شناسهٔ دیجیتال (DOI): 10.22106/JLJ.2023.553967.4837

مجله حقوقی دادگستری

مقالهٔ پژوهشی، دورهٔ ۸۷، شمارهٔ ۱۲۲، تابستان ۱۴۰۲، صفحات ۲۱ تا ۴۴
تاریخ دریافت: ۱۴۰۱/۰۲/۲۷ - تاریخ پذیرش: ۱۴۰۱/۰۶/۲۱

# نقش دوگانهٔ ابزار رایانه‌ای در تحقق کلاهبرداری

وحید بازوند*، حسین نورمحمدی**

## چکیده

ماهیت ابزارهای رایانه‌ای به‌گونه‌ای است که نحوهٔ به‌کارگیری و نوع کارکرد آن که به دو شکل فعّالِ باغلبهٔ کارکرد فنی، یا منفعلِ با غلبهٔ کنشگری فریبکارانهٔ انسانی قابل‌مشاهده می‌باشد، آن‌ها را قادر به ایفای دو نقش کاملاً متفاوت و نهایتاً شکل‌گیری دو گونه مجزای کلاهبرداری مشتمل بر کلاسیک و رایانه‌ای می‌نماید. بر این اساس قائلین به تفسیر موسع از کلاهبرداری رایانه‌ای، مجرد استفاده از یک ابزار ماهیتاً رایانه‌ای در خلال کنشگری مجرم را جهت تحقق عنوان کلاهبرداری رایانه‌ای کافی قلمداد می‌نمایند. در طیف مقابل پیروان برداشت مضیق از این مفهوم، با ارائهٔ تفسیر منطقی و حتی منطوقی از ماده ۷۴۱ قانون مجازات اسلامی (بخش جرایم رایانه‌ای) ابزار رایانه‌ای را صرفاً در صورتی در شکل‌گیری کلاهبرداری رایانه‌ای مؤثر تلقی می‌کنند که در دو بخش «نحوهٔ به‌کارگیری و نوع کارکرد» و «بستر ارتکاب» که در خلال پایش و پردازش داده‌ها و تعامل دو سامانه در مبدأ و مقصد که با کنشگری غیرمستقیم انسانی همراه است، واجد شرایط خاصی باشد. این پژوهش با روش مطالعهٔ منابع رسمی و کتابخانه‌ای و ارزیابی رویهٔ قضایی و برخی آرای محاکم موفق به شناسایی و استخراج سه معیار عینی «رایانه‌ای به‌عنوان وصف ذاتی یک ابزار با قابلیت پردازش داده»، «لزوم بهره‌گیری مرتکب از کارکرد فنی و فعال یک ابزار» و در نهایت «مجازی بودن بستر از ابتدا تا انتهای فرایند تکوین جرم و تحقق نتیجه در همین بستر» شده است که به نظر می‌رسد در مقام ارزیابی افتراقی این دو شکل از کلاهبرداری در مصادیق مشتبه کاملاً کارآیی خواهند داشت. در همین راستا پیشنهاد می‌شود ضوابط سه‌گانهٔ مذکور در قالب مصوبهٔ تقنینی به‌کارگیری شوند تا چالش مورد نظر

* قاضی دادگستری، دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق قضایی، دانشگاه علوم قضایی، تهران، ایران (نویسنده مسئول) vahidbazvand70@gmail.com

** قاضی دادگستری، دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران Hosein.normohamadi96@gmail.com

منجر به چنددستگی و اختلاف‌نظر در رویهٔ قضایی نشود.

**واژگان کلیدی:** کلاهبرداری، افتراق ابزاری، کارکرد فنی رایانه‌ای، انفعال ابزار، کنشگری انسانی، مجرای ارتکاب

**مقدمه**

تا پیش از تصویب قانون تجارت الکترونیکی در سال ۱۳۸۲ و قانون جرایم رایانه‌ای در سال ۱۳۸۸، کلاهبرداری صرفاً به شکل ساده و به تعبیری سنتی آن جرم‌انگاری شده بود.[۱] با تصویب قوانین مذکور و جرم‌انگاری کلاهبرداری رایانه‌ای و تشکیل پرونده‌های قضایی متعدد در این رابطه، چالش‌های متعددی پیرامون چگونگی تشخیص و تفکیک این دو شکل از کلاهبرداری مطرح گردیده است. همچون دیگر مصادیق مشابه، علت این امر بی‌توجهی مقنن به روش‌های دقیق و تکنیک‌های مؤثر در نگارش قانون است که ارائهٔ معیار و ضابطهٔ مشخص را در این رابطه دشوار نموده است. به‌عنوان مثال چنانچه شخص «الف» از طریق تارنمای «دیوار»[۲] مبادرت به تبلیغ و درج آگهی فروش یک دستگاه خودرو با قیمت کمتر از حد متعارف و کارشناسیِ آن نماید و شخص «ب» تحت تأثیر تبلیغ و مفاد آگهی فروش، اغفال و ضمن تماس با فروشنده درخواست خرید خود را عنوان نماید و در این مقطع فروشنده به‌منظور تضمین انجام معامله تقاضای پرداخت بخشی از ثمن را به‌عنوان بیعانه مطرح کند و سپس متقاضی خرید، این مبلغ را از طریق انتقال کارت به کارت در بستر شبکهٔ سراسری شتاب خودپردازهای بانکی، به شمارهٔ کارت اعلامی فروشنده واریز نماید؛ با فرض احراز سایر شرایط لازم آیا این اقدام مصداق کلاهبرداری مرتبط با رایانه محسوب می‌شود و یا کلاهبرداری کلاسیک است؟ در دکترین حقوقی و همچنین رویهٔ قضایی کشور دو دیدگاه غالب و کلی نسبت به کلاهبرداری از طریق ابزار رایانه‌ای وجود دارد. قائلین به دیدگاه سنتی با این استدلال که استفاده از ابزار رایانه‌ای به نوعی بخشی از رکن مادی کلاهبرداری محسوب می‌شود، برای ابزار رایانه‌ای اصالت جداگانه‌ای که منجر به تحقق کلاهبرداری رایانه‌ای شود، قائل نمی‌باشند. در مقابل عده‌ای نیز به‌طور

۱. ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری مصوب ۱۳۶۷: «هر کس از راه حیله و تقلب مردم را به وجود شرکتها یا تجارتخانه های یا کارخانه ها یا موسسات موهوم یا به داشتن اموال واختیارات واهی فریب دهد یا به امور غیر واقع امیدوار نماید یا از حوادث و پیش آمدهای غیر واقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر وجوه و یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و علاوه بر رد اصل مال به صاحبش، به حبس از یک تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود ...».

۲. سایت اینترنتی خرید و فروش کالا

مطلق هرگونه کلاهبرداری با ابزار رایانه‌ای را موجب تحقق کلاهبرداری رایانه‌ای می‌دانند. مستمسک عدهٔ اخیر مفاد نص مادهٔ ۷۴۱ قانون مجازات اسلامی ـ تعزیرات است که به نظر ایشان حاوی نوعی اطلاق می‌باشد. بدین معنی که هرگونه کلاهبرداری در نتیجهٔ عملیات مرتبط با ابزار رایانه‌ای، موجب تحقق کلاهبرداری رایانه‌ای می‌شود. البته در این رابطه قائل شدن به نظر بینابین نیز حائز اهمیت است که در این مقاله ارائه و بررسی می‌شود.

این تحقیق درصدد است تا با ارزیابی منابع رسمی و کتابخانه‌ای و همچنین برخی احکام قضایی موجود، ضوابط کاربردی جهت تشخیص افتراقی این دو شکل از کلاهبرداری را تعیین، احصا و پیشنهاد نماید.

## ۱. نقش حداکثری مرتکب در کلاهبرداری کلاسیک

در نخستین بخش از این مقاله با نقش مرتکب و عملکرد متفاوت او در فرایند تکوین جرم در دو گونهٔ مورد نظر کلاهبرداری پرداخته خواهد شد. هرچند در دو شکل از کلاهبرداری، کنشگری انسانی نقش اصلی را در تحقق رفتاربه‌عنوان بخش اساسی رکن مادی ایفا می‌کند، اما دارای تفاوت جزئی در چگونگی اجرا هستند. به این توضیح که رفتار مجرمانه در کلاهبرداری موضوع ماده ۱ قانون تشدید مجازات مرتکبین اختلاس، ارتشا و کلاهبرداری مصوب ۱۳۶۷ به‌صورت مستقیم و در مواجهه با بزه‌دیده و ابتکار عمل بالای مرتکب همراه است و این امر مستلزم هوشمندی مرتکب در تمام ابعاد و هماهنگی کامل در تمام بخش‌های رکن مادی با مدیریت وی می‌باشد، لکن کنشگری مرتکب در کلاهبرداری مرتبط با رایانه تا حدی متفاوت است به‌گونه‌ای که اصولاً شاهد فعالیت حداقلی مرتکب و کنشگری حداکثری سیستم پردازش رایانه‌ای هستیم. «در واقع کاربر سامانهٔ رایانه‌ای به‌عنوان مرتکب جرم صرفاً از خدمات و ظرفیت‌های پردازشی یک سامانه جهت تحقق رکن مادی مشتمل بر اضافه کردن، حذف، تغییر، تعویض اطلاعات ورودی و یا ارسال آن به محل نامناسب استفاده می‌کند» (زیبر اولریش، ترجمه محمدعلی نوری و دیگران، ۱۳۸۴: ۲۴). بنابراین در اولین گام اَعمال مجرمانهٔ مذکور توجه به این نکته ضروری است که در کلاهبرداری کلاسیک بار تحقق رفتار کاملاً بر دوش مرتکب است. هرچند ممکن است سامانهٔ رایانه‌ای نیز در این فرایند مورد استفادهٔ مرتکب قرار گیرد، اما این استفاده صرفاً به‌عنوان ابزاری در جهت تکوین رکن مادی وی ارزیابی می‌شود و بر اساس تحلیلی که پیش از این گذشت، در رایانه‌ای بودن این مصادیق کلاهبرداری، تردید جدی وجود خواهد داشت.

