آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، دورهٔ شانزدهم، شمارهٔ ۱۸، پاییز ـ زمستان ۱۳۹۸
**نوع مقاله: علمی ـ پژوهشی**

# کلاهبرداری رایانه‌ای؛
## تأملی بر ارکان جرم و آثار آن*

□ هادی رستمی[۱]

**چکیده**

کلاهبرداری رایانه‌ای به عنوان یک جرم به نسبت نوظهور در قوانین کیفری ایران، به لحاظ ارکان مادی و معنوی با کلاهبرداری کلاسیک (موضوع مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری) متمایز بوده و ویژگی‌های خاص خود را دارد. این نوع کلاهبرداری، که از رهگذر تقلب یا وارد کردن داده‌ها و یا اختلال در سامانهٔ رایانه‌ای و مخابراتی واقع می‌شود، به‌لحاظ رکن مادی، در زمرهٔ جرایم مطلق بوده و به مجرد تحصیل وجه یا مال یا امتیاز یا خدمات مالی واقع می‌شود و ضرورتی به فریب بزه‌دیده، بردن مال، ورود ضرر یا انتقاع مرتکب نیست. وارد کردن داده‌ها در کلاهبرداری رایانه‌ای می‌تواند در قالب داده‌های صحیح یا داده‌های جعلی باشد. آنچه مهم است، غیر مجاز بودن رفتار مرتکب در وارد کردن داده است. تحصیل در این نوع کلاهبرداری، نتیجه محسوب نشده و بخشی از فرایند رکن مادی (آخرین فرایند) را تشکیل



* تاریخ دریافت: ۹۸/۴/۲۸ ـ تاریخ پذیرش: ۹۸/۸/۲۹.
۱. استادیار دانشگاه بوعلی‌سینا (h.rostami@basu.ac.ir).

می‌دهد و از این رو، به لحاظ رکن معنوی، قصد نتیجه نیز شرط وقوع جرم نمی‌باشد. کلاهبرداری رایانه‌ای از حیث مرور زمان و انتشار حکم محکومیت، محدودیت‌های کلاهبرداری معمولی را نداشته و تابع مقررات عمومی است. چنانچه کلاهبرداری رایانه‌ای با سایر جرایم رایانه‌ای، مانند جعل، دسترسی غیر مجاز یا تخریب داده‌ها، تداخل نماید، تعدد منتفی بوده و فقط حکم به مجازات کلاهبرداری داده می‌شود.

**واژگان کلیدی:** کلاهبرداری رایانه‌ای، کلاهبرداری کلاسیک، تقلب، اختلال، سامانه، داده‌های رایانه‌ای.





## مقدمه

کلاهبرداری رایانه‌ای، پدیدهٔ تازه‌واردی است که به مدد صنعتی شدن جامعه و ظهور فناوری‌های رایانه‌ای و مخابراتی شکل می‌گیرد. با آغاز صنعتی شدن و تکامل و گسترش فناوری و به موازات آن رشد چشمگیر فناوری‌های نوین ارتباطی و اطلاعاتی، جرم‌هایی ارتکاب یافتند که پیش از آن سابقه نداشتند (برای آگاهی بیشتر ر.ک: رستمی و میرزایی، ۱۳۹۴: ۹۹ـ۱۳۱). پیدایش رایانه و فراگیری سریع فناوری ارتباطات، زمینه‌هایی را ایجاد کرد که امروزه کاربر برای تبدیل شدن به یک بزهکار سایبری، دیگر نیاز به برنامه‌نویسی و خلاقیت‌های زیادی نداشته و فضای مجازی، مکان مناسبی برای او فراهم می‌کند. از این رو، به موازات گسترش فعالیت‌ها در فضای سایبر، بخشی از بزهکاران نیز فعالیت‌های مجرمانه خود را به فضای مجازی انتقال دادند و بدین‌سان پدیدهٔ بزهکاری مجازی یا بزهکاری رایانه‌ای یا بزهکاری اینترنتی با طیف متنوعی از جرم‌های جدید که در گذشته پیشینه‌ای نداشتند یا نحوهٔ ارتکاب آن‌ها مانند کلاهبرداری، در فضای حقیقی متفاوت بود، شکل گرفتند (ر.ک: نجفی ابرندآبادی، ۱۳۸۹: ۹ـ۱۷).

در همین راستا، برای مبارزه با بزهکاری رایانه‌ای که افزون بر کلاهبرداری، بزه‌های زیادی را در بر می‌گیرد، قانون جرایم رایانه‌ای تحت تأثیر تحولات بین‌المللی و حقوق تطبیقی در چارچوب یک سیاست جنایی پیشگیرانه، هرچند به عنوان یک اقدام دیرهنگام، در سال ۱۳۸۸ به تصویب رسید و قانون‌گذار ایرانی با جرم‌انگاری،

کیفرگذاری و پیش‌بینی آیین دادرسی افتراقی، بـه مـصاف بزهکـاری رایانـه‌ای رفـت.[۱] پیش از این نیز قانون تجارت الکترونیکی مصوب ۱۳۸۲ برخی گونه‌های جـرم رایانـه‌ای را تصویب کرده بود.

کلاهبرداری رایانه‌ای که پیشتر با عنوان «کلاهبرداری کامپیوتری» شناخته می‌شـد، در مادهٔ ۱۳ قانون جرایم رایانه‌ای در ذیل فصل «سرقت و کلاهبرداری مرتبط بـا رایانـه» با دگرگونی‌هایی در رکن مادی و میزان مجازات مورد توجه قرار گرفت. به موجب این ماده:

«هر کس به طور غیر مجاز از سامانه‌های رایانه‌ای یا مخـابراتی یـا ارتکـاب اعمـالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یـا مختـل کـردن سـامانه، وجه یا مـال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحـصیل کنـد، علاوه بر رد مال به صاحب آن، به حبس از یک تا پنج سال یا جزای نقـدی از بیـست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجـازات محکوم خواهد شد».

مادهٔ مذکور که اینک به قـانون تعزیـرات (بخـش پـنجم قـانون مجـازات اسـلامی) الحاق شده و به عنوان مادهٔ ۷۴۱ شناخته می‌شود، به طور ضـمنی مفـاد مـادهٔ ۶۷ قـانون تجارت الکترونیکی مصوب ۱۳۸۲ را نسخ کرده[۲] و در مقایسه با کلاهبرداری کلاسیک (موضوع مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مـصوب

۱. در حقوق داخلی بـسیاری از کـشورها، کلاهبـرداری رایانـه‌ای بـه عنـوان یـک جـرم خـاص یـا در ذیـل کلاهبرداری کلاسیک پیش‌بینی شده است (در این باره ر.ک: عاملی، ۱۳۹۰: ۴۰۵ـ۴۱۸).

۲. برخی بر این باورند که کلاهبرداری کامپیوتری، موضوع مادهٔ ۶۷ قانون تجارت الکترونیکی با مادهٔ ۷۴۱ ق.م.ا.ت. نسخ نشده و مادهٔ اخیر در مقایسه با مادهٔ قبلی، خاص بوده و آن را تخـصیص مـی‌زنـد؛ زیـرا گسترهٔ شمول آن در مقایسه با مادهٔ ۷۴۱ ق.م.ا.ت. بازتر بوده و افزون بـر اخـتلال در سـامانه و گمراهـی سیستم، به «فریب» افراد نیز اشاره شده است (ر.ک: میرمحمدصادقی و شایگان، ۱۳۸۹: ۱۴۵). این دیدگاه با توجه به شباهت رکن مادیِ هر دو ماده و اینکه در هر دو به «ورود، محو، توقف داده‌ها و...» اشاره شده و ارتکاب جرم، مستلزم مداخله در داده و عملکرد سامانه رایانه‌ای و مخابراتی است، قابل تأمل می‌باشد. وانگهی، اشاره به عنصر «فریب» در مادهٔ مذکور به معنای آن نیست که مرتکب از رهگذر سامانهٔ رایانه‌ای و مخابراتی و با وسیله قرار دادن رایانه، دیگران را بفریبد، بلکه متضمن آن است که اقدامات مذکور (ورود، تغییر، محو یا توقف داده) ممکن است در نهایت کاربر را بفریبد، مانند ایجاد درگاه‌های جعلی پرداخـت وجه که سبب گمراهی اشخاص و انجام عملیات بانکی می‌شوند و بدین‌سان، اطلاعات کارت اعتبـاری خود را در اختیار کلاهبردار قرار می‌دهند. در اینجا فریب کاربر، متمایز از فریب خوردن در کلاهبرداری موضوع مادهٔ ۱ قانون تشدید است که مالباخته به سبب آن، مال را به مرتکب تسلیم می‌نماید.

۱۳۶۷) مجازات متمایزی دارد. کلاهبرداری رایانه‌ای از جهت ارکان مادی و معنوی، شیوهٔ ارتکاب و مطلق یا مقید بودن جرم، ابهام‌هایی دارد که مستلزم بررسی و تحلیل است. وانگهی، در اینکه آثار کلاهبرداری معمولی، مانند عدم شمول مرور زمان و انتشار حکم محکومیت در روزنامهٔ محلی، به کلاهبرداری رایانه‌ای تسری دارد، بحث‌های زیادی وجود دارد. این مقاله می‌کوشد با بررسی و تحلیل ماهیت کلاهبرداری رایانه‌ای و تمایزش با نوع کلاسیک آن، یعنی کلاهبرداری موضوع مادهٔ ۱ قانون تشدید (۱)، ارکان جرم کلاهبرداری رایانه‌ای (۲) و واکنش قانونی در برابر آن (۳) را تشریح کند. توجه به ویژگی‌های ارکان مادی و معنوی از جمله رفع ابهام از عبارتِ «وارد کردن داده‌ها» در مادهٔ ۷۴۱ ق.م.ا.ت.، تحلیل فنی شیوهٔ ارتکاب و نتیجهٔ جرم، بررسی آثار حاکم بر مجازات و سرانجام بررسی تداخل کلاهبرداری رایانه‌ای با سایر جرایم سایبری، از امتیازهای این مقاله در مقایسه با نوشتارهای دیگران[1] است.

## ۱. ماهیت کلاهبرداری رایانه‌ای

کلاهبرداری رایانه‌ای به لحاظ ارکان مادی و معنوی متمایز از کلاهبرداری کلاسیک می‌باشد. کلاهبرداری در مفهوم کلاسیک و معمول آن، که موضوع مادهٔ ۱ قانون تشدید است، به «اِعمال حیله و تقلب که منتهی به فریب دیگری و بردن مال او گردد» تعریف می‌شود (آقایی‌نیا و رستمی، ۱۳۹۷: ۳۷).[2] تعریف مذکور که با ابتناء بر مرکب بودن جرم کلاهبرداری عرضه شده است، در مورد «کلاهبرداری رایانه‌ای» صدق نمی‌کند؛ زیرا در مورد این جرم، رکنِ «فریب» به طور معمول مصداق نداشته و مرتکب به جای

۱. باید اشاره کرد که در رابطه با کلاهبرداری رایانه‌ای، کتاب‌های مربوط به حقوق جزای اختصاصی (جرایم علیه اموال و مالکیت) به اختصار وارد بحث شده‌اند. همچنین مقاله‌هایی که به این موضوع پرداخته‌اند و شمار آن‌ها در فهرست منابع دیده می‌شوند، قدیمی بوده و به طور عمده مربوط به پیش از سال ۸۸ و تصویب قانون جرایم رایانه‌ای می‌باشند.

۲. برخی نویسندگان، کلاهبرداری را به «سلطه یافتن بر مال دیگری از راه عملیات متقلبانه و فریفتن و وادار کردن صاحب مال به تسلیم مال به قصد تملک» تعریف کرده‌اند (زراعت، ۱۳۹۲: ۱۵). بعضی به «تحصیل مال دیگری با توسل به وسایل متقلبانه» (گلدوزیان، ۱۳۸۲: ۳۰۲) اشاره داشته‌اند. برخی نیز کلاهبرداری را «بردن مال دیگری از طریق توسل توأم با سوءنیت به وسایل یا عملیات متقلبانه» (میرمحمدصادقی، ۱۳۹۶: ۵۶) تعریف نموده‌اند.

