فصلنامه علمی- پژوهشی علوم اجتماعی، دوره ۱۱، ویژه‌نامه پیشگیری از جرم و حقوق، زمستان ۱۳۹۶

تاریخ دریافت: ۱۳۹۶/۱۱/۲۴ تاریخ پذیرش: ۱۳۹۶/۱۲/۱۷

صص ۵۳۱ - ۵۴۵

واکاوی ارکان جرم کلاهبرداری سایبری در سیاست کیفری ایران*

صالح اوجاقلو[۱]، محمدرضا زندی[۲]**

۱- دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران، ایران

۲- استادیار گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران

چکیده

کلاهبرداری سایبری به لحاظ خلاقیت مرتکب آن و سهولت ارتکاب مهمترین و شایع‌ترین جرم اقتصادی فضای سایبر محسوب می‌شود؛ هر چند به ظاهر در ارتکاب این جرم، رایانه و فضای سایبر در حد وسیله جرم ظاهر می‌شود. اما رایانه و فضای سایبر، کلاهبرداری را توأم با کیفیت و شرایط غیر قابل انکاری می‌کند که مقنن ناگزیر به شناسایی جرم جدید در کنار کلاهبرداری سنتی شده است؛ ماده ۶۷ قانون تجارت الکترونیکی و ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات؛ رکن قانونی جرم کلاهبرداری سایبری را تشکیل می‌دهند و رفتار مجرمانه در رکن مادی این جرایم شامل ورود، تغییر، محو و مختل کردن و دست-کاری غیرمجاز سیستم خواهد بود و موضوع آن‌ها مال متعلق به دیگری و نتیجه آن‌ها محروم ساختن مالباخته از مال خود است؛ از طرفی کلاهبرداری سایبری جرمی عمدی، آنی و مقید است و برای تحقق آن وجود سوء نیت عام (یعنی عمد در ارتکاب یکی از اعمال فیزیکی مذکور در ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات) و سوء نیت خاص (یعنی قصد تحصیل وجه، مال، منفعت، خدمات یا امتیازات مالی) هم برای تحقق عنصر روانی جرم کلاهبرداری سایبری ضروری است؛ کلاهبرداری سایبری جزء جرایمی می‌باشد که نظر بسیاری از بزهکاران را به خود جلب نموده است و نیاز به برخورد قاطع از سوی مراجع ذیربط دارد؛ کلاهبرداران با ارسال ایمیل و پیامک به اشخاص مختلف، آن‌ها را به انحای مختلف به پای دستگاه‌های خودپرداز (ATM) بانک‌ها می‌کشانند و اقدام به کلاهبرداری می‌نمایند و با وجود انواع کلاهبرداری اینترنتی مانند فیشینگ، ارسال ایمیل یا نفوذ به ایمیل باکس افراد و ارائه شماره حساب‌های جعلی در معاملات و استفاده از اسکیمرها در دستگاه‌های خودپرداز بانک‌ها برای سوءاستفاده از کارت‌های عابر بانک و با وجود افزایش این نوع کلاهبرداری‌ها، سیستم‌های ایمنی و حفاظتی بانک‌ها بسیار ضعیف عمل می‌کنند؛ از این رو با استاندارسازی و تجهیز وسائل ارتباطی می‌توان از این قبیل جرایم پیشگیری کرد.

واژگان کلیدی: کلاهبرداری سایبری، دستگاه‌های خودپرداز(ATM) ، فیشینگ، ارکان جرم.

---

* این مقاله مستخرج از رساله دکتری با عنوان «کلاهبرداری سایبری در پرتو رویه قضایی» در دانشگاه آزاد اسلامی واحد تهران جنوب است.

** نویسنده مسئول: Dr.z.cyber@gmail.com

مقدمه

کلاهبرداری از جمله جرایم علیه اموال است که تا پیش از این کلاهبردار با ریختن طرح و نقشه‌ای ماهرانه، شخص یا اشخاصی را فریب می‌داد و در نهایت، قربانی که گول مانورهای متقلبانه مرتکب را خورده بود، مالش را با رضایت خویش به وی تسلیم می‌کرد؛ اما در دنیای امروز با پیشرفت فناوری و ورود رایانه و اینترنت به زندگی بشری جرم کلاهبرداری نیز دست خوش تغییراتی گردیده و در دنیای مجازی بدون آنکه نیاز به فریب شخص یا اشخاصی باشد با وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم می‌تواند وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند. (دانشخواه، ۱۳۹۲: ۱۹)

با این اوصاف فضای سایبر دنیای دیگری است که در برابر دنیای فیزیکی قد برافراشته است؛ آنچه که فضای سایبر را دنیای جدید معرفی کرده، امکانات و قابلیت‌های متفاوت آن است و الا این فضا از همان واژگان دنیایی که در آن زندگی می‌کنیم مانند: شاهراه اطلاعات، کتابخانه مجازی، جریان اطلاعات و دهکده جهانی شکل گرفته است؛ در هر حال جرایم سایبری در فضایی ارتکاب می‌یابند که به قدری تبادل اطلاعات در آن سریع است که مراحل سنتی ارتکاب جرم یعنی اراده و قصد، تدارک مقدمات و شروع به اجرا به چشم نمی‌آید و مسیرهای اطلاعاتی‌اش به قدری زیادند که نتیجه جرم در یک لحظه در مکان‌های گوناگونی حاصل می‌شود.

اصطلاح «جرم سایبری» واژه‌ای به روز، رایج و مناسب است که می‌توان به جای جرم رایانه‌ای به کار برد، زیرا جرم سایبری شامل کلیه جرائمی می‌شود که به نوعی در آن‌ها رایانه ایفای نقش می‌کند و از آن جایی که قوام و دوام اینترنتی و فضای سایبر به وجود رایانه است و سیستم‌های ارتباطی و مخابراتی نیز با رایانه فعالیت می‌کنند و شبکه‌های محلی و منطقه‌ای نیز از رایانه شکل گرفته‌اند و از طرف دیگر نرم افزارهای رایانه‌ای جزیی از رایانه تلقی می‌شوند، جرم سایبری شامل همه این عناوین می‌شود. (عالی‌پور، ۱۳۹۲: ۶۳) البته جرم سایبری از حیث دایره شمول عنان گسیخته بوده و مفهومی عام‌تر از میزانی که مدنظر ماست، دارد. بنابراین جرم سایبری را باید منصرف به عملکرد رایانه، نرم افزارهای رایانه‌ای و داده و سیستم رایانه‌ای کرد و گرنه هیأت رایانه و لوازم سخت افزاری آن به تنهایی و بدون توجه به عملکرد و قابلیت آن‌ها مشمول مقررات و مباحث سنتی حقوق کیفری خواهد بود.

با پایان یافتن دهه هفتاد و با تشکیل پرونده‌های عدیده‌ای که بیشتر پیرامون دو دسته از بزه‌ها بود؛ یعنی نقض حق تالیف و ترجمه و بزه‌های مطبوعاتی از طریق واسطه‌های الکترونیکی، قانونگذار ایران، مسیر قانونگذاری در فضای سایبر را با دو قانون حمایت از نرم افزارهای رایانه‌ای و قانون اصلاح قانون مطبوعات هر دو مصوب ۱۳۷۹ یافت. پس از آن قانون‌های دیگری مانند قانون تجارت الکترونیکی و قانون مجازات بزه‌های نیروهای مسلح هر دو مصوب ۱۳۸۲ و نیز قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز می‌کنند مصوب ۱۳۸۶ تصویب شدند؛ و بالاخره با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ و قانون آیین دادرسی کیفری مصوب ۱۳۹۲ و الحاقات آن در بخش دهم در تاریخ ۱۳۹۳/۷/۸ مقنن در زمینه فضای سایبری مقرره تدوین کرده است.

۱. مفاهیم مقدماتی:

در این قسمت نگارندگان به تبیین مفاهیم کلیدی مقاله خواهند پرداخت.

۱-۱. مفهوم جرم سایبری

با آن‌که جرایم سایبری را باید با ویژگی‌ها یا نمونه‌هایش شناخت ولی از هنگامی که این پدیده شناسانده شد، تعریف‌های چندی از آن پیشنهاد شد. دلیل اصلی تلاش برای ارایه تعریف از جرم سایبری، بیشتر تفاوت مکانی‌اش با جرم معمولی است که چون در بستر فضای سایبر ارتکاب می‌یابد، بیش‌تر مواقع نه در اندازه قسمی کوچک از بزه‌ها، بلکه دسته‌ای بزرگ از بزه‌هایی که در عوض بزه‌های معمولی قرار می‌گیرد، معرفی می‌شود. از این رو تلاش‌ها برای جداسازی جرم سایبری از بزه‌های دیگر که در اثر پیشرفت و فناوری مطرح گردیده مانند بزه‌های مرتبط با هواپیما، بزه‌های مطبوعاتی، بزه‌های مرتبط با بهداشت، بزه‌های مرتبط با

صنایع و کارخانجات، بسیار بیشتر بوده که در زیر، هم از دید نهادها و سازمان‌ها اعم از داخلی و بین‌المللی و هم از نگاه اندیشمندان و حقوق‌دانان به برخی از تعاریف مربوط به جرم سایبری اشاره می‌کنیم:

جرم سایبری عبارت است از هرگونه تخلف از قانون کیفری که دانش فناوری رایانه‌ای را در ارتکاب، تحقیق و پیگرد شامل شود (Keyser, ۲۰۰۳,p۲۹۰) موسسه ملی عدالت در گزارش خود زیر عنوان «واحدهای جرم سایبری اختصاصی»[۱] جرم سایبری را هر رفتار غیرقانونی می‌داند که دانش فناوری رایانه‌ای برای ارتکاب جرم به کار گرفته می‌شود. در این گزارش قید شده که فضای سایبر نسبت به جرم می‌تواند دو حالت داشته‌باشد؛ حالت فعال که رایانه برای نفوذ در فایل‌ها و ربایش پول و رفتارهای غیرقانونی از این دست به کار گرفته می‌شود و حالت انفعال که رایانه نقش تسهیل کننده یا راهنما برای خریداران یا کالاها به ویژه در پرونده‌های قاچاق مواد مخدر دارد (Edgar, ۲۰۰۳, p۱۶۷).

