مقاله

# مجله پژوهشهای حقوقی

شماره ۶

هزار و سیصد و هشتاد و سه ـ نیمسال دوم





شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_44694.html

# کلاهبرداری رایانه‌ای

حسن عالی‌پور*

**چکیده:** *کلاهبرداری رایانه‌ای به لحاظ خلاقیت مرتکب آن و سهولت و کثرت ارتکابش، مهمترین و شایع‌ترین جرم اقتصادی فضای مجازی رایانه و اینترنت محسوب می‌شود. هر چند به ظاهر در ارتکاب این جرم، رایانه در حد وسیله جرم ظاهر می‌شود اما رایانه و اینترنت کلاهبرداری را توأم با کیفیات و شرایط غیرقابل انکاری می‌کنند که قانونگذاران ناگزیر به شناسایی جرم جدید در کنار کلاهبرداری سنتی هستند. کلاهبرداری رایانه‌ای چون در دنیای جدید به نام دنیای مجازی رایانه و اینترنت (فضای سایبر) با امکانات بی‌شماری تحقق می‌یابد فقط علیه انسان نیست و بلکه غالباً علیه سیستم رایانه‌ای و نرم افزارهای آن است و بنابراین شرط فریب قربانی در آن تا مرز حذف شدن تضعیف می‌شود. موضوع جرم کلاهبرداری رایانه‌ای نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده‌های رایانه‌ای دارای ارزش مالی نیز می‌شود.*

**واژگان کلیدی:** *کلاهبرداری (سنتی)، کلاهبرداری رایانه‌ای، رایانه، داده رایانه‌ای، اینترنت.*

## مقدمه

کلاهبرداری رایانه‌ای صرفاً «کلاهبرداری از طریق رایانه» نیست تا به واسطه آن نقش رایانه در حد یک وسیله ارتکاب جرم معرفی گردد؛ چه در این صورت بر کلاهبرداری به وسیله رایانه خاصیتی مترتب نیست تا با عنوان مجرمانه مجزایی در سیاهه‌های قانون نمود یابد و مباحث جداگانه‌ای را بطلبد. بلکه کلاهبرداری رایانه‌ای جرمی است که رایانه در آن نقش اساسی ایفا می‌کند و عمدتاً برخی از اجزای

* دانشجوی مقطع دکتری حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی

تشکیل دهنده رکن مادی کلاهبرداری را تحت تأثیر قرار می‌دهد و به همین دلیل است که کلاهبرداری رایانه‌ای از کلاهبرداری عام یا سنتی متمایز می‌شود و نسبت به آن جرم‌انگاری جدید و طرح مباحث متفاوت صورت می‌گیرد. بنابراین کلاهبرداری رایانه‌ای در ذیل جرائم رایانه‌ای قرار می‌گیرد که طبیعتاً برای اینکه بدانیم آیا اصولاً پدیده‌ای به نام کلاهبرداری رایانه‌ای وجود دارد یا خیر و چنانچه سایه این پدیده مجرمانه بر سر صنعت فناوری اطلاعات و شبکه‌های اطلاع رسانی رایانه‌ای سنگینی می‌کند چگونه و با توجه به چه معیاری باید شناخته شود، منوط به درک واقعیت و ماهیت جرم رایانه‌ای است.

واقعیت یا هستی جرم رایانه‌ای هنوز مورد تأیید برخی از حقوقدانان قرار نگرفته است و اصولاً این عده معتقدند که چیزی به نام جرم رایانه‌ای وجود ندارد تا «رایانه‌ای» را ویژگی برخی از جرائم سنتی همانند سرقت، جاسوسی، کلاهبرداری و غیره دانسته و معیار تفکیک قرار داد. آنچه که با عنوان جرم رایانه‌ای شناخته می‌شود کلاً در بطن سایر جرائم که مقررات کیفری پیش‌بینی کرده‌اند، قرار می‌گیرد؛ زیرا سیستم رایانه‌ای در ارتکاب جرائم فقط در حد وسیله جرم ظاهر می‌شود و به لحاظ تغییر ماهیت وسیله جرم هیچ گاه عنوان مجرمانه تغییر ماهیت نمی‌دهد.[1] به عنوان مثال با تمسک به وسیله جرم، قتل عمد را به قتل عمد با سلاح، قتل عمد با ریسمان، قتل عمد با چاقو و غیره تقسیم نمی‌کنند و هویت جداگانه‌ای برای آنها قایل نمی‌شوند. علاوه بر این برای تحقق هر جرم علاوه بر رکن قانونی و رکن روانی (عمد یا تقصیر) باید رکن مادی با تمام اجزای مورد نظر تحقق یابد که سه جزء زیر تقریباً مشترک اکثر جرائم است: تحقق فعل فیزیکی، شرایط و اوضاع و احوال توأم با فعل فیزیکی مجرمانه و حصول نتیجه مجرمانه در جرائم عمدی مقید و جرائم غیرعمدی. حال باید دید که پدیدهٔ جرم رایانه‌ای برای واقعیت و موجودیت داشتن در کدام یک از اجزاء یا ارکان با جرم سنتی متفاوت است. در تمامی موارد، جرم رایانه‌ای نیز توأم با ارکان سه گانه جرم و اجزای مورد نیاز ذیل آنها می‌باشد جز اینکه

[1] سوزان برنر در مقاله خود با عنوان «آیا چیزی به نام جرم مجازی وجود دارد؟» با طرح تک تک جرائم به این سؤال پاسخ منفی می‌دهد. نک: سوزان برنر؛ «آیا چیزی به نام جرم مجازی وجود دارد؟»، ترجمه عباس گودرزی، ***جزوه تحقیقاتی کمیته مبارزه با جرائم رایانه‌ای شورای عالی توسعه قضائی***، خرداد ۱۳۸۲.

در قسمت وسیله جرم، سیستم رایانه‌ای جایگزین سایر وسایل ارتکاب جرم می‌شود که این امر نیز تأثیری در ماهیت جرم ندارد. از حیث مکان وقوع جرم نیز نمی‌توان جرم رایانه‌ای را توجیه کرد؛ چه فضای مجازی اینترنت و رایانه جز اینکه موقعیت ارتکاب جرائم را از حیث تنوع و تکثر، افزایش و به طور خیره کننده‌ای مدت زمان ارتکاب جرم را کاهش داده‌اند، تغییری در ارکان و اجزای جرائم ایجاد نکرده‌اند و بدیهی است که همین جرائم با امکانات و مدت زمان بیشتر ولیکن با موقعیت کمتر در دنیای واقعی (بیرون از محیط مجازی اینترنت و رایانه) قابل ارتکاب‌اند. همچنان که به لحاظ مکان و بستر ارتکاب جرائم آنها را به اقسام مختلف تقسیم نمی‌کنند؛ به عنوان مثال جرم سرقت را بسته به مکان ارتکاب به سرقت از خیابان‌ها، سرقت از فروشگاه‌ها، سرقت از منازل، سرقت از بانک‌ها و... دسته‌بندی نمی‌کنند. نتیجتاً رایانه و اینترنت در قبال جرائم یا در حد وسیله ارتکاب جرم است یا مکان ارتکاب جرم که این مورد را همه به گونه‌ای می‌توان به عنوان وسیله جرم در نظر گرفت که قاعدتاً با این وصف رایانه و اینترنت موجبی برای جرم‌انگاری جدید و پدید آمدن عناوین مجرمانه نوین نخواهد بود.

در مقابل قائلین به عدم واقعیت جرم رایانه‌ای باید به واقعیت جرم رایانه‌ای صحه گذاشت؛ با این توضیح که اینترنت و رایانه هم وسیله ارتکاب جرم محسوب می‌شوند هر چند در ماهیت و اجزای جرم تغییر اساسی به وجود نمی‌آید اما غالب کشورها ناگزیر از شناسایی این جرائم و وضع مقررات خاص پیرامون آنها شده‌اند؛ زیرا وسیله ارتکاب جرم بودن رایانه به قدری با شداد و غلاظ همراه است که سایر اجزای تشکیل دهنده جرم را تحت تأثیر قرار می‌دهد. به عبارت دیگر در ارتکاب جرائم سنتی با رایانه، کیفیاتی به وجود می‌آید که جرم ارتکابی جدید را از جهات مختلف با جرم سنتی متفاوت می‌کند. وقتی کلاهبرداری از طریق سیستم رایانه‌ای ارتکاب می‌یابد برخلاف کلاهبرداری سنتی که به موجب ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ از طرق دیگر در عالم واقعی نمود می‌یابد، قربانی جرم غالباً برای مرتکب کلاهبرداری رایانه‌ای شناخته شده نیست، زمان لازم برای تحقق جرم به طور چشمگیر کاهش می‌یابد، لحظه ارتکاب جرم در هاله‌ای از ابهام فرو می‌رود و ممکن است به جای انسان، یک ماشین دچار اشتباه و اغفال شود. این کیفیات جدید به مقتضای رایانه پدید آمده‌اند و

شرایط تحقق اجزای جرائم سنتی را تحت تأثیر قرار می‌دهند و به همین دلیل اسناد بین‌المللی و قوانین کیفری اکثر کشورها جرائم سنتی قابل ارتکاب با رایانه را با عنوان مجرمانه جدید مانند کلاهبرداری رایانه‌ای، جعل رایانه‌ای، سرقت رایانه‌ای و... به رسمیت شناخته‌اند.

در جایی که اینترنت و رایانه هدف یا موضوع جرم قرار می‌گیرند، واقعیت بخشیدن به جرم رایانه‌ای آسانتر خواهد بود؛ چون اینترنت و رایانه به عنوان اجزای تشکیل دهنده دنیای جدید (فضای سایبر)[۲] موضوعات جدیدی ایجاد کرده‌اند که این موضوعات به لحاظ اینکه در دنیای واقعی وجود نداشته‌اند مورد توجه قانونگذاران نیز قرار نگرفته‌اند. بنابراین جرائمی همانند نفوذ غیرمجاز،[۳] جعل و تخریب دادهٔ رایانه‌ای، اختلال در سیستم رایانه‌ای، انتشار ویروس رایانه‌ای و... را نمی‌توان در قالب جرائم سنتی درآورد؛ زیرا موضوع این قبیل جرائم موضوعی است که فقط در فضای سایبر و با استعانت از رایانه واقعیت می‌یابد.

پس از پذیرش واقعیت وجودی جرم رایانه‌ای باید دید که ماهیت آن چیست و با توسل به چه شرایطی تعریف می‌شود. ماهیت جرم رایانه‌ای همانند واقعیت آن جدال‌آمیز و بحث‌انگیز است و هر شخص یا نهاد ملی یا بین‌المللی، تعریف متفاوتی از آن ارائه داده‌اند و به لحاظ اینکه در این مختصر مجال طرح آنها نیست، باید به همین میزان بسنده کرد که جرم رایانه‌ای جرمی است که یا اطلاعات و نرم افزارهای رایانه‌ای موضوع جرم واقع می‌شوند یا سیستم رایانه‌ای وسیله ارتکاب جرم قرار می‌گیرد. اما بحث مهمتر در ماهیت جرم رایانه‌ای که بر جرائم رایانه‌ای و از جمله کلاهبرداری نیز تأثیرگذار است، این است که چرا اصطلاح جرم رایانه‌ای از عناوین مشابه مانند جرم اینترنتی، جرم سایبری، جرم شبکه‌ای و جرم نرم‌افزاری مناسب‌تر است؟ جرم اینترنتی به جرم قابل ارتکاب در محیط اینترنت گفته می‌شود و اگر بین شبکه‌های اطلاع رسانی متصل به هم از حیث خاص و عام و محلی و ملی و بین‌المللی بودن قائل به تفکیک شویم، باید گفت اینترنت در مفهوم واقعی خویش به معنای شبکه‌های رایانه‌ای مرتبط به هم است که در سطحی گسترده کاربران و مشترکین متعددی را به هم پیوند می‌دهد. اما اگر شبکه‌های رایانه‌ای مرتبط به هم در

---

2 cyber space

3 Hack

قالب یک ساختمان یا شرکت یا نهاد بوده و یا اینکه محلی[۴] باشند، حمل شبکه اینترنت بر آنها بلااشکال نیست، چه اینترنت خصیصه جهانی داشته و محصول ارتباط رایانه‌های بی‌شماری است. از این حیث جرم اینترنتی حتی از جرم شبکه‌ای که ناظر به هر نوع شبکهٔ اطلاع رسانی می‌باشد، محدودتر خواهد بود.

