



امکان‌سنجی استناد به تئوری تعدیل در حقوق ایران به عنوان راهکاری در تعذر قراردادی - روش‌نعلی شکاری، سید مصطفی میلانی  
حمایت کیفری از حقوق نسل‌های آینده در اسناد بین‌المللی - عادل ساریخانی، مصطفی کرمی پور  
تحلیل حق نظارت مردم بر حکومت از دیدگاه علی (علیه السلام) با نگاهی به قانون اساسی جمهوری اسلامی ایران - ابراهیم موسی زاده،  
محمد صالحی

تاملاتی در تشریح قسامه با توجه به علوم جرم‌یابی - محمدعلی حاجی ده‌آبادی، روح‌الله شمشیری  
بازخوانش تعاملات (برخی گروه‌های مذهبی و بازیگران نظام بین‌الملل) حوزه تروریسم به عنوان وسیله دستیابی به منافع ملی با  
تاکید بر مسئولیت‌های حقوقی در کشورهای اسلامی - سید محمدرضا موسوی فرد، حمیدرضا نوروزیان، عارفه کردی نسب،  
نفیسه طوسی، آیدا قاسم زاده

اصل منع اعاده پناهندگان از منظر اسناد حقوق بشری با تاکید بر پناه‌جویان زیست محیطی - مهناز خرسندی، عسکر جلالیان  
خطرات اولویت یافتن مسائل مادی در مشاغل حقوقی - محمد ستایش‌پور، مریم فرجی ترک  
احکام و آثار اذن در نظام حقوقی ایران و فرانسه - حسن نجارها  
مقایسه رکن مادی جرم کلاهبرداری رایانه‌ای با سنتی - علی پایدارفرد، جواد نادری عوج بغزی، احمدرضا امتحانی  
مبانی نظری حاکم بر کنترل تسلیحات نظامی با تاکید بر مواضع متعارض سازمان ملل متحد و سازمان تجارت جهانی در خصوص تجارت  
تسلیحات نظامی متعارف - پوریا ابراهیم زاده، سمیه رحمانیان

کودک و کودکی از منظر فلسفه و ادبیات - مریم شعبان  
اعتبار امر مختوم در دعاوی مدنی و کیفری - امیر محمدی، محمدمهدی حیدری، سهیلا مرادی قلعه  
جایگاه شعب تخصصی کوزوو در نظام عدالت کیفری جهانی - مصطفی فضائلی، آرش ملک  
جرم‌انگاری اظهار خلاف واقع مطلع در حقوق ایران - سعید اسدزاده، فاطمه احدی، مجتبی کنجوری  
اقدامات شرکت‌های خارجی بابت استفاده عراق از تسلیحات شیمیایی در دفاع مقدس از منظر حقوق مسئولیت بین‌المللی -  
محمد ستایش‌پور، پریشان شفانی

مروری جامعه‌شناختی و جرم‌شناختی نسبت به پدیده روسپیگری در نظام بین‌الملل و ایران با تاکید بر آموزه‌های جرم‌شناسی  
اسلامی - سید محمدرضا موسوی فرد، اسد اخضری فرد، علی مردان احمدی  
تعامل پلیس با نهادهای پیشگیری از جرم - مینا مومنی، سید مهدی احمدی موسوی  
حقوق کودکان مهاجر در اسناد ملی و بین‌المللی - رضا خواجه نورالدینی، سیده پریسا میرابی  
صلاحیت واقعی قوانین کیفری از منظر حقوق اسلام - مصطفی کرمی پور، مونا رجب زاده باغی  
بررسی تغییر از جرائم خیابانی به جرائم سایبری در آغاز همه‌گیری کووید-۱۹ - رویکردی به نظریه فعالیت‌های روزانه - مریم کمائی  
جایگاه مأمورین امنیتی انگلستان در کشف جرایم - زهرا وهبی، آرش رزمی

استقلال قضات در نظام حقوقی جمهوری اسلامی ایران در پرتو آموزه‌های دین‌مبین اسلام - محمد ستایش‌پور، فاطمه زهرا آسیان  
شرایط قانونی و ابعاد حقوقی و کیفری مالکیت فکری در نظام حقوقی جمهوری اسلامی ایران - سمیه زیلابی، صادق فتیلی، ابراهیم مقدم  
امکان‌سنجی تحقق ایده جرم‌انگاری (جرم مسئولیت مدنی مدیران) از تئوری تا عمل بر اساس رویکردهای مدل مسئولیت کیفری  
قانون اقدام راهبردی لغو تحریم‌ها - سید محمدرضا موسوی فرد، حمیدرضا نوروزیان، نفیسه دهرویه، محمدرسول انصاری نیا،  
ندا حقیقی

ارزیابی فقهی-حقوقی تعدد واقعی در حدود، قصاص و دیات - علی محمدی جورکویه، احمدرضا امتحانی، جواد نادری عوج بغزی  
جایگاه و نقش مردم در استقرار و استمرار نظام امت و امامت در پرتو آراء شهید بهشتی - محمدصادق داریوند  
میانجیگیری، نظام عدالت مشارکتی، نسل سوم نظام عدالت کیفری و حقوق اطراف دعوا - صادق فتیلی، محمد فتیلی، ابراهیم مقدم



## Comparison of the Actus Reu of the Crime of Computer Fraud with Traditional

## مقایسه رکن مادی جرم کلاهبرداری رایانه‌ای با سنتی

Ali Paidarfard

Master of Criminal Law and Criminology, Mofid University of Qom, Qom, Iran

Javad Naderi ooj Boghzi

Student outside Qom seminary, PhD student in Criminal Law and Criminology, University of Tehran, Aras International Campus, Aras, Iran (Corresponding Author)

Ahmadreza Emtehani

Master of Criminal Law and Criminology, Mofid University of Qom, Qom, Iran

علی پایدارفرد

کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه مفید قم، قم، ایران  
alipaidar.f1375@gmail.com  
http://orcid.org/0000-0002-7848-9315

جواد نادری عوج بغزی

طلبه دروس خارج حوزه علمیه قم، دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشگاه تهران، پردیس بین‌المللی ارس، ارس، ایران (نویسنده مسئول)  
njavad71@gmail.com  
http://orcid.org/0000-0002-7440-8012

احمدرضا امتحانی

کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه مفید قم، قم، ایران  
emtehaniahmadreza@gmail.com  
http://orcid.org/0000-0002-0253-0342

### Abstract



Computer and traditional fraud is one of the most common crimes in society. Despite the similarities in the names, the two have differences and similarities. Of course, this computer crime has other similarities and differences with the same crime in the traditional form (such as evidence and jurisdiction of courts); But in this article, as the title, only the similarities and differences of those crimes in terms of the actus reus have been explained. The main question of the research is what are the most important results that can be obtained from comparing these two crimes and examining the challenges between them? In the crime of computer fraud, unlike traditional fraud, taking advantage of one's credulity and deception of the victim is not a condition for the realization of the crime. Also, in terms of result, the perpetrator's profit and harm to another is the similarity of these two crimes, but taking property in computer fraud (unlike traditional) is not part of the result in its actus reus, but part of the exclusive behavior in the second part of the physical behavior of this crime and subject It is a crime. The research method of this research is library and resources related to this subject have been used.

**Keywords:** Actus Reus, Computer Fraud, Traditional Fraud.

### چکیده

کلاهبرداری رایانه‌ای و سنتی از جرایم مبتلی به در جامعه است. علیرغم شباهت در اسم، این دو دارای وجوه تفاوت و شباهت‌هایی هستند. البته این جرم رایانه‌ای، تشابه و تفاوت‌های دیگری نیز با همان جرم به شکل سنتی دارد (مثل ادله اثبات و صلاحیت محاکم)؛ اما در این مقاله، همان‌طور که از عنوان آن پیدا است؛ تنها به تبیین شباهت و تفاوت‌های آن جرایم، از حیث رکن مادی پرداخته شده است. سؤال اصلی پژوهش آن است که مهم‌ترین نتایجی که از مقایسه این دو بزه و بررسی چالش‌های میان آن‌ها به دست می‌آید، چیست؟ در جرم کلاهبرداری رایانه‌ای برخلاف کلاهبرداری سنتی، اغفال و فریب بزه‌دیده 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 رایانه‌ای (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. روش تحقیق این پژوهش، کتابخانه‌ای است و از منابع مرتبط با این موضوع، استفاده شده است.

