

فصلنامه پژوهش‌های دانش انتظامی، سال بیست و چهارم، شماره ۲، تابستان ۱۴۰۱

صص ۵۳-۸۱

## طراحی الگوی جرم‌یابی سرقت هویت در فضای سایبری<sup>۱</sup>

کاووس محمدی<sup>۲</sup>، شهرام ابراهیمی<sup>۳</sup>، غلامرضا شاه‌محمدی<sup>۴</sup>، علی مجبی<sup>۵</sup>

تاریخ دریافت: ۱۴۰۰/۰۹/۲۳ تاریخ پذیرش: ۱۴۰۰/۱۱/۲۸

### چکیده

**زمینه و هدف:** سرقت هویت استفاده غیرقانونی یا غیرمجاز از اطلاعات شخصی، متعلق به شخص دیگری به نفع خود است. سرقت هویت رفتار مجرمانه‌ای است که سارقان هویت با دستیابی غیرمجاز به اطلاعات کاربران از این اطلاعات و بیشتر بانگیزه مادی در فضای سایبر سوءاستفاده می‌کنند. این پژوهش باهدف دستیابی به الگوی مناسبی از کشف جرم سرقت هویت، انجام شده است.

**روش:** این پژوهش به روش کیفی و با استفاده از تکنیک دلفی انجام شده است. جامعه این پژوهش کارشناسان و متخصصان جرم سرقت هویت در ۸ استان از کشور ایران بود که تعداد ۲۰ نفر از متخصصان حوزه سایبری به‌عنوان نمونه آماری با روش نمونه‌گیری هدفمند انتخاب که پس از اجرای هر مرحله از روش دلفی، برای تعیین میزان توافق، از آزمون‌های آماری مقایسه میانگین‌ها و ضریب توافق کندال با بهره‌گیری از نرم‌افزار آماری SPSS، استفاده شد.

**یافته‌ها و نتایج:** بر اساس یافته‌ها، الگوی جرم‌یابی سرقت هویت در ۶۶ شاخصه، ۱۱ مؤلفه و سه مقوله تنظیم شد. مقوله‌های جرم سرقت هویت، ۱- زمینه‌ها و علت‌های وقوع؛ ۲- شیوه و شگردهای مورد استفاده سارقان و ۳- روش‌های کشف سرقت هویت است. شناخت الگوی سرقت هویت در فضای مجازی، کارشناسان پلیس فتا را با علت‌ها، زمینه‌ها و شیوه و شگردهای وقوع و پیشگیری از جرم سرقت هویت سرقت هویت در فضای مجازی کمک می‌کند. از طرف دیگر با شناسایی و معرفی روش‌های کشف، توانایی آنها را در جرم‌یابی افزایش داده و رویه واحدی را ایجاد می‌کند.

**واژه‌های کلیدی:** جرم‌یابی، سرقت هویت، فضای سایبری، جرم سایبری

۱- این مقاله برگرفته از رساله دکتری جرم‌یابی دانشگاه علوم انتظامی امین باعنوان «جرم‌یابی سرقت هویت در فضای سایبری و ارایه الگوی مناسب» است.

۲- دانشجوی دکتری جرم‌یابی دانشگاه علوم انتظامی امین. Kavous1348@gmail.com

۳- دانشیار دانشکده حقوق و علوم سیاسی، دانشگاه شیراز، نویسنده مسئول. shahram.ebrahimi@gmail.com

۴- دانشیار دانشگاه علوم انتظامی امین. drshahmohammadi@chmail.com

۵- استاد دانشگاه علوم انتظامی امین. mohebbiarr@yahoo.com

## مقدمه

سرقت هویت زمینه‌ساز برخی از جرایم از جمله جعل هویت و کلاهبرداری در فضای سایبری بوده و ارتباط بسیار نزدیکی با این جرایم دارد. تاکنون پرونده‌های متعددی برای متهمان سایبری با موضوع سرقت اطلاعات اینترنتی، دسترسی غیرمجاز به داده‌های اینترنتی از طریق ایجاد درگاه‌های جعلی (فیشینگ) و کپی اطلاعات (اسکیمینگ) در محاکم کیفری تشکیل و منجر به صدور رأی شده است. انتقال سریع جرایم از فضای واقعی به فضای سایبری در سال‌های اخیر موانع و محدودیت‌های متعددی را در برخورد با این گونه جرایم ایجاد کرده است. افزایش بزه‌دیدگان جرائم مرتبط با سرقت هویت، خسارات مادی و معنوی ناشی از این جرائم، شناخت ابعاد گوناگون سرقت اطلاعات هویتی افراد، ابزارهای مورد استفاده سارقین هویت، روش‌ها و شگردهای خاص مورد استفاده مرتکبان جرم و مهم‌تر از همه مهارت‌افزایی پلیس برای کشف جرائم مرتبط با سرقت هویت با ارائه الگوی مناسبی از جرم‌یابی در این حوزه دارای اهمیت و ضرورت در این پژوهش است. محدود نبودن مجرمان به زمان و مکان از یک طرف و گستردگی و دسترسی بدون مرز همه افراد به بستر فضای مجازی، وقوع جرم را برای مجرمان آسان و جرم‌یابی آن را برای پلیس با موانع قانونی و مواجهه کرده است. این آسانی در دسترسی به بستر جرم بدون نیاز به حضور در محل دسترسی مجرمان سایبری را در هر نقطه‌ای از جهان به سرقت اطلاعات کاربران آسان و زمینه را برای افزایش جرایم دیگر فراهم می‌کند. محیط جرم‌زای فضای سایبری، متولیان مبارزه با جرایم سایبری را بر آن داشت تا در سال‌های اخیر سازوکاری را فراهم کنند که به کنترل جرم از طریق کشف و با آگاهی بخشیدن به کاربران با رویکرد پیشگیری از افزایش وقوع جرائم در این حوزه جلوگیری کنند. در این میان کشف جرایم و مقابله با مجرمان این حوزه به‌ویژه در جرم سرقت هویت نیازمند الگوی مناسبی از جرم‌یابی برای کارآگاهان فضای سایبری است. الگوی جرم‌یابی که برآیند روش‌های مجرمان و روش‌های جرم‌یابی خبرگان پلیس است، موجب کاهش هزینه‌ها، بهبود عملکرد پلیس و وحدت

رویه در جرم‌یابی پلیس می‌شود. در حال حاضر با توجه به تحقیقات پیشین الگویی که دربرگیرنده تمام ابعاد جرم‌یابی سرقت هویت باشد، وجود ندارد. نبود یک تحقیق جامع در رابطه با طراحی الگوی جرم‌یابی سرقت هویت در ایران و اهمیت این موضوع، محقق را بر آن داشت تا ضمن بررسی و شناخت شرایط (زمینه‌ها و علت‌ها)، شیوه‌ها و شگردهای مورداستفاده سارقان هویت و روش‌های کشف، الگوی مناسبی از جرم‌یابی را در این حوزه ارائه کند. در بررسی موضوع این که ابعاد گوناگون اعم از شرایط (زمینه‌ها و علت‌ها) شیوه‌ها و شگردهای سارقان، و روش‌های کشف سرقت هویت در فضای سایبری چیست؟ به دنبال دستیابی به الگوی مناسبی از جرم‌یابی سرقت هویت برای پلیس هستیم و سؤال اصلی پژوهش این است که؛ الگوی مناسب جرم‌یابی سرقت هویت در فضای سایبری چگونه است؟

### پیشینه و مبانی نظری

نظری منظم، مجیدی، هندیانی و وفادار (۱۳۹۸)، در پژوهشی با عنوان «بررسی عوامل مؤثر بر جرم‌یابی کلاهبرداری در فضای سایبر» نشان می‌دهد که همکاری پلیس با مقامات قضایی، تجهیزات مدرن، علم و آگاهی از علوم رایانه توسط کارآگاهان سایبری و... در کشف جرم کلاهبرداری سایبری تأثیر دارد.

دهکردی و حیدریان (۱۳۹۸)، در تحقیقی تحت باعنوان «تبیین سرقت هویت در نظام کیفری ایران» با روش کیفی (توصیفی-تحلیلی) به بررسی سرقت هویت و جرایم مشابه از دیدگاه کیفری پرداخته و سپس ضمن بررسی فرایند، کاربرد و مشکلات سرقت هویت چگونگی وقوع و ارتباط این جرم را با جرایم مشابه بررسی می‌کند. در نتایج این تحقیق بیان شده که به نظر می‌رسد، در جرایم عامی که بر اساس آن‌ها مرتکب سرقت هویت مجازات می‌شود، هیچ کدام ناظر بر رفتار فیزیکی محقق کننده آن نیست.

غلامی و ابراهیم‌نیا (۱۳۹۸)، در تحقیقی باعنوان «قربانیان سرقت هویت در فضای سایبر با تأکید بر نظام کیفری آمریکا»، بیان داشته‌اند که بسیاری از قربانیان سرقت هویت نه تنها

از منشأ سرقت هویت و دزدی اطلاعات هویتی خود اطلاعی ندارند، بلکه مدت‌های طولانی پس از وقوع سرقت و کلاهبرداری‌های بعد از آن، متوجه موضوع و خسارت می‌شوند و آنجاست که نه تنها یافتن عامل سرقت تقریباً غیرممکن است، بلکه حتی خسارات وارده نیز به راحتی جبران پذیر نیست.

