



## سیاست جنائی ایران نسبت به کلاهبرداری در فضای سایبری با رویکرد کیفرگذاری

محمود رشنواز

دانشجوی دکتری حقوق بین الملل، واحد امارات، دانشگاه آزاد اسلامی، دبئی، امارات، نویسنده مسئول

Email: parsains4@gmail.com

علیرضا انصاری مهبیاری

استادیار گروه حقوق واحد نجف آباد دانشگاه آزاد اسلامی، نجف آباد، ایران

Email: alimahyari63@gmail.com

### چکیده

کلاهبرداری در زمره جرائمی است که هم جنبه اقتصادی دارد و هم به ابعاد معنوی شخصیت انسان مربوط می‌شود، و به همین سبب ممکن است گستره وسیعی را شامل شود به همین دلیل قانون‌گذار در تعیین مجازات این جرم به طور اختصاصی به وضع قانون پرداخته است و قانون تشدید مجازات کلاهبرداری را در این باب وضع کرده است. پژوهش حاضر که با هدف بررسی مجازات کلاهبرداری در فقه و حقوق موضوعه با روش مطالعاتی کتابخانه‌ای و شیوه‌ی توصیفی-تحلیلی در پاسخ به این سوال که مجازات کلاهبرداری سنتی و رایانه‌ای در فقه و حقوق موضوعه ایران چیست؟ با استناد به منابع معتبر فقهی و حقوقی به این نتایج رسیده است که در قانون تشدید سه درجه مجازات برای کلاهبرداری تعیین شده که شامل مجازات کلاهبرداری ساده، مشدد و کلاهبرداری به‌عنوان افساد فی‌الارض می‌باشد که به تصریح قانون جدید مجازات اسلامی، اعدام است. در فقه اسلامی کلاهبرداری با اصطلاحاتی چون احتیال به‌کاربرده می‌شود و اصولی چون منع اکل مال بالباطل، احترام به مال مسلمان، قاعده‌ی لاضرر، تدلیس، غش در معامله و ... توجیه‌کننده جرم انگاری کلاهبرداری هستند. هرگونه کلاهبرداری و بردن اموال دیگران مستوجب کیفر و جرم است و تفاوتی نمی‌کند ابزار در آن سنتی باشد یا مانند فناوری‌های جدید شامل رایانه و ... باشد. احتیال در دسته‌ی جرائم مستوجب تعزیر باشد چرا که قراردادن این جرم در دسته‌ی حدود نیاز به اسناد و روایات قویتری دارد که در دسترس نیست

**کلید واژه‌ها:** کلاهبرداری، جرایم مالی سایبری، کیفرگذاری، سیاست جنائی.



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

## مقدمه

کلاهبرداری جرمی است که در اثر تحولات اجتماعی پدید آمده در جوامع و ماشینی شدن امر و توسعه پیدا کرده است و انتشار آن به بعد از جنگ جهانی دوم بر می گردد<sup>۱</sup>. شریعت اسلام برای تحصیل مال غیر از طریق حيله و فریب مجازات حد سرقت پیش بینی نکرده است و آن را در ردیف جرائم مستلزم تعزیر قرار داده است. (حبیب زاده، ۱۳۷۵، ۲۵-۲۶)

روزگاری تجاوز به مال غیر همراه با خشونت و اعمال زور، بیشتر به صورت سرقت واقع می شده است، ولی تحول جوامع و صنعتی شدن، این نوع ربودن را تغییر داده و به جای ربودن خدعه آمیز مال غیر که معمولاً دور از نظر صاحب مال صورت می گرفته است؛ کلاهبرداران امروزه با توسل به وسایل متقلبانه و از راه خدعه و نیرنگ بدون هیچگونه خشونتی مال دیگران را (حتی با رضایت صاحب مال) از چنگال آنها خارج می کنند و در ظاهر هم، خود را از نخبگان جامعه به شمار می آورند. هر چند کلاهبرداری و سرقت در ربودن مال غیر، مشابهند، کلاهبرداران از نظر جرم شناسی در ردیف مجرمین حرفه ای و انسانهای یقه سفید هستند، که به دلیل هوش و ذکاوت سرشار شناسایی آنها بسیار مهم و پیچیده است. همانطور که روش خدعه آمیز آنها در ربودن مال مردم عجیب و بعضاً بظاهر مواجه است، روش آنها در توجیه اعمال مجرمانه خود و فرار از چنگ قانون هم، چشم ظاهر بین را به شک و اطمینان می دارد که مبدا اینان از انسانهای خارق العاده ای هستند که دست خلقت در ذات آنها راه مال اندوزی را به ودیعت گذاشته است. لذا شناخت این قبیل مجرمین هم از نظر حقوقی و هم از نظر جرم شناسی واجد اهمیت است و نباید تصور کرد که عدالت اقتضا دارد اگر سارقی مالی را معادل یک چهارم دینار طلای مسکوک در غیر سال قحطی از حرز بر باید دستش باید قطع شود، اما یک کلاهبردار که با هزار حيله و تقلب دیگران را می فریبد و از این طریق میلیون ها تومان به دست می آورد، فقط باید تعزیر شود؛ آن هم به میزانی که مادون حد باشد.

بعید است کسی قائل به ابدی بودن مقررات الهی اسلام و جامع الاطراف بودن آن باشد و چنین تصور کند که کلاهبرداری که اموال مردم را به یغما می برند و نظم جامعه را به هم می زنند و پایه های اقتصادی و فرهنگی و سیاسی حکومت اسلامی را متزلزل می کنند، از سارقی که ربع دینار از حرز می رباید، خطرناکتر نیستند. اگر سرقت به دلیل خاص «السارق و السارقه فاقطعوا ایدیهما جزءاً بما کسبا نکالاً من الله» حرام و مذموم است کلاهبرداری نیز به دلیل عام «یا ایها الذین آمنوا لا تاكلوا اموالکم بینکم بالباطل» و با توجه به قاعده غرر که از حدیث «نهی النبی عن الغرر» اخذ شده، حرام و مذموم است. در کتب فقهی از «محتال» بحث شده و منظور کسی است که با حيله و نیرنگ مال را از دیگران اخذ می کند؛ به این صورت که با نامه های جعلی و دوروغین و امثال آن خود را عامل اخذ مال جلوه میدهد. (عبدالله پور، ۱۳۹۲، ۲۵-۲۶)

در شرایط جامعه امروزی و با گسترش وسایل ارتباط جمعی و ارتباطات الکترونیکی جرم کلاهبرداری نیز به سمتی رفته است که از این وسایل برای تحقق آن استفاده می شود و مباحث حقوقی پیچیده ای را به میان آورده است که موضوع پژوهش ما نیز از این پیچیدگی بی بهره نمانده است. به هر حال تلفیق مبانی فقهی با این عناصر جدید و وسایل پیشرفته در شناخت جرم کلاهبرداری خود مسئله قابل تأمل و مهمی است که ما سعی خواهیم کرد به این موضوع نیز در حد توان و فرصت خود بپردازیم. بنابراین گام اول در بررسی مجازات جرم کلاهبرداری شناخت همه جانبه آن است.

<sup>۱</sup> - از نظر تاریخی عنوان (Furtum) در حقوق قدیم رم به معنای سلب مال غیر شامل سرقت خیانت در امانت و کلاهبرداری می شده است. اولین بار عنوان کلاهبرداری (escroquerie) پس انقلاب فرانسه در سال ۱۷۹۱ م با تصویب قانون جزای انقلابی در متون قانونی وارد شد و قوانین سایر کشورها از جمله ایران نیز از مقررات مذکور الگو گرفت.



## ۱- مفاهیم

مفاهیمی که در این قسمت به آن‌ها خواهیم پرداخت عبارت‌اند از: کلاهبرداری و مصادیق آن خواهد بود به این صورت که ابتدا معنای لغوی و سپس معنای اصطلاحی آن را بررسی خواهیم کرد که به‌عنوان یک جرم علیه اموال شناخته می‌شود. که این جرم واجد عناصر مادی، معنوی و قانونی است. شناخت مصادیق کلاهبرداری نیز در تعیین نوع مجازات آن موثر است.

### ۱-۱- مفهوم کلاهبرداری

کلاهبرداری یک عنوان مجرمانه است که به نوعی معنای ظاهری و لغوی آن با عنوان مجرمانه ارتباط به شکل کنایه آمیز دارد. در این بخش ابتدا به تعریف لغوی و سپس به تعریف اصطلاحی می‌پردازیم.

