فصلنامه علمی تحقیقات حقوقی آزاد، دوره سیزدهم، شماره ۴۸، تابستان ۱۳۹۹
تاریخ دریافت: ۱۳۹۹/۱۰/۰۵ ؛ تاریخ پذیرش: ۱۳۹۹/۱۲/۲۵
صفحات: ۲۷۵-۲۵۵ نوع مقاله: پژوهشی

# کلاهبرداری اینترنتی در پرتو جرم‌شناسی نظری

محمد سجاد اعتباری،[۱] علی مزیدی شرف‌آبادی،[*۲] محمد رضا رحمت[۳]

**چکیده:**
امروزه فضای مجازی بخش لاینفک از زندگی بشر شده است و به اقتضای ویژگی‌های خاصی که دارد نه تنها از گزند مجرمان مصون نمانده است، بلکه افرادی که پیشتر منحرف نبوده‌اند را به ارتکاب رفتار مجرمانه به طمع انداخته است و مجموعه چالش‌هایی را برای مراجع قضایی و انتظامی که سعی در کنترل این پدیده دارند ایجاد کرده است. در حال حاضر ارتکاب جرایم مالی در فضای مجازی و کلاهبرداری‌های اینترنتی بخش قابل توجهی از پرونده‌های کیفری در مراجع قضایی را شامل می‌شود. در این میان جرم‌شناسی به عنوان علمی که به بررسی پدیده بزهکاری می‌پردازد، نظرات و دیدگاه‌های مختلفی را در تحلیل این مهم ارائه نموده است. در همین راستا تحقیق حاضر با موضوع «گسترش کلاهبرداری اینترنتی از دیدگاه جرم‌شناسی نظری» و با هدف تبیین و تشریح دیدگاه‌های نظری جرم‌شناسی پیرامون گسترش کلاهبرداری اینترنتی به انجام رسیده است. در این نوشتار که به روش توصیفی – تحلیلی و با بهره‌گیری از منابع و متون کتابخانه‌ای صورت پذیرفته است پس از بررسی و تجزیه و تحلیل نظریه‌های جرم‌شناختی و مطالب و مباحث مطروحه این نتیجه حاصل شده که گسترش کلاهبرداری اینترنتی در فضای مجازی در وهله نخست مرتبط با ویژگی‌های خاصی فضای مجازی از قبیل «حجم و مقیاس ارتکاب جرایم سایبری» است.

**واژگان کلیدی:** کلاهبرداری اینترنتی، فضای مجازی، جرم‌شناسی نظری، بزه‌دیده، یادگیری اجتماعی.

---

* دانشجوی دکتری حقوق کیفری و جرم شناسی، دانشکده علوم انسانی، واحد یزد، دانشگاه آزاد اسلامی، یزد، ایران.
** استادیار، گروه حقوق، دانشکده علوم انسانی، واحد یزد، دانشگاه آزاد اسلامی، یزد، ایران. (نویسنده مسئول)
mazidi_ali_46@yahoo.com
*** استادیار، گروه حقوق، دانشگاه میبد، میبد، ایران.

**مقدمه**

رشد سریع فناوری اطلاعات در سال‌های اخیر دستاوردها و تحولات بسیاری را در ابعاد گوناگون زندگی انسان‌ها به وجود آورده است. بیشتر فعالیت‌های روزمره زندگی به نوعی وابسته به رایانه‌هاست و روزبه روز بر این وابستگی افزوده می‌شود. این فناوری بزرگ که در ابتدا برای آسایش و رفاه هر چه بیشتر انسان‌ها مورد بهره‌برداری قرار می‌گرفت به تدریج به ابزاری برای مجرمان، جهت نیل به آمال مجرمانه نیز تبدیل شد. امروزه فعالیت بزهکارانه عمومی، دیگر منحصر به دنیای حقیقی نیست. به موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر، بخشی از بزهکاران نیز فعالیت مجرمانه خود را به فضای سایبر منتقل کرده‌اند یا از رهگذر چنین فضایی، مرتکب جرم یا جرائمی می‌شوند (پیکا، ۱۳۹۰: ۱۱). این فضای جدید به گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادی کرده که تعریف از جرائم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری موارد متفاوت است (حسن بیگی، ۱۳۸۴: ۳۵). همچنین جرائم سایبری به اقتضای ویژگی‌های منحصر به فرد خود همچون سهولت ارتکاب جرم، فرامرزی بودن جرم، کم سن بودن مجرمان، گستردگی خسارت، بالابودن رقم سیاه بزهکاری کثرت بزه‌دیدگان، ضرورت دقت در فرآیند جرم‌انگاری و شناسایی عوامل موثر در بروز این بزه را افزایش داده‌اند.

در این میان ارتکاب جرایم مالی و اقتصادی در این فضا، همچون فضای حقیقی دارای فراوانی زیاد و البته ابعاد و آثار مخرب‌تری است. بی‌گمان جذابیت‌های خاص مالی و ویژگی‌های ذاتی نوع بشر از قبیل طمع، حرص و مال اندوزی در این فضا بسیار تأثیرگذار است. با این حال ضرورت شناخت ابعاد مختلف پدیده نوظهور ارتکاب جرایم کلاهبرداری در فضای مجازی ما را بر آن داشته تا در نوشتار حاضر از دیدگاه جرم‌شناسی نظری به بررسی این مهم پرداخته و عوامل وقوع جرم کلاهبرداری اینترنتی را از دیدگاه جرم‌شناسان مختلف و نظرات و ایده‌های اندیشمندان مختلف و نظریه‌های مطرح جرم‌شناسی مورد بحث و بررسی قرار دهیم.

## ۱- گستره ارتکاب جرایم کلاهبرداری در فضای مجازی

فضای سایبر برخلاف سایر رسانه‌ها به لحاظ مجازی بودن خود، دنیایی در کنار دنیای واقعی ایجاد کرده است و برخلاف محیط های فیزیکی که در دنیای واقعی با مرزها و دیوارها از هم جدا می‌شوند، فاقد هرگونه حد و مرز تعیین‌کننده‌ای است؛ این امر در عمل خود مشکلات بسیاری را موجب می‌گردد. حجم و مقیاس بالای جرائم سایبری، وسعت ایراد ضرر، بالا بودن رقم سیاه جرائم سایبری، پراکندگی جغرافیایی و کثرت بزه‌دیدگان جرائم سایبری از جمله اصلی‌ترین

چالش‌هایی هستند که در مواجهه با کلاهبرداری اینترنتی با آن‌ها درگیر هستیم که همین امر نیز ضرورت اتخاذ سیاست کیفری افتراقی را در این زمینه توجیه می‌نماید؛ به‌طوری که بدون آن نمی‌توان امیدوار به کنترل و مبارزه کارآمد با ارتکاب کلاهبرداری در فضای مجازی داشت. در ادامه به بررسی چالش‌های مذکور خواهیم پرداخت.

### ۱-۱- حجم و مقیاس

از ویژگی‌های جرائم دنیای واقعی این است که مدل ارتکابی جرم به صورت نرم «یک به یک» تبعیت می‌نماید. بدین بیان که یک مرتکب معمولاً با یک قربانی درگیر می‌شود. در جرائم اساسی از جمله قتل، تجاوز به عنف، احراق و غیره، مرتکب معمولاً یک قربانی را هدف قرار می‌دهد و تمام توجهش به تکمیل آن جرم متمرکز می‌گردد. (Brenner,1993: 255) وقتی که جرم کامل شد در آن صورت مرتکب به سمت دیگر بزه‌دیدگان و دیگر جرایم حرکت می‌کند. قاعده «یک به یک» در جرایم دنیای واقعی ناشی از محدودیت فیزیکی تحمیل شده به فعالیت‌های انسان، می‌باشد؛ یک سارق نمی‌تواند در آن واحد بیش از یک کیف پول بردارد؛ از این رو جرایم دنیای واقعی، جرایم سریالی هستند. مضاف بر اینکه مجرم و قربانی عموماً در یک روستا یا یک محله‌ی شهری زندگی می‌کنند و مجرم از قبل قربانی خود را شناسایی می‌نماید آنگاه بر روی وی مرتکب جرم می‌شود. لذا همین امر یک فرصت مناسبی است که مجرم به واسطه قربانی جرم شناسایی شود؛ اگر مرتکب با مجرم روابط اجتماعی نداشته باشد و اصطلاحاً غریبه باشند، غریبگی مجرم احتمال شناسایی وی را افزایش می‌یابد و شهروندان محلی نقش بسزایی جهت توجه به کسانی که تعلقی به آن محل ندارند، می‌کنند. بنابراین، تحقیقات یک جرم سنتی اساساً روی یک منطقه جغرافیایی خاص که جرم در آن رخ داده متمرکز می‌شود (Steven,1990: 255).

