هویت سایبری، گذرواژه انتساب مسئولیت کیفری

عبدالرضا جوان‌جعفری بجنوردی* و محمد مقنی‌باشی**

نوع مقاله: پژوهشی	تاریخ دریافت: ۱۳۹۹/۶/۱۹	تاریخ پذیرش: ۱۴۰۰/۴/۲	شماره صفحه: ۳۶۶-۳۳۷

در عصر حاضر با پیشرفت تکنولوژی و وسایل ارتباطی، شاهد حضور چشمگیر کاربران در فضای مجازی هستیم. فضایی رمزآلود و بی‌انتها که با ویژگی‌های منحصربه‌فرد می‌تواند هر سلیقه‌ای را به خود جذب کند. افزایش ارتکاب جرائم سایبری بیانگر علاقه خاص مجرمان به این ویژگی‌ها از جمله گمنامی و حضور قربانیان بی‌اطلاع است. جوامع بشری در استفاده از مجازات به‌عنوان اولین وسیله دفاعی خود در برابر بزهکاران سایبری با چالش عدم شناسایی مجرم روبه‌رو می‌شوند. اما واقعیت این است که مجرمان سایبری از فضای حقیقی پا به این فضا گذاشته‌اند و هویتی نامعلوم ندارند. دستگاه عدالت کیفری با کمک تکنولوژی می‌تواند ردپای به‌جامانده از متهم را دنبال کند و با دستیابی به هویت سایبری و مرتبط کردن آن با اطلاعات موجود از نحوه دستیابی متهم به اینترنت، هویت حقوقی او را در فضای حقیقی شناسایی و مسئولیت کیفری رفتار مجرمانه را بر او بار کند. رمزگشایی از ارتباط میان تکنولوژی و حقوق کیفری در اولین گام از فرایند رسیدگی به جرم سایبری یعنی شناسایی متهم با کمک پروتکل اینترنت یا همان IP امکان‌پذیر می‌شود.

کلیدواژه‌ها: مسئولیت کیفری؛ انتساب؛ هویت سایبری؛ IP

---

* دانشیار گروه حقوق جزا و جرم‌شناسی دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد؛
Email: javan-j@um.ac.ir

** دانشجوی دکتری رشته حقوق جزا و جرم‌شناسی دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد (نویسنده مسئول)؛
Email: Mbm.1993@live.com

فصلنامه مجلس و راهبرد، سال بیست‌ونهم، شماره یکصدونهم، بهار ۱۴۰۱

doi: 10.22034/MR.2021.4296.4249

مقدمه

شاید تا قبل از ظهور اینترنت صحبت از جهانی دیگر منحصراً ذهن را به فضای ماورای زمین معطوف می‌کرد، اما با پیدایش و گسترش اینترنت، فضای سایبر به‌عنوان جهان مجازی زمینه‌ای جدید را برای اکتشافات علمی فراهم کرد، فضایی که در آن ناشناخته و فارغ از قید مکان بودن ویژگی‌های منحصربه‌فردی است که ارمغان آزادی بیان و رفتار را می‌آورد و هر فردی را به بودن و استفاده از آن ترغیب می‌کند (جوان‌جعفری بجنوردی، ۱۳۸۹). امروزه به «هر رفتاری که بر ضد رایانه یا اشخاص (اعم از حقیقی یا حقوقی) با استفاده از شبکه‌های ارتباط از راه دور ارتکاب یابد و در قانون برای آن مجازات‌انگاری شده باشد، جرم سایبری اطلاق می‌شود» (کوره‌پز، ۱۳۹۳). دهکده مجازی اینترنت علاوه‌بر میزبانی از مجرمان فضای حقیقی با توجه به ویژگی‌هایی که در خود دارد، امکان ظهور شکل جدیدی از ناهنجاری‌ها و جرائم را مهیا می‌کند. امروزه رشد جرائم سایبری چه از لحاظ قربانی و چه از حیث تعداد به یک چالش جدی برای جوامع بشری و نهادهای دخیل در مبارزه با جرم تبدیل شده است. مجازات به‌عنوان اولین وسیله‌ای که برای مبارزه با جرائم سایبری به ذهن می‌رسد، در آغاز راه با ابهام گمنامی کاربران سایبری مواجه است و اینکه رفتار مجرمانه به چه کسی منتسب می‌شود؟ شالوده آیین دادرسی کیفری را تعقیب و تحقیق تشکیل می‌دهد، به‌عبارت‌دیگر پس از ارتکاب جرم دستگاه عدالت کیفری به دنبال شناسایی هویت مجرم است تا انتساب مسئولیت کیفری بر وی را بررسی کند. مشخص است که عدم شناسایی هویت مهمترین ابزار مبارزه با جرم را از میدان خارج می‌کند. در فضای سایبری مشکل پیچیده‌تر می‌شود چون کاربران مجازی غالباً هویت حقیقی‌شان را در این فضا فاش نمی‌کنند، بنابراین برای انتساب مسئولیت کیفری و اجرای مجازات ابتدا باید هویت سایبری را شناسایی و سپس آن را به یک هویت حقیقی در فضای حقیقی گره زد. در واقع تعقیب مجرم سایبری عبارت است از تلاش برای برداشتن نقاب هویت سایبری و رسیدن به فردی که با ورود به فضای مجازی مرتکب جرم شده است.