کشمیری (۱۳۹۷)، در تحقیقی با موضوع «سرقت هویت در فضای مجازی» به بررسی تطبیقی این جرم در حقوق ایران و کانادا پرداخته و ضمن تبیین اهمیت این جرم در فضای سایبری ارکان و عناصر تشکیل دهنده این جرم را در حقوق ایران و کانادا به صورت تطبیقی مورد مطالعه و ارزیابی قرار داده است.

محسنی و صوفی زمرد (۱۳۹۶)، در پژوهشی با عنوان «پلیس و چالش‌های اجرایی تأمین امنیت سایبری» بیان داشته که هرچند سیاست‌های تقنینی در حوزه امنیت فضای مجازی تا حدودی جرایم و پاسخ‌های کیفری را تبیین کرده و مناسب با آن سیاست‌های قضایی شکل گرفته اما بسیاری از تدابیر کنشی نیازمند سیاست‌گذاری و تعیین وظایف برای نهادهای اجرایی است. از طرفی موانع عقیدتی و ایدئولوژیک، ابهام در معیارهای حاکم، بر سیاست‌گذاری، ضعف نهادهای اجرایی و دسترسی‌های فنی، تمایل نداشتن بخش‌های خصوصی و عمومی به مشارکت با پلیس، محدودیت‌های ساختاری و نبود توازن در بهره‌گیری از فناوری‌ها مانع از شکل‌گیری یک رویکرد هماهنگ و فراگیر برای مقابله با تهدیدات سایبری شده است.

خالقی و صالح آبادی (۱۳۹۳)، در تحقیقی با موضوع «مطالعه سرقت هویت در حقوق فدرال آمریکا» با روش توصیفی-تحلیلی، با نگاه اجمالی به حقوق ایران با تبیین گونه‌شناسی تغییر هویت، مکانیزم دست‌یابی به اطلاعات شخصی و سرقت هویت از دیدگاه حقوق کیفری آمریکا را مورد بررسی و به ارکان و مجازات این جرم در حقوق آمریکا و ایران به صورت تطبیقی پرداخته است.

فرحی و محمدنسل (۱۳۹۲)، در پژوهشی با موضوع «پیشگیری کیفی از کلاهبرداری اینترنتی» بیان داشته که از بین راه‌کارهای مورد ارزیابی، افزایش نظم حقوقی در جامعه مؤثرترین راه کار پیشگیری کیفی از کلاهبرداری در فضای مجازی است و در همین راه کار نیز مؤثرترین اقدام اطلاع‌رسانی به وسیله رسانه‌های گروهی است.

نیکول لیپر<sup>۱</sup> (۲۰۲۱)، در پژوهشی با موضوع «پیشگیری از سرقت هویت: دیدگاه‌های فناوری راه‌حل‌های خودی‌های صنعت» در مورد دیدگاه‌های شرکت‌کنندگان در گروه تمرکز درباره راه‌حل‌های فن‌آوری خاص برای قربانی سرقت هویت، از جمله اسکن بیومتریک، اسکن وب تاریک، برنامه‌های نظارت مبتنی بر اشتراک، و مشاهدات موضوعی گسترده‌تر در مورد خطر محیط فعلی برای حفاظت از اطلاعات، منابع نوظهور گزارش می‌دهد. ایشان تأکید می‌کند که تمرکز بر جلوگیری از سرقت هویت بدون کاهش آسیب ناشی از تقلب هویت ساده لوحانه خواهد بود. هر راهبردی برای مقابله با جرایم هویت محور، باید پیشگیری و کاهش را ادغام کند.

وین سنت العجا<sup>۲</sup> (۲۰۲۰)، در پژوهشی با موضوع «تحلیل مقایسه‌ای سرقت هویت در آمریکا و استرالیا» به دنبال ارائه بینشی در مورد دلایل نرخ بالای جرم سرقت هویت در ایالات متحده و مقایسه آن با تجزیه و تحلیل عوامل بالقوه با توجه به وقوع آن در استرالیا می‌باشد. وی در این پژوهش به این نتیجه رسیده که در آمریکا تعداد کل خانوارهای ایالتی که به رایانه و فضای نیز دسترسی دارند، بیشتر از استرالیا است. دومین موضوعی که وی به آن دست یافته، این است، در حالی که هم ایالات متحده و هم استرالیا توانایی پیگرد سرقت هویت را تحت کدهای قانونی مربوطه به خود، دارند. قوانین آمریکا متناسب با جرم مجازات بالقوه بیشتری را در برخورد با مرتکبین می‌تواند در پی داشته باشد. یافته‌ها این تحقیق نشان داد که اگرچه آمریکا مجازات‌های سخت‌تری دارد اما

---

1. Nicole Leeper Piquero.  
2. Vincent Alagna

استرالیا سرقت هویت را با نرخ بسیار بیشتری از ایالات متحده تحت پیگرد قانونی قرار می‌دهد.

راجیف گول<sup>۱</sup> (۲۰۱۸)، در تحقیقی با عنوان «سرقت هویت در عصر اینترنت، شواهدی از ایالات متحده آمریکا»، در ساختار اقتصادی دانشگاه ایالتی ایلینوز، به تعیین عوامل سرقت هویت با تمرکز ویژه بر روی نتایج نفوذ انتشار اینترنت می‌پردازد. بر اساس نتایج به دست آمده، در سراسر ایالات متحده سرقت هویت در خانواده‌هایی که امکان دسترسی به اینترنت دارند به ازای ۱۰ درصد افزایش ۹ درصد سرقت هویت افزایش داشته‌است و استخدام نیروهای پلیس در بازدارندگی از جرم سرقت هویت تأثیر داشته‌است.

یرشاد<sup>۲</sup> (۲۰۱۸)، در پژوهشی با عنوان «سرقت هویت و رسانه‌های اجتماعی» با تقسیم‌بندی انواع سرقت هویت به: مالی، پزشکی، کیفی، مصنوعی، کودک، گواهینامه رانندگان، مالیاتی و رسانه‌های اجتماعی، نشان داد که استفاده گسترده از وبگاه‌های رسانه‌های اجتماعی به وضوح قابل مشاهده بوده و ۹۸ درصد قریب به اتفاق افراد اعتراف کردند که حداقل در یکی از این وبگاه‌ها مشخصات شخصی دارند که از بین آن‌ها بهترین مدعی در فیس بوک با ۱۰۱ کاربر بود و در رده دوم اینستاگرام با ۷۷ کاربر و پس از آن گوگل، توئیتر، اسنپ چت و دیگر از شبکه‌های اجتماعی به ترتیب، ۵۲، ۵۱ و ۴۲ کاربر فعالیت داشته‌اند.

فیلیپ. آ.ک. لوریمر، ویکتور مینگ و باراک کانتارک<sup>۳</sup> (۲۰۱۷)، در تحقیقی با عنوان «ارائه الگوی شناسایی مشارکتی جرم‌یابی سرقت هویت بر روی شبکه‌های اجتماعی موبایل» بیان داشته‌اند که محبوبیت استفاده از ابزارهای هوشمند منجر به افزایش استفاده از شبکه‌های اجتماعی برای مقاصد مختلف شده است. هم‌زمان با مزایای آن‌ها، شیوع

1. Rajeevgoel

2. Irshad

3. Philip A. K. Lorimer, Victor Ming-Fai Diec, Burak Kantarci

سرویس‌های شبکه‌های اجتماعی منجر به رفتارهای دارای سوءنیت مانند حمله‌های سایبری یا سرقت هویت شده است.

جیونگ وو، هو جی چوی و جوهرن ترنر (۲۰۱۲)، در تحقیقی باعنوان «ارائه مدل خودکار و فوق‌فعال شناسایی سرقت هویت در بازی‌های آنلاین با کاربران انبوه نقش‌محور» بیان داشته که سرقت هویت معمولاً زمانی اتفاق می‌افتد که در بازی‌های چندکاربره نیاز به نقد کردن دارایی‌های سایبری دارد. در این پژوهش، یک مدل خودکار و فوق‌فعال شناسایی سرقت هویت در بازی‌های آنلاین ارائه شده است.

