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	۲۶	صفحات	۱۵-۱

تحلیل جرم‌شناختی چرخه بروز و تکرار کلاهبرداری‌های سایبری در بسترهای شبکه اجتماعی

آقای فرهود مدبر خاک‌نژاد

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

چکیده

کلاهبرداری سایبری در بستر شبکه‌های اجتماعی، از مهم‌ترین اشکال جرایم علیه اموال و مالکیت در محیط دیجیتال است که با بهره‌گیری از داده‌های شخصی، ارتباطات برخط، حساب‌های کاربری جعلی و شیوه‌های فریب مبتنی بر اعتماد ارتکاب می‌یابد در این جرم، برخلاف کلاهبرداری سنتی، غالبا در فضای فرامرزی، با هویت نامعلوم و از طریق ابزارهایی انجام می‌شود که امکان تکرار سریع و گسترده رفتار مجرمانه را فراهم می‌کنند. مقاله حاضر با روش توصیفی-تحلیلی، چرخه بروز و تکرار کلاهبرداری سایبری در شبکه‌های اجتماعی را از منظر جرم‌شناختی و با توجه به مبانی حقوق کیفری ایران بررسی می‌کند. در این پژوهش، نخست مفهوم کلاهبرداری سایبری، تحول آن و ارتباط آن با عناوین مجرمانه مقرر در قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری و قانون جرایم رایانه‌ای تحلیل می‌شود. سپس مبانی شکل‌گیری این جرم، از جمله فرصت مجرمانه، انتخاب بزه‌دیده، کاهش نظارت اجتماعی، ناشناختگی مرتکب و ضعف آگاهی حقوقی بررسی خواهد شد. یافته‌های پژوهش نشان می‌دهد که کلاهبرداری سایبری در شبکه‌های اجتماعی، نتیجه یک رفتار منفرد نیست؛ بلکه در قالب چرخه‌ای متشکل از شناسایی بزه‌دیده، ایجاد اعتماد، اعمال فریب، تحصیل مال، پنهان‌سازی آثار جرم و بازتولید شیوه مجرمانه شکل می‌گیرد. همچنین، تکرار این جرم با ضعف کنترل هویت، دشواری جمع‌آوری ادله الکترونیکی، انتقال سریع وجوه، استفاده از حساب‌های واسط و تأخیر در اعلام جرم ارتباط مستقیم دارد. نتیجه تحقیق آن است که پاسخ کیفری مؤثر، تنها با تشدید مجازات تحقق نمی‌یابد و باید هم‌زمان پیشگیری وضعی، ارتقای امنیت داده، تقویت ادله الکترونیکی، آموزش حقوقی کاربران و هماهنگی میان نهادهای قضایی، انتظامی و ارائه‌دهندگان خدمات ارتباطی مورد توجه قرار گیرد.

واژگان کلیدی: کلاهبرداری، فضای مجازی، شبکه اجتماعی، بزه‌دیده، فریب، ادله الکترونیکی، تکرار جرم

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

Criminological Analysis of the Emergence and Recurrence Cycle of Cyber Fraud in Social Media Platforms

Abstract

Cyber fraud within social media platforms represents one of the most critical forms of offenses against property and ownership in the digital environment. It is committed by leveraging personal data, online communications, fake user accounts, and trust-based deception techniques. Unlike traditional fraud, this crime frequently operates across borders, under concealed identities, and through tools that facilitate the rapid and extensive replication of criminal behavior. Employing a descriptive-analytical method, this study examines the cycle of emergence and recurrence of cyber fraud on social media platforms from a criminological perspective and in light of Iranian criminal law principles. The research first analyzes the concept and evolution of cyber fraud in relation to statutory offenses under Iranian law. It subsequently examines the criminological foundations of its emergence, including criminal opportunity, victim selection, diminished social control, offender anonymity, and legal awareness deficits. Research findings demonstrate that cyber fraud on social media is not an isolated act, but rather operates within a structured cycle comprising victim identification, trust cultivation, execution of deception, acquisition of property, concealment of traces, and reproduction of the modus operandi. Furthermore, crime recurrence directly correlates with inadequate identity verification, challenges in electronic evidence gathering, rapid fund transfers, the use of intermediary accounts, and delays in reporting offenses. The study concludes that an effective criminal justice response cannot rely solely on aggravating penalties; it requires the simultaneous implementation of situational crime prevention, data security enhancement, strengthening of electronic evidence preservation, public legal awareness, and structured coordination among judicial authorities, law enforcement agencies, and digital service providers.

Keywords: Fraud, Cyberspace, Social Media, Victim, Deception, Electronic Evidence, Recidivism

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

گسترش شبکه‌های اجتماعی، روابط مالی و غیرمالی اشخاص را با تغییر اساسی مواجه کرده است. بخش قابل توجهی از ارتباطات تجاری، تبلیغات، خرید و فروش، ارائه خدمات و انتقال اطلاعات در بسترهایی انجام می‌شود که تعیین هویت واقعی کاربران و ارزیابی اعتبار ادعاهای آنان همواره آسان نیست. این وضعیت، در کنار مزایای ارتباطات الکترونیکی، فرصت‌های جدیدی برای ارتکاب جرایم علیه اموال ایجاد کرده است. کلاهبرداری سایبری در این محیط، از طریق ساخت حساب‌های کاربری جعلی، انتشار آگهی‌های خلاف واقع، جعل عنوان، ارسال پیوندهای آلوده، سوءاستفاده از اعتماد کاربران و دریافت وجوه یا اطلاعات مالی تحقق می‌یابد.

در حقوق ایران، رفتارهای کلاهبردارانه در فضای سایبری ممکن است حسب مورد با عنوان کلاهبرداری موضوع قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری، کلاهبرداری مرتبط با رایانه موضوع قانون جرایم رایانه‌ای، جعل رایانه‌ای، سرقت داده، دسترسی غیرمجاز یا تحصیل مال از طریق نامشروع قابل ارزیابی باشد. تشخیص عنوان مجرمانه، به شیوه ارتکاب، موضوع رفتار، رابطه و ورود میان عملیات متقلبانه و ورود زیان، قصد مرتکب و نوع داده یا مال تحصیل‌شده وابسته است. بنابراین، تحلیل این جرم بدون توجه به مبانی حقوق کیفری و قواعد ناظر بر ادله الکترونیکی، ناقص خواهد بود.

وجه متمایز کلاهبرداری سایبری، قابلیت تکرار و توسعه آن است. مرتکب می‌تواند یک الگوی فریب را بدون حضور فیزیکی و با هزینه اندک، علیه شمار زیادی از اشخاص اجرادیده ممکن است برای شناس‌دست‌آمده از یک بزه‌دیده ممکن است برای شناسایی و فریب بزه‌دیدگان بعدی به کار رود. در نتیجه، جرم از حالت یک رابطه دوطرفه میان مرتکب و بزه‌دیده خارج شده و به فرایندی مستمر تبدیل می‌شود که در آن داده‌های شخصی، حساب‌های بانکی، شماره‌های تماس و محتوای ارتباطی، نقش ابزار ارتکاب یا زمینه‌ساز جرم را ایفا می‌کنند.

مسئله اصلی این پژوهش آن است که چرخه بروز و تکرار کلاهبرداری سایبری در شبکه‌های اجتماعی چگونه شکل می‌گیرد و چه عوامل جرم‌شناختی موجب استمرار آن می‌شود. فرض اصلی آن است که این جرم در نتیجه پیوند میان فرصت مجرمانه، ضعف کنترل اجتماعی، آسیب‌پذیری بزه‌دیده، امکان پنهان‌سازی هویت و دشواری کشف ادله ایجاد می‌شود. پژوهش حاضر با روش توصیفی ـ تحلیلی و از طریق بررسی مفاهیم حقوقی، مبانی جرم‌شناختی و مراحل عملی ارتکاب جرم، تلاش دارد الگوی مذکور را تبیین کند. اهمیت این موضوع در آن است که شناسایی مراحل چرخه جرم می‌تواند در طراحی سیاست جنایی پیشگیرانه و ارتقای کارآمدی پاسخ کیفری مؤثر باشد.

