Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

سال انتشار	۱۴۰۵	شماره انتشار	۲۷	صفحات	۱۵-۱

مطالعه عوامل محیطی و اجتماعی مؤثر بر گسترش کلاهبرداری‌های مجازی در میان گروه‌های سنی مختلف

آقای فرهود مدبر خاک‌نژاد

دانشجوی کارشناسی ارشد، رشته حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد تبریز، ایران.

چکیده

تحول بنیادین در سازوکارهای تبادل اطلاعات و استقرار مناسبات مالی در بستر سامانه‌های رایانه‌ای، بزهکاری سنتی را دچار دگردیسی ساختاری نموده و کلاهبرداری مجازی را به عنوان یکی از چالش‌های مبرم حوزه سیاست جنایی مطرح ساخته است. این پدیده مجرمانه تحت تأثیر تعامل پیچیده متغیرهای بافتی، پیرامونی و ویژگی‌های جمعیت‌شناختی بزه دیدگان بالقوه قرار دارد. هدف بنیادین پژوهش حاضر، تبیین و واکاوی نقش تعیین‌کننده عوامل محیطی و اجتماعی در شیوع کلاهبرداری‌های سایبری و تفکیک میزان آسیب‌پذیری گروه‌های مختلف سنی در مواجهه با این بزه است. روش تحقیق اتخاذ شده در این مطالعه مبتنی بر رویکرد توصیفی- تحلیلی بوده و گردآوری داده‌ها با استفاده از ابزار کتابخانه‌ای و استناد به منابع معتبر فقهی، حقوقی و جامعه‌شناختی صورت پذیرفته است. یافته‌های تحقیق دلالت بر آن دارد که بسترهای محیطی نظیر ضریب نفوذ اینترنت پرسرعت، همراه با گمنامی ساختاری در فضای مجازی و ناکافی بودن پایش‌های فنی، محیطی تسهیل‌کننده برای کنش مجرمانه فراهم می‌آورند. افزون بر آن، متغیرهای اجتماعی و اقتصادی از قبیل شکاف نسلی دیجیتال، بحران‌های معیشتی و کمبود آگاهی‌های حقوقی، گروه‌های سنی خردسال، جوانان و سالمندان را با الگوهای بزه‌دیدگی متفاوتی روبرو می‌سازد. بدین ترتیب، نتیجه‌گیری پژوهش نشان می‌دهد که اتکای صرف بر ابزارهای واکنشی کیفری از بازدارندگی لازم برخوردار نبوده و مهار بهینه این جرایم مستلزم اتخاذ تدابیر پیشگیرانه وضعی و اجتماعی، ارتقای سواد حقوقی جامعه و تقویت معماری امنیت سامانه‌ها بر مبنای مختصات جمعیتی آسیب‌پذیر است.

واژگان کلیدی: کلاهبرداری مجازی، فضای سایبر، عوامل محیطی، بزه‌دیدگی، پیشگیری وضعی، گروه‌های سنی.

طبقه‌بندی JEL : فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

A Study of Environmental and Social Factors Influencing the Proliferation of Virtual Fraud Across Different Age Groups

Abstract

The expansion of digital communication and the widespread transition of financial transactions into cyberspace have transformed virtual fraud into one of the most pressing challenges of the modern era. This study, employing a descriptive-analytical method and library-based research, examines the environmental and social factors contributing to the proliferation of online fraud, with a specific focus on variations across different age groups. The findings indicate that structural characteristics of the virtual environment, including relative anonymity, the transnational nature of interactions, and high-speed financial transactions, systematically generate criminal opportunities and undermine the efficacy of conventional enforcement mechanisms. Furthermore, social determinants, such as socioeconomic vulnerabilities, gaps in digital literacy, and deficient institutional and familial oversight, accelerate rates of victimization. The research demonstrates a marked divergence in victimization patterns across age cohorts: children and adolescents are predominantly targeted through gaming environments and social engineering, youth and adults frequently fall prey to fraudulent investment schemes and fake employment offers driven by financial incentives, while the elderly remain particularly vulnerable to impersonation of authority figures due to digital literacy disparities. Consequently, reducing the prevalence of virtual fraud necessitates moving beyond post-offense punitive models toward targeted situational and social prevention strategies tailored to the behavioral and cognitive realities of distinct age demographics.

Keywords: : Virtual Fraud, Cyberspace, Environmental Factors, Victimization, Situational Prevention, Age Groups

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

متن مقاله

گذار از جامعه صنعتی به عصر داده‌محور، ساختار کنش‌های انسانی و صورت‌بندی جرایم مالی را با دگرگونی بنیادین روبرو ساخته است. یکی از مهم‌ترین تجلیات این پدیده، بازتولید بزه سنتی کلاهبرداری در قالب جرایم رایانه‌ای و ظهور تدلیس سایبری است. این شیوه مجرمانه با تکیه بر ویژگی‌های ذاتی فضای مجازی نظیر سرعت فوق‌العاده انتقال داده، فرامرز بودن ارتباطات، استتار هویت و کاهش هزینه‌های عملیاتی بزهکاران، تهدیدی روزافزون علیه امنیت اقتصادی شهروندان ایجاد نموده است. اهمیت پرداختن به این مبحث از آن روی مضاعف می‌گردد که ارکان وقوع این جرایم صرفاً بر تصمیم‌گیری فردی مرتکب متکی نبوده، بلکه تحت تأثیر مستقیم ساختارهای محیطی و بافت اجتماعی میزبان بازتولید می‌شود.

در تحلیل جرم‌شناختی پدیده‌های مجرمانه در فضای سایبر، درک ارتباط میان عوامل اجتماعی، محیط پیرامونی و مشخصه‌های بزه دیدگان از جایگاه محوری برخوردار است. شرایط کلان اقتصادی، احساس ناامنی معیشتی، عدم توازن در سواد رسانه‌ای و کاستی‌های موجود در نظارت نهادهای متولی، وضعیتی مساعد را برای فریب کاربران فراهم می‌سازد. از سوی دیگر، توزیع سنی کاربران و ویژگی‌های روان‌شناختی هر نسل، الگوهای متمایزی از بزه‌دیدگی را پدید می‌آورد؛ جوانان به واسطه جسارت در انجام تعاملات نوین اقتصادی آنلاین و سالمندان در نتیجه عدم انطباق با ظرافت‌های فنی و سواد دیجیتال، در معرض فریب متقلبانه بزهکاران قرار می‌گیرند. شناخت این تمایزات، نقطه آغازینی برای تدوین راهبردهای واقع‌بینانه در حوزه سیاست کیفری به شمار می‌رود.

با وجود تدوین اسناد بین‌المللی و وضع مقررات خاص نظیر قانون جرایم رایانه‌ای در نظام حقوقی ایران، هنوز شکاف‌های عمیقی در کارآمدی تدابیر مقابله‌ای به چشم می‌خورد. ناتوانی رویکردهای تک‌بعدی کیفری در انسداد مسیرهای مجرمانه، ضرورت مداقه در متغیرهای وضعی و بسترهای اجتماعی را آشکار ساخته است. پژوهش حاضر بر آن است تا با رویکردی تلفیقی میان حقوق کیفری و جرم‌شناسی محیطی، عوامل تسهیل‌کننده کلاهبرداری مجازی را شناسایی نماید. از این منظر، تحقیق به واکاوی ریشه‌های پیرامونی و تأثیرات پایگاه‌های اجتماعی بر گرایش به این جرم و قربانی شدن اقشار گوناگون خواهد پرداخت تا در امتداد آن، افق‌های نوینی پیش روی پیشگیری وضعی و مداخله‌های قانونی ترسیم گردد.

۱- مفهوم کلاهبرداری مجازی

در حقوق کیفری کلاسیک، رکن مادی کلاهبرداری مستلزم اغفال شخص حقیقی، فریب متقلبانه قربانی و در پی آن، تسلیم ارادی مال ناشی از اشتباه بزه دیده است. حال آنکه در پهنه فضای سایبر، این تقلب غالباً نه از طریق ارتباط چهره به چهره یا اقناع فکری یک انسان، بلکه با دور زدن منطق برنامه‌ریزی‌شده سامانه‌های پردازش داده محقق می‌گردد. تغییر در داده‌ها یا ایجاد اختلال در فرایند رایانه‌ای به منظور انتقال نامشروع مال، هویت مفهومی این جرم را نسبت به مدلول ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری متمایز ساخته است. بزه کلاهبرداری مرتبط با رایانه در ماده ۱۳ قانون جرایم رایانه‌ای تجلی یافته است. قانون‌گذار با تصریح بر اعمالی نظیر ورود، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، بر تمایز بنیادین سازوکار ارتکاب این بزه تأکید ورزیده است. شرط اساسی در این بستر، عدم ضرورت اغفال مغز انسانی در تمامی شقوق جرم است؛ هرچند مواردی همچون مهندسی اجتماعی همچنان قربانی انسانی را هدف قرار می‌دهد، لیکن دستکاری نرم‌افزاری سامانه‌ها و انتفاع بلاجهت مرتکب، مصداق بارز این تدلیس الکترونیکی به شمار می‌آید. از این رهگذر، عنصر قانونی جرم با عنایت به خصیصه غیرملموس داده‌ها تدوین یافته است (باستانی، ۱۳۸۳، ص ۲۸).