### مبانی نظری

برای شناخت سرقت هویت، ابتدا باید به بررسی و شناخت هویت پرداخته شود. در بررسی منابع، نظریه‌های متعددی «هویت» را مورد بررسی قرار داده‌اند. از جمله این نظریه‌ها می‌توان به: نظریه مانوئل کاستلز<sup>۱</sup> که هویت را روند ساخته شدن معنا بر پایه‌ی یک ویژگی یا یک دسته ویژگی‌های فرهنگی که بر دیگر منابع معنا برتری دارند تعریف می‌کند (رضایی قادری، ۱۳۹۸، ۱۳). به نظر کاستلز «در جامعه‌ی شبکه‌ای»، برای اکثر کنش‌گران اجتماعی معنا حول یک هویت بنیادی سازمان می‌یابد. این هویت اساسی در طول زمان و مکان قائم به ذات است. اگرچه این رهیافت به نحوه‌ی فرمول‌بندی اریکسون از هویت شباهت دارد، اما در اینجا کانون توجه بیشتر معطوف به هویت جمعی خواهد بود تا به هویت فرد. هرچند که فردگرایی (که با هویت فردی تفاوت دارد) نیز می‌تواند شکلی از هویت جمعی باشد (کاستلز، ۱۳۸۵، ۳-۲۲). به نظر کاستلز تمام هویت‌ها برساخته می‌شوند، اما مسئله‌ی اصلی این است که چگونه از چه چیزی توسط چه کسی و به چه منظوری. برای برساختن هویت‌ها از مواد و مصالحی مثل تاریخ، جغرافیا، زیست‌شناسی، نهادهای تولید و بازتولید، خاطره‌ی جمعی، رویاهای شخصی، دستگاه و مجوز قدرت، وحی و الهامات دینی استفاده می‌شود. اما افراد،

گروه‌های اجتماعی و جوامع، تمامی این مواد خام را می‌پروراند و معنای آن‌ها را مطابق با الزامات اجتماعی و پروژه‌های فرهنگی که ریشه در ساخت اجتماعی و چارچوب زمانی - مکانی آن‌ها دارد، از نو تنظیم می‌کنند. به نظر کاستلنر، این که چه کسی و به چه منظوری هویت جمعی را برسازد تا حد زیادی تعیین کننده‌ی محتوای نمادین هویت مورد نظر و معنای آن برای کسانی است که خود را با آن یکی می‌دانند، یا بیرون از آن تصور می‌کنند. این پرسش که انواع مختلف هویت‌ها چگونه و به دست چه کسی ساخته می‌شوند و چه پیامدهایی دارند، نمی‌تواند به صورت کلی و انتزاعی مورد بحث قرار گیرد. چرا که امری است مربوط به متن و زمینه‌ی اجتماعی. به نظر کاستلنر سیاست‌های مربوط به هویت را باید در جایگاه تاریخی خود بررسی کرد (کاستلنر، ۲۴) و این زمینه‌ی خاص برای او شرط پیدایش جامعه‌ی شبکه‌ای است. بر اساس رویکرد بالا، کاستلنر بین سه صورت و منشاء بر ساختن هویت تمایز قائل می‌شود که هر کدام پیامدهای اجتماعی خاصی دارد:

۱- هویت مشروعیت بخش: این نوع هویت توسط نهادهای غالب جامعه ایجاد می‌شود تا سلطه‌ی آن‌ها را بر کنش‌گران اجتماعی گسترش دهد و عقلانی کند و با نظریه‌های ملی‌گرایی هم‌خوانی دارد و جامعه‌ی مدنی ایجاد می‌کند که منابع سلطه‌ی ساختاری را، البته گاهی به شیوه‌ای بر تعارض، عقلانی می‌سازد. ۲- هویت مقاومت: این هویت که شاید مهم‌ترین شکل هویت‌سازی در جامعه‌ی امروز است، به دست کنش‌گرانی ایجاد می‌شود که در اوضاع و احوال یا شرایطی قرار دارند که از طرف منطبق سلطه، بی‌ارزش دانسته می‌شود و یا داغ‌ننگ بر آن زده می‌شود. به نظر کاستلنر این نوع هویت‌سازی، منجر به ایجاد جماعت‌ها و اجتماعات می‌شود. این هویت شکل‌هایی از مقاومت جمعی را در برابر ظلم و ستم ایجاد می‌کند و معمولاً بر مبنای هویت‌هایی (مثلاً ملی‌گرایی مبتنی بر قومیت) ساخته می‌شود که آشکارا به وسیله‌ی تاریخ، جغرافیا یا زیست‌شناسی تعریف شده‌اند و تبدیل مرزهای مقاومت را به جنبه‌های اساسی و ذاتی آسان‌تر می‌کنند



(کاستلز، ۱۳۸۵، ۲۶). ۳- هویت برنامه‌دار: هنگامی که کنش‌گران اجتماعی با استفاده از هرگونه مواد و مصالح فرهنگی قابل دسترس، هویت جدیدی می‌سازند که موقعیت آنها را در جامعه از نو تعریف می‌کند و به این ترتیب در پی تغییر شکل کل ساخت اجتماعی هستند، این نوع هویت تحقق می‌یابد. از دیدگاه نظریه‌ی اجتماعی، هیچ هویتی نمی‌تواند، یک جوهر به شمار آورده شود و هیچ هویتی به خودی خود خارج از متن تاریخی خود، ارزش متریقی یا ارتجاعی ندارد (کاستلز، ۱۳۸۵، ۵-۲۴). نظریه هویت اجتماعی *تاجفیل* و *ترنر*<sup>۱</sup> هویت را شامل دو وجه فردی و اجتماعی می‌داند. هویت فردی بر جنبه‌های از خود ناظر است که سبب تمایز فرد از دیگران می‌شود و خاص فردی است (رضایی قادری، ۱۳۹۸، ۱۵). همچنین بر اساس نظریه هویت‌یابی آنتونی گیدنز<sup>۲</sup> که تمرکز خود را به ساختار کنش متقابل بین اعتقادات، نیت، اهداف و رفتارهای فردی و جمعی انسان از یک سو و شرایط ساختاری اندیشه و عمل از سوی دیگر معطوف می‌کند، بر اساس نظر ایشان، هرچه افراد در مواجهه با زندگی مجازی فعالیت و مشارکت بیشتری داشته باشند، هویت آنها بیشتر باز اندیشانه است و ویژگی‌های هویت مجازی را دارد و هرچه این مشارکت کمتر باشد، بیشتر شبیه هویت حقیقی است (بریان کرستوفر، جری دیوید و آنتونی گیدنز، ۲۰۰۳، ۲۲).

در بیان مفهوم هویت در فضای مجازی می‌توان گفت که؛ فضای مجازی شیوه تعامل انسان‌ها را متحول کرده است. این فضا دسترسی انسان به اطلاعات ایجاد ارتباطات و توسعه روابط را تسهیل کرده است (شکرخواه، ۱۳۹۰، ۵۷). پس از شناخت هویت و هویت مجازی با توجه به نظریه‌های مختلفی که در رابطه با سرقت هویت مطرح شده است، می‌توان گفت، که یکی از ویژگی‌های سارقان هویت گمنامی و ناشناس بودن است. بر اساس نظریه خود دوم شری *ترکل*<sup>۳</sup> حضور در فضای مجازی به علت

---

1. Henri Tajfel and John Turner

2. Antony Giddens

3. Sherry turkle

ویژگی‌های خاص آن، از جمله گمنامی و حذف آثار فیزیکی به کاربر فرصت می‌دهد که نقش‌های متفاوت را در زمان‌های مختلف بازی کند. از نظر وی کاربران در فضای مجازی از خاصیت گمنامی برای بیان و شرح بخش‌های جستجو نشده و محقق نشده خوده ایشان و ساخت خودی که جعلی است، استفاده می‌کنند (تری شرکل، ۱۹۹۵، ۱۷۸). بنابراین بر پایه این نظریه می‌توان گفت که سارقان هویت با سوءاستفاده از همین گمنامی در فضای مجازی با ترفندهای متفاوت به سرقت اطلاعات کاربران اقدام کرده و به انگیزه مجرمانه خود دست می‌یابند. جایشنکار<sup>۱</sup> در تئوری انتقال فضایی استدلال می‌کند که؛ وقتی افراد از یک فضا به فضایی دیگر می‌روند، متفاوت رفتار می‌کنند (جایشنکار، ۲۰۰۷، ۷). این نظریه دارای محورهای متعددی است که برخی از این محورها در راستای سرقت هویت در فضای سایبری قابل بیان است. وی تأکید می‌کند که ناشناس بودن یکی از مهم‌ترین عواملی است که منجر به فردیت می‌شود. لین لوپوکی<sup>۲</sup> در نظریه عدم دسترسی به اطلاعات شخصی مسئله سرقت هویت را در سرقت اطلاعات توسط سارق نمی‌داند، بلکه مسئله را در شناسایی انسان و امر تصدیق هویت او می‌داند. به نظر او اقداماتی که در رابطه با مبارزه با سرقت هویت انجام می‌شود، بیشتر بر مشکل کردن دسترسی به اطلاعات است و این امر برای مبارزه با سرقت هویت مؤثر و کارآمد نیست (هافنگل، ۲۰۰۴، ۵۹۴). پروفیسور سولو<sup>۳</sup> در نظریه عدم نظارت و کنترل بر اطلاعات شخصی به‌عنوان یک ساختار آسیب‌پذیر سرقت هویت را مسئله نبود کنترل بر اطلاعات شخصی می‌داند (سولو، ۲۰۰۳، ۱۲۳۰). بر اساس این نظریه، سرقت هویت صرفاً اتفاقی واقع نشده، بلکه به واسطه ساختار موجود قانونی شکل گرفته است. 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

- 
1. Jaishankar Karuppanan
  2. Lynn Lopocki
  3. Dannile j Solove

هویت کمتر خواهد بود (هافنگل، ۲۰۱۰، ۱۳). در بحث جرم‌یابی سرقت هویت، برخی از محققین به جرم‌یابی تخصصی بخشی از سرقت هویت پرداخته‌اند. فیلیپ. آ.ک. لوریمر، ویکتور مینگ و باراک کانتراک<sup>۱</sup> (۲۰۱۷)، در تحقیقی با عنوان «ارائه الگوی شناسایی مشارکتی جرم‌یابی سرقت هویت بر روی شبکه‌های اجتماعی موبایل» جرم‌یابی سرقت هویت اجتماعی را به‌طور خاص از طریق شناسایی مشارکتی در شبکه‌های اجتماعی بررسی کرده است. جیونگ وو، هاوا جی چوی و های کانگ کیم<sup>۲</sup> (۲۰۱۲)، در تحقیقی با عنوان «ارائه مدل خودکار و فوق‌فعال شناسایی سرقت هویت در بازی‌های آنلاین با کاربران انبوه نقش محور»، جرم‌یابی سرقت هویت در بازی‌های برخط را بررسی کرده است. بنابراین الگوی نظری تحقیق حاضر بر الگویی تلفیقی استوار است، چرا که مباحث سایبری آن چنان گستردگی خاصی دارد که شناخت دقیق آن نیازمند مباحث مختلف نظری است. براین اساس دیدگاه‌های مختلفی به این موضوع پرداخته‌اند. بدین ترتیب این نظریه‌ها بر اساس شیوه‌های شناسایی و جرم‌یابی سرقت هویت در فضای سایبری منطبق است.

