم استفاده می‌کند (اسمیت، ۲۰۱۰: ۲۷۴). برای سنجش این بعد، پس از مشخص نمودن مؤلفه‌ها و معرف‌ها، سه گویه در نظر گرفته شده است.

- 1.Spss
- 2.Lisrel
- 3.Computer offences

بعد فرهنگی: به هر نوع تخلف و جرمی اشاره دارد که علیه محتوا، مالکیت معنوی، ارزش‌های فردی و اجتماعی بوده و منجر به آزار و تهدید افراد شده و از لحاظ روانی به آن‌ها صدمه می‌زند. برای سنجش این بعد از چهار مؤلفه شامل پورنوگرافی، تهدید با ایمیل، شایعه پراکنی علیه دیگران و کرک کردن (شکستن قفل) نرم افزار استفاده شده و در نهایت پس از مشخص نمودن معرف‌ها، شش گویه به آن اختصاص داده شده است. فرآیند شاخص‌سازی بر مبنای پژوهش‌های تجربی پیشین (اسکینر و فریام، ۱۹۹۷؛ هلینگر، ۱۹۹۲؛ دولاند و همکاران، ۱۹۹۹؛ فاستر، ۲۰۰۴؛ هیندوجا، ۲۰۰۴؛ هیگینز و همکاران، ۲۰۰۸؛ هالت و همکاران، ۲۰۱۰ و کونگ و لیم، ۲۰۱۲) انجام شده است.

پیوند افتراقی: برای سنجش پیوند افتراقی، از دو بعد رفتاری - تعاملی و هنجاری استفاده گردید. دو مؤلفه تعداد دوستان و شدت رابطه با دوستان برای بعد رفتاری - تعاملی و مؤلفه نگرش دوستان صمیمی^۱ به تخلفات رایانه‌ای برای بعد هنجاری انتخاب گردید. این متغیر بر مبنای تحقیقات پیشین (وینفوری و همکاران، ۱۹۹۴؛ ایکرز و لی، ۱۹۹۶؛ ایکرز و همکاران، ۲۰۰۴؛ می و همکاران، ۲۰۱۰) مورد سنجش قرار گرفته است.

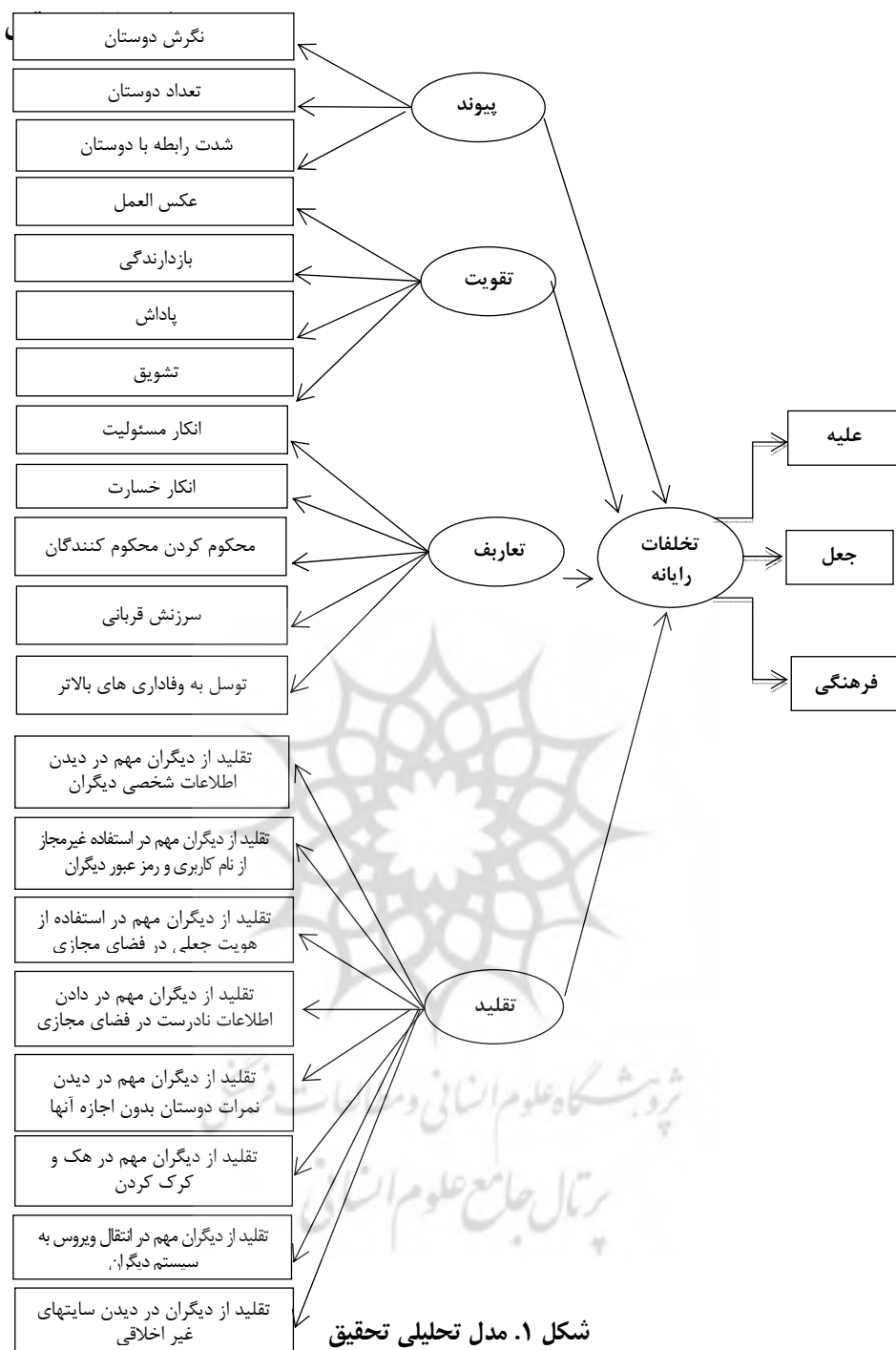
تقویت افتراقی: متغیر تقویت افتراقی در این تحقیق در چهار بعد شامل عکس العمل، بازدارندگی، پاداش و تشویق مورد بررسی واقع شده است. این سنجش بر مبنای تحقیقات تجربی پیشین (ایکرز و لی، ۲۰۰۴؛ ایکرز، ۲۰۰۹؛ ایکرز و دیگران، ۱۹۹۷؛ گانتر، ۲۰۰۸؛ هیگینز و همکاران، ۲۰۰۵) بوده است.

عکس العمل^۲: به واکنش دیگران مهم از قبیل خانواده، دوستان، معلمان و استادان نسبت به رفتار فرد اشاره می‌کند. برای سنجش بعد عکس العمل، مؤلفه عکس العمل تصویری دوستان^۳ انتخاب گردید.

بازدارندگی: بازدارندگی شامل سه بعد قطعیت^۴، شدت^۵ و سرعت مجازات نهاد‌های رسمی و غیر رسمی می‌باشد (ایکرز و همکاران، ۱۹۷۹). سنجش این بعد، با انتخاب دو مؤلفه بازدارندگی رسمی و غیر رسمی^۶ به عنوان مؤلفه درجه (۱) و سپس مؤلفه قطعیت به عنوان مؤلفه درجه (۲) صورت گرفته است. معرف بازدارندگی رسمی - قطعیت، بازدارندگی کمیته انضباطی دانشگاه بوده است. برای سنجش بازدارندگی غیر رسمی - قطعیت، معرف بازدارندگی دوستان نزدیک و صمیمی^۸ انتخاب گردید.

پاداش: سنجش بعد پاداش از طریق مؤلفه پاداش تصویری^۹ صورت گرفته است. معرف‌هایی که برای این مؤلفه عنوان شده، شامل: «حس متفاوت بودن، هیجان انگیز بودن، حس موفقیت و برتری، تفریح و کنجکاوی، انتقام از دیگران» که پاسخ‌گو قادر به انتخاب چند مورد از این موارد بوده است. نمره پاداش فرد از مجموع تعداد گزینه‌هایی که علامت زده، به دست آمده است.

1. Attitude of Close friends
2. Reaction
3. Perceived Reaction of friends
4. Certainty
5. Severity
6. Swiftness
7. Formal & Informal Deterrence
8. Deterrence of Close & best friends
9. Perceived reward



تشویق^۱: برای اندازه‌گیری این بعد، مؤلفه تشویق دوستان^۲ انتخاب گردید و این سؤال مطرح شد شد که «دوستانم مرا تشویق می‌کنند که تخلفات رایانه‌ای را انجام دهم».

تعاریف: برای سنجش این متغیر، مؤلفه تکنیک‌های خنثی سازی^۳ انتخاب گردید. معرف‌های این مؤلفه شامل پنج فن خنثی سازی انکار مسئولیت^۴، انکار خسارت^۵، سرزنش قربانی^۶، محکوم کردن محکوم کنندگان^۷ و توسل به وفاداری‌های بالاتر^۸ می‌باشد که با نه گویه مورد سنجش قرار گرفته است. مبنای سنجش این متغیر، تحقیقات (اسکینر و فریام، ۱۹۹۷؛ موریس و هیگینز، ۲۰۰۹؛ ایگرز و همکاران، ۲۰۱۰) بوده است.