بررسی عنصر روانی این بزهکاری آشکار می‌سازد که قصد مجرمانه در کلاهبرداری مجازی آمیخته‌ای از سوءنیت عام و سوءنیت خاص است. سوءنیت عام متضمن آگاهی مرتکب به غیرمجاز بودن عملیات مداخله‌گرانه بر روی سامانه‌ها یا محتواهای دیجیتال بوده و اراده آزاد در انجام افعال پیش‌گفته را می‌طلبد. از سوی دیگر، سوءنیت خاص در قصد

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

تحصیل مال، وجه، منفعت یا امتیازات مالی برای خود یا دیگری تبلور می‌یابد. پیچیدگی فنی افعال ارتکابی و تدارک ابزارهای پنهان‌ساز، نمایانگر اصرار آگاهانه بر نقض منافع مالی مجنی‌علیه بوده و امکان انتساب خطا یا غفلت محض را در احراز مسئولیت کیفری مرتکب سلب می‌کند (خداقلی، ۱۳۸۴، ص ۳۱).

در تبیین تطبیقی این مفهوم با بسترهای سنتی، عنصر نتیجه مجرمانه از حساسیت بسزایی برخوردار است. خروج مال از تصرف قانونی بزه دیده و ورود ضرر مسلم مادی، شاکله تکوین‌یافته نتیجه مجرمانه را بازنمایی می‌کند. در قلمرو مجازی، ضرر مادی ممکن است به صورت کسر وجوه از حساب‌های بانکی، ربودن دارایی‌های رمزنگاری‌شده یا انتقال مالکیت سهام در سامانه‌های معاملاتی تحقق پذیرد. گستره وسیع مال در حقوق جزا امروزه منافع الکترونیکی دارای ارزش مبادله‌ای را در بر می‌گیرد؛ از همین رو، انتزاعی بودن این منافع مانع از تطبیق تعریف کلاهبرداری مجازی نبوده و ضرورت بازخوانی مستمر مبانی مسئولیت کیفری را در عصر سامانه‌ها آشکار می‌سازد.

۲- بسترهای محیطی و اجتماعی شکل‌گیری کلاهبرداری‌های مجازی

تکوین جرایم سایبری را نمی‌توان پدیده‌ای منتزع از ساختار محیط پیرامونی و بسترهای کلان اجتماعی مورد واکاوی قرار داد. بر مبنای نظریات جرم‌شناسی، کنش مجرمانه نتیجه تلاقی یک بزهکار باانگیزه، یک هدف مناسب و فقدان محافظ آگاه در زمان و مکان مشخص است. فضای سایبر به منزله یک بستر محیطی بازتعریف‌شده، فواصل جغرافیایی را بی‌اثر ساخته و گستره بی‌سابقه‌ای از اهداف مناسب را در معرض دسترسی بزهکاران بالقوه می‌گذارد. دگرگونی در معماری ارتباطات اجتماعی، موقعیت‌های متعددی را می‌آفریند که پیش از این در فضاهای فیزیکی سابقه نداشته و این بافت نوین، بستر زایش شیوه‌های فریبکارانه نوین را شکل داده است (افشانی و همکاران، ۱۳۹۶، ص ۲۱۲).

در عرصه مناسبات جمعی، دگرگونی در الگوهای اعتماد عمومی نقشی تعیین‌کننده در گسترش بستر فریب مجازی ایفا می‌کند. گذار پرشتاب از روابط مبتنی بر شناخت مستقیم به تعاملات بی نام و نشان در پلتفرم‌های شبکه‌ای، ساختار سنجش ریسک را در میان شهروندان مخدوش ساخته است. بزهکاران با بهره‌گیری از ضعف سازوکارهای اعتبارسنجی اجتماعی و ایجاد هویت‌های دروغین، خود را در قالب نهادهای رسمی یا عرضه‌کنندگان کالا و خدمات معرفی می‌کنند. کاهش سطح انسجام اجتماعی در دنیای واقعی و اتکای فزاینده به شبکه‌های مجازی، سرمایه اجتماعی را آسیب‌پذیر نموده و سازوکارهای سنتی دفاع فردی در برابر تدلیس را خلع سلاح می‌نماید (باطبی، ۱۴۰۵، ص ۳).

ساختار پلتفرم‌های پیام‌رسان و درگاه‌های پردازش اطلاعات، محیطی ویژه با ویژگی‌های انحصاری بازتولید کرده‌اند. طراحی‌های کاربری فاقد استانداردهای امنیتی سخت‌گیرانه و تقدم سهولت دسترسی بر تدابیر حفاظتی، فرصت‌های فراوانی برای تولید محتواهای گمراه‌کننده می‌آفرینند. در این فضا، محیط به مثابه ابزار جرم عمل نموده و دستکاری نشانه‌ها، کدهای بصری و تائیدیه‌های جعلی را ممکن می‌گرداند. افزون بر این، تحولات سریع فناورانه مانع از تکوین هنجارهای نظارتی هماهنگ میان کاربران گردیده و این تأخر محیطی، فرصت‌های مغتنمی در اختیار بزهکاران برای بهره‌برداری از ناآگاهی جمعی قرار می‌دهد (رحمانی و خلیلی، ۱۳۹۰، ص ۵).

مجموعه فرایندهای یادشده نشان‌دهنده آن است که بسترسازی محیطی و اجتماعی، پیوندی لاینفک با شیوه زیست مدرن یافته است. جامعه‌پذیری سایبری نسل‌های نوپا بدون درونی‌سازی اصول احتیاطی، هم‌زمان با انزوای نسبی گروه‌های مسن‌تر در تطبیق با سامانه‌ها، شکافی ساختاری در تاب‌آوری عمومی پدید آورده است. هنگامی که تعاملات حیاتی روزمره از قبیل پرداخت‌ها، تدارکات و تفریحات به این محیط انتقال می‌یابد، احتمال تقاطع منافع نامشروع با زیست روزمره به بالاترین میزان خود می‌رسد. در نتیجه، واکاوی بسترها نه یک موضوع جنبی، بلکه رکن رکین ادراک چرایی وقوع کلاهبرداری کلان در سامانه نوین اجتماعی قلمداد می‌شود.

۳- عوامل محیطی مؤثر بر گسترش کلاهبرداری‌های مجازی

تحلیل ساختار محیطی جرایم مجازی بیانگر آن است که ویژگی‌های حاکم

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

بر بستر دیجیتال به طور مستقیم بر نرخ ارتکاب و تنوع شیوه‌های کلاهبرداری اثرگذار است. در جرم‌شناسی وضعی، محیط صرفاً صحنه نمایش جرم نبوده، بلکه عامل تعیین‌کننده در ترغیب یا بازداری مرتکب محسوب می‌شود. هنگامی که مختصات یک فضا بر پایه گمنامی، عدم قطعیت در رهگیری و محو ردپای مجرمانه سامان یافته باشد، احساس مصونیت از تعقیب قضایی در مرتکب تقویت می‌گردد. این ویژگی‌های وضعی فضای سایبر، آستانه مقاومت اخلاقی بزهکاران بالقوه را فروریخته و انگیزه انتفاع مالی نامشروع را از قوه به فعل درمی‌آورد. فراملیتی بودن و بی‌مرزی حاکم بر زیرساخت‌های محیطی شبکه، چالش‌های ژرفی در قلمرو صلاحیت سرزمینی مراجع قضایی پدید آورده است. بزهکار با استقرار در یک حوزه قضایی، داده‌ها را در کشوری ثانی ذخیره نموده و وجوه حاصل از تقلب را از طریق مجاری مالی بدون مرز نظیر رمزارزها در کشوری ثالث جابجا می‌سازد. این خصلت شبکه‌ای محیط، تعقیب کیفری را به شدت طولانی و با مانع روبرو ساخته و نرخ کشف جرم را تقلیل می‌دهد. فقدان تقارن اطلاعاتی میان مجریان قانون و تبهکاران در محیط‌های نامتمرکز، ریسک دستگیری را به حداقل رسانده و پیامد این امر، گسترش تصاعدی رفتارهای مجرمانه در غیاب بازدارندگی مؤثر است (جعفری و عبادی نفط چالی، ۱۴۰۵، ص ۳).