#### ۱-۱-۱- کلاهبرداری در لغت

در فرهنگ عامیانه فارسی اصطلاحاتی چون کلاه بر سر کسی گذاشتن و یا کلاه کسی را برداشتن کنایه از این است که با فریب و نیرنگ اموال شخصی را از چنگ او در بیاوریم و او را از حقوق خود محروم کنیم. این اصطلاحات عامیانه به تدریج وارد حقوق کیفری نیز شده است و یک عنوان مجرمانه را به خود اختصاص داده است که مانند برخی از عناوین مجرمانه دیگر نه ترجمه لغت خارجی است و نه از فقه اسلامی گرفته شده است. حال سعی می‌کنیم در این قسمت به تبیین مفهوم لغوی و اصطلاحی آن بپردازیم.

کلاهبرداری واژه‌ای فارسی مرکب از دو جزء (کلاه) و (برداری) است که معادل فرانسوی آن (escroquerie) و عربی آن (احتیال) است و در زبان انگلیسی در مقابل مفهوم مذکور واژه‌های Swindling, Cheat, Froud استعمال شده است لیکن واقعیت این است که در انگلیسی آن چه بیشتر در برابر کلاهبرداری به کار می‌رود عبارت (deception obtaining Property)

(by) که مصادیق متعددی در ذیل عنوان مذکور مورد بررسی قرار می‌گیرد. (حبیب زاده، ۱۳۷۷، ۲۴)

در حقوق رم جرائم سرقت، خیانت در امانت و کلاهبرداری از یکدیگر تفکیک نشده و «Furtum» شامل هر سه جرم می‌گردد است. (پاد، ۱۳۸۲، ۷) در زبان فارسی کلاهبرداری یعنی به دست آوردن چیزی از کسی از طریق خدعه و فریب و نیرنگ.

(عمید، ۱۳۷۵، ۸۳۸)

#### ۱-۱-۲- کلاهبرداری در اصطلاح

همانطور که گفتیم کلاهبرداری را نمی‌توان به معنای لغوی و تحت‌اللفظی آن مورد استفاده قرار داد چرا که با معنای مصطلح و رایج آن کاملاً متفاوت است بنابراین باید مفهوم اصطلاحی آن را بشناسیم.

قبل از اینکه به تعریف اصطلاحی جرم کلاهبرداری بپردازیم لازم است که به یک نکته اشاره شود. برخی از حقوقدانان جرائم را به دسته‌های مختلف تقسیم بندی می‌کنند، یک نوع از این دسته بندی‌ها این است که برخی از جرائم را در دسته جرائم یقه سفیدها قرار می‌دهند. این جرائم که بارزترین آن‌ها کلاهبرداری است توسط اشخاصی با ضریب هوشی بالا و موقعیت اجتماعی ممتاز صورت می‌گیرد و معمولاً جرائم علیه اموال است که در آن مقادیر زیادی پول و سایر اموال به مجرم می‌رسد برخلاف جرایمی مثل دزدی یا سرقت که توسط هر شخصی قابلیت تحقق دارد و البته بیشتر توسط اشخاص با طبقه اجتماعی پایین محقق می‌شود.

از نظر اصطلاحی کلاهبرداری عبارتست از تحصیل متقلبانه مال غیر یا بردن مال غیر از طریق به کار بردن وسایل متقلبانه، هر چند ماده ۱ قانون تشدید مجازات مرتکبین اختلاس، ارتشاء و کلاهبرداری، جرم مذکور را تعریف نکرده است، لیکن روبه

# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

قضایی تعریف مذکور را پذیرفته است و در تعاریفی که حقوقدانان هم ارائه داده‌اند تقریباً مفهوم مذکور مورد توافق قرار گرفته است. این معنا بیشتر بعد از انقلاب فرانسه با تصویب قانون جزای انقلابی در سال ۱۷۹۱ وارد متون حقوقی شده است و الا همانطور که گفتیم در حقوق روم باستان واژه (Furtum) به معنای سلب مال غیر، شامل کلاهبرداری، خیانت در امانت، سرقت و حتی جعل بوده با تصویب ماده ۳۰۰ قانون جزای عرفی در پنجم جمادی الاولی ۱۳۲۵ ه ق در ایران که از ماده ۴۰۵ قانون جزای فرانسه الهام گرفته بود، کلاهبرداری با مفهوم امروزی آن وارد حقوق ایران گردیده در سال ۱۳۰۴ ماده ۲۳۸ ق.م.ع جایگزین ماده مذکور شد و در سالهای ۱۳۵۲ و ۱۳۶۲ نیز با اندک تغییراتی وارد قانون مجازات عمومی و قانون مجازات اسلامی (تعزیرات) گردیده در سال ۱۳۶۷ بر اساس ماده ۱ ق.تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مجازات جرم مذکور تشدید شد و به رغم آن که مقنن در قانون تعزیرات مصوب ۱۳۷۵ فصل یازدهم را به‌عنوان (ارتشاء و ربا و کلاهبرداری) اختصاص داده است، هیچگونه حکمی در مورد کلاهبرداری بیان نکرده است که حاکی از تأیید ماده ۱ قانون تشدید است. ارجاع قانونگذار در ماده ۵۹۲ قانون اخیر الذکر به ماده سه قانون تشدید نیز مؤید آن است که نظر بر اجرای قانون تشدید داشته است. (حبیب زاده، ۱۳۷۷، ۲۴)

فارغ از تعریفاتی که ارائه می‌شود نکاتی که در تعریف کلاهبرداری باید رعایت شود عبارت‌اند از:

- فریب و حيله و اغفال قربانی حتماً در کلاهبرداری صورت می‌گیرد و در غیر این صورت بردن مال عناوین دیگری چون سرقت، راهزنی، جیب بری و ... را به خود می‌گیرد.
- بردن مال قربانی و تصرف آن به‌وسیله مجرم دیگر عنصر مهم تعریف کلاهبرداری است چرا که این جرم از جرائم علیه اموال است و خدشه دار کردن حیثیت شخص یا بردن آبروی او نمی‌تواند منجر به تحقق کلاهبرداری بشود.
- نقش قربانی در وقوع جرم یک نقش فعال است؛ به این معنی که قربانی جرم و مالباخته در اکثر موارد با رضایت اموال خود را در اختیار مجرم قرار می‌دهد و یا امکان دسترسی را برای او فراهم می‌کند، البته نه به قصد هبه یا صلح بلکه با فریبی که خورده است مال را در اختیار دیگری قرار می‌دهد و خود نقش فعال دارد. بردن اموال دیگران با هر روش خدعه آمیزی کلاهبرداری نیست بلکه در این بین باید قربانی فریب خورده و عمل فیزیکی تصاحب مال در اختیار کلاهبردار را انجام دهد.

## ۲- کلاهبرداری رایانه ای

قبل از بحث درباره کلاهبرداری رایانه‌ای لازم است تا یک مقدمه راجع به جرائم رایانه‌ای گفته شود تا ماهیت این جرائم مشخص گردد. جرائم رایانه‌ای در حقیقت به اعمالی گفته می‌شود که در ارتباط با رایانه و اینترنت و به طور کلی ارتباطات دیجیتالی صورت می‌گیرد و مطابق قانون برای آن مجازات تعیین می‌شود. به عبارت دیگر مرتکب آن‌ها مجرم و مسوولیت کیفری دارد.

آنچه امروزه جرم رایانه‌ای، جرم اینترنتی، جرم سایبر یا حتی جرم علیه فناوری اطلاعات و ارتباطات نام گرفته است، در واقع همگام با رشد و تکامل عصر حاضر توسعه یافته و هر روز جلوه‌های نوین و متنوع‌تری از آن مشاهده می‌شود. اما این اولین نکته‌ای که در درک مفهوم جرائم رایانه‌ای باید مدنظر داشت، این است که مفهوم رایانه فقط گزینه‌هایی که ذهن ما به آن‌ها معطوف می‌شود، مانند رایانه رومیزی یا قابل حمل را در بر نمی‌گیرد، بلکه همان طور که کنوانسیون بین‌المللی جرائم سایبر (مصوب ۲۰۰۱) به این موضوع صراحتاً اشاره کرده، «سیستم رایانه‌ای یک دستگاه یا مجموعه‌ای از دستگاه‌های



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

متصل به هم یا مرتبط با هم است که به وسیله یک برنامه، داده‌های دیجیتال را به طور خودکار پردازش می‌کند.» این تعریف همه دستگاه‌هایی که برنامه‌ای داشته باشند که داده‌های دیجیتال را پردازش کند، در برمی‌گیرد، مانند تلفن‌های همراه امروزی، سیستم‌های پی‌جو، تلفن‌های ثابت حافظه‌دار و موارد دیگر. هرچند این واقعیت نیز انکار نمی‌شود که مثال کامل این تعریف همان رایانه‌های رومیزی یا قابل حمل است. (جلالی فراهانی، ۱۳۸۳، ۹۰)

جرائم رایانه‌ای را می‌توان در سه رتبه یا نسل دسته‌بندی نمود:

۱ - جرائم نسل اول: تقریباً از سال‌های ۱۹۶۰ به بعد در کشورهای پیشرفته بابه خطر افتادن حقوق فردی شروع شد. کثرت پدیده سرقت برنامه‌ها، جاسوسی رایانه‌ای، سابوتاژ رایانه‌ای، استفاده غیر مجاز سیستم‌های رایانه‌ای جرائم اقتصادی مرتبط با رایانه، نفوذ در رایانه دیگران، تحت عنوان جرائم رایانه‌ای متجلی گردید.