این محدودیت‌ها به دستگاه عدالت کیفری این اجازه را می‌دهد که برنامه‌های ضروری را جهت مقابله با جرم و مجرم آن پیش‌بینی نماید. اما در جرایم سایبری و به خصوص در کلاهبرداری‌های اینترنتی به واسطه‌ی استفاده از تکنولوژی نوین، قاعده «یک به چند» مورد استفاده قرار می‌گیرد. لذا با توجه به ویژگی‌های انحصاری فضای سایبر، قربانی کردن هزاران یا حتی میلیون‌ها نفر طی اقدامی واحد، فرضی حقیقی و باورکردنی در این فضا است (Brenner,2005: 53). این امر باعث می‌شود که حجم و آمار بزه در دنیای دیجیتال با دنیای واقعی قابل قیاس نباشد. به طور مثال در سال ۲۰۰۲ در ایالات متحده، بیش از نود درصد بنگاه‌های صنعتی تحت تأثیر حملات سایبری بوده‌اند و صدها میلیون دلار خسارت دیده‌اند (R.Vaca,2002: 68). پژوهشی جدید نشان می‌دهد بیش از ۱۵ میلیارد اطلاعات حساب‌های کاربری سرقت شده در وب تاریک وجود دارد. محققان شرکت امنیت سایبری «دیجیتال شادوز» متوجه شده‌اند میلیاردها نام کاربری و پسورد

متعلق به حساب‌های کاربری مختلف در وب تاریک عرضه می‌شوند (به نقل از خبرگزاری مهر به تاریخ ۱۹ تیر ۱۳۹۹).

بنابراین در بحث گستره ارتکاب جرایم کلاهبرداری در فضای مجازی، «حجم و مقیاس» بزه‌دیدگی متفاوت از وضعیتی است که در خصوص وقوع جرایم در دنیای حقیقی قابل تصور و قابل پیش‌بینی است به گونه‌ای که حتی می‌توان این حجم را در برخی موارد بسیار بزرگتر تصور کرد.

## ۱-۲- وسعت ایراد ضرر

موضوع جرائم سایبری از لحاظ اهمیت و میزان خسارات وارده با جرائم سنتی تفاوت دارد. تصور کنید یک یا چند نفر سارق با ورود به یک منزل یا حتی بانک کلیه‌ی اثاثیه منزل یا وجوه موجود در بانک را سرقت می‌نمایند. حداکثر خسارات وارده را که می‌توان در اثر ارتکاب این جرم تصور نمود چقدر است؟ حال سرقت اطلاعات محرمانه یک شرکت تجاری یا سرقت فعالیت‌های پژوهشی که بر روی شبکه قرار دارد، حداقل خسارتی را که می‌توان از آن صحبت کرد شاید فراتر از میلیون‌ها دلار باشد که با ده‌ها سرقت گانگستری بزرگ نیز برابری نمی‌کند. تفاوت بین این دو از آنجا ناشی می‌شود که سرقت اطلاعات از روی شبکه با محدودیت‌های فیزیکی که در سرقت از منازل یا بانک وجود دارد مواجه نیست و تنها چیزی که می‌تواند برای متجاوز به سیستم محدودیت ایجاد کند، امکانات کامپیوتری است که در اختیار دارد. یا در جرمی مثل ترویج عکس‌ها و تصاویر مستهجن و مبتذل، اگر حالت سنتی و فیزیکی آن را در نظر بگیریم، مرتکب مزبور اگر امکانات بسیار پیشرفته تکثیر و چاپ و نیروی انسانی کافی در اختیار داشته باشد، چه تعداد از این گونه تصاویر را در اختیار چند نفر می‌تواند قرار دهد؟ در حالی که کافی است شما و میلیون‌ها نفر مثل شما با نشستن پشت کامپیوتر و اتصال به اینترنت، تنها با فشار یک کلید و در مدت زمان بسیار کوتاهی هزاران تصویر از این دست را منتشر نمایید.

تا یک دهه پیش، جرائم سایبری حجمی در کل جرائم جهان نداشت اما این رقم در سال‌های اخیر به صدها میلیارد دلار رسیده است؛ یافته‌های موسسه پژوهشی CSIS نشان می‌دهد جرائم سایبری سالانه ۴۴۵ میلیارد دلار به اقتصاد جهانی لطمه می‌زند و بیش از ۱۶۰ میلیارد دلار از این رقم خسارت مربوط به صاحبان مشاغل است. علت اصلی وارد شدن چنین خسارت سنگینی به صاحبان مشاغل و کسب وکار نقض حقوق مالکیت معنوی و سرقت داده‌های حساس است که در اثر فعالیت‌های مختلف هکری اتفاق می‌افتد. در گزارش CSIS (مرکز مطالعات استراتژیک و بین‌المللی)، تصریح شده که جرائم سایبری از جمله جرائم در حال رشد است که به خلاقیت،

فضای رقابتی بازار و انواع تجارت آسیب وارد می‌کند. این موسسه میزان این خسارت را در یک برداشت محافظه کارانه ۳۷۵ میلیون دلار و در برداشتی حداکثری بیش از ۵۷۵ میلیون دلار برآورد کرده است.

بنابراین، خسارات ناشی از جرائم کلاهبرداری اینترنتی که بیشتر مبتنی بر سوءاستفاده از نبوغ، توانایی فکری و استعداد افراد می‌باشد، در دهه‌ی اخیر بیش از پیش افزایش یافته است. در کشورهای توسعه‌یافته، محدود کردن آثار این نوع جرم به دلیل ساز و کارهای قانونیِ مناسب، برای جلوگیری از تکرار آن امکان‌پذیر است؛ لیکن در کشورهای در حال توسعه، ضعف و ناتوانی برخی نهادها و سازمان‌ها موجب شده است هزینه بزهکاری سایبری و نیز تأثیر درازمدت آن بر توسعه پایدار چشمگیر باشد؛ در واقع آسیب‌پذیری این دسته از کشورها در مقابل جرائم سایبری بیشتر می‌باشد. عواقب جرائم کلاهبرداری در فضای مجازی نه تنها خسارت‌های اقتصادی سنگینی را به دنبال داشته بلکه تهدیدی جدی برای امنیت بشر می‌باشد؛ زیرا تمام کشورها در امور حساس اعم از پزشکی، مخابراتی، هواپیمایی، امور امنیتی و غیره وابسته به عملکردهای رایانه بوده که کوچکترین اخلال در سیستم، صدمات جبران‌ناپذیری را بر جای خواهد گذاشت.

### ۱-۳- بالا بودن رقم سیاه بزهکاری

در جرم‌شناسی معاصر، آمار جنایی رسمی با وجود فواید تحسین برانگیز و بی‌شمار با چالشی جدی به نام «رقم سیاه» مواجه می‌باشد، تا جایی که باعث شده است برخی از جرم‌شناسان منتقد، اعتبار چنین آماری را زیر سوال ببرند.

با افزایش به‌کارگیری رایانه در تمامی عرصه‌های زندگی و همچنین سهولت استفاده از آن و گسترش شبکه جهانی اینترنت، امروزه جرائم کلاهبرداری در فضای مجازی می‌تواند به وسیله هر شخصی در هر نقطه‌ای از دنیا به وقوع بپیوندد و با آن‌که تحقیقات به عمل آمده نشان از روند رو به رشد جرائم سایبری دارند و لیکن تعداد آمار موجود نمی‌تواند ما را به نتیجه‌گیری مطلوب رهنمون سازد ؛ چه بسا این آمار منعکس‌کننده تعداد جرائم مکشوفه‌اند و نه تعداد جرائم واقعی (Rizgar,2010:610). به عنوان یکی از بارزترین خصوصیات جرائم اینترنتی که ناظر به ماهیت ویژه آن‌هاست، می‌توان به غیرقابل تخمین بودن میزان ارتکاب دقیق این‌گونه جرائم اشاره کرد؛ یعنی همان وجود رقم سیاه بسیار بالا می‌باشد. انجمن بین‌المللی حقوق جزا در گردهمایی خود درباره‌ی جرائم رایانه‌ای و دیگر جرائم علیه تکنولوژی اطلاعاتی در وستبورگ آلمان، گزارشی درباره‌ی جرائم رایانه‌ای بر پایه‌ی گزارش‌های دریافتی از کشورهای عضو ارائه نمود که مطابق آن تخمین زده شد تنها ۵ درصد جرائم رایانه‌ای به مقامات مجری قانون گزارش شده‌اند. بالا بودن رقم سیاه در جرائم سایبری مبتنی بر چند عامل می‌باشد: اول آنکه تکنولوژی پیشرفته یعنی