۱- مفهوم‌شناسی و تحول کلاهبرداری سایبری در بستر شبکه‌های اجتماعی

کلاهبرداری در مفهوم حقوق کیفری، رفتاری است که مرتکب با توسل به وسایل متقلبانه، موجب فریب بزه‌دیده شده و مال یا منفعتی را به زیان وی تحصیل می‌کند. در کلاهبرداری سنتی، معمولا میان مرتکب و بزه‌دیده ارتباط مستقیم وجود دارد و عملیات متقلبانه از طریق اسناد، گفتار، معرفی عنوان مجعول یا ایجاد مؤسسات و تشکیلات غیرواقعی انجام می‌شود. عنصر اساسی این جرم، رابطه میان عملیات متقلبانه، فریب بزه‌دیده، تسلیم مال و ورود ضرر است. در فضای سایبری، این عناصر با استفاده از ابزارهای الکترونیکی و ارتباطات برخط تحقق پیدا می‌کنند. کلاهبرداری سایبری را می‌توان هر رفتار عمدی و متقلبانه‌ای دانست که با استفاده از سامانه‌های رایانه‌ای، شبکه‌های ارتباطی یا داده‌های الکترونیکی، به فریب شخص و تحصیل مال، منفعت، خدمات یا امتیاز مالی منتهی شود. این تعریف، علاوه بر کلاهبرداری رایانه‌ای به معنای خاص، برخی رفتارهای مرتبط با جعل هویت، استفاده از داده‌های مجعول و انتشار محتوای خلاف واقع را نیز دربرمی‌گیرد؛ مشروط بر آنکه عناصر قانونی عنوان مجرمانه مربوط وجود داشته باشد. در هر مورد، صرف استفاده از شبکه اجتماعی برای ارتباط، به‌تنهایی موجب تحقق کلاهبرداری سایبری نیست و باید عملیات متقلبانه و نتیجه مالی آن احراز شود (اوجاقلو و همکاران، ۱۴۰۱، ص ۱۷۵).

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

شبکه اجتماعی، محیطی تعاملی است که کاربران در آن امکان ایجاد حساب کاربری، انتشار محتوا، ارسال پیام، تشکیل گروه، تبلیغ کالا و برقراری ارتباط با اشخاص متعدد را دارند. این ویژگی‌ها، ظرفیت مناسبی برای ارتکاب کلاهبرداری فراهم می‌کند؛ زیرا مرتکب می‌تواند با استفاده از تصویر، نام، نشان تجاری یا عنوان حرفه‌ای دیگران، اعتماد بزه‌دیده را جلب کند. همچنین، امکان مشاهده عمومی اطلاعات کاربران، زمینه جمع‌آوری داده‌های شخصی و طراحی عملیات متقلبانه متناسب با وضعیت هر بزه‌دیده را افزایش می‌دهد (بهاری غازانی، ۱۴۰۰، ص ۵).

تحول کلاهبرداری سایبری از الگوهای ساده مانند ارسال پیام‌های فریبنده به شیوه‌های پیچیده‌تر، از جمله مهندسی اجتماعی، جعل حساب‌های سازمانی، سوءاستفاده از اخبار روز، ایجاد صفحات تجاری غیرواقعی و هدایت بزه‌دیده به درگاه‌های جعلی منتهی شده است. در این تحول، فناوری صرفا ابزار ارتکاب نیست؛ بلکه محیطی برای شناسایی بزه‌دیده، تنظیم فریب، انتقال مال، حذف آثار جرم و تکرار رفتار مجرمانه ایجاد می‌کند. به همین دلیل، تحلیل این جرم باید هم‌زمان ناظر بر رفتار انسانی مرتکب و ساختار فنی محیط ارتکاب باشد.

۲- مبانی جرم‌شناختی شکل‌گیری کلاهبرداری سایبری در شبکه‌های اجتماعی

یکی از مبانی اساسی شکل‌گیری کلاهبرداری سایبری، نظریه فرصت مجرمانه است. بر اساس این دیدگاه، وقوع جرم زمانی محتمل‌تر می‌شود که مرتکب دارای انگیزه، بزه‌دیده مناسب و فقدان نظارت مؤثر در یک موقعیت واحد باشند. شبکه‌های اجتماعی، به دلیل دسترسی گسترده، سرعت ارتباط، ضعف احراز هویت و امکان فعالیت ناشناس، فرصت ارتکاب را افزایش می‌دهند. در چنین محیطی، مرتکب بدون تحمل هزینه‌های سنگین می‌تواند تعداد زیادی از کاربران را شناسایی و رفتار متقلبانه خود را تکرار کند (نیک-نژاد، ۱۴۰۰، ص ۳).

عامل دیگر، کاهش کنترل اجتماعی است. در محیط فیزیکی، اعتبار اشخاص، محل فعالیت، اسناد هویتی و حضور شاهدان می‌تواند در ارزیابی صحت ادعاها مؤثر باشد؛ اما در فضای مجازی، این عوامل همواره قابل مشاهده یا قابل اعتماد نیستند. حساب کاربری ممکن است با هویت غیرواقعی ایجاد شود و محتوای منتشرشده نیز بدون بررسی صحت آن در اختیار کاربران قرار گیرد. فقدان نظارت خانوادگی، صنفی، سازمانی و پلتفرمی، احتمال استمرار عملیات متقلبانه را افزایش می‌دهد (یوسفی-نژاد و پیمان، ۱۴۰۳، ص ۸).

آسیب‌پذیری بزه‌دیده نیز از مبانی مهم ارتکاب این جرم است. آسیب‌پذیری لزوما به معنای ضعف شخصی یا فقدان آگاهی نیست؛ بلکه ممکن است ناشی از وضعیت اقتصادی، نیاز فوری، اعتماد به عنوان‌های حرفه‌ای، ناآشنایی با روش‌های پرداخت الکترونیکی یا دسترسی ناقص به اطلاعات حقوقی باشد. مرتکب با شناسایی همین وضعیت، عملیات متقلبانه را به‌گونه‌ای طراحی می‌کند که بزه‌دیده در زمان کوتاه و بدون بررسی کافی، مال یا اطلاعات مالی خود را در اختیار وی قرار دهد. ناشناختگی مرتکب و دشواری انتساب رفتار نیز در تکرار جرم نقش دارد. مرتکب می‌تواند از ابزارهای تغییر نشانی، حساب‌های واسط، شماره‌های متعدد، سیم‌کارت‌های ثبت‌شده به نام اشخاص دیگر و حساب‌های کاربری موقت استفاده کند. این وضعیت، کشف هویت واقعی، توقیف اموال، شناسایی ارتباطات و جمع‌آوری ادله را دشوار می‌سازد. در نتیجه، هرگاه احتمال شناسایی و مجازات کمتر از منفعت مورد انتظار باشد، انگیزه تکرار رفتار مجرمانه افزایش می‌یابد (واضحی شکردشت و جوادنیا ریک، ۱۴۰۳، ص ۱۵).

۳- الگوی بروز و شکل‌گیری چرخه کلاهبرداری سایبری در شبکه‌های اجتماعی

کلاهبرداری سایبری در شبکه‌های اجتماعی معمولا در قالب یک چرخه چندمرحله‌ای تحقق می‌یابد. این چرخه از جمع‌آوری اطلاعات و انتخاب بزه‌دیده آغاز می‌شود و با ایجاد اعتماد، اجرای فریب، تحصیل مال، پنهان‌سازی آثار جرم و بازتولید روش ارتکاب ادامه پیدا می‌کند. ویژگی اصلی این چرخه، تکرارپذیری و قابلیت انتقال آن به بزه‌دیدگان متعدد است. مرتکب پس از موفقیت در یک عملیات، شیوه ارتباط، متن پیام، عنوان مجعول، حساب دریافت وجه یا ابزار فنی مورد استفاده را حفظ یا

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

اصلاح می‌کند. در برخی موارد نیز اطلاعات بزه‌دیده نخست، برای فریب اشخاص نزدیک به وی مورد استفاده قرار می‌گیرد. بنابراین، جرم نه‌تنها از حیث تعداد بزه‌دیدگان، بلکه از نظر استمرار روش مجرمانه نیز قابلیت توسعه دارد. هر مرحله ممکن است واجد آثار متفاوتی باشد. جمع‌آوری اطلاعات ممکن است در صورت دسترسی غیرمجاز یا تحصیل داده بدون مجوز، عنوان مجرمانه مستقل داشته باشد. استفاده از عنوان و اسناد جعلی می‌تواند با جعل یا استفاده از سند مجعول ارتباط پیدا کند و انتقال وجوه از طریق حساب‌های واسط ممکن است در ارزیابی معاونت، مشارکت یا معاملات مالی مرتبط با جرم مؤثر باشد. تعیین مسئولیت کیفری، نیازمند احراز نقش هر شخص، علم وی به ماهیت رفتار و رابطه او با عملیات اصلی است. شناخت این چرخه برای سیاست جنایی اهمیت ویژه دارد. اگر مداخله کیفری تنها پس از انتقال مال صورت گیرد، بخش مهمی از ظرفیت پیشگیری از جرم از دست می‌رود. اقدامات پیشگیرانه باید در مراحل اولیه، مانند احراز هویت حساب‌ها، شناسایی تبلیغات خلاف واقع، مسدودسازی سریع حساب‌های مشکوک، هشدار به کاربران و حفظ داده‌های الکترونیکی آغاز شود (اله-یاری و مجیدی پرست، ۱۳۹۳، ص ۱۵۷).

در ادامه، مراحل اصلی چرخه کلاهبرداری سایبری بررسی می‌شود.