۲ - جرائم نسل دوم: (جرائم علیه داده‌ها) هم‌زمان با گسترش سریع تکنولوژی اطلاعات در قلمرو زندگی و گسترش ارتباطات بین‌المللی و تکنولوژی مخابرات و ماهواره در دهه ۹۰، شاهد موج تازه‌ای از جرائم مرتبط با رایانه بوده‌ایم.

۳ - جرائم نسل سوم یا جرائم سایبر: رایانه آنگاه قدرت خود را به معنای واقعی به نمایش گذارد که در آستانه هزاره سوم «محیط سایبر» را به جهانیان عرضه نمود، این فضای مجازی از چنان قدرتی برخوردار است که به جرئت می‌توان گفت هر آنچه را که انسان بتواند تصور کند می‌تواند نمونه مجازی آن را در این محیط بیابد و در حوزه‌های مختلف در جهت مثبت و منفی از آن استفاده کند. این جرائم تحت عنوان «جرائم سایبر» یا (جرائم در محیط مجازی) معروف شدند که دربرگیرنده تمامی جرائم نسل قبلی البته به شکل کاملاً نوین چه از لحاظ نحوه ارتکاب و چه دادرسی در یک محیط مجازی می‌باشند. (گرایلی، ۱۳۸۹، ۱۶۱)

جرائم رایانه‌ای از جهت تأثیر به سه طبقه کلی قابل تقسیم است.

الف - جرائم رایانه‌ای فرهنگی: شامل جرائم بر ضد مالکیت فکری و جرائم بر ضد ارزش‌های فرهنگی چون: جرائم توهین و اهانت به دین مبین اسلام و مقدسات آن، جرائم محتوا (Content Crime)، افشای اسرار خصوصی افراد.

ب- جرائم امنیتی: مشتمل بر: ۱. جرائم علیه امنیت داده‌ها، شامل: جرائم علیه کاربرد مجاز داده‌ها مثل جاسوسی دسترسی غیر مجاز؛ و جرائم علیه صحت داده‌ها، همچون جعل؛ ۲. جرائم علیه امنیت سیستم.

ج- جرائم مالی: شامل کلاهبرداری و سرقت. (طارمی، ۱۳۸۶، ۱۷ و ۱۸)

در مورد تعریف جرم کلاهبرداری رایانه‌ای، نه در قانون تجارت الکترونیکی و نه در قانون جرائم رایانه‌ای تعریفی از جرم مذکور ارائه نشده است و تنها به مصادیق و شیوه‌های ارتکاب جرم اشاره شده است. اما با توجه به مفاد ماده ۶۷ قانون تجارت الکترونیک و ماده ۱۳ قانون جرائم رایانه‌ای، می‌توان دو تعریف ارائه نمود که یکی مربوط به کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی می‌باشد که ماده ۶۷ ق.ت.ا.بر آن اشاره دارد و آن عبارت است از «بردن مال یا تحصیل امتیازات مالی متعلق به غیر با عملیات متقلبانه از طریق سوء استفاده یا استفاده غیر مجاز از «داده‌پیام» ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور». تعریف دیگر با توجه به فحوای ماده ۱۳ ق.ج.ر. که به طور مطلق کلاهبرداری مرتبط با رایانه را جرم‌انگاری نموده است، عبارت است از: «تحصیل غیر مجاز مال، منفعت، خدمات و امتیازات مالی متعلق به غیر از سامانه‌های رایانه‌ای و مخابراتی» (صادقی، ۱۳۸۹، ۱۴۳)

ماده ۸ کنوانسیون جرایم سایبر کلاهبرداری رایانه‌ای را اینگونه تعریف کرده است: «هر گونه وارد کردن، تغییر دادن، حذف یا متوقف کردن داده‌های رایانه‌ای یا اخلال در عملکرد یک سیستم رایانه‌ای که به صورت عمدی وبدون حق و به قصد تحصیل متقلبانه یا ناروا و بدون حق یک منفعت اقتصادی برای خود یا دیگری انجام گرفته و موجب وارد شدن ضرر مالی به دیگری شود.» ( )

## ۱-۲- عناصر کلاهبرداری رایانه‌ای



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

کلاهبرداری رایانه‌ای نیز مانند کلاهبرداری سنتی و به مانند تمام جرائم دارای سه رکن قانونی، مادی و روانی است که به توضیح هر کدام خواهیم پرداخت.

## ۲-۱-۱- رکن قانونی کلاهبرداری رایانه‌ای

قوانینی که در باب کلاهبرداری رایانه‌ای قابل تأمل و توجه است و عنصر قانون این دسته از جرائم را تشکیل می‌دهد عبارت‌اند از: ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ مجمع تشخیص مصلحت نظام (که در ادامه قانون تشدید خوانده می‌شود) به‌عنوان عنصر قانونی جرم کلاهبرداری سنتی و همچنین ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ و ماده ۱۳ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ که به ترتیب تشکیل‌دهنده عنصر قانونی جرم کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی و کلاهبرداری رایانه‌ای در معنای عام می‌باشند.

فرآیند قانون‌گذاری توسط مجلس انجام می‌شود اما در فرآیند تهیه و تنظیم یک پیش‌نویس قانونی تا تحقیقات علمی عوامل مختلفی نقش دارند. از جمله: افکار عمومی، روشنفکران، سازمان‌های مستقل، احزاب و و گروه‌ها برای آگاه‌سازی مردم، نحوه تصویب، نوع تصویب، مفاد قوانین گذشته و... در بیش‌تر موارد قانون‌گذاری، قانون‌گذار ایرانی به پالایش محتوا توجه داشته در حالی که پالایه‌ی یک اقدام حفاظتی از اطلاعات در نظر گرفته نشده است. (توانا و کریمی،

۱۴۰۰: ۴۴۴)

در مورد ارتکاب اولین جرم کلاهبرداری رایانه‌ای در ایران اظهار نظر دقیقی نشده است. باین‌حال از لحاظ سابقه قانونگذاری به طور کلی می‌توان گفت با الحاق تبصره (۳) به ماده (۱) قانون مطبوعات در تاریخ ۷۹/۱/۳۰ با این مضمون که «کلیه نشریات الکترونیکی مشمول مواد این قانون است» اولین واکنش قانونی نسبت به این گونه جرائم بروز پیدا کرد. تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارها در تاریخ ۷۹/۱۰/۴ اقدام دیگر قانونگذار در قبال جرائم تجارت الکترونیکی بود. واکنش بعدی قانونگذار تصویب «قانون جرائم نیروهای مسلح» در تاریخ ۸۲/۲/۹ بود که در ماده ۱۳۱ سوء استفاده‌های مالی نظامیان با استفاده از رایانه (کلاهبرداری و اختلاس) را جرم‌انگاری نمود. تصویب قانون تجارت الکترونیکی در تاریخ ۸۲/۱۰/۷ واکنش قانونی دیگری نسبت به جرائم تجارت الکترونیکی بود که به تنظیم روابط تجاری در فضای مجازی پرداخته است. در نهایت قانون‌گذار با تصویب قانون جرائم رایانه‌ای در پنجم خرداد ماه ۱۳۸۸ که به جرم‌انگاری رفتارهای قابل ارتکاب در فضای سایبر اختصاص یافته، در فصل سوم تحت عنوان سرقت و کلاهبرداری مرتبط با رایانه، به جرم‌انگاری کلاهبرداری رایانه‌ای مبادرت نموده است. (صادقی، ۱۳۸۹، ۱۴۱)

## ۲-۱-۲- رکن مادی کلاهبرداری رایانه‌ای

در مورد رکن مادی این جرم همان مطالبی که در خصوص کلاهبرداری سنتی گفته شد در این مورد نیز صادق است و از تکرار آن‌ها پرهیز می‌کنیم، تنها جهت یادآوری بگوییم که این جرم نیز از طریق فعل مثبت مادی محقق می‌شود و وسیله در آن نقش اساسی دارد با این تفاوت که در این جرم وسیله مورد استفاده رایانه است. ممکن است این سؤال مطرح شود که آیا کلاهبرداری رایانه‌ای یا کامپیوتری با کلاهبرداری اینترنتی متفاوت است یا خیر؟ در پاسخ به این سؤال باید گفت: قبل از وجود اینترنت کامپیوتر وجود داشته‌است و کامپیوتر مفهومی قدیمی‌تر دارد.

