

## تبیین سرقت هویت در نظام کیفری ایران

الهام سلیمان دهکردی<sup>۱</sup>، ارشیاناز حیدریان<sup>۲</sup>

### چکیده

سرقت هویت یک رفتار تهدید آمیز نوظهور است که با استفاده از اطلاعات اشخاص صورت می‌گیرد و منجر به ضررهای غیر قابل جبرانی در حوزه‌های مختلف خصوصا در حوزه مالی می‌شود. سرقت هویت زمانی صورت می‌گیرد که یک فرد اطلاعات شخصی دیگری از قبیل شماره کارت بانکی، شماره حساب، نام و نام خانوادگی آن را متعلق به خود قلمداد کرده و از آن‌ها به منظور برداشت از حساب بانکی، افتتاح یک کارت اعتباری جدید یا انجام سایر فعالیت‌های غیرقانونی، استفاده و بهره برداری کند. در ایران قانون گذار تحت مقرر قانونی مستقل به جرم انگاری این رفتار در فضای واقعی و سایبری دست نیازیده است و مرتکب را تنها با تمسک به مقرره‌های عامی چون غصب عنوان، سرقت رایانه‌ای و یا کلاهبرداری رایانه‌ای و غیره می‌توان کیفر نمود در حالی که رفتار فیزیکی این مقرره‌ها چندان شباهتی به سرقت هویت ندارد. ایالات متحده آمریکا اولین کشوری است که به این رفتار وصف مجرمانه مستقل بخشیده است. در این کشور قانون گذار در سال ۱۹۹۸ در قانون فدرال سرقت هویت به جرم انگاری این رفتار پرداخت.

**واژگان کلیدی:** سرقت هویت، غصب عنوان، استبدال هویت دیگری، نظام تقنینی ایران.

۱- دکتری حقوق کیفری و جرم شناسی از دانشگاه علامه طباطبایی soleiman.elham@gmail.com

۲- کارشناس ارشد حقوق جزا و جرم شناسی (نویسنده مسئول) hydrn.rsh@gmail.com

## مقدمه

در سده‌های گذشته استفاده از فضای عینی و ملموس تنها فضای مساعد برای ارتکاب جرم به حساب می‌آمد اما امروزه استفاده از فضای سایبر به دلیل انباشت آن از اطلاعات اشخاص در کنار فضای عینی چالش جدیدی را در کیفیت ارتکاب جرم به وجود آورده است. اطلاعات در این فضا به دلیل سه ویژگی منقول بودن، دگرگون پذیر بودن و پویا بودن در معرض آسیب‌های گوناگونی قرار دارند که یکی از این آسیب‌ها، سرقت هویت است. فرایند سرقت هویت به این صورت است که مرتکب ابتدا اطلاعات اشخاص اعم از مالی و یا شخصی را با تکیه بر شیوه‌هایی چون دلالتی اطلاعات، سوءاستفاده از وب سایت کارمندان، فریب دادن مرورگرها و غیره جمع‌آوری نموده و سپس خود را به جای فرد صاحب اطلاعات قلمداد می‌کند و از آن اطلاعات جهت مقاصد سوء خود من جمله کلاهبرداری استفاده می‌کند. تسمیه این رفتار به سرقت هویت چندان صحیح نیست چرا که هویت چیزی نیست که اختصاصاً قابل دزدیده شدن باشد بلکه تنها اطلاعات هویتی افراد هستند بدون آن که خود شخص متوجه باشد به طور غیر قانونی مورد استفاده قرار می‌گیرد با این حال مساله اینجاست که به رغم ارتکاب این فرایند و ضررهای هنگفتی که از ارتکاب آن ناشی می‌شود قانون‌گذار به جرم‌انگاری آن نپرداخته است در حالی که در ماده ۱۰۲۸ قانون سرقت ایالات متحده آمریکا این رفتار به صراحت جرم انگاشته شده است. در این مقرر آمده: «هر کس آگاهانه و بدون مجوز قانونی اقدام به انتقال یا استفاده از ابزارهای تشخیص هویت کند به گونه‌ای که این عمل منجر به نقض قوانین فدرال آمریکا شود و یا به موجب قانون ایالتی حاکم بر قضیه جنایت محسوب شود قابل مجازات خواهد بود». در این مقرر سرقت هویت هم در فضای سایبر و هم در فضای فیزیکی قابلیت ارتکاب دارد. ضروری است که قانون‌گذار ایران نیز همانند قانون‌گذار ایالات متحده آمریکا به این رفتار تهدیدآمیز جامه کیفری پوشانده تا مجرمان با مشاهده دورنمای کیفری این رفتار از ارتکاب آن صرف نظر کنند. در ادامه نخست به تعریف سرقت هویت و دیدگاه‌های پیرامون آن پرداخته و سپس جایگاه آن را در نظام کیفری ایران تبیین نموده ایم.

## ۱- سرقت هویت

تاکنون هیچ تعریف رایج و مورد وفاقی از سرقت هویت ارائه نشده است، لذا مطالعه و بررسی تهدیدات واقعی این پدیده بدون وجود تعریف مشترک امکان پذیر نخواهد بود. سابقه این واژه به سال ۱۹۶۴ باز می‌گردد. سرقت اطلاعات هویتی تقریباً با جعل هویت در یک معنا به کار می‌روند.<sup>۱</sup> از آنجایی که در تعریف سرقت هویت از تصاحب نام یا استفاده از اطلاعات هویتی دیگری برای کلاهبرداری یا سایر فعالیت‌های غیرقانونی یاد می‌شود، غالباً این دو واژه به جای یکدیگر به کار می‌روند ولی به نظر می‌رسد جعل هویت نتیجه سرقت هویت است. فرد می‌تواند اطلاعات هویتی فرد دیگر را بدزدد یا بردارد بدون این که مرتکب جعل هویت شود (پورقهرمانی، ۱۳۹۰، ۳).

در اروپا این تعریف ارائه شده است: شخص دغل باز و حيله گری که داده یا اسناد متعلق به دیگری را به دست می‌آورد و سپس خودش را به جای قربانی جا می‌زند سارق هویت است (close, zinkhan, Finney, 2003, 2). در این تعریف به صراحت اشاره‌ای به سوءاستفاده مالی مرتکب از جزئیات هویتی نشده است. در این تعاریف چند ویژگی مشترک از سرقت هویت ارائه شده است: وجود نام، سند یا دیگر داده‌های شناسایی کننده، متعلق به دیگری بودن و غیرقانونی بودن این اقدامات. با توجه به این سه ویژگی می‌توان این تعریف را از سرقت هویت ارائه کرد: «هر کس از اطلاعات شناسایی شخصی دیگری از قبیل نام و نام خانوادگی، شماره امنیت اجتماعی، شماره شناسنامه و ... به منظور جعل هویت دیگری، سوءاستفاده مالی، کلاهبرداری هویت، انجام خریدهای غیرقانونی، برداشت از حساب بانکی، افتتاح یک کارت اعتباری جدید یا سایر فعالیت‌های غیرقانونی استفاده و بهره برداری کند سارق هویت است و به عمل وی سرقت هویت اطلاق می‌گردد» (Sanchez, University, 2012, 85). از این تعریف این گونه استنباط می‌شود که در سرقت هویت قربانی سرقت هنوز هویت اش را حفظ می‌کند و مجرمین هویت وی را به سرقت نمی‌برند چرا که هویت چیزی نیست که اختصاصاً دزدیده شود بلکه از هویت به عنوان ابزاری در جهت انجام سایر فعالیت‌های غیرقانونی استفاده می‌کنند. سرقت هویت چه در محیط سنتی و چه در محیط سایبری قابل ارتکاب است و محیط سایبر تنها ارتکاب این جرم را تسهیل می‌کند. در محیط سایبر اطلاعات شخصی با هدف به کارگیری در فعالیت‌های فریبکارانه آنلاین یا آفلاین

<sup>۱</sup>-لازم به ذکر است که برخی جعل هویت را معادل واژه identity fraud در نظر گرفته اند ولی به نظر می‌رسد identity

fraud کلاهبرداری

هویت می‌باشد.

با استفاده از وسایل الکترونیکی مثلاً مبتنی بر وب جهت انجام هر شکل از سرقت هویت تحصیل می‌شوند و در سایر فعالیت‌های غیرقانونی استفاده می‌شوند.