## روش

این پژوهش به‌صورت کیفی و با روش دلفی در سطح پلیس فتای ۸ استان (فارس، بوشهر، هرمزگان، اصفهان، خراسان رضوی، زنجان، شهرکرد و تهران) از کشور جمهوری اسلامی ایران و در سال ۱۴۰۰ انجام شد. در گام اول پس از شناسایی برخی از مؤلفه‌ها، از طریق تحلیل محتوای اسناد، مدارک و... با روش فیش‌برداری مؤلفه‌های اصلی شناسایی و سپس در گام دوم با ابزار پرسش‌نامه محقق ساخته، داده‌ها گردآوری شدند. روایی صوری و ضریب آلفا کرونباخ به ترتیب برای ارزیابی اعتبار و پایایی ابزار سنجش به کار گرفته شدند که ضریب به‌دست آمده در حد قابل قبول (بالای ۰/۷۰) بوده است. پس از دریافت نتایج گام سوم، با توجه به این که تمامی گویه‌ها نمره بالای ۴

1. Philip A. K. Lorimer, Victor Ming-Fai Diec, Burak Kantarci  
2. Jiyoung Woo, Hwa Jae Choi, Huy Kang Kim

و در حد خیلی زیاد و زیاد داشتند و ضریب هماهنگی کندال نیز بالای ۰/۷ حاصل شد، اجرای گام‌های بعدی دلفی متوقف و نتایج در این بخش جمع‌بندی شد. جامعه آماری این پژوهش در بخش تحلیل محتوا شامل مستندات از جمله پرونده‌های مرتبط با سرقت هویت پلیس فتا، ابلاغیه‌ها، دستورالعمل‌ها و برخی مقالات مرتبط با موضوع در سال‌های ۱۳۹۸ و ۱۳۹۹ است و در بخش دلفی تعداد ۲۰ نفر از متخصصان حوزه سایبری به عنوان نمونه آماری با نمونه‌گیری هدفمند انتخاب و دیدگاه‌های آنها درباره جرم‌یابی سرقت هویت مورد پرسش قرار گرفت. در این پژوهش، این گام‌ها تا رسیدن به اجماع درباره الگوی جرم‌یابی سرقت هویت در فضای سایبری از سوی کارشناسان شرکت کننده در مطالعه ادامه یافت و سپس برای دستیابی به الگوی جرم‌یابی، یافته‌های تحلیل محتوای کیفی و روش دلفی با هم مقایسه و مورد استفاده قرار گرفت. پس از اجرای هر گام از روش دلفی، برای تعیین میزان توافق از آزمون‌های آماری مقایسه میانگین‌ها استفاده شد. و در ادامه برای ارزیابی میزان توافق از آزمون آماری ضریب توافق کندال استفاده شد. آزمون‌های آماری گفته شده با استفاده از نرم‌افزار آماری SPSS انجام شد.

## یافته‌ها

### یافته‌های توصیفی:

در بررسی نمونه‌های آماری (جدول شماره ۱) مشارکت کنندگان برحسب درجه، سمت، سطح تحصیلات و سابقه کار مشخص شده‌اند. همین‌طور به تفکیک، طیف درجه کارشناسان با درجه سرهنگی (۴۰ درصد) بیشترین و درجه سرگردی با (۱۰ درصد) کمترین طیف را شامل می‌شود. سمت متخصصان حوزه فضای مجازی با رئیسی (۶۰) بیشترین را به خود نسبت داده‌اند. سنوات خدمتی متخصصان ۲۱ تا ۳۰ سال با (۶۰ درصد) بیشترین و ۱۱ تا ۲۰ سال با (۱۰ درصد) کمترین را شامل شد و تحصیلات مشارکت کنندگان کارشناسی ارشد با (۶۵ درصد) بیشترین و کارشناسی با (۱۵ درصد) کمترین را به خود نسبت داده‌اند.

جدول شماره ۱ توزیع فراوانی پاسخگویان بر حسب سمت، سنوات، تحصیلات و درجه

عنوان	مؤلفه	تعداد	درصد	مؤلفه	تعداد	درصد	عنوان	مؤلفه	تعداد	درصد		
سمت	رئیس	۱۲	۶۰	کارشناس ی	۳	۱۵	درجه، رتبه، رتبه	ستوانیکم	۴	۲۰		
	کارشناس	۵	۲۵	کارشناس ی ارشد	۱۳	۶۵		سروان	۳	۱۵		
	استاد	۳	۱۵	دکتر	۴	۲۰		سرگرد	۲	۱۰		
سنوات	۱۰-۱ سال	۶	۳۰				سرهنگ	۸	۴۰	دانشیار	۱	۵
	۲۰-۱۱ سال	۲	۱۰				استادیار	۲	۱۰			
	۳۰-۲۱ سال	۱۲	۶۰									

## بحث و تحلیل

در بخش تحلیل محتوا پس از استخراج کدها و مفاهیم، زیر مقوله‌ها و مقوله‌های به دست آمده از مصاحبه‌ها، پرونده‌ها و اسناد، نتایج دسته‌بندی شد و در نهایت سه بعد، شامل زمینه‌ها و علت‌های سرقت هویت، شیوه و شگرد سارقان هویت و روش‌های کشف سرقت هویت، مورد تجزیه و تحلیل محتوایی قرار گرفته شد. اولین بعد زمینه‌ها و علت‌های سرقت هویت خود شامل ضعف در زیر ساخت‌های فضای مجازی، ایمن نبودن زیرساخت‌های فضای مجازی، گستردگی جغرافیای جرم سرقت هویت، ضعف بر نظارت و کنترل حوزه فضای سایبری و مشکلات ناشی از سرقت هویت، ناآگاهی کاربران، هویت مجازی و گمنامی سارقان هویت و همچنین نقش بزه‌دیده در وقوع سرقت هویت که مهم‌ترین دلایل وقوع سرقت هویت به شمار می‌روند. دومین بعد یعنی شیوه و شگردهای سارقان هویت، شامل پنج مؤلفه است، که عبارتند از: روش‌های سرقت هویت، مراحل ارتکاب سرقت هویت، ابزار سرقت هویت، زمینه‌ساز بودن سرقت هویت برای سایر جرایم و انگیزه سارقان که در وقوع سرقت هویت تأثیر دارند. در نهایت سومین بعد یعنی روش‌های کشف سرقت هویت، شامل سه مؤلفه هستند، که

عبارتند از: پی‌جویی فنی و کشف سرقت هویت، ابزارهای پیشگیری و کشف سرقت هویت و هماهنگی بین‌المللی و قضایی که در کشف سرقت هویت تأثیرگذار هستند. با ارسال نخستین پرسش‌نامه به مشارکت‌کنندگان با تعداد ۴۱ گویه پاسخ‌های رسیده در گام اول تجزیه و تحلیل شد. در این گام تعدادی ۴۲ گویه جدید توسط شرکت‌کنندگان اضافه شد و یک گویه که نمره حد نصاب را کسب نکرده بودند، حذف شد. نتایج مرحله اول دلفی نشان داد که اکثر افراد نسبت به گویه‌های مورد نظر پاسخ نسبتاً هم‌سانی داشتند. بنابراین در این رابطه سوالاتی که بالای ۶۰ درصد توافق بر روی آنها حاصل شده بود را در گام دوم مدنظر قرار داده و از ۴۱ گویه مطرح شده تنها گویه شماره ۲۶<sup>۱</sup> بوده که نتوانست اجماع نظر مشارکت‌کنندگان را به دست آورد که توسط محقق حذف شد. همچنین تعداد ۴۲ گویه اضافه شده در گام دوم برای دریافت نظر سایر مشارکت‌کنندگان در پرسش‌نامه درج شد. پرسش‌نامه گام دوم (با بازنگری‌های مورد نیاز) با ۸۲ گویه و ثبت نمره میانگین اعضاء و نمره شخص در گام اول تهیه و برای مشارکت‌کنندگان ارسال شد. پاسخ‌های رسیده در گام دوم نیز مورد تجزیه و تحلیل قرار گرفت. در پرسش‌نامه گام دوم ۸۲ گویه مطرح شده مطابق گام اول در قالب طیف لیکرت در اختیار پاسخ‌گویان قرار گرفت که در این رابطه پس از جمع‌آوری پرسش‌نامه‌ها و بررسی آنها از طریق نرم‌افزار SPSS مشخص شد که تعداد ۱۶ گویه (پایین بودن ریسک شناسایی و دستگیری سارقان هویت، علاقه‌مندی بیش از حد کاربران به فعالیت در فضای مجازی، ضعف در پیگیری هویت واقعی مجرمین فضای مجازی، نفوذ به اطلاعات کاربران از طریق هک کردن، استفاده از ابزارهای سخت‌افزاری و نرم‌افزاری برای ذخیره اطلاعات، تخصص و مهارت برای ارتکاب جرم، سرک کشیدن به حریم خصوصی و عمومی کاربران در محیط وب، سرقت اطلاعات از طریق نفوذ با نصب فایل‌های هک‌بازی، سرقت اطلاعات با روش دامین‌های جعلی،