تقلید: برای سنجش تقلید، از مؤلفه تقلید از دیگران^۹ مهم استفاده شده که با این سؤال مورد سنجش واقع شد: «آیا هیچ گاه دیده یا شنیده‌اید کسانی که شما به آن‌ها احترام می‌گذارید و مورد تأیید شما هستند (مانند اعضای خانواده، دوستان صمیمی، اقوام، اساتید و معملین دوره دبیرستان) هریک از تخلفات رایانه‌ای را انجام داده باشند؟». مبنای سنجش این متغیر، تحقیقات (اسکینر و فریام، ۱۹۹۷؛ لی و همکاران، ۲۰۰۴) بوده است.

یافته‌های توصیفی

۱- توصیف پاسخگویان بر حسب متغیرهای جمعیت شناختی:

در نمونه مورد بررسی پژوهش حاضر، ۲۷۰ نفر (۱۶۷ درصد) از پاسخ‌گویان را دانشجویان دختر و ۱۳۳ نفر (۳۳ درصد) از آن‌ها را دانشجویان پسر تشکیل می‌دهند. دامنه سنی پاسخ‌گویان ۱۷ تا ۳۱ سال و میانگین سنی آن‌ها حدود ۲۱ سال است و گروه سنی ۲۲ - ۲۰ سال با ۲۲۶ نفر (۵۶/۱ درصد) بیشترین تعداد پاسخ‌گویان را تشکیل می‌دهند. به لحاظ مقطع تحصیلی، ۳۵۰ نفر (۸۶/۸ درصد) از پاسخگویان در مقطع کارشناسی و ۵۳ نفر (۱۳/۲ درصد) در مقطع کارشناسی ارشد مشغول به تحصیل می‌باشند. ۲۸۷ نفر (۷۱/۲ درصد) از پاسخ‌گویان در دوره روزانه و ۱۱۶ نفر (۲۸/۸ درصد) در دوره شبانه تحصیل می‌کنند. دانشکده علوم انسانی و اجتماعی با ۲۱/۸ درصد (۶۴ نفر دختر و ۲۴ نفر پسر) و بعد از آن دانشکده علوم اقتصادی و اداری با ۲۰/۶ درصد (۵۴ نفر دختر و ۲۹ نفر پسر) بیشترین تعداد پاسخ‌گویان را دارند. دانشکده هنر و معماری و دانشکده الهیات با ۴/۲ درصد (۱۷ نفر) کمترین میزان پاسخ‌گویان را به خود اختصاص داده‌اند.

- 1.Prais
- 2.Prais of Friend
- 3.Techniques of Neutralization
- 4.Denial of Responsibility
- 5.Denial of Injury
- 6.Denial of a Victim
- 7.Condemnation of Condemners
- 8.Appeal to Higher Loyalties
- 9.Imitation of significant others

۲. توصیف پاسخ‌گویان بر حسب میزان و نوع ارتکاب به تخلفات رایانه‌ای:

برای سنجش تخلفات رایانه‌ای، از سه بعد شامل «علیه داده و سیستم»، «جعل هویت» و «فرهنگی» استفاده شده است.

۱.۲. توزیع تخلفات رایانه‌ای پاسخگویان بر حسب بعد علیه جعل هویت

طبق جدول، بیشترین میزان تخلفات در این بعد مربوط به «دادن اطلاعات نادرست به دیگران در فضای مجازی» می‌باشد. ۲۶/۸ درصد (۱۱۸ نفر) از دانشجویان در طول یک سال گذشته به میزان زیاد و خیلی زیاد و ۳۱/۳ درصد (۱۲۶ نفر) نیز گاهی اوقات مرتکب این رفتار شده‌اند. کمترین میزان تخلفات در این بعد نیز مربوط به «ایجاد صفحه شخصی در فضای مجازی با هویت جعلی» بوده است که تنها ۸۳/۸ درصد (۳۳۸ نفر) از دانشجویان در طول یک سال گذشته اصلاً مرتکب این رفتار نشده‌اند و یا به میزان کمی این رفتار را انجام داده‌اند و تنها ۵ درصد (۲۰ نفر) از آنان به میزان

جدول ۲. توزیع فراوانی و درصدی بعد جعل هویت بر حسب جنس پاسخگویان

گروه‌های تخلفات رایانه‌ای	رتبه	گزینه	پسر		دختر		جمع کل	
			تعداد	درصد	تعداد	درصد	تعداد	درصد
برایم پیش آمده که در فضای مجازی در مورد ویژگی‌های شخصی ام به دیگران، اطلاعات نادرست بدهم.	۵	اصلاً و کم	۴۶	۳۴/۶	۱۲۳	۴۵/۶	۱۶۹	۴۱/۹
		گاهی اوقات	۳۶	۲۷/۱	۹۰	۳۳/۳	۱۲۶	۳۱/۳
		زیاد و خیلی زیاد	۵۱	۳۸/۴	۵۷	۲۱/۱	۱۱۸	۲۶/۸
از نام کاربری و رمز عبور دیگران بدون اجازه آن‌ها استفاده کرده‌ام	۵	اصلاً و کم	۷۵	۵۶/۴	۲۴۱	۸۹/۳	۳۱۶	۷۸/۴
		گاهی اوقات	۲۹	۲۱/۸	۱۸	۶/۷	۴۷	۱۱/۷
		زیاد و خیلی زیاد	۲۹	۲۱/۸	۱۱	۴/۱	۴۰	۹/۹
با هویت دیگران و بدون آگاهی آنان، صفحاتی شخصی (در فیس بوک یا دیگر فضاهای مجازی) ایجاد کرده‌ام.	۵	اصلاً و کم	۹۸	۷۳/۷	۲۴۰	۸۸/۹	۳۳۸	۸۳/۸
		گاهی اوقات	۲۲	۱۶/۵	۲۳	۸/۵	۴۵	۱۱/۲
		زیاد و خیلی زیاد	۱۳	۹/۸	۷	۲/۶	۲۰	۵

زیاد و خیلی زیادی این رفتار را انجام داده‌اند. مقایسه میان دو جنس نشانگر آنست که میزان ارتکاب به هر یک از این ۳ تخلف در میان دانشجویان پسر بیشتر از دانشجویان دختر می‌باشد. به عنوان مثال ۳۸/۴ درصد (۵۱ نفر) از دانشجویان پسر در طول یک سال گذشته به میزان زیاد و خیلی زیادی در فضای مجازی به دیگران اطلاعات نادرستی از ویژگی‌های شخصی خود داده‌اند در حالیکه این میزان برای دانشجویان دختر تنها ۲۱/۱ درصد (۵۷ نفر) می‌باشد.

۲.۲. توزیع تخلفات رایانه‌ای پاسخ‌گویان برحسب بعد علیه داده و سیستم جدول ۳. توزیع فراوانی و درصدی بعد علیه داده و سیستم بر حسب جنس پاسخ‌گویان

میزان تخلفات رایانه‌ای	توزیع	گویه‌های تخلفات رایانه‌ای	گزینه	پسر		دختر		جمع کل	
				تعداد	درصد	تعداد	درصد	تعداد	درصد
تخلفات رایانه‌ای علیه داده و سیستم		برایم پیش آمده که اطلاعات (داده، فیلم و عکس) شخصی و محرمانه دیگران را بدون آگاهی آن‌ها ببینم.	اصلاً و کم	۷۱	۵۳/۴	۲۰۶	۷۶/۳	۲۷۷	۶۸/۸
			گاهی اوقات	۳۹	۲۹/۳	۴۴	۱۶/۳	۸۳	۲۰/۶
			زیاد و خیلی زیاد	۲۳	۱۷/۳	۲۰	۷/۴	۴۳	۱۰/۶
تخلفات رایانه‌ای علیه داده و سیستم		اطلاعات (داده، فیلم و عکس) شخصی و محرمانه دیگران را بدون اجازه آن‌ها پخش کرده‌ام.	اصلاً و کم	۱۱۵	۸۶/۵	۲۵۶	۹۸/۲	۳۸۰	۹۴/۲
			گاهی اوقات	۱۳	۹/۸	۳	۱/۱	۱۶	۴
			زیاد و خیلی زیاد	۵	۳/۸	۲	۰/۷	۷	۱/۷
تخلفات رایانه‌ای علیه داده و سیستم		برایم پیش آمده که بدون اجازه دوستان خود، نمرات آن‌ها را در ببینم و به جای آن‌ها اعتراض ثبت کنم.	اصلاً و کم	۸۹	۶۶/۹	۲۶۲	۹۷	۳۵۱	۸۷/۱
			گاهی اوقات	۲۶	۱۹/۵	۴	۱/۵	۳۰	۷/۴
			زیاد و خیلی زیاد	۱۸	۱۳/۵	۴	۰/۱۴	۲۲	۵/۵
تخلفات رایانه‌ای علیه داده و سیستم		سیستم، رمز عبور و نام کاربری دیگران یا شبکه‌های سازمانی را هک کرده‌ام.	اصلاً و کم	۱۱۲	۸۴/۱	۲۶۶	۹۸/۵	۳۷۸	۹۳/۸
			گاهی اوقات	۱۶	۱۲	۳	۱/۱	۱۹	۴/۷
			زیاد و خیلی زیاد	۵	۳/۸	۱	۰/۴	۶	۱/۵
تخلفات رایانه‌ای علیه داده و سیستم		آگاهانه، ویروس یا هر برنامه مخرب دیگری را به سیستم دیگران انتقال داده‌ام.	اصلاً و کم	۱۲۳	۸۴/۹	۲۶۶	۹۸/۵	۳۷۹	۹۴/۱
			گاهی اوقات	۱۶	۱۲	۲	۰/۷	۱۸	۴/۵
			زیاد و خیلی زیاد	۴	۳	۲	۰/۷	۶	۰/۵

داده‌های جدول، بیانگر آنست که میزان دانشجویانی که اصلاً مرتکب این پنج تخلف نشده‌اند، بیشتر از دانشجویانی است که این رفتارها را انجام داده‌اند. کمترین میزان تخلفات در این بعد، مربوط به «انتقال و پخش ویروس به سیستم دیگران» و «هک کردن» می‌باشد که بیش از ۹۰ درصد دانشجویان، این رفتار را هرگز انجام نداده و یا به میزان کمی انجام داده‌اند. بیشترین میزان تخلفات در این بعد مربوط به «دست‌رسی غیر مجاز به اطلاعات شخصی دیگران» بوده است که ۱۰/۶ درصد از دانشجویان به میزان زیاد و یا خیلی زیادی مرتکب این رفتار شده‌اند. مقایسه میان دو جنس نشان می‌دهد که پسران بیشتر از دختران مرتکب هر یک از این پنج تخلف شده‌اند.