قانون سرقت هویت فدرال ایالات متحده آمریکا تنها قانون مدونی است که در سال ۱۹۹۸ جهت جلوگیری از سایر جرایم من جمله کلاهبرداری هویت، تروریسم، جاسوسی و مهاجرت غیرقانونی به تعریف منسجم این جرم پرداخته است. در ماده ۱۰۲۸ این قانون آمده: «هر کس آگاهانه و بدون مجوز قانونی اقدام به انتقال یا استفاده از ابزارهای تشخیص هویت دیگری نماید به گونه‌ای که این عمل منجر به نقض قوانین فدرال شود و یا به موجب قانون ایالتی یا محلی حاکم بر قضیه جنایت محسوب شود قابل مجازات خواهد بود». بر اساس این تعریف سرقت هویت اساساً یک جرم فرعی است چرا که اطلاعات هویتی جهت ارتکاب جرم دیگر مورد سوءاستفاده قرار می‌گیرند. با این که سرقت هویت اشکال متنوعی من جمله سرقت هویت کاری و تجاری، سرقت هویت جنایی، سرقت هویت پزشکی و تکثیر هویت دارد اما سارق هویت غالباً از این شناسه‌های هویتی به منظور جعل هویت و یا کلاهبرداری هویت استفاده می‌کند. سرقت هویت تقریباً با جعل هویت در یک معنا به کار می‌رود. در جعل هویت در محیط سنتی جاعل با احراز هویت کاربر مجاز یا با استفاده از کارت دسترسی به محدوده‌ای وارد می‌شود که به راحتی به اطلاعات شخصی دسترسی پیدا می‌کند. این عمل ممکن است با امضا نمودن دفتر ورود و خروج به جای فردی با شناسه‌های هویتی خاص باشد و در محیط سایبر نیز جاعل با سوءاستفاده از ناتوانی رایانه در شناسایی بدون خطا کاربر رایانه را فریب داده و از شناسه هویتی فرد دیگری به جای خود استفاده می‌کند. از آن جایی که هدف از سرقت اطلاعات دیگری استفاده غیرقانونی از آن‌ها می‌باشد لذا زمانی که فرد از اطلاعات هویتی فرد دیگر یا از ابزارهای تشخیص هویت دیگری استفاده می‌کند به نوعی هویت وی را به سرقت برده که این عمل را می‌توان به جعل هویت نیز تعبیر نمود زیرا فرد بعد از دستیابی به اطلاعات شخصی خودش را به عنوان فردی که صاحب این مشخصات است معرفی می‌کند.

در رابطه با این مسئله که چه فعالیت‌هایی به عنوان سرقت هویت یا جعل هویت در نظر گرفته می‌شوند لازم است که به گونه شناسی جرایم مرتبط با هویت پردازیم. جرایم مرتبط با هویت به تمام فعالیت‌های قابل مجازاتی اطلاق می‌شوند که در آنها هویت به عنوان هدف یا به عنوان ابزار اصلی جرم مدنظر است. روست، مینتس و هنس<sup>۱</sup> چهار نوع از جرایم مرتبط با هویت را ارائه می‌دهند: برخورد یا تصادم هویت: هنگامی که دو فرد نام مشابه دارند یا هنگامی که یک آدرس ایمیل به اشتباه استفاده می‌شود و این امر

معمولاً به صورت غیر عمدی واقع می‌شود. تغییر هویت: هنگامی که فردی هویت متعلق به دیگری را اتخاذ می‌کند و این عمل معمولاً عامدانه است. حذف هویت: مانند انتشار خبر مرگ فردی در یک روزنامه. تجدید و بازگرداندن هویت: بازگرداندن ارتباط بین شناسایی کننده و فرد. به عنوان مثال هنگامی که فردی که گزارش مرگ اش در روزنامه منتشر شده بود به همه اعلام کند که گزارش مرگ اش دروغ بوده است (Jaap koops, leenes, 2006, 554). این اعمال زمانی جرم هستند که با قصد و نیت انجام شوند. مثلاً تصادم هویت رفتاری است که اغلب به صورت اتفاقی روی می‌دهد و زمانی که این رفتار با قصد انجام شود احتمالاً در مقوله تغییر هویت قرار می‌گیرد. بازگردانی و تجدید هویت ضرورتاً به عنوان رفتاری که خصیصه جزایی داشته باشد، تلقی نمی‌شود و عمدتاً رفتاری معقول جلوه می‌کند در عوض تغییر هویت و حذف هویت اکثراً به عنوان رفتار سرزنش آمیز در قلمرو حقوق جزا در نظر گرفته می‌شود. به عنوان مثال هنگامی که یک هکر اسناد بیمار خاصی را در سیستم رایانه بیمارستان با هدف نابود کردن اطلاعات هویت اش مورد هدف قرار می‌دهد اقدام به حذف هویت نموده است یا کسانی که قصد دارند در کشوری پناهنده شوند و قبل از ورود به آن کشور پاسپورت شان را از بین می‌برند اقدام به حذف هویت کرده اند اما از سویی می‌توان این رفتار را در قالب ایجاد یک هویت جدید به جای نابود کردن محض یک هویت قدیمی نیز تفسیر نمود و این عمل را در مقوله تغییر هویت قرار داد. تغییر هویت نیز رفتاری غیرقانونی است که علیه هویت یا به وسیله هویت صورت می‌گیرد. کلاهبرداری هویت می‌تواند به عنوان تغییر دادن غیرقانونی هویت فرد توصیف شود که از طرق مختلف صورت می‌پذیرد.

روست، مینتس و هنسن چهار مقوله از تغییر دادن را از یکدیگر متمایز می‌کنند: تصاحب هویت: هنگامی که فردی هویت فرد دیگری را بدون رضایت آن فرد تصاحب می‌کند. واگذاری هویت: هنگامی که فردی از هویت فرد دیگری با رضایت وی استفاده می‌کند. مبادله هویت: هنگامی که دو یا چند نفر با رضایت متقابل و دو جانبه از هویت یکدیگر استفاده می‌کنند. ایجاد هویت: هنگامی که فرد هویت فردی که وجود خارجی ندارد را ایجاد می‌کند. تمامی این چهار مقوله زمانی به عنوان جرم در نظر گرفته می‌شوند که عالماً و با قصد صورت گرفته شوند. کلاهبرداری هویت زمانی مطرح می‌شود که یک شخص از طریق استفاده از نام کاملاً جعلی (که گاهی از آن به عنوان هویت کاذب یاد می‌کنند) یا تصاحب نام یک شخص حقیقی (زنده یا مرده) چه با رضایت یا بدون رضایت وانمود می‌کند فرد صاحب اطلاعات است و از این طریق کالا و خدماتی را تحصیل می‌کند. (de vrise, Tigchelaar & van der linden, 2008, 488). این تعریف دارای دو مولفه اساسی است: کلاهبرداری با استفاده از اطلاعات هویت دیگری صورت می‌گیرد. با استفاده از اطلاعات هویتی تحصیل کالا و خدمات صورت گیرد که این دو مولفه توأمان این جرم را محقق

می‌سازند. کلاهبرداری هویت اصطلاح عام و گسترده تری از سرقت هویت می‌باشد و در واقع سرقت هویت بخشی از مجموعه بزرگتر تغییر هویت (کلاهبرداری هویت) می‌باشد و تغییر هویت خود بخشی از مجموعه بزرگتر با عنوان جرایم مرتبط با هویت می‌باشد. در این دو جرم هویت به عنوان هدف یا ابزار اصلی ارتکاب جرم مورد استفاده قرار می‌گیرد اما در سرقت هویت تنها هویت فرد زنده و موجود بدون رضایت اش اتخاذ می‌شود اما در کلاهبرداری هویت مضاف بر هویت شخص زنده موجود هویت فرد موهوم نیز می‌تواند مورد هدف قرار گیرد و از سویی این جرم هم با استفاده از اطلاعات شخصی دیگری و هم بدون استفاده از این اطلاعات قابل ارتکاب است.

## ۲- دیدگاه‌ها پیرامون وجود سرقت هویت و کلاهبرداری هویت

با وجود ابزارهای شناسایی هویت و تکامل تکنولوژیکی آن، هنوز هم سرقت هویت و به تبع آن کلاهبرداری و سوء استفاده از کارت های اعتباری وجود دارد. سوء استفاده از کارت اعتباری مهم ترین انگیزه سرقت هویت می باشد. در این مورد نظرات و دیدگاه های گوناگونی ارائه شده که به چند مورد از آن اشاره می نماییم.