بر پایه قانون مجازات اسلامی فصل جرایم رایانه‌ای و قانون آیین دادرسی کیفری می‌توان گفت که جرم سایبری در حقوق کیفری ایران به جرمی گفته می‌شود که یا بر ضد داده یا رایانه رخ دهد یا با دستاویز رایانه یا فضای سایبر رخ دهد. با این حال گستره بزه سایبری از جهت ابزار و وسیله بودن ناروشن است.

دلیل گوناگونی عناوین جایگزین جرم سایبری، در تنوع موضوع و بستر آن است؛ ماهیت و ویژگی‌های بستر و لوازم فناوری اطلاعات آن قدر پیچیده و مرکب است، که با هر سنجه یا مشخصه‌ای می‌توان این فضا را نامگذاری کرد. فضای سایبر یا مجازی، فضای دیجیتال، فضای الکترونیکی، اینترنت و اطلاعات، یا بستر و مکان جرم سایبری هستند؛ یا موضوع آن که بر حسب گزینش آن‌ها عناوینی چون جرم سایبری، جرم دیجیتالی، جرم الکترونیکی، جرم اینترنتی و جرم اطلاعاتی مطرح خواهد شد و همه این تعابیر از زاویه‌ای که بر اساس آن نامگذاری شده‌اند، صحیح می‌باشد و در میان واژگان گفته‌شده اصطلاح «جرم سایبری» واژه‌ای به روز، رایج و مناسب است که می‌توان به جای جرم رایانه‌ای به کار برد، زیرا جرم سایبری شامل کلیه جرائمی می‌شود که به نوعی در آن‌ها رایانه ایفای نقش می‌کند و از آن جایی که قوام و دوام اینترنتی و فضای سایبر به وجود رایانه است و سیستم‌های ارتباطی و مخابراتی نیز با رایانه فعالیت می‌کنند و شبکه‌های محلی و منطقه‌ای نیز از رایانه شکل گرفته‌اند و از طرف دیگر نرم‌افزارهای رایانه‌ای جزیی از رایانه تلقی می‌شوند، جرم سایبری شامل همه این عناوین می‌شود. البته جرم سایبری از حیث دایره شمول، عنان گسیخته بوده و مفهومی عام‌تر از میزانی که مدنظر ماست، دارد. بنابراین جرم سایبری را باید منصرف به عملکرد رایانه، نرم افزارهای رایانه‌ای و داده و سیستم رایانه‌ای کرد و گرنه هیأت رایانه و لوازم سخت‌افزاری آن به تنهایی و بدون توجه به عملکرد و قابلیت آن‌ها مشمول مقررات و مباحث سنتی حقوق کیفری خواهد بود.

۱-۲. مفهوم کلاهبرداری سایبری

با پیشرفت تکنولوژی و فناوری اطلاعات جرمی به وجود آمده است که به آن کلاهبرداری سایبری می‌گویند؛ این کلاهبرداری یکی از جرائم ناشی از سوء استفاده از فناوری اطلاعات است. اما با توجه به ماده ۷۴۲ قانون مجازات اسلامی بخش تعزیرات در می‌یابیم که قانونگذار بدون تعریف دقیق جرم کلاهبرداری مرتبط با رایانه صرفاً به ذکر برخی از مصادیق آن اشاره نموده و بستر اقدام مجرمانه را سامانه‌های رایانه‌ای و مخابراتی دانسته است. نتیجه این پدیده مجرمانه به تعریف قانون نیز تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای مرتکب یا دیگری است.

کلاهبرداری سایبری به لحاظ خلاقیت مرتکب آن و سهولت ارتکاب مهمترین و شایع‌ترین جرم اقتصادی فضای مجازی رایانه محسوب می‌شود. هر چند به ظاهر در ارتکاب این جرم، رایانه در حد وسیله جرم ظاهر می‌شود. اما رایانه، کلاهبرداری را توأم با کیفیت و شرایط غیر قابل انکاری می‌کند که قانونگذاران ناگزیر به شناسایی جرم جدید در کنار کلاهبرداری سنتی هستند.

در تجارت مدرن (تجارت الکترونیک) نقل و انتقال پول نقد و خرید و فروش کالای تجاری، به سرعت جای خود را به انتقال سپرده‌ها از طریق وارد کردن تغییر، محو و موقوف سازی و خروجی سیستم

---

۱. Dedicated Cyber Crime Unites.

کامپیوتری (ماشین‌های تحویل دار خودکار بانک‌ها) معمول‌ترین شیوه ارتکاب کلاهبرداری سایبی می باشد؛ می‌دهد (باستانی، ۱۳۸۶: ۵۰).

شورای اروپا در فهرست حداقل خود مقرر می‌دارد:

کلاهبرداری کامپیوتری - وارد کردن، تغییر، امحاء یا ایجاد وقفه در داده‌های کامپیوتری یا برنامه‌های کامپیوتری یا دیگر مداخلات مربوط به پردازش داده‌ها که نتیجه پردازش داده‌ها را تحت تأثیر قرار می‌دهد، خواه موجب ضرر اقتصادی، خواه موجب از دست دادن اموال و تصرف آن اموال متعلق به غیر با قصد کسب منفعت وامتیار اقتصادی غیر قانونی برای خود یا دیگری شود (جاویدنیا، ۱۳۹۱: ۲۱۵).

کلاهبرداری از جمله جرایمی است علیه اموال و مالکیت اشخاص با این تفاوت که در کلاهبرداری سنتی فرد قربانی بر اثر مانورهای متقلبانه طرف مقابل فریب خورده و مال خویش را با میل و رغبت خود در اختیار کلاهبردار قرار می‌دهد؛ اما در جرم کلاهبرداری رایانه‌ای دیگر نیازی به مانورهای متقلبانه و فریب قربانی نیست بلکه بزه‌کار از راه تغییر و محو و ... در سیستم پردازش داده‌ها، اموال یا منفعت و... قربانی را به نفع خود یا دیگری تصاحب می‌کند؛ بنابراین در تعریف جرم کلاهبرداری سایبری می‌توان گفت: «هرگونه محو، ورود، پردازش، متوقف سازی، مداخله در سیستم و برنامه‌های رایانه‌ای به منظور بردن مال غیر و اخذ منافع مالی برای خود یا دیگری کلاهبرداری رایانه‌ای می‌باشد» (حسن بیگی، ۱۳۸۲: ۲۴۲).

۲. رکن قانونی جرم کلاهبرداری سایبری

بر پایهٔ اصل قانونی بودن جرم و مجازات، هر رفتاری زمانی جرم به شمار می‌آید که قانونگذار طی قاعده و حکمی آن را ممنوع کرده و مجازات (ضمانت اجرای کیفری) برای آن تعیین نموده باشد؛ به دیگر سخن، هر جرمی در گام نخست و پیش از هر چیز به موجب یک حکم قانونی، در عالم اعتبار به وجود می‌آید. از این حکم به عنوان «رکن/ عنصر قانونی» یاد می‌شود (منصورآبادی، ۱۳۹۴: ج۱، ۲۲۷)؛ با این اوصاف؛ رکن قانونی، آن مقرره (ماده و یا ماده‌هایِ) قانونی است که قانونگذار طی آن، دو ضابطه را برای ما بازگو کرده است: یکی «ضابطهٔ رفتار» مبنی بر این که «رفتار ممنوع و قابل مجازات چه رفتاری است؟» و دیگری «ضابطهٔ کیفر» مبنی بر این که «مجازات قابل اعمال نسبت به آن رفتار ممنوعه چه نوع و چه میزان مجازاتی است؟» رکن قانونی هر جرمی باید در بردارندهٔ این دو ضابطه باشد و بدون هر یک از این‌ها رکن قانونی ناتمام است.

جرم کلاهبرداری سایبری با بحث ورود دستورالعمل‌های اضافی شروع شده و در طول زمان، این جرم راه تکامل خود را پیموده است. چون در قوانین ناظر به کلاهبرداری ایران؛ لازم است انسان دیگری به طور مستقیم فریب بخورد و کلاهبرداری رایانه‌ای چنین لازمه‌هایی را دارا نیست؛ این رو، خلأ تقنینی پیش می-آید که در برخی کشورها با وضع قانون جرم کلاهبرداری سایبری خلأ موجود پر شده است.

به هر تقدیر می‌توان گفت مجوز قانونی مجازات کلاهبرداری سایبری در کنوانسیون جرایم سایبر: «ماده ۸- هر دولت عضو، تدابیر تقنینی و غیرتقنینی را تا آنجا که برای تصویب به عنوان جرایم کیفری تحت قوانین داخلی‌اش ضرورت دارد، اتخاذ خواهد کرد، زمانی که به طور عمدی و بدون حق، ایراد ضرر به اموال دیگی انجام پذیرد از طریق:

الف. هرگونه وارد کردن، تغییر دادن، حذف کردن یا متوقف ساختن داده‌های رایانه‌ای؛

ب. هرگونه ایجاد اختلال در عملکرد سیستم رایانه‌ای؛

با قصد تحصیل متقلبانه یا ناروا بدون حق یک منفعت اقتصادی برای خود یا دیگری».