**واژه‌گان کلیدی:** رکن مادی، کلاهبرداری رایانه‌ای، کلاهبرداری سنتی.

<p>ارجاع:                  پایدارفرد، علی؛ نادری عوج بغزی، جواد؛ امتحانی، احمدرضا؛ (۱۴۰۱)، مقایسه رکن مادی جرم کلاهبرداری رایانه‌ای با سنتی، تمدن حقوقی، شماره ۱۲.</p>
<p>Copyrights:                  Copyright for this article is retained by the author (s) , with publication rights granted to Legal Civilization. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<a href="http://creativecommons.org/licenses/by/4.0">http://creativecommons.org/licenses/by/4.0</a>) , which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.</p>



#### مقدمه

در این پژوهش، در خصوص هریک از جرایم کلاهبرداری رایانه‌ای و سنتی، ابتدا، به تمامی شرایط و رفتارهای فیزیکی که جهت شکل‌گیری آن‌ها ضروری هستند، پرداخته و در نهایت، نتیجه حاصله هریک از آن‌ها را تبیین خواهیم کرد. تعریف کلی هریک از جرایم فوق، قبل از تشریح رفتارهای فیزیکی لازم آن جرم، ضروری است؛ در نتیجه، ابتدا به تعریف آن‌ها پرداخته و سپس وارد عنصر مادی جرایم مذکور می‌شویم و رفتارهای فیزیکی لازم آن جرایم را تبیین می‌کنیم. نحوه ارتکاب این جرایم اعم از فعل یا ترک فعل، داخل رفتارهای فیزیکی لازم جرایم مذکور اشاره خواهد شد. در خصوص رفتارهای فیزیکی لازم در جرم کلاهبرداری رایانه‌ای، ابتدا به مصادیقی که قانون‌گذار در ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به صورت تمثیلی ذکر کرده، اشاره می‌کنیم و سپس به تعریف عبارت «تحصیل غیرمجاز» و موضوع این جرم، یعنی، وجه یا مال یا منفعت یا خدمت یا امتیازات مالی می‌پردازیم.

در واقع، علیرغم شباهت در ظاهر این دو جرم، با یکدیگر دارای تفاوت و شباهت‌هایی هستند که این مقاله به شکلی ویژه به مقایسه آن‌ها و تحلیل چالش و زوایای پنهان آن‌ها پرداخته است. البته همان‌طور که بیان گشت، کلاهبرداری رایانه‌ای، تشابه و تفاوت‌های دیگری نیز با همان جرم به شکل سنتی مانند ادله اثبات و صلاحیت محاکم دارد؛ اما در این مقاله، همان‌طور که از موضوع آن پیدا است؛ تنها به تبیین شباهت و تفاوت‌های آن جرایم، از حیث رکن مادی پرداخته شده است. در رفتار فیزیکی بزه کلاهبرداری

رایانه‌ای برخلاف کلاهبرداری سنتی، اغفال و فریب بزه‌دیده شرط تحقق جرم نبوده و از حیث نتیجه، انتفاع مرتکب و ضرر به دیگری وجوه تشابه این دو بزه است. اما بردن مال در کلاهبرداری رایانه‌ای (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. از اهمیت این موضوع می‌توان به نوع جرم و بستر خاص آن (مجازی) اشاره کرد که اصولاً بستری مناسب در جهت بزه‌دیده شدن افراد خصوصاً وفق نظریه‌های سبک زندگی و فعالیت‌های روزمره در جرم‌شناسی می‌باشد (بشیری و پایدارفرد، ۱۴۰۰، ۷۹). شیوه تحقیق این مقاله، کتابخانه‌ای است و از منابع مرتبط با این موضوع، استفاده شده است.

## ۱- کلاهبرداری رایانه‌ای

کلاهبرداری، به دو دسته کلی تقسیم‌بندی می‌شود؛ یکی کلاهبرداری سنتی که در ماده یک<sup>۱</sup> قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷، جرم‌انگاری شده است و دیگری کلاهبرداری رایانه‌ای است که این بزه را می‌توان به دو دسته، تقسیم‌بندی کرد: الف- در فضای مبادلات الکترونیکی رخ دهد: ماده «۶۷»<sup>۲</sup> قانون تجارت الکترونیکی مصوب ۱۳۸۲ در خصوص «کلاهبرداری

۱- ماده ۱: هر کس از راه حیل و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌های یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیش آمدهای غیرواقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر وجوه و یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصاحساب 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 هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود. در صورتی که شخص مرتکب برخلاف واقع عنوان یا سمت ماموریت 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 سه‌گانه و همچنین نیروهای مسلح و نهادها و مؤسسات مامور به خدمت عمومی اتخاذ کرده یا این که جرم با استفاده از تبلیغ عامه از طریق وسائل 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 به خدمت عمومی باشد علاوه بر رد اصل مال به صاحبش به حبس از دو تا ده سال و انفصال ابد از خدمت دولتی و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود.

۲- ماده ۶۷: 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 بفریبید و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری



کامپیوتری». ب- در فضای مبادلات الکترونیکی رخ ندهد: ماده «۱۳»<sup>۳</sup> قانون جرایم رایانه‌ای مصوب ۱۳۸۸ (عابدی، ۱۳۹۸، ۸۷-۸۸).

در ادامه، به رفتارهای فیزیکی لازم، جهت تشکیل بزه کلاهبرداری رایانه‌ای عام (نه خاص)، یعنی موضوع ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ (نه ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲) و شرایط لازم جهت تحقق این بزه به‌عنوان بخش‌های اصلی از عنصر مادی آن، خواهیم پرداخت؛ زیرا در حال حاضر، مقصود عام مقنن و حقوقدانان از «کلاهبرداری رایانه‌ای»، موضوع ماده ۱۳ (نه ماده ۶۷) است و منظور اصلی نگارندگان نوشتار حاضر نیز، از کلاهبرداری رایانه‌ای، موضوع ماده ۱۳ قانون مذکور است و تشریح ماده ۶۷ قانون تجارت الکترونیکی، نیازمند بررسی تخصصی و مجزا است، هرچند، در ادامه این نوشتار، جهت تبیین و شناخت بهتر مطالب و نتیجه‌گیری صحیح، وجوه تشابه و تفاوت مهم این دو با یکدیگر و با جرم کلاهبرداری سنتی، اشاره خواهد شد.

#### ۱-۱- رفتارهای فیزیکی لازم در کلاهبرداری رایانه‌ای

به نحو کلی، رفتارهای فیزیکی لازم، جهت شکل‌گیری کلاهبرداری رایانه‌ای، در دو قسمت، قابل بررسی است. نخست، رفتارهای تمثیلی موضوع ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است که تنها به صورت فعل مثبت، قابل تحقق می‌باشد و دوم، تحصیل غیرمجاز موضوع این جرم است که محصور در وجه یا مال یا منفعت یا خدمت یا امتیازات مالی می‌باشد؛ با عنایت به عبارت «تحصیل غیرمجاز» به این نتیجه می‌رسیم که این بخش از رفتار نیز، همچون بخش نخست، تنها به شکل، فعل مثبت (نه ترک فعل)، رخ می‌دهد. در این قسمت، این دو مورد را که مجموعاً رفتارهای فیزیکی لازم این جرم را تشکیل می‌دهد، بررسی می‌کنیم؛ ابتدا، رفتارهای وابسته به داده یا سامانه، یعنی، موارد تمثیلی را که قانون‌گذار، نام برده را تبیین و سپس به صورت مجزا، به تعریف تحصیل غیرمجاز و موضوع جرم یعنی، وجه، مال، منفعت

وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را برود، مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مآخوذه محکوم می‌شود.

۳- ماده ۱۳: هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

و خدمت یا امتیاز مالی می‌پردازیم.

#### ۱-۱-۱- هرگونه رفتار وابسته به داده یا سامانه

قانون‌گذار، در ماده ۱۳ قانون جرایم رایانه‌ای، درخصوص رفتار فیزیکی جرم کلاهبرداری رایانه‌ای، از عبارت «از قبیل»، استفاده کرده است که نشان‌دهنده تمثیلی بودن این موارد است. همان‌طور که اشاره شد، این نوع رفتار از سوی مرتکب تنها به صورت فعل مثبت است، زیرا، قانون‌گذار از عبارت «ارتکاب اعمالی» برای موارد تمثیلی استفاده کرده است و همچنین، تمام موارد تمثیلی که ذکر کرده، تنها به شکل فعل مثبت، قابل تحقق است؛ در نتیجه، بایستی تنها رفتارهای مرتبط و مشابهی که با فعل مثبت قابل تحقق است را مشمول این ماده دانست (نه رفتارهای مشابه و مرتبط به نحو ترک فعل؛ که به نظر، تحقق عملی این نوع رفتارها دور از ذهن است).