۱-۳- مرحله شناسایی و انتخاب بزه‌دیده

در مرحله نخست، مرتکب با بررسی اطلاعات عمومی یا قابل دسترس کاربران، اشخاصی را انتخاب می‌کند که احتمال فریب آنان بیشتر است. اطلاعات مربوط به وضعیت شغلی، روابط خانوادگی، نیاز مالی، علاقه‌مندی‌ها، خریدهای پیشین و موقعیت اجتماعی، ممکن است از طریق محتوای منتشرشده در شبکه اجتماعی به دست آید. این اطلاعات در صورتی که بدون مجوز و با هدف ارتکاب جرم جمع‌آوری یا پردازش شود، می‌تواند در ارزیابی مسئولیت کیفری مرتکب و نقض حریم خصوصی مؤثر باشد. انتخاب بزه‌دیده معمولا تصادفی نیست. مرتکب ممکن است اشخاصی را هدف قرار دهد که نیاز فوری به دریافت وام، خرید کالایگذاری یا دریافت استخدام، سرمایه‌گذاری یا دریافت خدمات دارند. در موارد دیگر، اشخاص دارای ارتباط با یک شرکت، مقام اداری یا شخصیت شناخته‌شده انتخاب می‌شوند تا جعل عنوان و انتساب سمت، احتمال فریب را افزایش دهد. این فرایند نشان می‌دهد که بزه‌دیده در بسیاری از موارد، پیش از آغاز ارتباط، از طریق تحلیل داده‌ها انتخاب شده است (فتحی، ۱۴۰۱، ص ۱۲۸).

انتخاب شخص بر مبنای وضعیت او، به معنای انتساب تقصیر به بزه‌دیده نیست. مسئولیت کیفری اصلی بر عهده مرتکبی است که با قصد فریب و تحصیل مال، عملیات متقلبانه را طراحی کرده است. با وجود این، بررسی وضعیت بزه‌دیده برای شناخت شیوه ارتکاب، تعیین تدابیر پیشگیرانه و تحلیل رابطه سببیت اهمیت دارد. در حقوق کیفری، اعتماد بزه‌دیده یا بی‌احتیاطی وی، در صورت احراز عملیات متقلبانه مرتکب، به‌تنهایی موجب زوال وصف مجرمانه رفتار نخواهد شد. در این مرحله، اقدامات پیشگیرانه شامل محدود کردن انتشار داده‌های حساس، تقویت سازوکار گزارش حساب‌های جعلی، احراز هویت تجاری، نظارت بر تبلیغات مالی و آموزش کاربران درباره نشانه‌های فریب است. همچنین، ارائه‌دهندگان خدمات شبکه اجتماعی باید امکان ثبت و حفظ سوابق فنی، گزارش‌دهی سریع و شناسایی رفتارهای هماهنگ و غیرعادی را فراهم کنند. این اقدامات، به‌ویژه پیش از ورود جرم به مرحله تحصیل مال، می‌تواند چرخه کلاهبرداری را متوقف سازد (تجری و صادقیان لمسراکی، ۱۴۰۳، ص ۵).

۲-۳- مرحله ایجاد اعتماد و فریب

پس از انتخاب بزه‌دیده، مرتکب تلاش می‌کند رابطه‌ای مبتنی بر اعتماد ظاهری ایجاد کند. این اعتماد ممکن است از طریق معرفی خود به‌عنوان نماینده شرکت، مأمور نهاد عمومی، فروشنده معتبر، کارشناس، صاحب حساب تجاری یا شخصی آشنا با بزه‌دیده شکل گیرد. استفاده از تصویر، نشان تجاری، عنوان شغلی و محتوای حرفه‌ای، از ابزارهایی است که برای ایجاد تصور اعتبار به کار می‌رود. در این مرحله، هدف اصلی آن است که بزه‌دیده ادعاهای مرتکب را بدون بررسی مستقل بپذ که بزه‌دیده ادعاهای

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

مرتکب را بدون بررسی مستقل بپذ نادرست به‌صورت هم‌زمان انجام می‌شود. مرتکب ممکن است بخشی از اطلاعات واقعی بزه‌دیده یا موضوع معامله را در پیام خود به کار گیرد تا ادعای وی معتبر به نظر برسد. همچنین، ارائه اسناد تصویری، رسیدهای ساختگی، قراردادهای غیرواقعی یا پیام‌های منتسب به نهادهای رسمی می‌تواند موجب تقویت فریب شود. از نظر حقوقی، ملاک، صرف دروغ‌گویی نیست؛ بلکه باید رفتار مرتکب در قالب عملیات متقلبانه و بلکه باید رفتار مرتکب در قالب عملیات متقلبانه و مؤثرهای رایج این مرحله است. مرتکب با اعلام مهلت کوتاه، تهدید به از بین رفتن فرصت، وعده سود فوری یا ادعای ضرورت پرداخت، امکان بررسی و تصمیم‌گیری آگاهانه را از بزه‌دیده سلب می‌کند. چنین رفتاری در کنار سایر اقدامات، می‌تواند در اثبات قصد فریب و رابطه سببیت میان عملیات متقلبانه و تسلیم مال مورد توجه قرار گیرد. البته تشخیص تحقق جرم، همواره به ارزیابی مجموع رفتارها و اوضاع‌واحوال پرونده وابسته است (ایزدی-زاد، ۱۴۰۴، ص ۲۹۸).

در این مرحله، حفظ ادله الکترونیکی اهمیت اساسی دارد. پیام‌ها، شناسه کاربری، شماره تماس، نشانی صفحه، فایل‌های ارسال‌شده، تصاویر، سوابق پرداخت و اطلاعات فنی می‌تواند برای احراز عملیات متقلبانه ضروری باشد. حذف یا تغییر محتوای حساب کاربری، موجب از بین رفتن ارزش احتمالی آن برای رسیدگی قضایی می‌شود. بنابراین، بزه‌دیده باید از حذف پیام‌ها یا ادامه ارتباط بدون ثبت مستندات خودداری کند و موضوع را از طریق مراجع قانونی گزارش دهد.

۳-۳- مرحله ارتکاب و تحصیل مال

مرحله ارتکاب زمانی تحقق می‌یابد که مرتکب، پس از ایجاد فریب، بزه‌دیده را به انتقال وجه، ارائه اطلاعات بانکی، تسلیم مال، پرداخت هزینه یا انجام یک عمل مالی وادار می‌کند. تحصیل مال ممکن است از طریق انتقال مستقیم به حساب مرتکب، استفاده از درگاه پرداخت، دریافت رمز پویا، برداشت از حساب یا انتقال وجه به حساب اشخاص ثالث انجام شود. در برخی موارد نیز مرتکب با دسترسی به حساب کاربری یا اطلاعات مالی، بدون رضایت واقعی دارنده، عملیات مالی را انجام می‌دهد. باید میان کلاهبرداری و سایر جرایم مالی سایبری تفکیک قائل شد. در کلاهبرداری، فریب و عملیات متقلبانه موجب می‌شود بزه‌دیده با اراده ظاهری، مال را تسلیم کند؛ اما در سرقت رایانه‌ای، ممکن است مال یا داده بدون رضایت معتبر دارنده و از طریق مداخله در سامانه یا داده تحصیل شود. همچنین، دسترسی غیرمجاز، جعل رایانه‌ای و برداشت غیرمجاز از حساب، حسب مورد ممکن است عناوین مستقلی داشته باشند. تعیین عنوان مجرمانه، به نحوه دسترسی، شیوه انتقال مال و وضعیت رضایت بزه‌دیده بستگی دارد (انصاری و همکاران، ۱۳۹۸، ص ۱۷۱).

استفاده از حساب‌های بانکی متعلق یا معاون جرم، شخص فریب‌خورده یا فردی بی‌اطلاع باشد. احراز مسئولیت وی نیازمند بررسی علم، قصد، نحوه در اختیار گذاشتن حساب، میزان انتفاع و ارتباط او با مرتکب اصلی است. صرف واریز وجه به حساب یک شخص، بدون احراز عناصر قانونی، برای انتساب مسئولیت کیفری کافی نیست؛ همان‌گونه که ادعای بی‌اطلاعی نیز در صورت وجود قرائن خلاف، مانع بررسی قضایی نخواهد بود. پس از تحصیل مال، سرعت عمل در توقیف وجوه و حفظ داده‌ها اهمیت زیادی دارد. انتقال سریع وجوه میان چند حساب، تبدیل آن به دارایی‌های دیگر یا برداشت نقدی، امکان استرداد مال را کاهش می‌دهد. از این رو، اعلام فوری جرم، ارائه مستندات پرداخت و درخواست اقدامات تأمینی از مراجع صالح می‌تواند در حفظ آثار جرم مؤثر باشد. با این حال، توقیف یا استرداد مال تابع احراز شرایط قانونی و تصمیم مرجع قضایی است و نمی‌توان بدون بررسی قضایی، نتیجه قطعی آن را تضمین کرد (سلطانی و میری، ۱۴۰۴، ص ۱۵).