جرم سایبری[۵] به جرم قابل ارتکاب در محیط مجازی اینترنت و مخابرات گفته می‌شود. جرم سایبری از جرم اینترنتی عام‌تر است و علاوه بر اینکه شامل جرائم مخابراتی می‌شود می‌تواند به جرائم علیه نرم‌افزارهای یک رایانه که به صورت مجازی در سیستم رایانه‌ای قرار دارد نیز تسری داده شود و به همین دلیل در مقررات کشورها و اسناد بین‌المللی به ویژه کنوانسیون جرائم قابل ارتکاب در محیط سایبر بوداپست مصوب سپتامبر ۲۰۰۱ از عنوان «جرم سایبری» استفاده شده است. جرم نرم‌افزاری نیز غیر از اینکه از حیث عنوان موضوعات محدودی را در بر می‌گیرد، جرائم مرتبط با عملکرد رایانه را نیز در بر نمی‌گیرد. اما با چشم پوشی از اصطلاح «جرم سایبری» که هم در حقوق کشورمان شناخته شده نیست و هم محدودتر از جرم رایانه‌ای است، اصطلاح «جرم رایانه‌ای»[۶] از جهات مختلف مناسب به نظر می‌رسد. توضیح اینکه جرم رایانه‌ای شامل کلیه جرائمی می‌شود که به نوعی در آنها رایانه ایفای نقش می‌کند و از آنجایی که قوام و دوام اینترنت و فضای سایبر به وجود رایانه است و سیستم‌های ارتباطی و مخابراتی نیز با رایانه فعالیت می‌کنند و شبکه‌های محلی و منطقه‌ای نیز از رایانه شکل گرفته‌اند و از طرف دیگر نرم‌افزارهای رایانه‌ای جزئی از رایانه تلقی می‌شوند، جرم رایانه‌ای شامل همه این

---

4 Local Area Network

5 cyber crime

۶ جرم رایانه‌ای معادل فارسی جرم کامپیوتری (computer crime) است که فرهنگستان زبان و ادبیات فارسی انتخاب نموده است و از آنجا که به موجب ماده واحده قانون ممنوعیت به کارگیری اسامی، عناوین و اصطلاحات بیگانه مصوب ۱۳۷۵/۹/۱۴، نهادها و مؤسسات دولتی و از جمله مراجع قانونگذاری موظف به استعمال اصطلاحات و عناوین فارسی یا فارسی‌شده هستند، در این مقاله نیز از اصطلاح کلاهبرداری رایانه‌ای استفاده شده است، هر چند مبحث اول از باب چهارم قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ بدون توجه به قانون فوق‌الذکر اصطلاح «کلاهبرداری کامپیوتری» را استعمال کرده است اما در لایحه مجازات جرائم رایانه‌ای که در کمیته مبارزه با جرائم رایانه‌ای معاونت حقوقی و توسعه قضائی قوه قضائیه تدوین شده، از اصطلاح «کلاهبرداری رایانه‌ای» بهره گرفته شده است. نگارش ماده مربوط به کلاهبرداری رایانه‌ای در لایحه مجازات جرائم رایانه‌ای بر عهده نگارنده بوده است.

عناوین می‌شود. البته جرم رایانه‌ای از حیث دایره شمول عنان گسیخته بوده و مفهومی عام‌تر از میزانی که مد نظر ماست، دارد. بنابراین جرم رایانه‌ای را باید منصرف به عملکرد رایانه، نرم‌افزارهای رایانه‌ای و داده و سیستم رایانه‌ای کرد والا هیأت رایانه و لوازم سخت‌افزاری آن بدون توجه به عملکرد و قابلیت آنها مشمول مقررات مباحث سنتی حقوق کیفری خواهد بود. با توجه به مباحث مطرح شده و با این پیش فرض که اولاً کلاهبرداری رایانه‌ای دارای واقعیت وجودی است و ثانیاً رایانه فراتر از وسیله جرم برای تحقق کلاهبرداری ظاهر می‌شود و ثالثاً کلاهبرداری رایانه‌ای عنوان مناسب‌تری از عناوین مشابه مانند کلاهبرداری اینترنتی، کلاهبرداری سایبری و... است، ابتدا به شناسایی کلاهبرداری رایانه‌ای و نحوه برخورد اسناد بین‌المللی و مقررات کیفری کشورهای پیشرفته با آن و سپس به طرح مباحث حقوقی آن در حقوق داخلی اشاره خواهیم کرد.

## بخش نخست: شناسایی کلاهبرداری رایانه‌ای

کلاهبرداری رایانه‌ای به عنوان یکی از مهمترین اشکال جرائم اقتصادی در فضای رایانه و اینترنت جایگاهی ویژه در قانونگذاری کشورهای مختلف و مباحث حقوقدانان یافته است. این جایگاه برجسته عمدتاً تابع سه عامل کثرت ارتکاب، سهولت ارتکاب و فاعل ارتکاب است. کثرت و تنوع ارتکاب کلاهبرداری رایانه‌ای در کشورهایی که رایانه و اینترنت در فعالیت‌های روزمره به طور کامل رسوخ یافته، بسیار نگران کننده است. علاوه بر اینکه کلاهبرداری یک پدیده همیشه بارور است که هر روز به اقسام مختلف نمود می‌یابد، کثرت وقوع آن نیز خیره کننده‌تر از سایر جرائم رایانه‌ای است؛ مثلاً در کشور آلمان طبق آمارهای جنائی پلیس، تعداد گزارش‌های واصله در سال ۱۹۹۹ به پلیس در قبال وقوع جرائم کلاهبرداری رایانه‌ای، تغییر داده‌ها، سابوتاژ رایانه‌ای و جاسوسی اطلاعات رایانه‌ای به ترتیب ۴۴۷۴، ۳۰۲ و ۲۱۰ بوده است. در همین سال تعداد محکومیت‌های صادره در خصوص کلاهبرداری رایانه‌ای ۲۱۵۷ فقره بوده است و حال آنکه در قبال سه جرم تغییر داده‌ها، سابوتاژ رایانه‌ای و جاسوسی اطلاعات تنها هشت حکم محکومیت از

سوی محاکم آلمان صادر شده است.[۷]

سهولت ارتکاب کلاهبرداری رایانه‌ای نیز یکی دیگر از خصایص این جرم است که عمدتاً تابع ارتباط بی‌قید و شرط کاربران اینترنتی با هم است. اگر در قبال جرائمی همانند نفوذ غیرمجاز[۸] یا شنود[۹] می‌توان از تدابیری همچون نصب باروی آتشین[۱۰] یا سایر تدابیر حفاظتی استفاده کرد یا اینکه انتشار محتویات مستهجن را با توسل به پالایش مهار کرد اما مرتکب کلاهبرداری رایانه‌ای از آنجا که رایانه و اینترنت و نرم افزارهای آن را هدف خود قرار نمی‌دهد و صرفاً از آنها به عنوان وسیله‌ای برای به دام انداختن کاربر استفاده می‌کند، از تار و پود تدابیر امنیتی و حفاظتی رسته است و فقط این زیرکی و درایت کاربر یا استفاده کننده از رایانه یا اینترنت خواهد بود که کلاهبردار را ناکام بگذارد والا کلاهبردار در هر شرایطی خواه قربانی در شبکه اینترنتی باشد یا بیرون از شبکه و خواه از طریق گپ اینترنتی[۱۱] و خواه از طریق ارسال رایانامه[۱۲] می‌تواند به مقاصد شوم خود برسد.

فاعل ارتکاب کلاهبرداری رایانه‌ای مهمترین عامل برجستگی این جرم است. هر چند غالباً مجرمان رایانه‌ای از استعداد نسبتاً بالایی برخوردار هستند اما کلاهبرداران رایانه‌ای اشخاصی هستند که زیرکی فریب دادن دیگران را با دانش رایانه‌ای در آمیخته‌اند و بدون تردید در زمره مجرمان یقه سفید قرار می‌گیرند که به میزان خطرناکی و استعداد جنائی بالا، قدرت انطباق اجتماعی قابل توجهی دارند و به همین ترتیب علی‌رغم اینکه توجهات دیگران را نسبت به اعمال غیرقانونی خود برنمی‌انگیزانند، به راحتی و به کرات رایانه و اینترنت را جولانگاه مانورهای متقلبانه خود می‌سازند. نظر به این ویژگی‌ها که کلاهبرداری رایانه‌ای به همراه دارد، توجه خاصی از سوی حقوقدانان نسبت به این جرم معطوف شده است و برخی از آنها کلاهبرداری رایانه‌ای را که مصداق برجسته سوءاستفاده از رایانه[۱۳] است در زمره

---

[۷] دکتر کریستین شوارتزینگه، ***جزوه مسؤولیت کیفری ارائه دهندگان خدمات اینترنتی، پخش ویروس‌های رایانه‌ای***، شورای عالی توسعه قضائی، کمیته مبارزه با جرائم رایانه‌ای، ص ۲.

[8] Hack-Illegal access

[9] Interception

[10] Firewall

[11] chat

[12] Electronic Mail

[13] computer Manipulation

شایع‌ترین جرائم اقتصادی رایانه‌ای قلمداد می‌کنند.[۱۴] با این وصف، اهمیت شناسایی جرم کلاهبرداری رایانه‌ای پوشیده نمی‌ماند و در راستای بررسی این مهم ناگزیر از طرح چهار بحث هستیم: تعریف کلاهبرداری رایانه‌ای، پیشینه کلاهبرداری رایانه‌ای، اقسام کلاهبرداری رایانه‌ای و عناوین مشابه با کلاهبرداری رایانه‌ای.

## بند نخست: تعریف کلاهبرداری رایانه‌ای

مناسب‌ترین تعریف از هر جرمی تعریفی است که خود قانونگذار ارائه می‌دهد و بنابه اینکه قانونگذار همواره از اینکه نتواند تعریف جامع و مانعی از یک عمل مجرمانه ارائه دهد، هراسان است؛ در غالب موارد بدون ارائه تعریف به ذکر اوصاف شرایط جرم اکتفا می‌کند و بنابراین جرائم عمدتاً از سوی حقوقدانان تعریف می‌شوند. کلاهبرداری عبارت است از بردن مال دیگری از طریق توسل توأم با سوءنیت به وسایل متقلبانه.[۱۵] تعریف کلاهبرداری رایانه‌ای نیز به لحاظ اینکه رایانه در تحقق آن عمدتاً وسیله ارتکاب است، قاعدتاً باید مشابه همین تعریف باشد. اما با توجه به نکات زیر ضرورت ارائه تعریفی جداگانه از کلاهبرداری رایانه‌ای احساس می‌شود:

**الف** – فعل فیزیکی جرم کلاهبرداری توسل به وسایل متقلبانه و بردن مال دیگری است که البته نسبت به وسایل پرداخت مال مانند چک، تحصیل آنها نیز به عنوان یکی از افعال فیزیکی مطرح می‌شود. به دلیل تعدد فعل فیزیکی در جرم کلاهبرداری است که از آن به جرم مرکب یاد می‌شود. اما کلاهبرداری رایانه‌ای سوءاستفاده مالی به وسیله رایانه است که از طریق افعال فیزیکی متعددی همچون وارد کردن، تغییر، محو و توقف داده‌های رایانه‌ای تحقق می‌یابد و در واقع فعل فیزیکی کلاهبرداری رایانه‌ای هرگونه سوءاستفاده مالی از طریق رایانه است هر چند در قالب افعال تمثیلی مذکور تحقق یابد و از این حیث یک جرم ساده تلقی می‌شود تا یک جرم مرکب.

---

[14] Ulrish Sieber, "Computer Crime and Criminal Information Law", *http://www.jura.uni-muenchen.de/sieber,p.4.*

[۱۵] دکتر حسین میرمحمد صادقی، ***جرائم علیه اموال و مالکیت***، تهران، نشر میزان، چاپ دوم، پائیز ۱۳۷۶، ص ۴۶.

**ب** – یکی از اجزای رکن مادی کلاهبرداری، فریفته شدن قربانی است و لازمه فریفته شدن این است که قربانی جرم انسان باشد و عموماً برای مرتکب نیز شناخته شده باشد؛ هر چند، در اکثر مواقع بین مرتکب و قربانی ارتباط عینی حاصل می‌شود اما در کلاهبرداری رایانه‌ای تحقق جزء فریب قربانی لازم نیست؛ چه علاوه بر اینکه در غالب موارد قربانی جرم برای کلاهبردار رایانه‌ای شناخته شده نیست، ممکن است اقدامات خدعه‌آمیز مرتکب علیه سیستم رایانه‌ای باشد، بدون اینکه در این میان انسانی فریفته گردد. پس به همین میزان که شخصی از طریق گمراه کردن رایانه و یا حتی بدون گمراه کردن آن و از طریق کسب برخی اطلاعات مالی از طریق رایانه مال یا مزایای مالی را تحصیل نماید، کلاهبردار رایانه‌ای محسوب می‌شود.

**ج** – موضوع یا هدف جرم کلاهبرداری مال یا وسیله تحصیل مال است؛ لیکن در کلاهبرداری رایانه‌ای موضوع جرم فراتر می‌رود و علاوه بر مال شامل منافع مالی، خدمات و امتیازات مالی نیز می‌شود؛ چون کلاهبرداری رایانه‌ای نوعی سوءاستفاده از رایانه و اینترنت است و از آنجایی که اکثر امکانات متضمن خدمات و مزایای مالی، رایانه‌ای شده‌اند، امکان سوءاستفاده از آنها زیاد است. جالب اینکه در قوانین برخی از کشورها کلاهبرداری از حد هر گونه سوءاستفاده مالی از طریق رایانه نیز فراتر رفته است؛ به عنوان مثال طبق بخش ۱۰۳۰ از ماده ۱۸ قانون جزای ایالات متحده امریکا مصوب ۱۹۸۳ و اصلاحی ۱۹۹۶، دسترسی بدون مجوز به اطلاعات طبقه‌بندی شده یا اطلاعات انرژی اتمی یا هر نوع اطلاعاتی که به کشور امریکا ضربه وارد نماید، در زمره کلاهبرداری و فعالیت‌های مرتبط با آن به حساب آمده است.