انسان، با یک سامانه (یا سیستم) رایانه‌ای و مخابراتی روبه‌رو خواهد بود. در روش اخیر، مال دیگری از طریق عملیات متقلبانه و نفوذ در سامانه‌های رایانه‌ای یا مخابراتی برده شده و رابطه قربانی با بزهکار در بیشتر موارد نامرئی و غیر مستقیم است. از این رو، کلاهبرداری رایانه‌ای را می‌توان به «بردن مال دیگری از طریق تقلب یا اختلال در سامانهٔ رایانه‌ای یا مخابراتی» (همان) تعریف کرد؛ هرچند که باید اشاره کرد مجرد بردن مال دیگری با استفاده از سامانه‌های رایانه‌ای یا مخابراتی و به طور کلی فضای سایبری، کلاهبرداری رایانه‌ای نبوده و لازمهٔ این جرم به طور معمول، تقلب در داده‌ها یا اختلال در سامانهٔ رایانه‌ای یا مخابراتی است. برخی نویسندگان، تمایز مهم کلاهبردای کلاسیک و رایانه‌ای را در این دانسته‌اند که در کلاهبرداری نوع اول، مرتکب سعی بر تأثیرگذاری بر بزه‌دیده را دارد، حال آنکه در کلاهبرداری رایانه‌ای بیشتر سامانه‌ها یا سیستم‌های پردازشِ داده هدف قرار می‌گیرند. قوانین مبنتی بر کلاهبرداری کلاسیک، اغلب نمی‌توانند کلاهبرداری مرتبط با رایانه و دستکاری در سامانه‌ها را پوشش دهند و از این رو، قوانین میان این دو نوع جرم متمایز هستند (Gerck, 2012: 30).

بنابراین اگر رایانه و یا دستگاه مخابراتی به عنوان یک وسیله برای انجام اعمال متقلبانه و فریب کاربران در فضای سایبر مورد استفاده قرار گیرد تا از رهگذر آن با اغفال افراد، مال آن‌ها برده شود، رفتار ارتکابی، کلاهبرداری از نوع رایانه‌ای نبوده و منطبق با مفهوم کلاسیک آن است؛ برای نمونه، چنانچه شخصی در فضای مجازی از طریق وعده‌های دروغ، مانند تسهیل اقامت در خارج یا ادامهٔ تحصیل در یک دانشگاه معتبر خارجی، کاربران را بفریبد و وجوهی را از این طریق به دست آورد، کلاهبرداری ارتکابی در این روش، هرچند با اِعمال حیله و تقلب، فریب و پرداخت وجه در فضای سایبر (مجازی) صورت گرفته است، از نوع کلاسیک و غیر رایانه‌ای آن می‌باشد.[1] مادهٔ ۷۸۰ ق.م.ا.ت. بر استدلال مذکور صحه می‌گذارد:

---

۱. در برخی منابع، تمایزی میان زمانی که رایانه تنها وسیلهٔ کلاهبرداری است و زمانی که موضوع جرم قرار می‌گیرد، گذاشته نشده و هر دو کلاهبرداری رایانه‌ای به شمار رفته‌اند. بر اساس این برداشت، وجه تمایز کلاهبرداری رایانه‌ای از کلاهبرداری کلاسیک در همان استفاده از ابزارهای الکترونیکی است (ر.ک: Kunz & Wilson, 2004: 9-10).

«در مواردی که سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد».



حال آنکه اگر شخصی، درگاه الکترونیکی یکی از بانک‌ها را جعل نماید و سبب گمراهی کاربران در انجام عملیات بانکی گردد و با صید اطلاعات کارت اعتباری و رمز اینترنتی آن‌ها، وجوهی را تحصیل نماید، کلاهبرداری، رایانه‌ای است. در این مثال اگرچه کاربران، درگاه الکترونیکی جعلی را با اصلی اشتباه گرفته و به نوعی فریب خورده‌اند، اما از آنجایی که رابطه مستقیمی میان بزهکار و بزه‌دیده نیست و سامانه نقش منحصر به فرد و تعیین‌کننده‌ای در دزدی اطلاعات داشته و قربانی خود وجهی به حساب مرتکب واریز ننموده است، کلاهبرداری از نوع رایانه‌ای است. همچنین اگر مرتکب با تماس تلفنی، بزه‌دیده را با دادن وعده‌هایی مانند واریز وجه ناشی از قرعه‌کشی و نظایر این‌ها فریب دهد و به پای دستگاه عابر بانک بکشاند و از وی بخواهد تا کدهای مورد نظرِ او را وارد دستگاه نماید و از این راه وجوهی از حساب وی کسر و به حساب مرتکب انتقال یابد، رفتار ارتکابی به سبب داده‌محور بودنِ شیوهٔ ارتکاب و مهندسی و نفوذ غیر مجاز به سیستم، بی‌گمان کلاهبرداری رایانه‌ای است. با این حال، در برخی آرای قضایی، اقدام مذکور کلاهبرداری کلاسیک محسوب شده که صحیح نیست.[1] در این نوع کلاهبرداری، سامانهٔ رایانه‌ای یا مخابراتی خود به مثابهٔ وسیله و موضوع جرم قرار گرفته و رابطهٔ مستقیمی میان کلاهبردار و شخص مالباخته وجود نداشته و هویت بزهکاری و بزه‌دیده اغلب (و نه همیشه) نامرئی و ناشناخته است.

۱. دادنامهٔ صادره از شعبهٔ ۱۰۳۹ دادگاه کیفری ۲ تهران به شمارهٔ ۹۸۰۹۹۷۲۱۹۱۴۰۰۱۶۱ مورخ ۱۳۹۸/۲/۲۲ در این مورد، نظر به کلاهبرداری کلاسیک دارد: «... متهم با شکات تماس تلفنی گرفته و وانمود می‌کند که مأمور خرید سپاه است و قصد واریز وجه به حساب شاکی را دارد. بنابراین از شکات خواسته که جهت واریز وجه به حساب آنان، کدهای اعلامی ایشان را وارد دستگاه ATM نمایند و با این کار وجه از حساب بانکی شکات به حساب‌های مورد نظر متهم انتقال یافته است.... دادگاه انتساب بزه‌های موصوف را محرز... با استناد به مادهٔ ۱ قانون تشدید». همین موضوع به موجب دادنامهٔ شمارهٔ ۹۸۰۹۹۷۲۱۹۰۵۰۰۱۳۸ مورخ ۱۳۹۸/۲/۲۲ صادره از شعبهٔ ۱۰۳۰ دادگاه کیفری ۲ تهران، مصداقی از کلاهبرداری رایانه‌ای محسوب می‌شود.

در واقع، کلاهبرداری کلاسیک و رایانه‌ای فقط در لفظ مشترک‌اند و به لحاظ ماهیت و شکل ارتکاب، هر کدام ویژگی‌های خاص خود را دارند. در بیشتر جرایم سایبری بر خلاف جرم‌های کلاسیک، بزه‌دیدگان به سرعت از مراتب بزه‌دیدگی خود مطلع نشده یا آنکه مدت‌ها (حتی ماه‌ها) بعد از ارتکاب جرم، در جریان آن قرار می‌گیرند (نجفی ابرندآبادی، ۱۳۸۸: ۱۱). ماهیت فضای مجازی، فقدان عوامل بازدارنده و نظارتی و قابلیت ناشناختگی در عمل مجال مناسبی برای بزهکارانِ دنیای مجازی فراهم کرده است.

## ۲. ارکان جرم کلاهبرداری رایانه‌ای

رکن قانونی کلاهبرداری رایانه‌ای، آن‌سان که گفته شد، مادهٔ ۷۴۱ قانون مجازات اسلامی (تعزیرات)[۱] است که در سال ۱۳۸۸ به تصویب رسید و اینک به عنوان مستند قانونی این جرم، مورد توجه قانون‌گذار قرار گرفته است. مادهٔ مذکور آشکارا از کنوانسیون جرایم سایبر (معروف به سند بوداپست ۲۰۰۱) تأثیر پذیرفته است.[۲] مادهٔ ۸ کنوانسیون مذکور، کلاهبرداری رایانه‌ای را به «هر گونه وارد کردن، تغییر، حذف یا متوقف کردن داده‌های رایانه‌ای یا اخلال در عملکرد سامانه رایانه‌ای به صورت غیر مجاز و عمدی که به قصد تحصیل متقلبانه یا ناروای یک منفعت اقتصادی برای خود یا دیگری انجام گرفته و سبب ضرر مالی دیگری شده است»[۳] تعریف می‌کند و از

۱. در ادامه، این قانون با نشان «ق.م.ا.ت.» و قانون مجازات اسلامی نیز با علامت «ق.م.ا.» به کار می‌رود.

۲. کنوانسیون جرایم محیط سایبر به عنوان نخستین معاهدهٔ بین‌المللی در رابطه با جرایم رایانه‌ای با هدف یکنواخت‌سازی قوانین داخلی و ارتقای همکاری‌های بین‌المللی، در ۲۳ سپتامبر ۲۰۰۱ به تصویب دولت‌های شورای اروپا و چهار کشور آمریکا، کانادا، آفریقای جنوبی و ژاپن رسیده است. از ابتدای ژوئیه ۲۰۰۴ کنوانسیون به اجرا درآمد. تا سال ۲۰۱۳، ۳۹ کشور از جمله دولت‌های عضو اتحادیه اروپا این کنوانسیون را مصوب نموده و ۱۲ کشور نیز آن را امضا کرده‌اند.

3. Article 8 – Computer-related fraud: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: (a) any input, alteration, deletion or suppression of computer data; (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

کشورهای عضو می‌خواهد تا در صورت لزوم، در قوانین داخلی خود اقدام به جرم‌انگاری آن و سایر تدابیر بازدارنده نمایند. با این حال، مادهٔ ۷۴۱ ق.م.ا.ت. از سه جهت با مادهٔ ۸ کنوانسیون متمایز است. نخست، افزون بر سامانه رایانه‌ای، سامانهٔ مخابراتی[1] را نیز در بر می‌گیرد. دوم، موضوع جرم به منفعت اقتصادی محدود نشده و به جای این عنوان، که تا حدودی مبهم و تفسیربردار است، به صراحتْ در کنار مال و وجه، به امتیاز و خدمات مالی اشاره شده است. سوم، بر خلاف کنوانسیون، ضرر مالی را شرط تحقق جرم ندانسته و صرف تحصیل وجه یا مال یا امتیاز یا خدمات مالی را حتی اگر منتهی به ضرر نشود، جرم محسوب نموده است.

### ۲ـ۱. رکن مادی

رکن مادی جرم کلاهبرداری رایانه‌ای به استناد مادهٔ ۷۴۱ ق.م.ا.ت. با ارتکاب اَعمال غیر مجازی مانند وارد کردن داده‌ها، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه محقق می‌شود. اقدامات مذکور به لحاظ ماهوی، کُنش ایجابی بوده و با ترک فعل محقق نمی‌شوند. به دلیل مرکب بودن جرم کلاهبرداری رایانه‌ای، همانند کلاهبرداری موضوع مادهٔ ۱ قانون تشدید، اقدامات مذکور به خودی خود کلاهبرداری نبوده و آخرین فرایند رکن مادی (بردن مال یا امتیاز یا منفعت یا خدمات مالی) نیز باید تحقق پیدا کند.

#### ۲ـ۱ـ۱. تقلب یا اختلال در سامانه

مادهٔ ۷۴۱ ق.م.ا.ت.، رکن مادی را به صورت تمثیل مطرح کرده و با تصریح به «مختل کردن سامانه» رویکرد موسعی برگزیده است. با این توصیف، هر نوع

۱. برخی بر این باورند از آنجایی که جرم فقط از طریق رایانه واقع نمی‌شود، عنوان «کلاهبرداری الکترونیکی» نسبت به «کلاهبرداری رایانه‌ای» جامع‌تر و مناسب‌تر است (قناد، ۱۳۸۷: ۱۲۷). سیستم رایانه‌ای مطابق مادهٔ ۲ قانون تجارت الکترونیکی، که منطبق با بند الف مادهٔ ۱ کنوانسیون فضای سایبر است، هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های سخت‌افزاری و نرم‌افزاری است که از طریق اجرای برنامهٔ پردازش خودکار داده‌پیام عمل می‌کند. با این حال، با رایانه‌ای شدن ارتباطات مخابراتی و افول سامانه‌های آنالوگ و نیز گستردگی سامانه رایانه‌ای که شامل شبکهٔ رایانه‌ای نیز می‌شود، ضرورتی به عنوان‌های دیگر نبوده و اصطلاح «رایانه‌ای» مناسب و نسبت به سایر عنوان‌ها جامع‌تر است.