۴-۳- مرحله پنهان‌سازی و بازتولید شیوه مجرمانه

پس از تحصیل مال، مرتکب معمولا برای جلوگیری از کشف جرم، آثار ارتباطی و مالی را حذف یا تغییر می‌دهد. بستن حساب کاربری، حذف

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

پیام‌ها، تغییر شماره تماس استفاده از حساب‌های جدید، انتقال وجه به به حساب‌های متعدد و قطع ارتباط با بزه‌دیده از جمله اقدامات این مرحله است. برخی مرتکبان برای دشوار کردن انتساب رفتار، از شبکه‌های ارتباطی مختلف و ابزارهای ناشناس‌ساز استفاده می‌کنند. این اقدامات ممکن است در ارزیابی قصد مجرمانه و تلاش برای مخفی کردن آثار جرم مؤثر باشد. پنهان‌سازی در برخی پرونده‌ها از طریق استفاده از اشخاص واسط انجام می‌شود. حساب‌های بانکی، شماره‌های تلفن، حساب‌های کاربری و ابزارهای پرداخت ممکن است به نام اشخاصی باشد که از ماهیت واقعی فعالیت مرتکب اطلاع ندارند یا با علم به موضوع، در انتقال وجوه همکاری می‌کنند. تشخیص وضعیت حقوقی هر واسطه، نیازمند بررسی عناصر معاونت، مشارکت، علم و قصد است. بنابراین، ارتباط مالی با مرتکب به‌تنهایی برای انتساب عنوان معاونت یا مشارکت کافی نیست (قاجار، ۱۳۸۶، ص ۷۸).

بازتولید شیوه مجرمانه زمانی رخ می‌دهد که مرتکب پس از موفقیت یا حتی پیش از شناسایی، همان الگوی فریب را علیه اشخاص دیگر اجرا کند. در این حالت، متن پیام، تصاویر، اسناد، درگاه پرداخت یا ساختار ارتباطی ممکن است با تغییرات جزئی دوباره مورد استفاده قرار گیرد. تجربه موفقیت در یک عملیات، اطلاعاتی درباره نقاط ضعف بزه‌دیدگان و سازوکارهای نظارتی در اختیار مرتکب قرار می‌دهد و به اصلاح روش ارتکاب منجر می‌شود. برای مقابله با این مرحله، حفظ سوابق فنی، تحلیل ارتباط میان حساب‌ها، ردیابی مالی، همکاری میان ارائه‌دهندگان خدمات و استفاده از ظرفیت کارشناسی پلیس فتا ضروری است. ادله الکترونیکی باید به‌گونه‌ای جمع‌آوری و نگهداری شود که تمامیت، اصالت و قابلیت استناد آن حفظ شود. همچنین، شناسایی الگوهای تکرارشونده می‌تواند به کشف پرونده‌های مرتبط و جلوگیری از ادامه فعالیت مرتکب کمک کند. پاسخ مؤثر به پنهان‌سازی، نیازمند ترکیب اقدامات قضایی، فنی و مالی است (گودرزی و همکاران، ۱۴۰۴، ص ۹۶).

۴- عوامل مؤثر بر تکرار و بازتولید کلاهبرداری‌های سایبری

تکرار و بازتولید کلاهبرداری‌های سایبری در شبکه‌های اجتماعی، حاصل یک عامل منفرد نیست؛ بلکه از مجموعه‌ای از عوامل فردی، محیطی، فنی، اجتماعی و حقوقی ناشی می‌شود. مرتکب زمانی به تکرار رفتار مجرمانه گرایش پیدا می‌کند که از یک‌سو انگیزه لازم برای تحصیل مال یا منفعت را داشته باشد و از سوی دیگر، محیط ارتکاب را برای تحقق هدف خود مناسب ارزیابی کند. سهولت ایجاد حساب کاربری، دسترسی به شمار زیادی از کاربران و دشواری شناسایی مرتکب، این ارزیابی را تقویت می‌کند. در این نوع جرایم، بازتولید رفتار مجرمانه معمولا از طریق استفاده مجدد از ابزارها و روش‌هایی صورت می‌گیرد که در عملیات پیشین موفق بوده‌اند. مرتکب ممکن است قالب پیام، عنوان مجعول، تصویر، شیوه تبلیغ، حساب دریافت وجه یا نشانی ارتباطی خود را با تغییرات جزئی دوباره به کار گیرد. به این ترتیب، هر عملیات موفق می‌تواند به منبعی برای کسب تجربه، شناسایی نقاط ضعف و اصلاح روش مجرمانه تبدیل شود. هرچه احتمال کشف، تعقیب و مجازات کمتر و منفعت مورد انتظار بیشتر باشد، زمینه تکرار جرم افزایش می‌یابد. در کلاهبرداری سایبری، انتقال سریع وجوه، استفاده از حساب‌های واسط، فعالیت با هویت‌های غیرواقعی و حذف ادله، هزینه ارتکاب را برای بزهکار کاهش می‌دهد. این وضعیت در کنار ضعف نظارت بر برخی حساب‌ها و تأخیر در اعلام جرم، چرخه تکرار را تقویت می‌کند (نظری منظم و همکاران، ۱۳۹۸، ص ۲۲۳).

از نظر نگارنده، بازتولید کلاهبرداری سایبری را باید نتیجه تعامل میان انگیزه مجرمانه و فرصت‌های موجود در محیط شبکه‌های اجتماعی دانست. بنابراین، پاسخ مؤثر به این پدیده صرفا با افزایش مجازات امکان‌پذیر نیست و باید عواملی که سودمندی جرم و امکان تکرار آن را افزایش می‌دهند، هم‌زمان کاهش داد. جلوگیری از فعالیت حساب‌های جعلیزمان کاهش داد. جلوگیری از فعالیت حساب‌های جعلی، انسداد سریع مسیر انتقال وج راهکارهای کاهش تکرار این جرم است.

۴-۱- عوامل فردی و انگیزشی بزهکاران

عامل اقتصادی، یکی از مهم‌ترین انگیزه‌های ارتکاب کلاهبرداری سایبری

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

است. مرتکب ممکن است با هدف تحصیل مال، دستیابی به درآمد سریع یا جبران وضعیت مالی خود، به طراحی عملیات متقلبانه اقدام کند. با وجود این، انگیزه اقتصادی به‌تنهایی برای تبیین رفتار کافی نیست؛ زیرا بسیاری از افراد با مشکلات مالی مواجه‌اند، اما مرتکب جرم نمی‌شوند. آنچه اهمیت دارد، پیوند میان نیاز مالی، پذیرش هنجارشکنی، ضعف کنترل درونی و ارزیابی پایین خطر کشف است. برخی بزهکاران از توانایی فنی یا مهارت ارتباطی خود برای ارتکاب جرم استفاده می‌کنند. آشنایی با سازوکار شبکه‌های اجتماعی، شیوه‌های پرداخت الکترونیکی، تنظیم محتوای اقناعی و بهره‌گیری از داده‌های کاربران، امکان طراحی فریب مؤثرتر را فراهم می‌کند. در این حالت، مهارت فنی که ذاتا واجد وصف مجرمانه نیست، در خدمت رفتار متقلبانه قرار می‌گیرد و به وسیله‌ای برای تحصیل مال دیگری تبدیل می‌شود (بهارستانی، ۱۴۰۱، ص ۱۲).

عوامل شخصیتی نیز در استمرار رفتار مجرمانه مؤثر است. احساس بی‌اعتنایی به حقوق مالی دیگران، توجیه رفتار با ادعای استحقاق، فقدان احساس مسئولیت اجتماعی و عادی‌سازی دروغ می‌تواند مانع بازدارندگی درونی شود. در برخی موارد، مرتکب به دلیل فقدان تماس مستقیم با بزه‌دیده، آثار زیان‌بار رفتار خود را کمتر احساس می‌کند. فاصله ارتباطی میان مرتکب و بزه‌دیده ممکن است موجب کاهش همدلی و افزایش آمادگی برای تکرار جرم شود (محمودی تکانلو و آسیایی، ۱۴۰۴، ص ۱۷۵).

از نظر نگارنده، تبیین عوامل فردی نباید به برچسب‌زنی یا انتساب جرم به ویژگی‌های ثابت شخصیتی محدود شود. مسئولیت کیفری باید بر مبنای رفتار خارجی، سوءنیت و عناصر قانونی جرم احراز شود. با این حال، برای پیشگیری از تکرار، شناسایی انگیزه‌های مالی، مهارت‌های مورد سوءاستفاده و الگوهای رفتاری مرتکبان اهمیت دارد. برنامه‌های اصلاحی و بازپرورانه در کنار مجازات قانونی، می‌تواند در کاهش احتمال تکرار جرم مؤثرتر از پاسخ صرفا تنبیهی باشد.