کلاهبرداری رایانه‌ای یا کامپیوتری قبل از به وجود آمدن اینترنت وجود داشته‌است ولی بعد از اینکه اینترنت به وجود آمد و محیط مجازی<sup>۲</sup> به وجود آمد کم‌کم اصطلاح کلاهبرداری کامپیوتری به کلاهبرداری اینترنتی تغییر نام پیدا کرد به نحوی که بعضی معتقدند کلاهبرداری رایانه‌ای همان کلاهبرداری اینترنتی می‌باشد و این دو اصطلاح را به جای همدیگر به کار می‌برند.

<sup>2</sup> - cyberspace



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

اما بعضی دیگر معتقدند باید بین این دو اصطلاح تفاوت قائل شد و به طوری که باید کلاهبرداری رایانه‌ای یا کامپیوتری را اعم از کلاهبرداری اینترنتی تلقی کنیم پس از این حیث کلاهبرداری رایانه‌ای مفهومی عام نسبت به کلاهبرداری اینترنتی دارد. به طور کلی بستر ارتکاب این جرم محیط رایانه است. بنابراین وسیله جرم یعنی رایانه، جزو اجزاء تشکیل دهنده عنصر مادی این جرم محسوب می‌شود (خرم‌آبادی، ۱۳۸۴، ۱۵۳) مانورهای متقلبانه که در کلاهبرداری سنتی به صورت انجام افعال، طرح اقوال و اتخاذ سمت و عنوان مجعول به منظور بردن مال غیر متجلی می‌گردد آنگاه که در بستر فناوری‌های نوین اطلاعات و ارتباطات محقق می‌شود، اشکال دیگری به خود می‌گیرد که در قالب سوء استفاده یا استفاده غیر مجاز از داده پیام، برنامه‌ها و سیستم‌های رایانه ای و وسایل ارتباط از راه دور قابل بررسی هستند اگرچه ذکر این مصادیق جنبه تمثیلی دارد (قناد، ۱۳۸۷، ۱۳۴)

هدف از جرم‌انگاری کلاهبرداری رایانه ای، جرم شناختن هرگونه سوء استفاده در زمینه پردازش داده‌ها به خاطر تأثیرگذاری بر نتایج و انتقال غیر قانونی اموال و ایجاد خسارت است. بنابراین متن ماده ۶۷ ق.ت.ا. سوء استفاده به هر شکل را شامل می‌شود و نحوه عمل مرتکب را بیان کرده است. وارد کردن، تغییر، محو، ایجاد، متوقف کردن داده‌ها و یا مختل کردن عملکرد سیستم رایانه ای عناصر تشکیل دهنده جرم هستند.

منظور از ورود، وارد کردن اطلاعات به رایانه برای پردازش است و اعم از وارد کردن اطلاعات نادرست و نیز اطلاعات صحیح به صورت غیر مجاز است. محو داده پیام نیز عبارت از حذف اطلاعات به منظور از میان برداشتن دائمی آن است به نوعی که اطلاعات حذف شده قابل بازسازی و دستیابی مجدد نباشد. توقف داده پیام به معنای هر فعلی است که از فراهم بودن داده‌ها برای فردی که حق دسترسی به رایانه را دارد جلوگیری می‌کند یا جریان دسترسی به اطلاعات را قطع می‌کند. تغییر شامل اصلاح، تغییر جزئی یا کلی است. محو شامل حرکت و انتقال داده‌ها از محل اصلی خود مثلاً از نوار است. اختلال در سیستم رایانه‌ای نیز با خارج کردن عملکرد سیستم رایانه‌ای از حالت عادی خود به طوری که پردازش سیستم با مشکل مواجه شود، محقق می‌گردد. (صادقی، ۱۳۸۹، ۱۴۹)

در مورد شروع به کلاهبرداری رایانه‌ای نیز قانونگذار در تبصره ماده ۶۷ ق.ت.ا. شروع به جرم کلاهبرداری در بستر مبادلات الکترونیکی را جرم و مجازات آن را حداقل مجازات مقرر در ماده مذکور دانسته است. به موجب این ماده مجازات کلاهبرداری علاوه بر رد اصل مال به صاحبش، حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه می‌باشد. در اینجا نیز مانند کلاهبرداری سنتی چون در شروع به جرم هنوز مالی برده نشده است مجازات جزای نقدی منتفی است و تنها حکم به حداقل مجازات حبس می‌شود. قابل ذکر است که هم در اینجا و هم در تبصره ۲ ماده یک قانون تشدید... منظور از قید «حداقل مقرر» مجازاتی است که قاضی به آن حکم می‌کند نه صرفاً حداقلی که قانونگذار خود در ماده مقرر نموده است زیرا ممکن است قاضی با اعمال کیفیات مخففه به مجازاتی کمتر از حداقل مقرر در مواد مذکور حکم کند و ممنوعیتی در این باره وجود ندارد. نکته دیگر این که قانونگذار در ماده ۱۳ ق.ج.ر. اشاره‌ای به مجازات شروع به جرم کلاهبرداری رایانه‌ای نکرده است که بهتر بود قانونگذار همانند ماده یک قانون تشدید... و ماده ۶۷ ق.ت.ا. در اینجا نیز تکلیف را روشن می‌کرد. (صادقی، ۱۳۸۹، ۱۵۴)

## ۲-۱-۳- رکن معنوی کلاهبرداری رایانه‌ای

جرم کلاهبرداری در بستر مبادلات الکترونیکی موضوع ماده ۶۷ ق.ت.ا. و همچنین جرم کلاهبرداری موضوع ماده ۱۳ ق.ج.ر. نیز از زمره جرائم عمدی می‌باشند که در آن‌ها نیز همانند کلاهبرداری از نوع سنتی علاوه بر احراز سوء نیت عام وجود سوء نیت خاص هم برای تحقق جرم ضرورت دارد. بنابراین برای تحقق جرم کلاهبرداری رایانه‌ای مرتکب باید اعمال مصرحه در مواد قانونی فوق، اعم از ورود، محو و... را به طور عمدی انجام دهد یعنی در انجام عمل اراده داشته باشد دیگر اینکه نسبت به غیر مجاز بودن عمل ارتكابی مطابق ماده ۱۳ ق.ج.ر. و نسبت به استفاده سوء و یا استفاده غیر مجاز از «داده



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

پیام» ها و...، مطابقت. ا. علم و آگاهی داشته باشد. علاوه بر لزوم سوء نیت عام برای تحقق جرم کلاهبرداری رایانه‌ای، داشتن قصد نتیجه یعنی سوء نیت خاص نیز شرط است. در مورد کلاهبرداری رایانه‌ای، با توجه به نص ماده ۶۷ ق.ت.ا. و ماده ۱۳ ق.ج.ر. قصد نتیجه ناظر به تحصیل امتیازات مالی و یا بردن اموال دیگران برای خود یا دیگری است. بنابراین در صورتی که مرتکب بدون داشتن قصد نتیجه اعمال مذکور را انجام دهد عمل او کلاهبرداری رایانه‌ای محسوب نمی‌شود. (صادقی، ۱۳۸۹، ۱۵۳)

## ۲-۲- تفاوت کلاهبرداری سنتی و رایانه‌ای

تفاوت‌های اساسی بین ماده ۱۳ ق.ج.ر. با ماده یک از قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری وجود دارد که عبارت‌اند از:

در کلاهبرداری رایانه‌ای وسیله جرم رایانه است و اعمال ارتكابی نیز متفاوت است. اغفال قربانی ضرورتی ندارد. چون از طریق رایانه صورت می‌گیرد و ممکن است بدون هر گونه ارتباطی با شخص قربانی صورت بگیرد. البته بحث فریب سیستم‌های رایانه‌ای و دستکاری در آن وجود دارد که با فریب مستقیم قربانی متفاوت است. بردن مال در تعریف سنتی جرم مدنظر است و این در حالی است که در تعریف کلاهبرداری رایانه‌ای خدمات و امتیازات مالی نیز مشمول جرم شده است. که هم منطقی است و هم دایره شمول جرم را به درستی توسعه داده است. یعنی از طریق این اعمال اگر مرتکب موفق بشود امتیاز وامی را اخذ نماید و یا خدماتی را به صورت رایگان کسب نماید، جرم مزبور واقع می‌شود. برخی معتقدند: «در جرم کلاهبرداری رایانه ای برخلاف کلاهبرداری سنتی، اغفال و فریب بزه دیده شرط تحقق جرم نیست. همچنین، از حیث نتیجه، انتفاع مرتکب و ضرر به دیگری وجوه تشابه این دو بزه است اما بردن مال در کلاهبرداری رایانه ای (برخلاف سنتی) جزو نتیجه حاصله در رکن مادی آن نبوده بلکه بخشی از رفتار حصری در قسمت دوم رفتار فیزیکی این جرم و موضوع آن بزه است.» (پایدار فرد، نادری عوج بغزی، امتحانی، امتحانی، ۱۴۰۱: ۱۲۹) کلاهبرداری رایانه ای باید به تحصیل مال یا منفعت یا خدمات مالی یا امتیازات مالی بینجامد. این تحصیل می‌تواند برای خود مرتکب یا دیگری باشد. دیگری، کسی است که مرتکب تحصیل را برای وی خواسته باشد، (یار احمدی و براتی، ۱۴۰۱، ۶۴۹)

تفاوت بعدی در مرتکبین آن است که مطابق با تعریف سنتی آن اگر توسط کارمند دولت صورت بگیرد و یا مشمول موارد خاصی بشود کلاهبرداری از نوع مشدده خواهد شد و این در حالی است که در قانون مزبور به این موضوع اشاره نشده است.