الف- عدم دسترسی به اطلاعات شخصی: لین لوپوکی<sup>۱</sup>، این گونه بیان می کند که سرقت هویت در سال ۱۹۹۰، به علت عدم توانایی اعطاءکنندگان اعتبار در شناسایی تصدیق هویت قرض گیرندگان صورت گرفت و این مسئله به دلیل خصوصی تر شدن زندگی و عدم دسترسی به اطلاعات شخصی می باشد. لین لوپوکی مسئله سرقت هویت را در سرقت اطلاعات توسط سارق نمی داند بلکه مسئله را در شناسایی انسان و امر تصدیق هویت او می داند. به نظر او اقداماتی که در رابطه با مبارزه با سرقت هویت انجام می شود بیشتر بر مشکل کردن دسترسی به اطلاعات می باشد و این امر برای مبارزه با سرقت هویت مؤثر و کارآمد نیست. یکی از اقداماتی که سارق هویت پس از کسب اطلاعات شخصی انجام می دهد درخواست اعتبار از اعطاءکنندگان اعتبار است. از آنجایی که تأیید اعتبار و تصدیق هویت متقاضی اعتبار بر اساس روش مقایسه می باشد؛ بنابراین اگر این اطلاعات به اندازه کافی در اختیار اعطاءکنندگان اعتبار نباشد عمل مقایسه و شناسایی دقیق افراد به درستی انجام نمی شود و در نتیجه سرقت هویت همچنان ادامه خواهد داشت. او معتقد است که کاهش زندگی عمومی، حذف تدریجی اطلاعات تماس از رکودهای عمومی همانند مبنای داده DMV، کتاب های تلفن، دفترچه راهنما باعث می شود که اطلاعات لازم و کافی در مورد اشخاص در اختیار اعطاءکنندگان اعتبار نباشد و در نتیجه آنها در موقع تقاضای اعتبار،

1-Lynn lopocki

بدون این که از هویت متقاضیان مطمئن شوند اعتبار لازم را پرداخت می کنند. در نتیجه فرصت سرقت هویت فراهم می شود. او بیان می دارد به گفته دنیس بیلی زندگی مدرن به نحوی است که شناسایی نمی شویم و نمی توانیم شناسایی کنیم و این ناشناس ماندن و کاهش زندگی عمومی، توانایی غاصبان را در جهت جعل هویت دیگران تسهیل می نماید. لوپوکی بیان می کند که این خصوصی بودن، محرومیت از اطلاعات موجود عمومی ممکن است باعث اپیدمی سرقت هویت شده و این امکان و فرصت را برای غاصبان هویت فراهم آورد تا پشت نقاب دیگران به فعالیت های غیرقانونی بپردازند. بر این نظریه این انتقاد وارد است که اولاً اعطاءکنندگان اعتبار، از منابعی که او یاد آوری می کند (دفترچه تلفن، راهنمای ثبت شهری و مانند آن) استفاده نمی کنند. اعطاءکنندگان اعتبار میناهای داده و ابزارهای ضد کلاهبرداری را بسیار غنی تر از هر دفترچه تلفن یا مبنای داده DMV گردآوری کرده اند (Hoofnagle, 2004, 595). ثانیاً با توجه به پیشرفت و تکامل فناوری های اطلاعات، زندگی شخصی افراد بیش از گذشته عمومی شده است. فروشندگان و دلالتی هستند که با استفاده از ابزارهای پیشرفته، سوابق آدرس، شماره تلفن و دیگر اطلاعات شخصی را به دست آورده و آن را در اختیار متقاضیان قرار می دهند؛ بنابراین امروزه اطلاعات بیشتر عمومی است تا خصوصی. این مسئله شاید یک علت باشد اما علت اصلی نمی باشد. ب- عدم نظارت و کنترل بر اطلاعات شخصی: پروفیسور سولو، سرقت هویت را به عنوان یک مسئله عدم کنترل بر اطلاعات شخصی می داند. او بیان می کند شیوه سنتی محافظت از حریم خصوصی افراد، که صدمات را به عنوان رویدادهای مجزایی در نظر می گیرد که بر افراد تاثیر می گذارد، نمی تواند تکامل های تکنولوژیکی و اجتماعی جدید را که تغییرات نظام مندی را به وجود آورده اند مورد خطاب قرار دهد (solove, 2003, 1230). به عنوان مثال پذیرش شماره امنیت اجتماعی (SSN)، بدون حمایت از آن در برابر انواع سوء استفاده ها، همه افراد را در معرض خطر بزرگ سرقت هویت قرار می دهد. سولو این امر را به عنوان «ساختار آسیب پذیر» می نامد. بر اساس این نظریه، سرقت هویت صرفاً اتفاقی واقع نشده، بلکه به واسطه ساختار موجود قانونی شکل گرفته است. سرقت هویت نتیجه شکستن ساختار خصوصی است جایی که هیچ شخصی کنترل بر اطلاعات شخصی ندارد. بنابراین بر اساس این نظریه سارقان هویت یکی از متهمین هستند. دولت و مؤسسات بخش خصوصی نیز می توانند از دیگر متهمین باشند که در این زمینه مسئولیت دارند. سولو معتقد است از حقوق اساسی و حقیقی افراد است که درباره شناسایی و تصدیق اعتبار و محدودسازی ارائه و پخش داده، آگاهی لازم را

داشته باشند. باید متناسب با تکامل و پیشرفت تکنولوژیکی و اجتماعی، ساختارهای قانونی نیز تکامل یابد. بنابراین سولو مسئله سرقت هویت را در عدم کنترل بر اطلاعات شخصی می‌داند. او بیان می‌کند که به نظر نمی‌رسد کسی در کنترل باشد و اگر در مورد مجموعه اطلاعات شخصی، محدودیت‌هایی در استفاده و انتشار آن وجود داشته باشد، احتمال سرقت هویت کمتر خواهد بود. لوپوکی از روش سولو به عنوان روشی غیرعملی یاد می‌کند. چرا که هیچ روش موثقی جهت جلوگیری از آشکارسازی اطلاعات شخصی برای سارقان هویت وجود ندارد. اما یافته‌های (FACTA) نشان می‌دهد که به گونه‌ای کنترل خصوصی ریشه مسئله می‌باشد. ج- تحمل خطر توسط اعطاءکنندگان اعتبار: بر اساس این دیدگاه سرقت هویت صرفاً به دلیل بیش از حد خصوصی بودن اطلاعات شخصی و یا عدم کنترل بر اطلاعات شخصی نمی‌باشد. بلکه مسئله در اولویت دادن به ایجاد حساب جدید برای متقاضیان اعتبار و تحمل خطر می‌باشد. سرقت هویت به این دلیل رایج است که تحمل کلاهبرداری برای اعطاءکنندگان اعتبار هزینه کمتری را در بر دارد (Hoofnagle, 2010, 13). سرقت هویت برای کلاهبرداری مخصوصاً کلاهبرداری حساب جدید، به دلیل عدم توجه و دقت و بررسی اعطاءکنندگان اعتبار، در اطلاعات ارائه شده به آنها می‌باشد. بر اساس این دیدگاه اعطاءکنندگان اعتبار، در زمان درخواست متقاضی برای اعتبار جدید، خیلی سریع و بدون توجه لازم اعتبار درخواست شده را اعطاء می‌کنند. بررسی‌ها نشان می‌دهد که حتی اگر متقاضی اطلاعات نادرستی را ارائه دهد باز هم اعطاءکنندگان اعتبار، اعتبار درخواست شده را ارائه می‌دهند. اگر چه ممکن است متقاضی کلاهبردار بوده و با جعل هویت دیگران، درخواست اعتبار نموده باشد. از دیدگاه تجاری، پذیرش و تحمل خطر سرقت هویت و پذیرش زیان‌های آن تصمیم منطقی است. بسیاری از شرکت‌ها میزانی از خطر سرقت هویت و خطر کلاهبرداری را تحمل می‌کنند. انگیزه خاص صنعت اعتباری و رقابت در بازارهای اعتباری، فضایی را به وجود آورده است که غاصبان هویت با اتکاء به این فضا، به اقدامات خود می‌پردازند.