قانون تجارت الکترونیکی در تاریخ ۱۳۸۲/۱۰/۱۷ به تصویب رسیده و کلاهبرداری در بسته تجارت الکترونیکی را جرم تلقی و برای آن مجازات تعیین گردیده است که ماده ۶۷ قانون مذکور مقرر می‌دارد: «هرگونه توسل به وسایل متقلبانه نظیر سوء استفاده و یا استفاده غیر مجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف (داده پیام)، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن‌ها شود و از این طریق برای خود یا دیگران وجوه، اموال یا امتیازات مالی تحصیل کند و

اموال دیگران را ببرد، مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تاسه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود».

بالاخره در تاریخ ۱۳۸۸/۳/۵ فصل جرایم رایانه‌ای[1] به بخش تعزیرات قانون مجازات اسلامی ملحق شد و رکن قانونی جرم کلاهبرداری سایبری را طی یک ماده قانونی پیش‌بینی نموده و دو ضابطه رفتار و کیفر را در ماده ۷۴۱ قانون مذکور تشکیل داده و مقرر نموده است: «هرکس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه، وجه یا مـال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد».

۳. رکن مادی جرم کلاهبرداری سایبری

دومین رکن جرم، رکن مادی است؛ رکن مادی، رکن واقعی، عینی و بیرونی جرم است؛ اصطلاح «رکن مادی»، ساخته و پرداخته حقوق کیفری است و هیچگاه در قوانین جزائی از آن استفاده نشده است (آقایی نیا، ۱۳۹۶: ۲۲)؛ منظور از آن یعنی پدیده‌ای که در دنیای دور و بر می‌توان آن را مشاهده کرد و نشان داد و یا دست کم پیامدهای آن را دید. رکن مادی، مجموعه‌ای از اجزا و شرط‌های مادی و بیرونی است که با وجود آن‌ها جرم در جهان بیرون پدیدار می‌شود و بر حسب نوع جرم‌ها، این اجزا و شرط‌ها متفاوت است. (منصورآبادی، ۱۳۹۴: ج۱، ۲۲۸). به عبارتی دیگر برای اینکه جرمی وجود خارجی پیدا کند پیدایش یک عنصر مادّی ضرورت دارد و شرط تحقق جرم آنست که قصد سوء ارتکاب عمل خاصی دست کم به مرحلهٔ فعلیّت برسد؛ بنابراین قصد باطنی، زمانی قابل مجازات است که تظاهر خارجی آن به صورت عملی، مغایر با اوامر و نواهی قانونگذار آشکار شود. و عامل درونی ذاتی از قبیل فکر و طرح و قصد تا زمانی که در همین مرحله بماند از تعقیب جزائی مصون می‌مانند. (اردبیلی، ۱۳۹۲: ج۱، ۳۰۲).

کلاهبرداری سایبری دارای عنصر خاص خود است و مصادیق آن در کلاهبرداری سنتی سابقه نداشته است و عنصر مادی کلاهبرداری سایبری با با جرایم سایبری دیگر متفاوت است؛ از این رو در این قسمت به بررسی ویژگی‌های بزهکاران و بزه‌دیدگان این نوع جرائم؛ رفتار مجرمانه؛ موضوع جرم و نتیجه جرائم کلاهبرداری سایبری خواهیم پرداخت.

۳-۱. ویژگی‌های بزهکاران جرایم کلاهبرداری سایبری

به نظر نگارندگان سطح مهارت بسته به نوع جرم در محیط سایبری متفاوت است؛ در کلاهبرداری‌های مرتبط با رایانه که با فریب و اغوای بزه‌دیده همراه می‌باشد مرتکب نیاز به مهارت بالایی در کار با رایانه ندارد بلکه زیرکی او است که قربانیان را با شگرد خاصی به انجام کار مورد نظرش ترغیب می‌نماید؛ به گونه‌ای که این خود قربانیان هستند که گاه به آگاهی و رضایت کامل هر چند ظاهری، مال خود را در اختیار بزهکار قرار می‌دهد. اما در کلاهبرداری مصرح در ماده۷۴۱ قانون مجازات اسلامی بخش تعزیرات که بدون دخالت مجنی‌علیه و فریب او عملیات دستکاری محو، ایجاد و سایر مصادیق بر شمرده در قانون انجام می‌گیرد به مهارت بالایی نیاز است و قابل ذکر است این نوع کلاهبرداری بیشتر توسط کارمندان انجام می‌گیرد (شیرزاد، ۱۳۸۸: ۹۰).

در واقع عصر دیجیتالی شبکه‌ای شده نه تنها بزهکاران را به شیوه‌های جدید، جرایم ارتکاب جرم مجهز کرده، بلکه افرادی که پیشتر منحرف نبودند را نیز توانمند و برای آن‌ها رفتارهای مجرمانه جدیدی را ترسیم کرده است (pease, ۲۰۰۱, P۲۸).

اصولاً مرتکبین جرایم کلاهبرداری سایبری دو دسته‌اند.

---

۱. «قانون جرایم رایانه‌ای» در ۵۶ ماده و در تاریخ ۱۳۸۸/۳/۵ به تصویب مجلس شورای اسلامی رسیده و در روزنامه رسمی ۱۳۸۸/۴/۱۷ منتشر شد و شماره مواد ۱ تا ۵۴ این قانون به عنوان مواد ۷۲۹ تا ۷۲۸ قانون مجازات اسلامی بخش تعزیرات با عنوان فصل جرایم رایانه‌ای منظور و شماره ماده ۷۲۹ بخش تعزیرات به شماره ۷۸۳ اصلاح گردید.

۱. مجرمانی که به دنبال منافع خود هستند.

۲. متخصصان و اهل فن و تحقیق که به دلایل گوناگون مثل ارضای حس کنجکاوی و یا رسیدن به یک نتیجه علمی و یا سرگرمی و ... مرتکب این جرایم می‌شوند. طبیعی است که اقدامات این عده علیرغم اینکه غیرمجاز و غیرقانونی و به تعبیر دیگر جرم تلقی می‌شود، ممکن است سبب توسعه و تکامل در امری خاص گردد.

بنابراین هرچند غالباً مجرمان سایبری از استعداد نسبتاً بالایی برخوردار هستند؛ اما کلاهبرداران سایبری اشخاصی هستند که زیرکی فریب دادن دیگران را با دانش رایانه‌ای و سایبری در آمیخته‌اند و بدون تردید در زمره مجرمین یقه سفید[1] قرار می‌گیرند که به میزان خطرناکی و استعداد جنایی بالا، قدرت انطباق اجتماعی قابل توجهی دارند و به همین ترتیب علیرغم این‌که توجهات دیگران را نسبت به اعمال غیرقانونی خود بر نمی انگیزند به راحتی و به کرات رایانه و اینترنت را جولانگاه مانورهای متقلبانه خود می‌سازند (سالاری شهر بابکی، ۱۳۸۶: ۲۵۳).

نکته قابل ذکر این است که بزه کلاهبرداری ناظر به افعال انسان است؛ اما لازم نیست همواره انسان خود مستقیماً مباشر عمل باشد بلکه ممکن است از طریق ویروس و برنامه‌های امثال آن مرتکب شود؛ ؛ اما نکته قابل ذکر در خصوص فاعل جرم در کلاهبرداری سایبری استفاده قانونگذار از عبارت «هرکس» می‌باشد به گونه‌ای که با استناد مواد ۶۷ قانون تجارت الکترونیکی در کلاهبرداری مرتکب جرم هر کسی می‌تواند باشد. همانگونه که در صدر مواد ۷۴۰ و ۷۴۱ قانون مجازات اسلامی بخش تعزیرات می‌خوانیم: «هر کس به طور غیر مجاز...»، اشاره این مواد به واژه «هرکس» به جای «هرشخص»، نظر قانونگذار را به انجام این فعل توسط یک شخص حقیقی به ذهن متبادر می‌سازد؛ بنابراین بهتر بود که قانونگذار از واژه «هر شخص» استفاده می-کرد تا اشخاص حقوقی را هم در بر می‌گرفت.

۳-۲. ویژگی‌های بزه‌دیدگان جرایم کلاهبرداری سایبری

کلاهبرداری سایبری در یک محیط سایبری تحقق می‌یابد؛ بنابراین به طور بالقوه این امکان وجود دارد که تمام این محیط مورد تهاجم واقع شود (شیرزاد، ۱۳۸۸: ۹۵)؛ از این رو کلاهبرداری سایبری چون در دنیای مجازی رایانه و سایبر با امکانات بی‌شماری تحقق می‌یابد فقط علیه انسان نیست بلکه غالباً علیه سیستم رایانه‌ای و نرم افزارهای آن است.

در کلاهبرداری رایانه‌ای اولیه، فرد مرتکب با دادن دستورالعمل‌های اضافی، وجوه دیگران را به خود اختصاص می‌داد بدون اینکه آنان را بفریبد. در شکل جدید و اخیر این شکل از بزه‌دیده به ماشین تغییر یافته است؛ که بیشترین مورد تحقق آن در جرایم تجارت الکترونیک و جرایم بانکداری الکترونیک است. مرتکب بدون آنکه بزه‌دیده را ببیند، وجوه و اموال دیگران را به خود اختصاص می‌دهد (زندی، ۱۳۹۳: ۴۵).