### ۱-۱. ساحَت انسانی محض در رفتار مجرمانه

یکی از مهم‌ترین دستاوردهای حقوق کیفری جدید، تأکید بر این امر است که جرم و مجرم صرفاً در حدود دو رکن مسئولیت کیفری یعنی ادراک و اختیار قابلیت سرزنش خواهند داشت. این دو مؤلفه

به‌عنوان بخشی از اختصاصات انسانی مؤید این گزاره است که جرم صرفاً توسط نوع انسان قابل‌ارتکاب است، اما نوع، میزان و نحوهٔ مداخلهٔ انسان در فرایند ارتکاب جرایم همیشه یکسان نبوده و دارای شدت و ضعف است. با این توضیح که در دسته‌ای از جرایم، ماهیت رکن مادی و به‌طور خاص رفتار مجرمانه به‌گونه‌ای بوده که انسان قادر است نقش مستقیم و بدون واسطهٔ خود را تا تکمیل فرایند ارتکاب جرم ایفا و در این مسیر سخن از هیچ عامل مستقل یا مؤثر دیگری مطرح نخواهد شد. مواردی مانند توهین و تهدید از زمرهٔ این جرایم می‌باشند. در مقابل در برخی جرایم شرایط به‌گونه‌ای است که اگر بنا بر تعیین و توسعهٔ قلمرو مسئولیت به اشیا باشیم، شرایط به‌گونه‌ای خواهد شد که به‌دلیل نقش غیرمستقیم و مبتنی بر راهبری و هدایت انسان، منجر به خروج انسان و یا پیش‌بینی کمترین سطح از مسئولیت کیفری برای وی خواهد شد. به‌عنوان مثال نرم‌افزاری را تصور نمایید که صرفاً با فشردن یک کلید فرایند طراحی و پردازش یک پلان و به دنبال آن ایجاد داده‌های متقلبانه و ارسال آن به سامانهٔ رایانه‌ای دیگر را اجرا و در نهایت موفق به دریافت امتیازات مالی مورد نظر و ارائهٔ آن به کاربر شود. در جرایم رایانه‌ای همواره شاهد حضور فعال و مؤثر سامانهٔ رایانه‌ای و بالعکس موقعیت منفعل و محدود به «کاربری» انسان می‌باشیم، که از این تفکیک می‌توان در افتراق انواع کلاهبرداری از یکدیگر استفاده نمود.

### ۲-۱. رفتار مجرمانه در تکاپوی ابزار

اصولاً بزه کلاهبرداری بنا به‌طبع و ماهیت آن بر فریب و تزویر استوار است. بنابراین ماهیت ابزار در تحقق این جرم واجد وصف موضوعیت است. بر همین مبنا در بزه کلاهبرداری «متقلبانه بودن» وصف اساسی در رابطه با ابزار محسوب می‌شود، لکن در مقام تمیز میان نحوهٔ تحقق رکن مادی در بزه کلاهبرداری رایانه‌ای و سنتی بر این نکته تأکید می‌شود که در کلاهبرداری رایانه‌ای، وسایل رایانه‌ای و مخابراتی علاوه بر اینکه ابزار ارتکاب جرم محسوب می‌شوند، مجری تحقق آن نیز هستند. بنابراین صرف استفادهٔ ابزاری از وسایل و سامانه‌های رایانه‌ای و مخابراتی بدون اینکه فرایند پردازش هوشمند داده‌های مجرمانه و ارسال آن در این سامانه‌ها انجام شود، دلیلی بر رایانه‌ای تلقی نمودن کلاهبرداری نخواهد بود. به‌عنوان مثال اگر شخص «الف» تصویر خود را با استفاده از برخی نرم‌افزارهای رایانه‌ای در کنار فرد مشهوری قرار داده و با نشان دادن آن تصویر در رایانهٔ شخصی به دیگری، خود را شخصی بانفوذ معرفی و از این طریق اموالی را از او دریافت کند، با رعایت سایر شرایط کلاهبرداری کلاسیک خواهد بود چراکه در این حالت سامانهٔ رایانه‌ای صرفاً ابزار ارتکاب جرم بوده و نه مجری ارتکاب جرم. با این توضیح اشاره به برخی طُرُق تحقق رکن مادی جرم کلاهبرداری رایانه‌ای، با تأکید بر مفهوم «ابزار» ارتکاب جرم، به این دلیل که در نهایت منجر به تبیین ضوابط اختصاصی این شکل از جرم کلاهبرداری می‌شود، خالی از فایده نخواهد بود.

### ۱-۲-۱. وارد کردن داده‌ها

ازجمله بارزترین مصادیق رفتاری کلاهبرداری رایانه‌ای وارد کردن داده‌ها به‌صورت غیرمجاز در سامانه‌های رایانه‌ای و مخابراتی می‌باشد. لازم به ذکر است که «واژهٔ داده به‌صورت خاص در نظام حقوقی ایران معرفی نشده است ولی به‌صورت داده‌پیام و داده‌ترافیک[1] از آن تعریف به عمل آمده است» (تبریزی و دیگران، ۱۴۰۱: ۱۳۴). «هنگامی که داده‌های موجود در سیستم رایانه‌ای به‌صورت آنلاین در فضای سایبر قرار می‌گیرد، با امکاناتی که هم اکنون خود فضای سایبر در اختیار همگان قرار می‌دهد، با پیاده کردن و اجرای برنامه‌های متنوعی که کار با آن‌ها نیازمند تخصص بالایی نیست می‌توان به آن‌ها دسترسی پیدا کرد که بدیهی است این خود به معنی آسیب‌پذیری بالای داده‌های الکترونیکی است» (جلالی فراهانی، ۱۳۸۹: ۲۱۴). این رفتار از طرق مختلف قابل ارتکاب است مانند وارد کردن رمز کارت بانکی دیگری که به‌صورت غیرمجاز تحصیل گردیده است، هم از طریق صفحه کلیدهای فیزیکی دستگاه خودپرداز و هم به‌صورت مجازی در فضای سایبر که در نهایت منجر به بردن یا تحصیل مال یا منفعت و امتیاز مالی دیگری شود. نکتهٔ مهم در این رابطه آن است که منظور از «غیرمجاز بودن» در واقع فقدان جواز قانونی برای کلاهبردار در وارد کردن داده می‌باشد، هرچند که این داده‌ها به‌صورت مجاز در اختیار وی قرار گرفته باشد اما اجازهٔ استفاده از آن را نداشته باشد. اطلاق مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) نیز مبین صحت این ادعا می‌باشد. در مقابل ممکن است ایراد شود که جرایم رایانه‌ای، موضوع‌محور بوده و نخستین قربانی این نوع جرایم، سامانهٔ رایانه‌ای و مخابراتی است و استفادهٔ غیرمجاز از داده‌هایی که به‌صورت مجاز در اختیار مرتکب قرار گرفته است، به‌دلیل عدم شمول تقلب یا اختلال در سامانه، کلاهبرداری رایانه‌ای محسوب نمی‌شود. این نگرش، هرچند قابل‌تأمل است، اما ظاهر مادهٔ ۷۴۱ مطلق بوده و تمایزی میان داده‌های واقعی و جعلی قائل نیست و همچنین تعریفی از عبارتِ مطلق «غیرمجاز» بیان نشده تا بتوان به‌صراحت بین غیرمجاز از نظر مقنن و صاحب مال یا امتیاز مالی تفکیک نمود. برهمین اساس به نظر می‌رسد برای تحقق کلاهبرداری رایانه‌ای محض، جعلی بودن داده‌هایی که توسط کلاهبردار در سامانهٔ رایانه‌ای یا مخابراتی وارد می‌شود، لزومی ندارد، زیرا که واژهٔ «غیرمجاز» در صدر مادهٔ ۷۴۱ مذکور اطلاق دارد (رستمی، ۱۳۹۸: ۶۰) و «هم شامل داده‌های صحیحی می‌شود

۱. تبصره ۱ ماده ۶۶۷ قانون آیین دادرسی کیفری ۱۳۹۲: «داده ترافیک، هر گونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیرهٔ ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آن‌ها ازمبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدا، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود».

که به‌صورت غیرمجاز استفاده شده است و هم داده‌های جعلی را دربرمی‌گیرد» (دزیانی، ۱۳۷۶: ۱۳۲) و آنچه ملاک است عدم جواز مرتکب در استفاده از داده‌های مذکور است. با این توضیح اگر شخصی اطلاعات ورود به حساب بانکی دیگری را به‌صورت مجاز در اختیار داشته باشد ولی بدون اجازهٔ صاحب آن با مراجعه به دستگاه خودپرداز بانکی از این حساب وجهی دریافت یا از طریق شبکهٔ پرداخت اینترنتی مبادرت به خرید کالا نماید و یا اقساط بدهی ناشی از اخذ تسهیلات بانکی سابق خود را بپردازد، مرتکب کلاهبرداری رایانه‌ای محض شده است.[۱]

لازم به ذکر است بر اساس یافته‌های این پژوهش وجود دو سامانهٔ رایانه‌ای در مبدأ و مقصد جهت تحقق بزه کلاهبرداری رایانه‌ای ضروری است و بر این اساس این شائبه به ذهن متبادر می‌شود که در مصداق فوق صرفاً یک سامانهٔ رایانه‌ای حضور دارد، لکن توجه به این نکته ضروری است که در این مورد، سامانه رایانه‌ای به‌صورت هم‌زمان به‌عنوان سامانهٔ مبدأ و ابزار مورد استفادهٔ مرتکب (صفحه کلید جهت ورود داده) و در مقصد به‌عنوان متصدی پردازش داده عمل می‌نماید.

### ۲-۲-۱. تغییر داده‌ها

یکی دیگر از طرق تحقق رکن مادی بزه موضوع ماده ۷۴۱ قانون مجازات اسلامی تغییر داده‌ها می‌باشد. این امر از طریق تغییر داده‌های واقعی یا تبدیل آن امکان‌پذیر است. به‌عنوان مثال چنانچه شخص «الف» عکس متعلق به خود را از طریق نرم‌افزارهای تغییر چهره شبیه عکس شخص «ب» تغییر دهد و با ورود به نرم‌افزار تاکسی‌های اینترنتی و بارگذاری عکس مجعول، از تاکسی اینترنتی استفاده، لکن مبلغ کرایه از حساب شخص «ب» کسرشود، مرتکب کلاهبرداری رایانه‌ای شده است.

نکتهٔ حائز اهمیت آن است که تغییر داده زمانی واجد عنوان مجرمانهٔ کلاهبرداری رایانه‌ای می‌باشد که منجر به تحصیل مال یا منفعت یا خدمات و امتیازات مالی برای مرتکب شود (قناد، ۱۳۸۷: ۱۳۹)؛ در غیر این صورت این رفتار قابل‌انطباق با عناوین مجرمانهٔ دیگری مانند «جعل

۱. در این رابطه اداره حقوقی قوه قضاییه نیز طی یک نظریه مشورتی به شرح ذیل و به شماره ۷/۹۳/۱۱۶۱ مورخ ۱۳۹۳/۵/۱۸ ادعای فوق را تأیید می‌نماید: «۱. منظور از فعل وارد کردن در ماده ۷۴۱... وارد کردن داده ها به هر ترتیبی است که منتهی به تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا اشخاص دیگر باشد؛ اعم از اینکه شخص مذکور قبلاً اطلاعات مربوط به داده ها را در اختیار داشته یا به وسایل متقلبانه، اطلاعات مورد نظر خود را کسب نماید. ۲. چون ملاک تحقق جرائم مندرج در قانون جرایم رایانه ای، استفاده از سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده است و در فرض سؤال به لحاظ اینکه سرقت انجام شده با استفاده غیر مجاز از داده های رایانه‌ای و وارد نمودن رمز کارت عابر بانک دیگری صورت گرفته است، موضوع مشمول ماده ۷۴۱ الحاقی به قانون مجازات اسلامی... است».