ظرفیت حافظه‌ی رایانه و سرعت بالای عملیات موجب کشف دشوار جرائم سایبری است. دوم، به دلیل عدم وجود سابقه و شناخت در خصوص جرائم سایبری بزه‌دیدگان و مأمورین اجرای قانون پس از مدتی متوجه وقوع جرم می‌شوند و دسته آخر بسیاری از بزه‌دیدگان توان تشخیص، پیشگیری و مقابله با حوادث مربوط به این‌گونه جرائم را ندارند.از طرف دیگر مرتکبین حرفه‌ای، غالباً از خود مدرکی به جای نمی‌گذارند. اطلاعات قابل نسخه‌برداری‌است بدون آنکه از محل خود برداشته شود و سوابق هم قابل پاک شدن هستند. بخش جرائم سایبری سازمان اطلاعات امنیت آمریکا تخمین زده که بین ۸۵ تا ۹۵ درصد جرائم سایبری حتی کشف هم نمی‌شوند. سوم، عدم تمایل بزه‌دیدگان برای اعلام وقوع جرائم سایبری پس از کشف آن‌ها می‌باشد. در بخش تجارت این عدم تمایل به دو امر مربوط می‌شود. برخی از بزه‌دیدگان ممکن است به دلیل هراس از تبلیغات سوء، رسوایی و یا از دست دادن حسن شهرت خود تمایلی به فاش ساختن اطلاعات نداشته باشند. دیگر بزه‌دیدگان نیز از سلب اعتماد سرمایه‌گذاران و یا عامه مردم و پیامدهای اقتصادی ناشی از آن واهمه دارند. برخی از کارشناسان بر این باورند که این عامل تأثیر چشمگیری بر کشف جرایم سایبری دارند. «قربانی که کارش بر مبنای شهرت به مورد اعتماد بودن استوار است (مانند بانک یا شرکت بیمه) بعید است این واقعیت را که سوابق اطلاعاتی آن دستکاری شده و مجرم نیز ناشناس است، علنی سازد.» همچنین بزه‌دیدگان چون احتمال کمی برای پیدا کردن مجرم با گرفتن غرامت به خاطر ضرر وارده می‌دهند، از پیگیری آن دوری می‌کنند. لذا برای مبارزه و پیشگیری از جرائم سایبری همکاری بزه‌دیده بسیار مهم و حائز اهمیت است (گرایلی، ۱۳۸۹ : ۱۶۹).

از دیگر دلایل بالا بودن رقم سیاه بزهکاری در جرایم کلاهبرداری در فضای مجازی پایین بودن ارقام کلاهبرداری شده در خصوص یک نفر می‌باشد. با این حال مجموع ارقام کلاهبرداری شده ممکن است به میلیاردها ریال نیز برسد به عنوان مثال معاون اجتماعی پلیس فتا ناجا در مرداد ماه ۹۹ اعلام داشت فردی که مدعی خدمت رسانی به خانواده‌ای نیازمند و دارای بیمار صعب‌العلاج بود، با دریافت وجوهات مختلف از خیرین مبلغ ۱۵ میلیارد ریال کلاهبرداری کرده بود (به نقل از خبرگزاری مهر به تاریخ ۶ مرداد۱۳۹۹) این در حالی است که ارقام مربوطه از ده هزار تا چند میلیون تومان متفاوت بود و در این میان فردی که تنها چند هزار تومان خود را از دست رفته می بیند پیگیری قضایی به منظور بازگرداندن مال خود را از نظر وقت و هزینه مقرون به صرفه ندانسته و احتمالاً تمایلی به پیگیری نیز نخواهد داشت. این در حالی است که کلاهبردار از مجموع مبالغ ناچیز این چنینی سود کلانی برده است.

از جمله مهم‌ترین آثار بالا بودن رقم سیاه یک بزه، کاهش اثر بازدارندگی مجازات‌های احتمالی موجود است. زیرا بالا بودن رقم سیاه به معنی کاهش احتمال دستگیری و اعمال کیفر است. در تحلیل اقتصادی از جرم و مجازات و در چارچوب تئوری انتخاب عقلایی، هر چه احتمال دستگیری و در نتیجه اجرای مجازات کاهش یابد، اثر بازدارندگی مجازات‌های قانونی موجود کمتر شده و در نتیجه احتمال ارتکاب جرم افزایش می‌یابد (Cooter& Thomas,2004: 34).

## ۱-۴- پراکندگی جغرافیایی

شاید یکی از بارزترین ویژگی اساسی جرائم محیط واقعی این است که مرتکب و بزه‌دیده به صورت فیزیکی در زمان ارتکاب جرم یا شروع به جرم نزدیک یکدیگر قرار دارند. در جرائم سنتی بزهکار در اکثر موارد چاره‌ای جز حضور در صحنه ارتکاب جرم ندارد. به طور مثال، در جهان واقعی، گرفتن اموال بزه‌دیده به زور و یا برداشتن کیف پول دیگری، در صورتی که بزهکار و بزه‌دیده در دو کشور مختلف باشند، امکان‌پذیر نیست. پس از ارتکاب جرم نیز معمولاً بزهکار جهت محو کردن آثار جرم ارتکابی و جلوگیری از شناسایی خویش، اقداماتی انجام می‌دهد که همین موضوع تحقیق و تعقیب مجرم را به واسطه علوم جرم‌یابی تسهیل می‌نماید. به عبارت دیگر، مشخصه اصلی جرائم دنیای واقعی این است که این جرائم تابع محدودیت‌های فیزیکی هستند که بر فعالیت‌های انسان در دنیای واقعی حاکم است. زیرا ما محکوم به زندگی تحت این محدودیت‌ها هستیم و درک نمی‌کنیم که چگونه طبیعت، تلاش‌ها در راه ارتکاب جرم را مشکل‌تر می‌نماید. هر جرمی، حتی جرم‌های رایج مانند جیب‌بری و یا فروش مواد مخدر در خیابان، به سطحی از آمادگی، برنامه‌ریزی و تمرکز برای انجام موفقیت‌آمیز نیاز دارد. برای جرائم دنیای واقعی این فعالیت‌ها می‌بایست در فضای واقعی و فیزیکی انجام پذیرد.

بنابراین، کسی که تصمیم دارد که از یک بانک سرقت کند، باید آن بانک را در ابتدا بررسی کند و با قسمت مختلف آن مانند ورودی‌ها، خودپردازها، راه‌های فرار، سیستم‌های هشدار، محافظان، دوربین‌های کنترل و اینکه چه ساعتی کارکنان شروع بکار کرده و یا کار را ترک می‌کنند و چه ساعتی بانک مشتری کمتری دارد و چه ساعتی پول به بانک می‌آید، آشنا شود. این فرآیند دقت عموم را برای سارق افشاء می‌کند که می‌تواند منجر به بازداشت شدن او پس از ارتکاب جرم شود، در مورد سرقت نیز چنین است، هنگامی که سارق درون بانک است، می‌تواند از خود شواهدی را بر جای بگذارد که به دستگیر شدن او منجر می‌شود. در مورد فرار مجرم هنگامی که سرقت انجام شده است هم صادق است. مجدداً مجرم در ملأعام و انظار عمومی مشاهده شده و خطر شناسایی و تشخیص هویت وی بالا می‌رود. علاوه بر خطر مشاهده شدن که به علت برنامه‌ریزی و ارتکاب جرم پدید می‌آید، سارق احتمالاً نیاز به حمل سلاح و یا لباس‌های

مبدل دارد و شاید نیاز به پولشویی هم دارد. مانند فرآیندهای موجود در سرقت، هرکدام از این مراحل زمان‌بر است و نیاز به سعی و تلاش فراوانی دارد تا عملیات سرقت انجام گردد. لذا جرائم سنتی حتی پس از ارتکاب هم محدودیت‌های فراوانی از حیث اختفاء، فروش و نقل و انتقال اموال و امثال آن را به همراه دارد؛ ازاین رو، این آیتم‌ها خطر شناسایی شدن و دستگیر شدن مجرم را افزایش می‌دهد. (کرمی، ۱۳۹۴: ۷۱).