اهمیت شناختن هویت سایبری به‌عنوان شرط ضروری آغاز تعقیب و انتساب مسئولیت کیفری، ضرورت انجام چنین پژوهشی را هویدا می‌کند. مطالعات قبلی فقط بر

سرقت هویت متمرکز شده‌اند و به تعریف و بیان ویژگی‌های آن پرداخته‌اند. ازاین‌رو لازم است تا پیشینه پژوهش‌های انجام شده در زمینه هویت سایبری را برای شناسایی نتایج علمی آن مورد واکاوی قرار داد.

۱. پیشینه پژوهش

در تحقیقی با عنوان «مطالعه سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران» که توسط ابوالفتح خالقی و زهرا صالح‌آبادی به رشته تحریر درآمده است، ابتدا درباره مفهوم سرقت هویت و تفاوت آن با جعل و کلاهبرداری هویت بحث شده و سپس قانون فدرال سرقت هویت آمریکا برای توضیح ارکان جرم سرقت هویت در حقوق فدرال آمریکا مورد مطالعه قرار گرفته است. در پایان نیز سعی شده است موارد مشابه در حقوق ایران احصا و نبود جرم‌انگاری مشابه به تصویر کشیده شود.

طیبی و خدادادی در مقاله‌ای با عنوان «سرقت هویت» به بیان مفهوم و انواع آن پرداخته و مثالی از بزرگترین سرقت هویت در جهان را ذکر کرده‌اند. در پایان قوانین ایران از حیث عدم پوشش کیفری این عنوان را مورد بررسی قرار داده‌اند.

نتیجه بررسی منابع گوناگون نشان می‌دهد مطالعات داخلی در این زمینه با کمبود جدی محتوای پژوهشی مواجه است، اما در میان منابع معتبر لاتین هویت سایبری به‌عنوان دغدغه پژوهشی سهم قابل توجهی از مطالعات حقوق کیفری سایبری را به خود اختصاص داده است.

پژوهش مارکو کاربالو و همکارانش در زمینه مقابله با جرائم سایبری از طریق مطالعه بر ادله فارانزیک در ایالت فلوریدای آمریکا، منجر به انتشار مقاله‌ای با عنوان «هویت سایبر: ویژگی برجسته ماهیتی و چارچوب محاسباتی برای کمک به حل جرائم سایبری» شد. در این پژوهش نویسندگان پس از بیان رشد چشمگیر جرائم سایبری و ناکارآمدی قوانین فدرال و ایالتی در کنترل میزان جرائم سایبری، اقدام به مطالعه پرونده‌های کیفری در این زمینه کردند و مواردی را که مجرمان این حوزه با توسل به آنها اقدامات مجرمانه‌شان را سروسامان می‌دهند را برای یافتن نقطه مشترک برای پنهان سازی هویت را لیست می‌کنند

و نتیجه می‌گیرند با توجه به رشد چشمگیر تکنولوژی و بهره‌برداری مجرمان از این موضوع باید برای کم کردن فاصله سیستم عدالت کیفری با مجرمان از ادله الکترونیکی و شواهد سایبری برای کشف جرم استفاده کرد. برای این منظور هویت سایبری را مطرح و شناسایی آن را با یافتن سه ویژگی رفتاری، بیومتریک و بیوگرافی در شواهد فارانزیک گره می‌زنند. سپس با توضیح هر یک از این عوامل، نقش آنها را برای دستیابی به مجرم سایبری تبیین می‌کنند.

«ویژگی‌های مجرم سایبری بین‌المللی در ایالات متحده آمریکا» عنوان تحقیق دیگری است که توسط هژیدیموا و برایان پین به رشته تحریر درآمد. محققان در این پژوهش با بررسی سوابق مجرمان سایبری زندانی در آمریکا سیمای جنایی آنها را ترسیم کردند. در این مقاله کشور رومانی به‌عنوان کشوری که بیشترین مجرم را در زندان‌های آمریکا دارد و کشور نیجریه به‌عنوان کشوری که بیشترین اقدامات مجرمانه در خصوص سرقت هویت از آنجا پیاده‌سازی شده است، معرفی می‌شوند. بیشترین فراوانی محدوده سنی ۲۴ تا ۲۸ سال اعلام شده است و مرتکبان مرد به‌عنوان گروه پیشتاز از حیث جنسیتی معرفی می‌شوند.