رایانه‌ای» و «دسترسی غیرمجاز رایانه‌ای» به اطلاعات و داده‌های غیر می‌باشد.

### ۳-۲-۱. ایجاد داده‌ها

ایجاد داده‌های غیرمجاز می‌تواند از طریق تولید داده‌های متقلبانه با صفحه کلید یا دیگر ابزارهای رایانه‌ای صورت گیرد. یکی از رایج‌ترین نمونه‌های کلاهبرداری رایانه‌ای، راه‌اندازی صفحه‌های جعلی پرداخت شتابی در فضای سایبر است. در این روش کاربرانی که در فرایند خرید اینترنتی، قصد انجام عملیات پرداخت را دارند به صفحه‌ای که توسط کلاهبردار با استفاده از ریزداده‌های مجعول ایجاد شده است هدایت می‌شوند و کاربر مربوطه اطلاعات حساب خود را در آن صفحه وارد نموده و از این طریق راه را برای دسترسی افراد کلاهبردار به حساب بانکی خود فراهم می‌سازند. این عمل از منظر فناوری اطلاعات، صید اطلاعات[1] نامیده می‌شود (ویلیامز، ۱۳۹۱: ۶۶).

### ۴-۲-۱. توقف داده‌ها

توقف داده نیز به‌عنوان شکل دیگری از رکن مادی کلاهبرداری رایانه‌ای می‌باشد. به این صورت مرتکب با ایجاد اختلال در سامانه، در عملکرد منطقی داده‌ها توسط کاربر مجاز مانع و توقف ایجاد می‌کند و از این فرصت و وقفه سوءاستفاده کرده و مال یا امتیاز مالی تحصیل نماید. البته باید توجه داشت که اختلال و توقف در عملکرد داده در صورتی کلاهبرداری رایانه‌ای تلقی می‌شود که به همراه سایر شرایط منجر به تحصیل مال یا امتیاز مالی برای کلاهبردار یا فرد مورد نظر او شود.

### ۵-۲-۱. امحای داده‌ها

نوع دیگری از کلاهبرداری رایانه‌ای، از بین بردن تمام یا بخشی از داده‌های متعلق به دیگری از طریق سامانهٔ رایانه‌ای است. در این شکل از کلاهبرداری مرتکب با حذف و محو نمودن داده‌های دیگری به منابع و حساب‌های مالی دسترسی پیدا می‌کند. برای مثال کلاهبردار رمز ورود به حساب بانکی متعلق به دیگری را از بین برده و وجوهی را از طریق سامانهٔ رایانه‌ای به حساب بانکی خود منتقل و تحصیل نماید و یا داده‌هایی که وظیفه حفظ و حراست از اموال امتیازات مالی را دارد به‌نحوی بی‌اثر نموده و از این طریق مبادرت به کسب مصادیق مالی مورد نظر در این فضای محافظت نشده نماید.

### ۶-۲-۱. اختلال در سامانه

این حالت به وضعیتی اطلاق می‌گردد که سامانهٔ رایانه‌ای از نظر عملکرد پردازش صحیح و منطقی با مشکل مواجه شود. «اختلال در سامانه شامل هر نوع مداخلهٔ نرم در این فرایند از قبیل جلوگیری از خروج داده‌ها، تأثیر گذاشتن بر ثبت و ذخیره یا جریان داده‌ها یا توانایی اجرای برنامه‌ها می‌شود» (خرم آبادی، ۱۳۸۶: ۹۳).

1. Fishing

یکی از مصادیق اختلال در سامانه وضعیتی است که کلاهبردار از طریق فضای اینترنت مبادرت به فروش کتاب‌های الکترونیکی می‌نماید؛ به این نحو که درحالت عادی (غیرکلاهبرداری) کاربر، پس از پرداخت اینترنتی هزینه خرید، قادر به دریافت نسخهٔ الکترونیکی کتاب می‌باشد. در چنین حالتی اگر فروشنده با سوءنیت و پس از پرداخت هزینهٔ اینترنتی توسط کاربرِ خریدار اختلالی در سامانه ایجاد نماید که کاربر قادر به دریافت نسخهٔ الکترونیکی کتاب نباشد، مرتکب کلاهبرداری رایانه‌ای شده است.

## ۲. الگوی بزه‌دیدگی

از دیگر وجوه افتراق بین کلاهبرداری کلاسیک و کلاهبرداری رایانه‌ای شرایط و ویژگی‌های مربوط به بزه‌دیده این جرایم می‌باشد. «در کلاهبرداری کلاسیک، بزه‌دیده شخص حقیقی یا حقوقی است و این شخص به‌طور مستقیم متأثر از عملیات فریب و اغفال است» (علی‌نژادی و علی‌نژادی، ۱۳۹۷: ۷۳). از طرف دیگر بین مرتکب و بزه‌دیده ارتباط عینی و ملموس ایجاد می‌گردد (عالی‌پور، ۱۳۸۳: ۲۱۱) و بزه‌دیده نیز در تحقق بزه کلاهبرداری کلاسیک نقشی مؤثر ایفاء می‌کند و با رضایت مال خود را تحویل کلاهبردار می‌دهد. در نوع کلاسیک این جرم، مرتکب با توسل به وسایل تقلبی، مال‌باخته را اغفال می‌کند تا با رضایت (هرچند معیوب) مال خود را به او تسلیم کند. ازاین‌رو ناآگاهی قربانی از متقلبانه بودن، شرط تحقق جرم است (حبیب‌زاده، ۱۳۸۰: ۷۲). لکن در کلاهبرداری رایانه‌ای «فریب» یا «اغفال» بزه‌دیده جزء ضروری و لازم جهت تحقق این جرم نیست و اساساً ممکن است هویت بزه‌دیده برای مرتکب نامشخص باشد و هیچ گونه مواجهه یا ارتباطی میان این دو نباشد و بر همین اساس هیچ‌گونه نقش فعّال یا مبتنی بر تقصیر از جانب قربانی جرم متصور نباشد. «در واقع در این شکل از کلاهبرداری بدون اینکه بزه‌دیده به‌طور مستقیم فریب بخورد، توسط کلاهبردار عملیاتی از طریق سیستم رایانه‌ای صورت می‌گیرد که با فریب یا حتی عدم فریب رایانه منجر به تحصیل مال یا امتیازهای مالی برای کلاهبردار می‌گردد» (باستانی، ۱۳۸۳: ۱۲۴). در قانون کلاهبرداری مصوب ۲۰۰۶ کشور انگلستان، جرم مشابه با کلاهبرداری رایانه‌ای موضوع بحث ما با عنوان «تحصیل متقلبانهٔ خدمات» شناخته می‌شود که جرمی مقید است (Catherin Elliot and Frances Quinn, 2010: 241). مطابق با این قانون تحقق جرم مذکور نیازمند اثبات فریب قربانی یا بزه‌دیده نیست و به همین سبب این جرم می‌تواند نسبت به دستگاه‌هایی مانند خودپرداز یا رایانه نیز ارتکاب یابد (Noel, 2010: 159).

### ۲-۱. بزه‌دیدگی علمی و درجاتی از تقصیر در کلاهبرداری کلاسیک

همان گونه که ذکر گردید در تحقق کلاهبرداری وجود شرایطی ضروری است که ازجمله این شروط، اغفال بزه‌دیده می‌باشد. این وضعیت به دنبال اجرای عملیات متقلبانه و مؤخر بر آن، در

بزه‌دیده پدیدار می‌شود. برخلاف کلاهبرداری رایانه‌ای، در کلاهبرداری کلاسیک می‌توان در بسیاری از موارد نقش مؤثر بزه‌دیده یا قربانی را در تحقق این جرم را مشاهده و تأیید نمود. در جرم‌شناسی بزه‌دیده‌شناسی،[1] رفتار این دسته از بزه‌دیدگان، غالباً بر اساس الگوی بزه‌دیدگی علمی یا اولیه مورد تحلیل و بررسی قرار می‌گیرد. مطابق با این دیدگاه، بزه‌دیده یکی از ارکان پیش جنایی و مؤثر در تحقق جرم است که در تصمیم‌گیری بزهکار برای به فعلیت درآوردن اندیشهٔ مجرمانه و یا گذار از اندیشهٔ مجرمانه به عمل مجرمانه ایفای نقش می‌کند و هدف دیدگاه مورد اشاره تبیین و تحلیل تقصیر بزه‌دیده در تکوین جرم و آثار آن بر میزان مسئولیت کیفری بزهکار است (زررخ، ۱۳۸۹: ۱۳۲). خصوصیاتی از قبیل ساده‌لوح بودن، زود اعتماد کردن، اموال و دارایی‌های خود را در دسترس عموم گذاشتن، ارتباط با افراد یقه‌سفید و کلاهبردار و... (زررخ، ۱۳۸۹: ۱۳۲) ازجمله رفتارهایی می‌باشد که به‌عنوان نقش یا تقصیر بزه‌دیده درارتکاب جرم کلاهبرداری قابل‌ذکر می‌باشد (محسنی، ۱۳۹۴: ۳۶۰).

در ادامه نمونه‌ای که درحال حاضر از شیوع بالایی برخوردار است و تقصیر بزه‌دیده در آن قابل‌بررسی می‌باشد مطرح می‌شود. به این نحو که گاهی مشاهده می‌شود با شمارهٔ همراه شخصی (نه شماره خط ثابت سازمان یا اداری) با شخص هدف و قربانی تماس تلفنی برقرار و به ایشان اعلام می‌شود که برندهٔ سفر زیارتی به مقصد مشخص وبا تخفیف ویژه شده است و می‌بایست مبلغی به حساب شخص تماس گیرنده که خود را به‌عنوان مسئول دفتر خدمات زیارتی و سیاحتی شهر محل سکونت بزه‌دیده معرفی نموده، از طریق انتقال در بستر اینترنت یا دستگاه خودپرداز پرداخت نماید. بزه‌دیده نیز قبل از هرگونه اقدامی مانند مراجعه به دفاتر مربوطه جهت احراز صحت ادعای تماس گیرنده یا بدون توجه به شخصی بودن شمارهٔ تماس گیرنده، مبلغی را به یکی از طرق مذکور به حساب تماس گیرنده پرداخت می‌نماید. در این مثال اگر بزه‌دیده کمی دقت یا تحقیق بیشتری می‌نمود، قربانی کلاهبرداری نمی‌گردید.[2]

موضوع نقش بزه‌دیده غالباً در کلاهبرداری کلاسیک مطمح نظر قرار می‌گیرد و در کلاهبرداری رایانه‌ای در عمدهٔ موارد کلاهبردار هیچ‌گونه ارتباطی با بزه‌دیده نداشته و اساساً شناختی وجود ندارد (مرادی زاده، ۱۳۹۹: ۸۱۰) و رفتار مرتکب (یا رکن مادی این جرم)، از طریق سامانه‌های رایانه‌ای انجام می‌شود. هرچندکه در کلاهبرداری رایانه‌ای نیز حضور بزه‌دیده محتمل است ولی نه در مقام دادن مال بر اثر حیلهٔ مرتکب؛ بلکه به‌عنوان مباشر ضعیف و جاهل بخشی از رفتارهای مورد نظر

1. Victimology

۲. این مثال با فرض احراز سایر شرایط کلاهبرداری مطرح شده است.