تعداد بزه‌دیدگان با توجه به اینکه هر لحظه امکان دسترسی بیشتر به شبکه جهانی اینترنت برای افراد از طیف‌های مختلف فراهم می‌شود و قابلیت بزهکاری و قابلیت بزه‌دیدگی به نحو چشم‌گیری افزایش خواهد یافت؛ تا دیروز شاید فقط مراکز حساس امنیتی و شرکت‌های مهم تجاری در معرض وقوع جرایم کلاهبرداری رایانه‌ای واقع می‌شدند؛ اما امروزه؛ که حتی برخی از افراد غیرحرفه‌ای هم پایگاه اینترنتی خاص خود را دارند و برخی فعالیت‌های تجاری نه چندان بزرگ هم از طریق اینترنت انجام می‌شود، طیف گسترده‌تری از افراد در معرض وقوع جرایم کلاهبرداری سایبری قرار گرفته‌اند؛ این امر به ویژه در زمینه دستگاه‌های عابر بانک، و دیگر شبکه‌های مربوط به مصرف‌کنندگان و همچنین در زمینه کلاهبرداری علیه کاربران رایانه‌ای شخصی مصداق دارد (زیبر،۱۳۹۰: ۷۴).

---

۱. نظریه «مجرمین یقه سفید» توسط ادوین ساترلند آمریکایی که در سال ۱۹۴۰ میلادی ارائه شده و امروزه در قالب جرایم سایبری در جدیدترین شکل خود ظهور و بروز پیدا کرده است (سلامی، ۱۳۹۴: ۲۱).

در نگاه اولیه مجنی‌علیه کلاهبرداری در محیط رایانه، یک دستگاه می‌تواند باشد؛ اما آیا اساساً یک ماشین یا دستگاه الکترونیکی قابلیت فریب خوردن[۱] یا غافلگیری در ربودن را دارد یا اینکه تحقق این امور مستلزم وجود یک انسان است؛ در کلاهبرداری سایبری مرتکب از طریق یک سیستم رایانه‌ای یا ماشین الکترونیکی اقدام به بردن مال دیگری می‌نماید. هرچند عامل انسانی در جرم در ظاهر دخالت ندارد؛ اما در نهایت این انسان است که بزه‌دیده قرار گرفته هر چند مرتکب به واسطه رایانه اقدام به ارتکاب جرم می‌نماید اما مال افراد برده می‌شود (جاویدنیا، ۱۳۹۱: ۱۳۲).

اصولاً کلاهبرداری‌های اینترنتی نسبت به موسسات و شرکت‌های بزرگ مخصوصاً موسسات مالی و اعتباری نظیر بانک‌ها واقع می‌گردد؛ البته ذکر این نکته به این معنی نمی‌باشد که افراد عادی قربانی کلاهبرداری واقع نمی‌شوند؛ شرکت‌های بزرگ به دلیل دارا بودن سرمایه بیشتر به میزان افزون‌تری در معرض قربانی کلاهبرداری می‌باشند.

یکی از مشکلاتی که در این جرایم وجود دارد این است که این دسته از بزه‌دیدگان تمایلی به اعلام جرم نداشته و در نتیجه رقم سیاه این جرایم بالاست و این بی‌میلی در گزارش جرم می تواند دلایلی داشته باشد. برخی به دلیل هراس از تبلیغات سوء رسوایی و یا از دست دادن حسن شهرت خود تمایلی به فاش ساختن اطلاعات ندارند. دیگر بزه‌دیدگان نیز از سلب اعتماد سرمایه‌گذاران و یا عامه مردم و پیامدهای اقتصادی ناشی از آن واهمه دارند «به ویژه در کلاهبرداری که برخلاف سایر جرایم علیه اموال، انواع آن معمولاً تحت پوشش بیمه قرار نمی‌گیرند و در نتیجه منفعتی برای موسسه در گزارش کردن آن‌ها متصور نیست» (خانلر تبار، ۱۳۸۹: ۳۸).

بزه‌دیدگان کلاهبرداری سایبری در واقع قربانیان پیشرفت تکنولوژی هستند؛ اما نکته قابل توجه در این بین آن است که بسیاری از بزه‌دیدگان جرایم سایبری استعدادی قابل توجه برای قربانی شدن[۱] بروز می‌دهند و به راحتی طعمه بزهکاران سایبری می‌شوند برخی کلاهبرداریهای اینترنتی ناشی از کسب اطلاعات به روش‌های بسیار ساده و سوء استفاده از عکس‌ها و اسرار شخصی نمونه‌هایی از این موضوع می باشند؛ به نظر نگارندگان قربانی این جرایم همیشه بیگناه نیستند و چه بسا خودشان ناخواسته آغازگر یک کلاهبرداری سایبری می‌باشند.

ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و ... مواردی است که قربانی کلاهبرداری را در قربانی شدنش مساعدت می‌کند. نمونه بارز این موارد کلاهبرداری از طریق فریب و ارسال پیامک مبنی بر برنده شدن است که بزه‌دیده با باور غلط و فقدان اطلاعات کافی و بی احتیاطی به خواست مرتکب به پای عابر بانک کشیده می‌شود و با توجه به راهنمایی‌های بزه‌کار درخواست‌های وی را انجام می‌دهد و این گونه با عدم دقت با دست خود، مبالغی از حسابش به حساب فرد کلاهبردار منتقل می‌نماید. همچنین است بزه‌دیدگان با بی‌احتیاطی و عدم دقت در محافظت داده‌هایشان زمینه کلاهبرداری‌ها را فراهم می‌نمایند. اطلاعات خود را در اختیار دیگران از جمله کافی نت‌ها قرار می‌دهند و مرتکبین با در اختیار داشتن اطلاعات وجوه آن‌ها را از طریق اینترنت به شیوه‌های مختلف از جمله خرید شارژ تلفن همراه یا انتقال وجه یا سایر خریدهای اینترنتی بدست می‌آورند.

---

۱. یکی از اختلافات اساسی محاکم در دستکاری شخص در برنامه‌های رایانه و انتقال پول به حساب خودش؛ عنصر فریفتن است؛ برخی از قضات ارتکاب جرم کلاهبرداری سایبری را تنها علیه یک انسان قابل تصور می‌دانند و معتقدند کسی نمی‌تواند کامپیوتر و دستگاه *ATM* را فریب دهد و این موارد را مشمول ماده ۲ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ می‌دانند ولی برخی از قضات با توجه به ماده ۶۷ قانون تجارت الکترونیکی که علاوه بر فریب دیگران، به گمراه سازی سیستم-های پردازش خودکار اشاره کرده؛ این رفتار را از کلاهبرداری سنتی متفاوت و مشمول کلاهبرداری سایبری می‌دانند.

۱. Victimation.

۳-۳. مصادیق؛ شیوه‌ها و وسیله رفتار مجرمانه در کلاهبرداری سایبری

استفاده از واژه «رفتار» در ماده ۲ قانون مجازات اسلامی مصوب ۱۳۹۲، ابداع مقبولی است که نیاز به ذکر مصادیق را مرتفع میسازد ولی متأسفانه قانونگذار به واژه رفتار اکتفا نکرده و از فعل یا ترک فعل به عنوان مصادیق حصری آن نام برده که صحیح به نظر نمی‌رسد، زیرا از موارد دیگری مانند داشتن، نگهداری و یا حتی مشاهده کردن می‌توان نام برد که رفتار مجرمانه بعضی از جرایم هستند (آقایی نیا، ۱۳۹۶: ۳۱).

۳-۳-۱. مصادیق رفتار مجرمانه در کلاهبرداری سایبری

کلاهبرداری کامپیوتری نیز مستلزم فعل مادی مثبت است و مشتمل بر موارد ذیل است:

۳-۳-۱-۱. ورود

ورود؛ شامل وارد کردن داده‌ها در کامپیوترها است که آن ممکن است موجب تأثیر بر داده پردازی موجود یا سبب شروع آن شود؛ کلاهبرداری سایبری با سوء استفاده از ورودی، از معمول‌ترین نوع کلاهبرداری است، زیرا انجام آن آسان و کشف آن دشوار است؛ این شیوه که به «حقه بازی اطلاعاتی» معروف است به دانش سطح بالای رایانه‌ای نیاز ندارد و هر فردی که به عملیات پردازش داده در مرحله ورودی دسترسی داشته باشد می‌تواند مرتکب آن شود (خداقلی، ۱۳۸۳: ۷۹).

۳-۳-۱-۲. تغییر

تغییر باید غیرقانونی یعنی بدون حق انجام شود؛ به عنوان نمونه در پرونده‌ای در آلمان غربی در سال ۱۹۸۴ یک برنامه نویس و یک کارمند بورس، برنامه و پایگاه‌های داده کامپیوتری که لوازم یدکی را به گونه-ای تغییر دادند که لوازم یدکی بدست آمده توسط آن‌ها، در صورت حساب به قیمتی بسیار کمتر از قیمت واقعی ثبت شد و خسارات وارده در این پرونده بالغ ۳۱۰۰۰ مارک آلمان بود (زیبر،۱۳۹۰: ۲۵).