دستکاری سخت‌افزاری و نرم‌افزاریِ غیر مجاز که به اختلال در سامانه و تحصیل مـال، خدمات، امتیاز مالی یا منفعت بینجامد، کلاهبرداری رایانه‌ای خواهـد بـود. از ایـن رو، کلاهبرداری رایانه‌ای نوعی سوءاستفاده از رایانه یا سوءاستفاده از فناورهای اطلاعات و ارتباطات از رهگذر مداخله غیر مجاز در داده‌ها و عملکرد سامانه است که بر پـردازش آن تأثیر می‌گذارد (ر.ک: باستانی، ۱۳۹۰: ۵۰ـ۵۱). رفتار مرتکب در مـادهٔ ۷۴۱ ق.م.ا.ت.، به شرح زیر قابل بررسی و تحلیل است.

**الف) وارد کردن داده‌ها:** یکی از مصادیق شایع رکـن مـادی کلاهبـرداری رایانـه‌ای، وارد کردن داده‌ها در سامانه‌های رایانه‌ای و مخابراتی است. وارد کردن داده‌ها به شیوه‌های گوناگون مانند وارد کردن از طریق صفحه‌کلیدهای واقعی یا مجازی یا دیگـر ابزارهـای ورودی رایانه و یا شبکه‌های شتاب انجام می‌گیرد. وارد کردن داده‌ها می‌تواند در قالـب داده‌های صحیح یا داده‌های جعلی باشد. در این رابطه آنچه مهم است، غیر مجاز بودن رفتار مرتکب در وارد کردن داده و نه جعل آن‌هاست. بدین‌سان اگـر فـردی اطلاعـات حساب یا کارت عابربانک و رمز آن را به صورت مجاز در اختیار داشـته باشـد و بـدون اجازهٔ صاحب آن، با وارد کـردن گـذرواژه از طریـق عـابر بانـک و یـا شـبکهٔ پرداخـت اینترنتی، وجهی دریافت نماید، مرتکب کلاهبرداری رایانه‌ای شده است.[1] فقدان اجازهٔ برداشت از حساب، برای شمول جرم کفایت می‌کند و لازم نیست که فـرد بـه صـورت

---

۱. نظریهٔ مشورتی ادارهٔ حقوقی قوهٔ قضاییه به شمارهٔ ۷/۹۳/۱۱۶۱ مـورخ ۱۳۹۳/۵/۱۸ نیـز بـر دیـدگاه بـالا صحه می‌گذارد: «۱. منظور از فعل وارد کردن در مادهٔ ۷۴۱... وارد کردن داده‌ها به هر ترتیبی است کـه 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 داده‌ها را در اختیار داشته یا به وسایل متقلبانه، اطلاعات مورد نظر خود را کسب نماید. ۲. چون ملاک تحقق جرائم مندرج در قانون جرایم رایانه‌ای، اسـتفاده از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده است و در فرض سؤال به لحاظ اینکه سرقت انجام‌شده با استفاده غیر مجاز از داده‌های رایانه‌ای و وارد نمـودن رمـز کـارت عابربانـک دیگـری صـورت گرفتـه است، موضوع مشمول ماده ۷۴۱ الحاقی به قـانون مجـازات اسـلامی... اسـت» (بـه نقـل از: صـنعتی و عطائی جنتـی، ۱۳۹۷: ۸۵). در مقابـل، رأی شـمارهٔ ۹۲۰۹۹۷۰۲۲۰۹۰۱۰۶۶ مـورخ ۱۳۹۲/۹/۱۱ دادگـاه تجدیدنظر استان تهران، برداشت وجه بدون اجازه از عابربانک دیگری را مصداق تحصیل مـال از طریـق نامشروع پنداشته که نادرست است؛ زیرا بـدونِ وارد کـردن داده (گـذرواژه)، برداشـت وجـه از دسـتگاه ATM امکان‌پذیر نبوده و این امر با توجه به اشارهٔ مادهٔ ۷۴۱ ق.م.ا.ت. به «وارد کردن» داده، مـصداقی از کلاهبرداری رایانه‌ای است.

غیر مجاز به اطلاعات حساب و کارت اعتباری دیگری دست پیدا کرده باشد.[1] همین اتهام، در مورد اقدام فردی که بدون اجازه با وارد کردن گذرواژهٔ واقعی، از حجم ترافیک اینترنت دیگری استفاده می‌کند، نیز صادق است.

ممکن است ایراد شود که جرایم رایانه‌ای، موضوع‌محور بوده و نخستین قربانی این نوع جرایم، سامانهٔ رایانه‌ای و مخابراتی است و استفاده از داده‌های مجاز به صورت غیرمجاز، به دلیل عدم شمول تقلب یا اختلال در سامانه، کلاهبرداری محسوب نمی‌شود و با این تفسیر، دایرهٔ شمول کلاهبرداری گسترده خواهد شد. این نگرش، هرچند قابل تأمل است، اما ظاهر مادهٔ ۷۴۱ مطلق بوده و تمایزی میان داده‌های واقعی و جعلی قائل نیست.[2] مناسب‌تر آن بود که قانون‌گذار وارد کردن داده‌های صحیح را از شمول ماده خارج می‌کرد. این سیاست، با عنوان کلاهبرداری رایانه‌ای که هویت مالباخته به طور معمول برای مرتکب ناشناخته است، و نیز با جرم کلاهبرداری عام که حیله و تقلب نقش اساسی در ارتکاب آن بازی می‌کند، سازگارتر خواهد بود.

**ب) تغییر داده‌ها:** مصداق دیگری که در مادهٔ ۷۴۱ ق.م.ا.ت. مورد توجه قانون‌گذار قرار گرفته است، «تغییر» داده‌ها می‌باشد. تغییر داده همراه با دستکاریِ داده‌های واقعی یا تبدیل آن‌ها به گونه‌ای است که در پردازش سامانه اثرگذار باشد. این روش که با جعل رایانه‌ای تداخل پیدا می‌کند و حتی ممکن است به هک داده‌ها (نفوذ به سامانه) نیز بینجامد، اگر به بردن مال یا خدمات و یا امتیاز یا منفعت مالی منتهی گردد، کلاهبرداری رایانه‌ای خواهد بود و رفتار مرتکب به دلیل وجود حکم خاص، از شمول جعل رایانه‌ای خارج است.

---

۱. رأی صادرهٔ از شعبهٔ ۱۰۳۰ دادگاه کیفری دو تهران به شمارهٔ ۹۷۰۹۹۷۲۱۹۰۵۰۰۰۶۶ مورخ ۱۳۹۷/۲/۳ در این رابطه قابل توجه است: «... نظر به اینکه متهم پس از دسترسی به داده‌های شاکیه (رمز اینترنتی حساب) و وارد کردن داده‌ها در سامانه‌های رایانه‌ای به طور غیر مجاز وجوه مورد ادعای شاکیه را... تحصیل نموده است، لذا دادگاه رفتار متهم را با مادهٔ ۷۴۱ قانون مجازات اسلامی از فصل مربوط به جرایم رایانه‌ای مطابق دانسته...».

۲. این رویکرد تحت تأثیر سند بوداپست ۲۰۰۱ صورت گرفته و سند مذکور تمایزی میان داده‌های صحیح و جعلی نمی‌گذارد. در توصیه‌نامهٔ شمارهٔ R(۸۹)۹ مصوب ۱۳۸۹ شورای اروپا نیز هرچند به «وارد کردن داده‌ها» اشاره شده است، اما به سبب آنکه در فراز پایانی تعریف کلاهبرداری با این قید آمده که رفتار مذکور باید «بر نتیجه پردازش اثر بگذارد»، آن را به داده‌های غیر صحیح محدود می‌نماید.

**پ) ایجاد داده‌ها:** ایجاد داده‌های متقلبانه می‌تواند همراه با ساختن داده‌پیام‌ها از طریق صفحه‌کلید یا دیگر ابزارهای ورودی سامانهٔ رایانه‌ای باشد. راه‌اندازی تارنماهای جعلیِ پرداخت شتابی در عمل موجب می‌شوند که کاربران به اشتباه آن را واقعی پنداشته و اطلاعات حساب و کارت بانکی خود را در آن‌ها وارد نمایند و بدین‌سان، راه را برای شیادان جهت دسترسی به حساب و برداشتن وجوه فراهم سازند.[1] این عمل که در زبان فنی و تخصصی، فیشینگ (صید اطلاعات)[2] نامیده می‌شود (ر.ک: ویلیامز، ۱۳۹۱: ۶۶)، روشی است که برای تحصیل اطلاعات کاربران از جمله مشخصات کارت اعتباری و گذرواژهٔ آن، از طریق ساخت درگاه‌های پرداخت الکترونیکی به کار گرفته می‌شود.

**ت) توقف داده‌ها:** رکن مادی کلاهبرداری رایانه‌ای می‌تواند از طریق «توقف» در داده‌ها ارتکاب یابد. با این شیوه، مرتکب با انجام اقدامات متقلبانه، مانع دسترسی به داده برای افرادی می‌شود که به لحاظ قانونی مجاز به دسترسی به آن‌ها می‌باشند. عملکرد داده‌ها از این رهگذر متوقف شده و بزهکار مجال آن را پیدا می‌کند که مال و یا امتیاز مالی به دست آورد. گاه رفتار مرتکب موجب توقف داده نشده و تنها کارکرد سامانه را کندتر می‌کند. این روش، اگر مصداقی از اختلال در سامانه باشد، با اجتماع سایر شرایط، کلاهبرداری رایانه‌ای خواهد بود.

**ث) امحای داده‌ها:** محو داده‌ها که شیوهٔ دیگری برای ارتکاب کلاهبرداری رایانه‌ای است، به صورت حذف یا از بین بردن تمام یا قسمتی از داده، به نحوی که برای افراد قابل تشخیص نباشد، محقق می‌گردد. امکان بازیابی داده از طریق داده‌های پشتیبان، مانع تحقق تخریب نیست. تخریب داده‌ها به طور معمول از طریق رخنه یا هک سامانه انجام می‌شود، مانند هک مودم وای‌فای[3] با حذف تدابیر امنیتی آن و استفادهٔ غیر مجاز از حجم اینترنت. رخنه به سامانه رایانه‌ای و مخابراتی دیگری که با

---

۱. برای پیشگیری از کلاهبرداری رایانه‌ای و راهکارهای مقابله با آن، ر.ک: زیبر، ۱۳۹۰: ۱۹۹ـ۲۲۷؛ میرمحمدصادقی و شایگان، ۱۳۸۶: ۱۰۹ـ۱۲۶.

2. Phishing.

۳. وای فای (Wi-Fi) یک نوع شبکهٔ بی‌سیم محلی است.

تدابیر امنیتی حفاظت شده باشد، هرچند مصداقی از دسترسی غیر مجاز به داده‌های دیگری می‌باشد، اما لازمهٔ این دسترسی هک سامانه و امحای داده‌هاست. هکرها (رخنه‌گرایان)[1] کسانی هستند که با شکستن سیستم و برنامه‌های حفاظتی، به درون سامانه یا داده نفوذ می‌کنند و بیشتر به دنبال اثبات مهارت و توانایی‌های خود هستند (عالی‌پور، ۱۳۹۵: ۱۶۶). در برخی موارد نیز هدف آن‌ها دسترسی به منابع و حساب‌های مالی است.

**ج) اختلال در سامانه:** این عبارت که در رابطه با مصداق‌های دیگر مادهٔ ۷۴۱ ق.م.ا.ت. فراگیری بیشتری دارد، شامل هر نوع رفتاری می‌شود که به مختل کردن سامانه و تحصیل مال یا خدمات مالی از رهگذر آن می‌انجامد. در واقع، اختلال به‌معنای ایجاد آشفتگی و ناتوانی در وضعیت سامانه به گونه‌ای است که کارکرد و یا پردازش صحیح خود را از دست بدهد. در خصوص مفهوم اختلال گفته شده که این اقدام، شامل هر نوع دستکاری سخت‌افزارها، جلوگیری از خروج داده‌ها، تأثیر گذاشتن بر ثبت و ذخیره یا جریان داده‌ها یا توانایی اجرای برنامه‌ها می‌شود (خرم‌آبادی، ۱۳۸۶: ۹۳). روش سنتی در این رابطه، برنامهٔ «اسب تراوا»[2] است که در آن دستورالعمل‌هایی به صورت مخفیانه در برنامه‌های رایانه‌ای قرار داده می‌شوند تا عملیات مجاز و غیر مجاز را بدون آنکه ردی بر جای بماند، همزمان اجرا نموده و باعث اختلال یا خرابی در سامانه یا داده‌ها گردند. برنامهٔ کرم رایانه‌ای[3] نیز شیوهٔ دیگری از اختلال در سامانه است که توانایی نفوذ به سیستم و کپی اطلاعات آن و ارسال به دیگر رایانه‌های موجود در شبکه را دارد و به طور معمول دسترسی به داده‌ها را برای کاربر به تأخیر می‌اندازد. شیوهٔ دیگر اختلال در سامانه، حالتی است که کاربر به رغم انجام عملیات خرید در فضای مجازی و کسر وجوه از حساب خویش، به سبب اختلال در پردازش سیستم، موفق به خرید نشده و متضرر می‌گردد.