دسترسی‌پذیری آسان به کدها و ابزارهای خرابکارانه در محیط‌های تحت وب، وجه محیطی دیگری از تشدید بزهکاری است. امروزه نیاز به مهارت‌های پیچیده برنامه‌نویسی برای ارتکاب کلاهبرداری الکترونیکی رنگ باخته و پدیده‌ای موسوم به جرم به مثابه خدمت در گوشه‌های پنهان اینترنت رواج یافته است. بزهکاران کم‌تجربه با بهره‌برداری از صفحات آماده جعل درگاه و ابزارهای توده‌ای ارسال پیامک‌های فریبنده، وارد چرخه بزه‌کاری می‌شوند. ساختار محیط به گونه‌ای است که امکان توزیع انبوه پیام‌های جعلی را با کمترین هزینه مالی ممکن می‌سازد و بخت صید طعمه‌ها را به میزان قابل توجهی ارتقا می‌دهد (رحمتی و سیفی، ۱۴۰۰، ص ۲۸).

پیچیدگی ساختاری محیط‌های مجازی به گونه‌ای است که حتی تغییرات فنی کوچک در پروتکل‌های ارتباطی می‌تواند جغرافیای بزه‌دیدگی را متحول سازد. وابستگی اجتناب‌ناپذیر تمامی سطوح حیات فردی به اتصالات داده‌ای، محیط پیرامون کاربر را آکنده از نقاط آسیب‌پذیر ساخته است. عدم انطباق سرعت پیشرفت شیوه‌های دفاعی با شگردهای هجومی تدلیس‌گران، محیط شبکه را به بستری نامتعادل به نفع مهاجم بدل نموده است. بنابراین، عوامل پیرامونی نقشی محوری در گسترش کمی و کیفی این جرایم ایفا کرده و مهار آنها مستلزم دگرگون‌سازی تدابیر امنیتی در بطن طراحی زیرساخت‌ها خواهد بود.

۱-۳- دسترسی گسترده به فناوری و فضای مجازی

توسعه روزافزون زیرساخت‌های مخابراتی، فراگیری اینترنت نسل نوین و دسترسی ارزان به تجهیزات پردازشی، زمینه را برای نفوذ همه‌جانبه ابزارهای دیجیتال در تمام لایه‌های اجتماع فراهم کرده است. اگرچه گسترش پهنای باند و توزیع ابزارهای متصل به شبکه به عنوان شاخص توسعه‌یافتگی جوامع تلقی می‌شود، اما هم‌زمان به مثابه گسترش دامنه فرصت‌های مجرمانه عمل می‌کند. زمانی که جامعه بدون تمهید زمینه‌های آموزشی و بدون توجه به ظرفیت‌های صیانتی به سمت دیجیتالی شدن مطلق سوق داده شود، جمعیت آسیب‌پذیر بدون سپر دفاعی کافی به فضایی وارد می‌گردند که مخاطرات مالی فراوانی در کمین آنان است. وفور درگاه‌های پرداخت، نرم‌افزارهای مدیریت مالی روی تلفن‌های همراه و سهولت جابجایی وجوه، سرعت وقوع کلاهبرداری را شتاب بخشیده است. تسریع فرایندهای مالی به همان میزان که کارایی اقتصادی را بالا برده، زمان تأمل و امکان بازنگری کاربر را پیش از اتخاذ تصمیمات زیان‌بار به حداقل تقلیل داده است. مرتکبان با اتکا به همین دسترسی بی‌وقفه و با ارسال پیام‌های حاوی فوریت‌های دروغین مالی، افراد را در موقعیت تسلیم شتاب‌زده اطلاعات حساس قرار می‌دهند. دسترسی دائم به ارتباطات آنلاین سبب شده است تا قربانیان در هر لحظه از شبانه‌روز و در هر موقعیت مکانی در معرض حملات مهندسی اجتماعی قرار گیرند (باباحسن-زاده و حیدرنژاد، ۱۴۰۴، ص ۶).

تنوع‌بخشی به ابزارهای دسترسی، دایره شمول کاربران را به گروه‌های با

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

سواد اطلاعاتی محدود بسط داده است. پیش‌تر، بهره‌مندی از امکانات سایبری مستلزم سطحی از دانش فنی بود که نوعی خودکنترلی را بر فضا حاکم می‌کرد؛ اما رابط‌های کاربری ساده‌سازی‌شده کنونی، افراد با حداقل آگاهی را نیز به سوی مراودات پولی مجازی هدایت می‌کنند. این گروه از کاربران، به دلیل ناتوانی در اعتبارسنجی منابع دیجیتال و عدم درک لایه‌های زیرین نرم‌افزارها، به سهولت تسلیم ادعاهای غیرواقعی می‌گردند. در واقع، دموکراتیزه شدن افراطی دسترسی به فناوری، بستری برای ایجاد تله‌های مالی گسترده از سوی شیادان رایانه‌ای پدید آورده است (معتمدنژاد، ۱۳۹۰، ص ۵۳).

پیامد مستقیم این دسترسی فراگیر، تکثیر بی‌رویه نقاط انتهایی آسیب‌پذیر در معماری شبکه است. هر تلفن هوشمند متصل به اینترنت به مثابه روزنه‌ای بالقوه برای نفوذ و فریب محسوب می‌شود که دفاع از تمام آن‌ها برای نظام‌های نظارتی ناممکن می‌نماید. مرتکبان جرایم مالی با آگاهی از این واقعیت، کارزارهای تقلب خود را نه بر رخنه به سرورهای مستحکم، بلکه بر دستکاری ذهن کاربران پرشمار این سامانه‌ها مستقر می‌کنند. بدین ترتیب، شتاب توسعه اتصال‌پذیری دیجیتال در صورتی که با افزایش مهارت‌های بازدارنده همراه نباشد، مستقیماً به بسترسازی برای شکوفایی آمارهای کلاهبرداری مجازی منجر خواهد گردید.

۲-۳- ضعف نظارت و کنترل در محیط‌های مجازی

نظارت و اعمال کنترل قانونی همواره با چالش‌های ساختاری، فنی و حقوقی مواجه بوده است. ماهیت غیرمتمرکز شبکه و حجم غیرقابل سنجش داده‌های مبادله‌شده، اعمال پایش متمرکز را برای دستگاه‌های حاکمیتی و نهادهای ناظر فوق‌العاده دشوار می‌سازد. از سوی دیگر، ضرورت احترام به حریم خصوصی شهروندان و حفظ آزادی‌های مشروع، اعمال نظارت‌های حداکثری و پیشگیرانه را در تنگناهای موازین قانونی و حقوق بشری قرار می‌دهد. این تضاد بنیادین میان امنیت عمومی و حفظ حریم خصوصی، مناطقی خاکستری در فضای دیجیتال ایجاد کرده که به جولانگاه امنی برای کلاهبرداران بدل شده است. ضعف سازوکارهای احراز هویت در بسترهای ثبت سیم‌کارت‌ها، افتتاح حساب‌های بانکی آنلاین و تخصیص درگاه‌های واسط، نقصی زیرساختی در زنجیره کنترل محسوب می‌شود. استفاده مکرر بزهکاران از هویت‌های جعلی یا حساب‌های اجاره‌ای متعلق به افراد بی‌خانمان و معتادان متجاهر، سلسله‌مراتب پی‌جویی مجرمانه را به بن‌بست می‌کشاند. در بسیاری موارد، فقدان یکپارچگی میان سامانه‌های قضایی، بانکی و انتظامی سبب اطاله زمان مسدودسازی حساب‌های مبدأ و مقصد گردیده و به کلاهبردار فرصت کافی برای تبدیل عواید جرم به دارایی‌های نقدناپذیر یا دارایی‌های رمزنگاری‌شده را اعطا می‌کند (امانی کلاریجانی، ۱۳۹۶، ص ۹۳).

کاستی‌های نظارتی در پلتفرم‌های خارجی و شبکه‌های اجتماعی نامحدود، بعد دیگری از این معضل را هویدا می‌سازد. بخش اعظم اقدامات متقلبانه در محیط‌هایی طراحی و اجرا می‌شود که خارج از حوزه اعمال حاکمیت ملی و مقررات‌گذاری سرزمینی فعالیت می‌کنند. عدم پایبندی این پلتفرم‌ها به تعامل با ضابطان قضایی، حذف کانال‌های جعلی و افشای مشخصات فنی مجرمان را ناممکن یا بسیار زمان‌بر می‌سازد. این مصونیت عملکردی در محیط‌های پیام‌رسان فرامرزی، کلاهبرداران را تشویق می‌کند تا بدون بیم از تعقیب، الگوهای فریب خود را در ابعادی گسترده و به شکل علنی به نمایش بگذارند (همان، ص ۹۴).