در واقع، جرائم سنتی از یک الگوی دموگرافیک و جغرافیایی معین پیروی می‌کنند. جرائم معمولاً در مکان‌های مشخص از یک شهر رخ می‌دهند. از طرف دیگر، گروه‌های انسانی که مرتکب جرم می‌شوند، قابل شناسایی هستند. جرائم در حد قابل شناسایی در یک حوزه مشخص جغرافیایی و دموگرافیک رخ می‌دهند. این امر نهادهای اجرای قانون را قادر می‌سازد تا نیروها و منابع خود را در مناطقی که جرائم احتمالاً واقع می‌شوند؛ متمرکز سازند و نسبت به ارتکاب آن‌ها، واکنش‌های به موقع و مناسب از خود بروز دهند. اما در محیط سایبر به دلیل عدم حضور فیزیکی مجرم در صحنه وقوع جرم، سبب می‌شود شیوه‌های کلاسیک کشف جرم و شناسایی مجرم با دشواری و یا کُندی صورت گیرد؛ و در غالب موارد مرتکب و بزه‌دیده هزاران کیلومتر از هم فاصله دارند و معمولاً بزهی که واقع می‌شود، بزهکار و بزه‌دیده ناشناس باقی می‌ماند و غالباً نیز دستگیر نمی‌شود. بنابراین، این خصیصه جرائم کلاهبرداری در فضای مجازی، روند جمع‌آوری ادله اثبات جرم را با مشکلات و محدودیت‌های خاص خود توأمان می‌سازد. از این رو، مفهوم متعارف زمان و مکان در فضای مجازی دچار تحول شده است؛ زیرا از جمله فاکتورهای کُندی وقوع پدیده مجرمانه در دنیای واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، بزه‌دیده و مکان ارتکاب بزه است. ساختار فضای سایبر به نحوی است که در آن قرابت مکان میان سه عنصر مذکور، ضرورتی ندارد. این وضعیت موجب صرفه‌جوییِ شگرفی از بعد زمان و هزینه بری بزهکاران سایبری گردیده و آن‌ها را قادر ساخته بدون وجود مانعی به نام مکان، جرائم متعددی را در سریع‌ترین زمان مرتکب شوند.

### ۱-۵- کثرت بزه‌دیدگان

در جرائم محیط واقعی معمولاً میزان جرم و تعداد بزه‌دیدگان غالباً مشخص است. برای مثال در جرائم محیط واقعی می‌توان آن را به چند فقره قتل، سرقت، کلاهبرداری یا امثال آن محصور نمود؛ در واقع جرائم در محیط واقعی در بسیاری موارد معدود و البته قابل شمارشند. البته این امر نیز یک قاعده محسوب نمی‌شود، چرا که در برخی اوقات این جرائم از جهت بزه‌دیده‌ای که دارد قابل شمارش نیست و اساساً رقم سیاه بزهکاری که در جرم‌شناسی از آن گفتگو می‌شود

اشاره به همین موضوع دارد. اما این امر در محیط سایبر امری طبیعی است. برای نمونه آنگاه که شخصی با نوشتن تنها یک برنامه متضمن حملات تخریب و اختلال در داده‌ها و سیستم‌های رایانه‌ای سبب می‌گردد که هزاران رایانه‌ی کارگزار در سطح جهان از ارائه خدمات باز بمانند عملاً مرتکب یک جرم شده است، لکن بزه‌دیدگانی پراکنده در سطح جهان دارد. چنین فضایی در واقع ارتکاب فعل واحد مجرمانه را که دارای نتایج متعدد است سبب شده است که خود از منظر تعدد جرم در حقوق کیفری قابل تدقیق است. بنابراین، در جرائم کلاهبرداری در فضای مجازی اولاً، تعداد بزه‌دیدگان معمولاً بسیار بالاست و شاید از مرز هزاران و میلیون‌ها نفر یا سامانه هم فراتر رود. ثانیاً، معمولاً نمی‌توان آمار دقیقی از تعداد بزه‌دیدگان داشت. چه، جرائم در شبکه شیوع می‌یابند و حالت اشاعه‌ی جرم ارتکابی که در بسیاری موارد به صورت خودکار صورت می‌گیرد، بسیاری از سیستم‌های رایانه‌ای و اطلاعات را درگیر خود می‌سازد و این امر قابل شمارش نیست لذا، نرخ ارتکاب جرم هم بالاست و در یک لحظه از زمان به میزان بسیار زیادی ممکن است واقع شود. از این رو، رویکرد کیفری در قلمرو جرائم کلاهبرداری در فضای مجازی با سختگیری بیشتری توأم است و مثلاً با مقدماتی‌ترین رفتارهای احتمالی که منجر به وقوع جرم بزرگ سایبری می‌شود، برخورد کیفری می‌نماید. امری که در جرائم سنتی معمول نیست. مانند جرم‌انگاری اعمال مقدماتی به عنوان جرم مستقل در قلمرو سایبر؛ که در حقوق کیفری سنتی اعمال مقدماتی اصولاً جرم نیست. به عنوان مثال دسترسی غیرمجاز به سیستم رایانه‌ای و یا نفوذ غیرمجاز که مقدمه اکثر جرایم کلاهبرداری در فضای مجازی محسوب می‌شود در حقوق ایران جرم‌انگاری شده است (روزبهان، ۱۳۹۵ : ۲۶)

## ۲- تحلیل نظری

در دومین قسمت از این مقاله به تحلیل نظری جرم‌شناختی ارتکاب جرایم کلاهبرداری در فضای مجازی خواهیم پرداخت. این مبحث براساس نظریهٔ چند عاملی «کوراکیس» در تبیین جرایم اقتصادی، در دو قسمت طراحی شده است.

به عقیده کوراکیس، بزهکاری ناشی از ترکیب عواملی نظیر شهرنشینی، توسعهٔ صنعت و فناوری و شخصیت بزهکار است (زراعت، ۱۳۹۵ : ۶۱) بدین ترتیب ابتدا به عوامل وضعی توجه خواهیم نمود و در این راستا به نقش توسعهٔ صنعت و فناوری نوین، فراگیری فضای مجازی، عمومی شدن استفاده از اینترنت توجه خواهیم نمود همه این عوامل باعث شده تا ابزارهای نوین از جمله نقل و انتقالات بانکی در فضای مجازی و بانکداری نوین به وسیله‌ای مجرمانه برای دستیابی به سودهای نامشروع و ارتکاب جرم به ویژه جرایم کلاهبرداری اینترنتی تبدیل شود. روش‌های استفاده شده در این قسمت با نظریات جرم‌شناسی عمل مجرمانه (تجربی) تبیین شده، جنبهٔ

علت شناختی ندارد و شگردهای بزهکاری را براساس شرایط و موقعیت بزه‌دیده و سبک ارائهٔ خدمات توضیح خواهد داد. در قسمت دوم، نظریات جامعه‌شناسی جنایی در رابطه با روش‌های ارتکابی جرایم کلاهبرداری اینترنتی نقد و ارزیابی خواهد شد. این نظریات جنبهٔ علت‌شناسی دارد و با تمرکز بر نوع آلت ارتکاب جرم در جرایم اقتصادی و از جمله کلاهبرداری اینترنتی مسائل را مطرح می‌نماید. بدین ترتیب در این دو قالب، روش‌های ارتکاب کلاهبرداری در فضای مجازی، با نظریات جرم‌شناسی مرتبط می‌گردد.

## ۲-۱- نظریه‌های مبتنی بر عوامل وضعی

بانک جهانی از وجود ۲۹/۱ شعبهٔ بانک در ایران به ازای هر یکصد هزار نفر خبر داده است. این تعداد شعبه، بالاتر از استانداردهای جهانی است و نشان دهنده‌ی عدم توسعهٔ بانکداری الکترونیک در کشور است. در عین حال، آمارهای بانک مرکزی حکایت از آن دارد که در شبکهٔ بانکی کشور تا پایان شهریور ۱۳۹۵، حدود ۳۵۰ میلیون کارت بانکی صادر شده و جمع تراکنش‌ها بالغ بر ۴۵۰ میلیون است[1] از این آمار، ۴۵۰ هزار کارت و ۵ میلیون تراکنش مربوط به شرکت دولتی پست بانک است. این شرکت، وظیفهٔ ایجاد و گسترش خدمات پست مالی در مناطق روستایی را بر عهده دارد. مقایسهٔ این آمارها نشان‌دهنده‌ی ماهیت شهری بانکداری الکترونیک است و از این لحاظ به رشتهٔ جامعه‌شناسی شهری مرتبط است. زیرا بانکداری الکترونیک از نظر اقتصادی به عنوان یکی از کارکردهای پایهٔ شهری مطرح است و در جامعه‌شناسی شهری به مباحث توسعهٔ اقتصادی نیز پرداخته شده است.