مصادیق مذکور به شرحی که آمد، تمثیلی‌اند و کلاهبرداری رایانه‌ای منحصر به

1. Hackers.
2. Trojan horse.
3. Computer Worm.

موارد فوق نبوده و روش‌های ارتکاب آن متنوع می‌باشند. فیشینگ ایمیل‌ها (تلاش برای به دست آوردن اطلاعات حساب دیگران از طریق ارسال پیام‌هایی که از کاربر می‌خواهد که حساب بانکی خود را به روز نماید)،[1] دستگاه‌های کارت‌خوان جعلی (اسکیمرها)[2] که قابلیت کپی کردن کارت‌های اعتباری و رمز آن را دارند، پیام‌های الکترونیکی ناخواسته یا اسپم‌ها،[3] شگردهای دیگری از اعمال متقلبانه در فضای مجازی می‌باشند که بستر مناسبی برای کلاهبرداران رایانه‌ای فراهم می‌کنند.

### ۲ـ۱ـ۲. تحصیل وجه، مال و...

کلاهبرداری رایانه‌ای مانند کلاهبرداری در مفهوم معمول آن، جرمی مرکب است و به مجرد وارد کردن یا تغییر یا محو یا توقف داده‌ها و یا اختلال در سامانه واقع نشده و لازمهٔ تحقق آن، وقوع بخش دوم رکن مادی، یعنی «تحصیل» است، وگرنه اقدام انجام‌گرفته کلاهبرداری رایانه‌ای محسوب نشده و در حد شروع به جرم و یا جرم خاص باقی می‌ماند.

تحصیل که در مادهٔ ۷۴۱ ق.م.ا.ت. به آن تصریح شده است، به نحو خلاف‌ناپذیری پس از تحقق مراحل پیشین، یعنی تقلب یا اختلال در سامانه واقع می‌شود. تحصیل در کلاهبرداری به معنای دستیابی به مال بدون اِعمال زور یا خشونت است و در این رابطه لازم نیست که مال یا امتیاز مالی به طور فیزیکی تحصیل شود و دریافت اعتباری نیز کفایت می‌کند. همین که مال یا وجه به حساب فرد کلاهبردار واریز گردد، تحصیل محقق شده و ضرورتی به خارج کردن مادی وجه از حساب نیست؛ برای مثال، اگر شخصی از طریق تقلب در سامانه، وجهی را از حساب دیگری برداشت و به حساب خویش واریز کند، کلاهبرداری محقق شده و همین مقدار عمل برای تحقق

---

۱. فیشینگ پیام‌ها اغلب شبیه آگهی‌های قانونی از نهادها و مؤسسات خدماتی بوده و به طور معمول حاوی برخی نشانه‌ها و زبان‌های مورد استفاده و رایج آن نهادهاست که در جهت اقناع مخاطب مبنی بر واقعی بودن پیام به کار گرفته می‌شود (در این باره، ر.ک: هولت و همکاران: ۱۳۹۷: ۱۵۴ـ۱۵۵).

2. Skimmers.

۳. در رابطه با پیام‌های الکترونیکی ناخواسته (Spams) و مبانی جرم‌انگاری آن‌ها، ر.ک: پاکزاد و آزادی‌خواه، ۱۳۹۵: ۱۹۵ـ۲۱۷.

کلاهبرداری کفایت می‌کند. بر خلاف کلاهبرداریِ موضوع مادهٔ ۱ قانون تشدید، که پس از عبارت «تحصیل»، به این جمله که مرتکب باید «از این راه مال دیگری را ببرد»، اشاره می‌کند، در کلاهبرداری رایانه‌ای، قانون‌گذار به عبارت «تحصیل» اکتفا کرده است. بدین‌سان، تمایز کلاهبرداری رایانه‌ای و کلاهبرداری کلاسیک در اینجا نیز نمایان است. چنانچه فردی دیگری را فریب دهد و در اثر فریب، وجهی به حساب او واریز شود و فرد پیش از برداشت وجه از حساب دستگیر شود و نتواند به مقصود خویش یعنی بردن وجه نائل گردد، اقدام وی شروع به کلاهبرداری است؛ زیرا آخرین شرط رکن مادی که همان بردن مال غیر است، محقق نشده و مرتکب بر اساس مقررات شروع به جرم مجازات می‌شود. در این مورد، تمام شرایط شروع به جرم (قصد ارتکاب جرم، شروع به اجرا، وجود مانع خارجی و تعلیق قصد) وجود داشته و تنها آخرین بخش رکن مادی (بردن مال) واقع نشده است. اگر در مثال مذکور، واریز وجه به حساب، ناشی از وارد کردن یا تغییر داده‌ها و یا تقلب در سامانه باشد، رفتار مرکب کلاهبرداری رایانه‌ای محسوب می‌شود، حتی اگر وجه تحصیل‌شده چند دقیقه‌ای در حساب باشد و به سبب آگاهی بانک یا اعلام مالباخته، از حساب کلاهبردار برداشته شده و به حساب مالباخته برگشت داده شود.

### ۱.۲.۱.۲. موضوع تحصیل

موضوع تحصیل، آن‌سان که مادهٔ ۷۴۱ ق.م.ا.ت. تصریح می‌کند، «وجه یا مال یا منفعت یا خدمات یا امتیازات مالی» است و بر خلاف کلاهبرداریِ مادهٔ ۱ قانون تشدید، موضوع کلاهبرداری رایانه‌ای وسیع‌تر بوده و افزون بر وجه و مال، «منفعت، خدمات و امتیازات مالی» را نیز شامل می‌شود. البته موضوع کلاهبرداری رایانه‌ای در بادی امر «داده‌ها به عنوان نمایندهٔ اموال و خدمات» است. داده‌ها به روش‌های مختلف دستکاری می‌شوند و موارد شایع و شناخته شدهٔ آن‌ها، دست بردن در سپرده‌ها، مطالبات، زمان کار، ترازنامه‌های سود و زیان بانکی، حقوق کارمندان، صورت‌حساب‌ها، مستمری‌ها، حق بیمه‌ها و نرم‌افزارهای مالی است (ر.ک: زیبر، ۱۳۹۰: ۲۰).

واژهٔ «منفعت» که در مادهٔ ۷۴۱ به آن تصریح شده است، شامل سود مال می‌شود و

نمونهٔ روشن تحصیل متقلبانهٔ منفعت آن است که شخصی به طـور غیـر مجـاز از طریـق سامانه‌های رایانه‌ای یا مخابراتی با نفوذ به درگاه مجازی یکـی از بانـک‌هـا، میـزان سـود سپرده خود را افزایش دهد و منفعتی را به دسـت آورد کـه مجـاز بـه تحـصیل آن نبـوده است. منظور از «خدمات» نیز مجموعه‌ای از فعالیـت‌هـای کـم یـا بـیش نامحـسوس و ناملموس می‌باشد. خدمات در واقع شامل سرویسی است که یک طرف به طرف دیگر ارائه می‌کند و بـه طـور معمـول در تعـاملات میـان مـشتری و کارکنـان یـا سیـستم‌هـای عرضه‌کننده صورت می‌گیرد (Grönroos, 2000: 20). خدمات شـامل خـدمات سـنتی و الکترونیکی می‌شود.[1] این خدمات ممکن است توسط یک شخص عرضه شـود، ماننـد اصلاح موی سر توسط یک سلمانی و یا خدمات وکیل، مـشاور حقـوقی و پزشـک، یـا اینکه به وسیلهٔ سازمان‌های تولیدی ارائه گردد، مانند خدمات آب، برق، گاز و یا تلفن و یا اینکه نظیر خدمات اشتراک اینترنت یـا خـدمات مربـوط بـه بانکـداری الکترونیکـی، به‌صورت الکترونیکی عرضه شوند. در رابطه با تحصیل متقلبانه خدمات و اینکه خدمات، مال محسوب می‌شوند یا خیـر، بحـث‌هـای زیـادی وجـود دارد و دیـدگاه حقـوق‌دانـان یکسان نیست، اما بیشتر ترجیح می‌دهند که مـال را بـه بعـد مـادی و ملمـوس آن تقلیـل دهند (ر.ک: آقایی‌نیـا و رسـتمی، ۱۳۹۷: ۶۹ـ۷۰؛ میرمحمدصـادقی، ۱۳۹۶: ۹۵).[2] بـا ایـن حـال در کلاهبرداری رایانه‌ای، رویکرد قانون‌گذار روشن بـوده و «خـدمات و امتیـازات مـالی» موضوع این جرم قرار می‌گیرند. بدین‌سان اگـر شخـصی بـا انجـام اقـداماتی بـه سـامانهٔ همراه اول نفوذ کرده و از سـرویس اینترنـت آن بـدون پرداخـت هزینـه اسـتفاده نمایـد، بی‌گمان مرتکب کلاهبرداری رایانه‌ای شده است. بـه همـین ترتیـب، شخـصی کـه بـه صورت غیر مجاز با وارد کردن داده یا تقلب در آن، از شبکه بی‌سـیم[3] دیگـران اسـتفاده می‌کند و سبب می‌شود که افزون بر کند شدن سرعت اتصال به اینترنت و دانلود فایل‌ها برای مشترک اصلی، هزینه‌هایی برای وی ایجاد نماید، کلاهبردار است. افزون بر مـوارد

---

۱. برای آشنایی با انواع خدمات و مدل‌های آن، ر.ک: Santos, 2003: 233-246.

۲. برای اطلاع از دیدگاه مخالف، که خدمات را مال پنداشته و آن را موضوع کلاهبرداری موضـوع مـادهٔ ۱ قانون تشدید می‌داند، ر.ک: قیاسی، ۱۳۹۳: ۱۶۳ـ۱۹۰.

3. Wireless network.

مذکور، «امتیازات مالی» نیز در شمول موضوع جرم قرار می‌گیرد و از این رو، تحصیل متقلبانه امتیاز مالی، مانند وام بانکی، ترفیع سالیانه یا پاداش و مزایای شغلی، با دستکاری در داده‌های رایانه‌ای، کلاهبرداری محسوب خواهد شد. همچنین اگر رفتار مرتکب منتهی به تحصیل داده‌ها یا نرم‌افزارهای مالی شود که قابلیت تبدیل به پول را داشته باشند، در شمول عنوان کلاهبرداری رایانه‌ای است.