**د** – پیشرفت هر روزه صنعت انفورماتیک و توسعه حیرت‌انگیز فناوری اطلاعات از یک سو و تنوع‌یابی اشکال سوءاستفاده مالی از طریق رایانه و اینترنت از سوی دیگر این موضوع را پیش می‌کشد که کلاهبرداری رایانه‌ای باید دایره‌ای بس وسیع‌تر از کلاهبرداری سنتی داشته باشد تا بتواند برای هر شکل از سوءاستفاده‌های مالی رایانه‌ای با تمسک به قانون، پاسخ کیفری داشته باشد و قاعدتاً کلاهبرداری رایانه‌ای تعریفی گسترده‌تر از تعریف کلاهبرداری سنتی می‌طلبد.

هر چند قوانین کیفری اکثر کشورها از تعریف کلاهبرداری رایانه‌ای امتناع ورزیده‌اند اما شورای اروپا با توجه ملاحظات فوق‌الذکر در یک تعریف موسع مقرر می‌دارد که کلاهبرداری رایانه‌ای عبارت است از وارد کردن، تغییر یا ایجاد وقفه در

داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای یا دیگر مداخلات نسبت به پردازش داده‌ها که نتیجه پردازش داده‌ها را تحت تأثیر قرار می‌دهد، خواه موجب ضرر اقتصادی، خواه موجب از دست دادن اموال و تصرف آنها با قصد کسب منفعت و امتیاز اقتصادی غیرقانونی برای خود یا دیگری شود.[۱۶]

بنابراین با توجه به این مطالب و با الهام از تعریف شورای اروپا که در سال ۱۹۸۹ ارائه داده است، کلاهبرداری رایانه‌ای را می‌توان به این صورت تعریف کرد: «هر گونه سوءاستفاده مالی یا تحصیل منفعت یا خدمات مالی یا امتیازات مالی با انجام اعمالی نظیر وارد کردن، تغییر، محو، ایجاد یا توقف داده از طریق سیستم رایانه‌ای».

## بند دوم: پیشینه کلاهبرداری رایانه‌ای

کلاهبرداری رایانه‌ای در زمره جرائم نسل اول رایانه‌ای است که در این نسل رایانه صرفاً وسیله ارتکاب جرم تلقی می‌شود و بنابراین می‌توان کلاهبرداری رایانه‌ای را به عنوان یکی از اولین جرائم رایانه‌ای پس از دخالت بی‌چون و چرای رایانه در فعالیت‌های روزمره زندگی بشر دانست. قضیه رویس نخستین پرونده کلاهبرداری رایانه‌ای شناخته شده است که در دهه ۱۹۶۰ مطرح و منجر به محکومیت مرتکب شد. «در این قضیه رویس حسابدار یک شرکت بود و چون به زعم وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پول‌های شرکت را به خود اختصاص می‌داد. مکانیزم کار به این‌گونه بود که شرکت محل کار وی یک عمده فروش میوه و سبزی بود و محصولات متنوعی را از کشاورزان می‌خرید و با استفاده از تجهیزات خود از قبیل کامیون، انبار و بسته‌بندی و سرویس‌دهی به گروه‌های فروشندگان، آنها را عرضه می‌کرد. به دلیل وضعیت خاص این شغل، قیمت‌ها در نوسان بود و ارزیابی امور تنها می‌توانست از عهده رایانه برآید تا کنترل محاسبات و عملیات این شرکت عظیم را عهده‌دار شود. کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورت‌حساب‌ها به صورت اطلاعات مضبوط در نوارهای الکترونیکی بود. رویس در برنامه‌ها دستورالعمل‌های اضافی را گنجانده بود و قیمت کالاها را با

[۱۶] بتول پاکزاد، «اقدامات سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرائم رایانه‌ای»، ***مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات***، خرداد ماه ۱۳۸۳، ص ۴۸.

ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس وی مبلغی را کاهش می‌داد و مبالغ حاصله را به حساب‌های مخصوصی واریز می‌کرد. بعد در برهه‌های زمانی خاص چکی به نام یکی از ۱۷ شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند».[۱۷] در دهه ۶۰ سوءاستفاده‌های مالی همچون سوءاستفاده مالی رویس کمتر با مقررات مربوط به کلاهبرداری منطبق بود؛ زیرا عمل مرتکب با فقدان فریب قربانی نوعی سوءاستفاده مالی صرف یا اختلاس بود و همین امر قانونگذاران برای تجدید نظر در مقررات مربوط به کلاهبرداری به تکاپو واداشت.

با ظهور اینترنت و با مطرح شدن دنیای مجازی جدید، تعدد و تکثر کلاهبرداری‌ها به قدری است که به طور قطع نمی‌توان تاریخ نخستین کلاهبرداری در محیط مجازی اینترنت را تعیین کرد؛ مخصوصاً اینکه مرتکبان با مهارت خاصی از خود کمترین نشانه‌ای باقی نمی‌گذارند و با توجه به این نکته که قربانیان نیز بنا به برخی مسائل مثل برچسب ساده‌لوحی یا ترس از آبروریزی از طرح شکایت استنکاف می‌ورزند، آمار سیاه بزهکاری کلاهبرداری رایانه‌ای بسیار بالاست اما هر چند طلیعه کلاهبرداری رایانه‌ای چندان روشن نیست اما تا زمانی که فضای سایبر باقی است و تا زمانی که انسان قدم‌های مجازی خود را در آن می‌نهد، نمی‌توان از غروب و افول کلاهبرداری رایانه‌ای سخن گفت.

## بند سوم: اقسام کلاهبرداری رایانه‌ای

موضوع جرم کلاهبرداری رایانه‌ای، مال، وسایل تحصیل مال از قبیل چک، منافع مالی، خدمات مالی و مزایای مالی است. بنابراین هدف جرم حول محور مال یا هر چیز دارای ارزش مالی می‌چرخد. کلاهبرداری اطلاعاتی که در حقوق برخی کشورها شناخته شده است، از آنجا که ممکن است برخی از این اطلاعات یا داده‌ها دارای ارزش مالی نباشد، دقیقاً منطبق بر کلاهبرداری رایانه‌ای مورد نظر ما نیست همچنان که اگر شخصی با روش‌های خدعه‌آمیز صرفاً حق استفاده از رایانه یا فرصت بهره‌برداری از نرم افزارهای دیگری را به دست آورد، نیز کلاهبردار شناخته

[۱۷] محمدحسن دزیانی، «جرائم کامپیوتری»، ***خبرنامه انفورماتیک***، ش ۶۲، ص ۵۳.

نمی‌شود. با توجه به اینکه موضوع کلاهبرداری هر چیز دارای ارزش مالی است و روش ارتکاب آن نیز تمثیلی می‌باشد، در بادی امر اثری بر تقسیم‌بندی نسبت به این جرم مترتب نیست. اما از آنجایی که تقسیم‌بندی کلاهبرداری علاوه بر اینکه پرده از طرق مختلف توسل کلاهبرداران به فریب کاربران برمی‌دارد و کاربران را از اقدامات و فریب‌های مشابه برحذر می‌دارد، موجب مطالعه آماری این جرم و بررسی میزان شیوع آن در فضای سایبر می‌شود تا بدین وسیله قانونگذار تدبیری در پیشگیری از وقوع کلاهبرداری رایانه‌ای اتخاذ نماید. نخستین و مهمترین تقسیم‌بندی از کلاهبرداری رایانه‌ای متعلق به مرکز دادخواهی کلاهبرداری اینترنتی[۱۸] ایالات متحده امریکا است. این مرکز که با همکاری اداره تحقیقات جنائی فدرال[۱۹] و مرکز ملی جرائم یقه سفید،[۲۰] فعالیت خود را از سال ۲۰۰۰ آغاز کرده، مطالعه آماری جالبی پیرامون میزان شکایت‌ها از کلاهبرداری رایانه‌ای، تعداد متهمان و محکومان و تعداد شکات و بعضی از دیگر جرائم رایانه‌ای را در سطح داخلی و بین‌المللی انجام داده است.

مرکز دادخواهی کلاهبرداری اینترنتی پس از یک سال مطالعه و بررسی مستمر در سال ۲۰۰۱ مجموعاً کلاهبرداری رایانه‌ای بر نه قسم دسته‌بندی کرد که در ذیل هر قسم انواع دیگری از مصادیق این جرم قرار می‌گیرند:[۲۱]

**۱- کلاهبرداری از مؤسسات مالی:**[۲۲] در این قسم از کلاهبرداری رایانه‌ای، مرتکب از طریق سوءاستفاده از کارت‌های اعتباری یا بدهی[۲۳] یا سرقت هویت[۲۴] دیگری و اتخاذ یک هویت جعلی مبادرت به فریب یک تجارتخانه یا سازمان می‌کند و سرمایه آن را تصاحب می‌کند. این قسم از کلاهبرداری رایانه‌ای از حیث تعداد شکایت در رأس سایر اقسام قرار دارد.

**۲- کلاهبرداری در بازی:**[۲۵] تقلب در شرطبندی از طریق تبانی ورزشی یا

18 Internet Fraud complaint center (IFCC)

19 Federal Bureau of Investigation (FBI)

20 National white collar crime center (NW3C)

21 IFCC 2001 Internet Fraud Report; January, 2001-December 31, 2001, p. 19.

22 Financial Institution Fraud

23 Credit/Debit card Fraud

24 Identity theft

25 Gaming Fraud

ادعاهای دروغین و غیره برای بردن یک جایزه یا برنده شدن در مسابقه از دیگر اقسام کلاهبرداری رایانه‌ای است.

**۳- کلاهبرداری در ارتباطات:**[۲۶] در این قسم، کلاهبردار در فرآیند مبادله اطلاعات و ارتباطات متوسل به تقلب می‌شود و به این وسیله استفاده غیر مجاز از ارتباطات می‌نماید. سرقت خدمات ارتباطی بیسیم، ماهواره‌ای، امواج رادیویی و خطوط زمینی از نمونه‌های کلاهبرداری در ارتباطات است.

**۴- کلاهبرداری در کسب منفعت:**[۲۷] در این جا شخص حقیقی یا حقوقی با به کار بردن مانورهای متقلبانه، قوانین و مقررات موجود در استفاده خدمات را دور زده و به صورت غیرمجاز از آنها استفاده می‌کنند. مثل نفوذ به سیستم رایانه‌ای اداره آب و برق و استفاده مجانی از آنها.

**۵- کلاهبرداری از بیمه:**[۲۸] مرتکب در این قسم از کلاهبرداری در میزان خسارت واقعی وارده بر خود از طریق صحنه‌سازی یا ادعای دروغین تقلب می‌کند. حتی ممکن است مرتکب دچار هیچ گونه خسارتی نشده باشد اما با مانورهای متقلبانه خواستار جبران آن شود.

**۶- کلاهبرداری از دولت:**[۲۹] کلاهبرداری از دولت عبارت است از قلب عمدی حقیقت یا پنهان ساختن حقیقت یک موضوع به قصد انجام عملی به ضرر دولت مشروط بر اینکه این ضرر وارد شود. فرار از پرداخت مالیات یا وانمود ساختن مبنی بر پرداخت مالیات یا تقلب در امور خیریه را می‌توان در ذیل این قسم از کلاهبرداری قرار داد.

**۷- کلاهبرداری در سرمایه‌گذاری:**[۳۰] کلاهبرداری در سرمایه‌گذاری عبارت است از به کار بردن اعمال خدعه‌آمیز در راستای سرمایه‌گذاری برای تحصیل پول یا سود بیشتر. طرح‌های پونزی و هرمی[۳۱] برجسته‌ترین قسم از اقسام سوءاستفاده از سرمایه‌گذاری هستند. طرح پونزی متعلق به چارلز پونزی ایتالیایی است که نخستین

---

26 communications Fraud
27 utility Fraud
28 Insurance fraud
29 Government Fraud
30 Investcent Fraud
31 Ponzi/Pyramid schemes

بار این طرح در امریکا اجرا شد. وی ابتدا از افراد دعوت می‌کند تا در طرح وی مبلغی سرمایه‌گذاری کنند. سپس در قبال آن با دادن سفته‌هایی که به عنوان تضمین به آنها می‌داد، تعهد می‌کرد که طی نود روز اصل سرمایه آنها را به همراه سودی برابر با نصف مبلغ سرمایه‌گذاری شده بپردازد. از این رو اگر کسی ۱۰۰ دلار در طرح وی سرمایه‌گذاری می‌کرد طی نود روز ۱۵۰ دلار و اگر کسی ۱۰۰۰ دلار سرمایه‌گذاری می‌کرد، ۱۵۰۰ دلار دریافت می‌کرد. در واقع کاری که پونزی انجام می‌داد، استفاده از سرمایه‌گذاران جدید جهت پرداخت اصل مبالغ و سود سرمایه‌گذاران جدید بود و چون به تدریج وی با پرداخت به موقع سود افراد، خوش حسابی خود را ثابت کرده بود؛ افراد، دیگر سود خود را هم دریافت نکرده و از آن به عنوان مبلغ جدیدی جهت سرمایه‌گذاری بیشتر و بردن سود فزونتر استفاده می‌کردند.[۳۲] طرح‌های هرمی نظیر پنتاگونا و گلدکوئیست نیز تحصیل سود خیره کننده از طریق جست و جوی سرمایه‌گذاران جدید بود که افزونی هر طبقه از این سرمایه‌گذاران، ثروت انبوه را برای اشخاص فرادست آنها به همراه داشت.