آقای پل چیبوئیک و همکارانش در پژوهشی با عنوان «ابعاد گرایش هویت به‌عنوان همبستگی رفتار سایبری - تهاجمی در بین دانش‌آموختگان دانشگاه آنامبرا نیجریه» عنوان کردند که فضای مجازی ناشناختگی را برای کاربرانش به ارمغان می‌آورد و این مهم موجب ایجاد خلأ هویتی در میان کاربران می‌شود. نحوه فعالیت کاربران که منبعث از شخصیت شکل گرفته آنها در دنیای حقیقی است، نقش بسزایی در پر کردن این خلأ دارد. این امر موجب می‌شود تا گرایش‌های هویتی مختلف در میان کاربران بروز کند. حال اگر این گرایش نشئت گرفته از کاستی‌های شخصیتی کاربر باشد؛ می‌تواند با چاشنی کنجکاوی او را به سمت گرایشی تهاجمی از هویت سوق دهد که موجب شکل‌گیری هویت مجرمانه می‌شود. نتیجه تحقیقات میدانی آنها نشان داد که هرچه تکنولوژی این خلأ را با هویت حقیقی کاربران مرتبط کند، امکان شکل‌گیری بزهکاری سایبری به حداقل می‌رسد. البته محققان به این نکته اذعان داشتند که جمع‌آوری کنترل نشده اطلاعات برای پر کردن این خلأ می‌تواند به نقض حریم خصوصی منجرشود. اما با توجه به نتایج حاصل از رگرسیون خطی

پژوهش نشـان می‌دهند پرخاشـگری حاصل از هویت خودساخته کاربران، قادر خواهد بود میزان بزهکاری و بزه‌دیدگی سایبری را از کنترل خارج کند.

همان‌طـور کـه ملاحظـه می‌شـود در مطالعـات قبلی به یکـی از چالش‌هـای پیش‌روی هویت سایبری با عنوان سرقت هویت پرداخته شده است و در مواردی به بیان ویژگی‌هایی که باید هویت سایبری متصف به آن باشد، بسنده شده است، اما پژوهش حاضر سعی دارد تـا با اسـتفاده از منابـع کتابخانـه‌ای، پرونده‌های کیفری دادسـراهای ویژه جرائم سـایبری، مقـالات تخصصـی فنـاوری اطلاعـات، مؤلفه‌هـای هویـت سـایبری را بـرای برقـراری ارتبـاط بـا هویـت حقیقـی در یک مطالعـه میان‌رشـته‌ای از لحاظ حقوقی شناسـایی کنـد و قابلیت انتساب مسئولیت کیفری را به استناد آن مورد بررسی قرار دهد. ازاین‌رو ابتدا هویت سایبری تبیین، سپس نحوه ایجاد هویت و در نهایت استنادپذیری آن مورد مطالعه قرار می‌گیرد.

۲. از هویت حقوقی تا هویت سایبری

هویت یعنی حقیقت شخص یا شیء که مشتمل بر صفات جوهری او باشد (عمید، ۱۳۹۰). این واژه در علـوم اجتماعـی تعاریـف گوناگونـی را به خود اختصاص داده اسـت و به‌عنوان مفهومی میان‌رشـته‌ای شـناخته می‌شـود. گافمن[1] هویت را این‌گونه تعریف می‌کند: «تلاش انسان برای بـروز تمایـز نسـبت به دیگران اسـت، درحالی‌که بـه رفتار خود شـکل می‌دهد» (ریتـرز، ۱۳۸۲). هویـت از دیـدگاه جامعه‌شناسـی مجموعـه‌ای از ویژگی‌هاسـت کـه فـرد بـه وسـیله آنهـا خود را می‌شناسـد و از دیگران متمایز می‌کند؛ به‌عبارت‌دیگر هویت تلاش انسـان برای یافتن پاسخ به این سؤال است که «من کیستم؟» (باقری دولت‌آبادی و زارعیان جهرمی، ۱۳۹۲).

۲-۱. هویت حقوقی

تعریـف هویـت با توجه به چندبُعدی و وابسـته بودن به رشـته‌های گوناگـون علمی کماکان مبهـم اسـت. در واقـع نگاه کـردن به هویت از ابعاد مختلف پاسـخ‌های مختلفـی را هم برای

1. Goffman

پرسش «من کیستم؟» لیست می‌کند. گاهی این پرسش از قومیت، نژاد، وضعیت اجتماعی یا اقتصادی است و گاهی هم از یک خصیصه حقوقی متمایزکننده میان هم‌نوعانی که در اوصاف گوناگون با هم یکسان هستند (کوهی و حسنی، ۱۳۹۱). به موجب مواد (۹۵۷ و ۹۷۶) قانون مدنی و ماده (۳) قانون الزام اختصاص شماره ملی و کدپستی برای کلیه اتباع ایرانی؛ زنده متولد شدن از پدر ایرانی شرط دارا شدن اهلیت و بهرمندی خصیصه‌های حقوقیِ هویتی مانند نام و نام‌خانوادگی و مهمتر از همه کدملی است. این خصایص در حقوق کیفری نیز اثرگذارند؛ به‌نحوی‌که این موارد برای شناسایی کامل هویت متهم در ماده (۱۹۴) قانون آیین دادرسی کیفری ذکر شده است. برخلاف سایر خصایص هویتی مانند هویت مذهبی یا ملی، هویت حقوقی ثابت است و فرد به سختی می‌تواند آن را انکار کند، به همین دلیل انتساب جرم به افراد، مبتنی‌بر شناسایی این بُعد هویتی خواهد بود.