۳.۲. توزیع تخلفات رایانه‌ای پاسخ‌گویان بر حسب بعد فرهنگی
 جدول ۴. توزیع فراوانی و درصدی بعد فرهنگی بر حسب جنس پاسخ‌گویان

ردیف	گویه‌های تخلفات رایانه‌ای	گزینه	پسر		دختر		جمع کل	
			تعداد	درصد	تعداد	درصد	تعداد	درصد
۱	برایم پیش آمده که به شکستن قفل نرم افزار یا (کرک کردن) اقدام کنم.	اصلاً و کم	۷۸	۵۸۷/۷	۲۴۲	۸۹/۶	۳۲۰	۷۹/۴
		گاهی اوقات	۲۲	۱۶/۵	۱۹	۷	۴۱	۱۰/۲
		زیاد و خیلی زیاد	۳۳	۲۴/۸	۹	۳/۳	۴۲	۱۰/۴
۲	برایم پیش آمده که از سایت‌های غیر اخلاقی و با مضامین جنسی دیدن کنم.	اصلاً و کم	۳۷	۲۷/۸	۱۸۶	۶۸/۹	۲۲۳	۵۵/۳
		گاهی اوقات	۵۶	۴۲/۱	۶۲	۲۳	۱۱۸	۲۹/۳
		زیاد و خیلی زیاد	۴۰	۳۰/۱	۲۲	۸/۲	۶۲	۱۵/۴
۳	برایم پیش آمده که فیلم و یا تصاویر غیر اخلاقی را تماشا کنم.	اصلاً و کم	۴۹	۳۶/۸	۱۸۸	۶۹/۶	۲۳۷	۵۸/۸
		گاهی اوقات	۴۶	۳۴/۶	۵۷	۲۱/۱	۱۰۳	۲۵/۶
		زیاد و خیلی زیاد	۳۸	۲۸/۵	۲۵	۹/۲	۶۳	۱۵/۶
۴	برایم پیش آمده که فیلم‌های غیر اخلاقی را در اختیار دوستان و یا دیگران قرار بدهم.	اصلاً و کم	۷۴	۵۵/۶	۲۳۳	۸۶/۳	۳۰۷	۷۶/۲
		گاهی اوقات	۳۸	۲۸/۶	۳۱	۱۱/۵	۶۹	۱۷/۱
		زیاد و خیلی زیاد	۲۱	۱۵/۸	۶	۲/۲	۲۷	۶/۷
۵	برایم پیش آمده است، در اینترنت درباره دیگران مطالبی را منتشر کنم و یا علیه آن‌ها شایعه پراکنی نمایم.	اصلاً و کم	۱۱۸	۸۸/۷	۲۶۸	۹۹/۳	۳۸۶	۹۵/۸
		گاهی اوقات	۹	۶/۸	۲	۰/۷	۱۱	۲/۷
		زیاد و خیلی زیاد	۶	۴/۵	-	-	۶	۱/۵
۶	برای دیگران ایمیل‌های تهدید آمیز فرستاده‌ام.	اصلاً و کم	۱۰۷	۸۰/۵	۲۶۷	۹۸/۹	۳۷۴	۹۲/۸
		گاهی اوقات	۱۴	۱۰/۵	۲	۰/۷	۱۶	۴
		زیاد و خیلی زیاد	۱۲	۹	۱	۰/۴	۱۳	۳/۲

از میان شش تخلف رایانه‌ای در این بعد، کمترین میزان ارتکاب مربوط به «شایعه پراکنی علیه دیگران» می‌باشد که ۹۵/۸ درصد (۳۸۶ نفر) از دانشجویان در طول یک سال گذشته اصلاً این رفتار را انجام نداده و یا به میزان کمی آن را انجام داده‌اند. «فرستادن ایمیل‌های تهدید آمیز برای دیگران» نیز در میان دانشجویان فراوانی کمی دارد. به گونه‌ای که ۹۲/۸ درصد (۳۷۴ نفر) از دانشجویان اصلاً مرتکب این رفتار نشده‌اند و یا به میزان کمی این رفتار را انجام داده‌اند و تنها ۳/۲ درصد از آنان به میزان زیاد و خیلی زیادی مرتکب این رفتار شده‌اند. «دیدن سایت‌های غیر اخلاقی» بیشترین فراوانی تخلفات رایانه‌ای در بعد فرهنگی را در میان دانشجویان دارد، که ۱۵/۴ درصد (۶۲ نفر) از دانشجویان به میزان زیاد و خیلی زیاد و ۲۹/۳ درصد (۱۱۸ نفر) گاهی اوقات مرتکب این رفتار شده‌اند. مقایسه دو جنس نشان می‌دهد که میزان ارتکاب به هر یک از ۶ تخلف رایانه‌ای در بعد فرهنگی در دانشجویان پسر بیشتر از دانشجویان دختر می‌باشد. به عنوان مثال به عنوان مثال، ۲۸/۵ درصد از دانشجویان پسر در طول یک سال گذشته، به میزان زیاد و خیلی زیادی

فیلم‌ها و تصاویر غیر اخلاقی را تماشا کرده‌اند، در حالی که این میزان برای دانشجویان دختر ۹/۲ درصد می‌باشد.

۴.۲. توزیع تخلفات رایانه‌ای پاسخ‌گویان بر حسب ابعاد سه گانه

متغیر تخلفات رایانه‌ای از ترکیب سه بعد «علیه داده و سیستم»، «جعل هویت» و «فرهنگی» به دست آمده است. با توجه به برابر نبودن گویه‌های این سه بعد، ابعاد این متغیر هم ارز شده و سپس با یکدیگر ترکیب شده‌اند و در نهایت بر اساس دامنه نظری در سه سطح پایین، متوسط و بالا رتبه بندی شدند که در جدول شماره ۵ نشان داده شده است.

جدول ۵. توزیع فراوانی پاسخ‌گویان بر حسب میزان تخلفات رایانه‌ای

تخلفات رایانه‌ای	فرهنگی		جعل هویت		علیه داده و سیستم		تخلفات رایانه‌ای
	تعداد	درصد	تعداد	درصد	تعداد	درصد	
کم	۲۳۲	۵۷/۶	۲۱۳	۵۲/۹	۳۰۴	۷۵/۴	۲۳۱
متوسط	۱۵۲	۳۷/۷	۱۴۹	۳۷	۸۹	۲۲/۱	۱۶۱
زیاد	۱۹	۴/۷	۴۱	۱۰/۲	۱۰	۲/۵	۱۱
کل	۴۰۳	۱۰۰	۴۰۳	۱۰۰	۴۰۳	۱۰۰	۴۰۳

داده‌های جدول بیانگر آنست که نیمی از دانشجویان به میزان کمی مرتکب تخلفات رایانه‌ای شده‌اند. بیشترین میزان تخلفات در میان دانشجویان در بعد «جعل هویت» می‌باشد که ۱۰/۲ درصد (۴۱ نفر) از دانشجویان به میزان زیاد و ۳۷ درصد (۱۴۹ نفر) به میزان متوسطی مرتکب تخلفات رایانه‌ای در بعد جعل هویت شده‌اند. کمترین میزان تخلفات رایانه‌ای مربوط به بعد «علیه داده و سیستم» می‌باشد که ۷۵/۴ درصد (۳۰۴ نفر) از دانشجویان به میزان کم و ۲۲/۱ درصد (۸۹ نفر) به میزان متوسطی مرتکب این نوع از تخلفات شده‌اند.