### ۳- فرآیند سرقت هویت

در ابتدا سارق معمولاً حوزه‌ها و روش‌های سرقت هویت را انتخاب می‌کند و سپس وارد مرحله سرقت هویت می‌شود. برنامه ریزی: سارقان هویت تصمیم می‌گیرند که کدام شرکت، شخص و ... را هدف قرار دهند و تعیین می‌کنند که چگونه آدرس‌های پست الکترونیکی آن شرکت را به دست آورند، چگونه به اطلاعات شخصی مشتریان و یا سایر اشخاص دسترسی داشته باشند. آنها اغلب مشابه ارسال کنندگان هرنامه از اصول فنی ارسال حجم بالایی از نامه و جمع‌آوری آدرس استفاده می‌کنند. راه اندازی: وقتی



سارقان هویت تصمیم گرفتند از کدام شرکت تقلید کنند و قربانی های خود را تعیین کردند، روش هایی را برای تحویل پیغام و جمع آوری اطلاعات ایجاد می کنند. بیشتر اوقات این کار مستلزم آدرس های پست الکترونیکی و یک صفحه وب است. حمله: بیشتر کاربران با این مرحله آشنا هستند، سارق هویت یک پیغام ساختگی که به نظر می رسد از طرف یک منبع قابل اطمینان است، ارسال می کند. معمولاً از شیوه های مهندسی اجتماعی<sup>۱</sup> برای جلب اطمینان قربانی و سپس به دست آوردن اطلاعات استفاده می کند. جمع آوری: سارقان هویت، بعد از انجام مراحل قبلی وارد مرحله جمع آوری اطلاعات می شوند و اطلاعاتی که قربانی ها در صفحه های وب و یا پنجره های باز شو وارد می کنند، ثبت می نمایند. سرقت هویت و کلاهبرداری: اگر چه سرقت هویت در مواردی هدف اول مجرمین می باشد، اما غالباً سرقت هویت برای تسهیل انجام سایر جرائم ارتکاب می یابد (Winn, 2009, 49). طرح و پلان کار برای انجام سرقت هویت می تواند شامل وضعیتی، شود که کلاهبرداری نیز اتفاق بیافتد. سارقان هویت از اطلاعاتی که به دست آورده اند برای خریدهای غیرقانونی یا کلاهبرداری های دیگر استفاده می کنند. اگر سارق هویت قصد داشته باشد سرقت دیگری را هماهنگ کند، موفقیتها و شکست های سرقت انجام شده را می سنجد و مراحل بالا را دوباره طی می کند. سارقان هویت معمولاً اطلاعات شخصی افراد را می توانند با استفاده از دو مکانیزم سرقت فیزیکی و سایبری تحصیل کنند. در روش فیزیکی سارق کیف مدارک، کیف دستی، رکوردهای شخصی و انواع و اقسام نامه ها (شامل صورت حساب ها، کارت های اعتباری، اظهارنامه های بانکی و ...) را به سرقت می برد اما در روش سایبری سارق با استفاده از شیوه هایی همچون دلالی اطلاعات، سوءاستفاده از کارمندان، فریب دادن، در دسترس گذاشتن، کلک و حقه در محدوده کلک و حقه، معرفی خود به جای فرد دیگر، سرک کشیدن، بازیافت زباله، هک کردن، فیشینگ، فارمینگ، اسکیمینگ، اسپوفینگ، اسنیفر، اسپوی ویر، تروجان، ویروس، کوکی و ... به سرقت اطلاعات هویتی مبادرت می ورزد.

#### ۴- کاربرد سرقت هویت

مجرمین از اطلاعات شخصی قربانی در راه های متعدد و گوناگون استفاده می کنند. رایج ترین نمونه های استفاده از این اطلاعات عبارتند از: سارقین ممکن است از صادرکننده کارت اعتباری درخواست تغییر آدرس صورت حساب بر حساب کارت اعتباری قربانی داشته باشند. بر این اساس هزینه ها و مسئولیت را بر حساب قربانی محول نمایند. از آنجایی که صورت حساب های اش به حساب های مختلف

فرستاده می شود، ممکن است زمان زیادی طول بکشد تا قربانی متوجه مشکل شود. سارقین هویت ممکن است که یک حساب کارت اعتباری جدید به اسم قربانی باز کنند. زمانی که آنها از کارت های اعتباری استفاده کرده و صورت حسابها را پرداخت نکنند گزارش تخلف حسابها به نام قربانی صادر می شود. سارقین هویت ممکن است از اطلاعات شخصی دیگران در قاچاق انسان یا مواد مخدر استفاده کنند. سارقین ممکن است از این اطلاعات در تماس های تلفنی استفاده کنند. سارقین ممکن است چک ها، کارت های اعتباری و بستنکاری یا مجوز نقل و انتقالات الکترونیکی به اسم دیگری را جعل نماید. سارقین ممکن است از آن اطلاعات برای اعلام ورشکستگی به اسم دیگری برای پرداخت نکردن بدهیها یا اخراج نشدن استفاده کنند. اگر شرکت بازرگانی بخواهد اعلام ورشکستگی نماید باید دلایل قانع کننده برای اعلام ورشکستگی داشته باشد حال در مواردی که دلایل قانع کننده ندارد و با استفاده از اطلاعاتی که سارق هویت به آنها داده شرکت اعلام ورشکستگی می کند. این اطلاعات ممکن است مربوط به دیگر افراد باشد یا اطلاعات تقلبی باشد. سارق هویت با تحصیل اطلاعات و صورت حساب های شرکت های دیگر آن را به متقاضیان می فروشد. ممکن است آنها با دریافت وامی که به اسم دیگری است، ماشین بخرند. ممکن است که سارقین در زمان دستگیری، اطلاعات هویتی فرد دیگری را به پلیس ارائه دهند. در چنین مواردی، اگر آنها در جلسه رسیدگی دادگاه حاضر نشده باشند، حکم بازداشت به اسم قربانی صادر خواهد شد. ممکن است از اطلاعات هویتی فرد دیگری برای صدور گواهینامه رانندگی، با تصویر خودشان استفاده کنند (Ayotte, 2010, 248).

## ۵- مشکلات سرقت هویت

سرقت هویت یکی از بزرگ ترین و دشوارترین تهدیدات محسوب می شود. سرقت هویت اشکال و درجات متفاوتی دارد، که از استفاده غیرمجاز از کارت های اعتباری تا تصاحب کامل هویت شخص را در بر می گیرد. یکی از عمده ترین مشکلات سرقت هویت این است که شناسایی و دستگیری سارقین هویت برای مأمورین اجرای قانون بسیار مشکل است و این مسئله به این دلیل است که مجرمین با استفاده از تکنولوژی های نوین و روش های رمزگذاری و یا با جعل هویت افراد بی گناه، موقعیت فیزیکی و هویت واقعی خود را پنهان می کنند در نتیجه تلاش مأموران قانون برای شناسایی موقعیت آنها به جایی نمی رسد. در دنیای واقعی از آنجایی که ارتکاب جرم غالباً از طریق مجاورت مباشر و قربانی صورت می پذیرد، بر این اساس در روند رسیدگی کیفری قضات بر صحنه جرم به عنوان بهترین راه شناسایی مرتکب جرم و ارتباط دادن مجرم به جرم تأکید می‌ورزند (Copes, 2009, 239). با وجود این امر در جرایم سایبری یا

صحنه جرم وجود ندارد یا ممکن است صحنه های جرم بسیاری با مدارک خود از جرایم که در سرتاسر فضای سایبر پراکنده شده اند وجود داشته باشد. بنابراین شناسایی صحنه جرم الکترونیکی بسیار مشکل خواهد بود. زمانی که مرتکب جرم، ارتباطات اش را از طریق رایانه با چند کشور، با شبکه های ناشناس برقرار می کند، دستیابی به آنها برای رسیدگی به جرم امکان پذیر نمی باشد. علاوه بر آن، از نظر میزان ضرری که یک جرم وارد می کند میزان ضرر سرقت هویت آنلاین نسبت به سرقت هویت در دنیای واقعی بسیار گسترده تر است.

افرادی که هویت شان مورد سرقت واقع شده باید ماهها یا سالها زمان صرف کنند و بودجه کلانی پرداخت نمایند تا بتوانند وضعیت نابسامانی که توسط سارقین هویت با استفاده از نام و سوابق اعتباری آنها به وجود آمده را پاکسازی کنند (Garoupa, 2004, 11). این قربانیان ممکن است با مشکلات فراوانی مواجه شوند از جمله این که توسط طلبکارانی که خواستار پرداخت بدهی هستند به ستوه آورده شوند، بدهی هایی که در واقع آنها به وجود نیآورده اند همچنین به دلیل جرایمی که مرتکب نشده اند دستگیر شوند و در نهایت این که برای رسیدگی به این امور ارتکاب نیافته باید هزینه اجرای قانون که گزاف است را نیز متقبل شوند.