حال، به تعریف هریک از این موارد تمثیلی می‌پردازیم؛ «وارد کردن» داده‌ها در این‌جا، به دو شکل قابل تحقق است؛ یکی وارد کردن داده‌های غیرصحیح و غیرمجاز و دیگری وارد کردن غیرمجاز داده‌های صحیح؛ که می‌تواند از طریق صفحه کلید رایانه‌ها رخ دهد (بابایی، ۱۳۹۷، ۱۳۷). چون در ماده فوق، قبل از این رفتارهای تمثیلی، عبارت «غیرمجاز» ذکر شده است، بنابراین، کلاهبرداری رایانه‌ای از دو راه فوق، قابل ارتکاب است؛ هک کردن و سپس برداشت وجه دیگران، مشمول وارد کردن داده غیرمجاز است ولی منظور از وارد کردن غیرمجاز داده، این است که خود داده مجاز است اما وارد کردن آن به نحو غیرمجاز و بدون اجازه یا مجوز قانونی رخ می‌دهد؛ مثلاً، زمانی که شخصی کارت بانکی خود را که رمز اول آن را رویش نوشته است، گم کند و فردی دیگر آن را بیابد و از طریق دستگاه خودپرداز بانک<sup>۴</sup>، وجوه حساب فرد را برداشت کند، رمز اول کارت بانکی فرد که توسط سیستم آن بانک، مورد تأیید بوده، داده صحیح محسوب می‌گردد و چون رفتار یابنده (وارد کردن آن رمز)، غیرمجاز است، رفتار وی تحت عنوان کلاهبرداری رایانه‌ای قابل پیگیری کیفری است و نظریه مشورتی نیز تقویت‌کننده این استدلال است؛ در این نظریه، وارد کردن داده‌ها به هر نحوی که منجر به موضوع این جرم گردد را مشمول کلاهبرداری رایانه‌ای دانسته است؛ البته برخی از حقوقدانان، این موارد را با عنایت به سپرده‌شدن یا نشدن، مشمول جرایم عادی می‌دانند. حتی اگر صاحب کارت بانکی، کارت و اطلاعات ورودی آن را جهت گرفتن موجودی به دیگری بدهد و فرد، وجهی از آن حساب را برای خود بردارد، مشمول این ماده است؛

زیرا، هرچند با اجازه صاحب کارت و به طور مجاز وارد کردن داده صورت گرفته اما برای شروع به وارد کردن داده که در نهایت آن منجر به دریافت وجه به نفع خود شود، اجازه نداشته و مشمول کلاهبرداری رایانه‌ای می‌شود (بابایی، ۱۳۹۷، ۱۳۷-۱۳۹).

مثال‌های فراوانی، در خصوص این دو مورد می‌توان ذکر کرد؛ از موارد مبتلابه می‌توان به هک کردن جهت یافتن اطلاعات کارت بانکی افراد، با گذاشتن لینک جعلی جهت خریدهای اینترنتی اشاره کرد؛ با این توضیح که ممکن است برخی از افراد با ارائه پایگاه‌های اینترنتی جعلی و مشابه با سایت‌های اصلی آن، با تبلیغ لینک سایت‌های جعلی خود از طریق پیامک، پیام‌رسان و یا شبکه‌های اجتماعی به کاربران، اطلاعات کارت بانکی افراد را به طور غیرمجاز دریافت کنند و سپس از حساب بانکی آن‌ها، وجوهی دریافت کنند. بی‌توجهی به مسئله فوق، می‌تواند، سبب این شود که سودجویان، به طور غیرمجاز، از حساب بانکی افراد وجوهی دریافت کنند؛ یا حتی، اگر یک فروشگاه اینترنتی، به طور مجاز اطلاعات بانکی افراد را دریافت کند و سپس از حساب آن‌ها، وجهی برداشت کند، چون این برداشت، وارد کردن غیرمجاز داده است؛ کلاهبرداری رایانه‌ای تحقق یافته است.

«تغییر داده» نیز از مواردی است که ممکن است فرد را در شرایطی کلاهبردار رایانه‌ای بدانیم؛ به این صورت که فرد اگر داده‌ای را تغییر دهد و این تغییر داده او، سبب یکی از موارد پنج‌گانه ماده ۱۳ قانون جرایم رایانه‌ای، یعنی، تحصیل مال، منفعت، امتیاز و خدمات مالی شود، کلاهبرداری رایانه‌ای تحقق یافته است؛ مثلاً، اگر فردی، در سامانه نمرات دانشجویی دانشگاه خود، نمره خود را تغییر دهد (افزایش دهد) تا رتبه سوم را کسب کند و از این طریق، مبلغی را از دانشگاه، به‌عنوان جایزه دریافت کند، مرتکب بزه کلاهبرداری رایانه‌ای شده است.

منظور از «محو داده»، پاک کردن، حذف و از بین بردن داده می‌باشد؛ به طور مثال، همان فرد در مثال فوق، دروسی را که نمرات پایینی داشته است را به همراه ضریب آن‌ها از سایت حذف کند تا از این طریق، خود را جزء دانشجویان برتر به جهت دریافت مبلغی از دانشگاه، به‌عنوان جایزه، معرفی کند.

عمل اضافه کردن به داده‌های ورودی و یا افزایش مقادیر ورودی را اصطلاحاً «ایجاد داده» می‌گویند (ترکی، ۱۳۸۹، ۳۴). ایجاد وقفه پردازش جزئی یا کلی داده از هر طریقی به منظور دستیابی به موارد پنج‌گانه محصور در ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ را «متوقف کردن داده» می‌گویند. خارج کردن تمام یا قسمتی از سیستم یا سامانه از برنامه و نظم همیشگی خود به جهت رسیدن به موارد

پنج‌گانه مزبور را «مختل کردن سامانه»، می‌نامند؛ مثلاً فردی، با اختلال در سامانه ثبت تخلفات راهنمایی و رانندگی، سبب حذف پیشینه تخلفات رانندگی خود گردد (صنعتی و عطایی جنتی، ۱۳۹۷، ۸۱).

#### ۲-۱-۱- تحصیل غیرمجاز موضوع جرم

در این بخش، در خصوص قسمت دوم از ماده ۱۳ قانون جرایم رایانه‌ای، سخن خواهیم گفت و بیان خواهیم کرد که منظور از تحصیل غیرمجاز موارد پنج‌گانه محصور در این ماده، یعنی، وجه، مال، منفعت، خدمت و امتیازات مالی چه خواهند بود.

#### ۲-۱-۲-۱- تعریف تحصیل غیرمجاز

به طور کلی، منظور از تحصیل در این ماده، یعنی هرگونه کسب کردن و به دست آوردن و منظور از غیرمجاز، هر چیز بدون جواز از صاحب اصلی آن، می‌باشد. در نتیجه، در خصوص عبارت «تحصیل غیرمجاز» می‌توانیم بگوییم که هر نوع امری که سبب کسب غیرمجاز به چیزی گردد، تحصیل غیرمجاز است که در این ماده، مواردی که لزوماً بایستی به نحو غیرمجاز کسب گردند، به طور محصور بیان شده‌اند؛ در ادامه به تعریف هر یک از آن‌ها خواهیم پرداخت؛ بنابراین، بدون رسیدن به هر یک از این موارد، بزه تام کلاهبرداری رایانه‌ای تحقق نیافته است و نهایتاً مرتکب، مشمول عناوین مجرمانه شروع به کلاهبرداری رایانه‌ای یا دیگر جرایم مرتبط خواهد بود؛ که این امر، حاکی از آن است که بزه کلاهبرداری به صورت رایانه‌ای هم مانند کلاهبرداری سنتی، مقید به نتیجه است.

#### ۲-۱-۲-۲- تعریف وجه، مال، منفعت، خدمت و امتیازات مالی

در این قسمت، هر یک از عبارات وجه، مال، منفعت، خدمت و امتیازات مالی را تشریح می‌کنیم. همان‌طور که اشاره شد، بدون دستیابی مرتکب به این پنج مورد محصور و سپس وارد کردن ضرر به دیگری (به عنوان نتیجه جرم)، بزه تام کلاهبرداری رایانه‌ای قابل تحقق نخواهد بود.