چنانچه رفتار مرتکب در تحصیل متقلبانهٔ خدمات مشمول قانون مجازات استفاده‌کنندگان غیر مجاز از آب، برق، تلفن، فاضلاب و گاز مصوب ۱۳۹۶/۳/۱۰ باشد، از شمول حکم کلاهبرداری خارج می‌شود. مطابق مادهٔ ۲ قانون مذکور، دستکاری یا هر نوع تصرف یا تغییر در وضعیت دستگاه‌های اندازه‌گیر آب، برق، گاز، تلفن و یا شبکهٔ فاضلاب به نحوی که موجب اخلال در کارکرد صحیح و ثبت ارقام مصرفی گردد، جرم خاص محسوب شده و کلاهبرداری نیست.[۱] بنابراین چنانچه دستگاه‌های اندازه‌گیر، دیجیتالی یا رایانه‌ای باشند و فرد با تغییر یا تصرف در داده‌ها موجب شود که در فرایند ثبت مصرف انرژی، اخلالی ایجاد شده و از این راه خدمات رایگان یا خدمات به بهای کمتر یا خدماتی افزون بر میزان استاندارد تحصیل نماید، رفتار وی هرچند با مادهٔ ۷۴۱ ق.م.ا.ت. منطبق است، ولی به دلیل جرم‌انگاری خاص، از شمول آن خارج و تابع مادهٔ ۲ قانون مذکور است. همچنین استفاده غیر مجاز از اینترنت دیگری بدون آنکه مستلزم وارد کردن داده یا دستکاری در آن باشد، مانند آنکه کاربر به طور خودکار به شبکهٔ اینترنت دیگری که فاقد تدابیر امنیتی و رمز عبور است، متصل شده و از خدمات آن استفاده نماید، مشمول مادهٔ ۱ قانون استفاده‌کنندگان غیر مجاز خواهد بود و به سبب عدم ارتکاب رکن مادی به شرح مادهٔ ۷۴۱ ق.م.ا.ت.، مانند وارد کردن داده‌ها و...، از شمول کلاهبرداری رایانه‌ای خارج است. در مادهٔ ۱

۱. مادهٔ ۲ قانون مجازات استفاده‌کنندگان غیر مجاز از آب، برق، تلفن، فاضلاب و گاز، مصوب ۱۳۹۶/۳/۱۰: «هر شخصی به هر طریقی مبادرت به هر نوع تصرف یا تغییری در وضعیت دستگاه‌های اندازه‌گیری آب، برق، گاز، تلفن و یا شبکه فاضلاب نماید، به نحوی که منجر به اخلال در کارکرد صحیح و ثبت ارقام مصرفی گردد، علاوه بر الزام به اعاده وضع به حال سابق، به پرداخت بهای خدمات مصرفی و جبران خسارت و جزای نقدی درجه شش موضوع ماده ۱۹ قانون مجازات اسلامی مصوب ۱۳۹۲/۲/۱ محکوم می‌گردد».

قانون استفاده‌کنندگان غیر مجاز، به «اشتراک خدمات ارتباطی و فناوری اطلاعات» تصریح شده و منظور، استفاده از این خدمات بدون نیاز به گذرواژه یا تقلب یا اختلال در سامانه است. فقدان رمز در شبکهٔ بی‌سیم یا مودم، به منزلهٔ اجازهٔ استفاده به دیگران نیست. چنانچه استفاده از این خدمات از طریق شکستن گذرواژه و رخنه به سامانهٔ مخابراتی باشد، رفتار کاربر بدون تردید کلاهبرداری از نوع رایانه‌ای است.

### ۲ـ۱ـ۲ـ۲. تحصیل به مثابهٔ رفتار

تحصیل در جرم کلاهبرداری رایانه‌ای، بخشی از فرایند رکن مادی است و برخلاف آنچه که نوشته‌اند، نتیجه محسوب نمی‌شود (در این باره ر.ک: میرمحمدصادقی، ۱۳۹۶: ۱۵۵؛ میرمحمدصادقی و شایگان، ۱۳۸۹: ۱۵۲؛ الهی‌منش و مرادی اوجقاز، ۱۳۹۵: ۱۱۳)؛ زیرا به مجرد تحصیل کلاهبرداری واقع می‌شود و انتفاع مرتکب یا دیگری، ضرر مالباخته و بردن مال شرط نبوده و به صرف تحصیل، حتی اگر منتهی به بردن مال نشود، جرم واقع می‌گردد. در واقع، کلاهبرداری رایانه‌ای جرمی است مطلق، و ضرر مالباخته و یا انتفاع کلاهبردار، شرط تحقق آن نیست. کافی است که مال به روش‌های متقلبانه تحصیل گردد و این تحصیل به شرحی که گفته شد، ممکن است «اعتباری» و در قالب واریز وجه به حساب خاصی باشد. همین نکته در رابطه با تحصیل متقلبانه خدمات نیز صدق می‌کند؛ برای مثال، اگر شخصی به صورت غیر مجاز از اشتراک اینترنت دیگری استفاده نماید، رفتارْ مشمول مادهٔ ۷۴۱ ق.م.ا.ت. است، حتی اگر آن اشتراک بدون محدویت حجمی برای یک سال یا بیشتر خریداری شده و با استفادهٔ دیگران هیچ‌گونه ضرری متوجه صاحب آن نگردد.

منطوق و مفهوم مادهٔ مذکور هیچ گونه دلالتی بر مقید بودن جرم نداشته و ارتکاب آخرین بخش رفتار مادی، که در جرایم مرکب و به‌عادت ضروری است، ارتباطی با نتیجه ندارد. اگر نتیجه به وضعیتی محدود شود که متعاقب رفتار و مترتب بر آن واقع می‌شود،[۱] مانند مرگ در قتل یا ازهم‌گسیختگی بافت‌ها در جرح یا تغییر رنگ پوست یا

۱. برخی در این باره می‌گویند: «نتیجه به عنوان یک پدیدهٔ مادی، تغییری است که در عالم بیرونی در اثر رفتار مجرمانه به وجود می‌آید» (حسنی، ۱۳۸۵: ۷۲).

تورم در ضرب یا تحت پیگرد قرار گرفتن در افترای عملی (مادهٔ ۶۹۹ ق.م.ا.ت.)، در آن صورت، عبارت «تحصیل کند» در مادهٔ ۷۴۱ ق.م.ا.ت. نتیجه نبوده و بخشی از فرایند ارتکاب رفتار مجرمانه می‌باشد. بی‌گمان مجرد تقلب یا اختلال در سامانه همواره منجر به تحصیل نشده و مرز میان این دو، هرچند در مواردی غیر قابل تفکیک است، متمایز می‌باشد و این گونه نیست که به صرف تقلب در سامانه، وجه یا مال یا خدماتی تحصیل گردد. لازمهٔ تحصیل، دستیابی به مال و یا خدمات است که تحقق آن، مستلزم انجام اقداماتی مانند افتتاح حساب برای واریز وجه یا منفعت یا امتیاز مالی و بهره‌برداری یا استفاده از خدمات مالی است.[۱]

اگر نتیجه، به معنای ضرر بزه‌دیده یا انتفاع کلاهبردار یا شخص مورد نظر وی تقلیل یابد، در آن صورت، صرف تحصیل وجه یا مال یا امتیاز مالی کفایت نکرده و لازم است که ضرری به مالباخته وارد گردد و یا نفعی دریافت شود که با اثبات خلاف آن، یعنی با اثبات اینکه مال برده نشده و پیش از برداشت و بردن آن، به دلیل اقدام فوری بانک یا اطلاع مقامات، مرتکب دستگیر شده است، کلاهبرداری منتفی می‌باشد. این موضوع در رابطه با وجوه ناشی از پولشویی یا سرقت یا هر مالی که از رهگذر جرم به‌دست آمده است، چالش‌برانگیز خواهد بود و کافی است که با اثبات منشأ نامشروع وجه، مقوله ضرر کنار گذاشته شود. به نظر نمی‌رسد که قانون‌گذار در جرم‌انگاری کلاهبرداری رایانه‌ای، به مقولهٔ «ضرر» و یا «نفع» توجهی داشته باشد و به همین دلیل از به کارگیری واژگان مذکور اجتناب کرده و فقط به عبارت «تحصیل» اکتفا می‌نماید.

شایان ذکر است که چنانچه بزهکاران متعدد باشند، برای تحقق شرکت، لزومی به مداخلهٔ همهٔ آن‌ها در تمام اجزای جرم مرکب نبوده و کافی است هر یک بخشی از فرایند رکن مادی را انجام دهند. بنابراین اگر تقلب در سامانه به وسیلهٔ یک نفر و تحصیل وجه با افتتاح حساب توسط دیگری انجام شود و این اقدامات ناشی از تبانی

۱. با این حال، کلاهبرداری رایانه‌ای در کنوانسیون جرایم سایبر (سند بوداپست ۲۰۰۱)، جرم مقید به ضرر تعریف شده است. مادهٔ ۸ این کنوانسیون، «ورود ضرر مالی به دیگری» را شرط تحقق کلاهبرداری رایانه‌ای دانسته است.

میان آن‌ها باشد، هر دو به اتهام شرکت در کلاهبرداری رایانه‌ای قابل مجازات می‌باشند.



### ۲ـ۲. رکن معنوی

رکن معنوی به فعل و انفعالات ذهنی مرتکب گفته می‌شود که گاه به صورت قصد مجرمانه (در جرایم عمدی) و گاه به شکل تقصیر جزایی (در جرایم غیر عمدی) ظاهر می‌شود. این رکن در کنار رکن مادی، پدیدهٔ مجرمانه را رقم می‌زند و بدون وجود آن، جرمی پدید نمی‌آید. کلاهبرداری در زمرهٔ جرایم عمدی است. افزون بر منطوق این واژه که دلالت بر عمد دارد، اصل عمدی بودن جرایم نیز بر این نکته صحه می‌گذارد که جرایم جز در مواردی که به غیر عمدی بودن آن‌ها تصریح گردد، عمدی محسوب می‌شوند. اجزای عمد در کلاهبرداری رایانه‌ای به شرح زیر قابل توجه و بررسی است:

#### ۲ـ۲ـ۱. علم به موضوع

موضوع آن چیزی است که جرم علیه آن واقع می‌شود. در جرایم علیه اموال و مالکیت، موضوع جرم، مال متعلق به غیر است و در کلاهبرداری رایانه‌ای نیز موضوع، «وجه، مال، منفعت، امتیاز و خدمات مالی» می‌باشد که قانون‌گذار در مقام حمایت کیفری از آن‌ها برآمده است. هر گونه جهل یا اشتباه نسبت به موضوع، رکن معنوی جرم را زائل می‌کند. از آنجایی که علم به موضوع، به تصریح مادهٔ ۱۴۴ ق.م.ا. بخشی از ساختار رکن معنوی جرایم عمدی است، فقدان آن مانع شکل‌گیری عمد خواهد شد. از این رو، اگر کارمند بانک از طریق سامانه‌های رایانه‌ای با وارد کردن داده‌ها به‌اشتباه وجهی را به حساب دیگری واریز نماید، به اتهام کلاهبرداری رایانه‌ای قابل تعقیب نخواهد بود. در این شرایط، چنانچه کارمند مربوطه بعد از اقدام مزبور به رغم اطلاع، اقدامی در جهت اعاده وجه انجام ندهد، رفتار وی به سبب عدم تقارن میان رکن مادی و معنوی[1] قابل تعقیب نیست؛ زیرا به هنگام ارتکاب رکن مادی، فاقد رکن معنوی و علم به تعلق مال به غیر بوده است. افزون بر علم به موضوع، مرتکب باید به

۱. برای اطلاع بیشتر دربارهٔ تقارن رکن مادی و معنوی (Coincidence of actus reus and mens rea)، ر.ک: Clarkson, 1987: 22-26؛ لفیو، ۱۳۹۷: ۱۱۹ـ۱۲۰. برای نقد رویکرد تقارن ارکان مادی و معنوی به ویژه رویکرد مطلق‌گرا به این موضوع، ر.ک: صابری و دیگران، ۱۳۹۷: ۳۵۷ـ۳۷۷.

متقلبانه بودن رفتار خویش نیز آگاه باشد و با علم به غیر مجاز بودن رفتار مبادرت به کلاهبرداری نماید.



تصور مجاز بودن رفتار غیر مجاز، از آنجایی که ماهیت آن به جهل حکمی برمی‌گردد، تأثیری در ماهیت جرم کلاهبرداری ندارد. بنابراین ادعای مرتکب به اینکه نسبت به قانونی بودن رفتار خویش در وارد کردن یا تغییر یا دستکاری داده‌ها جاهل بوده است، پذیرفته نمی‌شود.