مرتکب را انجام می‌دهد. بزه‌دیده در اینجا برخلاف حالت سنتی قصد تسلیم مال به بزهکار را ندارد، ولی بخشی از رفتارها را از باب مباشر جاهل برای سبب اقوی انجام می‌دهد.

### ۲-۲. بزه‌دیدگی محض و رویکرد حمایتی در گونهٔ رایانه‌ای

الگوی بزه‌دیدگی در کلاهبرداری کلاسیک مبتنی بر اغفال مستقیم و بدون واسطهٔ بزه‌دیده است. بدین توضیح که «بزه‌دیده با درجاتی از تقصیر، نقش فعال در کنشگری مجرمانه مرتکب ایفاء می‌کند و به طمع سود بیشتر یا کسب امتیازات دیگر با رضایت و تمایل، مال خود را تقدیم کلاهبردار می‌کند» (میرفردی، ۱۳۹۷: ۲۴).

در کلاهبرداری رایانه‌ای، رکن اغفال و فریب بزه‌دیده به‌گونه‌ای که در کلاهبرداری کلاسیک اشاره گردید، وجود ندارد. بدین معنی که در کلاهبرداری کلاسیک اغفال بزه‌دیده به‌منظور اخذ مال و در نوع رایانه‌ای می‌تواند جهت انجام تمام یا بخشی از رکن مادی، توسط بزه‌دیده ناآگاه باشد. در کلاهبرداری رایانه‌ای در غالب موارد امکان آشنایی و رویارویی میان بزهکار و بزه‌دیده وجود ندارد و اساساً ممکن است هیچ‌گونه ارتباطی میان آن دو برقرار نباشد. بنابراین الگوی بزه‌دیدگی به‌صورت غیرمستقیم است و شخص بزه‌دیده در نتیجهٔ رفتار مرتکب فریب نمی‌خورد، بلکه مرتکب با عملیاتی که علیه سامانهٔ رایانه و سیستم پردازش مربوط به آن انجام می‌دهد، موجب تحصیل مال یا امتیازهای مالی متعلق به دیگری می‌گردد. البته مقنن با ذکر عبارت «... سبب گمراهی سیستم‌های پردازش خودکار یا نظایر آن شود ...» در مادهٔ ۶۷ قانون تجارت الکترونیکی[1] به «فریب» سیستم‌های پردازش خودکار اشاره کرده است که از لحاظ عقلی و منطقی قابل‌پذیرش نمی‌باشد؛ چراکه متعلق اغفال، فریب و گمراهی به‌عنوان اوصاف و خصایص انسانی، لزوماً یک انسان است (طباطبایی، ۱۳۹۴: ۱۴۹). بنابراین عملاً کسی را می‌توان فریب داد یا اسباب گمراهی او را فراهم کرد، که انسان ودارای اراده و اختیار باشد (گلدوزیان، ۱۳۸۰: ۲۸۵).

۱. ماده ۶۷ قانون تجارت الکترونیکی: «هرکس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز از «داده‌پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسائل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده‌پیام»، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظائر آن شود و از این طریق برای خود یا دیگری 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 تا سه سال و پرداخت جزای نقدی معادل مال ماخوذه محکوم می‌شود.

تبصره: شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرّر در این ماده می‌باشد».

در رابطه با مقررهٔ مورد بحث به نظر می‌رسد که این مادهٔ قانونی نسخ جزئی شده است، لکن در شرایطی که تحصیل مال دیگری در بستر مبادلات الکترونیکی صورت گیرد، کماکان به قوت خود باقی است؛ زیرا مقنن در قانون جرایم رایانه‌ای و پس از وضع ماده ۷۴۱ قانون مجازات اسلامی که کلاهبرداری رایانه‌ای را جرم‌انگاری نموده است، صراحتاً اشاره‌ای به نسخ کلی مادهٔ ۶۷ قانون تجارت الکترونیکی نکرده است و از طرفی با توجه به عبارت «در بستر مبادلات الکترونیکی» در صدر مادهٔ ۶۷ قانون تجارت الکترونیکی که خاص بودن آن را نسبت به مقررات عام مادهٔ ۷۴۱ قانون مجازات اسلامی متبادر به ذهن می‌کند (قیاسی و نیک نسب، ۱۳۹۳: ۱۷۴)، می‌توان نتیجه گرفت که عام مؤخر، خاص مقدم را نسخ کلی نکرده است. بنابراین در حال حاضر هر دو مادهٔ مورداشاره قابل‌اجرا هستند، به‌نحوی که اگر رفتار ارتکابی صرفاً در بستر مبادلات الکترونیکی، شرایط مذکور در ماده ۶۷ قانون تجارت الکترونیکی را داشته باشد، مشمول مقررات آن ماده، در غیر این صورت با احراز شرایط مادهٔ ۷۴۱ قانون مجازات اسلامی، رفتار ارتکابی مشمول مقررات عام مادهٔ اخیر قرار خواهد گرفت.

از نظر نگارندگان، منظور قانون‌گذار از عبارت «گمراهی سیستم‌های پردازش خودکار» در مقررهٔ قانونی مورد اشاره، آن است که مرتکب در بستر مبادلات الکترونیکی علیه سیستم پردازش خودکار عملیاتی در رابطه با داده‌های الکترونیکی انجام دهد که سامانه یا سیستم پردازش خودکار به‌مثابهٔ یک سیستم (ونه انسان) دچار خطای محاسباتی شده و با تلقی اینکه کاربر مجاز در حال انجام این عملیات بوده فضای لازم را در اختیار قرار داده و مرتکب از این طریق بتواند مال دیگری را ببرد. با این توضیح واضح است که آنچه به‌عنوان یک برنامهٔ رایانه‌ای برای سیستم پردازش خودکار تعریف می‌شود، متشکل از تعدادی دادهٔ خاص است و سیستم به‌گونه‌ای طراحی شده است که با ورود داده‌ها به آن، عملیاتی از پیش تعریف شده را انجام می‌دهد. درواقع این امر برای سیستم مستلزم آن نیست که به‌کارگیری این داده‌ها صرفاً باید توسط کاربر مجاز صورت پذیرد؛ بلکه اگر کاربر غیرمجاز نیز این داده‌ها را در اختیار داشته باشد یا آنکه اختلال یا تغییراتی در سیستم پردازش ایجاد کند که آن را مجاب به انجام عملیات مورد نظر نمایند، این موضوع توسط قانون‌گذار و با مسامحه به‌عنوان «گمراهی سیستم‌های پردازش خودکار» قلمداد شده است. به بیان دیگر منظور از این عبارت آن است که به‌طور مفروض سیستم پردازش خودکار می‌بایست خدمات الکترونیکی یا رایانه‌ای خود را صرفاً به کاربر مجاز ارائه نماید، اما با عملیاتی که توسط کاربر غیرمجاز یا مرتکب علیه آن انجام شده (که از آن به‌عنوان گمراهی سیستم پردازش خودکار یاد گردید) بزه مذکور محقق خواهد شد.

در کلاهبرداری رایانه‌ای محض، قانون‌گذار دارای رویکرد حمایتی از بزه‌دیده می‌باشد. در این‌گونه از کلاهبرداری در واقع بزه‌دیده نقشی در بردن مالش توسط مرتکب ندارد. هیئت عمومی دیوان عالی

کشور در صدور رأی وحدت‌رویهٔ شمارهٔ ۷۲۹ مورخ ۱۳۹۱/۱۲/۱[1] بر همین رویکرد حمایتی در قبال بزه‌دیدگان جرایم رایانه‌ای محض که مبتنی بر دیدگاه بزه‌دیده شناسی حمایتی[2] بوده، تأکید داشته است. طبق مفاد رأی مذکور، بزه‌دیدهٔ کلاهبرداری رایانه‌ای محض که نقش فعال در محرومیت از مال خود و ارتکاب جرم توسط کلاهبردار نداشته است، چنانچه جهت طرح شکایت و پیگیری حق تضییع شدهٔ خود به محل وقوع جرم که ممکن است بسیار دورتر از محل سکونت وی باشد مراجعه نماید، با تحمیل هزینه و سختی‌های مجدد برایشان، گویی برای بار دوم از جانب نظام عدالت کیفری مورد بزه واقع می‌گردد. بنابراین برای جلوگیری از این موضوع که عادلانه به نظر نمی‌رسد، مراجع قضایی صالح به تحقیق و رسیدگی را مراجع محل افتتاح حساب بزه‌دیده تعیین نمود.

از دیگر موارد رویکرد حمایتی سیاست جنایی قضایی از بزه‌دیدگان جرایم کلاهبرداری رایانه‌ای می‌توان به بخشنامهٔ دادستان کل کشور درخصوص الزام بانک‌ها به جبران خسارت ناشی از عدم اجرای الزامات رمزهای پویا اشاره نمود.[3] با این توضیح به نظر می رسد سیاست جنایی قضایی کشور

۱. رأی وحدت رویهٔ شمارهٔ ۷۲۹ مورخ ۱۳۹۱/۱۲/۱: «نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز ـ مستفاد از ماده ۲۹ ـ مورد تأکید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشد، دادگاهی که بانك افتتاح کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد صالح به رسیدگی است. بنا به مراتب آراء شعب یازدهم و سی و دوم دیوان عالی کشور که بر اساس این نظر صادرشده به اکثریت آراء صحیح و قانونی تشخیص و تأیید می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌ها لازم‌الاتباع است».