**۸- کلاهبرداری تجاری:**[۳۳] این قسم از کلاهبرداری عبارت است از توسل به اینترنت برای قلب واقعیت از طریق اعمالی چون ورشکستگی به تقلب یا نقض حق مؤلف و مترجم.

**۹- کلاهبرداری از اعتماد دیگران:**[۳۴] این قسم از کلاهبرداری عبارت است از سوءاستفاده از اعتماد دیگران با توسل قلب حقیقت یا کتمان موضوع که منجر به ضرر دیگری شود. حتی اگر قلب حقیقت موجب شود که دیگری به خود ضرری وارد سازد، در زمره همین قسم از کلاهبرداری است. تقلب در حراج اینترنتی یا عدم تحویل بهای کالای دریافت شده را می‌توان در شمار کلاهبرداری از اعتماد دیگران ذکر کرد.

اقسام گفته شده از کلاهبرداری همگی قابلیت ارتکاب در شبکه اینترنت را دارند اما محدوده کلاهبرداری رایانه‌ای فراتر از این اقسام است و شامل مواردی که

---

[۳۲] مهدی فضلی، «طرح‌های هرمی، باز اریابی‌های چند سطحی و حقوق مصرف کننده»، ***ترجمان حسبه***، سال سوم، بهار و تابستان ۱۳۸۲، ش ۱۰ و ۱۱، ص ۵۳.

[33] Business Fraud

[34] Confidence Fraud

مرتکب یا قربانی جرم یا هر دو آنلاین[۳۵] یا داخل شبکه اینترنت نیستند، نیز می‌شود. مشهورترین کلاهبرداری رایانه‌ای که لزومی به ارتکاب در شبکه اینترنت ندارد، کلاهبرداری از طریق کارت‌های پلاستیکی است. کارت‌های پلاستیکی که با استفاده از رایانه قابلیت کارکرد دارند به سه گروه قابل تقسیم‌اند: اولین گروه کارت‌های دارای ارزش ذخیره شده[۳۶] هستند که ارزش مورد نظر به طور الکترونیکی روی آنها ثبت شده و مشتری‌ها برای انجام معاملات از آنها استفاده می‌کنند. گروه دوم کارت‌های بدهی[۳۷] هستند که امکان می‌دهند عملیات و معاملات انجام شود و حساب‌های بانکی بلافاصله از طریق ارتباطات پیوسته ایجاد شده بین ماشین‌های تحویلدار خود کار و پایانه‌های انتقال وجوه الکترونیکی در محل فروش و بانک‌ها ثبت شود. بالاخره کارت‌های اعتباری[۳۸] که برای خریداری کالا یا استفاده از خدمات مورد استفاده قرار می‌گیرند که پرداخت قیمت آنها موکول به زمان آینده می‌شود.[۳۹] معمولاً سوءاستفاده مالی از کارت‌های مزبور با جعل آنها همراه است. جعل کارت‌های مورد بحث اگر منجر به تحصیل مال نشود، قطعاً توأم با تحصیل خدمات و منافع مالی خواهد بود و چون عملکرد آنها تابع امکانات اینترنت نیست غالباً با توسل به مقررات کیفری سنتی نیز قابل کیفر هستند. البته همچنان که پیش از این گفته شد کارت‌های اعتباری و بدهی می‌توانند موضوع کلاهبرداری مؤسسات مالی که در زمره کلاهبرداری‌های نه گانه اینترنتی است نیز واقع شوند.

نکته‌ای که قابل ذکر است این است که عنوان کلاهبرداری با شرایط ویژه‌اش منصرف به حقوق کیفری ایران است و به طور دقیق منطبق بر واژه Fraud نیست؛ چه، معنای اصلی و اولیه این اصطلاح، تقلب است که در برخی از مصادیق فوق‌الذکر صرف قلب حقیقت یا کتمان آگاهانه موضوع از نظر قانونگذار برای تحقق جرم کفایت می‌کند. در تقلب (Fraud) برخلاف کلاهبرداری نه تنها در همه مصادیق، فریب قربانی شرط نیست، بلکه صرف بردن مال یا وسیله تحصیل مال نیز در آن

---

35 online

36 stored Value cards

37 Debit cards

38 Credit cards

۳۹ راسل اسمیت، «کلاهبرداری از طریق کارت‌های پلاستیکی»، ترجمه ناهید جعفرپور، ***خبرنامه انفورماتیک***، ش ۶۸، ص ۸۴.

مطرح نبوده و محدودهٔ آن وسیعتر است. غیر از اینکه کلاهبرداری جرم مرکب است و از دو فعل فیزیکی توسل به وسایل متقلبانه و تحصیل و بردن مال دیگری تشکیل یافته است ولیکن چون مرکب بودن جرم، محدودهٔ آن را تنگ‌تر می‌کند نمی‌توان گفت تقلب در حقوق کشورهای غربی با توجه به انبوه مصادیق آن، جرم مرکب است. برخی از کشورها همانند هند اصولاً Fraud را ناظر به تقلب مدنی و Cheating را در مفهوم تقلب کیفری می‌دانند.

## بند چهارم: کلاهبرداری رایانه‌ای و عناوین مشابه

کلاهبرداری رایانه‌ای همانند کلاهبرداری سنتی جرمی مقید به حصول نتیجه مجرمانه است و باید بواسطه سوءاستفاده از رایانه از طریق افعالی نظیر ایجاد، محو، توقف داده و یا اختلال در سیستم رایانه‌ای، مال یا منفعت یا مزایای مالی عاید مرتکب شود و همچنان که توسل به وسایل متقلبانه و بردن مال با رضایت قربانی وجه تمایز کلاهبرداری از سایر جرائم علیه اموال در حقوق کیفری سنتی است، در حقوق کیفری رایانه‌ای نیز سوءاستفاده از نرم افزارهای رایانه‌ای برای تحصیل مال یا منفعت یا مزایای مالی وجه تمایز بین کلاهبرداری رایانه‌ای از سایر جرائم یا عناوین مشابه است. برخی از این عناوین مشابه به طور واقعی عنوان مجرمانه ندارند و حتی در ادبیات حقوقی نیز ناشناخته هستند؛ اما به لحاظ اینکه این عناوین بعضاً در میان متخصصین امور رایانه‌ای رد پایی گذاشته است، ناگزیر از معرفی برخی از موارد مهم آن هستیم:

**۱- کلاهبرداری رایانه‌ای و سرقت رایانه‌ای:**[40] کلاهبرداری در مفهوم عام خود شامل سرقت رایانه‌ای نیز می‌شود اما از آنجا که سرقت رایانه‌ای ناظر به سرقت داده‌ها و فایل‌هاست، علاوه بر اینکه یک جرم رایانه‌ای محض محسوب می‌شود، موضوع آن نیز صرفاً مال نیست و از همین مجرا بین کلاهبرداری رایانه‌ای که منتج به تحصیل مال یا منافع مالی است و سرقت رایانه‌ای که منجر به ربودن داده‌ها و فایل‌های رایانه‌ای می‌شود، تفاوت حاصل می‌شود. در واقع رایانه در کلاهبرداری رایانه‌ای وسیله ارتکاب جرم است و در سرقت رایانه‌ای موضوع ارتکاب جرم.

40 cyber theft-piracy

**۲- کلاهبرداری رایانه‌ای و جاسوسی رایانه‌ای:**[۴۱] جاسوسی رایانه‌ای دستیابی غیرمجاز به اطلاعات طبقه‌بندی شده سری و محرمانه و همچنین اسرار صنعتی و تجاری است. جاسوسی رایانه‌ای صرفاً یک جرم علیه امنیت تلقی نمی‌شود بلکه محدوده آن گسترده‌تر بوده و شامل دسترسی غیرمجاز به اسرار تجاری یا اطلاعات مالی یک شرکت نیز می‌شود و از این مجرا می‌تواند مقدمه وقوع کلاهبرداری رایانه‌ای باشد، اما چون در جاسوسی رایانه‌ای مال یا منفعت مالی تحصیل نمی‌شود در زمره جرائم علیه اموال به شمار نمی‌رود. غالباً جاسوسی رایانه‌ای نسبت به جرم نفوذ غیرمجاز (هک) مؤخر و نسبت به کلاهبرداری رایانه‌ای مقدم است.

**۳- کلاهبرداری رایانه‌ای و حملات مهندسی اجتماعی:**[۴۲] حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه.[۴۳] مهندسی اجتماعی نوعی نفوذ غیرمجاز یا هک شفاهی به شمار می‌رود که در آن مرتکب با تماس تلفنی یا ارتباط از طریق پست اینترنتی یا گپ‌زنی و با معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبر سعی در تخلیه اطلاعاتی مخاطب خود پیرامون سیستم رایانه‌ای مربوطه می‌کند. در مهندسی اجتماعی، مرتکب قبل از اینکه به دانش فنی مربوط به نفوذ به سیستم رایانه‌ای متکی باشد، متکی به میزان نفوذ کلامی یا رفتاری خویش است و این شیوه به نحو خطرناکی رو به افزایش است. مهندسی اجتماعی هر چند مقدمه کلاهبرداری رایانه‌ای است ولی از مقدمات بعیده به شمار می‌رود و می‌توان آن را معادل توسل به وسایل متقلبانه در کلاهبرداری سنتی دانست. البته قابل ذکر است که طراح حمله مهندسی اجتماعی همواره به دنبال به دست آوردن اطلاعات مالی نیست و محتمل است که به دنبال اطلاعات امنیتی شرکت یا سیستم یا اصولاً نوعی اطلاع یابی بی‌هدف باشد.

**۴- کلاهبرداری رایانه‌ای و کسب اطلاعات مالی:**[۴۴] کسب اطلاعات مالی نوعی

---

41 cyber spionage - Netspionage

42 Social Engineering

۴۳ ***فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت***، هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، ترجمه فرهاد قلی‌زاده نوری، چاپ اول، ۱۳۸۱، ص ۶۸۸.

44 Phishing

مهندسی اجتماعی به شمار می‌رود اما این مانع از آن نیست تا شخصی از طریق نفوذ به سیستم رایانه‌ای (هک) اطلاعات مالی را کسب نماید که البته تفاوت کسب اطلاعات مالی با جاسوسی رایانه‌ای در این است که کسب اطلاعات مالی غالباً با نفوذ شفاهی به سیستم است و جاسوسی رایانه‌ای با نفوذ فنی. غیر از این کسب اطلاعات مالی همواره برای ارتکاب جرم نیست و می‌تواند در راستای رقابت تجاری بین دو شرکت صورت بگیرد. حمله مهندسی اجتماعی و کسب اطلاعات مالی غیر از اینکه دو اصطلاح فنی هستند تا حقوقی، چون با سایر عناوین مجرمانه پوشش داده می‌شوند، تحت عنوان مجرمانه مجزایی در قوانین کیفری انعکاس نیافته‌اند.

**۵- کلاهبرداری رایانه‌ای و ارسال نامه‌های الکترونیکی نامربوط:**[۴۵] نامه‌های الکترونیکی ناخواسته یا اسپم‌ها علی‌رغم اینکه به ظاهر کم اهمیت جلوه می‌کنند اما چون از یک سو دارای محتوای نامربوط بوده و به تعداد زیادی از کاربران ارسال می‌شود و از سوی دیگر سیل این پیام‌ها موجبات عصبانیت کاربران زیادی را فراهم می‌سازد، امنیت اطلاع رسانی رایانه و اینترنت و به ویژه حریم خصوصی افراد را تهدید می‌کند و به همین دلیل کشورهای اروپایی در قبال جرم‌انگاری آن اقدامات جدی به عمل آورده‌اند. هر چند اکثر کاربران نسبت به نامه‌های الکترونیکی ناخواسته بی‌اعتنا هستند اما چون قالب این نامه‌ها عمدتاً درخواست کمک اضطراری یا وعده مسابقه یا جایزه کاذب است می‌تواند موجبات تحقق کلاهبرداری رایانه‌ای را فراهم سازد و اصولاً یکی از طرق صید قربانیان ناشناخته برای کلاهبردار در فضای سایبر، ارسال نامه‌های نامربوط است. برخی مواقع هم ممکن است شخصی کاربران را جهت ارسال پیام‌های نامربوط به سایت‌های وب فریب دهد تا صدها نسخه پنهان از کلمات کلیدی متداول را به سایت‌ها بارگذاری کنند، حتی اگر آن کلمات ربطی به سایت وب نداشته باشند.[۴۶]

**۶- کلاهبرداری رایانه‌ای و دسترسی غیرمجاز به سیستم رایانه‌ای:**[۴۷] نفوذ غیرمجاز مقدمه اکثر جرائم رایانه‌ای محسوب می‌شود و نسبت به کلاهبرداری

---

45 Spamming

۴۶ ***فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت***، ص ۶۹۴.