فریب کاربران با روش اتهام‌زنی، دلالتی با اطلاعات مسروقه، ارسال رایانه‌های جعلی برای فریب و سرقت اطلاعات، هک و نفوذ به شبکه‌های رایانه‌ای از طریق ضعف در شبکه، کنجکاوی سارقین هویت در جستجوی کاربران و برنامه‌ریزی مجرمانه در پوشش جستجوی مرسوم و معمولی، بهره‌گیری از ربات‌های الکترونیکی جستجوگر در فضای مجازی، رصد تارنماها و درگاه‌های جعلی بانکی)، نتوانستند حداقل اجماع نظر مشارکت کنندگان را به خود اختصاص دهند و به دلیل این که کمتر از ۶۰ درصد امتیاز را به دست آوردند، این گویه‌ها حذف شدند. همچنین ضریب هماهنگی کندال طبق جدول شماره (۲) برابر ۰/۶۹۵ است که نشان می‌دهد ۶۹ درصد از مشارکت کنندگان با مجموع گویه‌ها هماهنگی دارند.

جدول شماره ۲ ضریب هماهنگی کندال پرسشنامه گام دوم

عوامل تأثیرگذار بر سرقت هویت	
۰/۶۹۵	ضریب هماهنگی کندال
۰/۱۰۰۰	سطح معناداری
۲۰	تعداد

پس از بازنگری در پرسش‌نامه گام دوم تعداد ۱۶ گویه که نمره حد نصاب را کسب نکرده بودند، حذف و پرسش‌نامه گام سوم با ۶۶ گویه نیز با ثبت نمره میانگین اعضاء و نمره شخص شرکت کننده برای مشارکت کنندگان در این پژوهش ارسال شد. پاسخ‌های رسیده در گام سوم مورد تجزیه و تحلیل قرار گرفت (جدول شماره ۳). در این پرسش‌نامه مجموعه‌ای از عوامل ارائه شد که شرکت کنندگان در هر دو دوره اول و دوم آنها را به عنوان عوامل کلیدی و مؤثر بر موضوع مطرح کرده بودند که میانگین تأثیر این عوامل زیاد و بسیار زیاد بود. گویه‌ها دارای وزن ۴ به بالا در مقابل هر عامل نیز میانگین پاسخ‌های اعضای کارگروه در دوره‌های پیشین و پاسخ هر فرد نیز به صورت جداگانه درج شد.

در این گام پاسخ دهندگان باید دوباره نظر خود را درباره میزان تأثیر هر یک از عوامل مؤثر بر موضوع با انتخاب یکی از گزینه‌های موجود در مقابل آنها اعلام می‌کردند و ضریب هم‌هنگی کندال برای پاسخ‌های این دو معادل ۰/۷۹۲ است که نشان از هم‌هنگی حدود ۸۰ درصدی پاسخ‌گویان است (جدول شماره ۳).

جدول شماره ۳ نتایج گام سوم دلفی

ابعاد	مؤلفه‌ها	شاخص‌ها	تعداد پاسخ	میانگین پاسخ	انحراف معیار
	ضعف و نقص در زیرساخت‌های حوزه بانکی.	ضعف در پیش‌بینی الزامات و زیرساخت‌های امنیتی	۲۰	۴,۲۹	۰,۴۶
		ضعف ارائه خدمات توسط سازندگان یا شرکت‌های شبکه‌های اجتماعی در ارائه اطلاعات مورد نیاز	۲۰	۴,۴۱	۰,۵۰۷
		ضعف و نقص در زیرساخت شرکت‌های ارائه‌دهنده خدمات فضای مجازی و کاربرها	۲۰	۴,۳۵	۰,۴۹
		در دسترسی پلیس فتا به زیرساخت‌های داخلی	۲۰	۴,۳۵	۰,۴۹
		ناهماهنگی میان شرکت‌های متولی واگذاری سیم کارت	۲۰	۴,۴۷	۰,۵۱
		ضعف نظارت ناظران و صاحبان فضای سایبری (رها بودن)	۲۰	۴,۸۲	۰,۳۹
زمینه‌ها و علت‌ها	ضعف نظارت بر فضای سایبری	رها بودن فضای کسب‌وکار در فضای مجازی	۲۰	۴,۲۹	۰,۴۶
		نبود مدیریت واحد برای نظارت بر فضای مجازی	۲۰	۴,۵۲	۰,۵۱
		بکارگیری شناسه‌های هویتی جعلی یا عارضیتی	۲۰	۴,۴۷	۰,۵۱
گم‌نامی و ناشناس بودن کاربران در فضای سایبری	گم‌نامی و ناشناس بودن کاربران در فضای سایبری	نبود محدودیت مکانی و زمانی برای بزه‌دیده و بزه‌کار	۲۰	۴,۱۷	۰,۳۹
		به روز شدن مجرمین سنتی در فضای مجازی	۲۰	۴,۱۷	۰,۳۹
		نبود امکان شناسایی هویت کاربران	۲۰	۴,۴۱	۰,۵۰۷
		پایین بودن سطح آگاهی و دانش کاربران	۲۰	۴,۷۶	۰,۴۳
		فرب، تحریک، ترغیب و تطمیع کاربران	۲۰	۴,۲۹	۰,۴۶
		عادی‌انگاری بیش از حد کاربران	۲۰	۴,۵۲	۰,۵۱
		حضور کودکان و نوجوانان در فضای مجازی	۲۰	۴,۱۷	۰,۳۹



۰,۳۹	۴,۸۲	۲۰	متناسب نبودن شبکه‌های اجتماعی بومی با خاستگاه کاربران		
۰,۳۹	۴,۸۲	۲۰	پایین بودن حساسیت کاربران در مراقبت از اطلاعات		
۰,۴۳	۴,۲۳	۲۰	نبود مؤلفه‌های تشویقی دریافت مجوزهای قانونی	نبود نظارت بر حوزه	
۰,۵۰۷	۴,۴۱	۲۰	ورود فرایندها و فعالیت‌های اقتصادی، اجتماعی	کسب و کار در فضای سایبری	
۰,۴۹	۴,۳۵	۲۰	پیچیدگی فعالیت‌ها در فضای مجازی		
۰,۵۱	۴,۴۷	۲۰	اعتماد غیرمنطقی کاربران فضای مجازی		
۰,۴۹	۴,۳۵	۲۰	علاقه‌مندی کاربران به فعالیت‌ها و درآمدهای زود بازده	نبود نظارت بر حوزه کسب و کار در فضای سایبری	زمینه‌ها و علت‌ها
۰,۵۰۷	۴,۴۱	۲۰	ضعف قوانین در الزام سرویس دهندگان	ضعف قوانین در فضای سایبری	
۰,۴۶	۴,۷۰	۲۰	ایجاد درگاه‌های جعلی		
۰,۴۳	۴,۲۳	۲۰	ایجاد وسوسه و تطمیع برای سرقت اطلاعات	روش‌های سارقان هویت	
۰,۴۶	۴,۲۹	۲۰	فرب و اغفال برای ارتکاب جرم		
۰,۴۶	۴,۲۹	۲۰	ارسال دسترسی‌های آلوده برای کاربران		
۰,۴۳	۴,۲۳	۲۰	استفاده از وبگاه‌های قمار آنلاین و پنهان کردن هویت واقعی مجرمین برای سرقت اطلاعات		
۰,۴۹	۴,۳۵	۲۰	کسب منافع مادی و مالی با سرقت اطلاعات		شیوه‌ها و شگردهای سارقان هویت
۰,۵۱	۴,۴۷	۲۰	هدف گذاری سارقین هویت		
۰,۵۱	۴,۴۷	۲۰	استفاده از هویت جعلی و مجازی برای سرقت		
۰,۵۰۷	۴,۴۱	۲۰	استفاده از سرورهای مجازی در خارج از کشور		
۰,۴۳	۴,۲۳	۲۰	کپی برداری از اطلاعات کاربران		
۰,۵۱	۴,۴۷	۲۰	طراحی وب‌گاه‌های سایت جعلی		
۰,۵۰۷	۴,۵۸	۲۰	استفاده از آی پی سیم کارت‌ها و کارت بانکی		