یافته‌های تحلیلی

مدل معادلات ساختاری:

مدل‌یابی معادلات ساختاری^۱، تکنیک تحلیل چند متغیری بسیار کلی و نیرومند از خانواده رگرسیون چند متغیری است که به پژوهشگر امکان می‌دهد مجموعه‌ای از معادلات رگرسیون را به گونه هم زمان مورد آزمون قرار دهد. این مدل، یک رویکرد جامع برای آزمون فرضیه‌هایی درباره روابط متغیرهای مشاهده شده و مکنون است. از طریق این روش می‌توان قابل قبول بودن مدل‌های نظری را در جامعه‌ای خاص با استفاده از داده‌های همبستگی، غیر آزمایشی و آزمایشی آزمود. مدل سازی معادلات ساختاری به لحاظ روش شناختی از دقت بالایی برخوردار است زیرا با متغیرهای پنهان به عنوان سازه‌هایی برخورد می‌کند که در سنجش آن‌ها خطا وجود دارد و به لحاظ کاربردی

1. Structural Equation Modeling = SEM

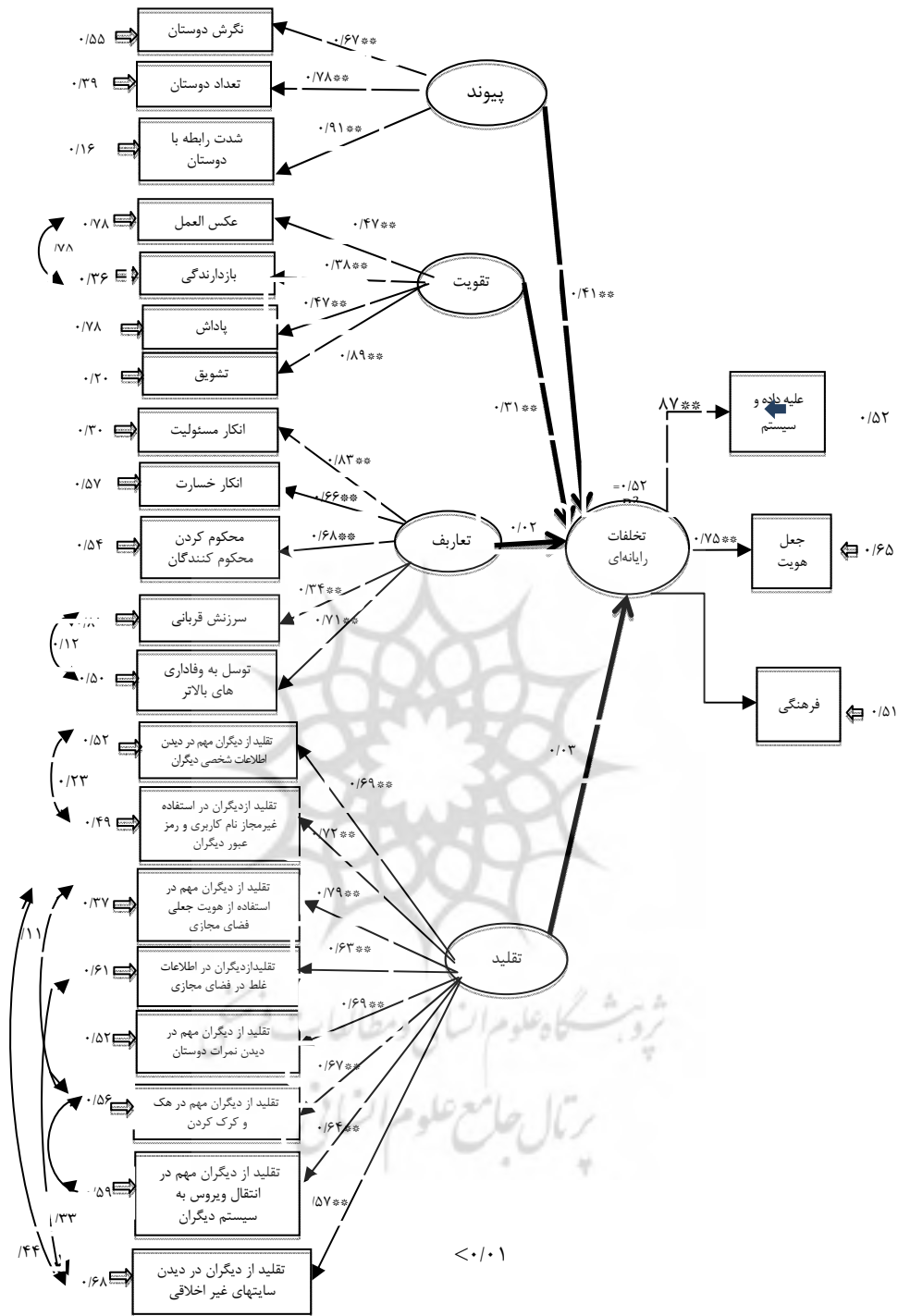
به واقعیت زندگی اجتماعی نزدیک می‌شود چرا که در فضایی چند متغیره امکان تحلیل داده‌ها را فراهم می‌آورد (هومن، ۱۳۹۱). این مدل را می‌توان با استفاده از نرم افزار LISREL تحلیل کرد و برازش آن را برای جامعه‌ای که نمونه از آن استخراج شده آزمود. شکل ۲ مدل معادلات ساختاری تحقیق را نشان می‌دهد.

داده‌های حاصل از مدل نشانگر آن است که ۵۲ درصد تغییرات تخلفات رایانه‌ای توسط متغیرهای مستقل تبیین می‌شود ($R^2=0/52$). بیشترین تأثیر بر تخلفات رایانه‌ای مربوط به متغیر پیوند افتراقی با ۰/۴۱ و بعد از آن، متغیر تقویت افتراقی با ۰/۳۱ بوده که این تأثیر معنادار می‌باشد؛ در نتیجه با افزایش پیوند و تقویت افتراقی، بر میزان ارتکاب به تخلفات رایانه‌ای افزوده می‌شود. متغیرهای تعاریف و تقلید، سهم اندکی در تبیین تخلفات رایانه‌ای داشته که البته معنادار نیز نمی‌باشد. در میان ابعاد سه گانه تخلفات رایانه‌ای، «بعد فرهنگی»، بیشترین رابطه را با تخلفات رایانه‌ای داشته است (۰/۸۹) و بعد از آن به ترتیب، بعد «علیه داده و سیستم» و «جعل هویت» با تخلفات رایانه‌ای رابطه دارند.

با توجه به آن که محاسبه کواریانس خطاهای میان متغیرها، راهی برای بهبود برازش مدل می‌باشد (براون و کادک^۱، ۱۹۹۳)، در نتیجه در این مدل، کواریانس خطای شاخص‌ها، محاسبه شده و در مدل لحاظ گردیده است. جدول (۷) شاخص‌های برازش مدل را نشان می‌دهد. آماره χ^2 دو اندازه‌ای برای نیکویی برازش است و سطح عدم تناسب بین ماتریس کواریانس نمونه و ماتریس کواریانس برازش شده را نشان می‌دهد؛ بنابراین غیرمعنادار بودن این آماره مطلوب است. با این وجود، این آماره تحت تأثیر عواملی چون حجم نمونه می‌باشد (هو و بنتلر^۲، ۱۹۹۸). مقدار این آماره در این مدل، برابر ۳۲۲/۸۲ می‌باشد و در سطح $P < 0/001$ معنادار می‌باشد. اما چون حجم نمونه، تقریباً بزرگ است ($n=403$)، معناداری آن موجه می‌نماید (یورسکاک و سوربوم^۳، ۱۹۹۳). نسبت χ^2 دو بر درجه آزادی (df) باید دارای مقدار ۲ و کمتر از آن باشد و در این مدل، این نسبت برابر با ۱/۹۲ می‌باشد که نشانگر برازش مطلوب مدل است. شاخص (RMSEA)^۵ ریشه دوم میانگین مربعات خطای برآورد می‌باشد. مقدار این شاخص در صورتی که کوچکتر از ۰/۰۵ باشد، حاکی از برازش قابل قبول مدل، بین ۰/۰۵ تا ۰/۰۸ نشان دهنده برازش تقریباً خوب، بین ۰/۰۸ تا ۰/۱ نشان دهنده برازش متوسط و بزرگتر از ۰/۱ حاکی از برازش ضعیف مدل می‌باشد (براون و کادک، ۱۹۹۳). در این مدل، مقدار این شاخص برابر با ۰/۰۴۸ می‌باشد که نشان می‌دهد، مدل از برازش خوبی برخوردار است. شاخص نرم شده برازندگی (NFI)^۶، شاخص نیکویی برازش (GFI)^۷، شاخص نیکویی برازش اصلاح

1. Browne & Cudeck
2. Chi-square
3. Hu & Bentler
4. Joreskog & Sorbom
5. Root Mean Square Error of Approximation
6. Normed fit index
7. Goodness of fit index

شکل ۲: مدل معادلات ساختاری عوامل موثر بر تخلفات رایانه‌ای



شده (AGFI)^۱ و شاخص برازندگی تطبیقی (CFI)^۲ برای مدل‌های خوب، مقادیر بالای ۰/۹۰ قابل قبول و نشانه برازندگی مدل است (هومن، ۱۳۹۱). با توجه به جدول (۷) شاخص‌های برازندگی مدل، حاکی از برازش مطلوب مدل می‌باشند. در نتیجه اگر مدلی رد نشود و شاخص‌های برازش به دست آمده از آن مناسب باشد، مدل محکم قلمداد می‌شود (بلانچ، ۲۰۰۸).