وجه و مال تا حدودی با یکدیگر هم‌پوشانی دارند اما در حقیقت، متفاوت هستند؛ به نوعی، رابطه منطقی این دو عموم و خصوص مطلق است؛ با در نظر گرفتن ملاک عرف، می‌توان بیان داشت که منظور از وجه، پول ملی رایج یا ارزهای خارجی رایج در کشور هستند؛ همچنین، میزان موجودی در حساب‌های بانکی که نشان‌دهنده پول نقد است؛ عرفاً وجه نامیده می‌شود؛ زیرا، اصولاً، قابلیت تبدیل به پول نقد را دارد؛ اما منظور از مال، هر شیء مادی یا معنوی است که از نظر عرف، ارزشمند است و قابلیت



قیمت‌گذاری دارد؛ مثل اتومبیل یا خانه که از نظر عرف ارزشمند هستند. بنابراین، مال اعم از وجه است. منفعت، از ریشه «نفع» گرفته شده است؛ یعنی هر آنچه که سبب کسب سود گردد را، منفعت می‌نامیم. منفعت، امری تبعی نسبت به مال است که در صورت وجود مال قابل تحقق است اما در عین حال، آن را نیز، می‌توان مال دانست. در این جا، منظور مقنن، به نظر می‌رسد مواردی نظیر تسهیلات بانکی است. منظور از امتیازات مالی هم می‌تواند، امتیازات یا حقوقی باشد که نتیجه آن مال است؛ مثلاً فردی با تغییر داده‌های مربوط در سایت مرتبط، مجوز ساخت خانه با طبقات زیاد را دریافت کند (بابایی، ۱۳۹۷، ۱۴۲).

## ۱-۲- شرایط لازم جهت تحقق کلاهبرداری رایانه‌ای

در کنار رفتارهای فیزیکی لازم، تحقق این جرم، نیازمند وجود شرایطی نیز می‌باشد که به آن اشاره خواهد شد.

### ۱-۲-۱- متعلق بودن اموال به دیگری

شرط نخست تحقق این جرم، این است که این اموال حاصل از جرم، متعلق به دیگری باشد؛ بنابراین، اگر این اموال، برای خود مرتکب باشد، کلاهبرداری چه به نحو سنتی و چه به صورت رایانه‌ای رخ نداده است؛ ممکن است ایراد شود که در ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ و ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷، صراحتاً این شرط، ذکر شده است و مقنن، عامداً در ماده ۱۳ قانون جرایم رایانه‌ای، آن را ذکر نکرده است و در نتیجه این شرط در خصوص کلاهبرداری رایانه‌ای الزامی نیست؛ این نظر قابل پذیرش نیست؛ زیرا، بدیهی است که اگر شخصی رفتار و شرایط فیزیکی لازم برای کلاهبرداری از اموال و داده‌های خویش را حتی داشته باشد؛ به‌هیچ‌وجه رسیدن به نتیجه حاصله در خصوص اموال وی قابل تصور نیست؛ زیرا، وی بابدن مال خویش، نه نفعی برده و نه به کسی ضرر وارد کرده است.

### ۱-۲-۲- نیازمندی مستقیم به داده و سامانه‌های رایانه‌ای در زمان ارتکاب

شرط دوم و مهمی که می‌توان به آن اشاره کرد، این است که تمامی اموال موضوع این بزه، در هنگام ارتکاب، احتیاج مستقیمی به داده‌ها و سامانه‌های رایانه‌ای دارند؛ در حقیقت، در کلاهبرداری رایانه‌ای، هم بایستی رفتارهای تمثیلی ماده مذکور (وارد کردن و...) و هم ضرر (نتیجه) پس از موارد پنج‌گانه (وجه، مال و...) از طریق سیستم‌های رایانه یا مخابراتی و بی‌واسطه (بدون عامل بیرونی) رخ دهد تا این جرم محقق گردد؛ بنابراین، اگر فردی تبلیغات واهی و متقلبانه‌ای در فضای مجازی داشته باشد و از این راه، شخصی را

اغفال کند و آن شخص یا به شماره حساب او و یا در فضای حقیقی به او وجهی دهد، نهایتاً با جمع سایر شرایط، بزه کلاهبرداری سنتی (نه رایانه‌ای) قابل تحقق است. همچنین، ملموس بودن یا نبودن مال تأثیری در عدم تحقق این بزه ندارد؛ یعنی، چه وجه به صورت نقدی و ملموس باشد و چه در حساب شخص به صورت داده‌های رایانه‌ای باشد (غیرملموس) امکان تحقق کلاهبرداری رایانه‌ای وجود دارد (بابایی، ۱۳۹۷، ۱۴۲-۱۴۳).

### ۳-۱- نتیجه حاصله و شروع به جرم در کلاهبرداری رایانه‌ای

بزه کلاهبرداری رایانه‌ای همچون کلاهبرداری سنتی جرمی مقید به نتیجه است؛ در این قسمت، لازم است نتیجه حاصله این بزه به همراه شروع به جرم، تبیین گردد.

#### ۱-۳-۱- نتیجه حاصله

همان‌طور که اشاره شد، جرم کلاهبرداری رایانه‌ای، تنها در صورتی به شکل کامل محقق می‌شود که منجر به نتیجه گردد؛ این نتیجه در ماده ۱۳ قانون جرایم رایانه‌ای، مستتر است؛ پس از موارد محصور به‌عنوان آخرین رفتار فیزیکی، یعنی وجه یا مال یا منفعت یا خدمات یا امتیازات مالی، نتیجه این بزه را بایستی ضرری که به دیگری وارد می‌شود، بدانیم (بابایی، ۱۳۹۷، ۱۴۵-۱۴۴)؛ همچنین، شخص بایستی از این رفتار منتفع گردد که آن هم جزو نتیجه است. به طور خلاصه، نتیجه حاصله در این بزه، ورود ضرر به بزه‌دیده (نه قابلیت تحقق ضرر) و انتفاع مالی خود شخص مرتکب و یا شخص مورد نظر او است.

در خصوص انتفاع شخص، لازم به ذکر است که در صورتی که مثلاً وی به سیستم‌های مرتبط در بانک به نحوی، ورود پیدا کند و با اعمال تمثیلی موجود در ماده ۱۳ قانون جرایم رایانه‌ای، نظیر اختلال در داده، با اشتباه سبب آن شود که وجه اعتباری که وی می‌خواسته، به حساب نفر دیگری غیر از خودش یا دیگری (که قصد واریز وجه به حساب وی را داشته است)، واریز نماید یا واریز گردد، بزه فوق محقق نشده است (عالی‌پور، ۱۳۹۵، ۲۸۳). البته در این جا، اگر وی سبب بزه اختلال در سیستم‌های رایانه‌ای گردد؛ تحت آن عنوان، مورد تعقیب و کیفر قرار می‌گیرد.

همان‌طور که در شرط نخست تحقق این بزه در گذشته اشاره شد، تعلق مال به دیگری در کلاهبرداری رایانه‌ای نیز الزامی است؛ نتیجه پذیرش این شرط، پذیرش دو شرط دیگر، یعنی ورود ضرر به دیگری (بزه‌دیده) و انتفاع مالی خود شخص مرتکب و شخص مورد نظر او است؛ در حقیقت، بردن مال دیگری

مستلزم شکل‌گیری این دو شرط است (میرمحمدصادقی، ۱۳۹۴، ۹۵). در این جرم، برخلاف برخی جرایم دیگر مثل جعل سنتی، ورود ضرر به دیگری (بزه‌دیده) و نه صرفاً قابل تحقق بودن ضرر، شرط است. بزه‌دیده خاص یا عام باشد و یا شخص حقیقی و یا حقوقی باشد، تأثیری در عدم تحقق این جرم ندارد. انتفاع از اموال حاصل از جرم برای خود مرتکب این بزه یا سایر افرادی که مدنظر او هستند شرط است؛ بنابراین، اگر بر اثر هر نوع اشتباهی، اموال حاصله، به نفع مرتکب و یا افرادی که مدنظر او بوده‌اند، نرسد، بزه کلاهبرداری رایانه‌ای رخ نداده است. بنابراین، در بزه کلاهبرداری رایانه‌ای، یک‌سری رفتارهای فیزیکی تمثیلی مانند ایجاد کردن، تغییر دادن، وارد کردن و... وجود دارد که لزوماً رفتار ابتدایی این جرم را تشکیل می‌دهد و یک‌سری رفتار ثانویه دارد که محصور در پنج مورد فوق است؛ نتیجه حاصله، پس از رفتارهای فیزیکی تشکیل‌دهنده این بزه است که ماده به آن تصریح نکرده است اما در آن مستتر است و آن ضرر به دیگری و انتفاع مرتکب است.