47 Illegal Access

رایانه‌ای در برخی مواقع در مقام توسل به اقدامات مقدماتی برای تحصیل مال یا منافع دیگری ظاهر می‌شود. نفوذکنندگان به سیستم رایانه‌ای عمدتاً بر پنج قسم هستند: الف - هکرها:[۴۸] کاوشگرانی هستند که از روی کنجکاوی یا مقتضیات فعالیت‌های رایانه‌ای خویش به سیستم نفوذ می‌کنند. هک ماهیتاً نوعی دانش فنی است و جرم به شمار نمی‌رود. ب- کراکرها:[۴۹] نفوذگران بدخواه هستند که از روی سوءنیت به سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایل‌ها را پاک کنند یا مرتکب سایر جرائم رایانه‌ای شوند.[۵۰] ج- فریک‌ها:[۵۱] نفوذگران به خطوط تلفن در فضای سایبر را گویند. این دسته از نفوذگران از طریق سیستم رایانه‌ای به سیستم ارتباطی و مخابراتی دست می‌یابند و آن را مورد استفاده قرار می‌دهند. از کراکرها به کلاه سیاه‌ها نیز یاد می‌شود.

د- نفوذگران غیر حرفه‌ای:[۵۲] این قسم از نفوذگران به دو صورت به سیستم رایانه‌ای نفوذ پیدا می‌کنند؛ یا وارد قسمت‌هایی از سیستم می‌شود که نیازی به دانش فنی قابل توجه ندارد و به پردازه‌های ساده و آسان اتکا می‌کند یا اینکه در مقام لاشه‌خوار پس از نفوذ یک هکر حرفه‌ای به دنبال وی وارد سیستم می‌شود و اهداف و اغراض خود را محقق می‌سازد.

## بخش دوم: مبارزه با کلاهبرداری رایانه‌ای

کنترل و مهار کلاهبرداری رایانه‌ای در وهله نخست از طریق جرم‌انگاری آن میسر خواهد بود؛ زیرا کلاهبرداران رایانه‌ای همچنان که طرق سوءاستفاده مالی از رایانه و فریفتن دیگران را به ظریف‌ترین حالت می‌دانند، نقاط کور قوانین کیفری را نیز می‌خوانند و به این ترتیب طریقی را پیش می‌گیرند که حتی‌الامکان در صورت گرفتار شدن بتوانند به انحای مختلف از ابهامات قانون موجود استفاده کرده و از دام عدالت

---

48 Hackers

49 Crackers

۵۰ جنیا دی آنجلیز؛ ***جرائم سایبر***، ترجمه سعید حافظی و عبدالصمد خرم آبادی، دبیرخانه شورای عالی اطلاع رسانی، چاپ اول، ۱۳۸۳، ص ۱۳.

51 Phreaks

52 Script Kiddie

بگریزند. به همین دلیل اکثر قانونگذاران این شکاف عمیق قوانین موجود در قبال کلاهبرداری رایانه‌ای را دیده و مبادرت به جرم‌انگاری جدید کرده‌اند. فارغ از سیاست واکنشی علیه این جرم که مبتنی بر جرم‌انگاری و به تبع آن کیفرانگاری است، سیاست کنشی یا اقدامات پیشگیرانه نیز در راستای مبارزه با کلاهبرداری رایانه‌ای مؤثر خواهد بود، چه فقط با تکیه بر حربه کیفر نمی‌توان از جانب لشکری از مرتکبان یقه سفید زیرک و دوراندیش مطمئن شد و بلکه با تکیه بر کیفر، فضای سایبر را برای ماجراجویی‌های این عده تنگ و کاربران را برای مقابله با آنها آموزش داد. از این رو در این بخش ابتدا به برخورد کیفری اسناد بین‌المللی و قوانین کشورهای پیشرفته در برابر کلاهبرداری رایانه‌ای و سپس به عملکرد قانونگذار کشورمان در قبال این جرم اشاره می‌کنیم و در نهایت به نحوه پیشگیری از کلاهبرداری رایانه‌ای اشاره خواهیم کرد.

## بند نخست: کلاهبرداری رایانه‌ای در اسناد بین‌المللی و قوانین کشورهای پیشرفته

اسناد بین‌المللی در قبال کلاهبرداری رایانه‌ای بیشتر معطوف به تعریف یا دسته‌بندی این جرم بوده است و علی‌رغم خطرناکی و شیوع آن کمتر سعی شده است تا پیرامون آن مقررهٔ مجزایی وضع شود. علت این امر این است که کلاهبرداری رایانه‌ای اولاً به نحو مقتضی در قوانین داخلی کشورها پیش‌بینی شده است یا حداقل با همان مقررات سنتی مربوط به کلاهبرداری می‌توان با آن برخورد کرد و ثانیاً دیدگاه غالب نیز بر این بود که به طور واقع کلاهبرداری رایانه‌ای جرم جدیدی نیست که احتیاج به مقرره جدیدی داشته و بلکه در نهایت سیستم رایانه‌ای برای تحقق کلاهبرداری در مقام وسیله ارتکاب ظاهر می‌شود. اما کنوانسیون جرائم محیط سایبر که در بیست و سوم سپتامبر ۲۰۰۱ در بوداپست به تصویب شورای اروپا رسید، در کنار معدود جرائم رایانه‌ای که پیش‌بینی کرده، کلاهبرداری رایانه‌ای و جرائم مرتبط با آن نیز پرداخته است و این خود بیانگر این است که در ابتدای هزاره سوم باید یک عزم بین‌المللی در مبارزه با کلاهبرداری رایانه‌ای صورت پذیرد. به موجب ماده ۸ کنوانسیون بوداپست هر یک از کشورها باید در حقوق داخلی خود اقدام به قانونگذاری در این زمینه کنند که هر گونه اقدامات عمدی بدون مجوز با قصد تقلب

یا دیگر مقاصد ناروا در راستای اضرار به دیگری یا جلب منافع اقتصادی برای خود یا دیگری قابل کیفر گردد. این اقدامات عبارتند از:

الف – هر گونه وارد کردن، تغییر، حذف یا متوقف نمودن داده‌های رایانه‌ای

ب – هر گونه ایجاد اختلال در عملکرد یک سیستم رایانه‌ای[۵۳]

نحوه نگارش ماده ۸ کنوانسیون به گونه‌ای است که سیستم رایانه‌ای را صرفاً وسیله تحصیل منافع اقتصادی می‌داند و گویا از این موضوع غافل مانده است که اگر افعال فیزیکی وارد کردن یا تغییر یا حذف داده یا اختلال در سیستم منجر به تحصیل داده‌ها یا نرم افزارهای رایانه‌ای یا استفاده از عملکرد رایانه یا نرم افزارهای خاصی شود آیا باز هم کلاهبرداری شکل می‌گیرد یا خیر؟ کما اینکه در کنوانسیون به جز اختلال در سیستم یا تخریب داده که اگر به توان آنها را جرائم علیه اموال دانست (همان طور که در تقسیم‌بندی‌های جدید آنها را در زمره جرائم علیه تمامیت داده یا سیستم می‌دانند تا جرائم علیه اموال)[۵۴] به جرائم مالی دیگر مثل سرقت رایانه‌ای و غیره اشاره نشده است. البته شاید از اصطلاح کش‌دار و قابل تفسیر «منافع اقتصادی»

---

53 convention on cybercrime: Article 8: computer Related Fraud Each party shall adopt such legislative and other ceasures 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 by:

a: any onput, 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 one self or for another.

۵۴ در جایی که رایانه موضوع یا هدف ارتکاب جرم است، مشهورترین طبقه‌بندی که از جرم رایانه‌ای که هم اکنون ارایه می‌دهند، به این صورت است: الف– جرائم علیه محرمانه بودن داده‌ها و اطلاعات (confidentiality) نفوذ غیرمجاز به سیستم، شنود غیرمجاز، افشای غیرمجاز و جاسوسی رایانه‌ای در زمره این دسته از جرائم قرار می‌گیرند. ب – جرائم علیه صحت و تمامیت داده‌ها و اطلاعات (Integrity) تخریب داده‌ها، اختلال در سیستم رایانه‌ای و جعل رایانه‌ای در این دسته جای می‌گرند. ج – جرائم علیه قابلیت دسترسی و موجودیت داده‌ها و اطلاعات (Avialability) ممانعت از دستیابی یا ارسال سرویس‌های کاذب یا برخی ویروس‌ها که قابلیت دسترسی را مختل می‌سازند در این دسته قرار می‌گیرند. (سخنرانی پرفسور اولیرش زیبر در هفدهمین کنگره بین‌المللی حقوق جزا در چین، سپتامبر ۲۰۰۴ (شهریور ۱۳۸۳) کلاهبرداری ماهیتاً در هیچ یک از سه دسته فوق قرار نمی‌گیرد هر چند جرائم ذیل هر سه دسته می‌توانند مقدمه کلاهبرداری واقع شود. اما در جایی که مرتکب با اقدامات متقلبانه در صدد تحصیل داده‌ها یا اطلاعات رایانه‌ای دارای ارزش مالی باشد، در این جا کلاهبرداری در ذیل جرائم علیه محرمانه بودن داده‌ها و اطلاعات قرار می‌گیرد.

بتوان استفاده کرد و گفت که اگر داده دارای ارزش مالی بوده و منفعت اقتصادی داشته باشد، می‌تواند موضوع کلاهبرداری رایانه‌ای واقع شود؛ آن وقت می‌توان گفت که کنوانسیون بوداپست دو قسم از کلاهبرداری رایانه‌ای پیش‌بینی کرده است: کلاهبرداری‌ای که رایانه در آن وسیله ارتکاب جرم است و کلاهبرداری‌ای که در آن رایانه هم وسیله ارتکاب جرم است و هم موضوع ارتکاب جرم. در حال حاضر کنوانسیون محیط سایبر بوداپست تنها سند بین‌المللی است که به مقررات ماهوی و شکلی جرائم رایانه‌ای اشاره کرده است و به لحاظ جامع بودن و پیشرفتگی‌اش در حال حاضر الگوی مناسبی برای کشورها در زمینه قانونگذاری فضای سایبر به شمار می‌رود. از این سند بین‌المللی که بگذریم، اسناد یا اقدامات بین‌المللی دیگر که در زمینه جرائم رایانه‌ای صورت گرفته است مانند اقدامات سازمان توسعه و همکاری اقتصادی (که اولین بار به طور جدی در سطح بین‌المللی به جرائم رایانه‌ای پرداخت و دست به تقسیم‌بندی آنها زد و از سال ۱۹۸۳ تا ۱۹۸۵ یک کمیته تخصصی را برای مطالعه و بررسی راه‌های ممکن جهت هماهنگی بین‌المللی قوانین کیفری برای مبارزه با جرائم اقتصادی مرتبط با رایانه مشغول نمود.)، اقدامات شورای اروپا (که در سال ۱۹۸۵ کمیته منتخب کارشناسان جرائم رایانه‌ای را ایجاد کرد و همچنین فهرست قابل توجهی از حداقل جرائم رایانه‌ای به همراه تعریف آنها تدارک دید)، اقدامات انجمن بین‌المللی حقوق جزا (که در سال ۱۹۹۴ در ریودوژانیرو توصیه نامه‌ای برای پیشگیری و کنترل جرائم انفورماتیک تدارک دید و معمولاً از این زمان به بعد در کنگره‌های پنجسالانه خود میزگرد و یا کنفرانسی را به جرائم رایانه‌ای اختصاص می‌دهد که آخرین بار در کنگره هفدهم در چین در سپتامبر ۲۰۰۴ کنفرانسی با حضور اساتید برجسته دنیا در مورد جرائم رایانه‌ای صورت گرفت) و اقدامات سازمان ملل متحد (که در کنگره نهم در کنار توجه به جرائم سازمان یافته فراملی به جرائم رایانه‌ای نیز پرداخت و همچنین در کنگره دهم به اشکال جدید جرائم رایانه‌ای اشاره کرد.) همگی در راستای تعریف، طبقه‌بندی، پیشگیری و همکاری‌های بین‌المللی در مبارزه با جرائم رایانه‌ای بوده‌اند و کمتر به وضع مقرره در ارتباط با مجموع جرائم رایانه‌ای و به ویژه کلاهبرداری رایانه‌ای اقدام نمودند.