جدول ۶: ارزیابی برازش کل مدل

مقادیر شاخص‌ها	مقادیر قابل قبول شاخص‌ها	شاخص‌های برازش مدل
۰/۹۳	GFI > ۰/۹۰	Goodness of fit index (شاخص برازندگی)
۰/۹۰	AGFI > ۰/۹۰	Adjusted Goodness of Fit Index (شاخص تعدیل برازندگی)
۰/۹۶	CFI > ۰/۹۰	Comparative fit index (شاخص برازندگی تطبیقی)
۰/۹۷	NFI > ۰/۹۰	Normed Fit Index (شاخص نرم شده برازندگی)
۰/۰۴۸	RMSEA < ۰/۰۸	Root Mean Square Error of Approximation (ریشه دوم میانگین مربعات خطای برآورد)
۳۲۲/۸۲	-	Chi-Square
۰/۰۰۰۱	-	p-value
۱۶۸	-	df
۱/۹۲	Chi-Square/df < ۲	Chi-Square/df (نسبت خی دو بر درجه آزادی)

ضرایب تأثیر متغیرهای مستقل بر تخلفات رایانه‌ای به تفکیک جنسیت

جدول ۷: ضرایب تأثیر متغیرهای مستقل در ابعاد تخلفات رایانه‌ای به تفکیک جنس

مدل	بعد علیه داده و سیستم		بعد جعل هویت		بعد فرهنگی		تخلفات رایانه‌ای	
	پسر	دختر	پسر	دختر	پسر	دختر	پسر	دختر
پیوند افتراقی	۰/۳۴**	۰/۲۸**	۰/۳۲**	۰/۳۱**	۰/۴۸**	۰/۳۰**	۰/۴۳**	۰/۳۵**
تقویت افتراقی	۰/۰۶	۰/۰۷	۰/۰۷	۰/۱۳**	۰/۰۶	۰/۱۸**	۰/۰۳۱	۰/۱۶**
تقلید	۰/۰۴	۰/۰۴	۰/۱	۰/۰۰۶	۰/۰۲	۰/۰۳	۰/۰۱	۰/۰۱
تعاریف	۰/۰۰۲	۰/۱۳**	۰/۰۵	۰/۱۰*	۰/۰۶	۰/۱۵**	۰/۰۰۱	۰/۱۵**
ضریب تعیین تعدیل شده	۰/۳۸۷	۰/۲۹۲	۰/۲۸۳	۰/۳۷۷	۰/۴۱۵	۰/۳۹۲	۰/۴۴۲	۰/۴۲۸

1. Adjusted Goodness of Fit Index
2. Comparative fit index
3. Blunch

جدول (۷)، ضرایب تأثیر متغیرهای مستقل بر تخلفات رایانه‌ای و ابعاد سه گانه آن بر حسب جنسیت است. ضریب تعیین تعدیل شده نشان می‌دهد که ۴۴ درصد از تغییرات تخلفات رایانه‌ای دانشجویان پسر و ۴۲ درصد از تغییرات تخلفات رایانه‌ای دانشجویان دختر توسط متغیرهای چهارگانه مستقل تبیین می‌شود. همچنین داده‌های جدول بیانگر آن است که ۴۱ درصد تغییرات «بعد فرهنگی»، ۲۸ درصد تغییرات بعد «جعل هویت» و ۳۸ درصد تغییرات بعد «علیه داده و سیستم» در میان دانشجویان پسر توسط متغیرهای پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف تبیین می‌شود که این میزان برای دختران به ترتیب ۳۹ درصد، ۲۷ درصد و ۲۹ درصد می‌باشد. مقایسه ضرایب تأثیر استاندارد شده متغیرهای مستقل بر حسب جنسیت نشان می‌دهد که در تبیین تخلفات رایانه‌ای دانشجویان پسر، تنها متغیر پیوند افتراقی ($Beta=0/441$) معنادار می‌باشد. در تبیین تخلفات رایانه‌ای دختران، پیوند افتراقی ($Beta=0/35$) بیشترین سهم و بعد از آن به ترتیب تقویت افتراقی ($Beta=0/16$)، تعاریف ($Beta=0/15$) و تقلید ($Beta=0/1$) قرار دارند که متغیر تقلید معنادار نمی‌باشد. داده‌ها نشانگر آن است که سهم پیوند افتراقی در تبیین تخلفات رایانه‌ای پسران بیشتر از سهم آن در تبیین تخلفات رایانه‌ای دختران می‌باشد و این ادعا در مورد ابعاد سه گانه تخلفات رایانه‌ای نیز صدق می‌کند.

نتیجه گیری

تردیدی نیست که تکنولوژی تبدیل به عامل مسلطی در زندگی بشر شده است. تجربه کشورهای توسعه یافته نشان می‌دهد، به میزانی که استفاده از تکنولوژی و فناوری اطلاعات افزایش می‌یابد، پیامدها و خطرات آن نیز شیوع بیشتری می‌یابد. روند رو به افزایش جمعیت جوانان و گرایش آنان به استفاده از رایانه و اینترنت، شیوع و گسترش تخلفات و جرایم رایانه‌ای و اینترنتی را سرعت می‌بخشد. بدین ترتیب، این تحقیق درصد بررسی تبیین میزان و تخلفات رایانه‌ای در میان دانشجویان دانشگاه مازندران با تکیه بر تئوری یادگیری اجتماعی ایگز است. نتایج همبستگی میان متغیرهای مستقل و وابسته تحقیق گویای آن است که از میان چهار متغیر نظریه یادگیری اجتماعی، تنها دو متغیر پیوند افتراقی و تقویت افتراقی رابطه مثبت و مستقیم معناداری با تخلفات رایانه‌ای دارند، که از این میان، متغیر تقویت افتراقی دارای بیشترین میزان ضریب تأثیر بر تخلفات رایانه‌ای می‌باشد. فرضیات این تحقیق بر مبنای چارچوب نظری- تئوری یادگیری اجتماعی ایگز- بنا شده است که شامل یک فرضیه اصلی و چهار فرضیه فرعی می‌باشد. آزمون فرضیات تحقیق با تکیه بر مدل معادلات ساختاری صورت گرفته است. نتایج حاکی از آن است:

فرضیه اول، مدعی است بین پیوند افتراقی و تخلفات رایانه‌ای رابطه مستقیم و معناداری وجود دارد. این فرضیه مورد تأیید واقع شده است. متغیر پیوند افتراقی، قوی‌ترین و مهمترین متغیری است که بر تخلفات رایانه‌ای تأثیر می‌گذارد. به‌طور کلی، طول مدت، فراوانی و ماهیت ارتباط با دوستان عوامل تعیین کننده‌ای در ارتکاب به تخلفات رایانه‌ای می‌باشند. در نتیجه هرچه تعداد دوستان متخلف فرد و میزان رابطه‌اش با آنها بیشتر باشد و رابطه صمیمی‌تری با آنها داشته باشد، احتمال ارتکاب او به تخلفات رایانه‌ای افزایش می‌یابد. از آنجایی که گروه همسالان مهمترین زمینه اجتماعی در روابط دوستانه می‌باشد، بی شک تأثیر زیادی بر یادگیری تخلفات رایانه‌ای دارد.

دوستان می‌توانند منبعی برای یادگیری مؤلفه‌های "حرفه‌ای" تخلفات رایانه‌ای باشند (مثلاً چگونگی دور زدن یک سیستم امنیتی یا نوشتن برنامه ویروس) (اسکینر و فریام، ۱۹۹۷). از همه مهمتر، گروه همسالان جایی است که افراد در معرض هنجارهای متنوع و ارزش‌های مربوط به فعالیت‌های قانونی یا غیر قانونی رایانه‌ای قرار می‌گیرند. هم چنین، تصور فرد از نگرش دوستان صمیمی و نزدیکی نسبت به تخلفات رایانه‌ای، نقش مهمی در ارتکاب به این دسته از تخلفات بازی می‌کند. به گونه‌ای که اگر فرد تصور کند که نگرش دوستان نزدیک وی به تخلفات رایانه‌ای مثبت و مطلوب است، میزان ارتکاب او به تخلفات رایانه‌ای افزایش می‌یابد. چرا که براساس نظریه ایگز، افراد از طریق تعامل با همسالان و دوستان خود، تعاریف مطلوب و موافق جرم را فرا گرفته و آن را درونی می‌کنند. هم چنین از نظر ایگز، تصور فرد از رفتار همسالان، به اندازه رفتار واقعی آن‌ها مهم می‌باشد. به زعم وی، حتی اگر رفتار همسالان منحرف، بدرستی درک نشود، باز هم تأثیر آن‌ها از طریق این تصور، عملی خواهد شد (ایگز، ۱۹۹۸). نتایج این تحقیق همسو با تحقیقات پیشین (باسلر و باراس^۱، ۲۰۱۰، هیگینز، ۲۰۰۵؛ هیگینز و همکاران، ۲۰۰۶؛ هیگینز و ویلسون، ۲۰۰۶؛ اسکینر و فریام، ۱۹۹۷؛ گانتز، ۲۰۰۸؛ فیسک، ۲۰۰۶؛ موریس و هیگینز، ۲۰۰۹؛ ولف و هیگینز، ۲۰۰۹؛ هالت و همکاران، ۲۰۱۰) می‌باشد.