2. Supportive victimization

۳. این بخشنامه خطاب به دادستان های سراسر کشور صادر گردیده و متن آن به این شرح است: «باتوجه به اینکه به موجب بخشنامه شماره ۱۸۶۷۱۷/۹۷ مورخ ۱۳۹۷/۶/۱ و بندهای ۱و۳ بخشنامه شماره ۵۱۶۹۱/۹۸ مورخ ۱۳۹۸/۲/۲۱ وشماره ۱۶۳۵۷۵/۹۸ مورخ ۱۳۹۸/۵/۱۴ بانک مرکزی، ارائه خدمات غیرحضوری (نظیرتراکنش‌های بانکی اینترنتی) دربانک‌ها ضرورتاً مستلزم استفاده ازرمزهای پویابوده و ازتاریخ ۱۳۹۸/۳/۱ هرگونه استفاده از رمزهای دوم ایستا درتراکنش‌های غیرحضوری ممنوع اعلام و ادامه بکارگیری رمزدوم ایستا از مصادیق آسیب پذیری امنیتی خدمات بانکی محسوب شده و به عنوان ضمانت اجرا مقرر داشته است که هر گونه سوءاستفاده از حساب‌های مشتریان به دلیل آسیب پذیری‌های امنیتی (ناشی از عدم اجرای الزامات رمزهای پویا) درسرویس‌های بانکی مستقیماً به عهده بانک بوده و در این موارد تأیید مرجع قضایی(دادسرا)، برای جبران خسارت مشتریان کفایت می‌کند، لذا مقتضی است در پرونده‌های کلاهبرداری رایانه‌ای (برداشت غیرمجاز از حساب‌های بانکی) که پس از الزامی شدن استفاده از رمزهای پویا تشکیل شده است بررسی‌های لازم انجام شود و در صورت احراز انجام تراکنش مجرمانه با رمز دوم ایستا ←

در قبال کلاهبرداری رایانه‌ای محض، سعی نموده با مواردی مانند صدور رأی وحدت‌رویه و بخشنامهٔ مورد اشاره تاحدودی نسبت به بزه‌دیده رویکرد حمایتی داشته باشد؛ امری که در رابطه با بزه‌دیدهٔ کلاهبرداری کلاسیک به‌جهت نقش فعال ایشان و نوع رابطهٔ وی با مرتکب در فرایند ارتکاب جرم، مشاهده نمی‌گردد.

در جمع‌بندی مطالب مذکور در این بخش، به‌عنوان یک گزارهٔ افتراقی میان دو شکل بزه‌دیدگی در گونهٔ رایانه‌ای و کلاسیک بر این امر تأکید می‌شود که در کلاهبرداری کلاسیک، بزه‌دیدگی با درجاتی از تقصیر و نقش کم‌وبیش اثرگذار بزه‌دیده در فرایند تکوین جرم همراه است؛ حال آنکه در گونهٔ رایانه‌ای بیش از بزه‌دیده، سامانه یا سیستم پردازش‌گر است که متأثر از رفتار بزهکار دچار گمراهی در مفهوم پیش‌گفته می‌شود که این ضابطه در تشخیص افتراقی بر اساس مؤلفهٔ بزه‌دیدگی حائز اهمیت است.

### ۳. اصالت و موضوعیت ابزار

یکی از شاخصه‌های مهم در تفکیک کلاهبرداری کلاسیک از رایانه‌ای، نوع ابزار یا وسیله‌ای است که توسط مرتکب جهت ارتکاب این جرایم به کار گرفته می‌شود. در این رابطه دیدگاه‌های متفاوتی وجود دارد. به این توضیح که مطابق با دیدگاه مضیق، صرف استفاده از ابزار رایانه‌ای تغییردهندهٔ عنوان مجرمانه کلاهبرداری از کلاسیک به رایانه‌ای نبوده و عنوان مجرمانهٔ کلاهبرداری، از نوع کلاسیک تلقی و مجازات کلاهبردار مشمول قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ می‌باشد. دیدگاه موسع در این رابطه به‌طور کلی بر این ضابطه اصرار دارد که هر گونه کلاهبرداری که از طریق سامانهٔ رایانه‌ای یا مخابراتی صورت گیرد، کلاهبرداری رایانه‌ای محض و در غیر این صورت کلاهبرداری کلاسیک است. دیدگاه سوم که تاکنون به‌صورت دقیق توسط حقوق‌دانان مورد بررسی قرار نگرفته است و مطابق با نظر نگارندگان این پژوهش می‌باشد، آن است که باید قائل به‌تفکیک شد. بدین معنی که هرگاه در بزه کلاهبرداری که در مبدأ و مقصد رفتار ارتکابی آن جرم، دو شخص حقیقیِ (مرتکب و بزه‌دیده) با نقش فعّال و مؤثر حضور داشته باشند، هرچند در این بین بردن مال از طریق عملیات غیرمجاز در رابطه با داده یا مختل کردن سامانه صورت پذیرد، کلاهبرداری از نوع کلاسیک است. البته به شرط آنکه در نتیجهٔ رفتارمرتکب، بزه‌دیده مستقیماً موضوع فریب قرار گرفته باشد. در غیر این صورت در مواردی که مرتکب به تنهایی

به لحاظ عدم رعایت بخشنامه بانک مرکزی وعدم رفع آسیب پذیری امنیتی، دستور پرداخت خسارت بزه دیده صادر و از طریق سامانه کاشف به بانک متخلف ابلاغ گردد».

و بدون حضور فعّال بزه‌دیده، عملیاتی غیرمجاز در رابطه با داده‌ها یا مختل کردن سامانهٔ رایانه‌ای انجام داده باشد و از این طریق مال دیگری را تحصیل نماید کلاهبرداری رایانه‌ای محسوب می‌گردد. به‌عنوان مثال چنانچه شخص «الف» از طریق رایانهٔ شخصی و از طریق نرم‌افزارمخصوص ویرایش تصویر، تغییراتی در عکس‌های ذخیره شدهٔ خود ایجاد و به‌صورت غیرواقعی تصویر خود را به‌عنوان عضو اصلی هیئت مدیره یک شرکت معروف و درحال برگزاری جلسات رسمی آن شرکت تغییر دهد و در ادامه این تصاویر را به شخص «ب» نشان دهد و از این طریق اعتماد وی را با وعدهٔ استخدام در آن شرکت جلب نماید و با فریب شخص «ب» مبلغی را از ایشان به‌عنوان وعدهٔ استخدام تحصیل نماید، اگرچه مرتکب تغییراتی در داده‌ها (عکس‌های ذخیره شده در رایانهٔ شخصی) ایجاد نموده است، لکن پرواضح است که این عملیات صرفاً به‌عنوان بخشی از کلاهبرداری کلاسیک و تحت عنوان «توسل به وسایل متقلبانه» محسوب می‌گردد؛ ازاین‌رو از شمول کلاهبرداری رایانه‌ای خارج است.

### ۱-۳. الزامات غیرابزاری در تکوین رفتار در ارتباط با کلاهبرداری کلاسیک

در کلاهبرداری کلاسیک نه‌تنها نقش مؤثری برای ابزار مشخص پیش‌بینی نشده است، حتی در برخی اشکال ارتکاب رفتار در رکن مادی چنین مستفاد می‌شود که ارتکاب برخی رفتارهای متقلبانهٔ محض انسانی مانند ترساندن همراه با فریب دیگری، بدون به‌کارگیری و استفاده از ابزارهای متقلبانهٔ دیگری قادر به تکوین بزه مورد نظر خواهد بود. فارغ از چالش‌های نظری مرتبط با تفسیر مذکور، آنچه مسلّم است مقنن در رابطه با کلاهبرداری کلاسیک بر مفهوم «تقلب» اصرار ویژه داشته است، به‌گونه‌ای که هر رفتاری و با استفاده از هر ابزاری اعم از ساختگی و اصیل، می‌باید در یک فرایند از پیش‌طراحی شده منجر به شکل‌گیری مفهومی مرکب به نام «تقلب» شود، بنابراین حتی با فرض فریب مخاطب و دریافت مال از او، چنانچه در شکل‌گیری مفهوم مذکور با تأکید بر معیار نوعی[1] تردید ایجاد شود، بزه مورد نظر محقق نخواهد بود. درمقابل در کلاهبرداری رایانه‌ای، «ابزار» نقش محوری را با «کارکرد فنی» خود در تحقق جرم ایفا می‌نماید، که لزوماً منجر به تحقق مفهوم «تقلب» نمی‌شود؛ مانند مواردی که شخصی با استفاده از رایانهٔ شخصی مبادرت به ارسال بدافزاری نماید که سیستم برق‌رسانی سامانهٔ هدف را از کار انداخته و به راحتی امتیازات مالی را تحصیل نماید، رفتار وی با وجود ماهیت تهاجمی و قهرآمیز آن، مصداق بزه کلاهبرداری رایانه‌ای خواهد بود؛ لیکن در بزه کلاهبرداری کلاسیک، ابزار

۱. یعنی مطابق با قضاوت عرف جامعه، ابزار و وسایلی که مرتکب به وسیلهٔ آن‌ها کلاهبرداری می کند، متقلبانه محسوب شوند.

مشخصی مدنظر مقنن نبوده است و آنچه در خلال ارتکاب رکن مادی واجد وصف موضوعیت می‌باشد، «تحقق وصف تقلب» است. البته مطابق با نظریهٔ مشورتی شماره ۷/۲۳۵۰ مورخ ۱۳۷۳/۴/۴ اداره حقوقی قوه قضائیه[1] به امکان کلاهبرداری از «دولت» به‌عنوان یک شخص حقوقی اشاره شده است. شخص حقوقی مانند دولت مطابق با تعریفی عبارت است از «گروهی از افراد انسان یا منفعتی از منافع عمومی که قوانین موضوعه آن را در حکم شخص طبیعی و موضوع حقوق و تکالیف قرار داده باشد. مانند شرکت تجاری و انجمن‌ها و دولت و شهرداری‌ها» (جعفری لنگرودی، ۱۳۷۸: ۳۷۸). زمانی که کلاهبرداری علیه دولت به‌عنوان شخص حقوقی ارتکاب یابد، در حقیقت افراد و انسان‌ها به‌عنوان نمایندهٔ دولت یا مدیرعامل آن نهاد یا سازمان دولتی اغفال شده و در نتیجه اموال دولت که در اختیار ایشان است تحویل کلاهبردار می‌شود. در این حالت مانند نظریهٔ مشورتی مذکور با مسامحه گفته می‌شود که کلاهبرداری علیه دولت صورت گرفته است، در حالی که در واقع بزه‌دیده‌ای که نقش فعال در ارتکاب کلاهبرداری داشته، انسان می‌باشد.

در رابطه با تحقق و شکل‌گیری رفتار مجرمانه در کلاهبرداری کلاسیک، شرایط و الزامات دیگری مانند مال بودن موضوع جرم، تعلق مال به دیگری و... وجود دارد که به‌جهت پرهیز از تکرار کلام تنها به موارد پیش‌گفته بسنده می‌گردد.