در پایان می‌توان دریافت که ناکارآمدی کنترل‌ها بیش از آنکه حاصل تعلل ارگان‌ها باشد، ریشه در خصلت پویای فناوری دارد. مقررات نظارتی سنتی همواره گامی عقب‌تر از پیشرفت ابزارهای مجرمانه حرکت می‌کنند و این عقب‌ماندگی قانونی، قدرت واکنش به‌موقع را سلب می‌نماید. نبود سامانه‌های کشف برخط تقلب بر پایه هوش مصنوعی در شبکه بانکی و عدم وجود رصدهای مستمر سایبری، سبب شده است نظارت‌ها از حالت پیشگیرانه به رویکردهای پسینی و انفعالی تقلیل یابد. از این رو، اصلاح بنیادی نظام‌های کنترلی بر پایه همکاری‌های فرابخشی و ابزارهای هوشمند احراز هویت، ضرورتی اجتناب‌ناپذیر برای مقابله با این معضل به شمار می‌آید.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

۳-۳- شرایط اقتصادی و اجتماعی محیط

شرایط نامساعد اقتصادی همواره به عنوان یکی از پیش‌ران‌های اصلی در پدیداری و تشدید رفتارهای ضد اجتماعی و جرایم مالی شناسایی شده است. در دوره‌های رکود تورمی، کاهش شدید ارزش پول ملی و افت توان معیشتی، فشارهای فزاینده‌ای بر اقشار مختلف مردم تحمیل می‌گردد. بر مبنای نظریه فشار رابرت مرتون، هنگامی که میان اهداف فرهنگی مقبول نظیر دستیابی به رفاه و ابزارهای مشروع دستیابی به آن شکاف عمیق ایجاد شود، تمایل به نوآوری‌های نامشروع تقویت می‌شود. کلاهبرداری مجازی در این بافت، به عنوان شیوه‌ای سریع و کم‌هزینه برای کسب درآمد نامشروع از سوی افرادی که در تنگنا قرار دارند برگزیده می‌شود. همین وضعیت اقتصادی ناپایدار، ساختار روانی جامعه مخاطب را نیز به شدت دگرگون و پذیرای فریب می‌نماید. افراد تحت فشار دغدغه‌های معیشتی، در مواجهه با پیام‌های گمراه‌کننده‌ای که وعده سودهای کلان، پرداخت وام‌های فوری بدون ضامن یا سرمایه‌گذاری‌های پرسود را می‌دهند، به راحتی مسلوب‌الاختیار می‌شوند. تقلیل قدرت تحلیل عقلانی تحت تأثیر اضطراب اقتصادی، بستر مناسبی را برای اجرای فنون مهندسی اجتماعی پدید می‌آورد. طمع کاذب که غالباً ریشه در درماندگی اقتصادی دارد، قربانی را وادار می‌سازد تا از اصول اولیه مراقبت و راستی‌آزمایی چشم‌پوشی کرده و سرمایه اندک خویش را در طبق اخلاص فریبکاران نهد (باطبی، ۱۴۰۵، ص ۷).

علاوه بر ابعاد مادی، آشفتگی‌های ساختار اجتماعی و زوال ارزش‌های اخلاقی جمعی نیز بر شتاب این فرایند می‌افزاید. گسترش فرهنگ مادی‌گرایی، تمایل به کسب ثروت بادآورده و تغییر نگرش نسل جوان نسبت به زحمت و کار مشروع، انگیزه‌های ارتکاب تخلفات مالی را تسهیل می‌نماید. در محیط‌هایی که موفقیت صرفاً با شاخص‌های مصرفی سنجیده می‌شود، بازدارنده‌های وجدانی رنگ باخته و قبح فریب دیگران در بستر غیرشخصی فضای مجازی شکسته می‌شود. مرتکب با پنهان شدن در پس صفحه‌کلید، خود را نه یک دزد، بلکه فردی زرنگ تلقی می‌کند که از غفلت بزه دیده ارتزاق نموده است (امیدوار و صارمی، ۱۳۸۱، ص ۴۸).

در فرجام این مبحث، آشکار می‌گردد که تکوین جرایم سایبری با منظومه شاخص‌های توسعه پایدار و رفاه اجتماعی پیوندی ناگسستنی دارد. هرگونه انباشت ناکامی‌های شغلی، نابرابری در توزیع فرصت‌ها و تضعیف تورهای حمایتی دولت، مستقیماً نرخ کلاهبرداری‌های مجازی را از دو سو تحریک می‌کند؛ نخست با تأمین نیروی انسانی تازه برای ارتکاب جرم و سپس با تولید قربانیان مستعد و کم‌طاقت. بر این مبنا، کاربست راهکارهای صرفاً انتظامی بدون التیام‌بخشی به شکاف‌های اقتصادی و ساختاری، قادر به خشکاندن ریشه‌های رو به تزاید کلاهبرداری در متن جامعه نخواهد بود.

۴- عوامل اجتماعی مؤثر بر گسترش کلاهبرداری‌های مجازی

گسترش کلاهبرداری‌های مجازی تنها به ضعف‌های فنی سامانه‌ها یا مهارت مرتکبان وابسته نیست، بلکه محیط اجتماعی نیز در شکل‌گیری فرصت‌های مجرمانه و افزایش شمار بزه‌دیدگان نقش مهمی دارد. افراد در خانواده، مدرسه، محل کار، گروه‌های دوستانه و شبکه‌های اجتماعی، شیوه استفاده از فناوری و نحوه مواجهه با پیام‌ها و پیشنهادهای مالی را می‌آموزند. هر اندازه این فرایند با آموزش، نظارت و تقویت مسئولیت‌پذیری همراه باشد، احتمال گرفتار شدن در دام فریب‌های اینترنتی کاهش می‌یابد (افشانی و همکاران، ۱۳۹۶، ص ۲۲۱).

روابط اجتماعی می‌تواند هم نقش حمایتی داشته باشد و هم به عامل آسیب‌زا تبدیل شود. اعتماد بیش از اندازه به اعضای گروه، پذیرش توصیه‌های افراد ناشناس و انتقال سریع پیام‌های تأییدنشده، زمینه گسترش شایعات و تبلیغات فریبنده را فراهم می‌کند. بسیاری از کلاهبرداری‌ها از طریق پیام‌هایی سوی دوستان، بستگان، همکاران یا مؤسسات معتبر ارسال شده‌اند. همین امر موجب می‌شود مخاطب بدون بررسی منبع پیام، به آن اعتماد کند. در برخی موارد، بزهکاران با ایجاد شبکه‌های اجتماعی جعلی و استفاده از تبلیغات گسترده، خود را بخشی از یک گروه معتبر معرفی می‌کنند. عضویت ظاهری افراد متعدد در یک کانال، صفحه یا گروه اینترنتی نیز می‌تواند نوعی اعتبار کاذب ایجاد کند. مخاطب با مشاهده تعداد زیاد دنبال‌کنندگان یا پیام‌های رضایت‌مندانه، تصور می‌کند فعالیت موردنظر قانونی و قابل اعتماد است؛ در حالی که

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

بسیاری از این حساب‌ها و پیام‌ها ممکن است ساختگی یا هدایت‌شده باشند(Chi hung, ۲۰۰۵, p ۲۷۴).

به نظر نگارنده، مقابله با این عامل مستلزم تقویت اعتماد اجتماعی آگاهانه است. شهروندان باید بیاموزند که اعتماد در فضای دیجیتال باید بر پایه نشانه‌های قابل بررسی، هویت روشن و اطلاعات مستقل شکل گیرد. خانواده، مدرسه، رسانه و نهادهای عمومی در این زمینه مسئولیت مشترک دارند و نمی‌توان تمام بار پیشگیری را بر عهده کاربر گذاشت.

۴-۱- نقش خانواده و نظارت خانوادگی

خانواده نخستین محیطی است که در آن الگوهای رفتاری، میزان احتیاط و شیوه مواجهه با خطرات به فرد آموزش داده می‌شود. کودکان و نوجوانان بخش قابل توجهی از اطلاعات خود درباره استفاده از تلفن همراه، بازی‌های اینترنتی، خرید آنلاین و شبکه‌های اجتماعی را از طریق مشاهده رفتار والدین به دست می‌آورند. اگر والدین بدون رعایت اصول امنیتی، اطلاعات بانکی یا رمزهای ورود خود را در اختیار دیگران قرار دهند، احتمال تکرار این رفتار در فرزندان افزایش می‌یابد. نظارت خانوادگی باید متناسب با سن و میزان استقلال فرد انجام شود. کنترل افراطی و مداخله مستمر ممکن است موجب پنهان‌کاری کودک یا نوجوان شود و ارتباط او با والدین را کاهش دهد. در مقابل، بی‌توجهی کامل نیز فرصت مناسبی برای سوءاستفاده افراد ناشناس، تبلیغات فریبنده و ارتباطات ناسالم ایجاد می‌کند. نظارت مؤثر باید بر گفت‌و ارتباطات ناسالم ایجاد می‌کند. نظارت مؤثر باید بر گفت‌و باشد (مشاک، ۱۳۹۴، ص ۸).

در خانواده‌هایی که والدین با فناوری آشنایی کافی ندارند، احتمال بروز شکاف اطلاعاتی میان نسل‌ها افزایش می‌یابد. در چنین شرایطی، فرزندان ممکن است با تهدیدهای دیجیتال آشنا باشند، اما والدین نتوانند نشانه‌های فریب یا رفتارهای پرخطر را شناسایی کنند. گاهی نیز سالمندان خانواده به دلیل اعتماد به فرزندان یا نوه‌ها، اطلاعات حساب‌های بانکی و رمزهای خود را بدون رعایت اصول امنیتی در اختیار دیگران قرار می‌دهند. مسئولیت خانواده در این حوزه به معنای دسترسی بدون محدودیت به حریم خصوصی اعضا نیست. اطلاعات شخصی، مکالمات خصوصی و حساب‌های کاربری افراد باید با رعایت شأن و حقوق آنان محافظت شود (معمار و همکاران، ۱۳۹۱، ص ۱۵۹).