طبق نظریه ایگز، ابتدا پیوند افتراقی رخ می‌دهد که مهمترین عنصر در فرایند یادگیری اجتماعی است و شامل تعاملات منظم با دیگران در یک گروه می‌باشد. این تعاملات در توسعه تکنیک‌ها، توجیهات، انگیزه‌ها و محرک‌هایی که به یک رفتار می‌انجامد، نقش مهمی بازی می‌کنند. ارتباطات در ابتدا، معمولاً پیرامون جاذبه‌ها و موقعیت‌هایی چون همسایگی، محل سکونت خانواده و ترجیحاتی که ارتباط کمی با ارتکاب رفتارهای انحرافی دارد، شکل می‌گیرند. اگرچه در اغلب موارد، ارتکاب به رفتار انحرافی یا تمایل به آن، باعث می‌شود فرد جذب گروه همسالان منحرف شود یا گروه‌های همسالان منحرف جذب او شوند، با این حال، ارتباط بیشتر با کسانی که الگوهای رفتارهای انحرافی می‌باشند، باعث ایجاد یا تقویت رفتارهای منحرفانه می‌شود و تداوم و تکرار رابطه قدیمی و جستجوی یک رابطه جدید را تحت تأثیر قرار می‌دهد. به تعبیر ایگز، رابطه با دوستان منحرف به عنوان عاملی جهت شروع بزهکاری، مقدم بر بزهکاری به عنوان عاملی در شروع روابط منحرفانه می‌باشد. هرچند، توسعه نگرش‌ها و رفتارهای بزهکارانه قبل از ارتباط با همسالان منحرف با این نظریه ناسازگار نیست زیرا پیوند و ارتباط با گروه، پیوسته بر رفتار افراد تأثیر می‌گذارد (حتی اگر بزهکاری قبل از عضویت در گروه باشد) (ایگز و جنسن، ۲۰۰۶: ۶-۸) پژوهش‌های طولی نشان داده است که علاوه بر تداوم و استمرار بزهکاری، آغاز رفتار بزهکارانه به پیوند با گروه‌های همسالان مرتبط است (ایگز و سلرز، ۲۰۰۴: ۱۶). گروه‌های دوستان، محیط‌های اجتماعی را فراهم می‌کنند که فرد در معرض تعاریف، تقلید از الگوها و تقویت اجتماعی برای تداوم یا پرهیز از هر نوع عمل خاصی قرار می‌گیرد. تعاریف از طریق تقلید یاد گرفته می‌شوند و به وسیله اعضای گروه‌هایی که فرد با آن‌ها در ارتباط است، تقویت می‌شوند و به محض یادگیری، این تعاریف به عنوان محرکی در تداوم یا پرهیز از رفتار به کار گرفته می‌شوند. در نتیجه، هر یک از متغیرها، نقشی را در فرایند پیچیده

یادگیری رفتار قانونی یا غیر قانونی بازی می‌کنند. از طرفی، نظریه یادگیری اجتماعی بر این نکته تأکید دارد که پیوند افتراقی، در میزان تأثیرگذاری جنبه‌های متفاوت تقویت نیز مهم می‌باشد (برگس و ایکرز، ۱۹۶۶: ۱۳۱). این نقش، ناشی از این واقعیت است که پاداش‌ها یا پیامدهای منفی رفتار بستگی به این دارد که رفتار تا چه اندازه از لحاظ اجتماعی، خوب و مطلوب تعریف شود و مورد پذیرش دوستان یا کسانی که با آن‌ها در ارتباط هستیم، قرار بگیرد (ایکرز، ۱۹۹۸).

فرضیه دوم مبنی بر وجود رابطه مستقیم و معنادار بین تقویت افتراقی و تخلفات رایانه‌ای می‌باشد که مورد تأیید قرار گرفته است. بدین ترتیب هرچه میزان عکس العمل دوستان فرد نسبت به انجام تخلفات رایانه‌ای ضعیف تر باشد، رفتار فرد را مورد تأیید قرار دهند و فرد را به انجام تخلفات رایانه‌ای تشویق نمایند، در نتیجه احتمال درگیر شدن فرد در تخلفات رایانه‌ای افزایش می‌یابد. از طرفی، هر چه فرد از مجازات شدن بعد از ارتکاب تخلف، اطمینان بیشتری داشته و یقین بدارد که رفتارش مورد مجازات از سوی دوستان و نهادهای رسمی از قبیل کمیته انضباطی دانشگاه، پلیس فتا و یا نیروی انتظامی قرار می‌گیرد، احتمال این که مرتکب این دسته از تخلفات شود کمتر می‌گردد. نهایتاً افرادی که تصور می‌کنند انجام تخلفات رایانه‌ای، احساس مطلوبی برای آنان به همراه دارد، بیشتر مرتکب این تخلفات می‌شوند. برگس و ایکرز (۱۹۶۶) مدعی‌اند که صرف پیوند با کج رفتار آن کسی را کج رفتار نمی‌کند، بلکه همین افراد، کج رفتاری را در صورتی که نسبت به هم‌نوابی - با مقدار فراوانی و احتمال بیشتر - رضایت بخش تر باشد، به هم‌نوابی ترجیح خواهند داد. آن‌ها براساس قانون نیروی تقویت افتراقی می‌گویند که اگر تعدادی از عوامل، نیروهای تقویت کننده تولید کنند، آن عاملی بیشترین احتمال وقوع را دارد که بیشترین تقویت کننده را به لحاظ مقدار، فراوانی و احتمال، تولید کند (صدیق سروستانی، ۱۳۸۷: ۵۰).

طبق نظریه ایکرز، تقویت کننده‌های منفی و مثبت نقش مهمی در رفتارهای انحرافی دارند. در واقع، افراد در صورتی مرتکب اعمال مجرمانه یا بزهکارانه می‌شوند که باور داشته باشند عمل آن‌ها باعث پذیرش یا تأیید توسط دوستان و دیگران مهم گردد. همچنین اگر تجارب حاصل از انجام یک رفتار، رضایت بخش، شادی آور یا هیجان انگیز باشد و فرد به دلیل انجام آن رفتار، پاداش دریافت کند احتمال تکرار و تداوم رفتار افزایش می‌یابد. ایکرز معتقد است اگر افراد در گذشته، عملی که انجام داده‌اند تقویت شده باشد و پیامدهای منفی رفتارشان جزئی باشد در نتیجه احتمال تکرار رفتار مجرمانه افزایش می‌یابد (ایکرز و همکاران، ۱۹۷۹). پژوهش‌های پیشین «هلینگر، ۱۹۹۲؛ اسکینر و فریام، ۱۹۹۷؛ پارکر، ۱۹۹۸؛ راجرز، ۲۰۰۱؛ فیسک، ۲۰۰۶؛ هیگینز و همکاران، ۲۰۰۶» نیز فرضیه مذکور را تأیید می‌نمایند.

فرضیه سوم تحقیق، مبنی بر رابطه مستقیم و معنادار تقلید و تخلفات رایانه‌ای است که مورد تأیید قرار نگرفته است. طبق نظریه ایکرز، مشاهده رفتار دیگران مهم، تأثیر زیادی بر مشارکت در رفتارهای سازگارانه و ناسازگارانه دارد (ایکرز و سلرز، ۲۰۰۴). این فرضیه مدعی است که رفتار دیگران مهمی از قبیل اعضای خانواده، دوستان، استادان و معلمان دوره دبیرستان به عنوان الگوی فرد در تخلفات رایانه‌ای می‌باشد و هرچه تخلفات رایانه‌ای از سوی این افراد بیشتر مشاهده شود، میزان ارتکاب فرد به

تخلفات رایانه‌ای افزایش می‌باشد که در این تحقیق، این ادعا مورد قبول واقع نشده است. یافته‌های این تحقیق در تناقض با نتایج به‌دست آمده از تحقیق «اسکینر و فریام، ۱۹۹۷؛ هیگینز و همکاران، ۲۰۰۶؛ فیسک، ۲۰۰۶» می‌باشد. در تحقیق اسکینر و فریام، علاوه بر دوستان، استادان دانشگاه، خانواده، کتب و مجلات، تلویزیون، فیلم و بولتن‌های رایانه‌ای نیز منبع تقلید محسوب شده و میزان فراگیری رفتارهای انحرافی رایانه‌ای از این منابع به طور جداگانه مورد بررسی واقع شده است. در حالیکه در تحقیق حاضر، منابع تقلید در قالب یک سوال و بطور کلی مورد سنجش واقع شده است که این مسأله می‌تواند عاملی در جهت رد این فرضیه محسوب شود. همچنین، مفهوم تقلید در این تحقیق، به‌طور مستقیم ارزیابی نشده و فرض بر این بوده که با مشاهده یک رفتار یا شنیدن و یا خواندن در مورد آن، دانشجویان از این منابع یاد می‌گیرند و تقلید می‌کنند.

طبق فرضیه چهارم، بین تعاریف و تخلفات رایانه‌ای رابطه مستقیم و معناداری وجود دارد. با توجه به داده‌های حاصل از آزمون، این فرضیه تأیید نشده است. بدین ترتیب، میزان موافقت فرد با تکنیک‌های خنثی کننده شامل فنون انکار مسئولیت، انکار خسارت، سرزنش قربانی، محکوم کردن محکوم کنندگان و توسل به وفاداری‌های با ارتکاب به تخلفات رایانه‌ای رابطه‌ای ندارد. یافته‌های این تحقیق در تناقض با نتایج تحقیقات اسکینر و فریام، ۱۹۹۷؛ فیسک، ۲۰۰۶؛ موریس و هیگینز، ۲۰۰۹، می‌باشد.