## ۲-۳- روش‌های کلاهبرداری رایانه ای

روش‌های زیادی وجود دارد که از طریق آن‌ها می‌توان به کلاهبرداری رایانه‌ای پرداخت و اموال دیگران را به صورت متقلبانه تحصیل کرد و این روش‌ها نیز هر روز شکل جدیدی به خود می‌گیرد و همچنین انواع جدیدی به آن‌ها اضافه می‌شود. امروزه شیوه‌های مختلفی برای فریب افراد در فضای مجازی طراحی و اجرا می‌گردد. یکی از شایع‌ترین جرایم در این ارتباط، فیشینگ است. با راه اندازی سایت‌های مختلف جعلی و تبلیغات گوناگون در فضای مجازی و ارسال پیامک به شهروندان با موضوعات مختلف از قبیل ثبت نام برای جلوگیری از قطع یارانه‌ها، اختصاص سهمیه بنزین، دریافت مجوز طرح تردد زوج و فرد و سایر مواردی که بسته به موقعیت احتمال مطرح شدن آن‌ها نیز از سوی فرد کلاهبردار وجود دارد، اقدام به فریب دادن قربانیان برای دریافت هزینه ارائه این خدمات می‌کنند. شیوه‌های دیگری از جمله: اسکیم، سایت‌های شرط بندی، جعل اسناد خانه‌های بدون مالک، برنده شدن در قرعه‌کشی، پیشنهاد شغلی و موارد دیگری است که منجر به ازدیاد این نوع جرم شده است. (توانا و کریمی، ۱۴۰۰: ۴۴۳)

در ادامه به برخی از این روش‌های شناخته شده خواهیم پرداخت:

- تغییر و دستکاری اطلاعات ورودی به کامپیوتر



# چهارمین کنفرانس ملی پدافند سایبری

آبان ۱۴۰۲

ساده‌ترین و رایج‌ترین روش کلاهبرداری رایانه‌ای که در بسیاری از موارد از سوی کاربران سیستم مورد استفاده قرار می‌گیرد، دستکاری آگاهانه داده و اطلاعات در هنگام ورود آن به سیستم و یا تغییر آن در مراحل اداری بعدی است که معمولاً چنین تغییری با قصد بهره‌مند شدن از منافع مشروع آن انجام می‌گیرد. البته مقاصد دیگری نیز ممکن است مطرح باشد؛ به‌عنوان مثال، کاربر مجازی که در یک شرکت یا سازمان، ساعات اضافه‌کار خود را در سیستم حقوق و دستمزد افزایش می‌دهد، یا کارمند یک بانک، مؤسسه اعتباری، یک شرکت یا فروشگاه که بخشی از وجوه نقد یا اسناد مالی دیگر را در هنگام واریز آن‌ها به صندوق و یا حساب‌های بانکی کارفرما، به حساب بانکی خاصی که خود و یا افراد همدست با او در اختیار دارند، واریز می‌کند. از چنین روش کلاهبرداری رایانه‌ای بهره می‌گیرند.

این نوع دستکاری اطلاعات از سوی جرم‌شکنانی که به‌روشهای گوناگون و غیر مجاز به سیستم راه می‌یابند، نیز اعمال گردد، حتی در ظاهر با نام کاربر و گذر واژه کاربرد مجاز، در برخی موارد کاربران یا افرادی که به سیستم دسترسی ندارند، مستقیماً اطلاعات را دستکاری نمی‌کنند، بلکه اطلاعات محرمانه را، خود در اختیار می‌گیرند و یا در اختیار دیگران می‌گذارند و این اطلاعات برای سوء استفاده به‌کار گرفته می‌شود؛ به‌عنوان مثال، اطلاعات کارت‌های اعتباری به‌میزان زیادی از سوی کلاهبرداران رایانه‌ای برای کسب منافع نامشروع، مورد استفاده قرار گرفته است. حتی ممکن است اطلاعات ذی‌ربط، اطلاعاتی باشد که برای افراد جنبه محرمانه یا خصوصی داشته باشد و مجرمان در صورت دسترسی به آن، به باجگیری یا اخذ حق السکوت اقدام نمایند و افراد نیز برای حفظ آبروی خود با پوشاندن خلافشان، حاضر به پرداخت پول گردند. برخی شرکت‌ها، سازمان‌ها و مؤسسات حاضر می‌شوند برای حفظ اعتبار خود و از دست ندادن اطمینان افکار عمومی حق السکوت بپردازند.

(معاونت کشف علمی جرائم، ۱۳۸۰، ۷۰)

- پرداخت پول واهی به افراد توسط اشخاص حقوقی

از دیگر انواع کلاهبرداری رایانه‌ای، مواردی است که شرکت‌ها و مؤسسات خاصی نسبت به پرداخت پول یا صدور چک در وجه افراد یا مؤسسات دیگر اقدام می‌کنند و کلاهبرداران از این طریق به سوء استفاده مالی می‌پردازند؛ برای مثال، اضافه کردن نام افراد واهی و یا غیر شاغل در فهرست پرداخت حقوق، ترتیب دادن صدور چک‌های بازپرداخت هزینه بیمه و بازنشستگی، برای هزینه‌های دروغین گزارش شده به حساب افراد خاطی یا همکاران او و بازپرداخت چک‌های جعلی و اضافه مالیات، مواردی از این نوع سوءاستفاده‌ها محسوب می‌گردند.

- پاک کردن بدهی بدون پرداخت آن

نوع دیگر کلاهبرداری رایانه‌ای، مربوط به حذف یا کسر بدهی‌های شرکت‌ها یا افراد می‌باشد؛ به‌عنوان نمونه، پاک کردن بدهی جرائم راهنمایی و رانندگی، اقساط وام و یا هزینه‌های خدمات عمومی نظیر آب برق، تلفن یا گاز و سایر بدهی‌ها نیز از جمله موارد مشاهده‌شده کلاهبرداری رایانه‌ای است.

- کلاهبرداری ثبتی در فضای مجازی

با توجه به تغییر شکل بستر جرایم ثبتی از فضای سنتی به فضای مجازی که به وسیله رایانه در فضای ارتکاب متفاوت که همان تفاوت در رکن مادی است، صورت می‌گیرد، از آنجا که قوانین ثبتی که ناظر بر مواد و آیین نامه‌های ثبتی است لذا ضرورتاً باید اصلاحاتی در همگام سازی قوانین ثبتی با ضروریات روز جامعه نمود زیرا این قوانین به دلیل کهنگی بعضاً خود قوانین جرم زدا هستند و بر ارتکاب جرایم صحنه بیشتری می‌گذارند. در حوزه فضای مجازی نیز کلاهبرداری و جعل های رایانه ای به وسیله توکن سردفتر، اثر انگشت غیر واقعی از بیشترین جرایم موجود در بستر مجازی است. بنابراین با مذاقه در قانون به نظر می‌رسد، کلی گویی قانونگذار در خصوص جرایم ثبتی که باز به کهنگی و پراکندگی قوانین مربوط به آن مرتبط است موجب عدم تناسب مجازات با جرایم مربوطه علی‌الخصوص در فضای مجازی می‌گردد. (ساجدی، رضوی فرد، صادقی، ۱۴۰۰،

(۶۱)



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

- فریفتن افراد از طریق تبلیغات در اینترنت

درمقابل، انواع خاصی از کلاهبرداری‌های رایانه‌ای وجود دارد که مجرمان از طریق فریفتن سایبرین، به کسب مال مبادرت می‌نمایند و از رایانه بیشتر به‌عنوان کانالی برای تبلیغ کالا یا خدمات و یا ابزار خرید و فروش در معاملات تجارت الکترونیکی استفاده می‌کنند. نمونه‌های متنوع این نوع کلاهبرداری شامل فروش کالا بدون تحویل آن، فروش کالای مسروقه یا ممنوعه، دریافت پول برای عرضه کارت اعتباری یا سایر کارت‌های بهادار بدون تحویل آن و یا تحویل نمونه تقلبی آن می‌شود. همچنین مواردی از قبیل تبلیغ سرمایه‌گذاری‌های پرسود با قصد کلاهبرداری، نظیر شرکت‌های کلاهبرداری، که در ایران اصطلاحاً به شرکت‌های مضاربه‌ای معروف گردیدند. کلاهبرداری از طریق دریافت پول جهت فراهم کردن امکانات مهاجرت یا اشتغال پردرآمد و یا جامه عمل پوشاندن به مقاصد نامشروع افراد در جعل و اسناد نیز از جمله این نوع کلاهبرداریها می‌باشند که نوع جدیدتر کلاهبرداریهای کلاسیک محسوب می‌شوند.