۲-۴- عوامل محیطی و فنی شبکه‌های اجتماعی

ساختار شبکه‌های اجتماعی، فرصت ارتباط سریع میان اشخاص ناشناس را فراهم می‌کند. کاربر می‌تواند در مدت کوتاه با اشخاص متعددی ارتباط برقرار کند، محتوای خود را منتشر سازد و به گروه‌های مختلف دسترسی پیدا کند. این قابلیت، در صورت فقدان سازوکارهای مناسب احراز هویت و نظارت، برای ارتکاب کلاهبرداری مورد استفاده قرار می‌گیرد. مرتکب می‌تواند بدون حضور فیزیکی و بدون ایجاد سابقه تجاری واقعی، خود را فروشنده، سرمایه‌گذار، کارشناس یا نماینده یک نهاد معرفی کند. امکان ایجاد حساب‌های متعدد و تغییر سریع مشخصات آن‌ها نیز از عوامل فنی مؤثر بر تکرار جرم است. حساب کاربری جعلی ممکن است پس از دریافت وجه یا انتشار محتوای فریبنده حذف شود و حساب دیگری با همان روش ایجاد گردد. استفاده از تصاویر سرقت‌شده، نام اشخاص معتبر، نشان‌های تجاری و محتوای ساختگی، تشخیص هویت و اعتبار واقعی حساب را دشوار می‌سازد (نیک-نژاد فشتمی، ۱۴۰۰، ص ۴).

ویژگی‌های فنی شبکه‌های اجتماعی، امکان انتشار گسترده و سریع محتوای مجرمانه را نیز فراهم می‌کند. یک آگهی یا پیام فریبنده ممکن است در مدت کوتاه در چندین گروه و صفحه منتشر شود. همچنین، امکان ارسال خصوصی پیام، برقراری تماس صوتی یا تصویری و استفاده از پیوندهای خارجی، ابزارهای متعددی برای تکمیل عملیات فریب در اختیار مرتکب قرار می‌دهد. هرچه مسیرهای ارتباطی بیشتر باشد، جمع‌آوری ادله و تعیین نقطه آغاز جرم دشوارتر خواهد بود (همان، ص ۵).

از نظر نگارنده، مسئولیت پیشگیری را نمی‌توان تنها بر عهده کاربران گذاشت. سکوهای ارائه‌دهنده خدمات شبکه اجتماعی نیز باید متناسب با ظرفیت فنی خود، سازوکار گزارش‌دهی، احراز هویت حساب‌های تجاری، تشخیص رفتارهای غیرعادی و حفظ سوابق ارتباطی را تقویت کنند. این اقدامات باید با رعایت حریم خصوصی، اصل قانونی‌بودن مداخله و الزامات مربوط به صیانت از داده‌های شخصی انجام شود.

۳-۴ - ضعف کنترل رسمی و غیررسمی و پایین‌بودن هزینه ارتکاب

کنترل رسمی شامل اقدامات نهادهای قضایی، انتظامی، بانکی و نهادهای ناظر بر خدمات ارتباطی است. هرگاه این نهادها در شناسایی، ثبت، حفظ

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 تحلیل ادله الکترونیکی با محدودیت مواجه باشند، احتمال کشف جرم کاهش می‌یابد. پراکندگی داده‌ها میان سکوهای اجتماعی، بانک‌ها، اپراتورها و ارائه‌دهندگان خدمات اینترنتی نیز می‌تواند فرایند تحقیقات را طولانی کند. کنترل غیررسمی به نظارت خانواده، جامعه، محیط شغلی و روابط اجتماعی مربوط است. در فضای شبکه‌های اجتماعی، ارتباطات غالبا بدون شناخت پیشین و بر اساس اطلاعاتی شکل می‌گیرد که صحت آن‌ها برای کاربر روشن نیست. نبود اعتبارسنجی اجتماعی، کاهش نقش شاهدان و ضعف امکان بررسی سوابق واقعی اشخاص، کنترل غیررسمی را کاهش می‌دهد و به مرتکب اجازه می‌دهد با هویت ساختگی فعالیت کند (ادیبی رکاوندی، ۱۴۰۵، ص ۱۵).

پایین‌بودن هزینه ارتکاب، از عوامل مهم استمرار این جرم است. ایجاد یک حساب کاربری، انتشار پیام و برقراری ارتباط معمولا به منابع مالی زیادی نیاز ندارد؛ در حالی که منفعت احتمالی می‌تواند قابل توجه باشد. همچنین، اگر مرتکب تصور کند که احتمال شناسایی وی پایین است، مجازات احتمالی در تصمیم او اثر بازدارنده کافی نخواهد داشت. این وضعیت در نظریه انتخاب عقلانی جرم، با مقایسه سود مورد انتظار و هزینه احتمالی رفتار قابل تبیین است (پورهاشمی و همکاران، ۱۴۰۳، ص ۱۳۹). از نظر نگارنده، کاهش هزینه ارتکاب باید از طریق افزایش احتمال کشف و سرعت واکنش قانونی انجام شود، نه صرفا از طریق تشدید کیفر. ثبت دقیق اطلاعات هویتی، ردیابی مالی، ارتباط منظم میان ضابطان و بانک‌ها، رسیدگی سریع به گزارش‌ها و آموزش کارشناسان، می‌تواند هزینه عملی ارتکاب را افزایش دهد. بازدارندگی واقعی زمانی شکل می‌گیرد که مرتکب، کشف و تعقیب رفتار خود را محتمل و سریع ارزیابی کند.

۵- نقش بزه‌دیده در شکل‌گیری و تداوم چرخه کلاهبرداری سایبری

بزه‌دیده در کلاهبرداری سایبری، موضوع رفتار مجرمانه و شخص زیان‌دیده از آن است. بررسی نقش بزه‌دیده نباید به معنای انتقال مسئولیت جرم از مرتکب به او باشد؛ زیرا عنصر اصلی جرم، عملیات متقلبانه و قصد تحصیل مال دیگری است. با این حال، وضعیت اطلاعاتی، اقتصادی و ارتباطی بزه‌دیده می‌تواند بر انتخاب وی، میزان موفقیت فریب و استمرار چرخه جرم اثر بگذارد. انتشار گسترده اطلاعات شخصی، اعتماد به حساب‌های ناشناس، انجام پرداخت بدون بررسی هویت طرف معامله و ارسال اطلاعات بانکی، از رفتارهایی است که آسیب‌پذیری بزه‌دیده را افزایش می‌دهد. این اقدامات ممکن است ناشی از ناآگاهی، اضطرار، اعتماد به عنوان‌های رسمی یا تصور امنیت کاذب باشد. در برخی پرونده‌ها، مرتکب با ایجاد فشار زمانی یا وعده سود فوری، فرصت تصمیم‌گیری محتاطانه را از بزه‌دیده می‌گیرد (باستانی، ۱۳۹۰، ص ۵۲).

عدم اعلام فوری جرم نیز می‌تواند به تداوم فعالیت مرتکب کمک کند. برخی بزه‌دیدگان به دلیل نگرانی از افشای اطلاعات شخصی، احساس شرمساری، بی‌اعتمادی به نتیجه رسیدگی یا ناچیز دانستن مبلغ زیان، از گزارش موضوع خودداری می‌کنند. این سکوت موجب می‌شود حساب‌ها و ابزارهای مورد استفاده همچنان فعال بماند و اشخاص دیگری نیز در معرض فریب قرار گیرند (انصاری و همکاران، ۱۳۹۸، ص ۱۷۰).

از نظر نگارنده، نقش بزه‌دیده باید در چارچوب بزه‌دیده‌شناسی حمایتی بررسی شود، نه با رویکرد سرزنش‌گر. آموزش حقوقی، تسهیل ثبت شکایت، حمایت از محرمانگی اطلاعات، تسریع در انسداد وجوه و اطلاع‌رسانی درباره شیوه‌های رایج فریب، مسئولیت نهادهای عمومی و خصوصی است. بی‌احتیاطی احتمالی بزه‌دیده، در صورت وجود عملیات متقلبانه، وصف کیفری رفتار مرتکب را از بین نمی‌برد.

۶- شبکه‌های اجتماعی به‌مثابه محیط جرم‌زا و بستر بازتولید کلاهبرداری

شبکه‌های اجتماعی به دلیل ترکیب ارتباط گسترده، دسترسی سریع، تعامل مستمر و امکان فعالیت ناشناس، می‌توانند در شرایط خاص به محیط جرم‌زا تبدیل شوند. محیط جرم‌زا محیطی است که فرصت ارتکاب جرم را افزایش می‌دهد و موانع کنترل آن را کاهش می‌دهد. شبکه اجتماعی ذاتا مجرمانه نیست؛ اما ضعف نظارت، فقدان احراز هویت مؤثر و انتشار محتوای بدون اعتبارسنجی می‌تواند قابلیت سوءاستفاده از آن را افزایش دهد. در این محیط، مرز میان ارتباط خصوصی، تبلیغ عمومی و فعالیت تجاری همواره روشن نیست. مرتکب ممکن است ابتدا از طریق یک پیام خصوصی ارتباط برقرار کند، سپس با ارائه محتوای عمومی 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

جلب تأیید دیگران، اعتماد بزه‌دیده را افزایش دهد. استفاده از نظرهای ساختگی، دنبال‌کنندگان غیرواقعی و تصاویر حرفه‌ای، به ایجاد ظاهر اعتبار کمک می‌کند. ظاهر اجتماعی و عمومی حساب کاربری، در بسیاری از موارد جایگزین بررسی واقعی هویت می‌شود (خداقلی، ۱۳۸۴، ص ۳۹).