### ۲ـ۲ـ۲. قصد کلاهبرداری

از آنجایی که کلاهبرداری به شرحی که گفته شد، در زمرهٔ جرایم مطلق می‌باشد، قصد نتیجه نسبت به آن منتفی خواهد بود. اما قصد ارتکاب نسبت به اجزای جرم مرکب لازم است. اجزای رکن معنوی در هر مرحله، ویژگی خاص خود را داشته و قصد کلاهبرداری وجه مشترک همهٔ آن‌هاست. منظور از قصد کلاهبرداری، همان قصد تحصیل مال، منفعت، خدمات یا امتیاز مالی برای خود یا دیگری است. در مرحله نخست، قصد تقلب یا اختلال در سامانه ضروری است. قصد تقلب با ارتکاب آگاهانه و ارادی رفتارهایی مانند وارد کردن، تغییر، محو، ایجاد یا توقف داده‌ها همراه است و قصد اختلال نیز ارتکاب هر گونه رفتاری است که عملکرد یا پردازش سامانه را بر هم می‌زند. چنانچه اقدامات مذکور عمدی نباشند، رفتار مرتکب، حتی اگر به تحصیل وجه یا مال یا خدمات مالی بینجامد، کلاهبرداری نخواهد بود. برای مثال، اگر «الف» کارت عابربانک متعلق به «ب» و گذرواژه آن را برای انجام عملیات انتقال وجه به حساب «پ» در اختیار داشته باشد و پس از وارد نمودن رمز که به صورت مجاز انجام شده است، طمع نموده و پول را به نفع خود تحصیل نماید، به دلیل آنکه دسترسی به سامانه قانونی می‌باشد، کلاهبرداری رایانه‌ای واقع نشده و موضوع بیشتر با خیانت در امانت منطبق است.

در مرحله بعد، قاصد بودن مرتکب به تحصیل وجه، مال، منفعت، خدمات یا امتیاز مالی نیز ضروری است و با فقدان این قصد، کلاهبرداری محقق نمی‌شود. پیوستگی مراحل کلاهبرداری ایجاب می‌کند که تحصیل مال، زمانی در زنجیرهٔ کلاهبرداری

به‌عنوان بخشی از این جرم قرار می‌گیرد که بتوان گفت تحصیل، در پی تقلب یا اختلال در سامانه بوده است. در صورتی که قصد مرتکب از انجام اقدامات مذکور، تنها نفوذ به سامانه (هک)[1] یا رمزگشایی (کِرَک)[2] از آن یا به قصد اختلال در سود حساب‌های سپردهٔ بانکی و کم کردن درصد سود مشتریان باشد، بدون آنکه منفعتی تحصیل گردد، اقدام وی حتی در فرض ضرر مالی اشخاص، کلاهبرداری نبوده و با اتهام‌هایی چون دسترسی غیر مجاز، جاسوسی رایانه‌ای، جعل یا تخریب رایانه‌ای قابل انطباق است؛ زیرا مال یا خدمات یا منفعتی تحصیل نشده و ضرر به دیگران به معنای تحصیل نیست. بدین‌سان به نظر می‌رسد کم کردن درصد وام دریافتی و یا صفر نمودن بدهی بانکیِ خود از طریق دستکاری در داده‌ها، صرف‌نظر از مقولهٔ تقارن میان ارکان مادی و معنوی، با منطوق کلاهبرداری رایانه‌ای که از «تحصیل» سخن می‌گوید، سازگاری ندارد.

قصد تحصیل باید مقدم بر رکن مادی باشد و در صورتی که این قصد مؤخر بر تحصیل مال یا منفعت شکل گیرد، ارتکاب کلاهبرداری به دلیل عدم تقارن رکن معنوی و مادی منتفی خواهد بود. از این رو، اگر فردی بعد از واریز وجهِ ناروا به حساب او، با انجام اقداماتی مانند تقلب یا دستکاری در سامانه، آن وجه را متعلق به خود قلمداد نماید، رفتار وی کلاهبرداری رایانه‌ای نیست.

بدیهی است که در کلاهبرداری، قصد نتیجه محملی نداشته و قصدِ آخرین رکن جرم مرکب را نمی‌توان به عنوان قصد نتیجه محسوب کرد. در جرایمی که نتیجه شرط نیست، قصد نتیجه توجیهی ندارد. بر خلاف کنوانسیون جرایم سایبر (سند بوداپست) که کلاهبرداری را جرمی مقید به ضرر تعریف می‌کند و لازمهٔ تحقق آن را به لحاظ رکن معنوی، افزون بر قصد متقلبانه یا ناروای یک منفعت اقتصادی برای خود یا دیگری، قصد نتیجه (قصد ضرر دیگری) می‌داند، در حقوق ایران، قصد ضرر لازم نبوده و ضرڑ شرط وقوع کلاهبرداری رایانه‌ای نیست.

---

1. Hack.
2. Crack.

## ۳. واکنش قانونی و آثار آن

واکنش قانونی در مقابل کلاهبرداری رایانه‌ای در مقایسه با کلاهبرداری موضوع مادهٔ ۱ قانون تشدید، متفاوت بوده و قانون جرایم رایانه‌ایِ سال ۱۳۸۸ و پیش از آن، قانون تجارت الکترونیکیِ سال ۱۳۸۲ رویکرد متمایزی در قبال کلاهبرداران رایانه‌ای اتخاذ نموده‌اند که علت این سیاست دوگانه روشن نیست. البته با تصویب قانون کاهش حبس تعزیری (۱۳۹۹) و اصلاح مادهٔ ۱۰۴ ق.م.ا.، کلاهبرداری کلاسیک در صورتی که مبلغ آن تا یک میلیارد ریال باشد، قابل گذشت بوده و مجازات حداقل و حداکثر آن به نصف تقلیل می‌یابد. از این جهت، کلاهبرداری رایانه‌ای به دلیل غیر قابل گذشت بودن و نیز میزان مجازات حبس تا حدودی شدت یافته است. تداخل مجازاتِ کلاهبرداری رایانه‌ای با سایر جرایم رایانه‌ای که مقولهٔ تعدد را دامن می‌زند، چالش دیگری است که نیازمند بررسی می‌باشد.

### ۳ـ۱. ضمانت اجراها

مجازات کلاهبرداری رایانه‌ای به شرح مادهٔ ۷۴۱ ق.م.ا.ت. حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات است که تفاوت آشکاری با مجازات کلاهبرداری موضوع مادهٔ ۱ قانون تشدید دارد. دادگاه در انتخاب نوع مجازات یا هر دو، اختیار کامل دارد و از این رو می‌تواند برای کلاهبرداری رایانه‌ای با رقم‌های بسیار بالا، بیست میلیون ریال جزای نقدی تعیین نماید یا اینکه برای مبالغ اندک، حکم به پنج سال حبس و یکصد میلیون ریال جزای نقدی بدهد که این نوع آزادی عمل قابل توجیه نیست. میزان پایین جزای نقدی این جرم با توجه به پیمایش‌های تازه که نگرانیِ فزاینده از بزه‌دیدگیِ کلاهبرداری رایانه‌ای را به ویژه در برخی از گونه‌های آن مانند سوءاستفاده از کارت‌های اعتباری به تصویر می‌کشد، منطق قابل قبولی نداشته و چندان متناسب نیست. مقولهٔ ترس از جرم در این نوع کلاهبرداری‌ها، در مقایسه با کلاهبرداری کلاسیک در سال‌های اخیر افزایش یافته و به‌همین دلیل، حسِ بزه‌دیدگی به هنگام پرداخت‌های اینترنتی فزونی گرفته است.[۱]

۱. در رابطه با مقوله ترس از جرم در کلاهبرداری و جرایم یقه‌سفیدان، ر.ک: لِوی، ۱۳۹۲: ۱۴۰ـ۱۴۳.

مجازات‌های کلاهبرداری رایانه‌ای (حبس و جزای نقدی) از حیث نظام درجه‌بندی با توجه به مادهٔ ۱۹ ق.م.ا. در چارچوب درجهٔ پنج قرار گرفته و تمام آثار این درجه بر آن قابل اِعمال می‌باشد. مجازات معاونت در آن نیز مطابق بند ت مادهٔ ۱۲۷ ق.م.ا. یک تا دو درجه پایین‌تر از مجازات قانونی جرم (یعنی حبس یا جزای نقدی درجهٔ شش یا هفت یا هر دو مجازات) می‌باشد. مجازات شروع به این جرم با استناد به بند پ مادهٔ ۱۲۲ ق.م.ا.، حبس یا شلاق یا جزای نقدی درجهٔ شش به انتخاب دادگاه است. شروع به کلاهبرداری رایانه‌ای در حالتی محقق می‌شود که مرتکب به رغم تقلب در داده‌ها یا اختلال در سامانه، به علت وجود مانع خارجی، موفق به تحصیل وجه یا مال یا خدمات یا منافع یا امتیازهای مالی نشده و قصدش معلق می‌ماند؛ مانند آنکه کاربری با هک داده‌ها و نفوذ به سامانهٔ بانکی، در صدد برداشت وجه برمی‌آید، اما به جهت اقدام زودهنگام بانک، موفق به برداشت نمی‌شود.

در صورتی که مرتکب کلاهبرداری رایانه‌ای، کارمند دولت باشد یا جرم به مناسبت شغل متصدی و یا متصرف قانونی واقع شده یا جرم سازمان‌یافته یا در سطح گسترده‌ای ارتکاب یابد، مرتکب به استناد مادهٔ ۷۵۴ ق.م.ا.ت. به بیش از دوسوم حداکثر مجازات محکوم می‌شود. در صورت تکرار جرم برای بیش از دو بار، دادگاه می‌تواند مرتکب را به استناد بند ب مادهٔ ۷۵۵ ق.م.ا.ت.، یک تا سه سال از خدمات الکترونیکی عمومی محروم نماید. مادهٔ مذکور از آنجایی که ناظر به مجازات تکمیلی است و قانون‌گذار در تبصرهٔ ۱ مادهٔ ۲۳ ق.م.ا. مدت مجازات تکمیلی را جز در مواردی که قانون به نحو دیگری مقرر کرده باشد، حداکثر دو سال در نظر گرفته است، بنابراین مفاد این ماده که حکم خاص دارد، بر خلاف دیدگاه برخی نویسندگان (ر.ک: سالاری، ۱۳۹۳: ۲۸۷) نسخ نشده و اِعمال آن نافی مقررات تکرار جرم به شرح مادهٔ ۱۳۷ ق.م.ا. نیست.

حکم به رد مال به صاحب آن، از مواردی است که باید علاوه بر مجازات توسط دادگاه صادر گردد. مشکلْ آن است که فقط مال، موضوع کلاهبرداری رایانه‌ای نبوده و افزون بر مال، منفعت، امتیاز یا خدمات مالی نیز مورد توجه قانون‌گذار قرار گرفته و مناسب‌تر آن بود که در کنار رد مال، به رد امتیاز یا منفعت مالی تحصیل‌شده و جبران خسارات بابت خدمات مالی نیز اشاره می‌شد. با این حال، امتیاز یا منفعت مالی

به‌سهولت قابل استرداد بوده و نیاز به تقدیم دادخواست ندارند، اما رد خدمات بدون تقویم میزان خسارات و نظر کارشناسی امکان‌پذیر نبوده و لاجرم باید دادخواست ارائه گردد. پر واضح است که رد مال مجازات نبوده و یک ضمانت اجرای مدنی است.[1] الزام به رد مال به لحاظ آنکه مجازات محسوب نمی‌شود، از شمول مقررات تخفیف یا تشدید نیز خارج است.

### ۳ـ۲. بررسی آثار مجازات

مجازات کلاهبرداری رایانه‌ای از جهت تعلیق و تخفیف، تابع قواعد عمومی است. مجازات کلاهبرداری کلاسیک نیز با تصویب قانون کاهش مجازات حبس تعزیری (۱۳۹۹) مطابق مقررات عمومی قابل تخفیف و تعلیق بوده و محدودیت‌های سابق وجود ندارد. قانون مذکور با حذف تبصرهٔ ۱ مادهٔ ۱ قانون تشدید، راه را برای تخفیف و تعلیق مجازات فراهم نموده است. به رغم پیامدهایِ زیانبار این جرم، قانون‌گذار در عمل رویکرد ساده‌تری را در واکنش به آن برگزیده است که توجیه معقولی ندارد. اما در اینکه محکومیت به کلاهبرداری رایانه‌ای، در صورتی که مبلغ آن بیش از یک میلیارد ریال باشد، مشمول انتشار حکم قطعی در روزنامه محلی به شرح مادهٔ ۳۶ ق.م.ا. خواهد شد و یا اینکه با احتساب مبلغ مذکور، مقررات مرور زمان با عنایت به مادهٔ ۱۰۹ ق.م.ا. جاری نمی‌گردد و مهم‌تر از همه، امکان شمول مجازات مادهٔ ۴ قانون تشدید در فرض تحقق کلاهبرداری رایانه‌ای به صورت شبکه‌ای وجود دارد یا خیر، نص صریحی در قانون و رویهٔ قضایی مشاهده نمی‌شود. به نظر می‌رسد با توجه به اینکه عبارت «کلاهبرداری» به طور معمول صراحت در کلاهبرداری موضوع مادهٔ ۱ قانون تشدید دارد و از آنجایی که «کلاهبرداری رایانه‌ای» یک عنوان ترکیبی است و برای بیان مقصود و دریافت شنونده باید به طور کامل استعمال گردد و حتی عنوان فصل سوم از بخش سی‌ام قانون تعزیرات (قانون جرایم رایانه‌ای مصوب ۱۳۸۸) به تأسی از

۱. نظریهٔ شمارهٔ ۷/۹۷۰۹ مورخ ۱۳۸۰/۲/۱۳ ادارهٔ حقوقی به این دیدگاه متمایل است: «... در صورت احراز وقوع جرم، چون مقنن استرداد مال را به عنوان بخشی از مجازات در مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مقرر داشته، صرف‌نظر از اینکه مال در اختیار چه کسی باشد، دادگاه باید حکم به رد مال صادر نماید».