۲-۲. هویت ابرازی در فضای مجازی

از تعاریف گفته شده می‌توان نتیجه گرفت هویت مجموعه‌ای از معانی است که چگونه بودن را به فرد در یک نقش اجتماعی یا در یک موقعیت خاص القا می‌کند و می‌گوید که در شرایط فعلی او کیست. اما شکل‌گیری این معانی منبعث از ذهن خود فرد است، یعنی هر شخص با قرارگیری در یک نقش یا موقعیت اجتماعی معانی گوناگون را در کنار هم قرار می‌دهد و هویت خود را از آن استخراج و به منصه ظهور می‌گذارد (ذوالفقاری و پرهیز، ۱۳۹۷). حضور در فضای مجازی همان موقعیتی است که فرد را برای داشتن هویت جدید تشویق می‌کند و او را در شرایطی قرار می‌دهد که خود را در این فضا با آنچه از خود شناخته است صاحب هویت و به دیگران معرفی کند. بنابراین هویت ابرازی سایبری تجلی افکار و احساسات افراد نسبت به خودشان است که بدون دخالت عوامل بیرونی به وسیله اشخاص در فضای سایبر نقش می‌بندد، تغییر می‌کند یا از بین می‌رود، پس این هویت می‌تواند منطبق با هویت او در فضای حقیقی باشد یا نباشد (Nagy, 2010). کاربرد این نوع هویت در ساخت پروفایل‌های کاربران در شبکه‌های اجتماعی، سایت‌های اینترنتی، پست‌های الکترونیکی و اپلیکیشن‌های خدماتی مانند تاکسی‌های اینترنتی، دیده می‌شود. در این نرم‌افزارها کاربر

برای ورود و استفاده از قابلیت‌های آن باید خلاصه‌ای از هویت خود را ابراز کند. مطالعه آماری بر روی کاربران شبکه‌های اجتماعی در سطح شهر مشهد نشان می‌داد که ۴۱ درصد کاربران عادی و ۷۸ درصد متهمان به جرائم رایانه‌ای از هویتی ساختگی غیر از هویت واقعی‌شان برای عضویت در شبکه‌های اجتماعی استفاده می‌کنند (آمارنامه سایبری دادسرای ویژه جرائم رایانه مشهد، ۱۳۹۸). هرچند این آمار تأثیر مستقیمی بر عدم استفاده از هویت ابرازی سایبری برای انتساب رفتار مجرمانه به صاحب آن دارد، اما در کنار سایر قرائن می‌تواند به تحصیل علم و انتساب مسئولیت کیفری کمک کند. برای مثال در یکی از پرونده‌های سایبری دادسرای ویژه فضای مجازی مشهد، مدیر یک گروه تلگرامی فرهنگی با اعلام جرم مدعی شد که کاربر ناشناسی با ورود به گروه و ارسال محتویات مستهجن باعث بدبینی نسبت به اهداف گروه و ریزش اعضا شده است. مطالعه بر روی هویت اعلامی این کاربر شبکه اجتماعی تلگرام نشان می‌داد که نامبرده از هویت واقعی خودش برای ایجاد پروفایل[1] استفاده نکرده و صرفاً در قسمت توضیحات خود را حامی حقوق حیوانات معرفی کرده است. همین قرینه کوچک در فرایند تحقیقات، مقام قضایی را به یکی از آشنایان مدیر[2] گروه که مزرعه پروش شترمرغ داشت، مظنون می‌کند و با بررسی تلفن همراه او مشخص می‌شود که وی با همان اکانت[3] مجرمانه در تلگرام[4] فعالیت داشته است (سامانه مدیریت پرونده‌های قضایی، ۱۳۹۸).

هویت ابرازی در واقع محصول الزام کاربران سایت‌ها، درگاه‌ها و برنامه‌های مجازی به معرفی خودشان است. این موضوع سبب می‌شود تا در فضای مجازی، فرد حقیقی دارای هویت‌های ابراز شده متفاوتی باشد. مثلاً برای حضور در سایت کارگزاری بورس و خریدوفروش اوراق بهادار، لازم است ضمن ثبت‌نام در سامانه اینترنتی کارگزاری، برای احراز هویت به دفاتر خدمات الکترونیک مراجعه کند تا از طرف بورس، حائز دریافت کد بورسی