شبکه‌های اجتماعی همچنین امکان تشکیل اجتماعات مجرمانه و تقسیم وظایف را فراهم می‌کنند. یک شخص ممکن است مسئول ایجاد حساب جعلی، شخص دیگر مسئول برقراری ارتباط، فردی مسئول دریافت وجه و شخص دیگری مسئول انتقال آن باشد. در این وضعیت، تشخیص نقش هر فرد و احراز علم و قصد او اهمیت حقوقی دارد. تقسیم وظایف، لزوما به معنای تحقق مشارکت یا معاونت نیست؛ بلکه انتساب مسئولیت به بررسی دقیق رفتار و عنصر روانی نیازمند است (والایی، ۱۴۰۱، ص ۲).

از نظر نگارنده، رویکرد حقوقی به شبکه‌های اجتماعی باید میان آزادی ارتباطات، حریم خصوصی و ضرورت پیشگیری از جرم تعادل برقرار کند. حذف گسترده و بدون ضابطه محتوا، با اصول قانونی و حقوق کاربران سازگار نیست؛ اما بی‌توجهی به حساب‌های جعلی، تبلیغات متقلبانه و فعالیت‌های مالی مشکوک نیز زمینه گسترش جرم را فراهم می‌سازد. راهکار مناسب، نظارت مبتنی بر خطر، پاسخ مرحله‌ای، ثبت سوابق و مداخله قضایی در موارد لازم است.

۷- چالش‌های کشف، جرم‌یابی و پاسخ کیفری به کلاهبرداری‌های سایبری در شبکه‌های اجتماعی

نخستین چالش، شناسایی هویت واقعی مرتکب است. اطلاعات درج‌شده در حساب کاربری ممکن است جعلی باشد و شماره تماس، نشانی اینترنتی یا حساب بانکی نیز به نام شخص دیگری ثبت شده باشد. استفاده از حساب‌های متعدد و انتقال ارتباط میان سکوهای مختلف، انتساب رفتار را دشوار می‌کند. در نتیجه، صرف شناسایی یک حساب یا شماره تماس، برای اثبات هویت مرتکب کافی نیست و باید مجموعه‌ای از ادله فنی و مالی بررسی شود (فتحی، ۱۴۰۱، ص ۱۳).

چالش دوم، جمع‌آوری و اعتبارسنجی ادله الکترونیکی است. پیام‌ها، تصاویر، فایل‌ها، شناسه‌های فنی و سوابق تراکنش‌ها ممکن است به‌سرعت حذف یا تغییر داده شوند. تصویر صفحه نمایش، هرچند می‌تواند آغازگر تحقیقات باشد، در همه موارد برای اثبات اصالت و انتساب محتوا کافی نیست. مقام قضایی و ضابط باید با رعایت ضوابط قانونی، داده‌ها را حفظ و از تغییر یا مخدوش‌شدن آن‌ها جلوگیری کند (همان، ص ۱۴).

چالش دیگر، فرامرزی‌بودن بسیاری از خدمات و داده‌ها است. ممکن است بزه‌دیده، مرتکب، بانک، سرور و سکوی ارتباطی در حوزه‌های قضایی متفاوت قرار داشته باشند. دسترسی به داده‌های خارج از قلمرو کشور، مستلزم رعایت مقررات داخلی، همکاری قضایی بین‌المللی و تعامل با ارائه‌دهندگان خدمات است. این وضعیت، سرعت تحقیقات را کاهش می‌دهد و در برخی موارد امکان دسترسی به داده‌های ضروری را محدود می‌کند (پورهاشمی و همکاران، ۱۴۰۲، ص ۱۵۲).

پاسخ کیفری نیز با مسائل مربوط به تعیین عنوان مجرمانه، صلاحیت، ادله، انتساب رفتار و استرداد مال مواجه است. کلاهبرداری سایبری ممکن است با جرایم رایانه‌ای، جعل، استفاده از سند مجعول، دسترسی غیرمجاز یا پول‌شویی ارتباط پیدا کند. تشخیص عنوان صحیح و تعیین رابطه میان جرایم، نیازمند تحلیل فنی و حقوقی هم‌زمان است. همچنین، حمایت از بزه‌دیده و جبران زیان مالی باید در کنار تعقیب مرتکب مورد توجه قرار گیرد (فضلی، ۱۳۹۱، ص ۷۱).

از نظر نگارنده، مهم‌ترین راهکار، ایجاد سازوکار یکپارچه برای ثبت شکایت، حفظ فوری داده‌ها، ردیابی وجوه و تبادل اطلاعات میان نهادهای مرتبط است. آموزش تخصصی ضابطان، قضات و کارشناسان در زمینه ادله الکترونیکی باید مستمر باشد. همچنین، مقررات مربوط به شبکه‌های اجتماعی باید به‌گونه‌ای اجرا شود که ضمن حفظ حقوق بنیادین کاربران، امکان واکنش سریع به رفتارهای متقلبانه را فراهم کند. پاسخ کیفری مؤثر زمانی شکل می‌گیرد که کشف جرم، انتساب رفتار، توقیف مال و رسیدگی قضایی در یک فرایند هماهنگ انجام شود.

۸- راهکارهای جرم‌شناختی پیشگیری و قطع چرخه تکرار کلاهبرداری سایبری

پیشگیری از کلاهبرداری سایبری و متوقف ساختن چرخه بازتولید آن،

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

مستلزم اتخاذ رهیافتی چندبعدی در چارچوب سیاست جنایی مشارکتی است. تدابیر واکنشی و اعمال مجازات پس از وقوع بزه، به تنهایی توانایی مهار این پدیده را ندارند؛ زیرا ماهیت فرامرزی، سرعت بالای انتقال اموال و گمنامی نسبی مرتکبان، بازدارندگی عمومی کیفرهای سنتی را تضعیف کرده است. بنابراین، کانون توجه تدابیر جرم‌شناختی باید بر مرحله پیش از وقوع جرم و اختلال در توالی اقدامات بزهکارانه متمرکز گردد. قطع چرخه تکرار جرم ایجاب می‌کند که پیوند میان ابزارهای فنی، منافذ ارتباطی و منافع مالی مرتکب از بین برود. در این راستا، راهکارهای پیشگیرانه باید هم‌زمان بر محیط ارتکاب، آگاهی و واکنش آماج‌های جرم و سازوکارهای نظارتی ناظر بر سکوهای دیجیتال اثر بگذارند. خنثی‌سازی شیوه‌های بازتولید بزه، مستلزم طراحی پاسخ‌هایی است که منفعت حاصل از ارتکاب را به حداقل رسانده و در مقابل، خطر کشف و توقیف عواید مجرمانه را افزایش دهد (گودرزی و همکاران، ۱۴۰۴، ص ۱۰۴).

همچنین، تفکیک میان اقدامات فنی، حقوقی و اجتماعی در امر پیشگیری حائز اهمیت بنیادین است. پاسخ فنی شامل ایمن‌سازی زیرساخت‌های تبادل داده و مسدودسازی روزنه‌های سوءاستفاده است؛ در حالی که پاسخ حقوقی بر تعیین شفاف تکالیف پلتفرم‌ها و تسهیل جمع‌آوری ادله الکترونیکی تأکید دارد. هم‌افزایی این دو حوزه در بستر آموزش‌های عمومی، زمینه شکل‌گیری یک نظام جامع پیشگیرانه را در فضای شبکه‌های اجتماعی فراهم می‌آورد (تجری و صادقیان لمسراکی، ۱۴۰۳، ص ۱۱).

از نظر نگارنده، موفقیت راهکارهای جرم‌شناختی در گرو گذار از نگاه تک‌بعدی کیفری به سمت الگوی جامع مدیریت ریسک سایبری است. در این الگو، پیشگیری نباید صرفا به عنوان مداخله پسینی یا هشدارهای کلی تلقی شود، بلکه باید در معماری فنی شبکه‌های اجتماعی، نظام‌های پرداخت مالی و فرایندهای دادرسی سایبری تعبیه گردد تا انگیزه و فرصت تکرار جرم به شکل ساختاری مهار شود.