البته در مورد جرائم سطح اول رایانه‌ای که رایانه در آنها صرفاً وسیله ارتکاب جرم بود، قوانین کشورها زودتر از اسناد و اقدامات بین‌المللی دست به کار شدند. در

اواخر دهه هفتاد در قوانین بعضی کشورهای پیشرفته همچون کانادا یا برخی از ایالات امریکا مقررات جزائی خاص در ارتباط با وسیله قرار دادن رایانه برای ارتکاب جرم پیش‌بینی شد. مجموعاً در ارتباط با کلاهبرداری رایانه‌ای از جانب کشورهای دنیا سه رویکرد در امر قانونگذاری اتخاذ شده است: الف) برخی از کشورها صراحتاً مقررات جزائی جداگانه‌ای در ارتباط با کلاهبرداری رایانه‌ای وضع کرده‌اند که عملاً در این کشورها دو نوع کلاهبرداری وجود دارد: کلاهبرداری سنتی و کلاهبرداری رایانه‌ای. مثل مواد ۹۳ و ۱۱۵ قانون جرائم اقتصادی مرتبط با رایانه مصوب ۱۹۸۵ یا ماده ۳۶۳ قانون جزای آلمان اصلاحی ۱۹۸۶ و یا ماده ۲۷۹ قانون جزای دانمارک مصوب ۱۹۸۵ که در این کشورها تحصیل مال یا منفعت از طریق روش‌ها غیرقانونی داده‌پردازی یا محو یا تغییر یا ایجاد داده در سیستم رایانه‌ای به عنوان کلاهبرداری رایانه‌ای شناخته شده است. ب) برخی از کشورها هر چند مقرره جدیدی برای کلاهبرداری رایانه‌ای وضع نکرده‌اند اما با وضع یک مقرره کلی بیان کرده‌اند که چنانچه جرمی از طریق رایانه ارتکاب یابد بر اساس مقررات کیفری فعلی (سنتی) قابل مجازات است مثل قانون جزای هند. البته در حقوق جزای کشورمان نسبت به جرائمی که نظامیان از طریق سیستم رایانه‌ای مرتکب می‌شوند، همین سیاست اتخاذ شده است. وفق ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ هر گونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت می‌گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند. افشای غیرمجاز اطلاعات، سرقت اشیای دارای ارزش اطلاعاتی مانند سی دی یا دیسکت‌های حاوی اطلاعات یا معدوم کردن آنها یا سوءاستفاده‌های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند. البته هر چند این ماده به سوءاستفاده‌های مالی از رایانه اشاره کرده است اما اولاً فقط مختص نظامیان است و ثانیاً مجازات آن را به موجب مقررات قبلی قانون مجازات نیروهای مسلح تعیین کرده است و حال آنکه این قانون اصولاً به کلاهبرداری اشاره نمی‌کند و بنابراین اصطلاح سوءاستفاده‌های مالی از طریق رایانه منصرف از کلاهبرداری رایانه‌ای

است.

ج) برخی کشورها نیز اصولاً نسبت به جرم کلاهبرداری رایانه‌ای سکوت اختیار کرده‌اند و جرائم مرتبط با آن را با مقررات کیفری موجود پاسخ می‌دهند. این دسته از کشورها عمدتاً کشورهای در حال توسعه هستند که رایانه و اینترنت هنوز به طور کامل در آنها رشد نیافته است. در کشور ما نیز فارغ از ماده ۶۷ قانون تجارت الکترونیکی که به طور خاص به کلاهبرداری رایانه‌ای اشاره کرده است، همین حالت حاکم است و نه تنها کلاهبرداری بلکه سایر جرائم رایانه‌ای نیز با استفاده از مقررات کیفری موجود مجازات می‌شوند.

مقررات کیفری کشورهایی که به طور جداگانه در مورد کلاهبرداری رایانه‌ای اقدام به وضع قانون کرده‌اند، عمدتاً شبیه هم هستند اما می‌توان از دو جهت بین این مقررات تفاوت‌هایی را یافت: نخست از جهت موضوع جرم و دوم از جهت شرط توسل به وسایل متقلبانه. موضوع جرم کلاهبرداری در موسع‌ترین حالت، مال، وسایل تحصیل مال، منافع و خدمات مالی است. در ماده ۱۰۳۰ قانون کیفری فدرال امریکا موضوع جرائم مرتبط با کلاهبرداری تا حد کسب اطلاعات امنیتی یا ایراد ضربه به جسم و روح افراد فراتر رفته است. در کشورهایی مثل فرانسه و سوئد خدمات مالی موضوع جرم کلاهبرداری رایانه‌ای قرار نگرفته است. در ماده ۷-۱-۳۴۲ قانون کیفری کانادا مصوب ۱۹۸۵ و همچنین قانون جرائم رایانه‌ای ایالت ویرجینیای امریکا مصوب ۱۹۸۴ علاوه مال و وجوه، منافع و خدمات نیز به عنوان موضوع کلاهبرداری رایانه‌ای پیش‌بینی شده‌اند. ماده ۱۱۵ قانون جرائم اقتصادی مرتبط با رایانه غیر از مال یا منافع مالی، ایراد خسارت به دیگران از طریق رایانه را نیز در ردیف جرائم مرتبط با کلاهبرداری رایانه‌ای ذکر می‌کند. همچنان که شبیه همین مقرره در ماده ۱۴۷ قانون کیفری اتریش نیز آمده است.

در مورد شرط توسل به وسایل متقلبانه در قوانین برخی کشورها مثل بند الف ماده ۲۷۹ مقررات کیفری دانمارک مصوب ۱۹۸۵ یا بند الف ماده ۳۶۳ مجموعه قوانین کیفری اصلاحی ۱۹۸۶ آلمان فدرال و ماده ۱۴۷ قانون کیفری اتریش اثری از آن دیده نمی‌شود و در مقابل قوانین کیفری فنلاند، فرانسه و سوئد شرط گمراه شدن ماشین یا انسان یا استفاده متقلبانه را برای تحقق کلاهبرداری رایانه‌ای لازم دانسته‌اند. در ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ شرط فریب انسان یا

گمراه شدن رایانه یا ماشین‌های رایانه‌ای برای تحقق جرم پیش‌بینی شده است. نتیجتاً گرایش قانونگذاری‌های جدید بر این است که از یک سو شرایط و اجزای رکن مادی کلاهبرداری رایانه‌ای را در مقایسه با کلاهبرداری سنتی کاهش دهند همچنان که در قوانین بسیاری از کشورها شرط فریب انسان یا توسل به مانورهای متقلبانه یا هر دو در کلیه مصادیق کلاهبرداری رایانه ضروری شناخته نشده است. از سوی دیگر دایره جرم‌انگاری کلاهبرداری رایانه‌ای و جرائم مرتبط با آن را به واسطه سهولت ارتکاب و میزان شیوع آن افزایش دهند، همچنان که ماده ۳۰۷-۴ قانون کیفری فرانسه مصوب ۱۹۸۶ تحریک به تحصیل مال یا منافع مالی به وسیله استفاده متقلبانه از یک سیستم داده‌پردازی را نیز در زمره جرائم مرتبط با کلاهبرداری رایانه‌ای ذکر کرده است.

## بند دوم: کلاهبرداری رایانه‌ای در حقوق کیفری ایران

کلاهبرداری یکی از جرائم بحث‌انگیز حقوق کیفری کشورمان است که ارکان و شرایط تشکیل دهندهٔ آن به موجب ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۴/۶/۲۸ مجلس شورای اسلامی و تأیید ۱۳۶۷/۹/۱۵ مجمع تشخیص مصلحت نظام پیش‌بینی شده که این ماده خود با اندکی تغییر به ویژه در میزان مجازات، رونویسی شده از ماده ۲۳۸ قانون مجازات عمومی مصوب ۱۳۰۴ و اصلاحی ۱۳۵۲ است. به موجب ماده یک این قانون هر کس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیش‌آمدهای 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 حواله‌ها 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. در صورتی که شخص مرتکب برخلاف واقع عنوان یا سمت مأموریت از طرف سازمان‌ها و مؤسسات دولتی یا وابسته به دولت یا شرکت‌های دولتی یا شوراها یا شهرداری‌ها یا نهادهای انقلابی و به طور کلی قوای سه گانه و همچنین

نیروهای مسلح و نهادها و مؤسسات مأمور به خدمت عمومی اتخاذ کرده یا اینکه جرم با استفاده از تبلیغ عامه از طریق وسایل ارتباط جمعی از قبیل رادیو، تلویزیون، روزنامه و مجله یا نطق در مجامع و یا انتشار آگهی چاپی یا خطی صورت گرفته باشد یا مرتکب از کارکنان دولت یا مؤسسات و سازمان‌های دولتی یا وابسته به دولت یا شهرداری‌ها یا نهادهای انقلابی و یا به طور کلی از قوای سه گانه و همچنین نیروهای مسلح و مأمورین به خدمت عمومی باشد، علاوه بر رد اصل مال به صاحبش به حبس از ۲ تا ده سال و انفصال ابد از خدمات دولتی و پرداخت جزای نقدی معادل مالی که اخذ کرده است، محکوم می‌شود.

با توجه به توضیحاتی که از کلاهبرداری رایانه‌ای ارائه شد و با التفات به ماده یک قانون فوق‌الذکر دو نکته اساسی قابل ذکر است: نخست اینکه کلاهبرداری موضوع ماده یک قانون تشدید (کلاهبرداری سنتی) نسبت به کلاهبرداری رایانه‌ای از اجزاء و عناصر بیشتری برخوردار است و نتیجتاً محدودهٔ آن تنگ‌تر است چون کثرت اجزاء و عناصر جرم را به همراه دارد. کلاهبرداری موضوع ماده یک باید دارای اجزای زیر باشد: الف) حداقل از دو فعل فیزیکی شکل بگیرد. کلاهبرداری یک جرم مرکب است که در جایی که موضوع جرم مستقیماً وجه یا مال است، متضمن تحقق دو فعل فیزیکی توسل به وسایل و مانورهای متقلبانه و بردن مال است و در جایی که موضوع جرم وسیله تحصیل مال مانند چک یا قبض باشد، مستلزم تحقق سه فعل فیزیکی توسل به وسایل و مانورهای متقلبانه، تحصیل وسیله تحصیل مال و بردن مال است. ب) صاحب مال یا شخصی که رابطه قانونی معتبر با مال دارد (مانند امین) در اثر عملیات متقلبانه کلاهبردار فریب خورد. البته فریب در همه مصادیق به صورت ملموس و عینی وجود ندارد اما مجموعاً عملیات متقلبانه کلاهبردار قابلیت فریب را دارا می‌باشد بنابراین با وجود آگاهی صاحب مال اگر کلاهبردار با جعل اسناد در اثر حکم دادگاه مال وی را به چنگ آورد گویی که دادگاه را فریفته و به عنوان وسیله‌ای در نیل به اهداف خود به کار برده است. ج) بین توسل به وسایل متقلبانه و بردن مال رابطه علیت مستقیم باشد. پس اگر شخص دیگری را با مانورهای متقلبانه راضی به فروش ملکش به قیمت نازل نماید، کلاهبردار نیست، زیرا مانورهای متقلبانه برای وقوع معامله بوده است نه برای بردن مال و در واقع معامله مادامی که صحیح باشد این رابطه علیت را قطع کرده است. د) موضوع جرم

باید وجوه، اموال، اسناد یا حواله‌ها یا قبوض یا مفاصا حساب و امثال آنها باشد و چون در انتهای ماده به بردن مال دیگری به عنوان فعل فیزیکی و به تبع آن نتیجه مجرمانه اشاره شده است باید گفت اسناد یا حواله‌ها یا قبوض یا مفاصا حساب و موارد تمثیلی آن باید وسیله تحصیل مال باشند والا به خودی خود موضوع کلاهبرداری واقع نمی‌شوند. علاوه بر این منافع، مزایا و خدمات مالی نیز نمی‌توانند موضوع کلاهبرداری قرار بگیرند. ه) افعال فیزیکی کلاهبرداری باید منتج به نتیجه مجرمانه شوند. نتیجه جرم، برده شدن مال است نه بردن مال؛ چون بردن مال خود فعل فیزیکی است ولیکن نتیجه مجرمانه جزئی است که به تبع تحقق فعل فیزیکی حاصل می‌شود. پس اگر افعال فیزیکی کلاهبرداری تحقق یابند اما نتیجه مجرمانه حاصل نشود، جرم تمام نشده و مرتکب حسب مورد به مجازات شروع به کلاهبرداری محکوم خواهد شد. شاید به خاطر اجزای متعدد فوق‌الذکر که دایره تحقق کلاهبرداری را مضیق می‌کند، قانونگذار ناچار شده است بقیه مصادیق شبیه کلاهبرداری را یا در قوانین خاص یا به موجب ماده ۲ قانون تشدید که به طور افسار گسیخته تحصیل نامشروع مال را جرم‌انگاری کرده است، کیفر دهد.