۳-۳-۱-۳. محو

شامل حرکت و انتقال داده‌ها از محل اصلی مثلاً نوارهای ذخیره سازی مغناطیسی می‌شود؛ از این رو مصداق دیگری از رفتارهای مجرمانه این بزه، «محو» است؛ به معنای از بین رفتن یا شامل حرکت و انتقال داده‌ها از محل اصلی مثلاً نوارهای ذخیره مغناطیسی می‌باشد؛ باید این اعمال منجر به کسب منفعت یا مالی اقتصادی و یا تصرف اموال دیگری شود و نیز قصد مرتکب باید کسب چنین منفعت یا مالی باشد؛ کلاهبرداری با محور داده پیام به این ترتیب میسر است که مثلاً کارمندی با حذف سابقه‌ی دریافت حقوق خود از سیستم حسابداری شرکت، معادل حقوق خود را مجددا دریافت نماید و با این عمل منفعت مالی برای مرتکب حاصل گردیده است؛ یا حذف یا کسر بدیهی‌های شرکت یا افراد می‌باشد؛ به عنوان نمونه پاک کردن بدهی جرایم راهنمایی و رانندگی، اقساط وام و یا هزینه‌های خدمات عمومی از جمله آب، برق، تلفن، گاز و غیره از جمله کلاهبرداری‌های سایبری می‌باشد (سلامی، ۱۳۹۴: ۱۳۹).

۳-۳-۱-۴. مختل و دستکاری سیستم

یک عنوان کلی است که شامل اعمال و افعال زیادی می شود؛ عنوان کلی اختلال در سیستم رایانه‌ای است که شامل اعمالی نظیر: انواع دستکاری سخت افزارها، جلوگیری از خروج داده‌ها به صورت پرینت و تأثیر گذاشتن به ثبت و ذخیره یا جریان داده‌ها یا توانایی اجرای برنامه‌ها می‌باشد؛ به این ترتیب از آنجا که کلاهبرداری رایانه‌ای داده‌ها ذخیره شده در سیستم‌های پردازش داده دیگر توسط انسان‌ها مبادله نمی‌شود و این عمل را دستگاه انجام می‌دهد (زیبر،۱۳۹۰: ۳۴).

در مورد دستکاری برنامه و تغییر داده‌های مهم، تکرار مداوم عمل حالت خودکار به خود می‌گیرد؛ چرا که هر زمان که برنامه یا داده‌های مهم به (عنوان مثال، داده‌های مربوط به دستمزد ناخالص) مورد استفاده قرار گیرد، رایانه بدون نیاز به دخالت مجرم و به طور خودکار دست کاری را تکرار می‌کند (زیبر،۱۳۹۰: ۳۴).

نحوه دیگر رفتار کلاهبرداری رایانه‌ای را می‌توان به دستکاری عابر بانک‌ها دانست که امروزه این دستکاری‌ها از بزرگ‌ترین مشکلات جرایم سایبری تلقی می‌شود؛ تحول مشابهی نیز اکنون در مورد دستگاه-های الکترونیکی بسیار کارامد فروش کالا در حال وقوع است؛ بیشتر روش‌های پیچیده دستکاری کارت‌های

عابر بانک از این واقعیت که قسمت مغناطیسی لبه بیشتر کارت‌های عابر بانک را بعینه می‌توان کپی کرد و تغییر داد استفاده می‌کنند.

۳-۳-۲. شیوه‌های رفتار مجرمانه در کلاهبرداری سایبری

۳-۳-۲-۱. کلاهبرداری فیشینگ[۱]

کلاهبرداری فیشینگ با افزایش کاربری‌های اینترنت؛ در حال افزایش است؛ که روشی نوین در نفوذ به اطلاعات محرمانه و شخصی افراد محسوب می‌شود و در عصر حاضر توانسته خسارات گرانباری را بر کاربران اینترنتی وارد کند؛ این روش مجازی کلاهبرداری که تا حدی اختیار کاربران را برای استفاده از روش‌های پرداخت الکترونیکی و مبادلات مجازی سلب می‌کند، خودش را در پشت قالبی از سایت‌های معتبر پنهان می‌سازد و با ظاهری فریبنده که کاربر هم به سختی می‌تواند متوجه آن شود، اطلاعات شخصی و محرمانه را از کاربران دریافت می‌کند و به سرقت اطلاعات آن‌ها دست می‌زند؛ عمل فیشینگ به صورت گسترده از طریق پیامک و ایمیل افراد صورت می‌گیرد و آن‌ها را به پر کردن فرم‌هایی تشویق می‌کند که از طریق آن می‌توان به اطلاعات محرمانه افراد دسترسی پیدا کند.

در مورد چگونگی کارکرد فیشینگ باید گفت: «در یک سناریوی مشترک، کلاهبرداران فیشینگ یک ایمیل دسته جمعی ارسال خواهند کرد که به نظر می‌رسد این پست‌های الکترونیکی از یک شرکت مشروع رسیده است و معمولاً یک درخواست برای اطلاعات حساس است که گاهی اوقات گیرنده را به یک صفحه جعلی هدایت می‌کند؛ صفحه وب مانند پست الکترونیکی معتبر به نظر می‌رسد و در برخی موارد آدرس آن پوشانده شده است، بنابراین حتی به نظر می‌رسد آدرس وب سایت واقعی است و کلاهبرداران فیشینگ کار خود را با استفاده از ویروس آغاز می‌کنند، و گاه ایمیل‌ها با مهر بانکی وارد جعبه نامه کاربران می‌شود و از آن‌ها می‌خواهد تا مشخصات کارت‌های اعتباری خود را به دلایل متفاوتی عوض کرده و مجددا برای ارسال کننده بفرستند به این طریق با اطلاعات قربانی، از آن سوء استفاده می‌کنند (سلامی، ۱۳۹۴: ۱۵۲-۱۵۳).

۳-۳-۲-۲. سوء استفاده از دستگاه‌های عابر بانک

امروز با استفاده وسیع از سخت افزار و نرم افزار، اطلاعات الکترونیکی کذب به صورتی که روی لبه‌های مغناطیسی کارت‌های عابر بانک و اعتبار ثبت شده، مورد سوء استفاده قرار می‌گیرد؛ مرتکبین این نوع کلاهبرداری، شماره‌های محرمانه ضروری برای سوء استفاده از کارت‌ها را اغلب از طریق تجاوز به مکالمه تلفنی، از طریق تدارک صفحه کلیدهای جعلی، نفوذ کردن یا مختل نمودن خطوط مخابرات، داده‌ها را بدست می‌آورند.

در خصوص عابر بانک‌ها هم روش‌های خاصی از دست کاری وجود دارد؛ نمونه سوء استفاده از دستگاه-های عابر بانک اینگونه است که مجرمین یک کارت خالی کپی شده را وارد عابربانک می‌کنند؛ سپس یک ابزار کمکی ویژه را به دستگاه کارت خوان متصل می‌کنند؛ وقتی مشتری کارت خود را وارد قسمت کمکی می‌نمایند، کارت خالی فوق الذکر که قبلاً به دستگاه عابر بانک وارد شده است به قسمت کارت خوان عابر بانک وارد می‌شود؛ از آن جایی که شماره‌های رمز مشتری و شماره کارت خالی تطابق ندارد (با توجه به اقدامات امنیتی که در همه عابر بانک‌ها در نظر گرفته شده در صورتی که کاربر ۳ بار متوالی شماره رمز را اشتباه تایپ کند، کارت او به داخل دستگاه کشیده و از کارت محروم می‌شود)؛ پس از آن که کاربر این عمل را چندین بار تکرار می‌کند، عابر بانک کارت خالی را به داخل خود می‌کشد و مشتری که فکر می‌کند کارت خودش به داخل کشیده شده آن جا را ترک می‌نماید؛ در این زمان مجرم‌ها می‌آیند و کارت مشتری را از خشاب تقلبی بیرون می‌کشند؛ آن‌ها برای فهمیدن شماره سری مشتری هم راه حلی یافته و از قبل صفحه کلید را به روغن آغشته می‌نمایند، بدین ترتیب زمانی که کاربر شماره ۴ رقمی خود را وارد می‌کرد مشخص بود که کدام کلیدها دست خورده‌اند؛ پس مرتکب بین ۲۴ گزینه ۴ رقمی پیش رو دارند و با آزمایش تک تک آن‌ها شماره صحیح را پیدا می‌نمایند (زیبر،۱۳۹۰: ۳۲).

---

۱. Phishing.

۳-۳-۳. وسیله رفتار مجرمانه در کلاهبرداری سایبری

در حالی که در کلاهبرداری سنتی نوع وسیله در ماهیت جرم تأثیر دارد و به کار بردن وسیله متقلبانه، شرط تحقق رکن مادی جرم است و حقوقدانان نیز با اتفاق بر این موضوع، آن را شرط اساسی تحقق جرم می‌دانند؛ توسل به وسایل متقلبانه در کلاهبرداری در واقع روش خاصی است که برای استفاده از حیله و تقلب به کار می‌رود و حاکی از آن است که مرتکب، قصد اغفال طرف را داشته است (میرمحمدصادقی و شایگان، ۱۳۸۹: ۱۰۲).

وسایل متقلبانه از لحاظ قانونی در یک دسته بندی کلی به دو نوع وسایل متقلبانه معین و غیرمعین تقسیم می‌شوند (سالاری شهر بابکی، ۱۳۸۶: ۲۵۰)؛ بر این اساس می‌توان وقوع کلاهبرداری را از طریق وسایل الکترونیکی، مخابراتی، محاسباتی و رایانه‌ای و امثال آن و عموماً در فضای سایبر ممکن دانست؛ با این اوصاف امروزه در اثر افزایش تعداد عابر بانک ها و نیز «دستگاه های الکترونیکی بسیار کارآمد فروش کالا» مجهز به حسگرهای الکترونیکی، امکان ارتکاب گروه خاصی از جرایم سایبری از جمله کلاهبرداری سایبری فراهم آمده است که اصولاً به پول نقد ملموس، کالاها و خدمات ثبت شده به وسیله سیستم‌های الکترونیکی مربوط می‌شوند.