1. Profile
2. Admin
3. Account
4. Telegram

شـود. به همین ترتیب در اپلیکیشـن[1] تاکسـی اینترنتی باید اطلاعات دقیق‌تری مثل آدرس را وارد کنـد ولـی بـرای حضـور در شـبکه اجتماعـی فیس‌بـوک[2] می‌توانـد حتـی جنسـیت خـود را جابه‌جـا وارد کـرده و بـا تصویـر متناسـب بـا آن پروفایـل کاربـری خـود را سـامان دهـد (National Research Council, Kent and Millett, 2003). بنابرایـن هرچـه از اهمیـت فضایـی کـه هویـت حقیقـی کاربـر در آن کاسـته می‌شـود فاصلـه می‌گیریـم، میـزان اطلاعاتـی کـه کاربـر به‌عنـوان هویـت حقیقـی‌اش بایـد ابراز کنـد، کمتـر می‌شـود. نکته مهم ایـن اسـت که در فضای سـایبری امـکان مقایسـه و تطبیق هویت‌هـای ابـرازی در فضاهای مختلـف وجـود ندارد؛ بنابراین مجـرم در قاموس فردی که با انتخـاب عقلانی و برای مصون ماندن از تعقیب و مجازات، فضای گمنام سایبر را برای انجام عملیات مجرمانه‌اش انتخاب کـرده اسـت، سـعی می‌کنـد بـا هویتـی ناقـص ابـرازی از خـود، مرتکب جرم شـود نه بـا هویت دقیـق (هیگنـز و مارکم، ۱۳۹۷؛ Hadzhidimova and Payne, 2019). بنابراین سـایت‌هایی کـه اطلاعـات دقیق‌تری از کاربـر دریافت می‌کننـد، اغلب حوزه فعالیت محـدودی در فضای سـایبر دارنـد و صرفـاً امـکان دسترسـی بـه مخاطبشـان را بـه یـک فضـای محـدود از وب را می‌دهنـد. بـرای مثـال کاربر بـورس با هویت بورسـی خود امـکان حضور در فضای سـایبری بـورس را دارد و دسترسـی بـه شـبکه‌های اجتماعـی با این هویـت برایش مقدور نیسـت. اما نخ تسـبیح همه این هویت‌ها در نحوه اتصال کاربر به اینترنت نهفته شـده اسـت، جایی که تعقیـب زنجیـره اطلاعـات در هر نقطه‌ای از فضای سـایبر ما را به شـخص واحدی در فضای حقیقی می‌رساند.

۳-۲. هویت سایبری

قواعد و ویژگی‌های مربوط به هویت حقوقی در کشـورهای مختلف بسـته به قوانین داخلی کشورها متغیر است. ایران از سال ۱۳۷۶ کدملی را به‌عنوان خصیصه اصلی هویت حقوقی در نظر گرفته است؛ درحالی‌که ملاک اصلی هویت حقوقی در کشورهای توسعه‌یافته، استفاده

1. Application
2. Facebook

از ویژگی‌های بیومتریک مانند اسکن چهره یا اثر انگشت است که به صدور اسناد هویتی بیومتریک[1] منجر می‌شود (Yang and Yang, 2011). از طرفی هویت ابرازی سایبری زاده ذهن کاربران فضای مجازی است و اغلب با هویت واقعی‌شان در فضای حقیقی مطابقت ندارد یا معرف خودآرمان‌گرایی افراد از زندگی شخصی‌شان است (Manago et al., 2008). فضای مجازی متأثر از قوانین داخلی کشورها نیست تا بخواهد قواعد هویت حقوقی را برای انتساب جرم سایبری، به شبکه جهانی اینترنت تسری دهد. قواعد ناظر بر مسئولیت کیفری، التزام و تقبل آثار فعل مجرمانه را به شخص معین و معلوم می‌پذیرد (اردبیلی، ۱۳۹۳) نه شخصی که هویت او ساختگی است و اطلاعاتی از هویت حقوقی او در فضای حقیقی در دسترس نیست. بنابراین ضروری است تا هویتی مخصوص فضای سایبر بدون دخالت کاربران در ایجاد آن و فارغ از قوانین داخلی کشورها شناسایی شود.

نکته حائز اهمیت در این خصوص، نقض حریم خصوصی کاربران است. در واقع ویژگی گمنامی فضای سایبر، عامل مهم گرایش کاربران به استفاده از آن برای صیانت از حریم خصوصی‌شان است. به‌عبارت‌دیگر کاربران می‌خواهند کمترین اطلاعات از آنها برای شناسایی وجود داشته باشد تا فارغ از احتمال نقض حریم خصوصی‌شان، بتوانند آزادانه در فضای سایبر فعالیت کنند؛ اما هویت سایبری در نگاه اول نقض جدی حریم خصوصی را نوید می‌دهد و نگرانی کاربران را در پی دارد، امری که با فعالیت اقتصادی شرکت‌های بزرگ مانند گوگل،[2] مایکروسافت[3] و ... در تضاد است. برای مثال اخیراً درز اخبار همکاری محرمانه مدیرعامل فیس‌بوک با دستگاه‌های اطلاعاتی ایالت متحده در دادن اطلاعات کاربران، حجم عظیمی از نارضایتی کاربران را در پی داشت که منجر به احضار مدیرعامل آن توسط مجالس سایر کشورها شد (Ayaburi and Treku, 2020). بنابراین دست گذاشتن روی حریم خصوصی کاربران برای شناسایی هویت سایبری علاوه‌بر اعتراضات جامعه جهانی، مقاومت جدی شرکت‌های دست‌اندرکار در حوزه سایبری را برای جلوگیری از ریزش منافع

1. Biometric
2. Google
3. Microsoft

اقتصادی‌شان در پی خواهد داشت (Sun, Fang and Hwang, 2019). ازاین‌رو هدفگذاری برای پر کردن خلأ هویتی کاربران با استفاده از الزام آنها به درج اطلاعات بیشتر در این فضا و سپس بهره‌برداری از این اطلاعات برای اتصال هویت سایبری با هویت حقیقی امری غیرممکن است. از طرفی نتایج پژوهش‌های علمی نشان می‌دهد رهاسازی کاربران در خلأ هویتی سایبر می‌تواند به بروز هویت‌های ابرازی مجرمانه منجر شود که افزایش ارتکاب جرم و بزه‌دیدگی بیشتر را به دنبال دارد (Blessing Chidimma et al., 2020). بنابراین باید به دنبال روشی بود تا در عین صیانت از حریم خصوصی کاربران از قربانی شدن آنها نیز پیشگیری کند. به‌عبارت‌دیگر هویت سایبری مطلوب مجرمان را شناسایی و کاربران عادی را در برابر آنها محافظت می‌کند و مانع از نقض حریم خصوصی هر دو گروه می‌شود (Bernabe et al., 2020; Cusack and Ghazizadeh, 2019).