- نقض علائم تجاری

نقض مالکیت فکری اعم از حق مؤلف و علائم تجاری از جمله روش‌هایی است که بسیار در ارتباطات الکترونیکی به وقوع می‌پیوندد و سوء استفاده‌های زیادی از آن به عمل می‌آید به این صورت که افرادی با فریب دیگران به وسیله‌ی معرفی اثر سایرین به‌عنوان اثر خود و یا معرفی یک علامت تجاری به نام خود به کلاهبرداری می‌پردازند و وجوه و اعتباراتی را کسب می‌کنند.

علامت تجاری عبارتست از یک کلمه، تصویر، شعار، یا سایر چیزهایی که به منظور تمایز کالاها یا خدمات یک شخص خاص مورد استفاده قرار می‌گیرد. براساس قانون ۱۹۹۴ انگلستان هرگونه علامتی که آشکارا قابل تشخیص بوده و بتواند نوعی از کالاها و خدمات را از انواع دیگر متمایز گرداند علامت تجاری نامیده می‌شود که ممکن است به صورت یکی از اشکال زیر باشد. (انصاری، ۱۳۸۲، ۲۸ و ۲۹)

عبارت یا کلمه نظیر اسم شخص

طرح و تصویر

به صورت شکل یا حرف

به صورت شماره و عدد

به صورت شکل کالاها یا عدل بندی آنها

مطابق ماده ۶۶ قانون تجارت الکترونیکی هرگونه نمایش بر خط علائم تجاری را در صورتی که موجب فریب یا مشتبه شدن طرف به اصالت کالا و خدمات شود، ممنوع اعلام داشته است. بر این اساس چنانچه دارنده یک وب سایت مبادرت به نمایش یک علامت تجاری به صورت بر خط بنماید و علامت تجاری مزبور به نحو فریبنده‌ای مشابه یک علامت تجاری متعلق به دیگری باشد به طوری که مصرف‌کنندگان عادی را دچار اشتباه در اصالت کالا یا خدمات موضوع علامت مزبور نماید، عمل وی از مصادیق نقض علامت تجاری دیگری محسوب و مشمول ممنوعیت ماده ۶۶ قانون تجارت الکترونیکی می‌شود. ضمانت اجرای تخلف موضوع ماده ۶۶ در ماده ۷۶ پیش‌بینی شده است

ممکن است شخصی به انگیزه‌ی سودجویی و یا حتی بدون اطلاع و آگاهی یا به انگیزه‌های دیگر مانند انتقام جویی و ... یک علامت تجاری را نقض کند بدین معنا که از آن علامت برای معرفی کالای خود یا دیگری استفاده کند و یا اینکه علامت تجاری را به گونه دیگری معرفی کند. در تمامی این موارد شخص دیگران را نسبت به این علامت تجاری گمراه کرده است و اعتبار آن را نقض نموده است. این نقض ممکن است در دنیای واقعی و یا در فضای مجازی رخ بدهد و در نهایت در مسوولیت مرتکب آن تاثیری نباید داشته باشد چون نتیجه کار او یکسان است.



# چهارمین کنفرانس ملی پدافند سایبری

آبان ۱۴۰۲

با توجه به مصادیقی که برای کلاهبرداری در حقوق موضوعه ذکر کردیم و اصول و قواعد حقوقی که در حرمت این جرم بیان شد به نظر می‌رسد که می‌توان مصادیق دیگری نیز در جان امروز برای این عنوان کلی مجرمانه یافت. مصادیقی که به نوعی شامل زیان به دیگری می‌شود و از سوی دیگر با استفاده از وسایل و ابزار متقلبانه باید عمل مورد نظر ارتکاب یابد تا بتوان آن را در مصادیق کلاهبرداری قرار داد.

ارتباطات جدید موجب شده است تا بسیاری از روابط اقتصادی و غیراقتصادی چون روابط فرهنگی و ... در قالب‌های جدیدی مطرح شود. ظهور ارتباطات نو و اینترنت که دنیای مجازی را برای جهان امروز به ارمغان آورده است، موجب شده که اعمالی که ممکن است به شکل متقلبانه باعث بردن اموال دیگران یا لطمه به حیثیت و آبروی آنان گردد گسترش یابد و در نتیجه دایره مصادیق این عنوان مجرمانه گسترش یابد.

آنچه در مصادیق کلاهبرداری بین فقه و حقوق موضوعه اختلاف ایجاد می‌کند و در واقع وجوه تفاوت میان مصادیق کلاهبرداری در فقه و حقوق موضوعه است عبارتند از :

کلاهبرداری در فقه با عنوان احتیال، تدلیس، غش در معامله و ... بیان شده است و عنوانی به نام کلاهبرداری در فقه نداریم. مصادیق کلاهبرداری در حقوق موضوعه و فقه با یکدیگر متفاوت هستند. چنانکه در فقه فریبکاری برای بردن مال دیگری از طریق جعل سند مشمول احتیال است ولی در حقوق موضوعه ابزارهای متقلبانه در اعمال مختلف چون صدور چک، ورشکستگی، تقلب در امور ثبتی و مالیاتی شامل مصادیق کلاهبرداری است.

### ۳- مجازات کلاهبرداری رایانه‌ای

در مورد اینکه مجازات کلاهبرداری رایانه‌ای چیست بستگی به این دارد که کلاهبرداری رایانه‌ای را از چه دیدگاهی بررسی کنیم: همانطور که ملاحظه شد در مورد کلاهبرداری رایانه‌ای به معنی اعم چند عنصر قانونی متفاوت وجود دارد که هر یک در جای خود قابل بررسی اعمال است ولی آنچه که در اینجا مد نظر است کلاهبرداری به معنی اخص کلمه یا کلاهبرداری مندرج در قانون جرائم رایانه‌ای است که طبق ماده ۱۳ قانون مذکور «هر کس بطور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی با... وجه یا مال... برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا ۵ سال یا جزای نقدی از بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد» (پور قهرمانی، ۱۳۹۳، ۱۱۲) جزای نقدی در این ماده در مورد کلاهبرداری رایانه‌ای محدود است و بستگی به میزان اموالی که مورد کلاهبرداری قرار گرفته است ندارد و به همین دلیل به نظر می‌رسد که با توجه به گستردگی که ممکن است در کلاهبرداری‌های رایانه‌ای اتفاق افتاده است قانون‌گذار این محدودیت را ایجاد کرده است چراکه جزای نقدی در این سطح وسیع می‌تواند ناعادلانه و حتی غیر ممکن بوده و تنها موجب افزایش حجم زندانیان شود. در خصوص این ایراد که بر قوانین دیگر نیز در مورد جزای نقدی نیز وارد است و مربوط به تورم و کاهش بازدارندگی جزای نقدی است قانونگذار در ماده ۵۳ همین قانون راه حل را مشخص کرده است و بیان می‌کند که: «میزان جزای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است» که البته تا این تاریخ یعنی آبان ۱۳۹۵ هیچ تجدید نظری در این میزان از جرائم نقدی شکل نگرفته است و به همان شکل اولیه اجرا می‌شود.