### ۲-۳-۱- شروع به جرم

جرم ناقص در برابر جرم تام قرار دارد؛ در قسمت‌های پیشین، در خصوص بزه تام کلاهبرداری رایانه‌ای سخن گفته شد؛ در این بخش، در خصوص شروع به جرم به‌عنوان یکی از موارد جرم ناقص سخن خواهیم گفت؛ زیرا شروع به جرم بزه فوق، دارای مجازات است و نیازمند بررسی مجزا است. شروع به جرم یعنی این‌که مرتکب داخل قلمرو اجرایی بزه گردد و بنابر احوالی منصرف از خواست و اراده مرتکب، اتمام بزه به حالت تعلیق درآمده و نتیجه آن جرم محقق نمی‌گردد (الهام و برهانی، ۱۳۹۷، ج ۱، ۲۴۵). با عنایت به قانون کاهش مجازات حبس تعزیری مصوب ۱۳۹۹، شروع به جرم و معاونت در بزه کلاهبرداری غیررایانه‌ای، موضوع ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷، نسخ صریح و تابع قواعد عام شد (مصدق، ۱۳۹۹، ۵۸). بنابراین، در حال حاضر، شروع به جرم تمامی جرایم کلاهبرداری اعم از سنتی (ماده یک قانون فوق) و رایانه‌ای (ماده ۱۳ قانون جرایم رایانه‌ای)، ذیل بند «پ» ماده «۱۲۲»<sup>۵</sup> قانون مجازات اسلامی مصوب ۱۳۹۲، قرار می‌گیرد.

۵- ماده ۱۲۲: هر کس قصد ارتکاب جرمی کرده و شروع به اجرای آن نماید، لکن به واسطه عامل خارج از اراده او قصدش معلق بماند، به شرح زیر مجازات می‌شود: پ - در جرائمی که مجازات قانونی آن‌ها شلاق حدی یا حبس تعزیری درجه پنج است به حبس تعزیری یا شلاق یا جزای نقدی درجه شش.

همان‌طور که اشاره شد، جرم کلاهبرداری رایانه‌ای، جرمی مقید به نتیجه است؛ یعنی، اگر نتیجه محقق نشود، بزه تام کلاهبرداری رایانه‌ای نیز محقق نمی‌گردد؛ کلاهبرداری رایانه‌ای، جدای از شرایط لازم، شامل دو رفتار فیزیکی و نتیجه حاصله است؛ این نتیجه حاصله، ضرر به دیگری و انتفاع مرتکب است؛ بنابراین، هرگاه شخصی وارد عملیات اجرایی این جرم شود (که از رفتارهای تمثیلی نظیر وارد کردن داده، آغاز می‌گردد) و به واسطه عاملی خارج از اراده او به نتیجه (ضرر به دیگری و انتفاع وی)، نرسد، مرتکب شروع به جرم کلاهبرداری رایانه‌ای شده است که چون جرم تام آن، درجه پنج است، وفق بند «پ» از ماده ۱۲۲ قانون مجازات اسلامی مصوب ۱۳۹۲، مرتکب به حبس تعزیری یا شلاق یا جزای نقدی درجه شش محکوم می‌گردد.

به‌عنوان مثال، دانشجویی که رتبه علمی چهارم را کسب کرده و دانشگاه به نفرات اول تا سوم، وجهی می‌پردازد، وارد سایت دانشگاه شود و به قصد کلاهبرداری رایانه‌ای به جهت دریافت آن مبلغ از دانشگاه، نمره درس سه واحدی خود را دو نمره افزایش دهد تا نفر سوم شود ولی پس از آن دانشگاه متوجه شود و رفتار فیزیکی بعدی یعنی اخذ وجه محقق نشده، عمل وی در این قسمت متوقف شده و تنها مرتکب شروع به جرم شده است؛ حال در این فرض، فرد اگر پس از این تغییر داده، پشیمان گردد و برای بازگشت به همان معدل درسی سابق، دو نمره از همان درس کم کند و یا درس سه واحدی دیگری را کم کند، رفتار وی جرم نیست؛ زیرا، وفق ماده ۱۲۴ قانون مجازات اسلامی مصوب ۱۳۹۲، وی به اراده خود آن را ترک کرده است؛ مگر آن‌که تا این میزان از رفتار خود مستقلاً جرم باشد؛ مثلاً در این جا باید بررسی کرد که آیا تا این میزان رفتار سبب تحقق جرم دسترسی غیرمجاز و یا جعل رایانه‌ای شده است یا خیر؟

جرم محال، یعنی آن‌که مرتکب، قصد دارد جرمی را انجام دهد و تا انتهای مسیر آن بزه به حرکت خود ادامه دهد و تمام تلاش خویش را جهت تحقق آن جرم انجام دهد اما به نتیجه نرسد و این عدم نتیجه ناشی از عدم قابلیت نتیجه بخش آن رفتارها باشد؛ مثلاً فرد اشتباهاً آب را سمی کشنده تصور کند و آن را به دیگری بدهد و او بنوشد (اردبیلی، ۱۳۹۳، ج ۱، ۳۲۶). جرم محال (به‌عنوان یکی از جرایم ناقص) نیز در بزه کلاهبرداری رایانه‌ای قابل تحقق است؛ به‌عنوان مثال، فرد قصد تغییر داده و سپس کلاهبرداری رایانه‌ای از طریق یک نرم‌افزار خاصی مدنظر دارد ولی قابلیت این نرم‌افزار تغییر داده به صورت موقت سه روزه است و سپس به حالت قبلی باز می‌گردد و رسیدن به امتیاز موردنظر او و ضرر به دیگری در روز چهارم رخ می‌دهد، در این جا، از ابتدا محال بوده نرم‌افزار قابلیت تغییر داده را بیش از سه روز داشته باشد و تغییر داده مدنظر فرد بیش از این مدت بوده و از قابلیت محدود آن آگاهی نداشته است؛ در این جا

می‌توان گفت جرم محال رخ داده است؛ همچنین، در صورتی که تغییر داده توسط نرم‌افزار تنها در صفحه خود فرد نمایش داده شود (تغییر ظاهری نه واقعی)، مثل فتوشاپ و فرد گمان کند این تغییر تأثیر واقعی دارد؛ جرم محال رخ داده است.

جرم عقیم، مانند شروع به جرم است با این تفاوت که تا انتهای راه مجرمانه فرد حرکت می‌کند ولی به دلایلی از قبیل عدم مهارت به نتیجه نمی‌رسد (اردبیلی، ۱۳۹۳، ج ۱، ۳۲۸). در کلاهبرداری رایانه‌ای نیز جرم عقیم وجود دارد و فرد رفتاری مثل وارد کردن داده را نیز انجام می‌دهد و تا دریافت مال هم پیش می‌رود اما به جهاتی مانند حادثه غیرقابل پیش‌بینی و یا عدم مهارت نتواند به نتیجه این بزه یعنی ضرر به دیگری و انتفاع وی (مرتکب) دست یابد؛ مثلاً در مثال سایت دانشگاه، فرد که قصد دارد با افزایش نمره درسی خود (از طریق افزایش داده)، خود را جزو سه نفر برتر علمی دانشگاه جهت اخذ وجه تعیین شده، معرفی کند، اما مثلاً از طریق هک توسط یک دانشجوی دیگر که با دانشگاه مشکل داشته، سیستم دانشگاه مختل شود جوری که معدل نمرات برتر و غیربرتر غیر واقعی ظاهر گردد و یا خود فرد قصد داشته باشد؛ از طریق نرم‌افزاری وارد صفحه شخصی دانشگاهی نمرات برتر شود تا از هر کدام مثلاً یک نمره از درس دو واحدی کسر کند ولی چون تسلط به آن نرم‌افزار و زبان آن که مثلاً یونانی بوده نداشته و یا بایستی زبان برنامه‌نویسی خاصی را به عنوان مقدمه کار مثلاً زبان جاوا، کاملاً یاد می‌گرفته و سپس اقدام می‌کرده ولی انجام نداده، اشتباهها سبب شود تا به آنان هر کدام یک نمره از درس دو واحدی اضافه کند ولی خیال کند از آن‌ها نمره کم شده است، در این فرض‌ها رفتار وی می‌تواند جرم عقیم باشد که مجازات شروع به جرم بزه کلاهبرداری رایانه‌ای که همان بند «پ» ماده ۱۲۲ قانون مجازات اسلامی مصوب ۱۳۹۲ است، را دارد؛ البته اگر این میزان رفتار تحت عنوان خاص مجرمانه دیگری مانند ماده ۸ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ (اخلال در داده‌ها) قرار گیرد، وی تنها به آن جرم محکوم خواهد شد.