### ۲-۳. قیود ناظر به ماهیت تقنینی ابزار و کارکرد فنی در گونهٔ رایانه‌ای

با درنظر داشتن منطوق ماده ۷۴۱ قانون مجازات اسلامی، که موضوع بحث این بخش را تشکیل می‌دهد، تأکید مقنن بر الفاظی است که دربرگیرندهٔ لزوم توجه به ماهیت «ابزار» در خلال ارتکاب رفتار، در بخش رکن مادی این جرم است. بر این ملحوظ بر این گزاره تأکید می‌شود که چنانچه هر یک از طرق ارتکاب رفتار مشتمل برمحو، ایجاد یا توقف داده یا اختلال در سامانه، با استفاده از ابزاری به غیر از آنچه درصدر این مستند قانونی مورد تصریح مقنن قرار گرفته است انجام شود، موضوع از شمول این مستند قانونی خارج خواهد بود. به‌عنوان مثال چنانچه شخصی با استفاده از یک دستگاه دوربین فیلمبرداری دیجیتال مدرن مبادرت به تغییر داده‌های تصویری مانند QR

۱. نظریه مشورتی شماره ۷/۲۳۵۰ مورخ ۱۳۷۳/۴/۴: «با توجه به تعریفی که ماده یک قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری از بزه کلاهبرداری نموده است، قید «دیگری» مذکور در آن ماده اعم خواهد بود از دولت یا سایر اشخاص و با این ترتیب می‌توان گفت کلاهبرداری از افراد عادی نسبت به دولت هم می‌تواند مصداق داشته باشد و ذکر کلمه «مردم» در قانون از باب غالب است، زیرا غالباً کلاهبرداری از مردم صورت می گیرد و اختصاص به غیر دولت ندارد.»

CODE[۱] تجاری نموده و با ذخیره نمودن آن در یک حامل داده مانند فلش USB[۲] و وارد نمودن آن به دستگاه پردازشگر مبادرت به دریافت کالا یا امتیاز مالی نماید، رفتار وی مصداق کلاهبرداری رایانه‌ای نخواهد بود. همچنین لزوم احراز «رابطهٔ انتساب مؤثر» میان وسایل و ابزار مذکور و نتیجه محقق از سیاق نگارش این مستند قانونی مستفاد می‌شود. به این توضیح که علاوه بر لزوم استفاده از ابزار مشخص (سامانهٔ رایانه‌ای و مخابراتی)، ضروری است کارکرد «فنی» سامانه‌های مذکور از قبیل پردازش و در مجموع هوش مصنوعی آن، منجر به نتایج مذکور در مادهٔ ۷۴۱ قانون مجازات اسلامی شود. بنابراین در مواردی که سامانه یا ابزار رایانه‌ای نه از حیث کارکرد اساسی و پیش‌فرض آن، بلکه با اِعمال تغییرات به‌عنوان وسیله‌ای فاقد مختصات یک وسیله یا سامانهٔ مخابراتی یا رایانه‌ای مورد استفاده قرار گیرد، رفتار مرتکب حتی با وجود سایر شرایط مصداق بزه کلاهبرداری رایانه‌ای نخواهد بود. به‌عنوان مثال چنانچه شخص گوشی تلفن همراه خود را با اعمال تغییراتی تبدیل به ابزار شوک‌دهندهٔ الکتریکی ضعیف نموده و با نزدیک کردن آن به سامانهٔ شارژ کارت‌های تردد مترو[۳] و ایجاد اخلال در آن مبادرت به شارژ کارت خود نماید، رفتار وی مصداق بزه کلاهبرداری رایانه‌ای نخواهد بود؛ چراکه چنین ابزاری هرچند به ظاهر وسیله و سامانهٔ مخابراتی است، لکن ارتکاب عمل مجرمانه نه با استفاده از کارکرد رایانه‌ای یا مخابراتی آن، بلکه با استفاده از ظرفیت و توان الکترونیکی آن انجام شده است. بر این اساس با بررسی مقررهٔ مربوط به کلاهبرداری رایانه‌ای در قانون مجازات اسلامی مشخص می‌شود که جهت تحقق جرم مذکور باید قائل به موضوعیت داشتن ابزار ارتکاب این جرم بود. بدین صورت که عملیات مجرمانه از طریق داده‌های غیرمجاز در سامانهٔ رایانه‌ای در مبدأ آغاز و در نهایت عملیات غیرمجاز علیه داده‌ها در مقصد، مجدداً توسط سامانه پردازش شده و در غالب موارد بدون آنکه بزه‌دیده مطلع گردد، اموال ایشان در تصرف مرتکب قرار می‌گیرد (نجفی ابرندآبادی، ۱۳۸۸: ۱۱).

تفاوت ظریف دیگری که مرز بین کلاهبرداری کلاسیک از رایانه‌ای را در اینجا مشخص می‌نماید، آن است که در کلاهبرداری رایانه‌ای عملیات غیرمجاز علیه داده‌ها (مانند اموال مادی در

۱. مخفف Quick response code (کد پاسخ سریع) که دردسترسی سریع به اطلاعات در فضای سایبرو دیجیتال کاربرد دارد.

۲. مخفف Universal serial bus (گذرگاه سریال عمومی) که یک استاندارد صنعتی است که درآن، کابل ها و پروتکل های ارتباطی گذرگاه (باس) برای اتصال، ارتباط و هم چنین منبع تغذیه که بین رایانه و دستگاه الکترونیکی به کار می‌رود، تعریف شده است.

۳. قطار زیرزمینی درون شهری، جهت حمل و نقل روزانه مردم.

کلاهبرداری کلاسیک) که منجر به بردن مال دیگری می‌شود غالباً توسط مرتکب صورت می‌گیرد (نوری و دیگران، ۱۳۸۳: ۲۳) و یک شخص حقیقی دیگر به‌عنوان بزه‌دیده، نقش مؤثر و فعّال در تکوین این فرایند مجرمانه ندارد؛ هرچند گاهی ممکن است بخشی از رفتار مادی یا تمام آن توسط خود بزه‌دیده، به‌عنوان مباشر جاهل انجام شود. در مقابل در کلاهبرداری کلاسیک موضوع اندکی متفاوت است. به تعبیر دیگر دو شخص حقیقی در تحقق جرم نقش فعال دارند. بنابراین اگر مداخله در داده‌ها و سیستم رایانه‌ای به‌طور مستقیم موجب تصاحب یا انتقال اموال دیگری به مرتکب یا شخص دلخواه وی نشود و یک شخص حقیقی واسطهٔ تصاحب و یا انتقال اموال قرار گیرد، کلاهبرداری رایانه‌ای تحقق نخواهد یافت (خرم‌آبادی، ۱۳۸۶: ۹۴). به‌عنوان مثال چنانچه از ناحیهٔ مرتکب ایمیل با محتوای پذیرش اقامت در کشور خارجی برای دیگری ارسال و تقاضای واریز مقداری وجه به شماره حساب اعلامی مطرح شده باشد؛ در نتیجه بزه‌دیده اغفال گردیده و با مراجعه به دستگاه خودپرداز بانکی مبلغ مورد نظر را برای کلاهبردار کارت به کارت و منتقل نماید، در این حالت شاهد استفاده از ابزار رایانه‌ای صرفاً جهت اغفال بزه‌دیده می‌باشیم؛ زیرا که بزه‌دیده با رضایت خود مال را به مرتکب تحویل می‌دهد و این موضوع با کلاهبرداری رایانه‌ای محض که مالباخته نقشی در تحویل یا رضایت در ارائه مال به مرتکب ندارد، متفاوت است.

### ۳-۳. مدل حل مسئله در رویهٔ قضایی

تاریخچهٔ شکل‌گیری جرایم رایانه‌ای در ایران نسبت به سایر کشورها محدود به سه دههٔ اخیر می‌باشد؛ زیرا زمان ورود رایانه به کشور سال ۱۳۴۰ شمسی و پیوستن ایران به شبکه جهانی اینترنت و به‌تبع آن افزایش تعداد کاربران شخصی رایانه و اینترنت مربوط به دههٔ ۱۳۷۰ می‌باشد. بنابراین استفاده از فناوری اطلاعات و رایانه رواج چندانی نداشت و کمتر شاهد سوءاستفاده‌ها و تخلفات رایانه‌ای بودیم. به مرور و با مشاهدهٔ افزایش تدریجی تخلفات و رفتارهای غیرقانونی مرتبط با سیستم‌های الکترونیکی و رایانه‌ای، لزوم جرم‌انگاری این رفتارها توسط قانون‌گذار احساس که در نهایت منجر به تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲ و قانون جرایم رایانه‌ای مصوب ۱۳۸۸ گردید. یکی از مهم‌ترین دلایل کثرت ارتکاب کلاهبرداری رایانه‌ای محیط خاص ارتکاب آن است. فضای سایبر و اینترنت به‌دلیل ماهیت خود به‌صورت ذاتی موقعیت و شرایط ارتکاب جرم را در دسترس کاربران خود قرار می‌دهد. به همین سبب یعنی فراهم بودن شرایط و موقعیت سهل ارتکاب جرم، موجب افزایش چشمگیر این نوع کلاهبرداری شده است (Broadhurst, 2006: 19).

داده‌ها یا سیستم رایانه‌ای به‌عنوان ابزار ارتکاب جرایم رایانه‌ای دارای جنبهٔ فنی و تخصصی می‌باشند و این موضوع بسیاری ازمحاکم کیفری را در آشنایی با اصطلاحات فنی مربوط به رایانه،

نحوهٔ عملکرد و پردازش داده‌ها در سیستم رایانه‌ای و نهایتاً چگونگی ارتکاب جرم توسط این ابزار با مشکل مواجه می‌سازد. از سوی دیگر مقنن در قوانین پیش‌گفته ضمن جرم‌انگاری جرایم رایانه‌ای با پیش‌بینی یک یا دو مادهٔ قانونی به ذکر کلی برخی از این اصطلاحات اکتفا نموده است. برای نمونه با ذکر اصطلاح «مختل نمودن سامانه» در مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) مشخص نمی‌باشد که منظور و تعریف مقنن از اختلال در سامانه چیست؟ چه مواردی به‌عنوان مصادیق اختلال در سامانه تلقی می‌شوند؟ آیا این اختلال باید توسط مرتکب باشد یا اگر به علت قطعی سراسری برق صورت گیرد و مرتکب مال دیگری را ببرد آیا باز هم کلاهبرداری رایانه‌ای محسوب می‌گردد؟ و....

مسئلهٔ دیگر که به‌عنوان چالش رویهٔ قضایی محاکم کشور در رسیدگی به جرم کلاهبرداری رایانه‌ای تلقی می‌گردد، شباهت فراوان برخی مصادیق رایانه‌ای این جرم با شکل کلاسیک آن است. در هر دوی این جرایم شخص مرتکب با وسایل متقلبانه (در کلاسیک) و غیرمجاز (در رایانه ای) مال دیگری را تصاحب می‌کند. لکن برخی از محاکم مطابق با یک دیدگاه هر گونه کلاهبرداری با ابزار رایانه‌ای را کلاهبرداری رایانه‌ای محض تلقی و در مقابل عده‌ای دیگر معتقدند که کلاهبرداری با ابزار رایانه‌ای تحت شرایطی که اهّم آن در مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) ذکر شده، کلاهبرداری رایانه‌ای محض است و در غیر این صورت کلاهبرداری کلاسیک محسوب می‌شود. همین اختلاف دیدگاه موجب عدم یکپارچگی رویهٔ قضایی کشوردر برخورد با این مسئله قضایی در ابعاد مختلف وبه طورخاص تشخیص صلاحیت گردیده است که در نتیجه هم اکنون شاهد صدور آرای متفاوت در یک موضوع واحد، از محاکم کیفری مختلف می‌باشیم.