درمقایسه با کلاهبرداری سنتی مجازات اصلی کلاهبرداری رایانه‌ای با توجه به اینکه در سطح گسترده در فضای مجازی واقع شود اندک است هر چند در ماده ۲۶ قانون جرائم رایانه‌ای<sup>۳</sup> این نقیصه تا حدی رفع شده است همچنین مجازات معینه جرم

<sup>۳</sup> - ماده ۲۶ قانون جرائم رایانه‌ای. در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد: الف) هر یک از کارمندان و کارکنان ادارات و سازمان‌ها یا شوراها و یا شهرداری‌ها و موسسه‌ها و شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

مذکور مختص اشخاص حقیقی است و در صورتیکه این جرم توسط اشخاص حقوقی صورت گیرد مجازات جرم مذکور طبق ماده ۱۹ و ۲۰ قانون مذکور تشدید خواهد شد. همچنین در آخر باید خاطرنشان کرد که این قانون نسبت به قانون کلاهبرداری سنتی خاص است و بنابراین برخلاف کلاهبرداری سنتی منعی برای تخفیف، تبدیل یا تعلیق مجازات وجود ندارد. (پور قهرمانی، ۱۳۹۳، ۱۱۲) در واقع مواد یاد شده مجازات کلاهبرداری رایانه‌ای مشدد را بیان می‌کنند که در صورت ارتکاب کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی به موجب ماده ۶۷ ق.ت.ا. مرتکب علاوه بر رد اصل مال و امتیازهایی که تحصیل کرده به صاحبان آن‌ها، به ۱ تا ۳ سال حبس و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌گردد.

در اینجا قابل توجه است که قانونگذار برای کلاهبرداری رایانه‌ای به طور عام (ماده ۱۳ ق.ج.ر) و کلاهبرداری رایانه‌ای به طور خاص (ماده ۶۷ ق.ت.ا.) مجازات خفیف‌تری نسبت به کلاهبرداری سنتی پیش‌بینی کرده است. برخی در توجیه این عمل این استدلال ضعیف را ارائه می‌کنند که مجازات سنگین ماده یک قانون تشدید... به خاطر مرکب بودن جرم کلاهبرداری سنتی و دشوار بودن تحقق و احراز آن است و حال آنکه ماده ۱۳ ق.ج.ر. عملاً نوعی تحصیل مال به صورت غیر مجاز را پیش‌بینی کرده که مصادیق آن بسیار زیاد است. با بررسی تطبیقی مجازات‌های جرایم سرقت سنتی و سرقت سایبری، کلاهبرداری سنتی و کلاهبرداری سایبری و تشویق و ترغیب به فساد و فحشاء در فضای سنتی و فضای سایبری معلوم می‌شود اصل تناسب جرم و مجازات و توازن مجازات‌ها در جرایم مشابه رعایت نشده است و مجازات جرایم مشابه در فضای سایبر به مراتب سبکتر از ارتکاب همان جرایم در فضای سنتی است که به نظر می‌رسد این اختلاف در مجازات فاقد توجیه حقوقی و منطقی است و بازنگری و اصلاح قانون را مطالبه می‌کند. (فتحی، ۱۴۰۱، ۱)

با این حال به نظر می‌رسد که قانونگذار در تعیین مجازات باید دقت بیشتری می‌نمود و برای کلاهبرداری رایانه‌ای چه به طور عام و چه در بستر مبادلات الکترونیکی، مجازاتی سنگین‌تر از کلاهبرداری سنتی تعیین می‌کرد زیرا کلاهبرداری رایانه‌ای بسیار سریع‌تر و با کمترین هزینه واقع می‌شود و بیشترین خسارت را نیز به همراه خواهد داشت. قابل ذکر است، کلاهبرداری رایانه‌ای نیز همانند کلاهبرداری سنتی جرمی مرکب است که تنها فرآیند ارتکاب آن متفاوت است. دیگر اینکه جرم کلاهبرداری سنتی در محیط فیزیکی واقع می‌شود و نسبت به کلاهبرداری رایانه‌ای که در محیط سیستم‌های رایانه‌ای و به

اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضائی و به طور کلی اعضاء و کارکنان قوای سه گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند. (ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد. (ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد. (د) جرم به صورت سازمان یافته ارتکاب یافته باشد. ه) (جرم در سطح گسترده ای ارتکاب یافته باشد.

۴ - ماده ۱۹. در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود: الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود. ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد. ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود. د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد. تبصره ۱. منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد. تبصره ۲. مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقوقی مسؤول خواهد بود. ماده ۲۰. اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد: الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال. ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد. تبصره. مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت.



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

طور کلی در فضای مجازی واقع می‌شود احراز آن ساده‌تر است زیرا با توجه به اینکه در فضای مجازی اصل بر ناشناختگی است کشف و تعقیب جرائم ارتكابی در آن و اثبات آن‌ها بسیار دشوار و گاه غیر ممکن است. (صادقی، ۱۳۸۹، ۱۵۶)

## نتیجه گیری

برخی از جرایم و عناوین مجرمانه که در ارتباط با اموال می‌باشد هم در فقه اسلامی و هم در حقوق موضوعه مورد حمایت قانون‌گذار قرار گرفته است. در فقه اسلامی برای سارق حد قطع ید معین شده است که همین مجازات نشان دهنده اهمیت حمایت از حقوق مالی اشخاص است. در حقوق موضوعه نیز این مسئله در قوانین مختلف جزایی چه به شکل سنتی و چه به شکل رایانه‌ای و در ارتباطات جدید مورد حمایت قرار گرفته است. کلاهبرداری با هر شیوه و وسیله‌ای ممکن است ارتكاب یابد و این در حالی است که در اصل موضع هیچ تفاوتی ایجاد نمی‌کند یعنی قواعد احترام به مال مسلمان، لاضرر و امثالهم همگی مبین این مطلب هستند که کلاهبرداری و بردن مال دیگری به هر شیوه‌ای مستوجب مجازات است و تفاوت تنها در شدت مجازات و نوع آن است.

- با توجه به قانون تشدید مجازات کلاهبرداری، مجازات حبس ۲ تا ۱۰ سال و مجازات رهبری شبکه کلاهبرداری مطابق ماده ۴ همان قانون مجازات مفسد فی الارض است.
- مجازات جرم کلاهبرداری سنتی در سه درجه تقسیم بندی شده است که عبارت‌اند از: مجازات ساده: حبس از یک تا ۷ سال و پرداخت جزای نقدی معادل مالی که اخذ کرده. مجازات مشدد کلاهبرداری: حبس از ۲ تا ده سال و انفصال ابد از خدمت دولتی و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود. مجازات اشد که همان اعدام به جهت افساد فی الارض است و در ماده ۴ بیان شده است با توجه به این مطالب فرضیه مورد نظر تا حدودی صحیح است و تنها مجازات کلاهبرداری ساده در آن لحاظ نشده است. به عبارت دیگر مجازات کلاهبرداری همان ۲-۱۰ سال حبس و اعدام است و تنها در موارد کلاهبرداری ساده حبس یک تا ۷ سال به آن اضافه می‌شود.
- کلاهبرداری در شکل سنتی و رایانه‌ای آن با توجه به میزان اختلاتی که در جامعه ایجاد می‌کند می‌تواند در جرائم مستوجب حد یا تعزیر قرار گیرد.
- کلاهبرداری در فقه با تعبیر احتیال به کار برده می‌شود و به نظر می‌رسد که احتیال در دسته‌ی جرائم مستوجب تعزیر باشد چرا که قراردادن این جرم در دسته‌ی حدود نیاز به اسناد و روایات قویتری دارد که در دسترس نیست و اگر در روایتی مجازات اعدام یا قطع ید برای این جرم تعیین شده است از باب افساد فی الارض بوده که قابل بررسی است، ولی به هر حال نه کلاهبرداری و نه احتیال در زمره‌ی حدود نمی‌باشند. حتی محارب دانستن کلاهبردار نمی‌تواند دلیل موجهی داشته باشد و به دلایل متقن قابل رد است. با توجه به این نتایج نیز فرضیه مورد نظر ثبات می‌شود چرا که کلاهبرداری با توجه به نوع آن ممکن است در گروه هر کدام از مجازات‌ها (تعزیر یا حد) قرار بگیرد.
- قانون‌گذار با تصویب قانون تشدید مجازات مرتکبین کلاهبرداری خواسته است این جرم مهم و گسترده را به نوعی مهار کند و جنبه‌ی ارعایی مجازات را در این خصوص قابل توجه نماید تا اینکه از ارتكاب جرم جلوگیری نماید. در حقیقت قانون تشدید نوعی اعلام درک قانون‌گذار از شرایطی است که در آن جرم کلاهبرداری را آسیب‌های زیادی برای جامعه دارد.
- تعیین مجازات جزای نقدی نسبی برای جرم کلاهبرداری از مواردی است که قانون‌گذار کمتر از آن استفاده کرده و علت وضع آن در کلاهبرداری همان حساسیت بالای جرم و آثار مخرب آن بر جامعه است که قانون‌گذار سعی در جلوگیری از آن داشته است. و به نظر می‌رسد که قانون‌گذار در این زمینه به درستی عمل کرده است و اندیشه‌ای پیشگیرانه را مد نظر داشته است.