۳. اعطای هویت سایبری

«آرپانت»[1] در سال ۱۹۶۰ توسط وزارت دفاع ایالات متحده آمریکا به منظور سهولت تبادل اطلاعات بین مراکز تحقیقاتی نظامی و جلوگیری از قطع ارتباطات مراکز نظامی در زمان جنگ، شروع به کار کرد و رفته‌رفته با گسترش در سراسر دنیا و پیوستن سایر کشورها به آن، شبکه جهانی اینترنت را پایه‌گذاری کرد (جاویدنیا و کوشا، ۱۳۹۱). این شبکه جهانی از پروتکل‌های امنیتی و ارتباطی منحصربه‌فردی استفاده می‌کند تا انضباط لازم را برای پیوستن دستگاه‌های هوشمند به آن سامان‌دهی کند (Schafer and Serres, 2017). حجم وسیع اطلاعات موجود در این فضا سبب می‌شود تا پروتکل‌های[2] ارتباطی و مسیریابی برای تبادل اطلاعات میان کاربران ایجاد شود. TCP/IP که به اختصار IP[3] از آن یاد می‌شود به‌عنوان پروتکل اصلی ارتباطی در فضای مجازی، وظیفه شناسنامه‌دار کردن کاربران را برای ایجاد سهولت در انتقال اطلاعات را برعهده دارد به این صورت که

1. Arpanet
2. Protocols
3. Internet Protocol

هـر فـرد بـرای ورود به شـبکه جهانـی اینترنت باید از طریق سیسـتم مخابراتی کشـور IP لازم را دریافـت کنـد تـا بتواند بـه اینترنت متصـل شـود (Sridhar, 2019). بنابراین کلیـد ورود به فضـای مجـازی، دریافـت پروتـکل اینترنتـی یـا همان IP اسـت. برخـلاف هویت سـایبری که توسـط کاربران سـاخته و پرداخته می‌شـود، IP متشـکل از مقادیر فرمول‌نویسی شده است که هر جزء آن حامل ویژگی‌های ثابت و غیرقابل تغییری است که کاربر استفاده‌کننده از آن را در فضای مجازی از سایرین متمایز می‌کند و امکان برقراری ارتباط و تبادل اطلاعات را برای وی بـا ایجـاد یـک آدرس منحصربه‌فرد فراهـم می‌کنـد (Wang, Yuan and Archer, 2006). ازایـن‌رو کاربـر برخـلاف هویت ابرازی، نقشـی در ایجاد یا حذف آن نـدارد و داده‌های هویتی آن متأثـر از قواعـد حقوقـی کشـورها نیسـت و پروتـکل اینترنـت خصیصـه هویتـی کاربـر را در فضـای سـایبر تعییـن می‌کند و پاسـخ به پرسـش «من کیسـتم؟» را به نیابـت از او می‌دهد و بـا نگاهی سـایبری و فنی، شـاخه جدیدی را بـه تعاریف هویت تحت عنوان هویت سـایبری اضافـه می‌کنـد. در واقـع IP گواهی سـایبری از کاربر حقیقی به مراجـع قانونی می‌دهد که در صـورت بروز فعل مجرمانه سـایبری، می‌تواند برای دسـتیابی به هویـت حقوقی فرد در عالم واقع و بررسی انتساب جرم به وی کارآمد باشد. برقراری رابطه انتساب میان هویت سایبری و هویت حقوقی مسـتلزم شـناخت چگونگی توزیع و محافظت از IP است تا بتوان مفاهیمی که از هویت سایبری کاربر دریافت می‌شود را به هویت حقیقی او مرتبط کرد.

۱-۳. فرایند توزیع هویت سایبری

ورود بـه عرصـه بی‌کران اطلاعـات در فضای مجـازی در کنـار مزایـای بی‌شـمارش دربردارنده انـواع و اقسـام مختلـف تهدیـدات امنیتـی، اقتصـادی و فرهنگـی اسـت. با گسـترش فناوری و ایجـاد بسـتر اینترنتـی بـرای انجام بسـیاری از امور دولتی حتـی تبادل کوچکتریـن داده، ابتدا ورود آن را به سیسـتم‌های نظارتی آیکان یادآور می‌شـود و سـپس راه مقصد را ادامه می‌دهد. بـرای مثـال جسـتجوی کلمـه «مقالـه» از ایران در گـوگل موجب می‌شـود تا IP مورد اسـتفاده در ایـن زمینـه اطلاعـات درخواسـت شـده را در یک پک رمزنگاری شـده از ایران با اسـتفاده از