سیاست جنایی مقابله با جرایم اقتصادی و جرایمی که از طریق ابزارهای بانکداری الکترونیک رخ خواهد داد، باید «شهرمحور» بوده و با مقتضیات شهری تطابق داشته باشد. ویژگی شهرمحور بودن با نقش عوامل وضعی در ارتکاب جرم کلاهبرداری از طریق سرقت هویت، با ابزارهای بانکداری نوین در ارتباط است؛ چون رابطهٔ بین فقر و بیکاری با بزهکاری مطرح نیست، به نقش شخصیت بزهکار در گذر اندیشه به فعل نیز بی‌اعتناست و به بررسی ساختار اجتماع و محیط پیرامونی که شخص در آن زندگی می‌کند، خواهد پرداخت. به همین دلیل، کلاهبرداری از این طریق، با نظریهٔ فرصت تبیین خواهد شد. فرصت‌های ارتکاب جرم گاهی مربوط به افراد و گاهی مربوط به اشیا و اموال است (محمدنسل، ۱۳۸۶: ش۳/۳۰۴). رشد فناوری در صنعت بانکداری از جملهٔ فرصت‌های بزهکاری است که باعث تحول فعالیت‌های روزانهٔ مردم و ایجاد سیبل جاذبه‌دار گردیده و عدم حفاظت و مراقبت از سیبل را

---

۱. آمار منتشرشده در وبگاه بانک مرکزی به نشانی www.cbi.ir

جرم‌زا کرده است (فیشر و لب، ۲۰۹/۱۳۹۳:۱) به همین دلیل، ویژگی شهرمحور بودن، با دو نظریهٔ مشهور به انتخاب عقلانی: «نظریهٔ فعالیت روزانه» و «نظریهٔ شیوه و سبک زندگی» مرتبط است (صفاری و کونانی، ۱۳۹۲: ۱۱۳). در نظریه‌های مشهور به گزینهٔ عقلانی، انسان مجرم به عنوان یک انسان مقتصد، محاسبه‌گر و معقول ترسیم و مطالعه شده است. مجرم در این نظریه کسی است که هزینه‌های ارتکاب جرم را سنجیده و سپس انتخاب خواهد کرد. انتخاب بزهکار براساس موقعیت، سن، شغل و هویت اجتماعی بزه‌دیده شکل می‌گیرد (ویلیامز و دیگران، ۱۳۹۸: ۲۴۲).

کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. به عبارت دیگر پیشگیری وضعی بر وضعیت ماقبل جرم تمرکز می‌کند و با فرآیند گذار از اندیشه به عمل مواجه است، پیشگیری وضعی درصدد تغییر در اوضاع و احوال مشرف بر جرم است به منظور اینکه معادله جرم به ضرر مجرم تمام شود. از این رو در ادامه به مهترین نظریه هایی که امکان پیشگیری وضعی را میسر می‌سازد و بر عوامل وضعی در بحث ارتکاب جرایم کلاهبرداری در فضای مجازی مؤثر است اشاره خواهیم نمود.

### ۲-۱-۱- نظریه فعالیت روزانه

نظریه‌ی فعالیت روزانه بر این فرض استوار است که رخ دادن جرم تنها هنگامی امکانپذیر است که بزهکار با انگیزه‌ای با بزه‌دیده‌ی مناسبی بدون حضور مراقبی توانمند تماس برقرار کند. بسیاری از پیشرفت ها و اصلاحات اخیر این نظریه درباره مدیریت کارآمد یک مکان برای از میان بردن شرایط مناسب برای وقوع جرم است. برای نمونه، با اینکه برخی از پژوهش‌ها دریافته‌اند که وجود میکده‌ها بسیار بخت ارتکاب جرم را افزایش می‌دهند اما پژوهش‌های دیگری هستند که نشان می‌دهند که تنها برخی از میکده‌های دارای مجوز هستند که به میزان نامتناسبی، تماس‌های درخواست خدمات پلیسی را دارند. نظریه‌ی فعالیت روزانه، به طور خیلی خلاصه، نشان می‌دهد که بسیاری از ساختارهای فرصت‌ساز جرم با فعالیت‌های روزانه‌ی اجتماعی مشخص می‌شوند و بیشتر زمان بزهکاران نیز در جریان فعالیت‌های روزانه مانند کار یا رفت و آمد سپری می‌شود.

در بحث کلاهبرداری‌های اینترنتی نیز باید توجه داشت که از جمله شیوه‌هایی که در بانکداری نوین از دیدگاه بزه‌دیدگان قابل بررسی است، روش‌های غیر فنی دسترسی به گذرواژه به شیوه انواع مهندسی اجتماعی مبتنی بر انسان است. در این شیوه، بزه‌دیده به عنوان عامل شتاب‌دهنده و اثرگذار در ارتکاب جرم مطرح است و در شکل‌گیری و عملی نمودن اندیشهٔ مجرمانه، موجب تسریع در حرکت فرآیند جنایی خواهد شد. در نظریهٔ فعالیت روزانهٔ مطرح شده، تحولات اقتصادی که از طریق رشد فناوری و صنعت به وجود آمده، سبب تحول

فعالیت‌های روزانهٔ مردم شده است. از جملهٔ این تحولات، ارائهٔ خدمات بانکی بدون مراجعه به شعب بانک است. دستگاه‌های خودپرداز، کارت‌خوان‌های فروشگاهی یا درگاه‌های اینترنتی بانک از طریق کارت بانکی یا رمز عبور (گذرواژه) خدمات مالی ارائه می‌کنند. یکی از شیوه‌هایی که در بانکداری نوین، بزه‌دیده به عنوان علت ارتکاب جرم مطرح است، شیوه مهندسی اجتماعی است. در شیوه مهندسی اجتماعی مبتنی بر انسان از بی‌احتیاطی یا اطمینان بیش از حد انسان‌ها برای جمع‌آوری اطلاعات حساس استفاده شده است. با این توضیح، شیوه‌هایی که براساس این نظریه رخ داده، بررسی خواهد شد.

در روش خالی کردن حساب از طریق جستجو در زباله‌های بانکی، رئیس پلیس فتای تهران از دستگیری جوانی با مدرک کارشناسی خبر داد. وی کسانی را که در بانک اقدام به افتتاح حساب و دریافت کارت بانکی می کردند، شناسایی و تعقیب می کرد. هنگامی که این مشتریان برای تعویض رمز کارت خود به دستگاه خودپرداز مراجعه می‌کردند و پاکت حاوی رمز اولیهٔ کارت را باز کرده و به سطل زباله می‌انداختند، او این کاغذ را برداشته و با استفاده از اطلاعات درج شده (شامل رمز اول و دوم کارت) اقدام به برداشت اینترنتی می‌نمود و خرید اینترنتی کرده بود. در این رابطه رئیس پلیس فتای استان خراسان رضوی هشدار داد که در خریدهای آنلاین، تحت هیچ شرایطی از رمزهای اینترنتی در حضور دیگران استفاده نشود و در صورت اجبار، بلافاصله رمز تغییر داده شود.

روش دیگر، پرسه زنی در کنار دستگاه‌های خودپرداز بانک‌ها با نیت کمک به افراد مسن و بیسواد است. در پرونده نیکوکار قلابی، رئیس پلیس فتای استان فارس اعلام کرد که نیکوکار قلابی پس از جلب رضایت مراجعان و اخذ عابربانک به همراه رمز کارت، در یک فرصت مناسب اقدام به فعال‌سازی رمز دوم حساب (رمز اینترنتی) کرده و پس از ترک محل، کل حساب قربانیان خود را خالی نموده است. در روش دیگر، اداره نظام‌های پرداخت بانک مرکزی، نسبت به روش فیشینگ تلفنی هشدار داد و اعلام نمود که افرادی طی تماس تلفنی با برخی از مشتریان بانک، خود را به عنوان نماینده بانک در امور فناوری اطلاعات و خدمات الکترونیک معرفی کرده و به شیوه‌های گوناگون، مبادرت به اخذ اطلاعاتی نظیر رمز اول و دوم حساب بانکی و کلاهبرداری نموده‌اند.

### ۲-۱-۲- نظریه سبک زندگی

لارنس کوهن[1] و مارکوس فلسون[2] در سال ۱۹۷۹ نظریه سبک زندگی روزمره بزه‌دیدگان را با الهام از دیدگاه‌های مطروحه در نظریه انتخاب خردگرا که چهارچوبی برای فهم و اغلب تقلید و مدل سازی رفتارهای اجتماعی و اقتصادی است، مطرح نمودند (Miller, 2006: 81). کوهن و فلسون تعداد و طبیعت اعمال مجرمانه را به کمک «امکانات که بزه دیدگان بالقوه، از راه سبک زندگی خود برای تحقق بخشیدن به عمل مجرمانه در اختیار بزهکاران قرار می‌دهند» بیان می‌کنند. بدین نحو که، در بادی امر یک فرض ابتدایی وجود دارد که به موجب آن تحقق جرایم مستلزم برخورد دو عامل در زمان و مکان است: بزهکاران بالقوه و هدف‌های حمایت نشده. نظریه سبک زندگی روزمره سه رکن اصلی دارد که عبارتند از: ۱- یک مجرم تحریک شده: کسی که به اندازه کافی برای ارتکاب جرم برانگیخته شده باشد؛ ۲- هدف مناسب: که باید دارای ارزش، سکون، دید و دسترسی باشد.۳- فقدان محافظان توانا: محافظانی که از تحقق جرم در زمان فعالیت‌های روزمره مردم، که هر روز نیز تکرار می‌شوند، جلوگیری کنند (مالمیر؛ زررخ، ۱۳۸۹ : ۷۱ ). شایان ذکر است که بر مبنای این نظریه، برای تحقق جرم می‌بایست انحرافی در مکان یا زمان یکی از این سه رکن به وجود آید.