۰,۲۴	۴,۹۴	۲۰	استفاده از شبکه فیلتر شکن‌ها در کشور به صورت آسان و قابل دسترسی	ابزارها و نرم‌افزارهای سرقت هویت	
۰,۴۶	۴,۲۹	۲۰	استفاده از باج‌افزارها و بدافزارها برای سرقت اطلاعات		
۰,۴۶	۴,۲۹	۲۰	استفاده از نرم‌افزارهای جعلی پرداخت هزینه		
۰,۳۹	۴,۸۲	۲۰	استفاده از سیم کارت‌های بی نام و نشان		
۰,۴۳	۴,۲۳	۲۰	انجام مراحل سرقت هویت.		
۰,۴۶	۴,۲۹	۲۰	پی‌جویی از طریق شناسایی سارقان هویت	شیوه‌ها و شگردهای سارقان هویت	نحوه ارتکاب سرقت هویت
۰,۵۱	۴,۵۲	۲۰	بررسی صحنه و جمع‌آوری ادله برای کشف جرم	روش‌های کشف سرقت هویت	پی‌جویی فنی کشف سرقت هویت
۰,۳۳	۴,۸۸	۲۰	ارتقاء سامانه‌ها و بانک‌های اطلاعاتی		
۰,۴۳	۴,۷۶	۲۰	بهره‌گیری از ظرفیت سرویس‌های بین‌المللی		
۰,۲۴	۴,۹۴	۲۰	تعامل و همکاری سازمان‌های دارای زیرساخت		
۰,۲۴	۴,۹۴	۲۰	ایجاد دسترسی به همه سامانه‌ها از جمله سامانه‌های بانکی، ISP و ..		
۰,۵۰۷	۴,۵۸	۲۰	تربیت کارشناسان متخصص جرم‌یابی سرقت هویت		
۰,۳۹	۴,۸۲	۲۰	انتقال تجارب و روش‌های پی‌جویی جرایم سایبری		
۰,۳۹	۴,۸۲	۲۰	انتقال تجارب و روش‌های پی‌جویی جرایم سایبری		
۰,۴۶	۴,۲۹	۲۰	استخراج روش کاربردی و عملی هویت پست vpn		
۰,۵۱	۴,۵۲	۲۰	الزام بازارها و پایگاه‌های واسط مجازی		
۰,۴۳	۴,۷۶	۲۰	پی‌جویی از طریق تراکنش‌های مالی و بانکی		
۰,۴۳	۴,۷۶	۲۰	پی‌جویی از طریق تراکنش‌های مالی و بانکی		
۰,۴۳	۴,۷۶	۲۰	پی‌جویی از طریق اطلاعات و ارتباطات مخابراتی		
۰,۳۳	۴,۸۸	۲۰	ساماندهی کسب‌وکارهای دیجیتال در ابعاد ملی		

۰,۳۳	۴,۸۸	۲۰	تسریع در روند اعلام وقوع جرم برای پی‌جویی و کشف		
۰,۴۹	۴,۳۵	۲۰	دسترسی به داده‌های در اختیار بزه‌دیده برای کشف سرقت هویت		
۰,۳۹	۴,۸۲	۲۰	استخراج اطلاعات از ابزار الکترونیکی متهم مانند گوشی، تبلت و...		
۰,۴۳	۴,۲۳	۲۰	استفاده از نرم‌افزارها و اطلاعات به‌دست آمده در بررسی تشخیص هویت مجرم در فضای مجازی	ابزار کشف سرقت هویت در فضای سایبری	روش‌های کشف سرقت هویت
۰,۴۳	۴,۲۳	۲۰	دسترسی به هاست مرتکبین جرم سرقت هویت		
۰,۴۳	۴,۷۶	۲۰	شفاف‌سازی نحوه استفاده کاربران از فضای مجازی از طریق کد شناسایی و سیم کارت مشخص برای شناسایی سارقان هویت		
۰,۳۹	۴,۸۲	۲۰	بهره‌برداری از دست‌افزارها و نرم‌افزارهای به‌روز جهت استخراج اطلاعات مورد نیاز از ابزار کشف شده از مجرمین (نرم‌افزارها، فارتزیک)		
۰,۴۶	۴,۲۹	۲۰	اعلان قرمز بین المللی برای شناسایی و دستگیری مجرمین.		
۰,۳۳	۴,۸۸	۲۰	دسترسی به بانک‌های اطلاعاتی بین المللی از طریق همکاری پلیس بین الملل		
۰,۴۶	۴,۷۰	۲۰	ارتقاء همکاری‌های حقوقی و قضایی در سطح بین الملل به‌منظور شناسایی و دستگیری مجرمین سرقت هویت	هماهنگی‌های بین‌المللی و قضایی در کشف سرقت هویت	
۰,۴۶	۴,۷۰	۲۰	ارتقاء همکاری‌های حقوقی و قضایی در سطح بین الملل به‌منظور شناسایی و دستگیری مجرمین سرقت هویت		

جدول شماره ۴ ضریب هماهنگی کندال در گام سوم

عوامل تأثیر گذار بر سرقت هویت	
۰/۷۹۲	ضریب هماهنگی کندال

۰/۰۰۰	سطح معناداری
۲۰	تعداد

باتوجه به (جدول شماره ۴) مشاهده می‌شود که پس از توزیع پرسش‌نامه در سه گام بیشترین اجماع در گام سوم با انحراف معیار ۰/۴۴۳ حاصل شده است، در حالی که در گام اول انحراف معیار حدود ۰/۸۶۶ بوده است.

همچنین در بین سه متغیر بیشترین میانگین و کمترین انحراف معیار مربوط به متغیر روش‌های کشف بوده است که بیشترین اجماع در این قسمت حاصل شده است.

**جدول شماره ۵ مقایسه تاثیر گذاری متغیرها بر جرم‌یابی سرقت هویت در دوره‌های سه گانه**

#### دلفی

دور سوم n=17		دور دوم n=17		دور اول n=17		متغیرها
انحراف معیار	میانگین	انحراف معیار	میانگین	انحراف معیار	میانگین	
۰/۴۷	۴/۴۳	۰/۷۴	۴/۱۷	۰/۸۷	۴/۰۳	زمینه‌های و علت‌های وقوع سرقت
۰/۴۵	۴/۴۳	۰/۸۰	۳/۸۸	۰/۹۶	۳/۶۲	شیوه و شگردهای سارقان هویت
۰/۴۱	۴/۶۵	۰/۶۱	۴/۳۹	۰/۷۷	۴/۱۲	روش‌های کشف سرقت هویت
۰/۴۴۳	---	۰/۷۲۸	---	۰/۸۶۶	---	میانگین انحراف معیارها

بخش دوم این پژوهش به روش دلفی در مجموع در سه گام انجام شد. نتایج دوره‌های سه گانه روش دلفی نشان می‌دهند که به دلایل زیر اتفاق نظر میان اعضای کارگروه حاصل شده است و می‌توان به تکرار دوره‌ها پایان داد. اول این که میانگین نظر اعضای کارگروه ۴ به بالا است و این نشان دهنده توافق زیاد و بسیار زیاد در بین آنها دارد. دوم این که بر اساس جدول شماره (۵) میانگین انحراف معیار پاسخ‌های اعضاء درباره میزان اهمیت عوامل مؤثر از ۰/۸۶۶ در دور اول و ۰/۷۲۸ در دور دوم به ۰/۴۴۳ در دور سوم کاهش یافته است. سوم این که ضریب هم‌هنگی کندال برای پاسخ‌های دور سوم معادل ۰/۷۹۲ است که نسبت به ضریب هم‌هنگی کندال در دور دوم تنها ۰/۰۹۷ افزایش دارد که این ضریب با میزان اتفاق نظر میان اعضای کارگروه در میان دو دوره متوالی رشد

قابل توجهی ندارد. بنابراین پس از حصول نتایج گام سوم با توجه به احصاء ابعاد، مؤلفه‌ها و شاخص‌ها، الگوی جرم‌یابی سرقت هویت ترسیم و به شرح (شکل ۱، ۲ و ۳) ارائه شد.



شکل (۱) الگوی جرم‌یابی سرقت هویت در بعد زمینه‌ها و علت‌های وقوع



شکل (۲) الگوی جرم‌یابی سرقت هویت در بعد شیوه و شگردهای سارقان هویت



شکل (۳) الگوی جرم‌یابی سرقت هویت در بعد روش‌های کشف

### بحث و نتیجه‌گیری

برای طراحی الگوی مناسب جرم‌یابی سرقت هویت در فضای سایبری، پس از استخراج کدها و مفاهیم و اجرای گام‌های بخش دلفی، ابعاد، شاخص‌ها و مؤلفه‌های جرم‌یابی سرقت هویت احصاء (جدول شماره ۳)، و در نهایت الگوی جرم‌یابی سرقت هویت در سه بعد از جمله زمینه‌ها و علت‌های وقوع سرقت هویت شامل ۵ مؤلفه و ۲۶ شاخص و در بعد شیوه و شگردهای سارقان هویت شامل ۳ مؤلفه و ۱۷ شاخص و در بعد روش‌های کشف سرقت هویت شامل ۳ مؤلفه و ۲۳ شاخص تعیین و ترسیم شد (شکل ۳-۲-۱). در نتیجه باتوجه به ابعاد به‌دست آمده، مؤلفه‌ها و شاخص‌های جرم‌یابی سرقت هویت به شرح زیر احصاء و نتایج تحلیل شد.