این تحقیق، در پی آن بوده تا علاوه بر بررسی و تبیین تخلفات رایانه‌ای، گامی در جهت بسط تجربی نظریه یادگیری اجتماعی ایگرز بردارد. تحقیقات زیادی در حیطه جرم شناسی و جامعه شناسی وجود دارد که مرتبط با تئوری یادگیری اجتماعی بوده و موضوعات مختلفی را از قبیل آزار جسمی (ایگرز و کوکران، ۱۹۸۵؛ ایگرز و همکاران، ۱۹۷۹؛ ایگرز و لی، ۱۹۹۶؛ کرون و همکاران، ۱۹۸۵)، تقلب در دانشگاه (لرچ، ۱۹۹۹)، تخلفات عمومی (آدامز، ۱۹۹۶؛ براون فیلد و تامپسون، ۱۹۹۱)، جرایم رایانه‌ای (راجرز، ۲۰۰۱؛ اسکینر و فریام، ۱۹۹۷) و سرقت دیجیتالی (هیگینز و همکاران، ۲۰۰۶؛ هیگینز و ماکین، ۲۰۰۴؛ هیگینز و ویلسون، ۲۰۰۶؛ هیندوجا و اینگرام، ۲۰۰۸؛ اسکینر و فریام، ۱۹۹۷) شامل می‌شوند. این طیف وسیع از تحقیقات، رابطه قوی بین پیش‌بینی کننده‌های تئوریک یادگیری اجتماعی و متغیرهای وابسته یافته‌اند. ایگرز و همکارانش (۱۹۷۹) معتقدند فرآیند یادگیری اجتماعی از لحاظ تجربی، با عملیاتی کردن چهار مفهوم پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف قابل آزمون است. برای تأیید این مدعا، ایگرز بخش زیادی از تحقیقات انجام شده را مرور کرده و ادعا می‌کند که تقریباً تمامی تحقیقاتی که مبتنی بر تئوری یادگیری اجتماعی بوده‌اند، رابطه شدیدی را از لحاظ تئوریک میان متغیرهای نظریه یادگیری اجتماعی و متغیرهای وابسته یافته‌اند. به زعم وی وقتی تئوری یادگیری اجتماعی در این تحقیقات مورد آزمون قرار گرفت نسبت به دیگر نظریات مورد آزمون، با داده‌ها و نمونه‌های مشابه، واریانس بیشتری از متغیرهای وابسته را توضیح می‌دهد (ایگرز و جنسن، ۲۰۰۶). نتایج حاصل از این پژوهش حاکی از آن است که متغیرهای پیوند و تقویت افتراقی قابلیت تبیین تخلفات رایانه‌ای را دارند.

1. Lersch
2. Adams
3. Brownfield & Thompson

داده‌های تحقیق نشانگر آن است که متغیر تقویت افتراقی بیشترین قدرت تبیین‌کنندگی را داشته است. همچنین با توجه به داده‌های به‌دست آمده، متغیرهای این نظریه علاوه بر تبیین تخلفات رایانه‌ای پسران قادر به پیش‌بینی تخلفات رایانه‌ای دختران نیز می‌باشند. به‌گونه‌ای که مقایسه ضرایب تأثیر متغیرهای مستقل به تفکیک جنس، نشان می‌دهد که متغیر پیوند افتراقی سهم زیادی در تبیین تخلفات رایانه‌ای پسران در مقایسه با دختران دارد و متغیر تقویت افتراقی، تأثیر بیشتری در تخلفات رایانه‌ای دختران نسبت به پسران دارا می‌باشد. در نتیجه با توجه به سهم هر یک از این دو متغیر در تبیین تخلفات رایانه‌ای دختران و پسران، می‌توان به قابلیت این نظریه در تبیین تخلفات رایانه‌ای بین دو جنس اذعان داشت.

اگرچه داده‌های این پژوهش، از نظریه یادگیری اجتماعی حمایت می‌کند، در این تحقیق، تمام جنبه‌های این نظریه مورد بررسی واقع نشده است. بدین ترتیب، پژوهش ادعایی مبنی بر بررسی کامل این تئوری ندارد. در تحقیق حاضر، تلاش شده شاخص‌های سنجش تخلفات رایانه‌ای با توجه به شرایط اجتماعی و فرهنگی جامعه به خصوص در میان قشر دانشگاهی انتخاب شود که به تعداد معدودی از شاخص‌های این تخلفات اکتفا شده است. در نتیجه پیشنهاد می‌شود در تحقیقات آتی در این زمینه بررسی‌های تجربی بیشتری صورت بگیرد و شاخص‌های دیگری که در این تحقیق مورد بررسی واقع نشده‌اند از جمله کلاهبرداری‌های اینترنتی و تخلفات و جرایم رایانه‌ای اقتصادی مورد توجه واقع شوند.

نظریه یادگیری اجتماعی، رفتار را تابعی از پیوند افتراقی، تقویت افتراقی، تقلید و تعاریف می‌داند. در نتیجه اندیشه‌های سیاستی آن حول مفاهیم جامعه‌پذیری، آموزش، پاداش، بازدارندگی، ارزش‌ها، قوانین و ضمانت‌اجرائی آن‌ها می‌باشد. از جمله دلالت‌های سیاستی این نظریه می‌توان به دخالت در محیط‌های تربیتی و آموزشی خرد و کلان از قبیل خانواده، مدرسه، دانشگاه و محیط‌های فرهنگی و اجتماعی دیگر، در جهت افزایش آگاهی و هدایت به سمت هنجارمندی اشاره نمود. با توجه به آن‌که بخش عمده صدمات ناشی از جرایم و تخلفات رایانه‌ای به دلیل عدم آگاهی و اطلاعات است، در نتیجه آموزش و آگاه‌سازی افراد، عامل مهمی در پیشگیری و کاهش خطرات و آسیب‌های این دسته از اعمال انحرافی می‌باشد. در این میان می‌توان به نقش مهم رسانه‌ها از قبیل تلویزیون و اینترنت اشاره نمود که با ارائه اطلاعات کارآتر می‌توانند زمینه آگاهی و درک عمومی نسبت به امنیت حوزه خصوصی را فراهم نمایند. نظریه یادگیری به ما می‌گوید که رفتار بر پایه پاداش‌ها و مجازات‌های مستقیم و بی‌واسطه قرار دارد، مگر آن‌که انگیزه‌ای متمایز برای تقویت وجود پاداش‌های آتی ظاهر شود (ویلیامز و مک‌شین، ۱۳۸۸: ۲۳۷). بدین ترتیب بخشی از دلالت‌های سیاستی این نظریه به نقش قوانین و عملکرد اجرائی آن‌ها و تأکید بر ارزش‌های مهم موجود در قانون اختصاص می‌یابد که با بالابردن هزینه و کاهش نتیجه‌گیری از جرم، سعی در از بین بردن یا کاهش ارتکاب به جرم دارد. بدیهی است که فرایند یادگیری اجتماعی را نمی‌توان متوقف کرد، اما می‌توان آنچه که یادگرفته می‌شود را با تغییر دادن محیط، تغییر داد. در تلاش برای تغییر باورهای اخلاقی دانشجویان در قالب تعاریف نامطلوب جرم، می‌توان انتظار رشد اعتقادات ضد تخلفات رایانه‌ای را داشت. اگرچه کارایی این برنامه قابل تضمین نیست اما تحقیقات نشان می‌دهند که باورهای اجتماعی می‌توانند از انواع تخلفات رایانه‌ای جلوگیری به عمل آورند (گانتر، ۲۰۱۰).