از منظر دیدگاه مربوطه یکی از سه رکن اصلی در تحقق بزه‌دیدگی سایبری نقش عمده بازی می‌کند و آن فقدان حفاظت است؛ و دو رکن دیگر نیز عوامل وضعی اثرگذار هستند. بدین معنا که در فضای سایبر گروه‌های مجرمان با انگیزه می‌توانند هدف‌های مناسبی را از کاربرانی که به اینترنت وصل می‌شوند، پیدا کنند. (Yar, 2005: 417) بدین خاطر است که فلسون در نظریه سبک زندگی بیان می‌دارد که مناسب بودن هدف نشانگر چهار ضابطه است: ۱. ارزشمند بودن؛ ۲. استیصال هدف جرم؛ ۳. قابلیت رؤیت هدف جرم؛ ۴. دسترسی به هدف جرم، که بررسی چهار عنصر در فضای مجازی به خوبی این واقعیت را که مناسب بودن هدف در فضای سایبر امری مفروض است، به اثبات می‌رساند.

به عنوان مثال هنگامی که کاربری به اینترنت متصل می‌شود، رایانه وی اطلاعاتی را به فضای مجازی منتقل می‌کند که سبب جذب مجرمان سایبری می‌شود؛ به دیگر سخن از زمان اتصال اشخاص به اینترنت و حضور فرد در فضای مجازی، نحوه عملکرد و نوع و میزان تبادل اطلاعات از طرف ایشان، مجرمان سایبری را به سوی این قبیل افراد می‌کشاند تا شاید با یافتن راهی هر چند کوچک وی را قربانی نیات پلید خویش سازد. علاوه بر این ویژگی‌های محیط سایبر در رابطه با قابل رؤیت بودن و نیز در دسترس بودن، سبب شده است تا بزهکاران در جرایم کلاهبرداری اینترنتی در هر نقطه‌ای از جهان امکان معین کردن اهداف و ارتکاب جرم نسبت به آنان را داشته

1. Lawrence Cohen
2. Marcus Felson

باشند؛ بدین نحو که بزهکاران قربانیان خود را با ثبت اطلاعات سیستم آن‌ها و علی‌الخصوص پروتکل اینترنتی سیستم‌شان ردیابی و شناسایی کنند و از این طریق آن‌ها را مورد سوءاستفاده قرار دهند.

بنابر آنچه گفته شد می‌توان به راحتی سه عامل مجرم تحریک شده، هدف مناسب و فقدان محافظ توانا را در واقع شدن کلاهبرداری اینترنتی ترسیم نمود و از این طریق تطابق نظریه سبک زندگی روزمره را با بزه‌دیدگی در جرایم کلاهبرداری اینترنتی تبیین کرد، به دیگر سخن در فضای مجازی به علت وجود فرصت‌های ارزشمند مالی و نیز نبود جهان مادی و فیزیکی و ویژگی پنهان شدن و اختیار نمودن هویت‌های گوناگون، تحریک‌پذیری در ارتکاب جرم، برای بسیاری از بزهکاران بالقوه و بالفعل فراهم است و ایشان را به ارتکاب کلاهبرداری در فضای مجازی سوق می‌دهد.

بنابر آنچه در بالا گفته شد، نظریه سبک زندگی و فعالیت روزانه راهکار عملی‌ای را ارائه می‌کند که به وسیله آن پیشگیری وضعی از جرایم کلاهبرداری در فضای مجازی با تکیه بر تغییر شرایط و اوضاع و احوال میسر خواهد بود که خود بخشی از نظریه‌های مطرح شده در رابطه با پیشگیری وضعی از جرایم سایبری است (جلالی فراهانی، ۱۳۸۴ : ۱۶۱)

## ۲-۲- نظریه‌های مبتنی بر عوامل اجتماعی

در رابطه با کلاهبرداری در فضای مجازی، شرایط ایجادکننده توسعهٔ نوآوری‌های فنی مانند توسعهٔ پرداخت و دریافت پول با کارت بانکی است که موجب شکل‌گیری شرایط ایجادکننده دروغ گردیده و ارتکاب جرم کلاهبرداری را با نظریهٔ فرصت تبیین کرده است؛ زیرا در وضعیت کنونی، استفاده از فناوری‌های نوین اطلاعاتی با توسعه و رشد قابل توجه فرصت‌های کلاهبرداری قابل توجیه است.

اما باید خاطرنشان ساخت که اگر این اوضاع و احوال، اثر افزایشی بر برخی از اشکال دروغ داشته باشد، همه مرتکب آن نمی شوند. بی‌تردید شخصیت مرتکب در اینجا بی‌تأثیر نیست. در هر حالت، شرایط و اوضاع و احوال باید گذر از اندیشه به فعل را اجازه دهد. اینجاست که نوع دوم اوضاع و احوال یعنی شرایط محقق کننده ظاهر خواهد شد (پیشین: ۱۴۳ـ۱۴۷). شکل‌گیری این نگرش در ذهن همان چیزی است که دیوید متزا آن را فنون خنثی‌سازی نامیده است. فنون خنثی‌سازی نوعی توجیه‌سازی آگاهانهٔ اعمال مجرمانه است (پیشین: ۱۰۵). با این مقدمه به تحلیل و بررسی ارتکاب کلاهبرداری در فضای مجازی پرداخته خواهد شد. توضیح این روش‌ها بر پایهٔ نظریات جرم‌شناسی مبتنی بر عوامل اجتماعی

است که برخلاف نظریات عقلانی محور به علل اجتماعی و محیطی پرداخته خواهد شد و ساختار شکل‌گیری دروغ و چگونگی کاربرد آن در این جرایم را نشان خواهد داد.

### ۲-۲-۱- نظریه خنثی‌سازی و هک کردن

دیوید ماتزا و گریشام سایکز در نظریهٔ خنثی‌سازی به فرآیند بدل شدن جرم به یک تجربهٔ آموزشی توجه کرده‌اند. (Seigel. j Larry,2003: 232 به نقل از زررخ، ۱۳۸۹) این دو استدلال می‌کنند که تمام مجرمان ارزش‌های مرسوم و گرایش‌هایی مانند افراد عادی دارند، اما چیزی که آن‌ها را از دیگران متمایز می‌کند، توانایی غیرعادی آن‌ها در حرکت از زندگی عادی به ایجاد ارزش‌های پنهانی موازی از طریق فنون خنثی‌سازی ویژه مانند انکار مسئولیت، آسیب و قربانی است.

این اقدام به مجرمان کمک می‌کند تا وجدان اخلاقی خویش را پاک کنند و احساس گناه نکنند. اسپافورد سه توجیه اخلاقی را برای هک فهرست کرده است: بهبود امنیت با کشف حوزه‌های نفوذ، کسب آگاهی توسط دانشجویان و حمایت از جامعه در برابر شرکت‌ها از طریق تضمین دسترسی رایگان به اطلاعات. گروه‌های همتا، با افراط در تشویق سوءاستفاده‌های هکری افراد و ایجاد این گمان که این فعالیت‌ها توجیه شده‌اند، در این رهایی اخلاقی شرکت می‌کنند. راجر گزارش داده که: «خودسانسوری می‌تواند موجب رهایی یا ضعف از طریق تهی شدن قربانی از صفات انسانی، یا تبدیل شرمندگی به قربانی شود ... شرمندگی ناشی از قربانی شدن یا برخی شرایط به مرتکبان اجازه می‌دهد خودشان را قربانیان تحریک شده ببینند. اکنون اعمال مرتکبان به عنوان یک حالت تدافعی تعبیر می‌شود. قربانیان شرمنده و به دلیل ارتکاب افعال مجرمانه علیه خودشان متهم می‌شوند (Rogers,2001:40).