۳-۴. موضوع جرم در کلاهبرداری سایبری و ویژگی‌های آن

۳-۴-۱. موضوع جرم در کلاهبرداری سایبری

موضوع جرم کلاهبرداری مال یا وسیله تحصیل مال است، لیکن در کلاهبرداری سایبری نوعی سوءاستفاده از داده‌های رایانه‌ای و فضای سایبر است و از آنجائی که اکثر امکانات متضمن خدمات و مزایای مالی، رایانه‌ای شده‌اند امکان سوء استفاده از آن‌ها زیاد است؛ جالب این که در قوانین برخی کشورها کلاهبرداری از حد هر گونه سوء استفاده مالی از طریق رایانه نیز فراتر رفته است به عنوان مثال طبق بخش ۱۰۳۰ از ماده ۱۸ قانون جزایی ایالات متحده امریکا مصوب ۱۹۸۳ و اصلاحی ۱۹۹۶، دسترسی بدون مجوز به اطلاعات طبقه بندی شده یا اطلاعات انرژی اتمی یا هر نوع اطلاعاتی که به کشور آمریکا ضربه وارد نماید در زمره کلاهبرداری و فعالیت‌های مرتبط به آن به حساب آمده است (سالاری شهر بابکی، ۱۳۸۶: ۲۵۰).

جرم کلاهبرداری سایبری نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده‌های رایانه‌ای دارای ارزش مالی نیز می‌شود؛ در ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات موضوع جرم به صورت حصری ذکر شده است «وجه، مال یا منفعت یا خدمات یا امتیازات مالی»؛ مقنن در ماده مذکور؛ با به کار بردن واژه «یا» تحصیل هر یک از مصادیق را برای تحقق جرم کافی دانسته اما از آن جایی که قانونگذار مصادیق را به صورت حصری بیان نموده است، حیطه شمول قانون را از حیث موضوع محدود کرده است، بنابراین اگر فردی از طریق مذکور در این ماده چیزی غیر از مصادیق یاد شده را تحصیل کند؛ مانند سند، تا زمانی که منجر به تحصیل موارد مذکور در این ماده نشود، کلاهبرداری به صورت عام محقق نشده است (جاویدنیا، ۱۳۹۱: ۲۲۳).

۳-۴-۲. ویژگی‌های موضوع جرم در کلاهبرداری سایبری

۳-۴-۲-۱. مالیت داشتن

تحصیل وجوه و اموال و امتیازات مالی و بردن مال و داده‌های متعلق به غیر زمانی مصداق پیدا می‌کند که به طور کلی دارای ارزش اقتصادی باشد پس حتی اگر فرد به واسطه اعمال متقلبانه فی‌المثل در فضای اینترنت فریب بخورد و ایمیل و رمز عبور آن را به کسی بدهد و فرضاً آن شخص بعد رمز را تغییر دهد و ایمیل را به شخص، پس ندهد مرتکب جرم کلاهبرداری سایبری نشده است؛ زیرا فی‌الواقع از این طریق مالی نبرده است؛ البته موضوع بحث ما فرضاً ایمیلی است که هیچ اطلاعات مفیدی ندارد و حداقل برای ثبت نام آن وجهی پرداخت نشده باشد و امتیاز ویژه‌ای نیز در آن مستتر نباشد، مسلم است در غیر این صورت شامل کلاهبرداری سایبری خواهد بود؛ در ضمن این که دسترسی به اطلاعات شخصی و افشاء آن مطابق دیگر مواد قانونی قابل پیگرد خواهد بود (سلامی، ۱۳۹۴: ۵۲).

۳-۴-۲-۲. تعلق داشتن به غیر

تعلق داشتن موضوع جرم به دیگری؛ از وجوه جرم کلاهبرداری اعم از کلاسیک و سایبری و از عناصر تشکیل دهنده رکن مادی آن‌ها است؛ این شرط در دکترین حقوقی و رویه قضایی در مورد تمامی جرائم علیه اموال چه کلاسیک و چه سایبری مورد تأکید قرار گرفته است.

در کلاهبرداری رایانه‌ای ماده ۶۷ قانون تجارت الکترونیکی مثل سایر جرایم علیه اموال، تعلق مال برده شده، اعم از منقول و غیرمنقول، به دیگری شرط تحقق جرم است؛ بنابراین کسی که با توسل به وسایل متقلبانه مال خود را از تصرف دیگری خارج می‌کند، محکوم به ارتکاب جرم کلاهبرداری نمی‌گردد.

آنچه در این ماده قابل ابهام می‌باشد این است که مقنن بعد از ذکر موضوعات جرم، فقط به بردن اموال دیگری اشاره کرده است؛ آیا فقط تعلق اموال به دیگران شرط است و وجوه یا امتیازات مالی کسب شده لازم نیست متعق به دیگری باشد؟ (خانلرتبار، ۱۳۸۹: ۵۷)؛ به نظر می‌رسد، تمام موضوعات مدنظر چه اموال و چ امتیازات مالی باید متعلق به غیر باشند.

۳-۵. نتیجه جرم

کلاهبرداری سایبری از جرایم مقید می‌باشد و صرف وضع ید بر مال غیر بدون حصول نتیجه مجرمانه موجب تحقق جرم نیست؛ در عین حال، وجود رابطه سببیت بین رفتار و نتیجه جرم لازم است.

نتیجه جرم کلاهبرداری رایانه‌ای بر اساس ماده ۶۷ قانون تجارت الکترونیکی و ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات می‌خوانیم مشروط است به:

۱. تحصیل مال متعلق به دیگران برای خود یا دیگری.

۲. تحصیل وجوه برای خود یا دیگری.

۳. تحصیل امتیازات مالی برای خود یا دیگری.

صرف تحصیل این امور برای تحقق جرم تام کلاهبرداری کافی است و قطعاً این موارد جنبه مالی دارد.

نتیجه کلاهبرداری سایبری این است که این تحصیل برای خود یا دیگری باشد و از نظرات حقوقدانان چنین برداشت می‌شود که دیگری «باید» فرد مورد نظر مرتکب باشد ولو خود آن شخص از این قصد مرتکب اطلاع نداشته باشد؛ به عنوان مثال چنانچه فردی با نفوذ به سیستم‌های بانک مبلغی را به حساب پدرش بیفزاید، بدون آنکه پدرش مطلع شود، بزه کلاهبرداری محقق شده است، چون شخص مورد نظر مرتکب منتفع شده است؛ اما اگر با دستکاری سیستم یک بانک سبب شود حساب‌ها بهم ریخته و حساب برخی زیاد و حساب برخی کسر گردد، چون دیگرانی که از این عمل مرتکب منتفع شده‌اند، مورد نظر او نبودند، لذا بزه کلاهبرداری محقق نگردیده است.

۴. رکن معنوی جرم کلاهبرداری سایبری

رکن معنوی جرم از یک نیروی درونی/ باطنی و نفسانی سرچشمه می‌گیرد و این نیروی نفسانی همان توانمندی ادراک/ تمییز و اراده/ اختیار انسانی است؛ البته ادراک و اراده فعلیت یافته، رکن معنوی و روانی هر جرم را تشکیل می‌دهد. یعنی اراده‌ای که به نحو ایجابی یا سلبی به ارتکاب جرم تعلق گرفته باشد؛ به این ترتیب که مرتکب با علم و اطلاع از وصف عدم مشروعیت و غیرقانونی بودن رفتار، فکر و اندیشه خود را متوجه ارتکاب جرم و رفتار مجرمانه نموده باشد (منصورآبادی، ۱۳۹۶: ج۱، ۳۴۶).

۴-۱. علم و آگاهی مجرمانه در کلاهبرداری سایبری

کلاهبرداری سایبری از جمله جرایم مقید می‌باشد که احراز علم به موضوع و قصد لازم است؛ با این وجود علم به غیرواقعی بودن موضوع لازم است؛ مسلماً وقتی فرد برنامه نویس، برنامه‌ای غیر واقعی و نادرست به کامپیوتر می‌دهد، یا وقتی می‌داند که این کار وی غیر واقع و متقلبانه است (جوادی، ۱۳۸۷: ۱۲۷)؛ بدیهی است این عمل متقلبانه ملازمه با فریب قربانی کلاهبرداری سایبری ندارد.

۴-۱-۱. علم به موضوع

منظور از علم به موضوع، آگاهی مرتکب نسبت به اجزا و شرط‌ها رکن مادی جرم است. همانطور که می-دانیم رکن مادی هر جرمی دارای اجزا و شرط‌های ویژه‌ای است که مرتکب بایستی به آن‌ها علم و آگاهی

داشته باشد. عدم آگاهی نسبت به این اجزا و شرط‌ها حسب مورد می‌تواند موجب رفع یا تغییر عنوان کیفری شود و در پاره‌ای از موارد ممکن است بر وضعیت مرتکب اثرگذار نباشد؛ افزون بر این، باید توجه داشت که از نگاه روان شناختی، ناآگاهی به موضوع و اجزای رکن مادی، بر ارادهٔ مرتکب اثرگذار است و موجب ناهمخوانی خواسته و ارادهٔ مرتکب و چیزی که اراده کرده است، می‌شود و از این نگاه، رکن معنوی را خدشه دار می-سازد.