### ۴-۳. توسیع مصادیق به نفع گونه رایانه‌ای با تمرکز بر ابزار و کاربر

همان طور که ذکر گردید در دیدگاه موسع به‌طور مطلق چنانچه مرتکب به هر نحوی با ابزار رایانه‌ای انسان دیگری را فریب داده و اموال او را تصاحب کند، کلاهبرداری از گونهٔ رایانه‌ای می‌باشد. به عبارت دیگر آنچه موضوعیت دارد حضور یک شخص حقیقی به‌عنوان کاربر است که از طریق سیستم رایانه‌ای به‌عنوان وسیله یا ابزار، مال دیگری را تصاحب نماید. مطابق با این دیدگاه، به نظر می‌رسد اینکه داده‌ها یا سیستم رایانه‌ای به چه نحوی به کار گرفته شود که در نتیجه آن بزه‌دیدهٔ اغفال شده و با رضایت خود، مال را تحویل کلاهبردار نماید، ملاک و ضابطهٔ تشخیص نمی‌باشد. دادنامهٔ صادره از شعبه ۱۰۷ کیفری دو دادگاه‌های عمومی خرم آباد با شماره ۱۴۰۰۳۶۳۹۰۰۰۱۱۶۰۶۵۵ مربوط به پرونده شماره کلاسه ۹۹۰۹۹۸۶۶۱۲۴۰۰۶۰۴ در راستای دیدگاه مورد بحث صادر شده

است.[۱]

در این رأی جهت گیری مقام قضایی به دیدگاه موسّع مبتنی بر ابزار کاملاً مشهود است. به این معنی که صرف به‌کارگیری ابزار رایانه‌ای موجب می‌گردد که جرم کلاهبرداری مشمول مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) شود.

در منابع حقوقی موجود، دفاع نظری قابل‌قبولی از این دیدگاه مشاهده نمی‌شود و استدلال خاصی نیز ارائه نگردیده است؛ از سوی دیگر با بررسی نصّ قانونی مذکور به دشواری می‌توان گفت که آنچه به‌عنوان موضوع شکایت دررأی مذکور مطرح گردیده، کلاهبرداری رایانه‌ای تلقی گردد.

در تحقق کلاهبرداری رایانه‌ای ضروری است از طریق عملیات غیرمجاز در رابطه با داده‌های اینترنتی یا مختل کردن سامانه، مال یا امتیاز مالی دیگری توسط مرتکب تحصیل گردد. در رأی مورد اشاره رفتارمتهم فاقد چنین خصوصیتی می‌باشد، چراکه از سامانهٔ رایانه‌ای صرفاً به‌عنوان ابزاری جهت فریب بزه‌دیده به‌عنوان جزئی از رکن مادی کلاهبرداری کلاسیک استفاده شده است.[۲] بدون تردید دیدگاه موسّع درخصوص تلقی چنین مواردی به‌عنوان کلاهبرداری رایانه‌ای، بدون مبنای استدلالی قابل‌قبول بوده و در مغایرت با اصل تفسیر منطقی نصوص قانونی در حقوق کیفری قرار دارد. همچنین در صورتی که قائل به تفسیر موسّع به شرح پیش گفته باشیم، تغییرات اساسی در فرایند ماهوی و شکلی دادرسی ایجاد می‌گردد؛ ازجمله تغییر در نوع مجازات، قابل‌گذشت بودن یا نبودن کلاهبرداری حسب کلاسیک یا رایانه‌ای بودن آن،[۳] تعیین دادگاه صالح و... که در کلاهبرداری کلاسیک و رایانه‌ای با هم متفاوت می‌باشند.

۱. خلاصه مفاد رای مذکور بدین شرح است: « ... راجع به اتهام آقای ا.م.م دائر بر کلاهبرداری رایانه ای به میزان هفده میلیون ریال، موضوع شکایت خانم ش.ن.ف و کیفرخواست شماره ۱۴۰۰۳۶۴۳۰۰۰۰۰۵۹۶۵۶ صادره از دادسرای عمومی و انقلاب خرم آباد، دادگاه ضمن تدقیق در محتویات پرونده امرونظر به اینکه بزه کلاهبرداری رایانه ای در حوزه قضایی شهرستان چگنی به وقوع پیوسته چرا که بانک محل افتتاح حساب زیان دیده در آن حوزه قضایی می باشد(صفحه ۱۴ پرونده)، بنابراین دادگاه با تاکید براستدلال پیشین، مستنداً به رای وحدت رویه شماره ۷۲۹- ۱۳۹۱/۱۲/۱ هیات عمومی دیوان عالی کشور ومواد ۳۱۰ و۳۴۱ قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۱۲/۴ بااصلاحات بعدی، قرار عدم صلاحیت به اعتبار، شایستگی وصلاحیت محاکم کیفری دو شهرستان چگنی صادر و اعلام می نماید. رأی صادره قطعی است».

۲. شرح مختصر ماوقع پرونده، در بخش بعدی مقاله ذکر می شود.

۳. مطابق با نظر نگارندگان کلاهبرداری رایانه‌ای از زمرهٔ جرایم غیرقابل‌گذشت می‌باشد و تصویب قانون کاهش مجازات حبس تعزیری سال ۱۳۹۹ تاثیری در تغییر این وصف نداشته است.

### ۵-۳. تضییق دامنهٔ مصادیق در جهت کلاهبرداری کلاسیک

دیدگاه مضیّق در رابطه با تعیین مصادیق کلاهبرداری رایانه‌ای، قائل به محدود بودن مصادیق این جرم با در نظر داشتن کیفیت رکن مادی به شرح مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) می‌باشد. در واقع منشأ چنین برداشتی اعتقاد به نص‌گرایی است که مانع از هرگونه تفسیردرخصوص نص قانون می‌شود (الماسی و واعظی، ۱۴۰۱: ۲و۳). مطابق با این دیدگاه، زمانی کلاهبرداری از طریق سامانهٔ رایانه‌ای از نوع رایانه‌ای محض می‌باشد که مرتکب یا از طریق عملیاتی غیرمجاز در رابطه با دادهٔ اینترنتی و یا مختل نمودن سامانه، از مال یا خدمات مالی دیگری بهره‌مند شود. در غیر این صورت به معنی فقدان هر یک از شرایط مذکور، عمل وی مصداق کلاهبرداری کلاسیک خواهد بود. بنابراین به کارگیری سامانه رایانه‌ای در کلاهبرداری به دوشکل می‌باشد:

به‌کارگیری رایانه به‌عنوان وسیلهٔ کلاهبرداری کلاسیک، به این نحو که مرتکب از طریق سامانه رایانه‌ای به وسایل متقلبانه متوسل شود، سپس باعث اغفال دیگری شده و مال او را ببرد. در اینجا رایانه صرفاً وسیلهٔ ارتکاب جرم بوده و نوع ابزار یا وسیله در تغییر نوع کلاهبرداری از کلاسیک به رایانه‌ای مؤثرنیست. بر همین اساس موضوع مشمول ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ می‌باشد.

استفاده از سامانهٔ رایانه‌ای جهت کلاهبرداری رایانه‌ای محض، بدین صورت که مرتکب بدون آنکه مبادرت به فریب بزه‌دیده نماید، از طریق مداخلهٔ غیرمجاز در داده‌های رایانه‌ای یا اختلال در عملکرد سامانهٔ رایانه‌ای هم در مبدأ و هم در مقصد، مال یا امتیاز و خدمات مالی متعلق به دیگری را تصاحب نماید. در اینجا کلاهبرداری از نوع رایانه‌ای و مشمول مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) محسوب می‌گردد. دادنامهٔ شمارهٔ ۱۴۰۰۳۶۳۹۰۰۰۱۳۰۸۱۳۲ مربوط به پرونده کلاسهٔ ۹۹۰۹۹۸۶۶۱۲۴۰۰۶۰۴ مورخ ۱۴۰۰/۴/۲۳ از شعبهٔ ۱۰۱ دادگاه کیفری دو شهرستان چگنی تحت تأثیر دیدگاه مورد اشاره صادر شده است.[1] در این رأی قاضی صادرکننده به درستی به

۱. مفاد رأی مختصراً به شرح ذیل می باشد: «... در این پرونده شاکی خانم ش.ن با تقدیم شکواییه ای به تاریخ ۱۳۹۹/۷/۲۲ علیه آقای ا.م.م ... مدعی وقوع بزه کلاهبرداری رایانه‌ای گردیده است. به این توضیح که در تاریخ ۱۳۹۹/۷/۲۲ از طریق برنامه دیوار شهر تهران، کالای مورد نیاز خود را که عبارت است از یک دستگاه ماشین شارژی (اسباب بازی) جستجو و پس ازتماس با شخصی که خود را مالک آن معرفی نموده است (ا.م.م) و اعلام موضوع به وی، تصاویر و فیلم ماشین شارژی از سوی مالک برای ایشان ارسال و این گونه توافق می‌شود که پس از ارسال کالا ازسوی فروشنده وارسال رسید باربری که حکایت از ارسال کالا از سوی فروشنده دارد، مبلغ کالا شامل یک میلیون و ←

محدود بودن دامنهٔ مصادیق جرایم رایانه‌ای اشاره و آن را یک امر استثنایی تلقی و بر این امر تأکید شده است که در کلاهبرداری رایانه‌ای کنشگری مجرمانه مرتکب از طریق وسیلهٔ رایانه‌ای می‌باشد؛ لکن کنش‌پذیری متوجه سیستم پردازش رایانه می‌باشد نه قربانی به‌عنوان یک شخص حقیقی. بر این اساس با وجود استفاده از سامانهٔ رایانه‌ای در مبدأ و استفادهٔ غیرمجاز از داده‌ها به‌دلیل اینکه عملیات مورد نظر متوجه سامانه رایانه‌ای در مقصد نبوده است چنین مواردی را کلاهبرداری کلاسیک تلقی نموده است.

**نتیجه**

ابزارهای رایانه‌ای به اشکال و انحاء مختلفی در خلال ارتکاب جرم کلاهبرداری مورد استفاده قرار می‌گیرد که این امر در صورت عدم توجه کافی می‌تواند تشخیص گونهٔ کلاهبرداری کلاسیک از رایانه‌ای را با دشواری مواجه سازد؛ اما به‌کارگیری سه ضابطهٔ عینی مستنبط از مفهوم و منطوق مادهٔ ۷۴۱ قانون مجازات اسلامی (جرایم رایانه‌ای) در تفکیک دو شکل از کلاهبرداری راهگشا خواهد بود.