الف- زمینه‌ها و علت‌ها، که مؤلفه‌های آن عبارتند از: ضعف و نقص در زیر ساخت‌ها، ضعف نظارت بر فضای سایبری، گمنامی و ناشناس بودن کاربران در فضای سایبری، ضعف نظارت بر کسب‌وکار و ضعف قوانین که شاخص‌های آن در جدول شماره (۳)

آمده است، این نتایج با تحقیقات پیشین محسنی و صوفی‌زمرد (۱۳۹۶) مبنی بر «پلیس و چالش‌های اجرایی تأمین امنیت سایبری» از حیث ضعف نهادهای اجرایی و... هم‌سو است. باتوجه‌به نظریه نبود نظارت و کنترل بر اطلاعات شخصی به‌عنوان یک ساختار آسیب‌پذیر پروفیسور سولو، سرقت هویت به‌عنوان یک مسئله عدم کنترل بر اطلاعات شخصی است و نبود حفاظت کامل از اطلاعات شخصی که سارقان هویت را قادر می‌سازد به راحتی به این داده‌ها دسترسی پیدا کنند و آن‌ها را به روش‌های تخریبی و مضر مورد استفاده قرار دهند. بنابراین پایین بودن سطح آگاهی و دانش کاربران از مخاطرات فضای مجازی، پایین بودن حساسیت کاربران نسبت به مراقبت از اطلاعات خصوصی از جمله رمز و... در فضای مجازی، عادی‌انگاری بیش از حد کاربران در قبال مخاطرات فعالیت در دنیای مجازی و اعتماد غیرمنطقی کاربران به فعالان فضای مجازی در حوزه‌های اقتصادی و اجتماعی که ناشی از ضعف مراقبت کاربران بر اطلاعات شخصی می‌باشد، در بعد علت‌های احصاء شده در نتایج تحقیق با نظریه‌ی پروفیسور سولو و نظریه نبود دسترسی به اطلاعات شخصی لین لوپوکی و تحقیقات پیشین نظری منظم، مجیدی، هندیانی و وفادار (۱۳۹۸) مبنی بر «بررسی عوامل مؤثر بر جرم‌یابی کلاهبرداری در فضای سایبر» هم‌سو هستند. در مقایسه این پژوهش با تحقیقات پیشین می‌توان گفت که در این بخش علت‌ها و زمینه‌های وقوع جرم به‌عنوان شرایط زمینه‌ساز وقوع جرم مورد توجه قرار گرفته است. همچنین علاوه بر ضعف و نقص‌های زیرساختی به‌عنوان عوامل زمینه‌ساز، به ضعف کاربران در مراقبت از اطلاعات خصوصی خود در فضای سایبری به‌عنوان علت‌های وقوع جرم که زمینه‌ساز جرایم مرتبط در این فضا می‌باشند، به آن نیز پرداخته شده است.

باتوجه‌به نظریه‌ی خود دوم شری‌ترکل، کاربران در فضای مجازی از خاصیت گمنامی برای بیان و شرح بخش‌های جستجو نشده و محقق نشده خود ایشان و ساخت خودی که جعلی است، استفاده می‌کنند. هم‌چنین باتوجه‌به تئوری انتقال فضایی جایشنکار،

مبنی بر ناشناسی در دنیای سایبر، هویت قابل تغییر و انعطاف‌پذیر در این دنیا، که شرایط ارتکاب جرم سایبر را از سوی مجرمان فراهم می‌نماید تا به‌طور ناشناس و با همان ویژگی‌های مطلوبشان مرتکب جرم شوند. بر این اساس سارقان هویت پس از انتقال از فضای واقعی به فضای مجازی با کسب هویت مجازی و عاریتی و تغییر پی‌درپی هویت در فضای مجازی ترفندهای گوناگونی را برای ارتکاب جرم به کار می‌برند، به همین دلیل شناسایی و کشف این‌گونه جرائم نیز با موانع و محدودیت‌های روبرو هستند. بنابراین با توجه به شاخص‌های به‌دست آمده در نتایج ابعاد زمینه‌ها و علت‌های سرقت هویت، هویت جعلی، ناشناس بودن، گمنامی سارقان هویت و پائین بودن سطح آگاهی کاربران از هویت واقعی سارقان هویت را می‌توان با تئوری انتقال فضایی یا نظریه جابجایی مکانی جایسینکار و نظریه‌ی خود دوم شری ترکل در حوزه فضای مجازی هم‌سو و تبیین کرد.

ب- شیوه و شگرد سارقان هویت: یکی دیگر از ابعاد احصاء شده از نتایج این پژوهش شیوه و شگردهای سارقان هویت است که مؤلفه‌های آن شامل: روش‌های سارقان هویت، ابزارها و نرم‌افزارهای سرقت هویت و نحوه ارتکاب سرقت هویت که شاخص‌های آن برابر جدول شماره (۳) است. با توجه به شاخص‌های به‌دست آمده در بعد شیوه و شگردهای سارقان هویت، این نتایج با نتایج تحقیقات خالقی و صالح آبادی (۱۴۰۰) مبنی بر «مطالعه سرقت هویت در حقوق فدرال آمریکا» و با نتایج کشمیری (۱۳۹۷)، مبنی بر «سرقت هویت در فضای مجازی، بررسی تطبیقی حقوق ایران و کانادا» هم‌سو است.

ج- روش‌های کشف سرقت هویت: یکی دیگر از ابعاد حاصله از نتایج این پژوهش، روش‌های کشف سرقت هویت است که مؤلفه‌های آن شامل: روش‌های فنی کشف سرقت هویت، ابزار کشف سرقت هویت و هماهنگی‌های بین‌المللی و قضایی در کشف که شاخص‌های آن در جدول شماره (۳) آمده است. در بررسی مؤلفه‌ها و



شاخص‌های حاصله از نتایج حوزه کشف سرقت هویت، این نتایج با نتایج تحقیقات جیونگ وو، هو جی چوی و جوهرن ترنر (۲۰۱۲) مبنی بر «کشف سرقت هویت از طریق دسترسی به کد شناسایی سارقان هویت در مدل طبقه‌بندی خودکار برای تشخیص هویت سرقت» هم‌سو است.

در رابطه با چگونگی ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌های جرم‌یابی سرقت هویت در فضای سایبری با توجه به ابعاد این پژوهش در نتایج تحقیق که شامل: زمینه‌ها و علت‌های وقوع سرقت هویت، شیوه و شگردهای سارقان هویت و روش‌های کشف می‌باشد، می‌توان گفت که با نظر به این که محقق در این پژوهش به دنبال مشخص کردن روند شکل‌گیری سرقت هویت و کشف آن است، بنابراین در ارتباط بین ابعاد و مؤلفه‌ها و شاخص‌های به‌دست آمده در انجام سرقت هویت باید زمینه‌ها و علت‌های شکل‌گیری هر مؤلفه و شاخص فراهم باشد، تا سارقان هویت با در نظر گرفتن این شرایط، شیوه‌ها و شگردهای جرم را انتخاب و با استفاده از این روش‌ها در فضای سایبری دست به ارتکاب جرم بزنند. از سوی دیگر در مرحله بعدی، روش‌های کشف به‌عنوان یکی از مهم‌ترین ابعاد جرم‌یابی سرقت هویت قرار دارد که در این مرحله جرم‌یابان سرقت هویت باید با شناخت مؤلفه‌ها و شاخص‌های به‌دست آمده در بعد زمینه‌ها و علت‌های وقوع سرقت هویت و دستیابی به شیوه و شگردهای سارقان هویت، بر اساس مؤلفه‌ها و شاخص‌های این بعد که همان روش‌های سارقان هویت است، روش‌های فنی کشف را برای شناسایی و دستگیری سارقان به کار گیرند.

بنابراین این تحقیق ابعاد جرم‌یابی سرقت هویت را به‌صورت همه‌جانبه از شناسایی زمینه‌ها و علت‌های وقوع جرم، شیوه و شگردهای سارقان تا روش‌های کشف سرقت هویت را در نظر گرفته و به آن پرداخته تا روند جرم‌یابی سایبری در این حوزه دقیق و هدفمند صورت گرفته و علاوه بر آن یافته‌های این پژوهش موجب مهارت‌افزایی جرم‌یابان فضای سایبر در رابطه با جرایم مرتبط با سرقت هویت خواهد شد. (شکل

شماره ۲، ۱ و ۳).