به نظر نگارنده، بهترین شیوه نظارت خانوادگی، ایجاد محیطی امن برای طرح مسئله است؛ به گونه‌ای که فرد پس از دریافت پیام مشکوک یا ارتکاب اشتباه، به جای پنهان‌کاری بتواند موضوع را با خانواده در میان بگذارد و از زیان بیشتر جلوگیری شود.

۴-۲- تأثیر گروه همسالان و شبکه‌های ارتباطی

گروه همسالان در شکل‌دهی به رفتارهای دیجیتال جوانان و نوجوانان اثر زیادی دارد. افراد معمولاً برنامه‌ها، بازی‌ها، صفحات اینترنتی و روش‌های کسب درآمد آنلاین را از دوستان خود می‌آموزند. اگر اعضای یک گروه، تبلیغات مشکوک را معتبر بدانند یا بدون بررسی در طرح‌های مالی اینترنتی شرکت کنند، احتمال پیروی سایر اعضا نیز افزایش می‌یابد. فشار روانی ناشی از تمایل به پذیرفته شدن در گروه، قدرت تصمیم‌گیری مستقل را کاهش می‌دهد. برخی کلاهبرداری‌ها با استفاده از همین الگو طراحی می‌شوند. در این شیوه، مرتکب از افراد محدود آغاز می‌کند و پس از جلب اعتماد آنان، از قربانیان می‌خواهد دوستان یا اعضای خانواده خود را نیز به طرح معرفی کنند. معرفی از سوی شخص آشنا، اعتبار ظاهری فعالیت را افزایش می‌دهد و موجب می‌شود افراد جدید بدون بررسی دقیق وارد رابطه مالی شوند. این وضعیت در طرح‌های سرمایه‌گذاری جعلی، فروش کالاهای غیرواقعی و تبلیغات استخدامی بیشتر دیده می‌شود (کاظمی و مسعودیان، ۱۴۰۳، ص ۱۲).

شبکه‌های ارتباطی مجازی نیز با سرعت زیادی اطلاعات را منتشر می‌کنند. پیام‌هایی که در گروه‌های خانوادگی، دوستانه یا کاری بازنشر می‌شوند، غالبا به دلیل انتساب به یک فرد آشنا، معتبر تلقی می‌گردند. در حالی که بازنشر پیام به معنای صحت محتوای آن نیست. ممکن است شخصی بدون قصد مجرمانه، یک لینک جعلی، آگهی دروغین یا شماره

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

حساب متعلق به کلاهبردار را منتشر کند و موجب زیان دیگران شود (فصیح رامندی، ۱۴۰۲، ص ۴۹).

لذا از دیدگاه نگارنده، آموزش مهارت توقف و بررسی پیش از بازنشر اهمیت زیادی دارد. کاربران باید بدانند که هیچ پیشنهاد مالی، استخدامی یا تجاری صرفا به دلیل ارسال از سوی دوست یا خویشاوند معتبر نیست. بررسی منبع اصلی، تماس با سازمان مربوط، پرهیز از واریز فوری و گزارش حساب‌های مشکوک، اقداماتی ساده اما مؤثر هستند. مسئولیت اجتماعی کاربران در شبکه‌های ارتباطی، بخشی از پیشگیری عمومی از بزه‌دیدگی محسوب می‌شود.

۴-۳- سطح آگاهی و سواد فضای مجازی

سواد فضای مجازی تنها به توانایی استفاده از تلفن همراه یا نصب برنامه‌ها محدود نمی‌شود. کاربر باسواد باید بتواند هویت فرستنده، اعتبار نشانی اینترنتی، نوع درخواست، شیوه پرداخت و پیامدهای افشای اطلاعات را ارزیابی کند. ناآگاهی نسبت به تفاوت میان نشانی اصلی و نشانی جعلی، بی‌توجهی به مجوزهای برنامه‌ها و ناتوانی در تشخیص پیام‌های اضطراری، از عواملی است که احتمال فریب را افزایش می‌دهد. کلاهبرداران معمولا از اطلاعات عمومی کاربران استفاده می‌کنند و پیام‌هایی را می‌فرستند که با شرایط روزمره آنان هماهنگ است. پیام مربوط به ابلاغ قضایی، یارانه، بسته پستی، ثبت‌نام دانشگاه، دریافت وام یا برنده شدن در مسابقه، نمونه‌هایی از پوشش‌های رایج هستند. شخصی که با سازوکار رسمی این خدمات آشنا نیست، ممکن است برای دریافت یک منفعت یا جلوگیری از یک زیان ادعایی، اطلاعات بانکی یا هویتی خود را افشا کند (رحمانی و خلیلی، ۱۳۹۰، ص ۷).

آگاهی حقوقی نیز بخشی از سواد فضای مجازی است. افراد باید بدانند که دستگاه‌های رسمی معمولا برای انجام امور اداری، رمز پویا، رمز کارت یا اطلاعات محرمانه بانکی را از طریق پیام‌های ناشناس درخواست نمی‌کنند. همچنین پرداخت وجه به حساب شخصی، استفاده از درگاه ناشناخته و نصب برنامه‌ای که از منبع نامعتبر دریافت شده است، خطرهای جدی به دنبال دارد. شناخت مسیرهای گزارش‌دهی نیز می‌تواند از استمرار زیان جلوگیری کند (کاوسی و سنجری، ۱۴۰۲، ص ۱۳).

به نظر نگارنده، آموزش عمومی باید مستمر، کاربردی و متناسب با گروه سنی باشد. ارائه توصیه‌های کلی و پیچیده تاثیر محدودی دارد؛ اما آموزش از طریق نمونه‌های واقعی، شبیه‌سازی پیام‌های جعلی و تمرین تشخیص نشانی‌های مشکوک، توان تصمیم‌گیری کاربران را افزایش می‌دهد. مدارس، دانشگاه‌ها، بانک‌ها، رسانه‌ها و نهادهای مسئول باید این آموزش را به عنوان بخشی از وظیفه اجتماعی خود دنبال کنند.

۵- نقش عوامل فردی و شناختی در آسیب‌پذیری در برابر کلاهبرداری‌های مجازی

آسیب‌پذیری افراد در برابر کلاهبرداری‌های مجازی تا حدی به ویژگی‌های شناختی و رفتاری آنان بستگی دارد. سرعت تصمیم‌گیری، میزان احتیاط، توانایی تحلیل اطلاعات، تجربه کار با فناوری و شیوه واکنش به فشار روانی، در ارزیابی پیام‌های مشکوک موثر است. دو نفر ممکن است با یک پیام مشابه مواجه شوند، اما به دلیل تفاوت در تجربه و قدرت تحلیل، واکنش‌های کاملا متفاوتی نشان دهند. یکی از روش‌های رایج کلاهبرداران، ایجاد احساس فوریت است. اعلام می‌شود که حساب بانکی در حال مسدود شدن است، فرصت دریافت جایزه رو به پایان است یا باید برای جلوگیری از یک پیامد فوری، مبلغی پرداخت شود. فشار زمانی، امکان بررسی مستقل را از فرد می‌گیرد. در این شرایط، مخاطب به جای تحلیل منطقی، برای رهایی از اضطراب یا دستیابی به منفعت ادعایی، دستورهای فرستنده را اجرا می‌کند(Smith, ۲۰۰۹, p ۲۸).

اعتمادپذیری بیش از اندازه نیز می‌تواند احتمال بزه‌دیدگی را افزایش دهد. برخی افراد تصور می‌کنند دیگران به دلیل شباهت فرهنگی، ظاهر رسمی یا استفاده از ادبیات محترمانه، قابل اعتماد هستند. در فضای مجازی، این برداشت ممکن است گمراه‌کننده باشد؛ زیرا تصویر، نام، نشان سازمانی و حتی صدای افراد قابل جعل است. عامل دیگر نیز تمایل به سود سریع یا جبران زیان‌های مالی است. وعده درآمد بالا با سرمایه اندک، سود تضمینی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

و استخدام بدون مهارت، معمولا با هدف تحریک امید اقتصادی افراد مطرح می‌شود. کسانی که با مشکلات مالی روبه‌رو هستند، ممکن است بیش از دیگران تحت تاثیر چنین وعده‌هایی قرار گیرند (معاضدی عالی و همکاران، ۱۴۰۴، ص ۸۸).

به نظر نگارنده، پیشگیری موثر باید علاوه بر آموزش فنی، مهارت کنترل هیجان، تشخیص طمع‌ورزی و تصمیم‌گیری در شرایط فشار را نیز تقویت کند.