ضابطهٔ اول ناظر به ماهیت رایانه‌ای یک ابزار است. مطابق با این مفهوم، «رایانه‌ای»، وصفی ذاتی برای یک ابزار است که اقتضای آن قابلیت پایش و پردازش است. بنابراین ابزاری که در کلاهبرداری رایانه‌ای مورد استفاده قرار می‌گیرد هرچند از نقطه نظر فنی و تکنولوژیک دارای فناوری پیچیده‌ای باشد، تا زمانی که فاقد قابلیت مذکور باشد، کلاهبرداری انجام شده رایانه‌ای نخواهد بود. ضابطهٔ دوم مربوط به تنوع کارکرد یک ابزار رایانه‌ای است. ابزارهای رایانه گاهی به‌صورت تخصصی، فنی و با مکانیزمی فعّال مورد استفاده قرار می‌گیرند و نقش محوری در بروز اخلال در فرایند پردازش

هفتصد هزار تومان وجه نقد را برای فروشنده واریز می نماید، اما به محض واریز وجه متوجه خاموش شدن خط تلفن همراه مندرج در برگه باربری و همچنین تلفن همراه فروشنده شده ... با این شرح بزه موردنظر به هیچ وجه ماهیت رایانه ای نداشته و به نظر این دادگاه استناد دادسرا و دادگاه محترم شهرستان خرم‌آباد به ماده ۷۴۱ ازقانون تعزیرات صحیح نمی باشد، با این توضیح که اصولاً ۱- ... ۲- ... ۳- «ابزار» مورد استفاده در جرایم رایانه‌ای که وجه افتراق سوم این جرم با سایر جرایم است صرفاً در «داده های قابل ارزیابی مربوط به فضای دیجیتال» است که درقالب متن، صوت، تصویروفیلم و ... قابل شناسایی است ... به طور خلاصه در این پرونده شخص حقیقی موضوع اغفال و فریب است و هیچ اختلال یا اخلالی در فرایند پردازش سامانه رایانه‌ای یا مخابراتی صورت نگرفته است ... بااین توضیح این دادگاه با تاکید بر اینکه اثرگذاری رفتار متهم در قالب توسط به وسایل متقلبانه و رویت این موارد درشهرستان خرم آباد توسط شاکیه و اغفال و فریب مشارالیها و بردن مال که به عنوان نتیجه درجرم کلاهبرداری در سیطره نظام بانکی در تمام شعب بانکی سراسر کشوردرشهرستان خرم آباد ازحساب شاکیه خارج ودراختیار متهم قرار گرفته است، مستنداً به ماده ۳۱۰ ازقانون آیین دادرسی کیفری مصوب ۱۳۹۲ شهرستان خرم‌آباد را صالح به رسیدگی دانسته و مبادرت به صدورقرارعدم صلاحیت می نماید. ...».

در سامانهٔ مقصد دارند؛ لیکن در مواردی این ابزارها صرفاً به‌عنوان بخشی از مانور متقلبانه در استخدام افراد قرار می‌گیرند و عملکرد آن‌ها در این شکل از کارکرد عمدتاً متوجه مخاطب انسانی می‌شود که در تحقق کلاهبرداری رایانه‌ای صرفاً کارکرد فنی این ابزار مدنظر است. و در نهایت ضابطهٔ سوم مربوط به نحوهٔ تعامل دو ابزار یا سامانهٔ رایانه‌ای است. در این چهارچوب ضروری است ارتباط میان ابزار رایانه‌ای مورد استفاده توسط کلاهبردار با سامانهٔ هدف در فضای دیجیتال که قابلیت دادوستد داده‌ها (در زنجیرهٔ صفر و یک) در آن فراهم است صورت گیرد (Lorena Montoya, Marianne Junger, Pieter Hartel, 2013: 31-32).

مطابق با این معیار لازم است که رفتار مجرمانه از ابتدای فرایند تکوین جرم (کلاهبرداری رایانه‌ای) تا حصول قطعی نتیجهٔ مجرمانه (کسب مال یا منفعت مالی) در فضای مذکور انجام شود و از مفهوم مخالف این گزاره چنین برمی آید که چنانچه تمام یا بخش مؤثری از رکن مادی در خارج از فضای مذکور انجام شود، در تحقق کلاهبرداری رایانه‌ای تردید جدی ایجاد خواهد شد. این معیارها ناشی از ارزیابی منطقی و مفهومی مادهٔ ۷۴۱ مذکور می‌باشد که با کمک مطالعهٔ منابع رسمی موجود استحصال و به کار گرفته شده است. بنابراین امکان درک متفاوت از حکم مقنن همواره وجود دارد و به همین منظور پیشنهاد می‌شود این سه معیار به‌عنوان وجوه تمایز کلاهبرداری رایانه‌ای از طریق اصلاحات تقنینی یا توسط ظرفیت‌های تکمیلی موجود مانند صدور رأی وحدت‌رویه از طریق هیئت عمومی دیوان عالی کشور، جهت ارشاد الزامی مراجع قضایی احصا شود.

## منابع

### فارسی


- الماسی مسعود و احمد واعظی (۱۴۰۱)، «پوزیتویسم حقوقی در نظام قضایی ایران؛ برایندتعاملی فرمالیسم حقوقی و نص گرایی قانونی»، **مجله حقوقی دادگستری**، دوره ۸۶، شماره ۱۱۷.
- باستانی، برومند (۱۳۸۳)، **جرایم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری**، تهران: انتشارات بهنامی.
- تبریزی، صادق، حسن عالی پور و محمدرضا الهی‌منش (۱۴۰۱)، «اصل تناسب در توقیف داده و سامانه در فرایند کیفری»، **مجله حقوقی دادگستری**، دوره ۸۶، شماره ۱۱۷.
- جعفری لنگرودی، محمدجعفر (۱۳۷۸)، **مبسوط در ترمینولوژی حقوق**، تهران: انتشارات گنج دانش.
- جلالی فراهانی، امیرحسین (۱۳۸۹)، **درآمدی بر آیین دادرسی کیفری جرایم سایبری**، چاپ اول، تهران: انتشارات خرسندی.
- حبیب زاده، محمدجعفر (۱۳۸۰)، **حقوق جزای اختصاصی، جرایم علیه اموال**، چاپ اول، تهران: انتشارات سمت.
- خرم آبادی عبدالصمد (۱۳۸۶)، «کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران»، **فصلنامه حقوق دانشکده حقوق و علوم سیاسی تهران**، دوره ۳۷، شماره ۲.
- رستمی، هادی (۱۳۹۸)، «کلاهبرداری رایانه ای، تاملی بر ارکان جرم وآثار آن»، آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، دوره ۱۶، شماره ۱۸ .
- رحیمی نژاد، اسماعیل (۱۳۸۸)، **جرم‌شناسی**، چاپ اول، تبریز: نشر فروزش.
- زررخ، احسان (۱۳۸۹)، «بزه‌دیده شناسی سایبری»، **فصلنامه مجلس و پژوهش**، سال ۱۷، شماره ۶۴ .
- دزیانی، محمدحسن (۱۳۷۶)، **جزوه «جرایم کامپیوتری»**، جلد دوم، تهران: خبرنامه تخصصی انفورماتیک (نشریه دبیرخانه شورای عالی انفورماتیک کشور).
- طباطبایی سیدحسین (۱۳۹۴)، «بررسی تطبیقی کلاهبرداری رایانه‌ای با کلاهبرداری سنتی بانگاه به امنیت تجاری الکترونیکی»، **مجله پژوهش‌های حقوق جزا و جرم‌شناسی**، دوره ۳، شماره ۶ .
- عالی پور، حسن (۱۳۸۳)، «کلاهبرداری رایانه ای»، مجله پژوهش‌های حقوقی، مؤسسه مطالعات و پژوهش‌های حقوقی، دوره ۳، شماره ۶ .
- علی نژادی محسن و علی نژادی زهرا (۱۳۹۷)، «بررسی آثار جرم کلاهبرداری در تجارت الکترونیک»، **فصلنامه علمی - حقوقی قانون یار**، دوره ۲، شماره ۵.
- قناد، فاطمه (۱۳۸۷)، «کلاهبرداری الکترونیکی دربسترفناوری‌های اطلاعات و ارتباطات»، مجله پژوهش و سیاست، دوره ۱۰، شماره ۲۵.
- قیاسی جلال الدین و عباسعلی نیک نسب (۱۳۹۳)، «تحصیل متقلبانه خدمات»، **پژوهشنامه حقوق کیفری**، دوره ۵، شماره ۲.
- گلدوزیان ایرج (۱۳۸۰)، **حقوق جزای اختصاصی، جرایم علیه تمامیت جسمانی، صدمات معنوی، اموال ومالکیت، امنیت وآسایش عمومی**، تهران: انتشارات دانشگاه تهران.
- مرادی زاده، کیوان (۱۳۹۹)، «بررسی جزایی ابعاد و ارکان جرم کلاهبرداری رایانه ای»، **فصلنامه علمی - حقوقی**

**قانون یار**، دوره ۴، شماره ۱۵.

- محسنی، فرید (۱۳۹۴)، **جرم‌شناسی**، چاپ اول، تهران: انتشارات دانشگاه امام صادق (ع) .
- میرفردی، عبداله (۱۳۹۷)، **کلاهبرداری سایبری در حقوق کیفری ایران: باتاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا**، چاپ اول، تهران: انتشارات هوشمند تدبیر.
- نجفی ابرند آبادی، علی حسین (۱۳۸۸)، «ازجرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، دیباچه برویراست دوم در: پیکا ژرژ، **جرم‌شناسی**، چاپ چهارم، تهران: انتشارات میزان.
- نوری، محمد علی و دیگران (۱۳۸۳)، **جرایم رایانه‌ای**، چاپ اول، تهران: انتشارات گنج دانش.
- ویلیامز، ماتیو (۱۳۹۱)، **بزهکاری مجازی، بزه، انحراف و مقررات گذاری برخط**، تهران: انتشارات میزان.

## لاتین

- Broadhurst, Robert (2006), Development in the global law enforcement of cyber-crime, An **international journal of police strategies and management**.
- Catherin Elliot and Frances Quinn (2010), **Criminal Law**, Pearson Education Limited, England, 8th Edition.
- Lorena Montoya, Marianne Junger, Pieter Hartel (2013), How 'Digital' is Traditional Crime? 2013 European Intelligence and Security Informatics Conference, sewden.
- Noel cross (2010), **criminal law and criminal justice**, an introduction, sage publication, first published.