### پیشنهادها

۱- در بررسی و تحقیق در مطالعات انجام شده، ضعف نظارت بر حوزه کسب و کار و ساماندهی کسب و کارهای دیجیتالی در فضای مجازی یکی دیگر از مؤلفه‌ها و شاخص‌های به دست آمده در این پژوهش است. در بررسی پرونده‌های پلیس فتا بسیاری از پرونده‌های حوزه کسب و کار مربوط به وبگاه دیوار است؛ بنابراین درپیش گرفتن تمهیداتی مناسب در حوزه ایمن‌سازی زیرساخت‌های فضای سایبری از جمله توسعه و بهره‌گیری از شبکه‌های فضای مجازی ملی و داخلی و تعیین وظایف و نقش و سازمان‌های مسئول در حوزه فضای مجازی از جمله وزارت اطلاعات و ارتباطات، دستگاه انتظامی و قضایی و ... توسط قانون‌گذار در این حوزه ضروری است و واپایش و نظارت بر کاربران به‌ویژه مجرمین این فضا و وبگاه‌ها از طریق یک سامانه نظارتی با مدیریت واحد از طریق دولت در فضای سایبری دارای اهمیت است.

۲- یکی از مؤلفه‌های احصاء شده در بعد زمینه‌ها و علت‌ها ضعف قانون در حوزه سرقت هویت است. در بررسی قوانین موضوعه ایران تاکنون از عنوان سرقت هویت در قانون مجازات اسلامی نامی برده نشده است. با توجه به (ماده ۱)، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ که جرم یاد شده را تحت عنوان، دسترسی غیرمجاز به داده‌ها و مواد (۷۲۹ و ۷۴۰)، قانون مجازات اسلامی مصوب ۱۳۹۲ که جرم مذکور را تحت عنوان (دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی و ربودن داده‌های متعلق به دیگری)، نام برده شده است؛ لذا با توجه به مواد یاد شده قانون‌گذار تاکنون این جرم را تحت عنوان سرقت هویت در قانون مجازات اسلامی، جرم‌انگاری نکرده است و این موضوع می‌تواند به‌عنوان یک کمبود قانونی موانع و محدودیت‌هایی را در برخورد با سارقان و جرم‌یابی سرقت هویت که زمینه‌ساز اغلب جرایم سایبری است را در برداشته باشد.

۳- علاقه‌مندی کاربران به فعالیت در فضای سایبر موجب ارائه حجم وسیعی از اطلاعات بدون در نظر گرفتن محرمانگی و حفاظت از این اطلاعات است که تاکنون در حوزه جرایم مرتبط با سرقت هویت از جمله جعل و کلاهبرداری، پرونده‌های متعددی در سطح کشور ایران تشکیل شده است؛ بنابراین آگاه‌سازی کاربران از طریق آموزش و اطلاع‌رسانی در فضای سایبر و ارائه سازوکار قانونی و زیرساختی مناسب برای حفاظت از این اطلاعات به منظور کاهش پرونده‌های قضایی در این حوزه ضروری به نظر می‌رسد.

### سپاسگزاری

از اساتید حوزه روش تحقیق دانشگاه به‌ویژه جناب دکتر میرفردی استاد دانشگاه شیراز، دکتر آقا رحیمی، دکتر عزیزی و همچنین متخصصان حوزه فضای سایبری، که در انجام این تحقیق، پژوهشگران را حمایت فکری و معنوی کردند تقدیر و تشکر می‌شود.

### منابع

۱. جایشنکار، کی. (۱۳۹۴). جرم‌شناسی فضای مجازی. (حمیدرضا ملک محمدی، مترجم). تهران: نشر میزان. قابل‌بازیابی از: <https://www.gisoom.com>
۲. خالقی، ابوالفتح؛ صالح آبادی، زهرا. (۱۳۹۳). مطالعه سرقت هویت در حقوق فدارال آمریکا با نگاه اجمالی به حقوق ایران. فصلنامه حقوق تطبیقی. (۱۱)، ۲، صص ۸۷-۱۱۴. قابل‌بازیابی از: [http://law.mofidu.ac.ir/article\\_24472.html](http://law.mofidu.ac.ir/article_24472.html)
۳. دهکردی، الهام؛ حیدریان، ارشیا ناز. (۱۳۹۸). تبیین سرقت هویت در نظام کیفری ایران. فصلنامه علمی تخصصی پژوهشنامه حقوق فارس. ۲(۲)، صص ۸۵-۶۳. قابل‌بازیابی از: <http://ensani.ir>

۴. رضایی قادری، خدیجه. (۱۳۹۸). هویت اجتماعی، بازخوانی هویت در رویکرد های نظری. مجله رشد علوم اجتماعی. ۲۲، (۱)، صص ۱۵-۱۲. قابل بازیابی از: <https://www.noormags.ir>
۵. شکرخواه، یونس. (۱۳۹۰). فضای مجازی، ملاحظات اخلاقی، حقوقی و اجتماعی. انتشارات دانشگاه تهران. قابل بازیابی از: <https://www.gisoom.com>
۶. غلامی، علی؛ ابراهیم‌نیا، علی. (۱۳۹۸). قربانیان سرقت هویت در فضای سایبر با تأکید بر نظام کیفری آمریکا. فصلنامه مطالعات حقوق کیفری و جرم‌شناسی. انتشارات دانشگاه تهران. ۴۹(۲)، صص ۴۶۸-۴۴۹. قابل بازیابی از: <https://jqclcs.ut.ac.ir>
۷. فرحی، مهتاب؛ محمد نسل، غلامرضا. (۱۳۹۳). پیشگیری کیفری از کلاهبرداری اینترنتی. فصلنامه پژوهش‌های دانش انتظامی. ۱۶(۳)، صص ۱۶-۱. قابل بازیابی از: <https://www.noormags.ir>
۸. کاستلز، مانوئل. (۱۳۸۵). عصر اطلاعات قدرت هویت. (حسن چاوشیان، مترجم). تهران: انتشارات طرح نو. قابل بازیابی از: <https://www.gisoom.com>
۹. کشمیری، مریم. (۱۳۹۷). سرقت هویت در فضای مجازی (بررسی تطبیقی حقوق ایران و کانادا). انتشارات آذرگان. قابل بازیابی از: <https://www.gisoom.com>
۱۰. گیدنز، آنتونی. (۱۳۷۸). تجدد و تشخیص، جامعه هویت در عصر جدید. (ناصر موفقیان، مترجم). تهران: نشر علم. قابل بازیابی از: <https://www.gisoom.com/book>
۱۱. محسنی، فرید؛ صوفی زمرده؛ محسن. (۱۳۹۶). پلیس و چالش‌های اجرایی تامین امنیت سایبری. فصلنامه پژوهش‌های دانش انتظامی. ۲۰(۴)، صص ۱۸۸-۱۶۳. قابل بازیابی از: [http://pok.rl.police.ir/article\\_18918.html](http://pok.rl.police.ir/article_18918.html)
۱۲. نظری منظم، مهدی؛ مجیدی، عبدالله؛ هندیانی، عبدالله؛ وفادار، حسین. (۱۳۹۸). بررسی عوامل مؤثر بر جرم‌یابی کلاهبرداری در فضای سایبر. فصلنامه پژوهش‌های

- دانش انتظامی. (۲۰۲۱)، صص ۲۴۵-۲۱۸ قابل بازیابی از [http://pok.rl.police.ir/article\\_92091.html](http://pok.rl.police.ir/article_92091.html) :
13. Baykara M. & Ziya Güre Z. (2018). *Detection of phishing attacks*. Retrieved from : <https://www.semanticscholar.org>
  14. Bryant Christofer and Jary David.(2003). Antony Giddens. In RitzerGoerg (eds) “The Blackwell companion to major social Theorists”. Oxford Blackwell.p.22. Retrieved from : <https://sk.sagepub.com>
  15. *Identity Theft And Social Media shareeen Irshad –Tariq Rahim soomro- January (2018). Ucsns International Journal of Computer science and Network security* .Retrieved from : <http://paper.ijcsns.org>
  16. Jaishankar.k.(2007 July 2). *Establishing a Theory of Cyber Crim. International Journal of Cyber Criminology*.Vol 1.p.7. Retrieved from : <https://www.researchgate.net/publication>
  17. Jay Hoofnagle, Chris. (2004). “Big Brother`s Little Helpers : how choicepoint and other commercial Date Brokers collect package your Date for law enforcement” .29 N.C.J.INT`LL & com.REG(2004), 585-598. Retrieved from : <https://scholarship.law.unc.edu/ncilj/vol29/iss4/1/>
  18. Jiyoung Woo, Hwa Jae Choi, Huy Kang Kim (2012). *An automatic and proactive identity theft detection model in MMORPGs*. Retrieved from: <https://koreauniv.pure.elsevier.com>
  19. Nicole Leeper Piquero.(2021).*Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders*. Retrieved from: <https://www.tandfonline.com>
  20. Philip, A. K. Lorimer, Victor Ming-Fai Diec, Burak Kantarci (2017). *PARTICIPATORY DETECTION OF IDENTITY THEFT ON MOBILE SOCIAL PLATFORMS*. Retrieved from: <https://ieeexplore.ieee.org/document>
  21. Rageev k.goel. (2018). *Identity Theft in Cyberspace: MethodsIdentity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing*. Retrieved from: <https://www.lex-electronica.org/files/sites>

22. Turkle.S.(1995). *Life on screen, identity in the age of the internet*. New York: Simon and Schuster.p.178. Retrieved from: <https://journals.sagepub.com>
23. Vincent Alagna (2020) . A Comparative Analysis of Identity Theft within America and Australia. Retrieved from: <https://scholarsarchive.library.albany.edu/honorscollege>
24. Designing a pattern for detecting the crime of identity theft in cyberspace