۶- عوامل مؤثر بر گسترش کلاهبرداری‌های مجازی در کودکان و نوجوانان

کودکان و نوجوانان به دلیل تجربه محدود، شناخت ناقص از ارزش پول و اعتماد طبیعی به دیگران، در برابر برخی شیوه‌های فریب مجازی آسیب‌پذیر هستند. آنان ممکن است تفاوت میان تبلیغ، سرگرمی، پیشنهاد تجاری و درخواست مجرمانه را به درستی تشخیص ندهند. بازی‌های آنلاین، شبکه‌های اجتماعی، مسابقات اینترنتی و برنامه‌های پخش زنده، از محیط‌هایی هستند که امکان ارتباط مستقیم افراد ناشناس با آنان را فراهم می‌کنند. دسترسی کودکان به ابزارهای پرداخت والدین نیز خطر قابل توجهی ایجاد می‌کند. ذخیره اطلاعات کارت بانکی در بازی‌ها، استفاده بدون اجازه از رمزهای خرید و کلیک بر پیوندهای ناشناس، ممکن است موجب برداشت وجه یا خریدهای ناخواسته شود. برخی افراد سودجو نیز با وعده دریافت امتیاز، ابزار بازی یا دنبال‌کننده بیشتر، کودکان و نوجوانان را به افشای اطلاعات یا نصب برنامه‌های آلوده ترغیب می‌کنند (حاج علی اکبری و همکاران، ۱۴۰۴، ص ۵۸).

نوجوانان معمولا به دلیل تمایل به استقلال و پذیرفته شدن در گروه دوستان، ممکن است هشدارهای والدین را نادیده بگیرند. پیشنهاد همکاری در فروش اینترنتی، کسب درآمد از تبلیغات، سرمایه‌گذاری در دارایی‌های دیجیتال یا فعالیت در صفحات پرمخاطب، گ سوءاستفاده از هیاده از هیجان و کم‌تجربگی آنان مطرح می‌شود. حتی اگر نوجوان مستقیما زیان مالی نبیند، ممکن است اطلاعات خانوادگی یا حساب کاربری خود را در اختیار افراد ناشناس قرار دهد (رحمتی و سیفی، ۱۴۰۰، ص ۳۱).

از نظر نگارنده، حمایت از کودکان و نوجوانان نباید صرفا با ممنوعیت و قطع دسترسی انجام شود. آموزش تدریجی، تنظیمات امنیتی مناسب، نظارت بر پرداخت‌ها و ایجاد امکان گفت‌وگوی بدون تنبیه، نتیجه بهتری دارد. والدین باید به فرزند خود بیاموزند که دریافت پیام مشکوک یا ارتکاب اشتباه، موضوعی قابل پنهان کردن نیست و باید در کوتاه‌ترین زمان با یک بزرگسال مورد اعتماد در میان گذاشته شود.

۷- عوامل مؤثر بر گسترش کلاهبرداری‌های مجازی در جوانان و بزرگسالان

جوانان و بزرگسالان بیشترین میزان استفاده از خدمات بانکی، خرید اینترنتی، کاریابی آنلاین و شبکه‌های ارتباطی را دارند. گستردگی فعالیت‌های آنان موجب می‌شود با فرصت‌های بیشتری برای تعامل مالی مواجه شوند. همین وابستگی به فضای مجازی، در صورت ضعف احتیاط، دامنه زیان احتمالی را نیز افزایش می‌دهد. کلاهبرداری‌های مرتبط با فروش کالا، اجاره مسکن، استخدام، سرمایه‌گذاری و خدمات تخصصی، معمولا این گروه را هدف قرار می‌دهند. جوانان به دلیل تمایل به کسب استقلال مالی ممکن است جذب پیشنهادهای شغلی غیرواقعی شوند. وعده استخدام فوری، درآمد ارزی، فعالیت از منزل یا دریافت حقوق بالا بدون سابقه کاری، از شیوه‌هایی است که برای جلب آنان به کار می‌رود. در برخی موارد، ابتدا مبلغ اندکی به عنوان هزینه ثبت‌نام، آموزش یا تشکیل پرونده مطالبه می‌شود و پس از پرداخت، ارتباط با مخاطب قطع می‌گردد. بزرگسالان نیز به دلیل اشتغال، مسئولیت خانوادگی و انجام مکرر امور مالی، ممکن است در معرض حملات مبتنی بر عجله قرار گیرند. فشار ناشی از کمبود وقت و اعتماد به عنوان سازمانی، قدرت بررسی را کاهش می‌دهد (فصیح رامندی، ۱۴۰۲، ص ۶۱).

به نظر نگارنده، پیشگیری در این گروه باید با اصلاح رویه‌های مالی همراه باشد. استفاده از حساب‌های جداگانه برای خرید اینترنتی، فعال‌سازی اعلان تراکنش‌ها، تعیین سقف انتقال، خودداری از ذخیره اطلاعات کارت در سایت‌های ناشناس و بررسی قراردادهای الکترونیکی، اقدامات موثری هستند. همچنین شرکت‌ها و مؤسسات باید هویت خود را شفاف اعلام

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

کنند و از دریافت وجه از طریق حساب‌های شخصی یا روش‌های غیرقابل ردیابی پرهیز نمایند.

۸- عوامل مؤثر بر گسترش کلاهبرداری‌های مجازی در سالمندان

سالمندان به دلیل فاصله بیشتر با فناوری‌های جدید، ممکن است در تشخیص پیام‌ها و تماس‌های جعلی با دشواری مواجه شوند. این وضعیت به معنای ناتوانی عمومی آنان نیست، بلکه نتیجه سرعت بالای تغییر ابزارها و پیچیدگی روش‌های جدید ارتباطی است. استفاده از اصطلاحات فنی، نشانه‌های رسمی و ادبیات اداری می‌تواند اعتماد سالمندان را جلب کند و آنان را به انجام اقداماتی سوق دهد که در شرایط عادی انجام نمی‌دهند. اعتماد به افراد دارای عنوان یا جایگاه رسمی، یکی از عوامل مهم در بزه‌دیدگی سالمندان است. کلاهبردار ممکن است خود را کارمند بانک، مامور قضایی، پزشک، مامور پست یا یکی از بستگان معرفی کند. تماس تلفنی یا پیام صوتی، به‌ویژه هنگامی که با اطلاعاتی درباره اعضای خانواده همراه باشد، می‌تواند وضعیت عاطفی سالمند را تحت تاثیر قرار دهد. نگرانی درباره سلامت یا گرفتاری یکی از نزدیکان، فرصت تصمیم‌گیری منطقی را محدود می‌کند. تنهایی اجتماعی و کاهش ارتباط روزمره نیز آسیب‌پذیری را افزایش می‌دهد. فردی که ارتباط محدودی با خانواده یا دوستان دارد، ممکن است پیام یا تماس مشکوک را بدون مشورت بپذیرد. برخی کلاهبرداران با ایجاد ارتباط مستمر، اعتماد سالمند را در طول زمان به دست می‌آورند و سپس درخواست مالی مطرح می‌کنند. این شیوه در روابط عاطفی جعلی و پیشنهادهای سرمایه‌گذاری ساختگی نیز مشاهده می‌شود (امانی کلاریجانی، ۱۳۹۶، ص ۱۰۲).

لذا حمایت از سالمندان باید همراه با حفظ استقلال و کرامت آنان باشد. اختصاص یک شماره تماس خانوادگی برای مشورت، فعال‌سازی اعلان‌های بانکی، تعیین سقف انتقال وجه و آموزش نشانه‌های تماس جعلی، بدون دخالت غیرضروری در زندگی خصوصی می‌تواند موثر باشد.

۹- مقایسه عوامل محیطی و اجتماعی مؤثر بر کلاهبرداری‌های مجازی در گروه‌های سنی مختلف

عوامل موثر بر کلاهبرداری مجازی در گروه‌های سنی یکسان نیست، هرچند برخی عناصر مانند ضعف نظارت، اعتماد نابجا و کمبود آموزش در همه گروه‌ها دیده می‌شود. کودکان بیشتر در معرض سوءاستفاده از بازی‌ها و برنامه‌های سرگرمی قرار دارند، نوجوانان با فریب‌های ناشی از فشار گروهی و پیشنهادهای جذاب اینترنتی روبه‌رو هستند، جوانان و بزرگسالان با کلاهبرداری‌های مالی و شغلی مواجه می‌شوند و سالمندان بیشتر در معرض تماس‌های جعلی و سوءاستفاده از اعتماد قرار می‌گیرند (باطبی، ۱۴۰۵، ص ۹).