در وقوع جرایم کلاهبرداری اینترنتی که توأم با هک سیستم‌ها است. غالباً هکرها اداره‌کنندگان سیستم را به خاطر امنیت نامناسب آن یا برای جلوگیری از دسترسی به سایت‌هایی که بطور قانونی فکر می‌کنند باید به آن‌ها دسترسی داشته باشند، سرزنش می‌کنند، مانند اداره‌کنندهٔ سیستم دانشگاهی که مانع دسترسی به سایت‌های پیاده‌سازی فیلم می‌شود، دستاویزی برای هک کردن به شمار می‌آید، زیرا سرگرمی کم هزینه و جزء ضروری زندگی یک دانشجو از سوی هکرها تلقی می‌شود. هکرها فروشندگان نرم افزار را به دلیل محدود کردن دسترسی به جریان آزاد اطلاعات سرزنش می‌کنند و بنابراین، از نظر اخلاقی فعالیتشان را به عنوان یک عمل سودمند و به منظور تضمین اطلاعات برای همه توجیه می‌کنند و خود را سلحشوری که به بینوایان کمک می‌کند، نشان می‌دهند. این رفتار سندروم محبوب «رابین هود» را نشان می‌دهد که افراد قضاوت اخلاقیشان را خنثی می‌کنند (Harrington,2002: 179). خرده فرهنگ‌های

هکر در اینترنت تقویت می‌شوند و نمونه‌هایی از فرهنگ نهانی مشابه را که بطور عمومی از فعالیت‌های غیرقانونی هک کردن حمایت می‌کند، ارائه می‌دهند. بنابراین، درست است که نتیجه بگیریم نظریهٔ خنثی‌سازی ماتزا و سایکس، با موفقیت رفتار هکر در ارتکاب کلاهبرداری در فضای مجازی را از دیدگاه یک کلاهبرداری سایبری توضیح می‌دهد.

## ۲-۲-۲- نظریه عمومی فشار رابرت اگنو

نظریهٔ عمومی فشار، از رویکرد اجتماعی ـ روان‌شناختی پیروی می‌کند و پیوند بین منابع فشار، احساسات منفی ناشی از فشار و رفتار مجرمانهٔ فردی را بررسی می‌کند. به بیان دیگر، رابرت اگنو مفهوم فشار را فراتر از رویکرد مرتون بسط داد و به جای تأکید صرف بر فشارهای اقتصادی مدنظر مرتون، چندین منبع فشار را معرفی کرد که ممکن است منجر به حالات یا احساسات منفی به ویژه خشم شده و در نهایت منجر به رفتارهای ضد اجتماعی گردد. نظریهٔ عمومی فشار، قابل تعمیم برای کلیهٔ افراد طبقات ضعیف، متوسط و ثروتمند است و از این جهت نیز نسبت به نظریهٔ مرتون عمومیت دارد. اما نکتهٔ مشترک در هر دو نظریه، نوآوری مجرمانه برای دستیابی به اهداف مادی است (نجفی ابرندآبادی و صادق نژاد نائینی، ۱۳۹۲: ۱۳) که برخی شیوه‌های جعل هویت از این طریق را قابل تحلیل کرده است و در ذیل خواهد آمد. نوآوری‌های مجرمین کلاهبردار در فضای مجازی عموماً به دو شیوه نوآوری در رفتار و نوآوری در امور فنی می‌تواند اتفاق بیفتد به عنوان مثال در بحث نوآوری در رفتار، این مجرمین با شناخت شرایط اجتماعی و هوشمندی زمانی اقدام به طراحی نقشه‌ها خود در فضای مجازی و فریب قربانیان خود می‌نمایند. به عنوان مثال یک مقام انتظامی در تشریح شیوه کار این مجرمان سایبری بیان داشت: در ایام عید فطر و یا ایام عید نوروز کلاهبرداران با طراحی سایت‌های جعلی و دروغین به عنوان مؤسسات و سازمان‌های شناخته شده و معتبر؛ با اعلام شماره حساب‌های شخصی، متقاضی واریز وجوهات به اینگونه حساب‌ها هستند.این افراد سودجو، با ترفند خیرین و راه‌اندازی صفحات شخصی در بستر شبکه‌های اجتماعی و پیام‌رسان‌ها و سوءاستفاده از نام و اعتبار افراد مشهور و شناخته شده در کشور شامل هنرمندان، ورزشکاران و سرشناسان کشور با انجام مهندسی اجتماعی نظیر تحریک احساسات هموطنان و تهیه کلیپ‌های تصویری شامل فیلم و عکس از نیازمندان، محرومان و خانواده‌های کم بضاعت مدعی دریافت وجوه نذورات به منظور کمک‌رسانی به افراد آسیب‌پذیر و نیازمند می‌شوند و از این طریق مبالغ کلانی را از افراد بسیار زیاد کلاهبرداری می‌نمایند به گونه‌ای که شاید فرد هیچگاه حتی نداند که یک بزه‌دیده جرم کلاهبرداری در فضای مجازی بوده است.

در نوآوری‌های فنی نیز عموماً هک و نفوذ به سیستم‌ها و تلفن‌های همراه مالباختگان اتفاق می‌افتد که این نفوذ ممکن است از طرق مختلف واقع شود. به عنوان مثال کلاهبرداران اینترنتی با ساخت و بارگذاری نرم‌افزار موبایلی ماهواره جیبی در کانال‌ها و گروه‌های تلگرامی که در قالب دانلود رایگان ارائه شده، اقدام به کلاهبرداری از کاربران می‌کنند.استفاده و فعال‌سازی قابلیت‌های این نرم‌افزار مستلزم پرداخت اینترنتی مبلغی از سوی مشتریان است که می‌تواند کاربران را به صفحه جعلی و شبیه‌سازی شده یک بانک هدایت کند که این اتفاق نهایتا منجر به سرقت اطلاعات حساب بانکی کاربران نظیر شماره کارت، رمز اینترنتی و تاریخ انقضای کارت برای کلاهبرداران می‌شود.[1]

## ۲-۲-۳- نظریه یادگیری اجتماعی

نظریه‌های یادگیری اجتماعی نظیر معاشرت‌های ترجیحی ساترلند، نظریهٔ فراگیری اجتماعی آلبرت بندورا و نظریهٔ خنثی‌سازی ماتزا، جرم را محصول یادگیری هنجارها، ارزش‌ها و رفتارهای مرتبط با فعالیت جنایی می‌دانند. این یادگیری شامل فراگیری دانش مرتبط با فنون ارتکاب جرم و رهایی اخلاقی به وسیلهٔ کشف توجیهات منطقی مناسب برای رفتارهای مجرمانه است.

براساس این نظریات، چون برخی روش‌های جعل هویت فنی است، به صورت اکتسابی باید فرا گرفته شود. این فراگیری شامل رفتار جزایی و فنون ارتکاب است و از طریق ارتباط معمولی با گروه‌های صمیمی انتقال می‌یابد. چون آثار منفی رفتار به منظور بازدارندگی مجرم در محیط ارتکاب ضعیف است، در طول زندگی فرد حفظ خواهد شد. آنچه در نهایت باعث بدل شدن این تجربهٔ آموزشی به جرم خواهد شد، ایجاد ارزش‌های پنهانی موازی است. انکار مسئولیت و آسیب به قربانی از جملهٔ این موارد است که باعث خواهد شد مجرم وجدان اخلاقی خود را پاک کرده و احساس گناه نکند (دالال و شارما، ۱۳۸۸: ۴۳۵ـ۴۴۰).

از جمله روش‌های فنی جعل هویت، مهندسی اجتماعی مبتنی بر رایانه است. ابزار استفاده شده رایانه است، صفحات جعلی یا «فیشینگ» یا «رمزگیری»، از این دست مهندسی اجتماعی است که سبب افشای کلمهٔ عبور یا گذرواژه کاربر می‌شود و پس از آن نفوذگر خواهد توانست به عنوان کاربر مجاز و از طریق درگاه‌های بانکی، اقدام به کلاهبرداری نماید. سرپرست اداره پیشگیری مرکز تشخیص و پیشگیری پلیس فتا نیز اعلام نمود که ۶۰ درصد جرایم سایبری در حوزه جرایم مالی و از طریق سرقت اطلاعات کارت‌های بانکی رخ داده است و روش ارتکاب، توسل به انتشار تبلیغ تخفیف‌های باورنکردنی، حراج کالاها یا فروش کالا از طریق

---

[1] . https://irancyberlawyer.ir

فروشگاه‌های اینترنتی است؛ به طوری که با این روش، افراد متقاضی خرید را به سمت صفحات جعلی درگاه‌های بانکی هدایت می‌نمایند و آنگاه اطلاعات بانکی خریدار به راحتی در اختیار فیشرها قرار خواهد گرفت. این روش که از شایع‌ترین روش‌های دسترسی به گذرواژه است، این امکان را برای مجرمان فراهم می‌سازد که بتوانند دامنهٔ ارتکاب جرم را از لحاظ کمی و کیفی ارتقا ببخشند؛ چون درگاه‌های جعلی بسیار شبیه درگاه‌های پرداخت بانک‌ها هستند و باعث فریب کاربران و در اختیار قرار دادن اطلاعات حساب بانکی آن‌ها خواهند شد. از طرف دیگر، برخلاف کلاهبرداری‌های سنتی که تحصیل مال محدود به موجودی بزه‌دیده است، مجرمان رایانه‌ای قادرند با ایجاد مبالغ و موجودی‌های واهی و غیر واقعی از مقدار حساب‌های موجود نیز فراتر روند و با روش اصطلاحاً برش کالباسی، خسارت‌های قابل توجهی وارد نمایند (زیبر، ۱۳۹۰: ۷۷).