اصولاً فقدان علم موضوعی، در جرم کلاهبرداری سایبری یا به طور کل در تمام جرایم علیه اموال، موجب جهل به موضوع جرم می‌شود و رکن روانی را متزلزل می‌کند؛ در کلاهبرداری سایبری؛ بردن مال غیر نیاز به قصد دارد و قصد نیز نیاز به علم به تعلق مال به غیر دارد؛ لذا اگر کسی، مال و داده‌ای را به تصور اینکه مال خودش است، تصرف کند؛ قصد تحصیل و ربودن مال غیر را نداشته و عملش واجد عنوان مجرمانه کلاهبرداری سایبری نیست.

۴-۱-۲. علم به حکم

هنگامی می‌توان از افراد، اجرا و رعایت قانون را خواست که پیشاپیش از قانون علم و آگاهی داشته باشند. اجرای قانون، بدون آگاهی از آن، مصداق بارز تکلیف به کاری است که توان انجام آن ناممکن است (تکلیف به مالایطاق) که از دید عقل و منطق زشت و ناپسند می‌باشد. از افراد نمی‌توان خواست قانونی را اجرا و رعایت کنند که از آن بی‌اطلاع و ناآگاه‌اند. چنین چیزی به هیچ روی ممکن نیست و نمی‌توان چنین خواسته‌ای را از کسی داشت. در عین حال، در جهان حقوق با اندیشه و نهادی روبرو هستیم که آن را «ناپذیرفتنی بودن ادعای ناآگاهی» می‌خوانند و از به عنوان «فرض علم به قانون» یاد کرده‌اند (دلشاد، ۱۳۹۰: ۱۷۷).

با توجه به اینکه جرم کلاهبرداری سایبری اختصاص به افراد یقه سفید دارد و عموماً دارای تحصیلات و تخصص در رایانه می‌باشند و خصوصاً که با توسعه فناوری و سرعت تبادل اطلاعات بعید به نظر می‌رسد که بتوان چنین فرضی را در مورد فرد تصور نمود و بعید است بتوان مرتکبی را معرفی نمود که به قبح عمل جرائم سایبری آشنا نباشد تا بتوان از چنین مجرمانی ادعای عدم علم به حکم را پذیرفت.

۴-۲. قصد و اراده مجرمانه در کلاهبرداری سایبری

اراده بخش ریشه‌ای و اساسی رکن معنوی در جرم‌های عمدی است؛ در ادبیات حقوقی، از آن به عنوان «قصد»، «نیت»، «عمد» و «خواست» نیز یاد می‌شود و به خاطر پیوند آن با رفتار مجرمانه، «قصد و ارادهٔ مجرمانه/ سوءنیت» خوانده می‌شود. در این‌جا، منظور از قصد و ارادهٔ مجرمانه/ سوءنیت، کارکرد ذهنی ویژهٔ مرتکب به هنگام ارتکاب جرم است؛ به دیگر سخن، قصد و اراده در معنای عام و گسترده، عبارت است از جهت‌گیری اراده برای به انجام رساندن کاری است و هرگاه چنین کاری مجرمانه باشد، قصد را مجرمانه/ جنایی یا سوءنیت می‌گویند (قماشی، ۱۳۹۲: ج۲، ۱۱۸).

در همهٔ جرم‌های عمدی، تعلق اراده فرد به ارتکاب رفتار مجرمانه، شرط پدیدار شدن رکن معنوی است و در جرم‌هایی که نتیجه، شرط پدید آمدن رکن مادی جرم است، تعلق اراده به پیدایش نتیجه نیز برای پدیدار شدن رکن معنوی شرط است. به دیگر سخن، رکن معنوی جرم‌های مطلق، تنها به اراده ارتکاب (سوءنیت عام) نیاز دارد و در جرم‌های مقید، افزون بر سوء نیت عام، ارادهٔ پیدایش نتیجه (سوء نیت خاص) نیز برای کامل شدن رکن معنوی لازم است.

۴-۲-۱. سوء نیت عام در جرم کلاهبرداری سایبری

سوءنیت عام همان قصد ارتکاب رفتار مجرمانه است؛ یعنی اینکه مرتکب با آگاهی از اینکه رفتار ممنوع و قابل مجازات است، تصمیم می‌گیرد که آن را انجام دهد. تصمیم‌گیری مرتکب برای انجام عمل، که فرع بر آگاهی او از ممنوعیت آن است، عمد و اراده او در انجام رفتار را تشکیل می‌دهد. به دیگر سخن، تعلق فکر و اندیشه مرتکب به انجام رفتار، سوء نیت عام را در درون او بر پا می‌دارد. سوء نیت عام یا اراده ارتکاب را می‌توان اینگونه تصویر کرد که قانونگذار با وضع هر مقرره کیفری اراده می‌کند که افراد رفتار موضوع آن مقرره کیفری را انجام ندهند و یا ترک کنند؛ حال اگر کسی با آگاهی از این امر و پی‌بردن به اراده قانونگذار،

اراده خود را در برابر اراده او بکار برد و به انجام عمل روی آورد، اراده سوء خود را آشکار ساخته و قابل سرزنش می‌باشد (منصورآبادی، ۱۳۹۶: ج۱، ۳۵۹).

در جرم کلاهبرداری سایبری مرتکب باید در حین عمل دارای سوءنیت باشد؛ یعنی علاوه بر این که اعمال و وسایل متقبانه را با اراده و علم به کار می‌برد، قصد استیلا بر مال غیر را نیز داشته باشد؛ این جرم چه به صورت سنتی واقع شود چه در شکل سایبری فرقی ندارد و از نظر عنصر روانی مشترک است و وجود سوءنیت در هر دو حالت لازم است تا کلاهبرداری واقع شود؛ در کلاهبرداری سایبری مرتکب باید افعالی نظیر ورود، تغییر، محو، ایجاد، توقف را از روی اراده و نه بی‌احتیاطی یا بی‌مبالاتی یا عدم رعایت نظامات دولتی - انجام داده باشد و بداند که عملش «غیر مجاز» است یا بر اساس ماده ۶۷ قانون تجارت الکترونیکی باید بداند عملش« سوء استفاده» یا «استفاده غیرمجاز» است (جاویدنیا، ۱۳۹۱: ۲۸۴).

اگر کسی بر اثر غفلت، عملی را انجام دهد که منجر به تسلیم اموال دیگران به خودش شده باشد، کلاهبرداری نیست؛ زیرا فاقد سوءنیت عام است؛ بنابراین اگر فردی به اشتباه و بدون قصد، با ورود دادهای غلط یا فشردن دکمه‌ای موجب انتقال مال غیر به خود یا دیگری شود مرتکب جرم کلاهبرداری سایبری نشده است.

در واقع «عمد در فعل ارتکابی» به عنوان اولین عنصر از عناصر متشکله رکن معنوی هر بزه از جمله کلاهبرداری سایبری و اولین جزء از اجزای سوءنیت عام در جرم محسوب می‌گردد؛ چنانچه مبرهن است مراد از این عنوان این است که مرتکب در انجام فعل مادی ربودن قصد و تعمد داشته باشد و بدون هرگونه اجبار یا اکراهی از روی اراده آزاد اقدام به ارتکاب نماید؛ کلاهبرداری سایبری نیز جرمی عمدی است؛ بنابراین نیاز به سوءنیت عام مرتکب دارد؛ سوءنیت عام مرتکب در این جرم عبارت است از ارتکاب یکی از اعمال مندرج در قانون که اگر مرتکب در اثر بی احتیاطی یا غفلت یکی از اعمال مذکور را انجام داده باشد، حتی اگر منجر به نتیجه مجرمانه هم بشود، جرم کلاهبرداری سایبری تحقق نخواهد یافت.

۴-۲-۲. سوء نیت خاص در جرم کلاهبرداری سایبری

منظور از سوء نیت خاص، قصد مرتکب برای دستیابی به نتیجهٔ مجرمانه است؛ یعنی مرتکب قصد کرده باشد که رفتار و عمل او یک پیامد ویژه‌ای داشته باشد. روشن است اگر چنین قصدی نداشته باشد، به عنوان جرم عمدی، قابل سرزنش و مجازات نیست، هرچند در انجام رفتار از عمد و اراده برخوردار باشد (نوربها، ۱۳۹۶: ۱۹۲).

بزه کلاهبرداری سایبری موضوع مواد ۶۷ قاتون تجارت الکترونیکی و ۷۴۱ قانون مجازات اسلامی بخش تعزیرات؛ یک جرم مقید است و همان طور که تحقق نتیجه در احراز عنصر مادی آن شرط است، تحقق قصد نتیجه نیز در احراز عنصر روانی شرط است که در کلاهبرداری سایبری با توجه به مواد مذکور، قصد تحصیل وجه، مال منفعت یا امتیاز به عنوان سوءنیت خاص تلقی می‌گردد.