در کودکان، عامل اصلی آسیب‌پذیری، ناتوانی در ارزیابی پیامدهای مالی و حقوقی رفتار است. نوجوانان از نظر فنی ممکن است مهارت بیشتری داشته باشند، اما هیجان‌طلبی، تمایل به استقلال و تاثیرپذیری از همسالان، خطرهای خاصی ایجاد می‌کند. جوانان و بزرگسالان به دلیل حضور گسترده در معاملات و فعالیت‌های اقتصادی، هدف ارزشمندتری برای مرتکبان هستند. سالمندان نیز ممکن است به دلیل کاهش توان تطبیق با فناوری یا اعتماد به عناوین رسمی، در برابر شیوه‌های فریب مستقیم آسیب‌پذیرتر باشند (باباحسن-زاده و حیدرنژاد، ۱۴۰۴، ص ۱۰). تفاوت دیگر به نوع محیط ارتباطی مربوط می‌شود. کودکان بیشتر در محیط بازی و شبکه‌های تصویری حضور دارند، نوجوانان در گروه‌های دوستانه و صفحات اجتماعی فعال‌اند، بزرگسالان از پیام‌رسان‌ها، سامانه‌های بانکی و سایت‌های خرید استفاده می‌کنند و سالمندان ممکن است بیشتر از تماس تلفنی، پیامک و ارتباطات خانوادگی بهره ببرند. بنابراین، آموزش و پیشگیری باید متناسب با محیطی طراحی شود که هر گروه در آن حضور بیشتری دارد (کاظمی و مسعودیان، ۱۴۰۳، ص ۱۵).

به نظر نگارنده، سیاست پیشگیری واحد و یکسان، کارایی لازم را ندارد. برای کودکان باید بر آموزش والدین و کنترل پرداخت‌ها تاکید شود؛ برای نوجوانان، تقویت مهارت تحلیل پیام و مقاومت در برابر فشار همسالان اهمیت دارد؛ برای جوانان و بزرگسالان، آموزش امنیت مالی و راستی‌آزمایی خدمات ضروری است؛ و برای سالمندان، حمایت خانوادگی، خدمات بانکی ایمن و ارتباط روشن با نهادهای رسمی باید در اولویت قرار گیرد. در نهایت، پیشگیری موفق زمانی تحقق می‌یابد که مسئولیت میان

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir
Print ISSN: 2717-1469 | Online ISSN: 2717-1477
ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

فرد، خانواده، ارائه‌دهندگان خدمات و نهادهای عمومی تقسیم شود.

۱۰- راهکارهای اجتماعی و محیطی پیشگیری از گسترش کلاهبرداری‌های مجازی

پیشگیری از گسترش کلاهبرداری در بستر ارتباطات، نیازمند بازطراحی سازوکارهای محیطی و بازتعریف مسئولیت‌های نهادهای اجتماعی است. تدابیر صرفاً سرکوبگرانه به دلیل ماهیت فراملی و سرعت دگرگونی شگردهای فریب، به تنهایی بازدارندگی پایدار ایجاد نمی‌کنند؛ از این رو، تمرکز بر پیشگیری وضعی از طریق دشوار ساختن دسترسی به اهداف آسیب‌پذیر در دستور کار قرار می‌گیرد. ساماندهی درگاه‌های پرداخت، الزام به کاربست سامانه‌های اعتبارسنجی چندمرحله‌ای و نظارت هوشمند بر الگوهای غیرمتعارف تراکنش‌ها، موانع فنی بازدارنده‌ای در برابر بزهکاران پدید می‌آورد که احتمال دستیابی به منفعت مالی را به حداقل ممکن کاهش می‌دهد(Ferris, ۲۰۲۲, p ۱۴).

همچنین، ترویج آموزش‌های هدفمند و ارتقای سواد دیجیتال در کلیه ارکان جامعه‌پذیری نقش بنیادین دارد. ورود مفاهیم ایمنی در فضای مجازی به متون آموزشی مدارس و دانشگاه‌ها، حس نقادی شهروندان را در مواجهه با پیشنهادهای مالی فریبنده تقویت می‌کند. از سوی دیگر، رسانه‌های جمعی با پخش منظم هشدارهای مصور و پرهیز از اطلاع‌رسانی مبهم، آگاهی آحاد جامعه را نسبت به شگردهای نوین صیانت از دارایی‌ها افزایش می‌دهند. تقویت سرمایه اجتماعی و احیای پیوندهای همیاری محلی و خانوادگی نیز مانع از انزوای قربانیان بالقوه و افتادن آنان در دام کلاهبرداران می‌گردد (افشانی و همکاران، ۱۳۹۶، ص ۲۳۴).

مسئولیت‌پذیری سکوهای ارائه‌دهنده خدمات عمومی و شرکت‌های واسط مالی، جزء دیگری از این چرخه حمایتی به شمار می‌رود. پلتفرم‌های واسطه‌گری خرید و فروش کالا ملزم هستند نظام‌های نظارتی خود را به ابزارهای کشف خودکار عبارات گمراه‌کننده، احراز هویت متقاطع کاربران و تضمین مبالغ امانی مجهز سازند. در صورت انفعال این سامانه‌ها در مسدودسازی حساب‌های مشکوک، بستر تبادل مالی به منطقه‌ای ناامن برای شهروندان مبدل خواهد شد. ایجاد پنجره‌های واحد گزارش‌دهی مردمی و پیگیری بدون فوت وقت نشانه‌های مجرمانه، احساس امنیت کاذب تبهکاران را زایل می‌سازد (ملکوتی، ۱۳۹۵، ص ۸۲).

به باور نگارنده، دستیابی به یک الگوی پیشگیرانه کارآمد منوط به تحقق هماهنگی نهادی میان متولیان حوزه ارتباطات، نظام بانکی و نهادهای مدنی است. بار پیشگیری نباید به شکل نامتوازن صرفاً بر دوش کاربران نهاده شود، بلکه تأمین‌کنندگان خدمات دیجیتال موظف هستند تدابیر صیانتی را در ذات طراحی سامانه‌های خود بگنجانند. برقراری تعادل میان سهولت بهره‌برداری شهروندان از خدمات آنلاین و حفظ ضوابط ایمنی، اصلی راهبردی است که در صورت نادیده انگاشتن آن، هزینه‌های اقتصادی ناشی از زیان‌های وارده بر دوش بخش عمومی سنگینی خواهد کرد.

نتیجه‌گیری و پیشنهادات

بررسی‌های به عمل آمده در این پژوهش نشان می‌دهد که کلاهبرداری مجازی پدیده‌ای چندوجهی بوده و برآیند تعامل ساختارهای محیطی نوین با آسیب‌پذیری‌های اجتماعی شهروندان است. یافته‌های تحقیق دلالت بر آن دارد که ویژگی‌های ذاتی فضای سایبر، از جمله گمنامی نسبی، فراملی بودن ارتباطات و سرعت سرسام‌آور نقل‌وانتقالات اعتباری، محیطی بسیار مساعد برای بزهکاران فراهم ساخته و بازدارندگی واکنش‌های سنتی را با چالش جدی روبرو نموده است. این بستر محیطی به همراه عواملی چون ضعف زیرساخت‌های احراز هویت متمرکز، خلأهای پایش در شبکه‌های پیام‌رسان و استمرار چالش‌های معیشتی که موجب وسوسه‌انگیزی وعده‌های سودآوری نامتعارف می‌گردد، نرخ شیوع این جرایم را به شکلی تصاعدی افزایش داده است.

یافته دیگر این مطالعه ناظر بر تمایز بنیادین الگوهای بزه‌دیدگی در میان گروه‌های سنی مختلف است. کودکان و نوجوانان به سبب تجربه زیسته اندک و هیجان‌طلبی در بسترهای سرگرمی و بازی‌های برخط، بیش از همه از طریق مهندسی اجتماعی ساده و ترغیب به در اختیار نهادن ابزارهای پرداخت اطرافیان صدمه می‌بینند. در مقابل، جوانان و بزرگسالان به عنوان فعال‌ترین کنشگران چرخه اقتصادی جامعه، در تله‌های پیچیده‌تری از قبیل فرصت‌های شغلی واهی، سرمایه‌گذاری‌های جعلی و

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

معاملات پلتفرمی نامعتبر گرفتار می‌شوند که انگیزه اصلی آن جبران فشارهای اقتصادی یا ارتقای شتابان وضعیت مالی است. سالمندان نیز به دلیل مواجهه با شکاف دیجیتال و تأخر در انطباق با ظرافت‌های سامانه‌های نوین، بیش از سایر اقشار در برابر تماس‌ها و پیام‌های جعلی مبتنی بر جعل عناوین رسمی و فوریت‌های ساختگی آسیب‌پذیر جلوه می‌کنند. از این رو، یکپارچه‌انگاری جامعه هدف در تدوین سیاست‌های مقابله‌ای، خطایی راهبردی بوده و رویکردها باید با تفکیک نیازها و آسیب‌پذیری‌های هر طیف سنی تدوین گردد.