بر خلاف دنیای واقعی که آسیب های فراوانی را بر هر قربانی وارد می آورد، سرقت هویت آنلاین هم موجب آسیب فردی و هم آسیب سیستمیک می شود. فضای سایبر و فناوری اطلاعات و ارتباطات تبدیل به بخش ضروری از زیرساخت های حیاتی یک ملت شده اند. در حالی که سرقت هویت آسیب های فراوانی به افراد وارد می آورد ولی این آسیبها به همین اندازه محدود نمی شوند بلکه می توانند زیرساخت های حیاتی یک ملت را تضعیف و یا حتی نابود کند و این امر تهدید سرقت هویت سایبری را بسیار بیشتر از تهدید سرقت هویت در دنیای واقعی می کند و در یک مفهوم سرقت هویت سایبری تمایز بین تهدیدات بیرونی و درونی را از بین می برد. در دنیای واقعی، جوامع تهدیدات را به دو دسته تهدیدات داخلی و خارجی تقسیم می کنند و بر اساس آن مسئولیت مقابله با آن را به هر یک از مؤسسات اجتماعی مربوطه محول می نمایند. در حالی که، همیشه نهادهایی برای مقابله با اشکال سنتی تهدیدات در دنیای واقعی داریم با این حال نیازمند استراتژی مناسب برای مقابله با تهدیدات فضای سایبر هستیم. در تهیه و تدوین این استراتژیها باید تجدیدنظر داشته باشیم و به کفایت و امکان نامگذاری سنتی و کلاسیک تهدیدات بیرونی و درونی توجه داشته باشیم. در نهایت این که با توجه به پیامدهای ذاتی فراملی و برون مرزی بودن این جرایم و تنوع نسبی و واگرایی ملی و منطقه و سیاست مقابله با این جرایم، سرقت هویت پتانسیل تضاد بین سیستم های حقوقی ملی را دارد. استراتژی های ملی یک دولت

نمی تواند برای مبارزه با سرقت هویت آنلاین مؤثر باشد؛ چرا که این استراتژی‌ها به منظور پیشگیری از قربانی شدن شهروندان یک دولت طراحی شده اند نه به منظور پیشگیری از قربانی شدن شهروندان دیگر دولت ها.

## ۶- سرقت هویت در حقوق کیفری ایران

در حقوق کیفری ایران نص قانونی خاصی که صریحاً جعل یا سرقت هویت را (با این عنوان) به عنوان یک جرم مستقل تلقی نموده باشد، وجود ندارد. قانون تجارت الکترونیکی و قانون جرایم رایانه ای هم در این مورد بیانی ندارند. ولی در حقوق سنتی می توان گفت برخی از مواد قوانین جزایی بر جعل هویت، سرقت هویت و کلاهبرداری هویت دلالت دارند که در ادامه به آنها اشاره می کنیم.

### ۶-۱- استفاده از اسناد هویتی دیگری

جعل هویت دیگری می تواند از طریق استفاده از اسناد هویتی دیگری یا جعل در اسناد هویتی صورت پذیرد. اسناد هویتی مدارکی می باشند که برای تعیین هویت افراد در جامعه به کار می روند، چه این مدارک از اسناد سجلی و شناسنامه باشند و یا این که اسناد دیگری را که می تواند در شناسایی مورد استفاده قرار گیرند شامل شود. جعل اسناد هویتی، عبارت است از ساختن متقلبانه شناسنامه یا اسناد مبین هویت افراد از زمان ولادت تا وفات یا قلب حقیقت در یک سند هویتی به صورت تقلبات مادی محسوس از قبیل تغییر دادن کلمه‌ها یا عبارت‌ها به انحاء مختلف به قصد اضرار به غیر به طریق پیش بینی شده در قانون (جرایم و مجازات های مربوط به اسناد سجلی).

مهم ترین و شایع ترین سند هویتی که بیشتر از سایر اسناد هویتی مورد سوءاستفاده واقع می شود شناسنامه است که غالباً از آن برای ارتکاب جرایم علیه اموال استفاده می شود. شناسنامه حاوی اطلاعاتی ناظر به شخص می باشد. از همین رو کاربردهای وسیعی در اثبات هویت فرد می تواند داشته باشد به دلیل همین اطلاعات است که شناسنامه سند محرمانه تلقی شده و به موجب ماده ۳۴ قانون ثبت احوال مصوب ۱۳۵۵ افشای اطلاعات مذکور در دفاتر ثبت کل وقایع و اسناد سجلی جز برای صاحب سند و مقامات قضایی و دولتی ذی صلاح ممنوع است. شناسنامه حاوی اطلاعاتی ناظر به هویت مدنی فرد در اجتماع می باشد و بیان کننده آن است که فردی با مشخصات خاص در جامعه وجود دارد. اما شناسنامه فی حد ذاته بر وجود عینی آن فرد خاص دلالتی ندارد و تنها مشخصاتی را به صورت ذهنی و فارغ از فرد خاص موجود در عالم خارج بیان می کند. برای آن که میان آن مشخصات تطابق برقرار باشد به «عکس»

متوسل شده اند، به این ترتیب که عکس فرد را منضم به شناسنامه می کنند تا میان آن مشخصات با خود فرد ارتباط و دلالت برقرار شود برای همین بند ۳ ماده ۳۶ قانون ثبت احوال مصوب ۱۳۵۵ محل الصاق عکس را از جمله مشخصات و اطلاعات شناسنامه می داند.

اسناد سجلی و شناسنامه از جمله اسنادی است که ممکن است به گونه های مختلفی مورد سوءاستفاده قرار گیرد. جعل هویت و استفاده از شناسنامه دیگری عموماً برای مقاصد نظیر فرار از تعقیب و اجرای مجازات، خروج غیرمجاز از کشور، کلاهبرداری، فرار از خدمت وظیفه عمومی، رأی دادن، ازدواج، تحصیل گذرنامه، تحصیل تابعیت یک کشور و ... انجام می شود. در جهت مقابله با هر گونه سوءاستفاده از اسناد سجلی و شناسنامه، قانون خاصی تحت عنوان «قانون تخلفات، جرایم و مجازات های مربوط به اسناد سجلی و شناسنامه» در سال ۱۳۷۰ به تصویب مجمع تشخیص مصلحت نظام رسید. قانون مزبور برای استفاده از شناسنامه دیگری، دریافت شناسنامه موهوم و جعل هویت مجازات هایی را پیش بینی نموده است. به موجب ماده ۲ قانون مذکور اشخاص زیر به حبس از نودویک روز تا یک سال و یا به پرداخت جزای نقدی از ۲۰۰/۰۰۰ ریال تا ۱/۰۰۰/۰۰۰ ریال و یا به هر دو مجازات محکوم می شوند. اشخاصی که در اعلام ولادت یا وفات یا هویت بر خلاف واقع اظهار می نمایند. اشخاصی که عالماً عامداً پس از رسیدن به سن هجده سال تمام از شناسنامه مکرر استفاده نموده یا به دریافت شناسنامه مکرر برای خود یا مولی علیه و یا به دریافت شناسنامه موهوم مبادرت نماید و یا از شناسنامه دیگری خواه صاحب آن زنده و یا مرده باشد به نام هویت خود استفاده نمایند. افرادی که شناسنامه خود را در اختیار استفاده کنندگان قرار دهند به همان مجازات محکوم می شوند. ماما یا پزشکی که در مورد ولادت یا وفات گواهی خلاف واقع صادر کند. اشخاصی که در مورد ولادت یا وفات شهادت دروغ بدهند و شهادت آنان در تنظیم دفتر ثبت کل وقایع و یا وفات مؤثر واقع شود. بر اساس تعریفی که از کلاهبرداری هویت به عمل آمد عمل اتخاذ هویت شخص موهوم یا فرضی، اتخاذ هویت شخص زنده یا مرده از مصادیق کلاهبرداری هویت می باشد. این اعمال می تواند از طریق سرقت اطلاعات شخصی و یا سایر اسناد و مدارک شناسایی واقع شود. تبصره این ماده حداکثر مجازات را در صورت تکرار برای مرتکب پیش بینی نموده است.

به موجب ماده ۹ قانون مذکور هر کس برای فرار از تعقیب یا اجرای مجازات قانونی و یا به قصد اقدام به خروج غیرمجاز از کشور مبادرت به استفاده از شناسنامه دیگری به نام هویت خود نمایند، علاوه بر تحمل مجازات اصلی به حبس از یک سال تا سه سال و پرداخت جریمه از ۵۰۰/۰۰۰ ریال تا ۱/۰۰۰/۰۰۰ ریال محکوم می شود. بنابراین اگر فردی که ممنوع الخروج بوده برای خروج از کشور با جعل هویت دیگری مبادرت به استفاده از شناسنامه دیگری نموده باشد بر اساس این ماده قابل مجازات خواهد بود.