۱-۸- پیشگیری وضعی و کاهش فرصت‌های ارتکاب

پیشگیری وضعی از طریق دستکاری در محیط مستقیم ارتکاب، به دنبال دشوار ساختن دستیابی به هدف، افزایش خطر دستگیری و کاهش عواید ناشی از جرم است. در بستر شبکه‌های اجتماعی، افزایش دشواری ارتکاب می‌تواند از طریق الزام به احراز هویت چندمرحله‌ای برای حساب‌های کاربری تجاری یا تبلیغاتی، اعتبارسنجی شماره‌های تماس و محدودسازی ایجاد انبوه حساب‌های نامعتبر محقق شود. این تدابیر امکان پنهان‌سازی هویت را که پیش‌شرط ورود به چرخه کلاهبرداری است، به شدت محدود می‌سازد. افزایش خطرات ارتکاب نیز از طریق به‌کارگیری سامانه‌های هوشمند کشف الگوهای مشکوک در بستر شبکه، نظارت بر تبادل لینک‌های ناشناس و پایش پیام‌های انبوه صورت می‌پذیرد. همچنین، کاهش جذابیت آماج جرم از طریق تعبیه هشدارهای خودکار هنگام انتقال اطلاعات حساس، اعمال محدودیت زمانی بر تراکنش‌های بانکی ناشی از ارجاعات مستقیم شبکه‌های اجتماعی و تفکیک درگاه‌های پرداخت استاندارد از پیوندهای فیشینگ، مانع از تسلیم شتاب‌زده مال توسط کاربران می‌گردد. حذف ابزارها و منافع مجرمانه از ارکان حیاتی پیشگیری وضعی است. ایجاد مکانیسم‌های انسداد برخط و فوری حساب‌های بانکی مقصد، غیرفعال‌سازی سریع صفحات مجعول گزارش‌شده و توقیف وجوه در لایه‌های نخستین تراکنش، عایدی اقتصادی بزهکار را سلب می‌کند. هنگامی که مرتکب نتواند وجوه تحصیل‌شده را در فاصله زمانی کوتاه جابه‌جا یا نقد کند، چرخه بازتولید عملیات متقلبانه با اختلال اساسی مواجه خواهد شد (بهارستانی، ۱۴۰۱، ص ۱۶).

از نظر نگارنده، اجرای تدابیر وضعی نباید به تحدید ناروای حقوق بنیادین کاربران و آزادی تبادل اطلاعات مشروع منجر گردد. اصل تناسب ایجاب می‌کند که تدابیر سخت‌گیرانه وضعی به طور هدفمند بر حساب‌های کاربری ارائه‌دهنده خدمات مالی، تبلیغات با ریسک بالا و تراکنش‌های بانکی کلان یا مشکوک متمرکز شود تا ضمن حفظ امنیت فضای مجازی، کارکرد تسهیل‌کننده شبکه‌های اجتماعی مخدوش نشود.

۲-۸- ارتقای آگاهی و تاب‌آوری کاربران

توانمندسازی شناختی کاربران و تقویت مهارت‌های اعتبارسنجی دیجیتال، از محوری‌ترین مؤلفه‌های پیشگیری اجتماعی و رشد تاب‌آوری

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

در برابر شیوه‌های متقلبانه است. از آنجا که کلاهبرداری سایبری غالبا بر فریب ذهنی و روان‌شناختی استوار است، مصون‌سازی بزه‌دیدگان بالقوه از طریق آموزش روش‌های مهندسی اجتماعی، شناخت جعل هویت و پرهیز از تصمیم‌گیری‌های شتاب‌زده، نخستین سد دفاعی در برابر شکل‌گیری جرم محسوب می‌شود. ارتقای سواد حقوقی و سایبری به کاربران می‌آموزد که چگونه ماهیت حساب‌های کاربری را پیش از هرگونه تعامل مالی بررسی کنند. کسب مهارت در تشخیص درگاه‌های پرداخت رسمی، عدم اعتماد به القاب و نشان‌های اعتباری ساختگی، بررسی اصالت مجوزهای کسب‌وکار برخط و امتناع از ارسال اطلاعات هویتی و رمزهای یک‌بارمصرف، موجب کاهش نرخ بزه‌دیدگی می‌گردد. این آگاهی‌ها بزه‌دیده را از حالت یک هدف منفعل به یک مانع جدی در برابر ارتکاب جرم تبدیل می‌کند. ترویج فرهنگ گزارش‌دهی فوری و مشارکت در پایش تخلفات نیز در تقویت تاب‌آوری جمعی نقش بسزایی دارد. آموزش نحوه ثبت شکایت در سامانه‌های انتظامی و قضایی، حفظ و نگهداری مستندات دیجیتال نظیر شناسه پیام‌ها، آدرس صفحات و تصاویر معتبر بدون ایجاد تغییر در آنها، از بین رفتن ادله الکترونیکی را ناممکن می‌سازد و زمان واکنش مراجع قانونی را به حداقل می‌رساند (ایزدی-زاد، ۱۴۰۴، ص ۳۰۳).

از نظر نگارنده، برنامه‌های آموزشی نباید به هشدارهای کلی و سطحی محدود بماند، بلکه باید به شکل مستمر، پرونده‌محور و منطبق با شیوه‌های نوظهور فریب طراحی شود. نهادینه‌سازی آموزش‌های حفاظت از داده‌های شخصی در برنامه‌های رسانه‌ای و آموزشی، نوعی خودکنترلی فعال ایجاد می‌کند که هزینه عملیات روانی بزهکاران را به شدت افزایش خواهد داد.

۳-۸- تقویت نظارت، کشف و همکاری سکوهای شبکه اجتماعی با نهادهای مسئول

مسئولیت اجتماعی و حقوقی سکوهای ارائه‌دهنده خدمات ارتباطی، رکن غیرقابل انکار در کشف سریع و مقابله با کلاهبرداری‌های سایبری است. این سکوها به دلیل تسلط فنی بر ساختار شبکه، موظف‌اند ابزارهای کارآمدی را برای گزارش‌دهی مستقیم و آسان تخلفات توسط کاربران فراهم آورند. پردازش بی‌درنگ گزارش‌های مردمی و به‌کارگیری هوش مصنوعی برای شناسایی رفتارهای غیرعادی، از تکثیر دامنه‌دار شیوه‌های مجرمانه جلوگیری به عمل می‌آورد. تعامل نظام‌مند و قانونمند میان مدیران سکوها، نهادهای قضایی، ضابطان تخصصی و شبکه بانکی، امکان مسدودسازی شبکه‌های بزهکاری را تسریع می‌بخشد. برقراری ارتباطات فنی ایمن جهت استعلام اصالت حساب‌ها و تبادل داده‌های مربوط به حساب‌های متخلف با رعایت الزامات صیانت از حریم خصوصی، زنجیره پنهان‌سازی هویت را منقطع می‌سازد. این همکاری مشترک، زمان طلایی مهار جرم را از دسترسی بزهکار خارج می‌کند. حفظ، نگهداری و ذخیره‌سازی استاندارد لاگ‌ها و سوابق ترافیکی توسط سکوها مطابق با ضوابط قانونی، ارزش اثباتی ادله الکترونیکی را در دادرسی کیفری تضمین می‌نماید. دسترسی مشروع و سریع مراجع تحقیق به زنجیره داده‌های ارتباطی، فرآیند انتساب جرم به مرتکب واقعی را تسهیل نموده و مانع از پنهان‌شدن وی در پس حساب‌های اجاره‌ای یا هویت‌های مجعول می‌گردد (نظری منظم و همکاران، ۱۳۹۸، ص ۱۸۰).

از نظر نگارنده، تنظیم‌گری قانونی باید تکالیف شفافی را برای سکوهای شبکه اجتماعی در جهت پیشگیری وضعی و همکاری با ضابطان تعیین کند و در عین حال ضمانت‌اجراهای مسئولیت مدنی و انتظامی را برای کوتاهی‌های فاحش پیش‌بینی نماید. ایجاد این چارچوب تعاملی، بدون تعرض به داده‌های خصوصی کاربران، تضمین‌کننده امنیت مبادلات و مانع از تبدیل سکوها به بستری امن برای بازتولید جرایم مالی خواهد بود.

نتیجه‌گیری

پژوهش حاضر با تحلیل جرم‌شناختی چرخه بروز و تکرار کلاهبرداری‌های سایبری در بستر شبکه‌های اجتماعی نشان داد که این پدیده، فرایندی ساختاریافته و چندمرحله‌ای است که از تعامل متقابل فرصت‌های فنی، انگیزه‌های فردی، ضعف نظارت و آسیب‌پذیری‌های شناختی بزه‌دیده ناشی می‌شود. یافته‌های تحقیق اثبات می‌کند که بزهکاران با بهره‌گیری از گمنامی، ساخت هویت‌های جعلی و تکنیک‌های مهندسی اجتماعی، اعتماد کاربران را جلب کرده و با تسهیل دسترسی به ابزارهای پرداخت

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

برخط، مال قربانی را تحصیل می‌کنند. پایداری و تکرار این چرخه ناشی از سهولت بازتولید شیوه مجرمانه با کمترین هزینه، بهره‌گیری از حساب‌های واسط و تأخیر در جمع‌آوری و تثبیت ادله الکترونیکی است که هزینه ارتکاب را کاهش داده و عواید مجرمانه را دست‌یافتنی می‌سازد. بنابراین، مواجهه با این جرایم مستلزم گذار از پاسخ‌های صرفا کیفری و پسینی به سمت رویکردهای جامع جرم‌شناختی، مبتنی بر پیشگیری وضعی، نظارت پلتفرمی و ارتقای مهارت‌های اعتبارسنجی دیجیتال نزد کاربران است.