شبکه جهانی اینترنت به سرورهای[1] موتور جستجوی شرکت گوگل ارسال کند، اما در بین راه چون وظیفه این نقل و انتقال برعهده اینترنت است ابتدا اطلاعات را به سرورهای آیکان منتقل و از آنجا راهی موتور جستجوی گوگل می‌کند و برعکس اطلاعات دریافتی از گوگل را پس از ورود به سرور آیکان[2] راهی رایانه کاربر در ایران می‌کند؛ درحالی‌که تمام این اقدامات در کسری از ثانیه رخ می‌دهد و کاربر احساس می‌کند که بدون واسطه با گوگل ارتباط گرفته است (Zalnieriute, 2019). موضوعی که در سال ۲۰۱۴ اعتراضات جهانی را علیه آیکان برای نقض حریم خصوصی و جاسوسی از کاربران اینترنت به نفع دولت آمریکا در پی داشت و موجب شد تا کشورها را به فکر تأسیس یک نهاد بین‌المللی در سازمان ملل برای مدیریت و نظارت بر پروتکل‌های اینترنتی بیندازد، طرحی که تاکنون با مقاومت آمریکا در سازمان ملل منتج به نتیجه‌ای نشده است (Perrin, 2018). از سوی دیگر مصارف اینترنت در بخش‌های مختلف نیازمند سرعت و دسترسی متفاوت است که مدیریت آن مستلزم در اختیار داشتن شاه‌راه اینترنت است. در کنار این موارد وقوع حملات و تهدیدهای سایبری در سال‌های اخیر سبب می‌شود تا دولت رأساً مدیریت اینترنت را برعهده گیرد و نحوه دستیابی کاربران به اینترنت را مدیریت کند. ازاین‌رو باید پروتکل اینترنت تهیه و طی فرایندی شفاف در بین کاربران توزیع شود (شهبازی، شفیعی و ابوطالبی، ۱۳۹۰). اما اینکه چه ارگانی وظیفه تهیه IP را برعهده دارد و چه اشخاصی در امر توزیع دخالت دارند، موضوعاتی هستند که توضیح آنها مشخص‌کننده پروسه‌ای است که دولت مطابق آن حاکمیت خود را بر موضوع اینترنت اعمال می‌کند.

۱-۱-۳. تأمین‌کنندگان خدمات دسترسی

در فضای حقیقی سازمان ثبت احوال وظیفه دارد تا برای ایرانیان مدارک هویتی از قبیل شناسنامه و کارت ملی صادر کند و افراد هم براساس اطلاعات هویتی‌شان می‌توانند نیازهای اجتماعی خود را برطرف کنند، برای مثال حساب بانکی افتتاح، سیم‌کارت خریداری و فعال‌سازی کنند. در فضای سایبر موضوع کاملاً متفاوت است و دولت‌ها نقشی در ایجاد

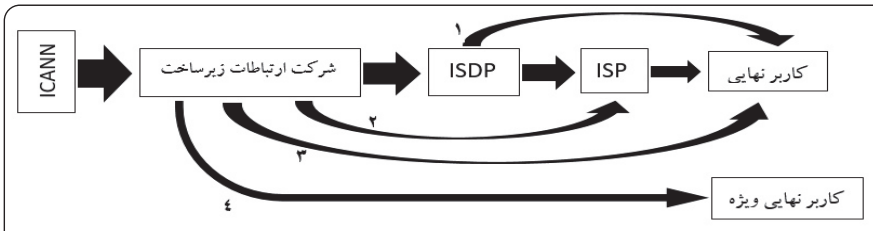
1. Servers
2. Internet Corporation for Assigned Names and Numbers

هویت سایبری ندارند، بلکه وظیفه توزیع آن را بین کاربران اینترنت برعهده دارند. همان‌طور که بیان شد وزارت دفاع ایالات متحده طراح و توسعه‌دهنده شبکه گسترده جهانی اینترنت است و از همان ابتدا صدور و واگذاری IPهای معتبر و دسترسی به این شبکه را در شرکت آمریکایی آیکان برعهده دارد و با تنظیم پروتکل اینترنت به افرادی اجازه اتصال به فضای مجازی را می‌دهد که IP معتبر داشته باشد. کشورها با اخذ IPهای معتبر از این شرکت و با سازوکار مختص به خود نسبت به توزیع آن بین کاربران اقدام می‌کنند تا اطلاعات افرادی که با استفاده از آن وارد فضای سایبر می‌شوند را در اختیار داشته باشند و نظارت لازم را اعمال کنند. برای تبیین بهتر موضوع پیگیری مباحث آتی با یک مثال عاریه‌ای راهگشا خواهد بود. رانندگی در جاده‌های شهری و بین‌شهری مستلزم استفاده از خودرویی است که دارای پلاک انتظامی است، در واقع شماره انتظامی موجب شناخته شدن اتومبیل در میان میلیون‌ها وسیله نقلیه دیگر خواهد شد. برای سامان‌دهی عبور و مرور و اعمال سیاست‌های ترافیکی باید تصویر روشنی از تردد وسایل نقلیه وجود داشته باشد. ازاین‌رو نیروی انتظامی برای نظم دادن به حوزه حمل‌ونقل مسئول صدور و توزیع پلاک شده است، وظیفه‌ای که در موضوع پروتکل اینترنت در سطح بین‌المللی به آیکان واگذار شده (Becker, 2019) و در سطح ملی به وزارت ارتباطات محول شده است. شرکت ارتباطات زیرساخت که یکی از شرکت‌های دولتی زیرمجموعه وزارت ارتباطات است، وظیفه تأمین IP مورد نیاز داخل را برعهده دارد. تأمین IP در واقع همانند فرایند صدور پلاک است با این تفاوت که برای صدور پلاک، شهروند متقاضی اطلاعات خود برای خرید وسیله نقلیه را قبلاً در اختیار ناجا قرار داده است و آنها براساس این اطلاعات هویتی، شماره انتظامی منحصربه‌فردی را صادر می‌کنند، سپس با اطلاعاتی که بر روی آن ثبت است سیاستگذاری می‌کنند. اما در خصوص IP قضیه کاملاً متفاوت است چراکه دولت IP را صادر نمی‌کند، بلکه آن را بعد از تأمین میان کاربران توزیع می‌کند. بنابراین دولت چگونه می‌خواهد بر IPهای بی‌نام و نشان اعمال حاکمیت کند؟ به‌عبارت‌دیگر چگونه متوجه خواهد شد که چه IPای در اختیار چه شخصی است؟ بنابراین لازم است تا بعد از تأمین پروتکل اینترنت و در زمان توزیع تدابیری را اتخاذ کند تا دغدغه‌های او را نسبت به بهره‌برداری از هویت سایبری تا حدودی مرتفع شود.