ماده ۳۷ قانون گذرنامه مصوب ۱۳۵۲ صراحت دارد هر کس برای دریافت گذرنامه یا اسناد در حکم گذرنامه به نام خود یا نام دیگری اسناد و مدارک خلاف واقع یا متعلق به غیر را عالمأ عامداً به مراجع مربوطه تسلیم نماید به حبس تأدیبی از دو ماه تا شش ماه محکوم می شود و در صورتی که عمل او منجر به صدور گذرنامه شود به حبس از ۲ ماه تا ۲ سال محکوم خواهد شد. همچنین مطابق ماده ۴۱ قانون مذکور: هر کس برای تحصیل گذرنامه یا اسناد در حکم گذرنامه عالمأ و عامداً و به قصد تقلب هر گونه اطلاع مربوط به خود و همراهان را که در صدور گذرنامه مؤثر است بر خلاف واقع در پرسشنامه ذکر نماید به شرط استفاده از گذرنامه به حبس تأدیبی از ۲ ماه تا ۶ ماه محکوم خواهد شد. جعل هویت می تواند از طریق جعل در شناسنامه و اسناد سجلی صورت گیرد. مرتکب با جعل در این اوراق برای خود هویت جدیدی کسب می کند که از آن در سایر فعالیت های غیرقانونی استفاده نماید (میرمحمدصادقی، ۱۳۸۸، ج ۲، ۳۱۶).

استفاده از شناسنامه دیگران برای رهایی از خدمت وظیفه عمومی در قانون اصلاح ماده ۶۰ و الحاق دو تبصره به آن و ماده ۶۱ قانون خدمت وظیفه عمومی مصوب ۱۳۶۳ و الحاق یک تبصره به آن مصوب ۱۳۶۸ جرم انگاری شده است. به موجب ماده ۶۰ این قانون: کسانی که با ارتکاب اعمالی چون جعل شناسنامه، مهر، امضاء، کارت پایان خدمت، کارت معافیت، استفاده از شناسنامه دیگران، اعمال نفوذ، شهادت کذب، گواهی خلاف واقع، مکتوم داشتن حقیقت، اخذ رشوه یا فریب دادن مشمول موجبات معافیت خود یا دیگران را از خدمت وظیفه عمومی فراهم سازند به اتهامات آنان در دادگاه صالحه رسیدگی شده و با رعایت شرایط و امکانات خاطی و دفعات و مراتب جرم و مراتب تأدیب از وعظ و توبیخ و تهدید به حبس تعزیری از یک تا پنج سال محکوم می شوند.

رای دادن با شناسنامه دیگری در قانون انتخابات مورد جرم انگاری قرار گرفته است. جدیدترین متن قانونی در این زمینه قانون انتخابات مجلس شورای اسلامی مصوب ۱۳۷۸ است. این قانون تا سال ۱۳۸۶ یازده اصلاحیه و استفساریه داشته است. به موجب ماده ۶۶ قانون یاد شده: علاوه بر جرایم مندرج در این قانون ارتکاب امور ذیل جرم محسوب می شود: خرید و فروش رای. رای گرفتن با شناسنامه کسی که حضور ندارد. تهدید یا تطمیع در امر انتخابات. رای دادن با شناسنامه جعلی. رای دادن با شناسنامه دیگری.

## ۶-۲- اختیار اسم یا عنوان مجعول

اختیار کردن اسم یا عنوان مجعول از مواردی است که از آن می توان به جعل هویت تعبیر کرد. اختیار اسم یا عنوان مجعول از مصادیق تمثیلی متقلبانه است که قانون گذار در ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ بر شمرده است. به موجب این ماده: هر کس از راه حیله و تقلب مردم را به وجود شرکتها یا تجارتخانهها یا کارخانهها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقعی امیدوار نماید یا از حوادث و پیشامدهای غیرواقعی بترساند و یا اسم و 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 صاحب اش از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می شود.

مراد از اختیار اسم مجعول آن است که مرتکب با صحنه سازی های متقلبانه، مثلاً با دست بردن در شناسنامه اش، برای خود اسم دیگری غیر از اسم واقعی اش اختیار کند. تعلق یا عدم تعلق اسم اتخاذ شده به شخص دیگر مهم نیست (میرمحمدصادقی، ۱۳۸۸، ج ۲، ۶۹). یک شخص معروف به بدحسابی و بی اعتباری ممکن است صرفاً به قصد پنهان کردن اسم اصلی اش در شناسنامه خود دست برده و نام دیگری را برای خود اختیار کند، بدون این که نام اتخاذ شده متعلق به شخص خاصی باشد. از سوی دیگر، ممکن است کسی نام یک شخص معتبر را اختیار کرده و از این طریق اموال مردم را ببرد. امری که در سرقت هویت واقع می شود این است که مرتکب معمولاً بعد از سرقت اطلاعات شخصی افراد (مخصوصاً افراد معتبر و خوش حساب) خود را به جای او معرفی می کند و بدین طریق از این اطلاعات در فعالیت های غیرقانونی اعم از مالی و غیرمالی استفاده می کند. بنابراین اگر فردی بعد از سرقت اطلاعات شخصی دیگری و اتخاذ هویت او، دیگران را فریب داده و از این طریق موفق به بردن مال شود عمل اش مشمول کلاهبرداری ماده مزبور خواهد بود. منظور از عنوان، تیتراژ دانشگاهی و هر نوع مقام دولتی و یا غیر دولتی است (میرمحمدصادقی، ۱۳۸۸، ج ۲، ۷۰). کسی که به صورت متقلبانه به اطلاعات شناسایی شخصی دیگران دست می یابد و خود را بر اساس آن اطلاعات پزشک، استاد یا رئیس دانشگاه، قاضی و ... معرفی می کند در واقع جعل عنوان نموده است. بنابراین ملاحظه می شود که جعل اسم یا عنوان با استفاده از مشخصات و مختصات هویتی دیگران صورت می پذیرد.

### ۶-۳- استفاده از مهر، علامت، تمبر

همان طور که قبلا در تعریف سرقت هویت اشاره شد سرقت هویت از طریق سرقت ابزارهای تشخیص هویت و استفاده از آنها در فعالیت های غیرقانونی انجام می شود. بنابراین شاید بتوان با تعریفی موسع از ابزارهای تشخیص هویت، مهر، علامت، تمبر و ... را نیز نوعی ابزار تشخیص هویت در نظر گرفت. چرا که علامت مخصوص، مهر مخصوص و مواردی از این قبیل، از هویت آن شرکت خاص، هویت آن شخص حقوقی حکایت دارد. بنابراین اگر فردی مهر، تمبر، علامت و... شرکت، اداره، مؤسسه، سازمان و دانشگاه و ... را به نوعی به دست آورد و سپس از آن در فعالیت های غیرقانونی استفاده کند نوعی سرقت هویت واقع شده است. ماده ۵۲۳ قانون تعزیرات مصوب ۱۳۷۵ به طور کلی به کار بردن مهر دیگری بدون اجازه صاحب آن را جعل تلقی نموده است.

سوءاستفاده از این موارد در ماده ۵۳۰ قانون تعزیرات مصوب ۱۳۷۵ جرم انگاری شده است. بر پایه این ماده: هر کس مهر یا تمبر یا علامت ادارات یا شرکتها یا تجارتخانه های مذکور در مواد قبل را بدون مجوز به دست آورد و به طریقی که به حقوق و منافع آنها ضرر وارد آورد استعمال کند یا سبب استعمال آن گردد علاوه بر جبران خسارت وارده به دو ماه تا دو سال حبس محکوم خواهد شد. استفاده از علائم تجاری دیگران در ماده ۶۶ قانون تجارت الکترونیک مصوب ۱۳۸۲ جرم انگاری شده است. علامت تجاری عبارت است از هر کلمه، نام، علامت، طرح یا حرفی که در عالم تجارت جهت تعیین هویت یک محصول خاص و تمییز آن از سایر محصولات استفاده می شود (میرمحمدصادقی، ۱۳۸۸، ج ۲، ۶۹). همین طور فردی که با سرقت مهر مخصوص پزشکی، از آن در سایر فعالیت های غیرقانونی استفاده می کند نیز نوعی سرقت هویت می باشد. جعل گواهی پزشکی ممکن است از طریق استفاده از مهر پزشک انجام شود. جعل گواهی پزشکی به اسم طبیب در ماده ۵۳۸<sup>۱</sup> قانون تعزیرات مصوب ۱۳۷۵ مورد جرم انگاری واقع شده است.

<sup>۱</sup> - هر کس شخصا یا توسط دیگری برای معافیت خود یا شخص دیگری از خدمت دولت یا نظام وظیفه یا برای تقدیم به دادگاه گواهی پزشکی به اسم طبیب جعل کند به حبس از شش ماه تا یک سال یا به سه تا شش میلیون ریال جزای نقدی محکوم خواهد شد.