لذا برای قطع پایدار چرخه کلاهبرداری سایبری در شبکه‌های اجتماعی، پیشنهاد می‌شود سامانه‌ای یکپارچه و برخط میان دادستانی، پلیس فتا، بانک مرکزی و سکوهای مجازی جهت مسدودسازی فوری حساب‌های مقصد و توقیف وجوه در کمتر از نیم ساعت پس از اعلام اولیه جرم راه‌اندازی شود؛ سکوها ملزم گردند سازوکار نماد اعتماد هوشمند را برای حساب‌های کاربری تجاری اجباری ساخته و هویت متقاضیان تبلیغات مالی را پیش از انتشار اعتبارسنجی کنند؛ شبکه بانکی سقف تراکنش‌های ارجاعی از بستر پیام‌رسان‌ها را برای حساب‌های با سابقه فعالیت نامشخص محدود ساخته و الگوریتم‌های هوش مصنوعی را در درگاه‌های پرداخت برای شناسایی رفتارهای مالی پرخطر تعبیه نماید؛ مراجع قضایی شعب تخصصی را به ابزارهای اعتبارسنجی خودکار ادله الکترونیکی مجهز سازند و در نهایت، نهادهای آموزشی و رسانه‌ای الگوهای سواد امنیتی و مهارت‌های واکنش به مهندسی اجتماعی را در قالب آموزش‌های عمومی مستمر نهادینه کنند.

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

الف- کتاب-ها

۱- باستانی، برومند (۱۳۹۰)، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ سوم، تهران: انتشارات بهنامی

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

۳- فضلی، مهدی (۱۳۹۱)، مسئولیت کیفری در فضای سایبر، چاپ دوم، تهران: انتشارات خرسندی

۴- قاجار، سیامک (۱۳۸۶)، حقوق سایبر، تهران: نشر میزان

ب- مقاله-ها

۱- ادیبی رکاوندی، روح‌الله (۱۴۰۵)، «مطالعه جرم‌شناختی تاثیر شبکه‌های اجتماعی بر الگوهای تکرار جرم و رفتارهای پرخطر»، دانشنامه فقه و حقوق تطبیقی، دوره ۵، شماره ۲، صص ۱-۲۵.

۲- انصاری، جلال؛ عطازاده، سعید؛ قیومزاده، محمود (۱۳۹۸)، «سیاست جنایی ایران و آمریکا در قبال جرایم کلاهبرداری و سرقت سایبری»، نشریه پژوهش‌های اطلاعاتی و جنایی، دوره ۱۴، شماره ۳، صص ۱۶۵-۱۷۶.

۳- اوجاقلو، صالح؛ زندی، محمدرضا؛ امیدی، جلیل (۱۴۰۱)، «کلاهبرداری سایبری در بستر رویه قضایی»، نشریه کارآگاه، دوره ۱۶، شماره ۶۱، صص ۱۷۴-۱۹۳.

۴- ایزدی‌زاد، حسن (۱۴۰۴)، «تحلیل جرم‌شناختی تاثیر شبکه‌های اجتماعی و تحولات فرهنگی بر دگرگونی الگوهای بزهکاری در ایران با تاکید بر جرایم نمایشی و هویت‌محور»، فصلنامه علمی مطالعات حقوق و علوم قضایی، سال دوم، شماره ۶، صص ۲۹۵-۳۱۱.

۵- بهارستانی، سمانه (۱۴۰۱)، «کلاهبرداری و تروریسم سایبری و جرایم اینترنتی در حقوق کیفری»، دومین کنفرانس ملی حقوق، فقه و فرهنگ، صص ۱-۲۳.

۶- بهاری غازانی، مجید (۱۴۰۰)، «واکاوی حقوقی کلاهبرداری سایبری»، چهارمین کنفرانس بین‌المللی مطالعات اجتماعی، حقوق و فرهنگ عامه، صص ۱-۱۸.

۷- پورهاشمی، سیده امسلمه؛ علی‌نقیان، نسرین؛ علی‌دوست معززی لاهیجان، امیرمحمد (۱۴۰۲)، «بررسی تاثیر کلاهبرداری سایبری بر قصد خرید آنلاین با استفاده از نظریه رفتار برنامه‌ریزی شده»، نشریه فناوری اطلاعات و ارتباطات انتظامی، دوره ۴، شماره ۱۶، صص ۱۳۴-۱۵۹.

۸- تجری، کامران؛ صادقیان لمسراکی، محدثه (۱۴۰۳)، «شیوه‌های جرم‌شناختی و کیفرشناختی پیشگیری از سرقت و کلاهبرداری سایبری در حقوق ایران»، اولین همایش ملی تاثیر متقابل حقوق بین‌الملل و حقوق داخلی در توسعه قوانین، صص ۱-۱۴.

۹- سلطانی، جهانبخش؛ میری، سید محمدحسین (۱۴۰۴)، «تحلیل فقهی-حقوقی مسئولیت مدنی بانک در قبال کلاهبرداری‌های سایبری و سرقت الکترونیکی منابع مشتریان»، شانزدهمین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق، صص ۱-۱۹.

۱۰- فتحی، حجت‌الله (۱۴۰۱)، «عناوین مجرمانه دستبردهای سایبری»، نشریه حقوق اسلامی، دوره ۱۹، شماره ۴، صص ۱۲۳-۱۴۵.

۱۱- گودرزی، مجتبی؛ خالقانی اصفهانی، مهدی؛ کنعانی، محمدعلی (۱۴۰۴)، «سیاست جنایی ایران در قبال رمز ارزها با تاکید بر پیشگیری از پولشویی در بستر کسب‌وکارهای دیجیتال»، پژوهشنامه حقوق کسب‌وکار و سرمایه‌گذاری، دوره ۱، شماره ۲، صص ۹۴-۱۱۴.

۱۲- محمودی تکانلو، حسین؛ آسیایی، رویا (۱۴۰۴)، «تحلیل جرم‌شناختی جرایم حوزه رمز ارزها؛ مطالعه کلاهبرداری‌های رایج در ایران»، نشریه تمدن حقوقی، دوره ۸، شماره ۲۶، صص ۱۶۷-۱۸۲.

۱۳- نظری منظم، مهدی؛ مجیدی، عبدالله؛ هندیانی، عبدالله؛ وفادار، حسین (۱۳۹۸)، «بررسی عوامل موثر بر جرم‌یابی کلاهبرداری در فضای سایبر»، فصلنامه پژوهش‌های دانش انتظامی، سال ۲۱، شماره ۲، صص ۲۱۷-۲۴۵.

۱۴- نیک‌نژاد فشتمی، علی (۱۴۰۰)، «تاثیر کلاهبرداری سایبری و اعتماد به سیستم تجارت الکترونیکی بر قصد خرید»، پنجمین کنفرانس بین‌المللی حقوق و علوم قضایی، صص ۱-۱۲.

۱۵- الهیاری، طلعت؛ مجیدی‌پرست، سجاد (۱۳۹۳)، «گونه‌شناسی باندهای جرم و فساد در فضای مجازی»، پژوهشنامه مددکاری اجتماعی، دوره ۱، شماره ۲، صص ۱۴۳-۱۶۵.

۱۶- واضحی شکردشت، بهرنگ؛ جوادنیا ریک، محمد (۱۴۰۳)، «کلاهبرداری اینترنتی و نحوه شکایت از کلاهبرداران اینترنتی»، هشتمین کنفرانس بین‌المللی مدیریت، علوم انسانی و رفتاری در ایران و جهان اسلام، صص ۱-۱۹.

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

۱۷- والایی، حمید (۱۴۰۱)، «بررسی حقوقی و ساختاری جرم فیشینگ در حوزه ارزهای دیجیتال»، سومین کنفرانس ملی پدافند سایبری، صص ۱-۲۱.

۱۸- یوسفی‌نژاد، محمدرضا؛ پیمان، محمدجواد (۱۴۰۳)، «تحلیل حقوقی و کیفری جرایم مرتبط با کلاهبرداری سایبری و پولشویی دیجیتال»، ششمین کنفرانس بین‌المللی و هفتمین کنفرانس ملی حقوق و علوم سیاسی، صص ۱-۲۱.