منابع

- جلالی فراهانی، امیرحسین (۱۳۸۳)، پیشگیری از جرایم رایانه‌ای، *مجله حقوقی دادگستری*، ۴۷: ۸۷-۱۱۹.
- جلالی فراهانی، امیرحسین؛ باقری اصل، رضا (۱۳۸۷)، پیشگیری اجتماعی از جرایم سایبری؛ راهکارهای اصولی برای نهادینه سازی اخلاق سایبری، *ره آورد نور*، ۲۴: ۱۹-۱۰.
- خرم آبادی، عبد الصمد (۱۳۸۴)، «جرایم فناوری اطلاعات»، پایان نامه مقطع دکتری، دانشکده حقوق و علوم سیاسی دانشگاه تهران.
- رازقی، نادر (۱۳۸۹)، «شناخت آسیب‌ها و جرایم اجتماعی در فضای مجازی»، *مجموعه مقالات همایش بررسی آسیب‌های اجتماعی*، بابلسر: انتشارات دانشگاه مازندران. ۲۲۸-۲۰۷.
- راووداد، اعظم (۱۳۸۴)، مسائل اجتماعی زنان در اینترنت، *فصلنامه ایرانی مطالعات فرهنگی و ارتباطات*، ۳و۲: ۷۴-۹۰.
- رضوی، محمد (۱۳۸۷)، «پیشگیری انتظامی از جرایم سایبری»، *مجموعه مقالات نخستین همایش ملی پیشگیری از جرم*، تهران: دفتر تحقیقات کاربردی پلیس پیشگیر ناجا، ۱۴۷-۱۷۹.
- شعاع کاظمی، مهرانگیز و مهرآور مؤمنی، جاوید (۱۳۹۱)، *آسیب‌های اجتماعی نوپدید: با تأکید بر تئوری‌های زیربنایی و راهکارهای مقابله‌ای*، تهران: نشر آواری نور.
- صدیق سروسناتی، رحمت الله (۱۳۸۷)، *آسیب شناسی اجتماعی (جامعه شناسی انحرافات)*، تهران: انتشارات سمت.
- طارمی، محمد حسین (۱۳۸۷)، طبقه‌بندی و آسیب شناسی جرایم رایانه‌ای «*مجله نگاه حوزه*، ۲۴: ۲۳۶-۱۴.
- عبدالهیان، حمید (۱۳۸۴)، نوع شناسی و بازتعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران، *فصلنامه ایرانی مطالعات فرهنگی و ارتباطات*، ۳: ۱۵۴-۱۳۵.
- مرکز آمار ایران (۱۳۹۰)، *گزارش نتایج سرشماری عمومی نفوس و مسکن سال ۱۳۹۰*.
- محسنی، منوچهر (۱۳۸۶)، *جامعه‌شناسی جامعه اطلاعاتی*، تهران: نشر دیدار.
- ویلیامز، فرانک پی. مک شین، ماری لین دی (۱۳۸۸)، *نظریه‌های جرم شناسی*، ترجمه حمیدرضا ملک محمدی. تهران: میزان.
- هومن، حیدرعلی (۱۳۹۱). «مدل یابی معادلات ساختاری با کاربرد نرم‌افزار لیزرل». تهران: سمت.
- http://www.mehrnews.com/detail/News/2036106 (۱۳۹۲) خبرگزاری مهر
- http://www.pouyasazan.org/viewnews.asp (۱۳۹۱) سایت پویاسازان فناوری اطلاعات
- Akers, R. (1977), *Deviant behavior: "A social learning approach"* (2nd ed). Belmont, CA: Wadsworth Publishing Company.
- _____. (1998), *"Social learning and social structure: A general theory of crime and deviance"*. Boston: Northeastern University Press.
- _____. (1999), "Social learning and social structure: Reply to Sampson, Morash, and Krohn". *Theoretical Criminology*. 3(4): 477-493.
- Akers, R. L & Lee, G (1996), "A longitudinal test of social learning theory: Adolescent smoking". *Journal of Drug Issues*. 26: 317-343.
- Akers, R.L., & Sellers, C.S. (2004), *"Criminological theories: Introduction, evaluation, and application"* (4th ed). Los Angeles: Roxbury.
- Akers, R. L & Jensen, G. F (2006), "The empirical status of social learning theory of crime and deviance: The past, present, and future".in F.T.

- Cullen, J.P., Wright & K.R. Blevins. *Taking stock: the status of criminological theory* (pp. 37-76). New Brunswick, NJ: Transaction Publishing.
- Bossler, A. M., & Burruss, G. W. (2010), "The general theory of crime and computer hacking: Low self-control hackers?". In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 57-81). Hershey: IGI Global.
- Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, NJ: Prentice-Hall, Inc.
- Buzzell, T. (2005). "Demographic characteristics of persons using pornography in three technological contexts". *Sexuality & Culture: An Interdisciplinary Quarterly*. 9:28-48.
- Browne, M. W., & Cudeck, R. (1993). "Alternative ways of assessing model fit".
- In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 136-162). Newbury Park, CA: Sage.
- Blunch, N.J. (2008). *Introduction to structural equation modeling using SPSS and AMOS*. London: Sage.
- Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. Westport: Praeger.
- Bryce, J. (2010). "Online sexual exploitation of children and young people". In Jewkes & Yar. *Handbook of Internet Crime*. Portland: Willan Publishing.
- Burgess, R & Akers, R (1966). A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*. 14:128-147.
- Cheon, Na Jin & Hao Wu & Yong Ji & Hao Mia (2009). "Analysis of Computer Crime in Singapore Using Local English Newspaper". *Singapore Journal of Library & Information Management*. 38: 77-102.
- Dowland, P.S., Furnell, S.M., Illingworth, H.M & P. L. Reynolds (1999). "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness". *Computers & Security*. 18(6): 715-726.
- Daniel J. A (2000). "An exploration of Middle and High School Students Perceptions of Deviant Behavior When Using Computer and The Internet". *The Journal of Technology studies*. 12: 70-80.
- Foster, D. R (2004). *Can The General Theory of Crime Account for Computer Offender: Testing low Self -Control as a Predictor of Computer Crime Offending* (M.A thesis). University Of Maryland. College Park.
- Fisk, Nathan (2006). *Social Learning Theory as a Model for Illegitimate Peer-to-Peer Use and the Effects of Implementing a Legal Music Downloading Service on Peer-to-Peer Music Piracy*. (M.A thesis). Faculty of the Department of Communication Rochester Institute of Technology.
- Furnell, S (2002). *Cybercrime: Vandalizing the information society*. Boston: Addison Wesley.
- Gunter, W. D (2008). "Piracy on the High Speeds: A Test of Social Learning Theory on Digital Piracy among College Students". *Criminal Justice Science*. 3 (1): 54-68.
- Higgins, G. E. (2005). "Can low self-control help with the understanding of the software piracy problem?". *Deviant Behavior*. 26(1): 1-24.

- Higgins E, George & Feel D Brian & Wilson L, Abby (2005). "An Application of Deterrence Theory to Software Piracy". *Journal of Criminal Justice and Popular Culture*. 12 (3): 166-184.
- Higgins, G. E., & Wilson, A. L.(2006). "Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling". *Criminal Justice Studies*. 19(1): 3-22.
- Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). "Digital piracy and neutralization: A trajectory analysis from short-term longitudinal data". *International Journal of Cyber Criminology*. 2(2): 324-336.
- Higgins, G. E, Marcum. D, Freiburger, T. L & Ricketts, M. L(2012). "Examining the Role of Peer Influence and Self-Control on Downloading Behavior". *Deviant Behavior*. 33(5): 412-423.
- Hinduja, S. (2007). "Neutralization theory and online software piracy: An empirical analysis". *Ethics and Information Technology*. 9(3): 187-204.
- Hinduja, S & Ingram, J (2009). "Social learning theory and music piracy: The differential role of online and offline peer influences". *Criminal Justice Studies*. 22(4): 405-420.
- Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyber bullying*. Thousand Oaks: Sage Publications.
- Hollinger, Richard C (1992). "Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access". *Security Journal*. 2(1): 2-12.
- Holt . j, bossler. M & may. c (2010). "Low Self-Control, Deviant Peer Associations and Juvenile Cyber deviance". *American Journal of Criminal Justice*. 3: 378-395.
- Holt, T. J., & Bossler, A. M. (2009). "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization". *Deviant Behavior*. 30: 1-25.
- Hu, L., & Bentler, P. M. (1998). "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification". *Psychological Methods*. 3: 424-453.
- Joreskog, K.G., & Sorbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Chicago: Lawrence Erlbaum Associates Inc.
- Jordan, T., & Taylor, P. (1998). "Sociology of hackers". *The Sociological Review*. 46: 757-780.
- Jewkes, Y (2010). "Public policing and Internet crime". In Jewkes & Yar (PP. 525-545). *Handbook of Internet Crime*. portland: Willan Publishing.
- Kong. j, lim. J(2012). "The longitudinal influence of parent-child relationships and depression on cyber delinquency in South Korean adolescents: A latent growth curve model". *Children and Youth Services Review*. 34 : 908-913.
- Lee, K & Ha, Y (2004). "Path analysis on the relationship between Internet-related crime and related factors among juveniles". *Journal of Home Economics*. 42:127-143.
- Liang, B and Lu, H (2010). "Internet Development, Censorship, and Cyber Crimes in China". *Journal of Contemporary Criminal Justice*. 26(1): 103-120.
- McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston, MA: Pearson.

- Morris, G & Higgins, G.E (2009). "Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates". *Criminal Justice Review*. 34 (2). 173- 193.
- Moon, B. , McCluskey, D & McCluskey, P (2010). "A general theory of crime and computer crime: An empirical test". *Journal of Criminal Justice*. 38 : 767-772.
- Pratt, T. C, Cullen, F. T & Sellers, C. S & Winfree, L. T & Madensen, T & Daigle, L. E et al (2009). "The empirical status of social learning theory: A meta-analysis". *Justice Quarterly*. 27: 765-802.
- Rogers, M. K. (2001). "A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study". Unpublished doctoral dissertation. Manitoba University Canada.
- Skinner F. William & Fream M. Anne (1997). "Social Learning Theory analysis of Computer Crime among College Students". *Journal of Research in Crime and Delinquency*. 34(4):495-518.
- Smith, R.G.. (2010). "Identity theft and fraud". in Jewkes, Yvonne & Yar, Majid (eds). *Handbook of Internet Crime*. Willan Publishing: 273- 301.
- Warr, M (2002). "Companions in Crime: The Social Aspects of Criminal Conduct". New York: Cambridge University Press.
- Wall, David (2001). *Crime and Internet*. New York: Routledge.
- _____ (2005). "The Internet as a conduit for criminal activity". In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 78-94). Thousand Oaks, CA: Sage.
- Winfree, L. T , Backstrom, T. V & Mays G.L (1994). "Social Learning Theory, Self Reported Delinquency and Youth Gangs: a New Twist on a General Theory of Crime and Delinquency". *Youth society*. 26(2):147-177.
- Wolak, J., Finkelhor, D., Mitchell, K.J. and Ybarra, M.L. (2008) "Online "predators" and their victims: Myths, realities, and implications for prevention and treatment." *American Psychologist*. 63: 111-28.
- Yar, M. (2006). "Cybercrime and Society". London: Sage.