نکته دوم اینکه در قسمت دوم ماده یک به موارد تشدید مجازات کلاهبرداری اشاره شده است که یک مورد آن ارتکاب جرم با استفاده از تبلیغ عامه از طریق وسایل ارتباط جمعی از قبیل رادیو، تلویزیون، روزنامه می‌باشد. حال با توجه به اینکه وسایل ارتباط جمعی به صورت تمثیلی به کار رفته است، اینترنت نیز می‌تواند در عرض آنها ذکر شود. نظر به اینکه برخلاف وسایل دیگر، اینترنت مالک مشخصی ندارد[۵۵] و اصولاً یک فضا یا دنیای جدید است تا یک وسیله جدید و از طرفی نیز صرفاً وسیله ارتباط جمعی محسوب نمی‌شود و قابلیت‌های بی‌شماری دارد، شاید بتوان گفت مصادیق تمثیلی ذکر شده در ماده منصرف از فضای سایبر یا اینترنت است اما حتی اگر هم بپذیریم که توسل به اینترنت برای ارتکاب کلاهبرداری،

---

[۵۵] فضای سایبر همانند فضای واقعی مالک نیست و اصولاً قابلیت تملک ندارد و همگان شریک در استفاده از این فضا هستند. اما عدم وجود مالک به معنای عدم نظارت بر فضای اینترنت نیست و به همین دلیل برای جلوگیری از هرج و مرج در فضای بدون مالک، در سال ۱۹۹۲ یک گروه غیر انتفاعی با عنوان «جامعه اینترنت» تشکیل یافته است که شکل‌گیری قوانین اینترنت و پروتکل‌هایی که نحوه استفاده و ارتباط با اینترنت را تعیین می‌کنند، مورد بازبینی قرار می‌دهد. (***مجله اینترنت***، سال دوم، اردیبهشت و خرداد ۱۳۸۳، ش ۸، ص ۶.)

هم‌عرض توسل به وسایل ارتباط جمعی نظیر رادیو، تلویزیون و روزنامه است با توجه به محدودیت‌های فوق‌الذکر در فضای سایبر که وادی امکانات و محیط سرعت است به قدری موقعیت سوءاستفاده مالی از رایانه و اینترنت پیش می‌آید که نمی‌توان با انطباق با ماده یک قانون تشدید آنها را کیفر داد؛ مثلاً در سال ۱۳۸۲ دو پرونده بزرگ نفوذ به سیستم رایانه‌ای بانک ملی در ابتدای پائیز این سال و اعتراضات همگانی به سوءاستفاده‌های عاملین شرکت هنگ‌کنگی گلدکوئیست[۵۶] دارای کیفیاتی بودند که به هیچ وجه منطبق بر ماده یک قانون تشدید نبودند؛ هر چند بتوان با عنوان مجرمانه تحصیل مال از طریق نامشروع پرونده‌ها را بست اما مجازات اندک این جرم و اصولاً کوچک و کم اهمیت بودن عنوان مجرمانه که تحصیل مال از طریق نامشروع یدک می‌کشد و از حیث روانشناسی مرتکبان را گستاخ‌تر در سوءاستفاده‌های رایانه‌ای می‌کند، نمی‌تواند یک سیاست جنائی مناسب برای مبارزه با کلاهبرداری رایانه‌ای باشد. مهر ضعف و ناتوانی که با پرونده‌های فوق‌الذکر و پرونده‌های اینترنتی دیگر بر پیشانی مقررات کیفری موجود خورد با تصویب قانون تجارت الکترونیکی در زمستان ۱۳۸۲ تا حدی برطرف شد. به موجب ماده ۶۷ این قانون، هر کس در بستر مبادلات الکترونیکی با سوءاستفاده و یا استفاده غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر 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 مأخوذه محکوم می‌شود.

تبصره: شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر

[۵۶] در قضیه نفوذ به سیستم بانک ملی در اوایل پائیز ۱۳۸۲ مرتکب به دلیل ضعف امنیتی موجود در سیستم، وارد شبکه داخلی شرکت خدمات انفورماتیک که فعالیت‌های بانک‌های دولتی را پشتیبانی می‌کند می‌شود و از طریق پروتکل vpn (virtual private Network) رایانه خود را جزیی از زیر گروه آن پیکربندی کرده و با گذاشتن نرم‌افزارهای خاص توانسته بود به کلیه رایانه‌های موجود در شبکه راه یابد و به این وسیله به هر حسابی که دوست داشت به نفع خود یا دوستانش دخل و تصرف می‌کرد. با توجه به مقررات سنتی و شرایطی که پیش‌بینی کرده‌اند، این عمل مرتکب نه کلاهبرداری است و نه سرقت. سرمایه‌گذاری در طرح هرمی گلدکوئیست نیز با هیچ یک از مقررات کیفری منطبق نیست.

در این ماده می‌باشد.

این ماده تلفیقی از ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری و ماده ۸ کنوانسیون جرائم محیط سایبر بوداپست است. البته رویکرد ماده ۶۷ به کلاهبرداری رایانه‌ای بیشتر رویکرد سنتی است و رایانه را صرفاً در حد وسیله ارتکاب جرم یا وسیله تحصیل مال می‌داند و از این حیث ایراد عمده و اولیه وارد بر این ماده این است که هر چند در سراسر قانون تجارت الکترونیکی از داده پیام سخن به میان آمده است اما موضوع جرم صرفاً مال است و صحت از تحصیل داده به میان نیامده است. البته این ایراد در جایی که مال را شامل داده‌های دارای ارزش مالی بدانیم، کمتر وارد است. این ماده هر چند از عنوان «کلاهبرداری کامپیوتری» به معنای عام استفاده کرده است اما مشخص نیست که آیا منظور فقط کلاهبرداری در مبادلات الکترونیکی است کما اینکه عنوان قانون ناظر به این است و در صدر ماده نیز مکان ارتکاب جرم «بستر مبادلات الکترونیکی» معرفی شده است که البته چون قانون تجارت الکترونیکی یک قانون خاص مبادلات الکترونیکی به شمار می‌رود طبیعتاً جرائم پیش‌بینی شده نیز منصرف به همین محدوده است. غیر از این ماده ۶۷ با ابهامات و ایرادات زیر مواجه است:

الف) دقیقاً مشخص نیست که فعل مادی کلاهبرداری رایانه‌ای چیست. سوءاستفاده یا استفاده غیرمجاز از داده پیام‌ها یا ارتکاب افعالی نظیر ورود، محو، توقف داده پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره. بهترین تعبیر این است که بگوئیم رفتار فیزیکی کلاهبرداری سوءاستفاده یا استفاده غیرمجاز از داده پیام‌ها است ولیکن این رفتار می‌تواند در قالب افعال تمثیلی نظیر ورود، محو، توقف داده پیام و... متجلی شود. البته استفاده از دو تعبیر «سوءاستفاده» و «استفاده غیرمجاز» بدون توجه به معادل انگلیسی آنها در کنار هم جالب به نظر نمی‌رسد؛ زیرا هر استفاده غیرمجازی قطعاً سوءاستفاده نیز خواهد بود و ذکر این تعبیر بیهوده به نظر می‌رسد.

ب) این ماده بدون ملاحظه فضای سایبر که در آن کاربران برای همدیگر ناشناخته هستند باز از جزء «فریفتن دیگران» سود جسته است و حال آنکه به نظر می‌رسد این شرط در اینترنت لازم نباشد، چه از خصایص کلاهبرداری رایانه‌ای سوءاستفاده مالی از طریق رایانه و نرم‌افزارهای آن است و کمتر در این فضا بحث

فریب قربانی پیش می‌آید، کما اینکه ضرورتی نیز بر وجود چنین جزئی احساس نمی‌شود. البته ادامه ماده ۶۷ در راستای تکمیل صنف خود به سیستم رایانه‌ای نیز توجه نشان داده است و شرط گمراهی این سیستم را در کنار فریفتن دیگران ذکر می‌کند که البته ایراد جدیدی مطرح می‌شود و آن اینکه گمراهی صفت رفتار انسانی است و ماشین اصولاً به لحاظ فقدان شعور قابلیت گمراهی نیز ندارد. در هر حال وجود این دو شرط برای کلاهبرداری رایانه‌ای ضرورتی ندارد و نوعی تقلید از مقررات سنتی است.

ج) در قسمتی از ماده ۶۷ آمده است: «و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد.» این عبارت کاملاً متأثر از ماده یک قانون تشدید است و حال آنکه قانون تشدید نیز در عبارت «وجوه و یا اموال یا اسناد یا حواله‌ها یا قبوض یا مفاصاحساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد...» مواجه با ایراد است چون ابتدا وجوه و اموال را در ردیف سایر موضوعات گفته و اشاره به تحصیل آنها، و سپس بردنشان کرده است و حال آنکه تحصیل وجوه و اموال به معنای بردن آنهاست و ضرورتی ندارد که دوباره در مورد آنها از تعبیر «مال دیگری را ببرد» استفاده شود. این ایراد در ماده ۶۷ قانون تجارت الکترونیکی برجسته‌تر است؛ زیرا با حذف وسایل تحصیل مال که در ماده یک قانون تشدید آمده است عملاً به سه موضوع وجوه، اموال و امتیازات مالی اشاره کرده است که در هر سه تحصیل به معنای بردن است و ضرورتی نداشت عبارت «اموال دیگران را ببرد» آن هم به صورت جمع به کار برد و به نوعی ماده ۶۷ از ماده یک قانون تشدید ضعیف‌تر عمل کرده است. غیر از ایرادات فوق باز هم این ماده خالی از ایراد نیست. در باب سوءاستفاده از داده‌ها، ذکر برنامه‌ها، که خود نوعی داده هستند، ضروری نبود. همچنین حکم به رد مال به صاحبان اموال علاوه بر اینکه نوعی شبهه در رعایت قواعد آئین دادرسی مدنی را به همراه دارد، در موضوع نحوه رد امتیازات مالی استفاده شده ساکت است و بالاخره تبصره این ماده با تکرار ایراد تبصره ۲ ماده یک قانون تشدید برای شروع به جرم کلاهبرداری رایانه‌ای حداقل مجازات مقرر در ماده را پیش‌بینی کرده است و حال آنکه در شروع به جرم اصولاً نتیجه مجرمانه حاصل نمی‌شود تا درباره جزای نقدی با احتساب معادل مال مأخوذه حکم دهیم، مضافاً اینکه مشخص نیست حکم به حداقل جزای نقدی با

توجه به نسبی بودن آن (معادل مال) چگونه و به چه میزان است بنابراین قاضی محکمه در شروع به کلاهبرداری اصولاً نباید جزای نقدی را مورد حکم قرار دهد. البته یکی از محاسن ماده ۶۷ توجه به ماهیت فضای سایبر و سهولت ارتکاب جرم در آن و نتیجتاً کاهش مجازات حبس از یک تا هفت سال به یک تا سه سال است.

با توجه به ایرادات عدیده ماده ۶۷ و از همه مهمتر اینکه این ماده منصرف به کلاهبرداری در بستر مبادلات الکترونیکی است و شامل کلیه مصادیق کلاهبرداری رایانه‌ای نمی‌شود، در ماده ۸ لایحه مجازات جرائم رایانه‌ای حتی‌الامکان با رفع ایرادات مطرح شده و با بیانی ساده، کلاهبرداری رایانه‌ای به این صورت پیش‌بینی شده است: «هر کس از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، توقف داده‌ها یا اختلال در عملکرد سیستم، سوءاستفاده نماید و از این طریق وجه یا مال یا منفعت یا خدمات مالی و یا امتیازات مالی برای خود یا دیگری تحصیل کند کلاهبردار محسوب و به مجازات مقرر در قانون مربوط محکوم خواهد شد. تبصره: مجازات شروع به جرم مذکور در این ماده حداقل مجازات حبس مقرر خواهد بود». ایراد وارده بر این ماده ارجاع مجازات کلاهبرداری به ماده یک قانون تشدید و به تبع آن سنگینی مجازات است که البته این ایراد با توجه به خطرناکی کلاهبرداران اینترنتی و رایانه‌ای و همچنین سابقه وقوع کلاهبرداری‌های بسیار بزرگ تا حدی قابل توجیه است.

در حال حاضر که ماده ۶۷ قانون تجارت الکترونیکی تنها مقرره لازم‌الاجراء مربوط به کلاهبرداری رایانه‌ای است، لازم است تا به اختصار ارکان و اجزای تشکیل دهنده آن تبیین شود: فارغ از رکن قانونی که خود ماده ۶۷ بوده و ارکان مادی و روانی را تبیین می‌کند: رکن مادی جرم موضوع این ماده از اجزای زیر تشکیل یافته است:

الف) فعل فیزیکی: فعل فیزیکی ماده ۶۷ مشتمل بر دو جزء است: نخست سوءاستفاده یا استفاده غیرمجاز از داده‌ها یا سیستم از طریق افعالی مانند ورود، محو، توقف داده پیام یا مداخله در برنامه یا سیستم رایانه‌ای. از آنجا که افعال متضمن سوءاستفاده از رایانه تمثیلی بوده، همگی در ذیل فعل فیزیکی سوءاستفاده قرار می‌گیرد. افعال تمثیلی ذکر شده در ماده مورد بحث هم فعل فیزیکی مضاعف محسوب می‌شود و هم فعل فیزیکی واقعی. فعل فیزیکی مضاعف از این حیث که به طور جداگانه و مستقیم تشکیل دهنده فعل فیزیکی جرم نیستند و بلکه خود در ذیل

فعل فیزیکی سوءاستفاده یا استفاده غیرمجاز که در این جا فعل فیزیکی اولیه و اصلی است قرار می‌گیرند و افعال تمثیلی ذکر شده، فعل فیزیکی واقعی می‌باشند زیرا به صورت فیزیکی و عینی در سیستم رایانه‌ای تحقق می‌یابند و حال آنکه سوءاستفاده یا استفاده غیرمجاز فعل فیزیکی اعتباری هستند که پس از تحقق یکی از افعال فیزیکی نظیر ورود یا محو یا توقف داده، اعتبار می‌شوند. البته افعال فیزیکی مضاعف مانند ورود یا ایجاد داده ذاتاً غیرقانونی نیستند و بلکه اگر مورد سوءاستفاده قرار بگیرند در مقام فعل فیزیکی ظاهر می‌شوند. دوم تحصیل و بردن مال دیگری که با ضرورت تحقق این فعل فیزیکی کلاهبرداری موضوع ماده ۶۷ نیز در زمره جرائم مرکب خواهد بود.