# چهارمین کنفرانس ملی پدافند سایبری

۸ آبان ۱۴۰۲

- مجازات کلاهبرداری رایانه‌ای با کمال تعجب خفیف‌تر از مجازات کلاهبرداری سنتی است که ممکن است باین دلیل باشد که کلاهبرداری رایانه‌ای آسان‌تر محقق می‌شود و یا اینکه امکان پیشگیری با ابزارهای دیگر در آن وجود دارد.
- تعیین مجازات برای کلاهبرداری در سایر قوانین نیز دیده می‌شود و در حقیقت قانون تشدید نوعی قانون عام در این زمینه است که در صورت نبودن قانون خاص می‌توان به آن رجوع کرد.
- در قانون مجازات جدید نهادهایی چون تعویق صدور حکم و جایگزین‌های حبس پیش‌بینی شده است که در مورد کلاهبرداری به نظر می‌رسد با توجه باینکه کلاهبرداری از نوع مجازات‌های درجه ۴ می‌باشد (بیش از پنج تا ده سال) و با عنایت به تبصره ۲ ماده ۱۹ قانون جدید مجازات اسلامی که اشعار داشته است "مجازات‌ی که حداقل آن منطبق بر یکی از درجات و حداکثر آن منطبق با درجه بالاتر باشد، از درجه بالاتر محسوب می‌شود" کلاهبرداری از درجه ۴ مجازات‌ها می‌باشد، بنابر این مشمول تعویق صدور حکم نخواهد شد. و تعلیق مجازات نیز به صراحت تبصره یک ماده ۱ قانون تشدید در خصوص مجازات کلاهبرداری ممکن نیست.

## پیشنهادها

- قانون تشدید باید در خصوص کلاهبرداری رایانه‌ای که امروزه بسیار شایع بوده و ارقام مالی کلانی در آن موضوع جرم قرار می‌گیرد نیز تعیین تکلیف کند مجازات‌های مشدد و اشد را برای این جرائم نیز به صراحت تعیین نماید.
- قوانین مختلف که مصادیق خاص کلاهبرداری را معین می‌کند گاها با قانون تشدید در تعارض و تناقض قرار دارند که لازم است قانون‌گذار یا رویه‌ی قضایی تکلیف را در این باب تعیین نماید و از تورم قوانین در این حوزه بکاهد.
- در مجازات‌های تبعی مانند محرومیت از حقوق اجتماعی در خصوص کلاهبرداری مواد قانونی زیادی وجود دارد که باید قانون‌گذار در مورد آن‌ها به جمع‌بندی رسیده و به صورت یکپارچه قانون‌گذاری نماید.
- ماده ۴ قانون تشدید بیان می‌کند کلاهبردار «در صورتیکه مصداق مفسد فی‌الارض باشد» به مجازات آن می‌رسد که مطابق قانون مجازات اسلامی ۱۳۹۲ به مجازات اعدام محکوم خواهد شد. تعیین اینکه چه نوع کلاهبرداری مصداق افساد فی‌الارض است کاری است دشوار و گذاشتن آن بر عهده‌ی قاضی خروج از صراط عدالت و نادیده گرفتن اصول حقوقی است. گرچه با توجه به اینکه کلاهبرداری گاها چنان در سطح وسیع ممکن است اتفاق افتد که مجازات اشد برای مرتکب آن عین عدالت باشد ولی باید توجه کرد که تعیین معیار در این زمینه باید دقیق باشد.



## منابع

### منابع فارسی

- انصاری، باقر (۱۳۸۲) مقدمه‌ای بر مسؤولیت مدنی ناشی از ارتباطات اینترنتی. مجله دانشکده حقوق و علوم سیاسی. دوره ۶۲، شماره ۵۱۲، صص ۵۲-۹
- پاد، ابراهیم (۱۳۸۲) حقوق کیفری اختصاصی. تهران، انتشارات رهام. جلد دوم.
- پایدارفرد، علی، نادری عوج بغزی، جواد، و امتحانی، احمدرضا. (۱۴۰۱). مقایسه رکن مادی جرم کلاهبرداری رایانه ای با سنتی. تمدن حقوقی، دوره ۵، شماره ۱۲، صص ۱۲۹-۱۴۷.
- پور قهرمانی، بابک (۱۳۹۳) بررسی حقوق کلاهبرداری رایانه ای با رویکردی به فقه، کنگره بین المللی فرهنگ و اندیشه دینی.
- جلالی فراهانی، امیر حسین (۱۳۸۳) پیشگیری از جرایم رایانه ای، نشریه حقوقی دادگستری، دوره ۶۸، شماره ۴۷، صص ۸۷-۱۱۹.
- حبیب زاده، محمد جعفر (۱۳۷۵) کلاهبرداری در حقوق تطبیقی. مجله حقوقی دادگستری، دوره ۶۰، شماره ۱۷ و ۱۸، صص ۲۵-۴۴.
- حبیب زاده، محمد جعفر (۱۳۷۷) مروری بر جرم کلاهبرداری در حقوق ایران. مجله دادرسی. شماره ۸، صص ۲۴-۲۸.
- خرم‌آبادی، عبدالصمد (۱۳۸۴) تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای. مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات؛ معاونت حقوقی و توسعه قضایی. تهران: انتشارات سلسبیل.
- ساجدی، حسین، رضوی فرد، بهزاد، و قاسمی، ناصر. (۱۴۰۰). تحلیل جرایم جعل ثبتي و کلاهبرداری ثبتي در فضای مجازی. کارآگاه، دوره ۱۵، شماره ۵۵، صص ۶۱-۸۰.
- طارمی، محمد حسن (۱۳۸۶) گذری بر جرایم رایانه ای، مجله ره آورد نور، شماره ۲۱، صص ۱۲-۲۱.
- عبدالله پور، اکرم؛ یحیی پور، حسن (۱۳۹۲) جرم کلاهبرداری و عناصر تشکیل دهنده‌ی آن در حقوق ایران. شماره ۱۰۰، صص ۲۵-۲۷.
- عمید، حسن (۱۳۷۵) فرهنگ عمید. چاپ ششم. تهران، انتشارات جاویدان.
- فتحی، حجت اله. (۱۴۰۱). عدم توازن مجازات جرایم سایبری با برخی از مجازات های جرایم سنتی همجنس. مطالعات حقوقی فضای مجازی، دوره ۱، شماره ۱، صص ۱-۱۵.
- قناد، فاطمه (۱۳۸۷) کلاهبرداری الکترونیکی در بستر فناوری‌های اطلاعات و ارتباطات. مجله پژوهش و سیاست، شماره ۲۵، صص ۱۲۵-۱۵۴.
- گرابلی، محمدباقر. (۱۳۸۹). بررسی جعل و تخریب و اخلال رایانه‌ای. آموزه های حقوق کیفری، دوره ۷، شماره ۱۴، صص ۱۵۹-۱۸۸.
- میر محمد صادقی، حسین (۱۳۸۹)، جرائم علیه اموال و مالکیت، تهران: نشر میزان.
- نجفی توانا، علی، و کریمی، فاطمه. (۱۳۹۹). سیاست پیش گیری و مبارزه با جرم کلاهبرداری اینترنتی. قانون یار، دوره ۴، شماره ۱۶، صص ۴۱۹-۴۴۶.
- یاراحمدی، حسین، و براتی بارویی، محبوبه. (۱۴۰۱). نقد و بررسی جرم کلاهبرداری رایانه ای و راهکارهای مقابله با آن. قانون یار، دوره ۶، شماره ۲۴، صص ۶۴۹-۶۶۸.



## Iran's criminal policy towards fraud in cyberspace with a criminalization approach

### Abstract

Fraud is one of the crimes that has both an economic aspect and is related to the spiritual dimensions of the human personality, and for this reason it may include a wide range. That is why the legislator has specifically established the law in determining the punishment for this crime, and the law of aggravation has imposed the penalty of fraud in this regard. The present study, which aims to examine the punishment of fraud in jurisprudence and subject law with a library study method and descriptive-analytical method, in response to the question that what is the punishment for traditional and computer fraud in Iranian jurisprudence and subject law? Citing reliable jurisprudential and legal sources, it has been concluded that three degrees of punishment for fraud have been determined in the Law of Intensification, which includes simple, aggravated fraud, and fraud as a corruption of the earth, which, according to the new Islamic Penal Code, is death. In Islamic jurisprudence, fraud is used with terms such as fraud, and principles such as the prohibition of misappropriation of property, respect for Muslim property, the rule of harm, tadbis, fainting in a transaction, etc. justify the criminalization of fraud. Any fraud and taking other people's property is subject to punishment and crime, and it doesn't matter if the tool is traditional or like new technologies, including computers, etc. Fraud should be punishable in the category of crimes, because placing this crime in the category of limits requires stronger documents and traditions that are not available. Keywords: Fraud. Cyber financial crimes. Punishment Criminal policy.

**Keywords:** Cybercrime, global jurisdiction. International cooperation, information security.