## ۶-۴- قلمداد کردن طفل به جای طفل دیگر

در جعل هویت غالباً خود فرد اقدام به جعل هویت و معرفی خود به جای دیگری می نماید. ولی می توان مواردی را که جعل هویت توسط دیگران صورت می پذیرد را یافت. از جمله اینها جعل هویت طفل تازه متولد شده می باشد. در این مورد برای طفل هویت جدیدی غیر از هویت واقعی او اتخاذ می شود. قانون گذار در ماده ۶۳۱ قانون تعزیرات مصوب ۱۳۷۵ بیان می دارد: هر کس طفلی را که تازه متولد شده است بدزدد یا مخفی کند یا او را به جای طفل دیگری یا متعلق به زن دیگری غیر از مادر طفل قلمداد نماید به شش ماه تا سه سال حبس محکوم خواهد شد و چنانچه احراز شود که طفل مزبور مرده بوده مرتکب به یکصد هزار تا پانصد هزار ریال جزای نقدی محکوم خواهد شد. ملاحظه می شود که در این ماده قلمداد نمودن طفل به زن دیگری غیر از مادر طفل نوعی جعل هویت می باشد. چرا که برای طفل هویت جدیدی غیر از هویت واقعی او اتخاذ می شود و معرفی نمودن طفل به جای طفل دیگر جعل هویت می باشد.

## ۶-۵- شرکت در آزمون به جای دیگری یا شرکت دادن دیگری به جای خود

یکی از مواردی که می توان از آن به جعل یا سرقت هویت یاد کرد شرکت در آزمون به جای دیگری می باشد. به موجب ماده ۵۴۱ قانون تعزیرات مصوب ۱۳۷۵: هر کس به جای داوطلب اصلی هر یک از آزمونها اعم از کنکور ورودی دانشگاهها و مؤسسات آموزش عالی، یا امتحانات داخلی یا نهایی واحدهای مزبور یا امتحانات دبیرستان ها، مدارس راهنمایی و هنرستانها و غیره در جلسه امتحان شرکت نماید حسب مورد مرتکب و داوطلب علاوه بر مجازات اداری و انتظامی به دوپست هزار تا یک میلیون ریال جزای نقدی محکوم خواهد شد.

شرکت در آزمون به جای دیگری تا قبل از قانون تعزیرات مصوب سال ۱۳۷۵ فاقد وصف کیفری بود و با مرتکب بر اساس قواعد انتظامی و اداری که احتمالاً در هر مورد وجود داشت، برخورد می شد. کثرت تعداد محصلین رشته های مختلف آموزشی و وسعت حوزه های امتحانی و پایین بودن سطح فرهنگ پاره ای از جوامع و عدم رشد اخلاقی عده ای از افراد جامعه، فلسفه جرم انگاری عمل موضوع ماده ۵۴۱ می باشد (پیمانی، ۱۳۸۵، ۱۴۸).

با توجه به این ماده می توان عمل فردی را که به جای داوطلب اصلی در آزمون شرکت می کند را جعل یا سرقت هویت دانست. چرا که در واقع مرتکب آگاهانه و بدون مجوز قانونی با اتخاذ هویت دیگری

(داوطلب اصلی) خود را به عنوان داوطلب معرفی نموده و از این طریق در آزمون شرکت می نماید. هر چند که این کار با توافق و تبنانی مرتکب و داوطلب اصلی انجام می شود اما می توان عمل فردی را نیز که با تحصیل مدارک شناسایی داوطلب، بدون رضایت او، در آزمون شرکت می کند مشمول این ماده دانست. این اقدام مشمول تعریفی که قانون فدرال از سرقت هويت به عمل آورده، می شود چرا که فرد بعد از تحصیل مدارک شناسایی داوطلب، از آنها در فعالیت غیرقانونی (شرکت در آزمون به جای دیگری) استفاده نموده است. هر چند که شاید فایده عملی در این کار برای سارق هويت مترتب نباشد اما می تواند انجام چنین اموری از جانب سارق هويت به دلایل گوناگونی از جمله ایراد ضرر و ... باشد.

#### ۶-۶- استبدال شخص (غصب هويت دیگری)

استبدال شخص یا بدل دیگری واقع شدن نوع خاصی از جعل امضاء است. بدین نحو که شخصی هويت دیگری را برای اضرار به او غصب می نماید. یعنی علی رغم این که صحیحا و واقعا امضای خود را ذیل نوشته یا سند می گذارد ولی به لحاظ اینکه به جای دیگری و بدل از او امضا می کند همین امضاء صحیح، جعل هويت غیر است و جرم جعل تحقق یافته است. مثل این که شخصی پس از سرقت ابزارهای تشخیص هويت دیگری از جمله شناسنامه و الصاق عکس خود به شناسنامه او به دفتر اسناد رسمی مراجعه و خود را به جای او معرفی و ذیل سندی را امضاء می کند که در این صورت جعل هويت و جعل محقق شده است. شخصی که به لحاظ هم نام بودن با دیگری خودش را جای وی معرفی و با علم به این که حواله ای متعلق به دیگری است آن را امضاء و دریافت می نماید نیز مرتکب جعل هويت شده است. در خصوص استبدال شخص، این که جاعل امضای واقعی خود را تغییر بدهد یا خیر مؤثر در مقام نیست و با همان علامتی که به عنوان امضاء در ذیل نوشته یا سند گذارده است منظور نهایی خود را که غصب هويت غیر و معرفی خویش به جای صاحب اصلی حواله بوده، عملی ساخته و استبدال شخص و جعل تحقق یافته است (مصلاهی، ۱۳۸۳، ۵۴). ماده ۵۲۳ استبدال و جانشینی اشخاص را در امضاء ولو با اجازه آنها، اجازه نداده است و آن را به عنوان جعل تلقی نموده است. البته در این خصوص نظر مخالفی نیز وجود دارد و آن اینکه اصل بر جواز است و منع قانون گذار باید صراحتاً بیان شود و چون در مورد نقش کردن امضای دیگری با اجازه وی زیر یک سند، قانون سکوت کرده است پس اصل بر این است که امضای دیگری را با اجازه خودش می توان ذیل سند نقش نمود بدون آن که عنوان جعل داشته باشد (مصلاهی، ۱۳۸۳، ۱۰۰).

آیا با وجود فقدان نص قانونی خاص می توان سرقت هویت را با قوانین و مقررات سرقت رایانه ای یا کلاهبرداری رایانه ای منطبق دانست؟ با نگاهی به ماده ۱۲ قانون جرایم رایانه ای در ارتباط با سرقت رایانه ای ملاحظه می شود رفتاری که به عنوان رکن مادی سرقت رایانه ای صورت می پذیرد، ربایش داده است. ربودن داده به معنای دست اندازی به داده دیگری است که یا با روگرفتن (کپی) است یا با برش (کات). بنابراین منظور از ربودن در ماده ۱۲ دو رفتار کپی یا برش داده متعلق به دیگری است. این رفتار باید در فضای سایبر انجام گیرد، به نحوی که کسی بدون این که داده دیگری را جعل کند یا تخریب نماید آن را بر روی افزارهای ذخیره کننده بفرستد یا بر روی لوح فشرده بنویسد یا به صندوق پستی خود ارسال کند و یا به هر نحو دیگری این کار را انجام دهد. از این رو اگر کسی به سامانه دیگری که با تدابیر امنیتی محافظت شده رخنه کند و داده یا اطلاعات را یافته و درون مایه آن را بر روی کاغذ بنویسد یا بخواند یا حتی از روی صفحه نمایشگر عکس بگیرد تنها جرم دسترسی غیرمجاز را انجام داده است. زیرا نگاه کردن به سامانه دیگری و به یاد سپردن آن یا نوشتن آن بر روی کاغذ یک رفتار فیزیکی و بیرون از فضای سایبر است و بزه به شمار نمی رود مگر در حالتی که رفتار شخص به رفتارهای بزهکارانه پسینی بیانجامد.

برش داده هم به حالتی می گویند که داده از جایگاه ذخیره شده خود برداشته شود و به جای دیگری خواه رایانه باشد و خواه رایانامه و یا ابزارهای حامل داده فرستاده شود. ربودن هر چند بر دو رفتار جداگانه روگرفتن و برش اشاره دارد اما این دو رفتار گونه ای دست اندازی سایبری به شمار می روند که افزون بر آن سبب می شوند تا مرتکب از داده دیگری بهره مند شود. بهره مندی از داده دیگری به معنای در اختیار گرفتن آنها است و لازم نیست تا مرتکب پس از روگرفتن یا برش از درون مایه داده آگاهی یابد یا در جایی از آنها بهره بگیرد. این حالت مانند هنگامی است که کسی خودرو دیگری را بر باید لازم نیست تا از درون آن بازدید کند یا بر آن سوار شده و بهره جویی کند. موضوع این جرم نیز داده متعلق به دیگری است که فرد بدون رضایت صاحب داده آن را می رباید.