سند بوداپست به «کلاهبرداری مرتبط با رایانه»[1] اختصاص داده شده و در متن مادهٔ ۷۴۱ ق.م.ا.ت. بر خلاف پیش‌نویس آن، قیدی بر «کلاهبردار محسوب می‌شود» وجود ندارد،[2] بنابراین از عموم و اطلاق اصطلاح «کلاهبرداری» و اشتراک لفظی میان این دو، که به لحاظ مفهومی تفاوت‌هایی زیادی با یکدیگر دارند، نمی‌توان نتیجه گرفت که در هر مورد که این عنوان به طور مطلق در قوانین به کار رفته است، عمومیت داشته و شامل هر دو نوعِ کلاهبرداری می‌شود. چنین پنداری با تفسیر مضیق قوانین کیفری و نیز قاعدهٔ درأ، که اینک مبنا و مستند قانونی دارد (مادهٔ ۱۲۰ ق.م.ا.)، ناسازگار بوده و پذیرفتنی نیست. هرچند باید پذیرفت که رویکرد قانون‌گذار در قبال کلاهبرداران رایانه‌ای در مقایسه با سایر کلاهبرداری‌ها، متناسب نبوده و قانون‌گذار به جهت نداشتن ارزیابی دقیق از شدت و ماهیت جرم و پیامدهای آن، تناسب نسبی میان گونه‌های جرایم و مجازات‌ها را نادیده گرفته و در نهایت فاصلهٔ میان جرایم همگون با ماهیت یا سرزنش‌پذیری مشابه یا جرم‌های با ضررهای یکسان را رعایت نکرده و مجازات‌ها فاصلهٔ چشم‌گیری با یکدیگر دارند.[3] این مورد اختصاص به گونه‌های کلاهبرداری نداشته و در مورد همهٔ جرایم تعزیری، کم یا بیش صادق است.

سرانجام لازم به تصریح است که مطابق رأی وحدت رویهٔ شمارهٔ ۷۲۹ هیئت عمومی دیوان عالی کشور[4] به تاریخ ۱۳۹۱/۱۲/۱، دادگاه صالح به رسیدگی به جرم کلاهبرداری رایانه‌ای، دادگاه محل بانک افتتاح‌کنندهٔ حساب زیان‌دیده، که پول به‌طور متقلبانه از آن برداشت شده است، می‌باشد. بدیهی است که رأی مذکور در چارچوب

---

1. Computer-related fraud.

۲. این موضوع (پرهیز از عنوان کلاهبرداری در متن ماده)، بیشتر به این دلیل بوده که قانون‌گذار در تعریف کلاهبرداری رایانه‌ای، تحت تأثیر کنوانسیون جرایم سایبر (سند بوداپست ۲۰۰۱) بوده و به تأسی از آن، از به کارگیری عنوان کلاهبرداری در متن ماده اجتناب نموده است (در این باره، ر.ک: گَسَن، ۱۳۹۳: ۹۲).

۳. برای آشنایی با نظام‌مندسازی کیفرگزینی، ر.ک: صبوری‌پور، ۱۳۹۷: ۱۲۳ـ۱۴۳.

۴. در کلاهبرداری موضوع مادهٔ ۱ قانون تشدید نیز چنانچه توسل به حیله و تقلب در یک حوزه و بردن مال در حوزهٔ دیگری واقع شده باشد، دادگاهِ صالح به رسیدگی، دادگاه محل وقوع آخرین فرایند رکن مادی جرم (بردن مال غیر) است. در همین رابطه، شعبهٔ دوم دیوان عالی کشور در رأی شمارهٔ ۹۱۰۹۹۷۰۹۰۹۰۰۰۵۲۵ مورخ ۱۳۹۱/۱۰/۵، که در مقام حل اختلاف بین دو حوزهٔ قضایی (حوزهٔ محل توسل به وسایل متقلبانه و حوزهٔ محل بردن مال) صادر شده است، دادگاه محل بردن مال را صالح به رسیدگی به جرم اعلام می‌کند.

حقوق داخلی قابل توجیه است؛ زیرا اگر بخشی از فرایند کلاهبرداری در ایران و بخش دیگر خارج از قلمرو حاکمیت ایران واقع شود، به تصریح مادهٔ ۴ ق.م.ا. در حکم جرم واقع‌شده در ایران بوده و دادگاه‌های ایران صلاحیت رسیدگی به جرم را دارند. در این حالت، اگر محل افتتاح حساب، یک کشور خارجی بوده و مرتکب از اتباع ایران باشد، به تصریح مادهٔ ۳۱۶ ق.آ.د.ک. دادگاه محل دستگیری صالح به رسیدگی خواهد بود.

### ۳ـ۳. تداخل مجازات‌ها

تداخل مجازات‌ها در کلاهبرداری رایانه‌ای، ناشی از تداخل عناوین مجرمانه دیگر با این جرم است. در صورتی که کلاهبرداری رایانه‌ای با جرایم دیگری مانند دسترسی غیر مجاز (مادهٔ ۷۲۹ ق.م.ا.ت.)، جعل رایانه‌ای (مادهٔ ۷۳۵ ق.م.ا.ت.)، تخریب یا اختلال داده‌ها (مواد ۷۳۶ـ۷۳۷ ق.م.ات.) یا سرقت داده‌ها (مادهٔ ۷۴۰ ق.م.ا.ت.) تداخل نماید، در بادی امر مقررات تعدد مورد توجه قرار می‌گیرد. پرسش مهم در این مورد آن است که آیا مجازات هر یک از جرایم، برابر مقررات تعدد مادی جرم (مادهٔ ۱۳۴ ق.م.ا.) تعیین می‌شود و یا اینکه به حکم خاص (مجازات کلاهبرداری رایانه‌ای) اکتفا می‌شود؟ پاره‌ای از حقوق‌دانان در این فرض، قائل به تعدد مادی بوده و شمول عنوان کلاهبرداری را نافی مقررات تعدد نمی‌دانند (زراعت، ۱۳۹۴: ۳۹۲/۲). برخی دیگر، اقداماتی مانند دسترسی غیرمجاز را مقدمه کلاهبرداری رایانه‌ای می‌دانند، اما تحصیل مال از طریق اخلال سامانه یا تخریب داده را مشمول حکم تعدد قرار می‌دهند (عالی‌پور، ۱۳۹۵: ۲۷۱ و ۲۸۱). به‌نظر می‌رسد اگر رفتار مرتکب در کلاهبرداری رایانه‌ای، با جرایم مذکور قابل انطباق باشد، فقط حکم خاص یعنی کلاهبرداری تعیین می‌شود و مقررات تعدد جرم در این مورد اِعمال نخواهد شد.

بند د مادهٔ ۱۳۴ ق.م.ا. بر تفسیر مذکور صحه گذاشته و مقرر می‌دارد:

«در صورتی که مجموع جرایم ارتکابی در قانون عنوان مجرمانه خاصی داشته باشد، مقررات تعدد جرم اعمال نمی‌شود و مرتکب به مجازات مقرر در قانون محکوم می‌گردد».

بنابراین تغییر یا وارد کردن داده‌های رایانه‌ای، هرچند به تصریح مادهٔ ۷۳۴ ق.م.ا.ت.

مصداق بارز جعل رایانه‌ای است، اما از آنجایی که بخشی از رکن مادی، کلاهبرداری رایانه‌ای است، مشمول حکم جعل نبوده و تابع کلاهبرداری است. بر همین مبنا، حذف داده‌ها که شکلی از تخریب رایانه‌ای است، در فرض صدق عنوان کلاهبرداری رایانه‌ای بر رفتار، موجبی برای انتساب اتهام تخریب داده وجود نداشته و مرتکب از این حیث قابل تعقیب و مجازات نمی‌باشد. پر واضح است که اگر تخریب یا تغییر داده به نتیجه نینجامد و فرد نتواند به مال یا خدمات دسترسی یابد، اتهام تخریب یا جعل رایانه‌ای قابل پیگیری می‌باشد. در این مورد، در صورت صدق عنوان «شروع به کلاهبرداری»، اِعمال قواعد تعدد معنوی بین جرایم مذکور و شروع به کلاهبرداری (در صورت تحقق شرایط شروع به شرح مادهٔ ۱۲۲ ق.م.ا.) و تعیین مجازات اشد الزامی است. ترتیب مذکور در مورد سایر مصادیق مانند دسترسی غیر مجاز باید اِعمال شود.

چنانچه تعدد در کلاهبرداری از نوع مادی باشد، مانند آنکه کاربر از طریق دزدیِ اطلاعات دیگران (فیشینگ)، از حساب اشخاص متعددی وجوهی خارج نماید، مطابق قواعد تعدد مادی مجازات تعیین می‌شود. اگر تقلب در سامانه به گونه‌ای باشد که همزمان موجب برداشت وجوه به صورت خودکار از حساب چند نفر گردد، رفتار مرتکب هرچند ناشی از یک ترفند رایانه‌ای باشد، مصداق تعدد نتیجه بوده که به تصریح تبصرهٔ ۱ مادهٔ ۱۳۴ ق.م.ا.[۱] تابع مقررات تعدد مادی است.

## نتیجه‌گیری

کلاهبرداری رایانه‌ای به عنوان یک نوع تقلب نسبت به سامانه‌های رایانه‌ای و مخابراتی با ارتکاب رفتارهایی نظیر وارد کردن، تغییر، ایجاد، محو یا توقف در داده‌ها و یا اختلال در سامانه شکل می‌گیرد. وارد کردن داده‌ها، به عنوان یکی از اقدامات موضوع مادهٔ ۷۴۱ ق.م.ا.ت.، اعم از داده‌های صحیح و جعلی است. آنچه در این رابطه اهمیت دارد، رفتار غیر مجاز شخص در ورود به سامانه است؛ مانند آنکه فردی اطلاعات کارت اعتباری و گذرواژه اینترنتی دیگری را در اختیار داشته و بدون اجازه،

۱. تبصرهٔ ۱ مادهٔ ۱۳۴ ق.م.ا.: «در صورتی که از رفتار مجرمانه واحد، نتایج مجرمانه متعدد حاصل شود، طبق مقررات فوق عمل می‌شود».

وجهی از حساب او برداشت نماید که در این صورت، رفتار وی مشمول کلاهبرداری رایانه‌ای است. ایرادی که بر مادهٔ ۷۴۱ ق.م.ا.ت. وارد می‌باشد، در همین نکته است که تمایزی میان داده‌های واقعی و غیر واقعی نمی‌گذارد و این مغایر با ضابطهٔ تقلب در کلاهبرداری است. این رویکرد بیشتر متأثر از سند بوداپست ۲۰۰۱ است که وارد کردن داده‌ها را به صورت مطلق به عنوان رکن مادی کلاهبرداری در نظر می‌گیرد.

رکن مادی کلاهبرداری، هرچند در عمل با جرایم دیگر مانند جعل یا تخریب رایانه‌ای یا دسترسی غیر مجاز تداخل نماید، اما مادامی که رفتار در شمول عنوان کلاهبرداری قرار دارد، موجبی برای اِعمال مقررات تعدد مادی یا معنوی وجود ندارد. اما در فرض عدم تحقق آخرین رکن مادی (تحصیل مال یا منفعت)، اِعمال قواعد تعدد معنوی بین جرایم مذکور و شروع به کلاهبرداری اجتناب‌ناپذیر است.