## ۲- تشابه و تفاوت‌های عنصر مادی جرایم کلاهبرداری رایانه‌ای و سنتی

در این قسمت، با تبیین وجوه تشابه و تفاوت میان جرایم کلاهبرداری رایانه‌ای و سنتی، به مقایسه و تطبیق آن‌ها خواهیم پرداخت.

## ۱-۲- وجوه تشابه این دو جرم

در ذیل، تحت پنج عنوان، موارد مشابه این جرایم را تبیین خواهیم نمود.

### ۱-۱-۲- ارتکاب بزه تنها از طریق فعل مثبت

با عنایت به مرحله اول از رفتارهای فیزیکی تشکیل دهنده جرم کلاهبرداری رایانه‌ای که شامل مصادیق تمثیلی نظیر حذف کردن، وارد کردن و ایجاد کردن است؛ متوجه می‌شویم که این بزه، تنها از طریق فعل مثبت قابل تحقق است؛ همچنین، بزه کلاهبرداری سنتی نیز، با توجه به رفتارهای فیزیکی و شرایط لازم تشکیل دهنده آن، صرفاً از طریق فعل مثبت رخ می‌دهد و ارتکاب این دو جرم به صورت ترک فعل، سبب تحقق آن‌ها نخواهد شد؛ مثلاً در کلاهبرداری رایانه‌ای، فرد نمی‌تواند رفتاری مانند وارد کردن و یا تغییر دادن داده را به صورت ترک فعل انجام دهد. بنابراین، این دو بزه، از حیث عنصر مادی (فعل)، مشابه هستند.

### ۲-۱-۲- مرکب بودن جرم

تشابه دیگر این دو بزه، در مرکب بودن آن‌ها است؛ دو بزه مذکور دو مرحله‌ای هستند؛ در جرم کلاهبرداری رایانه‌ای، در کنار شرایط ضروری، دو رفتار لازم نیز جهت رسیدن به نتیجه بزه وجود دارد که شامل دو مرحله می‌باشد و از این جهت جرم ساده نیست و مرکب قلمداد می‌شود؛ مرحله نخست آن شامل مصادیق تمثیلی مانند وارد کردن یا ایجاد داده و مرحله دوم دربرگیرنده پنج مورد محصور، مانند دریافت وجه یا امتیازات می‌باشد. در جرم کلاهبرداری سنتی نیز، دو مرحله جهت رسیدن به نتیجه حاصله وجود دارد؛ که شامل مانور متقلبانه و فریب بزه‌دیده می‌باشد؛ بنابراین این جرم نیز مرکب است.

### ۳-۱-۲- تعلق مال به دیگری

تعلق داده (دارای مالیت) به دیگری، از شرایط لازم این بزه در جرایم رایانه‌ای است؛ قطعاً اگر این شرط، نباشد تمامی رفتارهای فیزیکی این بزه بی‌معنا خواهند بود. منظور از مال متعلق به دیگری در این جا، اموال و مشترکات عمومی مانند وقف عامه نیست و همچنین، با عنایت به تفسیرهای حقوقدانان رویه قضایی، منظور از مال، اعم از منقول و غیرمنقول است. در بزه کلاهبرداری سنتی و جرایم در حکم آن، مانند انتقال مال غیر، تعلق مال به دیگری از شرایط اساسی تشکیل دهنده آن‌ها است. مثلاً اگر شخصی تصور کند، اطلاعات فلان کارت بانکی و وجه آن برای دیگری است ولی در حقیقت، وجه آن امانتی باشد که صاحب کارت بایستی عین آن را به او باز می‌گردانده و یا عیناً دینی باشد که قرار بوده به او برگرداند، ولی



پس نداده و مرتکب، وجه را اخذ کند؛ شرط فوق، وجود ندارد و در نتیجه، این بزه محقق نشده است؛ در این جا، چون این بزه، به صورت نسبی قابلیت تحقق نداشته، جرم محال نسبی است.

عدم وجود این شرط، نتیجه حاصله این جرم را نیز بی مفهوم می کند؛ نتیجه حاصله بزه رایانه ای که ضرر به دیگری و انتفاع مرتکب است؛ بدون وجود این شرط معنا ندارد و محقق نمی گردد؛ زیرا زمانی که داده، متعلق به مرتکب باشد، نه خود نفعی برده و نه دیگری، ضرر کرده است. البته، از ظاهر ماده ۱۳ قانون جرایم رایانه ای، ممکن است این چنین فهمیده شود که با بردن مال متعلق به خود نیز، این جرم محقق شده است؛ در نتیجه، بهتر است این ایراد توسط مقنن، برطرف و عبارت «مال متعلق به دیگری»، در این خصوص، تصریح گردد.

#### ۴-۱-۲- مجرم و بزه دیده

مجرم و بزه دیده، چه در جرم رایانه ای و چه در بزه سنتی آن، دربرگیرنده شخص حقیقی و حقوقی است که هر یک قابلیت ارتکاب و بزه دیده شدن در جرایم یاد شده را دارند. واضح است که یک شخص حقیقی می تواند مرتکب بزه های فوق شود و یا بزه دیده آن ها باشد اما با توجه به مسئولیت استثنایی شخص حقوقی، بایستی شرایط قانونی وجود داشته باشد تا شخص حقوقی مشمول آن گردد. وفق ماده «۱۴۳»<sup>۷</sup> قانون مجازات اسلامی مصوب ۱۳۹۲، شخص حقوقی، تنها زمانی بزه کار جرایم فوق است که آن جرایم، توسط نماینده قانونی آن صورت گیرد و بزه های مزبور بایستی به نام یا در راستای آن رخ دهد؛ این قابلیت ارتکاب، در دو بزه بالا وجود دارد.

به طور مثال، اگر نماینده قانونی شخص حقوقی، به نام یا در راستای منافع آن، داده ای غیرمجاز از شخص حقیقی یا حقوقی به دست آورد و با وارد کردن آن نهایتاً مال و یا امتیازی از آن کسب کند و تمامی شرایط این بزه وجود داشته باشد؛ جرم کلاهبرداری رایانه ای توسط شخص حقوقی رخ داده است؛ حال در این مثال، اگر رفتار فیزیکی تغییر کند و نماینده قانونی، با همان اهداف، مانور متقلبانه داشته باشد و شخص حقیقی و یا حقوقی فریب بخورد و مالی به دست آورد، با جمیع شرایط بزه کلاهبرداری سنتی، این بزه محقق می گردد. مثال دیگر در این زمینه این است که اگر یک نفر، با هک کردن خودپرداز و

۷- ماده ۱۴۳: در مسئولیت کیفری اصل بر مسئولیت شخص حقیقی است و شخص حقوقی در صورتی دارای مسئولیت کیفری است که نماینده قانونی شخص حقوقی به نام یا در راستای منافع آن مرتکب جرمی شود. مسئولیت کیفری اشخاص حقوقی مانع مسئولیت اشخاص حقیقی مرتکب جرم نیست.

داده‌های بانکی، سبب شود وقتی افراد، در آن فضا کارهای مالی مربوط به آن بانک را انجام می‌دهند، داده و اطلاعات مالی و رمزهای آنان در آن جا به شکل خودکار، ضبط گردد، در نهایت وجهی از آنان برداشته شود، این بزه رخ داده است؛ همچنین اگر یک شرکت غیردولتی که فعالیت‌های غیرقانونی انجام می‌دهد، برنامه‌ریزی دریافت مال از مراجعه‌کنندگان (اعم از اشخاص حقیقی و حقوقی) را به سیستم و برنامه‌ای مجزا از طریق نرم‌افزار و یا ربات‌هایی مخصوص، طراحی کند؛ جوری که تمام مراحل را تا نتیجه حاصله، سیستم انجام دهد؛ به جهت آن که در این جا، سبب اقوی از مباشر است، بزه کلاهبرداری رایانه‌ای، توسط مسبین آن، محقق شده است. با عنایت به مثال‌های فوق، در می‌یابیم که بزه دیده شدن شخص حقوقی نیز در دو جرم رایانه‌ای و سنتی مذکور، ممکن است.