نتیجه گیری

۱. پیدایش رایانه و پس از آن دنیای سایبری، همراه خود دستاوردهای مثبت و منفی بسیاری داشته و دارد از جمله پیامدهای منفی آن پیدایش جرایم نوظهور کامپیوتری و اینترنتی است؛ به طور طبیعی هر نوآوری در زمینه تکنولوژی و علوم به تبع خود توجه افراد سود جو را نیز جلب می‌نماید و این افراد، امکاناتی را که می‌تواند در جهت اعتلای تمدن بشری و امنیت و رفاه بکار رود، در جهت منافع خود و ارضاء حوائج شخصی به کار می‌برند، به طوری که جرایم مربوط به تکنولوژی کامپیوتری امروزه توجه حقوقدانان، جرم-شناسان، را به خود معطوف کرده است

۲. در میان سیل جرایم ارتکابی در محیط سایبر، جرایم علیه اموال به ویژه جرم کلاهبرداری سایبری از مهم‌ترین جرایم سایبری محسوب می‌شوند؛ مطالعات و تحلیل‌های تجربی بیانگر آن است که سیستم امنیتی نامطلوب در اکثر موارد، علت یا حداقل تسهیل کننده این جرایم است؛ خسارات ناشی از جرایم کلاهبرداری در محیط سایبر به مراتب از خسارات ناشی از این جرایم به شکل سنتی آن سنگین‌تر است و دلیل آن؛ بالا بودن خسارات در جرایم سایبری و اساساً ارزش زیاد داده‌های پردازش شده است؛ اغلب مرتکبان جرایم

کلاهبرداری سایبری را جمعیت جوان تشکیل می‌دهند این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می‌دهند.

۳. ماده ۶۷ قانون تجارت الکترونیکی و ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات؛ رکن قانونی جرم کلاهبرداری سایبری را تشکیل می‌دهند و رفتار مجرمانه در رکن مادی این جرایم شامل ورود، تغییر، محو و مختل کردن و دست‌کاری سیستم خواهد بود و موضوع آن‌ها مال متعلق به دیگری و نتیجه آن‌ها محروم ساختن مالباخته از مال خود است؛ در واقع قانونگذار در کلاهبرداری سایبری با بیان نمودن مصادیق به صورت حصری حیطه شمول قانون را از حیث موضوع محدود کرده است.

۴. کلاهبرداری سایبری جرمی عمدی، آنی و مقید است و برای تحقق آن‌ها علاوه بر سوءنیت عام، سوء نیت خاص نیز لازم است؛ بنابراین باید با آگاهی و عمد باشد و اگر مرتکب در اثر بی‌احتیاطی یا غفلت یکی از اعمال مذکور را انجام داده باشد، حتی اگر منجر به نتیجه مجرمانه هم بشود، جرم کلاهبرداری سایبری تحقق نخواهد یافت؛ علم به غیرواقعی بودن موضوع لازم است؛ مسلما وقتی فرد برنامه‌نویس، برنامه‌ای غیر واقعی و نادرست به کامپیوتر می‌دهد، یا وقتی می‌داند که این کار وی غیر واقع و متقلبانه است؛ بدیهی است این عمل متقلبانه ملازمه با فریب قربانی کلاهبرداری سایبری ندارد.

پیشنهادها:

۱. بهترین راه برای جلوگیری از وقوع جرایم کلاهبرداری سایبری به آگاهی ما بستگی دارد؛ اگر تعداد بیشتری از مردم از اشکال و روش‌های فعلی جرایم سایبر آگاهی یابند، تعداد قربانیان کاهش خواهد یافت؛ صدها شرکت مشاور امنیت رایانه در سطح جامعه و در تمام جهان پدید خواهد آمد و با برطرف کردن ضعف‌های سیستم‌های نرم افزارها، حفاظت بیشتری پدید خواهند آورد؛رمز گذاری روی داده‌ها (غیر قابل فهم یا غیر قابل خواندن داده‌ها)، لایه سوکت‌های امن به عنوان استاندارد ایمنی و رمز عبور معتبر، جداسازی داده‌ها روی رایانه و تفکیک پایگاه داده‌ها (جدا نگه داشتن اطلاعات مشتریان)؛ روش‌های پیشرفته در ایمنی داده‌ها و از جمله راه‌هایی برای حفاظت از خصوصی بودن مکاتبات پست الکترونیک و سایر داده‌ها می‌باشند و هرگز نباید اطلاعات شخصی خود مانند گذرواژه‌ها را در اینترنت بازگو کرد یا از طریق پست الکترونیک و بدون محافظت ارسال کرد.

۲. کلاهبرداری سایبری جزء جرایمی می‌باشد که نظر بسیاری از بزهکاران را به خود جلب نموده است و نیاز به برخورد قاطع از سوی مراجع ذیربط دارد؛ کلاهبرداران با ارسال ایمیل و پیامک به اشخاص مختلف، آن‌ها را به انحای مختلف به پای دستگاه‌های خودپرداز (ATM) بانک‌ها می‌کشانند و اقدام به کلاهبرداری می‌نمایند و با وجود انواع کلاهبرداری اینترنتی مانند فیشینگ، ارسال ایمیل یا نفوذ به ایمیل باکس افراد و ارائه شماره حساب‌های جعلی در معاملات و استفاده از اسکیمرها در دستگاه های خودپرداز بانک ها برای سوءاستفاده از کارت‌های عابر بانک و با وجود افزایش این نوع کلاهبرداری‌ها، سیستم‌های ایمنی و حفاظتی بانک‌ها بسیار ضعیف عمل می‌کنند.

فهرست منابع

۱. آقایی‌نیا، حسین(۱۳۹۶)؛ جرایم علیه اشخاص(جنایات)؛ تهران: انتشارات میزان، چاپ شانزدهم.

۲. اردبیلی، محمدعلی (۱۳۹۲)؛ حقوق جزای عمومی، جلد اول، تهران: انتشارات میزان، چاپ سی و دوم.

۳. باستانی، برومند(۱۳۸۶)؛ جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران: انتشارات بهنامی، چاپ دوم.

۴. حسن بیگی، ابراهیم(۱۳۸۴)؛ حقوق و امنیت در فضای سایبر، موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر تهران، چاپ اول، ۱۳۸۴.

۵. جاویدنیا، جواد (۱۳۹۱)؛ جرایم تجارت الکترونیکی، تهران: انتشارات خرسندی، چاپ سوم.

۶. جوادی، سید هادی(۱۳۸۷)؛ کلاهبرداری اینترنتی، فصلنامه گفتمان حقوقی، دانشگاه علوم اسلامی رضوی، سال پنجم، شماره ۱۳-۱۴.

۷. خانلر تبار، سمانه (۱۳۸۹)؛ بررسی تطبیقی کلاهبرداری رایانه‌ای و کلاسیک، پایان نامه کارشناسی ارشد، رشته حقوق کیفری و جرم‌شناسی، دانشگاه فردوسی مشهد.
۸. خداقلی، زهرا (۱۳۸۳)؛ جرایم رایانه‌ای، تهران: انتشارات آریان، چاپ اول.
۹. سالار شهر بابکی، میرزامهدی(۱۳۸۶)؛ مروری بر کلاهبرداری رایانه‌ای، تهران: انتشارات میزان، چاپ اول.
۱۰. سلامی، حمیده (۱۳۹۴)؛ بررسی و تطبیق سرقت سایبری و کلاهبرداری سایبری، تهران: انتشارات مجد، چاپ اول.
۱۱. شیرزاد، کامران(۱۳۸۸)؛ جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق جزای بین‌الملل، تهران: نشر بهینه، چاپ اول.
۱۲. دانشخواه، اعظم السادات (۱۳۹۲)؛ کلاهبرداری رایانه‌ای در ایران و امریکا، پایان نامه کارشناسی ارشد، رشته حقوق کیفری و جرم‌شناسی، دانشگاه تهران، پردیس قم/ فارابی.
۱۳. دلشاد، ابراهیم(۱۳۹۲)؛ فرض‌های حقوقی (پژوهشی از چشم انداز تاریخ و فلسفه حقوق)، قم، انتشارات دانشگاه مفید، چاپ اول.
۱۴. زبیر، اولریش(۱۳۹۰)؛ جرایم رایانه‌ای، ترجمه محمدعلی نوری و دیگران؛ تهران: انتشارات گنج دانش، چاپ دوم.
۱۵. زندی، محمدرضا (۱۳۹۳)؛ تحقیقات مقدماتی در جرائم سایبری، تهران: انتشارات جنگل، چاپ اول ویرایش جدید.
۱۶. عالی پور، حسن(۱۳۹۲)؛ حقوق کیفری فناوری اطلاعات، تهران: انتشارات خرسندی، چاپ دوم.
۱۷. قماشی، سعید (۱۳۹۲)؛ بازکاوی عنصر روانی در جرایم عمدی، مندرج در دایره المعارف علوم جنایی، تهران: انتشارات میزان، چاپ اول.
۱۸. منصورآبادی، عباس (۱۳۹۴)؛ حقوق کیفری عمومی، کلیات حقوق کیفری و پدیده مجرمانه؛ جلد اول، تهران: انتشارات میزان، چاپ اول.
۱۹. میرمحمدصادقی، حسین و شایگان، محمدرسول (۱۳۸۹)؛ بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات‌های آن در نظام حقوقی ایران، نشریه حقوق: دیدگاه‌های حقوق قضایی، شماره پاییز و زمستان: شماره ۵۱-۵۲.
۲۰. نوربها، رضا (۱۳۹۶)؛ زمینه حقوق جزای عمومی، ویراست جدید تجدیدنظر شده دکتر عباس شیری، تهران: انتشارات میزان، چاپ اول.
۲۱. Edgar, stacey(۲۰۰۳), morality and machines: perspectives on computer ethics, jones and Bartlett publishers, second edition.
۲۲. Keyser,mike.(۲۰۰۳), the council of Europe convention on cybercrime, journal of transnational law and policy, volume ۱۲.
۲۳. Pease.K(۲۰۰۱) Crime futures and foresight: challenging criminal behavior in the information age. In D.S. Wall(ed) Crime and the Internet, London: Oxford University press.