ب) موضوع جرم: موضوع یا هدف جرم آن چیزی است که جرم برای آن یا به خاطر آن ارتکاب می‌یابد و در کلاهبرداری رایانه‌ای موضوع ماده ۶۷ مال، وجه و امتیازات مالی است. امتیازات مالی هر چند منجر به تحصیل واقعی مال نشود اما می‌تواند موضوع جرم واقع شود. پس اگر شخصی با مداخله در سیستم، نام خود را در ردیف اشخاصی که یک امتیاز مالی به آنها تعلق گرفته اضافه کند یا حتی از حیث تعلق وام برای خود حق تقدم قائل شود، هر چند آن وام را به گونه‌ای مسترد خواهد داشت، اما وقوع کلاهبرداری رایانه‌ای بعید نیست.

ج) وسیله جرم: در کلاهبرداری رایانه‌ای وسیله جرم شرط تحقق آن است و وسیله جرم طبق ماده ۶۷، داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای است. به استناد بند الف ماده ۲ قانون تجارت الکترونیکی، داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. سیستم رایانه‌ای نیز طبق بند «و» همین ماده هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده پیام عمل می‌کند.

د) شرط فریفتن قربانی یا گمراهی سیستم: فریب قربانی یا گمراهی سیستم در زمره فعل فیزیکی نیستند، زیرا فعل فیزیکی فقط نسبت به مرتکب است. بنابراین در اثر فعل فیزیکی سوءاستفاده یا استفاده غیرمجاز از داده پیام‌ها یا سیستم رایانه‌ای باید شخصی فریب بخورد و چنانچه مرتکب فعل فیزیکی را نسبت به سیستم

رایانه‌ای انجام دهد باید موجب گمراهی آن شود تا کلاهبرداری تحقق یابد و البته باید رابطه علیت بین عمل مرتکب و فریب شخص یا گمراهی سیستم احراز شود.

هـ) نتیجه مجرمانه: کلاهبرداری رایانه‌ای جرمی مقید است و باید افعال فیزیکی منجر به برده شدن مال یا وجه یا امتیازات مالی از سوی مرتکب انجام شود. قابل ذکر است که برده شدن باید مستقیماً در اثر فریب قربانی یا گمراهی سیستم رایانه‌ای حاصل شود.

کلاهبرداری رایانه‌ای همانند کلاهبرداری سنتی در زمره جرائم عمدی است که متضمن وجود قصد عام و قصد خاص است. قصد فعل یا سوءنیت عام ناظر به عمد مرتکب در سوءاستفاده یا استفاده غیرمجاز از داده پیام‌ها یا سیستم رایانه‌ای از یک سو و عمد در تحصیل و بردن مال دیگری است. کلاهبرداری چون جرم مرکب است در هر دو فعل فیزیکی باید عمد وجود داشته باشد. قصد نتیجه یا سوءنیت خاص نیز ناظر به قصد بردن مال یا وجه یا امتیازات مالی دیگری است.

## بند سوم: پیشگیری از کلاهبرداری رایانه‌ای

پیشگیری واکنشی از کلاهبرداری رایانه‌ای ناظر به کیفر مرتکب یا آموزش و اصلاح وی یا وادار نمودن به فعالیت‌های رایانه‌ای عام‌المنفعه است اما منظور از پیشگیری کلاهبرداری عمدتاً پیشگیری کنشی یا پیشگیری قبل از ارتکاب جرم است. در مورد کلاهبرداری رایانه‌ای دو قسم از پیشگیری کنشی یا پیشینی مطرح می‌شود:

**الف) پیشگیری غیرمستقیم:** از آنجایی که کلاهبرداری رایانه‌ای عموماً مؤخر بر سایر جرائم رایانه‌ای مانند نفوذ غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، جعل رایانه‌ای و... است، ابتدا باید زمینه تحقق این جرائم- که به نوعی نسبت به کلاهبرداری، جرائم مانع تلقی می‌شوند- را از بین برد. مهمترین نوع از پیشگیری در این حالت پیشگیری وضعی یا موقعیت‌مدار است. اقداماتی همچون نصب دیوار آتشین، به کارگیری گذارواژه مناسب، به روز رسانی نرم‌افزار، رمزگذاری ارتباطات، خلاصه‌سازی سیستم، تهیه نسخه پشتیبان و کلاً ایمنی‌سازی سیستم رایانه‌ای، میزان ارتکاب جرائمی مثل نفوذ غیرمجاز، شنود، جعل و جاسوسی را کاهش می‌دهد که این خود نتیجتاً موجب ناکامی کلاهبرداران و از بین رفتن زمینه‌های تحقق جرم کلاهبرداری می‌شود. بنابراین اقدامات ایمنی در سیستم رایانه‌ای به طور غیرمستقیم

در پیشگیری از کلاهبرداری مؤثر خواهد بود.

**ب) پیشگیری مستقیم:** پیشگیری بلاواسطه یا مستقیم از کلاهبرداری گاهی ناظر به اتخاذ اقداماتی برای مرتکب است و گاهی نیز کاربران یا استفاده کنندگان از سیستم رایانه‌ای. نسبت به اشخاصی که احتمال وقوع کلاهبرداری از سوی آنها با توجه به قرائن یا گزارش‌ها و اوضاع و احوال می‌رود باید تهیه امکانات لازم و همچنین ارائه هشدارهای مستمر صورت بگیرد و نسبت به کاربران و استفاده کنندگان از سیستم رایانه‌ای نیز آموزش یا تدارک سایت اینترنتی خاص بر حسب جنس و سن، در پیشگیری مؤثر خواهد بود. شاید آموزش کاربران اینترنتی یا استفاده کنندگان از سیستم رایانه‌ای مؤثرترین راه برای بزه‌دیده واقع نشدن و یا به عبارت دیگر پیشگیری از وقوع کلاهبرداری رایانه‌ای باشد. به همین دلیل مرکز دادخواهی کلاهبرداری اینترنتی امریکا در سال ۲۰۰۱ آموزش‌هایی کافی برای پیشگیری از وقوع جرم کلاهبرداری رایانه‌ای ارائه داده است که برخی از این آموزش‌ها به شرح زیر است:[۵۷]

الف- تا آنجا که ممکن است درباره خصوصیات فروشنده به ویژه زمانی که تنها از وی یک آدرس ای‌میل دارید اطلاع کسب کنید.

ب - معین کنید که فروشنده چه شیوه‌ای را برای پرداخت پول تقاضا کرده است و در کجا درخواست کرده که پول را بفرستید. و از فروشنده بخواهید زمان تحویل کالا را مشخص کند هم چنین اطلاعاتی از او دریافت کنید که نحوه ضمانت و امکان تعویض کالا در صورت خواست شما چگونه خواهد بود.

ج- فقط زمانی شماره کارت اعتباری خود را در وب سایت اعلام کنید که از امنیت و شهرت آن مطمئن باشید. قبل از استفاده از سایت، امنیت و محفوظ بودن نرم‌افزار مورد استفاده را بررسی کنید تا مطمئن شوید که اطلاعات حفظ خواهند شد.

د - با خریدارانی که به شما اطلاعات شخصی را نمی‌دهند وارد معامله نشوید و حتی در صورت ارائه اطلاعات از دیگر سایت‌ها وضعیت این شخص یا شرکت را بررسی کنید.

---

[۵۷] قاسم بابازاده، «کلاهبرداری اینترنتی» (ترجمه و تلخیص)، ***خبرنامه انفورماتیک***، آبان ۱۳۸۱، ش ۸۱، ص ۵۴.

هـ – بر اساس ظاهر سرمایه‌گذاری نکنید. تنها به این دلیل که فرد یا شرکت یک سایت با ظاهری خیره کننده دارد آن را قانونی تلقی نکنید؛ چرا که وب سایت‌ها فقط در عرض چند روز می‌توانند ایجاد و بعد از یک دوره کوتاه و پس از دریافت پول و عدم انجام معامله‌ای ناپدید شوند.

و – در هر چیزی که نسبت به آن به طور قطعی اطمینان ندارید، سرمایه‌گذاری نکنید. برای اطمینان از قانونی و معتبر بودن طرف معامله هر اقدامی که لازم می‌دانید انجام دهید.

ز – کالا را از بنگاه‌ها و فروشندگان خوش نام و معتبر خریداری کنید.

ح – سعی کنید علاوه بر داشتن آدرس صندوق پستی و شماره تلفن آنها، آدرس فیزیکی از فروشندگان به دست آورید.

مورد «الف» و «ب» برای پیشگیری از کلاهبرداری در مزایده‌های اینترنتی، مورد «ج» و «د» برای پیشگیری از تقلب در کارت‌های اعتباری، مورد «هـ» و «و» برای پیشگیری از تقلب در سرمایه‌گذاری و بالاخره مورد «ز» و «ح» برای پیشگیری از کلاهبرداری تجاری پیشنهاد شده است.

## نتیجه

کلاهبرداری رایانه‌ای موجودیت خود را به واسطه کثرت ارتکاب و خطرناکی آن از یک سو و تأثیرگذاری رایانه بر برخی از اجزای تشکیل دهنده کلاهبرداری در فضای واقعی از سوی دیگر به دست آورده است. علی رغم اینکه به نظر می‌رسد، عنوان کلاهبرداری رایانه‌ای نوعی افراط بلاوجه در تولید عناوین مجرمانه جدید است از این حیث که صرف تغییر وسیله ارتکاب جرم قادر به ایجاد عنوان مجرمانه جدید نیست، باید ادعا کرد که پیش‌بینی کلاهبرداری رایانه‌ای در کنار کلاهبرداری سنتی نه بر مبنای جرم‌انگاری خودسرانه که بر اساس درک مقتضیات فضای سایبر یا فضای مجازی رایانه و اینترنت است. این فضای جدید که به حق دنیایی جدید در برابر دنیای واقعی و فیزیکی انسان‌هاست، امکانات و قابلیت‌های جدید و خارق‌العاده‌ای به وجود آورده است که بدون توجه به آنها نمی‌توان این فضا را قاعده‌مند ساخت. کلاهبرداری در چنین فضایی نمی‌تواند دارای همان چهره‌ای باشد که در فضای واقعی و به موجب مقررات کیفری سنتی دارد. از این رو کلاهبرداری که در محیط

مجازی رایانه و اینترنت سوار بر زمان همه مکان‌های مجازی را درمی‌نوردد، در واقع دنیایی از امکانات را برای رسیدن به مقاصد خویش به خدمت می‌گیرد. در چنین فضایی کلاهبرداری، بردن مال دیگر با توسل به وسایل و مانورهای متقلبانه نیست و بلکه به هر نوع سوءاستفاده مالی از طریق رایانه اطلاق می‌شود. پس شرط نیست تا کلاهبردار انبوهی از کاربران ناشناخته را به طرف خود بکشاند و یا اینکه با مداخله در سیستم و یا تغییر داده‌ها، مال یا منافع مالی یا مزایای مالی تحصیل نماید. لازم هم نیست تا کلاهبردار با سوءاستفاده خود به مال یا وجهی برسد. همین مقدار که امتیازات یا خدمات مالی یا داده‌های دارای ارزش مالی را تحصیل نماید کافی است. این موارد واقعیات فضای سایبر در جرم‌انگاری مناسب در ارتباط با کلاهبرداری رایانه‌ای بلکه سایر جرائم رایانه‌ای است اما این یک روی سکه است. روی دیگر سکه این است که به موازات جرم‌انگاری کلاهبرداری رایانه‌ای و توسعه محدوده آن نباید در فکر طرد یا حذف مرتکب آن شد. مرتکب این جرم که یک شخص خلاق و باهوش است، شخصی است که فضای سایبر را مورد تاخت و تاز خود قرار داده است و همین شخص می‌تواند این فضا را در خدمت انسان به کار گیرد و به نظر می‌رسد جایگاه کلاهبردار رایانه‌ای پس از محکومیت در دادگاه باید رو به روی مانیتور رایانه که پنجره‌ای رو به دنیای جدید است، باشد تا پشت میله‌های زندان.

# JOURNAL OF

# LEGAL RESEARCH

VOL. III, NO. 2 2004-2

**Articles**



**Special Issue : Combatting of the Criminal Law against Economic offences**



**Report and Critique**



ISSN: 1682-9220

S. D. I. L.
The S.D. Institute of Law
Research & Study