## ۲-۲- وجوه تفاوت این دو جرم

در کنار موارد مشابه فوق، در ذیل، مرز میان این دو بزه را با ارائه مواردی که نشانگر تفاوت آن‌ها است؛ تبیین خواهیم نمود.

### ۲-۲-۱- بستر بزه

بستر جرم کلاهبرداری سنتی با همان بزه به صورت رایانه‌ای، متفاوت است؛ کلاهبرداری سنتی و جرایم در حکم آن، مواردی را دربرمی‌گیرند که جرم، در بستری غیررایانه‌ای رخ دهد؛ البته لازم به توضیح مجدد است که بزه کلاهبرداری سنتی که از طریق رایانه محقق گردد، جزو مصادیق این بزه به شکل سنتی (نه رایانه‌ای) است؛ به طور مثال، اگر شخصی از طریق شبکه اجتماعی اینستاگرام که بستری رایانه‌ای است، قصد فروش صفحه اینستاگرامی خود را داشته باشد و مانوری متقلبانانه انجام دهد، مثلاً با استفاده از وسایل نوعاً متقلبانانه، مانند نرم‌افزارهای فالوورگیر غیرواقعی حرفه‌ای، فالوورهای غیرواقعی را درکنار فالوورهای واقعی قرار دهد ولی همه فالوورها را واقعی تبلیغ کند و آن صفحه را بفروشد و در نتیجه مالی کسب کند، با جمیع شرایط ذیل ماده نخست قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷، وی مرتکب بزه کلاهبرداری سنتی مشدد از طریق رایانه شده است (نه کلاهبرداری رایانه‌ای)؛ بنابراین، هرچند در این موارد، بستر رایانه‌ای، بستری جهت ارتکاب کلاهبرداری سنتی است اما چون در این جا، رفتار فیزیکی بزه کلاهبرداری رایانه‌ای، وجود ندارد، این بستر، صرفاً طریقی جهت ارتکاب بزه کلاهبرداری سنتی تلقی می‌گردد؛ به نظر، وجه تسمیه آن نیز به این جهت است.

جرم کلاهبرداری رایانه‌ای که در این نوشتار، منظور از آن، موضوع ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است (نه کلاهبرداری کامپیوتری، موضوع ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ که اخص از آن است)؛ تنها در بستر رایانه (نه به صورت سنتی و از طریق رایانه)، قابل تحقق است؛ برخلاف بزه سنتی آن، این بزه رایانه‌ای صرفاً مواردی را دربرمی‌گیرد که تمامی شرایط و رفتارهای فیزیکی آن را داشته و در بستر رایانه رخ می‌دهد.

#### ۲-۲-۲- مانور متقلبانه

این دو بزه در شرایط لازم جهت تحقق آن‌ها، کاملاً با یکدیگر متفاوت هستند (پایدارفرد، ۱۳۹۹، ۱۲۴). شرط اساسی جهت تحقق بزه کلاهبرداری سنتی، مانور متقلبانه از طریق وسایل نوعاً فریب‌دهنده است؛ اما این شرط، در جرم کلاهبرداری رایانه‌ای وجود ندارد؛ زیرا برخلاف ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷، ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تصریحی به این شرط نداشته و صرف ارتکاب رفتارهای دو مرحله‌ای مزبور، نتیجه حاصله و وجود سایر شرایط آن ماده، بزه تام رایانه‌ای، محقق شده است و نیازی به تحقق این شرط وجود ندارد. البته، این شرط در بزه کلاهبرداری کامپیوتری، موضوع ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ نیز وجود دارد اما به جهت اخص بودن آن نسبت به بزه کلاهبرداری رایانه‌ای، نمی‌توان آن شرط را در این جرم نیز جاری نمود؛ هرچند ممکن است خلاف آن را به دلیل تفسیر به نفع متهم، به علت باقی ماندن شک، استدلال نمود.

همچنین، در جرم کلاهبرداری سنتی، رفتار فرد بایستی ماهیتی دروغین جهت بردن مال دیگری داشته باشد (نه آن‌که دلیل دروغ وی، شوخی یا پیشگیری از یک حادثه باشد) که این مورد در کلاهبرداری رایانه‌ای وجود ندارد. در حقیقت، شرط لازم در بزه کلاهبرداری این است که مرتکبان، بایستی جهت دریافت وجه یا مال، لزوماً یک دلیل کذب داشته باشند که مقدمه مانور متقلبانه است؛ در این جا، بایستی این کذب همراه با آن مانور متقلبانه باشد و به تنهایی جهت تحقق این بزه، کافی نیست.

#### ۲-۲-۳- اغفال و فریب بزه‌دیده

شرط دیگری که در بزه کلاهبرداری سنتی وجود دارد اما در جرم کلاهبرداری رایانه‌ای وجود ندارد؛ شرط اغفال و فریب بزه‌دیده جرم است. در کلاهبرداری سنتی، شخص، با استفاده از وسایل متقلبانه و با ملاک عرفی، مانوری متقلبانه انجام می‌دهد اما این مانور و صحنه‌سازی متقلبانه بایستی منجر به فریب و

اغفال بزه‌دیده گردد تا نتیجه، حاصل گردد. در حقیقت، در بزه سنتی کلاهبرداری، شخص، فریب می‌خورد و در نتیجه آن، اموال خود را به مرتکب می‌دهد (حتی بعضاً فرد، اصرار در دادن اموال خود دارد) اما در جرم کلاهبرداری رایانه‌ای، بدون این شرط، شخص می‌تواند با دخالت غیرمجاز، مرتکب آن گردد. با عنایت به ماده ۱۳ قانون جرایم رایانه‌ای، این شرط که مرتبط با شرط قبلی است؛ از ماده مزبور به دست نمی‌آید؛ صرف تحقق رفتارهای دو مرحله‌ای فیزیکی این بزه، سایر شرایط و نتیجه حاصله، بدون آن که بزه‌دیده را بفریبید، قابل تحقق است. در حقیقت، مسامحتاً می‌توان بیان داشت که اگر شرط اغفال هم وجود داشته باشد؛ سامانه رایانه‌ای فریب می‌خورد (نه شخص).

#### ۴-۲-۲- نتیجه حاصله

نتیجه حاصله در دو بزه کلاهبرداری سنتی و رایانه‌ای، یکسان نیست؛ ضرر به دیگری و انتفاع مرتکب، نتیجه حاصله بزه کلاهبرداری رایانه‌ای است اما نتیجه حاصله بزه کلاهبرداری سنتی، بردن مال دیگری است که ضرر به دیگری و انتفاع مرتکب را نیز به همراه دارد؛ هرچند از این حیث، با یکدیگر تفاوت دارند اما از این جهت که در هر دو ضرر به دیگری و انتفاع مرتکب وجود دارد، شباهت دارند. همچنین لازم به ذکر است که مقنن، در کلاهبرداری سنتی، فقط به بردن مال دیگری و آن هم در نتیجه عنوان کرده اما در کلاهبرداری رایانه‌ای، پنج مورد محصور یعنی، مال یا وجه یا منفعت یا خدمات یا امتیازات مالی را آن هم به عنوان مرحله دوم از رفتار فیزیکی (نه نتیجه)، تبیین کرده است. به عبارتی دیگر، بزه کلاهبرداری سنتی با رایانه‌ای، از حیث نتیجه، در «انتفاع مرتکب» و «ضرر به دیگری»، مشابه ولی از این جهت که «بردن مال» نیز در بزه کلاهبرداری سنتی، جزو نتیجه است اما در جرم کلاهبرداری رایانه‌ای، جزو رفتارهای فیزیکی (نه نتیجه) است، متفاوت هستند.