همچنین دستاوردهای پژوهش مؤید آن است که اتکای انحصاری بر پیشگیری انفعالی و اقدامات تعقیبی پس از وقوع جرم، به علت امحای ردپای داده‌ها و امکان تبدیل سریع وجوه به دارایی‌های کم‌اثر در ردیابی، از کارآمدی کافی برخوردار نیست. در مقابل، پیشگیری وضعی متمرکز بر کاهش فرصت‌های مجرمانه و پیشگیری اجتماعی معطوف به ارتقای مهارت‌های رفتاری و تاب‌آوری جمعی، اثربخشی ماندگارتری از خود نشان می‌دهند. خانواده به عنوان کانون اولیه شکل‌گیری هنجارهای رفتاری و سواد رسانه‌ای، نقشی بی‌بدیل در مصون‌سازی نسل جوان و حمایت از سالمندان ایفا می‌کند و گسست پیوندهای نظارتی در درون آن، مستقیماً به تسریع روند بزهکاری یا قربانی‌شدن منجر می‌شود.

بر پایه این یافته‌ها، پیشنهاد می‌گردد سازوکار ملی کشف هوشمند تقلب در شبکه بانکی طراحی و پیاده‌سازی شود، به گونه‌ای که با تعریف سامانه‌ای یکپارچه مبتنی بر یادگیری ماشین، تراکنش‌های مالی افراد بر مبنای نمایه رفتاری و رده سنی آنان پایش گردد؛ برای نمونه، انتقال وجوه بیش از حد معین در حساب‌های متعلق به گروه‌های سنی سالمند یا کم‌سن، به صورت خودکار با تأخیر امنیتی مشروط یا نیازمند تأیید سرپرست یا امین خانوادگی انجام پذیرد. علاوه بر این، راه‌اندازی کارزار ملی شبیه‌سازی حملات فریب مجازی در بستر پیام‌رسان‌ها به منظور آزمون و آموزش عملی شهروندان، و نیز ملزم ساختن قانونی توسعه‌دهندگان سکوهای آنلاین به تعبیه نشانگرهای هوشمند سنجش اعتبار کاربران و معاملات امانی بدون واسطه، می‌تواند گامی نوین و بازدارنده در مهار کلاهبرداری‌های سایبری قلمداد شود.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

منابع

- منابع فارسی

الف- کتاب-ها

۱- امیدوار، احمدعلی؛ صارمی، علی اکبر(۱۳۸۱)، اعتیاد به اینترنت: توصیف، سبب شناسی، پیشگیری، درمان و مقیاس-های سنجش اختلال اعتیاد به اینترنت، مرکز مشاوره و خدمات روانشناختی پردیس، مشهد: انتشارات تمرین

۲- باستانی، برومند (۱۳۸۳)، جرائم کامپیوتری و اینترنتی، تهران: انتشارات بهنامی

۳- خداقلی، زهرا (۱۳۸۴)، جرایم کامپیوتری، چاپ اول، تهران: انتشارات آریان

۴- معتمد نژاد، کاظم (۱۳۹۰)، حقوق ارتباطات بین المللی، جلد دوم، تهران: دفتر مطالعات و توسعه رسانه‌ها

۵- ملکوتی، رسول (۱۳۹۵)، مسئولیت مدنی در فضای سایبر، تهران: انتشارات مجد

ب- مقاله-ها

۱- افشانی، سید علیرضا؛ پارسامهر، مهربان؛ کریمیان، کبری (۱۳۹۶)، عوامل موثر بر گرایش به شبکه‌های اجتماعی مجازی: مورد مطالعه دانش آموزان دختر دبیرستان‌های شهرکرد، فصلنامه علوم اجتماعی، سال ۲۷، شماره ۸۰، صص ۲۰۹-۲۳۷.

۲- امانی کلاریجانی، امرالله (۱۳۹۶)، فضای مجازی و واکاوی سیاست‌های پیشگیرانه در کنترل آسیب‌های اجتماعی نوپدید، نشریه علمی تخصصی رهیافت پیشگیری، پیش شماره اول، صص ۸۹-۱۰۵.

۳- بابا حسن‌زاده، نیلوفر؛ حیدر نژاد، کیوان (۱۴۰۴)، تاثیر فضای سایبری بر بزهکاری اطفال و نوجوانان (مطالعه موردی در سطح شهرستان ارومیه)، فصلنامه علمی فقه و حقوق نوین، سال ششم، شماره ۲۲، صص ۱-۲۱.

۴- باطبی، محمد مهدی (۱۴۰۵)، عوامل موثر بر پیشگیری از بزهکاری اطفال و نوجوانان در فضای مجازی، هفدهمین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق، صص ۱-۱۵.

۵- جعفری، محمد صادق؛ عبادی نفط چالی، احسان (۱۴۰۵)، چالش‌های احراز مسئولیت کیفری و تعیین ضمانت جاهای متناسب در بزهکاری مبتنی بر هوش مصنوعی؛ مطالعه موردی: تولید و انتشار دیپ فیک (جعل عمیق) پورنوگرافیک یا افترا آمیز توسط نوجوانان، دهمین همایش بین‌المللی فقه و حقوق، وکالت و علوم اجتماعی، صص ۱-۷.

۶- حاج علی اکبری، فیروزه؛ احمدی، حسین؛ ذوالقدر، علی (۱۴۰۴)، عوامل وابستگی دانش آموزان به فضای مجازی؛ نقش زمینه‌ای عوامل شناختی و فردی و میانجی‌های رفتاری-اجتماعی، نشریه مطالعات دانش پژوهی، دوره ۴، شماره ۱، صص ۴۶-۶۲.

۷- رحمانی، علی؛ خلیلی، زهرا (۱۳۹۰)، بررسی تاثیر استفاده از فناوری-های نوین ارتباطی (اینترنت، چت، بازی-های رایانه-ای) بر هویت فرهنگی نوجوانان گرگان، مجموعه مقالات برگزیده همایش منطقه-ای آسیب-های اجتماعی نوپدید، دفتر تحقیقات کاربردی و معاونت اجتماعی نیروی انتظامی استان مازندران، صص ۱-۱۴.

۸- رحمتی، صمد؛ سیفی، رضوان (۱۴۰۰)، شیوع شناسی و بررسی عوامل خطرساز و حفاظت کننده مزاحمت سایبری با رویکرد تحولی: یک مطالعه مروری روایتی، فصلنامه رویش روانشناسی، سال ۱۰، شماره ۱۱، صص ۲۵-۳۸.

۹- فصیح رامندی، منصوره (۱۴۰۲)، تبیین عوامل مرتبط با تمایل به بزهکاری در شبکه‌های اجتماعی بین نوجوانان دانش آموز (مطالعه موردی دانش آموزان مناطق پنج‌گانه تهران)، پژوهشنامه فرهنگی و اجتماعی کودک و نوجوان، سال اول، شماره ۳، صص ۴۵-۶۳.

۱۰- کاظمی، ابراهیم؛ مسعودیان، پریسا (۱۴۰۳)، رابطه بین خشونت‌های سایبری با ناسازگاری دانش آموزان شهر بهبهان، سومین همایش ملی امور تربیتی، صص ۱-۱۸.

۱۱- کاوسی، افشین؛ سنجری، مهدی (۱۴۰۲)، بررسی آسیب‌های فضای مجازی بر دانش آموزان و خانواده، هشتمین کنفرانس ملی رویکردهای نوین در آموزش و پرورش، صص ۱-۲۱.

۱۲- مشاک، مریم (۱۳۹۴)، بررسی نقش آسیب‌های فضای مجازی برای دانش آموزان و ارائه راهکارهای جهت جلوگیری از این قبیل آسیب‌ها، کنفرانس جهانی افق‌های نوین در علوم انسانی، آینده پژوهی و توانمندسازی، صص ۱-۱۲.

۱۳- معاضدی عالی، کاظم؛ رزاقی، نادر؛ عباسی کلان، هادی؛ محجوبی دریاکناری، محبوبه (۱۴۰۴)، آزار مجازی دانش آموزان در استفاده از شبکه‌های اجتماعی مجازی (مطالعه موردی دانش آموزان منطقه ۱ رشت)، فصلنامه پژوهشی روانشناسی مدرسه و آموزشگاه، دوره ۱۴، شماره ۲، صص ۸۵-۹۵.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Print ISSN: 2717-1469 | Online ISSN: 2717-1477

ISC | SID | NOORMAGS | MAGIRAN | Google Scholar

۱۴- معمار، ثریا؛ عدلی‌پور، صمد؛ خاکسار، فائزه (۱۳۹۱)، شبکه‌های اجتماعی مجازی و بحران هویت (با تاکید بر بحران هویتی ایران)، فصلنامه علمی پژوهشی مطالعات و تحقیقات اجتماعی در ایران، دوره اول، شماره ۴، صص ۱۵۵-۱۷۶.

- منابع انگلیسی

۱- Chi- Hung (۲۰۰۵), Gender Difference and Related Factors Affecting online Gaming Addiction Amoung Taiwanese Adolescent, The Journal of Nervous and Mental Disease, ۱۹۳(۴): ۲۷۳-۲۷۷

۲- Ferriis, Jennifer (۲۰۰۲), Internet Addiction Disorder: Causes, Symptoms and Consecuenses, Psychology Virginia Tech, Jferris@ vt.edu

۳- Smith, M (۲۰۰۹), Communities in Cyberspace, London, Routledge