موضوع کلاهبرداری رایانه‌ای، افزون بر وجه و مال، شامل منفعت، امتیاز و خدمات مالی نیز می‌شود. چنانچه تحصیل متقلبانهٔ خدمات به صورت دستکاری یا تصرف در دستگاه‌های اندازه‌گیری آب، برق، گاز یا تلفن باشد، حتی در فرض دیجیتالی بودن این دستگاه‌ها، رفتار کلاهبرداری رایانه‌ای نبوده و مشمول حکم جرم خاص (مادهٔ ۲ قانون مجازات استفاده‌کنندگان غیر مجاز از آب، برق، تلفن، فاضلاب و گاز، مصوب ۱۳۹۶) است. استفاده غیر مجاز از «اشتراک خدمات ارتباطی و فناوری اطلاعات» نیز به شرط باز بودن سامانه و ارتباط گرفتن با آن بدون نیاز به وارد کردن داده یا تقلب یا اختلال در سامانه، جرم خاص بوده و مشمول مادهٔ ۱ قانون مذکور است.

کلاهبرداری رایانه‌ای به شرحی که آمد، بر خلاف برداشت رایج، یک جرم مطلق بوده و تحصیل مال یا امتیاز مالی، نتیجه محسوب نشده و بخشی از فرایند رکن مادی محسوب می‌شود. وقوع ضرر یا انتفاع مرتکب شرط نبوده و به مجرد تحصیل، حتی اگر به بردن و تصاحب مال نینجامد، جرم واقع می‌شود. بر خلاف کلاهبرداری موضوع مادهٔ ۱ قانون تشدید که به فریب و بردن مال تصریح شده، در کلاهبرداری رایانه‌ای، همین که مال در سلطهٔ دیگری قرار گیرد، تحصیل محقق شده و بردن شرط نیست. واریز وجه به حساب کلاهبردار، اگر به سبب آگاهی بانک، به وصول و تصاحب آن منتهی نشده و در واقع بردن محقق نشود، کلاهبرداری رایانه‌ای محسوب می‌شود. بر

همین مبنا، رکن معنوی این جرم، قصد نتیجه نبوده و «تحصیل» نتیجه محسوب نشده و بخشی از فرایند رفتار مرکب است و از این رو، قصد تحصیل هرچند باید احراز شود، اما این قصد ارتباطی به خواست نتیجه نداشته و قصد ارتکاب بخشی از رکن مادی کلاهبرداری است.

مجازات کلاهبرداری رایانه‌ای، برابر مقررات عمومی قابل تعلیق و تخفیف است. البته با حذف تبصرهٔ ۱ مادهٔ ۱ قانون تشدید با مادهٔ ۱۵ قانون کاهش حبس تعزیری (۱۳۹۹)، مجازات کلاهبرداری کلاسیک نیز مشمول قواعد تخفیف و تعلیق می‌شود و از این حیث، تمایزی میان این دو نیست. انتشار حکم محکومیت و عدم شمول مرور زمان در روزنامهٔ محلی (مواد ۳۶ و ۱۰۹ ق.م.ا.)، در صورتی که مبلغ بیش از یک میلیارد ریال باشد، در مورد محکومان به کلاهبرداری رایانه‌ای و مخابراتی مصداق ندارد. این رویکرد، به جهت آن است که در متن مادهٔ ۷۴۱ ق.م.ا.ت.، جملهٔ «کلاهبردار محسوب می‌شود» به کار نرفته و از این رو نمی‌توان آثار کلاهبرداری را نسبت به آن پیاده کرد. این سیاستِ ارفاقی به کلاهبرداری رایانه‌ای، از آنجایی که برابر پیمایش‌های جهانی، ترس از قربانی شدن در برابر آن به ویژه در سال‌های اخیر، افزایش یافته است، توجیه معقولی ندارد و قانون‌گذار به جهت نداشتن درک درستی از پیامدها و وخامت و شدت این جرم، تناسب میان جرم و مجازات را رعایت ننموده و سرانجام سیاست جنایی مناسب و پیشگیرانه‌ای اتخاذ نکرده است.

## کتاب‌شناسی


۱. آقایی‌نیا، حسین و هادی رستمی، ***حقوق کیفری اختصاصی؛ جرایم علیه اموال و مالکیت***، چاپ دوم، تهران، میزان، زمستان ۱۳۹۷ ش.

۲. الهی‌منش، محمدرضا و محسن مرادی اوجقاز، ***جرایم علیه اموال و مالکیت***، چاپ چهارم، تهران، مجد، ۱۳۹۵ ش.

۳. باستانی، برومند، ***جرائم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری***، چاپ سوم، تهران، بهنامی، ۱۳۹۰ش.

۴. پاکزاد، بتول و محمدحسین آزادی‌خواه، «مبانی جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته»، ***مطالعات حقوق کیفری و جرم‌شناسی***، دانشگاه تهران، دورهٔ سوم، شمارهٔ ۲، پاییز و زمستان ۱۳۹۵ ش.

۵. حسنی، محمود نجیب، ***رابطهٔ سببیت در حقوق کیفری***، ترجمهٔ سیدعلی عباس‌نیای زارع، مشهد، دانشگاه علوم اسلامی رضوی، ۱۳۸۵ ش.

۶. خرم‌آبادی، عبدالصمد، «کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران»، ***فصلنامهٔ مطالعات حقوق خصوصی***، دانشگاه تهران، سال سی و هفتم، شمارهٔ ۲، تابستان ۱۳۸۶ ش.

۷. رستمی، هادی و فرهاد میرزایی، «تحولات تاریخی کیفر در پرتو صنعتی شدن»، ***مجلهٔ حقوقی دادگستری***، سال هفتاد و نهم، شماره ۹۲، زمستان ۱۳۹۴ ش.

۸. زراعت، عباس، ***حقوق جزای اختصاصی ۲؛ جرایم علیه اموال و مالکیت***، تهران، جاودانه، جنگل، ۱۳۹۲ ش.

۹. همو، ***شرح مختصر قانون مجازات اسلامی مصوب ۱۳۷۵ (اصلاحی ۱۳۹۲)***، چاپ دوم، تهران، ققنوس، ۱۳۹۴ ش.

۱۰. زیبر، اولریش، ***جرایم رایانه‌ای***، ترجمهٔ محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، چاپ دوم، تهران، کتابخانهٔ گنج دانش، ۱۳۹۰ ش.

۱۱. سالاری، مهدی، ***حقوق کیفری اختصاصی، کلاهبرداری و ارکان متشکلهٔ آن***، چاپ دوم، تهران، میزان، ۱۳۹۳ ش.

۱۲. صابری، راضیه و دیگران، «چالش‌های اِعمال مطلق اصل تقارن عناصر مادی و معنوی»، ***مطالعات حقوق کیفری و جرم‌شناسی***، دانشگاه تهران، دورهٔ چهل و هشتم، شمارهٔ ۲، پاییز و زمستان ۱۳۹۷ ش.

۱۳. صبوری‌پور، مهدی، «نظام‌مندسازی کیفرگزینی تعزیری در حقوق ایران»، ***مطالعات حقوق کیفری و جرم‌شناسی***، دانشگاه تهران، دورهٔ چهل و هشتم، شمارهٔ ۱، بهار و تابستان ۱۳۹۷ ش.

۱۴. صنعتی، سیدمهدی و مجید عطائی جنتی، ***تحلیلی بر جرایم رایانه‌ای و مخابراتی (جرایم در بستر رایانه، فضای مجازی، شبکه‌های اجتماعی و پیام‌رسان‌ها)***، قم، حقوق پویا، ۱۳۹۷ ش.

۱۵. عالی‌پور، حسن، ***حقوق کیفری فناوری اطلاعات***، چاپ چهارم، تهران، خرسندی، ۱۳۹۵ ش.

۱۶. عاملی، سعیدرضا، ***رویکرد دو فضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی***، تهران، امیرکبیر، ۱۳۹۰ ش.

۱۷. قناد، فاطمه، «کلاهبرداری الکترونیکی در بستر فناوری‌های اطلاعات و ارتباطات»، ***فصلنامه پژوهش حقوق عمومی***، سال دهم، شماره ۲۵، پاییز و زمستان ۱۳۸۷ ش.

۱۸. قیاسی، جلال‌الدین و عباسعلی نیک‌نسب، «تحصیل متقلبانه خدمات»، ***پژوهشنامه حقوق کیفری***، سال پنجم، شمارهٔ ۲، پاییز و زمستان ۱۳۹۳ ش.

۱۹. گسن، رمون، ***جرم‌شناسی بزهکاری اقتصادی (نظریهٔ عمومی تزویر)***، تحقیق و ترجمهٔ شهرام ابراهیمی، چاپ سوم، تهران، میزان، زمستان ۱۳۹۳ ش.

۲۰. گلدوزیان، ایرج، ***حقوق جزای اختصاصی؛ جرایم علیه تمامیت جسمانی، صدمات معنوی، اموال و مالکیت، امنیت و آسایش عمومی***، چاپ نهم، تهران، دانشگاه تهران، بهار ۱۳۸۲ ش.
۲۱. لفیو، واین آر.، ***جرم‌های مالی در نظام ایالات متحدهٔ آمریکا***، ترجمهٔ حسین آقایی‌نیا، تهران، میزان، زمستان ۱۳۹۷ ش.
۲۲. لِوی، مایکل، در: سیمپسون، سالی اس. و دیوید ویزبرد (ویراستاران)، ***جرم‌شناسیِ جرایم یقه سفیدان***، ترجمهٔ حمیدرضا دانش‌ناری و آزاده صادقی، تهران، مجد، ۱۳۹۲ ش.
۲۳. میرمحمدصادقی، حسین، ***حقوق کیفری اختصاصی (۲)؛ جرایم علیه اموال و مالکیت***، چاپ پنجاهم، تهران، میزان، ۱۳۹۶ ش.
۲۴. میرمحمدصادقی، حسین، و محمدرسول شایگان، «بررسی تطبیقی کلاهبرداری سنتی و رایانه‌ای و مجازات‌های آن‌ها در نظام حقوقی ایران»، ***دیدگاه‌های حقوق قضایی***، شماره‌های ۵۱ـ۵۲، پاییز و زمستان ۱۳۸۹ ش.
۲۵. همان‌ها، «راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران»، ***فصلنامه دیدگاه‌های حقوقی***، دانشکدهٔ علوم قضایی و خدمات اداری، شماره‌های ۴۲ـ۴۳، ۱۳۸۶ ش.
۲۶. نجفی‌ابرندآبادی، علی‌حسین، «از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، دیباچه بر ویراست دوم در: پیکا، ژرژ، ***جرم‌شناسی***، ترجمه علی‌حسین نجفی ابرندآبادی، چاپ چهارم، تهران، میزان، ۱۳۹۵ ش.
۲۷. همو، «دربارهٔ بزهکاری و جرم‌شناسی سایبری»، ***فصلنامهٔ تعالی حقوق***، ماهنامهٔ آموزشی دادگستری کل استان خوزستان، سال چهارم، شمارهٔ ۳۶، ۱۳۸۸ ش.
۲۸. ویلیامز، ماتیو، ***بزهکاری مجازی، بزه، انحراف و مقررات‌گذاری برخط***، تهران، میزان، ۱۳۹۱ ش.
۲۹. هولت، تامس ج. و همکاران، ***جرایم سایبری و پزشکی قانونی دیجیتال***، ترجمهٔ محمدسعید شفیعی، مهرنوش ابوذری و فرسیما خامسی‌پور، تهران، کتاب آوا، ۱۳۹۷ ش.
30. Clarkson, C.M.V., ***Understanding Criminal Law***, Fontana Press, London, 1987.
31. ***Convention on Cybercrime***, Budapest, 23.XI.2001, European Treaty Series - No. 185, Available at: <https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf>.
32. Gercke, Marco, ***Understanding Cybercrimes: Phenomena, Challenges and Legal Response***, ITU Publication, 2012, Available at: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014.pdf>.
33. Grönroos, Christian, ***Service Management and Marketing, A customer Relationship Management Approach***, 2nd Ed., England, John Wiley & Sons, 2000.
34. Kunz, Michael & Patrick Wilson, ***Computer Crime and Computer Fraud***, Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland, Department of Criminology and Criminal Justice, Fall 2004, Available at: <https://www.montgomerycountymd.gov/cjcc/resources/files/computer_crime_study.pdf>.
35. Santos Jessica, "E-service quality: a model of virtual service quality dimensions", ***Management Service Quality***, Vol. 13(3), 2003.