شیوه دریافت امواج از طریق درگاه‌های حضوری نیز امکانپذیر است. دستگاه خودپرداز و پایانهٔ فروش مانند هر رایانه‌ای امواج الکترومغناطیسی ساطع می‌کند که به آن «نشت الکترونیکی»[1] گفته می‌شود. به محض فشردن هر یک از کلیدهای صفحه کلید، امواج از طریق سیستم‌های حامل جریان الکترونیکی در محیط اطراف منتشر می‌شود که به وسیلهٔ تجهیزات خاصی قابل شنود و آشکارسازی است. چون صفحهٔ نمایشگر کاربر برای نفوذگر قابل رؤیت نیست، پیش‌بینی رمز عبور یا کد عبور متنی یک تدبیر امنیتی ضد شنود است.

## نتیجه‌گیری

در مقاله حاضر در پی آن بودیم تا از دیدگاه جرم‌شناسی نظری موضوع گسترش ارتکاب جرایم کلاهبرداری اینترنتی را مورد بررسی و تحلیل قرار دهیم. اساساً برخی از علل اساسی ارتکاب جرم در فضای مجازی، ناشی از مختصات و زیر ساخت‌های سخت‌افزاری و نرم‌افزاری فضای مجازی است ویژگی‌های این فضا همچون گمنامی، دیجیتالی بودن، مبتنی بر زمان مجازی بودن، جهانی بودن، سرعت، فراگیری، سیالیت، تشدید شدگی، متکثر بودن و در نهایت همه جا حاضر بودن، خود به خود فضایی را ایجاد میکند که اثرات اولیه و ثانویه آسیب در جهان دو فضایی را تشدید و تقویت می‌کند. گمنامی و ناشناختگی از اصول حاکم بر جرائم جهان مجازی است. نامرئی بودن این امر را به افراد می‌دهد که به هر کجا می‌خواهند سرک بکشند و کارهایی انجام دهند که در دنیای واقعی انجام نمی‌دهند. فضای مجازی علاوه بر ابزار قوی برای ارتکاب جرم، فرصت‌های

1. Electronic emanation

ارتکاب را نیز افزایش می‌دهد. از ویژگی‌های دیگر این فضا براساس نظرات سهل‌الوصول بودن و سرعت ارتکاب جرائم است. مجرمین سنتی اغلب در فرآیند گذار از اندیشه به عمل و ارتکاب یک جرم تام، زمان و فاصله زیادی را طی می‌کردند. شاید یکی از عوامل کندی وقوع پدیده بزهکارانه در جهان واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. حال اینکه ساختار فضای مجازی به گونه‌ای است که در آن قرابت مکانی میان سه عنصر فوق ضرورتی ندارد. لذا امروزه به مدد تکنولوژی‌های نوین، مرتکب اغلب با یک کلیک می‌تواند به عرصه ارتکاب جرم راه پیدا کند. مثلا در ارتکاب جرم کلاهبرداری دیگر به عوامل و ارکان خاص این جرم در دنیای فیزیکی از جمله مانورهای خاص متقلبانه و تعاملات رودرروی افراد با هم نیازی نیست. چرا که سایبر امکان بردن اموال دیگری را به سادگی فشردن تنها چند کلید و انجام عملیاتی پیش پا افتاده ممکن ساخته است. تحلیل نظری صورت پذیرفته در این مقاله که براساس نظریهٔ چندعاملی «کوراکیس» انجام پذیرفت هم از دیدگاه نظریه‌های مبتنی بر عوامل وضعی (نظریه فعالیت روزانه و نظریه سبک زندگی) و هم نظریه‌های مبتنی بر عوامل اجتماعی (نظریه خنثی‌سازی و هک کردن، فشار رابرت اگنو و یادگیری اجتماعی) ضمن تأیید ویژگی‌های خاص فضای مجازی در وقوع این جرایم بر نقش بزه‌دیدگان، شیوه و شگردهای نوین ارتکاب جرم، نقش عوامل اجتماعی و سبک زندگی در وقوع جرایم کلاهبرداری اینترنتی نیز تأکید داشتند. از این رو به نظر می‌رسد در راستای پیشگیری از ارتکاب جرایم مذکور تمرکز همزمان بر عوامل فردی، محیطی و اجتماعی تاحد زیادی می‌تواند به کنترل ارتکاب جرایم کلاهبرداری رایانه‌ای در فضای مجازی بیانجامد.

## تشکر و قدردانی

پژوهشگران، از عزیزانی که در فرآیند ویراستاری ادبی و صفحه‌آرایی این مقاله همکاری و راهنمایی داشتند، کمال تشکر و امتنان را دارند.

## منابع


- پیکا، ژرژ (۱۳۹۰). **جرم‌شناسی**، ترجمه علی حسین نجفی ابرندآبادی، تهران: میزان.

- جلالی فراهانی، امیرحسین (۱۳۸۴). **پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر**، فصلنامه فقه و حقوق، سال دوم، شماره۶.

- حسن بیگی، ابراهیم (۱۳۸۴). **حقوق و امنیت در فضای سایبر**، تهران: مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر.

- دالال ، ا. اس .؛ راقا، شارما (۱۳۸۸). **نیم نگاهی به ذهن هکرها: آیا نظریه‌های جرم‌شناسی می‌توانند هک کردن را تبیین کنند؟**، ترجمهٔ احسان زررخ ، روزنامهٔ رسمی کشور (مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات).

- روزبهان، فاطمه (۱۳۹۵). **بررسی جرم جعل و کلاهبرداری رایانه‌ای (از سال ۹۳ -۹۴) از دیدگاه کارشناسان و قضات دادسرای جرایم رایانه‌ای استان تهران**، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی.

- زراعت، عباس (۱۳۹۵). **حقوق کیفری اقتصادی**، تهران: انتشارات جنگل.

- زررخ، احسان (۱۳۸۹). **جرم‌شناسی فضای مجازی**، پایان‌نامه کارشناسی ارشد، موسسه آموزش عالی شهید اشرفی اصفهانی.

- زیبر، اولریش (۱۳۹۰). **جرائم رایانه‌ای**، چاپ دوم، تهران، انتشارات گنج دانش.

- فیشر، بونی اس . و استیون پی . لب (۱۳۹۳). **دانشنامهٔ بزه‌دیده‌شناسی و پیشگیری از جرم**، ترجمهٔ اساتید حقوق کیفری و جرم‌شناسی سراسر کشور، زیر نظر علی حسین نجفی ابرندآبادی، تهران، میزان.

- کرمی، داود (۱۳۹۴). **سیاست افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران**، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق دانشگاه قم.

- گرایلی، محمدباقر (۱۳۸۹). **بررسی جعل و تخریب و اخلال رایانه‌ای**، آموزه‌های حقوقی، شماره ۱۴.

- مالمیر، محمود؛ زررخ، احسان (۱۳۸۹). **پیشگیری از بزه‌دیدگی سایبری**، فصلنامه مطالعات پیشگیری از جرم، سال ۵، شماره۱۷.

- ویلیامز؛ فرانک پی، ماری لین دی،مک شین (۱۳۹۸). **نظریه‌های جرم‌شناسی**، ترجمه حمیدرضا ملک محمدی، تهران: نشر میزان.

- Brenner, Susan, W. Rico, CCE, and other Complex Crime: Traus formation of American Criminal Law, 2wm&mary billrts.j, 1993.

- Brenner, W.S. (2010). Cybercrime criminal threats from cyberspace. Santa Barbara: Praeger.

- Cooter Robert & Thomas Ulen, Law and Economic, Harper Collins publisher, 2004.

- R.Vaca John, 2002, Computer Forensics, Computer Crime Scene Investigation, Chorles River Media.

- Rizgar, Mohammed Kadir, The Scope and the Nature of Computer Crimes Statutes, German Law Journal, Vol.11, No.06, 2010.
- Rogers, Marcus (2001), "A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study", University of Manitoba, Canada
Steven A.Egger, Linkage Blindness: A systemic Myopia, in 8 serial murder: an Elusive Phenomenon, 1990.
- Yar, M. (2005). The novelty of 'cyber crime': An assessment in light of routine activity theory. European Society of Criminology, 2.