#### نتیجه

رکن مادی کلاهبرداری رایانه‌ای، دربردارنده رفتار فیزیکی که شامل هرگونه رفتار وابسته به داده یا سامانه و تحصیل غیرمجاز موضوع جرم است و نتیجه حاصله است. شرایط لازم جهت تحقق کلاهبرداری رایانه‌ای، شامل متعلق بودن اموال به دیگری، نیازمندی مستقیم به داده و سامانه‌های رایانه‌ای در زمان ارتکاب و نتیجه حاصله می‌شود. وجوه تشابه این دو جرم، ارتکاب بزه تنها از طریق فعل مثبت، مرکب بودن جرم، تعلق مال به دیگری و مجرم و بزه‌دیده می‌باشد. وجوه تفاوت این دو جرم، بستر بزه،

مانور متقلبانه، اغفال و فریب بزه‌دیده و نتیجه حاصله است. در این پژوهش، مهم‌ترین نتایجی که از مقایسه این دو بزه از حیث رکن مادی به دست می‌آید آن است که در جرم کلاهبرداری رایانه‌ای برخلاف کلاهبرداری سنتی، اغفال و فریب بزه‌دیده 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 رایانه‌ای (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.

**ملاحظات اخلاقی:** موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

**تعارض منافع:** تعارض منافع در این مقاله وجود ندارد.

**تأمین اعتبار پژوهش:** این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

## منابع

- اردبیلی، محمدعلی، ۱۳۹۳، **حقوق جزای عمومی**، جلد اول، چاپ سی و پنجم، تهران، انتشارات میزان.
- الهام، غلامحسین و برهانی، محسن، ۱۳۹۷، **درآمدی بر حقوق جزای عمومی: جرم و مجرم**، جلد اول، چاپ چهارم، تهران، انتشارات میزان.
- بابایی، جواد، ۱۳۹۷، **جرایم رایانه‌ای و آیین دادرسی حاکم بر آن**، چاپ دوم، تهران، مرکز مطبوعات و انتشارات قوه قضاییه.
- بشیری، قدرت و پایدارفرد، علی، ۱۴۰۰، **سرقت‌های خشن از نگاه جرم‌شناسی و جامعه‌شناسی جنایی**، چاپ اول، تهران، انتشارات مهر کلام.
- پایدارفرد، علی، ۱۳۹۹، **رکن مادی جرایم علیه اموال و مالکیت در بستر رایانه**، چاپ اول، تهران، انتشارات سیمای قلم.
- ترکی، غلامعباس، ۱۳۸۹، نگرش علمی و کاربردی به قانون جرایم رایانه‌ای، **ماهنامه دادرسی**، شماره ۸۳.
- صنعتی، سیدمهدی و عطایی جنتی، مجید، ۱۳۹۷، **تحلیلی بر جرایم رایانه‌ای و مخابراتی (جرایم در بستر رایانه، فضای مجازی، شبکه‌های اجتماعی و پیام‌رسان‌ها)**، چاپ اول، قم، انتشارات حقوق پویا.
- عابدی، احمدرضا، ۱۳۹۸، **آیین دادرسی کیفری**، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه قضاییه.

- عالی پور، حسن، ۱۳۹۵، **حقوق کیفری فناوری اطلاعات**، چاپ چهارم، تهران، انتشارات خرسندی.
- میرمحمدصادقی، حسین، ۱۳۹۴، **حقوق کیفری اختصاصی جرایم علیه اموال و مالکیت**، چاپ چهل و ششم، تهران، انتشارات میزان.
- مصدق، محمد، ۱۳۹۹، **شرح قانون کاهش مجازات حبس تعزیری**، چاپ دوم، تهران، انتشارات جنگل.

### قوانین

- قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷
- قانون تجارت الکترونیکی مصوب ۱۳۸۲
- قانون جرایم رایانه‌ای مصوب ۱۳۸۸
- قانون مجازات اسلامی مصوب ۱۳۹۲
- قانون کاهش مجازات حبس تعزیری مصوب ۱۳۹۹



Feasibility of Referring to Adjustment Theory in Iranian Law as a Solution in Contractual Excuse - Roshan Ali Shekari, Sayyed Mostafa Milani

Criminal Protection of the Rights of Future Generations in International Documents - Adel Sarikhani, Mostafa Karami Pour

Analysis of the Right of the People to Control the Government from the Point of View of Ali (PBUH) by Looking at the Constitution of the Islamic Republic of Iran - Ebrahim Musazadeh, Mohammad Salehi

Reflections on the Legislation of Oath (Qassameh) According to the Science of Criminalistics - Mohammad Ali Hajidehabadi, Ruhollah Shamshiri

Rereading Interactions (Some Religious Groups and Actors in the International System) the Field of Terrorism as a Means of Achieving National Interests with an Emphasis on Legal Responsibilities in Islamic Countries - Sayyed Mohammadreza Mousavifard, Hamidreza Norozian, Arefeh Kordi Nasab, Nafiseh Tosi, Ayda GHasem Zadeh

The Principle of Prohibition of Repatriation of Refugees from the Perspective of Human Rights Documents with Emphasis on Environmental Refugees - Mahnaz Khorsandi, Asgar Jalalian

Dangers of Prioritizing Financial Issues in Legal Professions - Mohammad Setayesh Pur, Maryam Faraji Tark

The Rulings and Effects of Permission in the Legal System of Iran and France - Hasan Najjarha

Comparison of the Actus Reus of the Crime of Computer Fraud with Traditional - Ali Paidarfard, Javad Naderi ooj Boghzi, Ahmadreza Emtehani

Theoretical Foundations of Military Weapons Equipment Control with an Emphasis on Contradictory Stands of UN and WTO on Conventional Military Weapons Trade - Pouria Ebrahimzadeh, Somayeh Rahmanian

Child and Childhood from the Perspective of Philosophy and Literature - Maryam SHA'ban

Validity of Sealed Order in Civil and Criminal Cases - Amir Mohammadi, Mohammadmahdi Heydari, Soheyla Moradi GHaleh

The Status of the Kosovo Specialist Branches in Global Criminal Justice System - Mostafa Fazaeli, Arash Maleki

Criminalization of Informing the Contrary in Iranian Law - Saeed Asadzadeh, Fatemeh Ahadi, Mojtaba Kanjori

The Actions of Foreign Companies Regarding Iraq's Use of Chemical Weapons in Holy Defense from the Perspective of International Responsibility Rights - Mohammad Setayesh Pur, Parnian Shafae

Sociological and Criminological Review of the Phenomenon of Prostitution in the International System and Iran with Emphasis on the Teachings of Islamic Criminology - Sayyed Mohammadreza Mousavifard, Asad Akhzari Fard, Ali Mardan Ahmadi

The Police's Interaction with the Crime Prevention Institutions - Mina Momeni, Sayyed Mahdi Ahmadi Musavi

Immigrant Children's Rights in National and International Documents - Reza Khaje Nooredini, Sayede Parisa Mirabi

The Real Competency of Criminal Laws from the Perspective of Islamic Law - Mostafa Karami Pour, Mona Rajabzade Baghi

Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic with an Approach to Routine Activity Theory - Maryam Kamaei

The Position of British Security Officers in the Detection of Crimes - Zahra Vahabi, Arash Razmi

The Independence of Judges in the Legal System of the Islamic Republic of Iran in the Light of the Teachings of Islam - Mohammad Setayesh Pur, Fatemeh Zahra Aslan

Legal Conditions and Legal and Criminal Dimensions of Intellectual Property in the Legal System of the Islamic Republic of Iran - Somayeh Zilabi, Sadeh Fetili, Ebrahim Moghaddam

Feasibility Study of the Realization of the Idea of Criminalization (Crime of Civil Liability of Managers) from Theory to Practice Based on the Approaches of the Model of Criminal Responsibility Model of the Law of Strategic Action to Cancel of Sanctions - Sayyed Mohammadreza Mousavifard, Hamidreza Norozian, Nafiseh Dharovieh, Mohammad Rasol Ansari Nia, Neda Haghghi Jurisprudential-Legal Evaluation of the Real Multiplicity in the Hodood, Retaliation and Diat - Ali Mohammadi Jurkoye, Ahmadreza Emtehani, Javad Naderi ooj Boghzi

The Position and Role of the People in the Establishment and Continuation of Ummat and Imamat System In the Light of Martyr Beheshti's Opinions - Mohammad Sadeq Darivand

Mediation, Participatory Justice System, Third Generation Criminal Justice System and the Rights of Parties the Lawsuit - Sadeh Fetili, Mohammad Fetili, Ebrahim Moghaddam