سرقت هویت دستیابی به اطلاعات دیگران و سوء استفاده از آن می باشد. دستیابی به اطلاعات هویتی دیگران می تواند از طرق مختلف از جمله هک و ربایش داده صورت پذیرد. بنابراین صرف دستیابی به اطلاعات دیگران جرم محسوب نمی شود مگر آن که رفتارهای شخص مصداقی از سایر رفتارهای بزهکارانه مانند سرقت رایانه ای، دسترسی غیرمجاز و ... باشد. رفتارهایی که جزء رکن مادی تشکیل دهنده سرقت هویت می باشد، استفاده از اطلاعات هویتی دیگری یا انتقال این اطلاعات به دیگری به منظور انجام کلاهبرداری یا سایر فعالیت های غیرقانونی است. ضمن این که به محض کپی یا برش داده دیگری سرقت رایانه ای تحقق می یابد و نیاز به بهره مندی از آن وجود ندارد ولی در سرقت هویت باید از

اطلاعات دیگری سوءاستفاده شود و این که سرقت رایانه ای اختصاص به فضای سایبر دارد اما سرقت هویت هم در فضای واقعی و هم فضای سایبر می تواند تحقق یابد. بنابراین سرقت هویت مشمول مقررات سرقت رایانه ای نمی شود جز این که ممکن است در مواردی یکی از شیوه های دستیابی به اطلاعات دیگران از طریق ربودن داده باشد که در این صورت با توجه به فقدان نص قانونی در باب سرقت هویت عمل این فرد سرقت رایانه ای می باشد. ضمن این که با توجه به تعریف هویت (آنچه که موجب شناسایی می شود) و داده شخصی (ممیزات، مشخصات و اطلاعات راجع به فرد معین که موجب شناسایی و تمایز شخص می شود) اگر جرمی بر علیه داده شخصی نیز صورت پذیرد در واقع جرم بر علیه هویت فرد واقع شده است. بنابراین فارغ از بحث سرقت هویت، اگر فردی داده شخصی متعلق به دیگری را بر باید با داشتن رکن روانی لازم (آگاهی و عمد رفتاری) به سرقت رایانه ای محکوم می شود و اگر داده پیام های شخصی متعلق به دیگری در بستر تجارت الکترونیکی جمع آوری، پردازش و یا توزیع شود نیز به نوعی جرم بر علیه هویت افراد واقع شده است. قانون تجارت الکترونیک مصوب ۱۳۸۲ در ماده ۵۸<sup>۱</sup> و ۵۹<sup>۲</sup> این رفتارها را جرم انگاری نموده است.

رفتارهای تشکیل دهنده کلاهبرداری رایانه ای نیز عبارت است وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم می باشد در حالی که در سرقت هویت لزوم به وقوع رفتارهای فوق وجود ندارد. همچنین سرقت هویت مقدم بر این‌ها است اما می توان سرقت هویت را به عنوان یکی از وسایل متقلبانه برای ارتکاب کلاهبرداری رایانه ای و یا در حد شروع به ارتکاب این جرم مطرح کرد. بنابراین اگر در نتیجه سرقت هویت و پرونده های رایانه ای متعلق به غیر و سوءاستفاده از آن موجبات فریب اشخاص یا سیستم های پردازش خودکار فراهم شده و مرتکب از این راه مال اشخاص را ببرد جرم کلاهبرداری الکترونیک محقق و مرتکب قابل مجازات است.

۱- ذخیره، پردازش و یا توزیع «داده پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است.

۲- در صورت رضایت شخص موضوع «داده پیام» نیز به شرط آن که محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع داده پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد: الف- اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند. ب- «داده پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد. ج- «داده پیام» باید صحیح و روزآمد باشد. د- شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام»های ناقص و یا نادرست را محو یا اصلاح کند. ه- شخص موضوع «داده پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای «داده پیام»های شخصی مربوط به خود را بنماید.

## نتیجه گیری

با توجه به مطالب فوق به نظر می‌رسد جرائم عامی که بر اساس آن‌ها مرتکب سرقت هویت مجازات می‌شود هیچ کدام ناظر بر رفتار فیزیکی محقق کننده آن نیست، برای نمونه در سرقت رایانه‌ای مرتکب خود را به جای مرتکب قلمداد نمی‌کند و صرفاً به برش و کپی اطلاعات اشخاص بسنده می‌کند و در کلاهبرداری رایانه‌ای نیز تنها یکی از پیامدهای این پدیده که بردن سود و مزایای مالی است، مطمح نظر است و آثار دیگر این رفتار از جمله باز کردن حساب بانکی به نام فرد صاحب اطلاعات و دیگر پیامدها را شامل نمی‌شود. در سایر جرایم مانند غصب عنوان نیز شباهت چندانی میان رفتار فیزیکی احساس نمی‌شود چرا که در سرقت هویت، هویت فرد غصب نمی‌شود و تنها از اطلاعات هویتی اشخاص در فعالیتهای غیرقانونی استفاده می‌شود در حالی که در غصب عنوان، فرد مرتکب عنوان دیگری و یا سمت آن را فرد را غصب می‌کند از این رو ضرورت جرم انگاری این رفتار در قالب مقرره‌ای مستقل بیش از پیش احساس می‌شود.

## منابع

- پورقهرمانی، بابک، ۱۳۹۰، سرقت هویت (جعل هویت) جرم ناشناخته رایانه ای، همایش منطقه ای چالش های جرایم رایانه ای در عصر امروز.
- پیمانی، ضیاءالدین، ۱۳۸۵، حقوق کیفری اختصاصی جرایم علیه امنیت و آسایش عمومی، چاپ هفتم، تهران، نشر میزان.
- مصلائی، علیرضا، ۱۳۸۳، جعل و تزویر در حقوق کیفری ایران، چاپ اول، تهران، انتشارات خط سوم.
- میرمحمدصادقی، حسین، ۱۳۸۸، حقوق جزای اختصاصی، جرایم علیه اموال و مالکیت، چاپ بیست و سوم، جلد دوم، تهران، نشر میزان.
- قانون گذرنامه مصوب ۱۳۵۲
- قانون ثبت احوال مصوب ۱۳۵۵
- قانون تخلفات، جرایم و مجازات های مربوط به اسناد سجلی و شناسنامه» در سال ۱۳۷۰
- قانون تعزیرات مصوب ۱۳۷۵
- Ayotte,shawn p,**balancing proportionality and deterrence:the first circuit of victims of identity theft in united states**v.stepanian,new England law review,volume 45,2010.
- Copes,heithand vieraitis,**bounded rationality of identity thieves:using offender based research to inform policy,criminology and public policy**,volume 8,issue 2,2009.
- de vrise, Bald, Tigchelaar, Jet & van der linden, Tina. **“Describing Identity fraud:Towards a common definition”**.vol 5,Issue 3(2008):482-500.
- Grace Close, Angeline: M. Zinkhan, George& R Zachary Finney **.”Cyber identity theft: a conceptual model and implication for public policy”**.( 2003): 1-8.
- Garoupa,nuno,**the economics of business crime,in new perspective on economic crime**,edited xy hans sjogern and goran skogh,new horizons in law and economics,published by Edward elgar publishing limited,2004.
- JAY Hoofnagle , Chris. **“Big Brother’s Little Helpers : how choicepoint and other commercial Data Brokers collect package your Data for law enforcement”**.29 N.C.J.INT’LL & com. REG (2004), 585-598.
- Jay hoofnagle , Chirs.” **InternalizingIdentity theft”**,2010,P1-19.

- Jaap koops, Bert: leenes, Ronald. “**ID Theft, ID Fraud and/or ID related crime**” . Diffinitions matter, Datensicherheit, (2006),553-556.
- Sanchez, Maria.University,Rider. “**The role of the forensic accountant in a medicare fraud identity theft case**”.volume 6,number 3, 2012, 85-92.
- solove, J. Danniel.” **identity theft, privacy , and the architecture of vulnerability**” . , vol 54, (2003), 1227,1232.
- Winn,john and govern,**identity theft:risks and challenges to business of data compromise**,temple journal of social technology and environmental,vohume 18,2009.