۲-۱-۳. توزیع‌کنندگان خدمات دسترسی

پس از تأمین خدمات دسترسی، وزارت ارتباطات به وسیله سازمان تنظیم مقررات رادیویی مجوز لازم را به شرکت‌های ارتباطی خصوصی برای توزیع IP میان کاربران نهایی یا شرکت‌های عرضه‌کننده اینترنت صادر می‌کند. عرضه‌کنندگان اینترنت[1] می‌توانند پهنای باند را به کاربران نهایی عرضه کنند یا به شرکت‌های دیگری برای توزیع میان کاربران نهایی واگذار کنند. بنابراین شرکت‌های توزیع‌کننده اینترنت[2] در نهایت وظیفه توزیع اینترنت را برعهده می‌گیرند. شرکت ارتباطی تلفن همراه و شرکت‌های ارائه‌دهنده خدمات ADSL به‌عنوان شرکت‌های شناخته شده توزیع اینترنت در ایران شناخته می‌شوند (جاویدنیا و کوشا، ۱۳۹۱). اهمیت شرکت‌های توزیع‌کننده اینترنت به این دلیل است که وظیفه نهایی توزیع هویت سایبری را میان کاربران برعهده دارند و باید اطلاعات استفاده کاربران را حفاظت و نگهداری کنند تا در مواقع ضروری ارائه این اطلاعات بتواند ارتباط لازم میان هویت سایبری و هویت حقوقی برای انتساب مسئولیت کیفری را برقرار کند (Bates, Bavitz and Hessekiel, 2017).

شکل ۱. ساختار توزیع هویت سایبری



۱- برخی کاربران برای داشتن اینترنت پرسرعت، دسترسی خود را از ISPDها خریداری می‌کنند.

۲- برخی ISPها برای ارائه توزیع اینترنت‌های با کیفیت‌تر IPهای خود را مستقیم از شرکت ارتباطات زیرساخت تهیه می‌کنند.

۳- برخی کاربران نهایی که نیازمند دسترسی بیشتر و پرسرعتر به اینترنت هستند مانند دانشگاه‌ها و مراکز تحقیقاتی، به صورت مستقیم رنج IPاشان را از شرکت ارتباطات زیرساخت تهیه می‌کنند.

٤- کاربرانی که سطح دسترسی آن‌ها نیازمند رعایت پروتکل‌های امنیتی و دسترسی هدفمند می‌باشد به صورت ویژه به وسیله‌ی شرکت ارتباطات زیرساخت به اینترنت دسترسی می‌یابند. مانند بانک‌ها و ارگان‌های دولتی.

1. Internet Service Distribution Provider (ISDP)
2. Internet Service Provider (ISP)

شکل ۱ نشان می‌دهد که چگونه پروتکل اینترنت توسط شرکت ارتباطات زیرساخت، تأمین و برای توزیع در اختیار شرکت‌های عرضه‌کنندگان اینترنت و توزیع‌کننده اینترنت قرار می‌گیرد. این شرکت‌ها به موجب دستورالعمل‌های سازمان تنظیم ارتباطات رادیویی زمانی مجوز واگذاری IP به کاربر را دارند که پس از احراز هویت حضوری کاربران در چارچوبی از قبل تعیین شده اطلاعات هویتی آنها را ثبت و ضبط کنند. ازاین‌پس مشخصات IP که برای هر بار اتصال به اینترنت در اختیار کاربر قرار می‌گیرد در ردیف اطلاعات هویتی او ثبت می‌شود. در واقع شناسنامه‌دار کردن هویت سایبری با اطلاعات هویت حقوقی وظیفه این شرکت‌هاست (سازمان تنظیم مقررات و ارتباطات رادیویی، ۱۳۸۵). برای مثال دانشگاه به‌عنوان کاربر نهایی نسبت به تهیه IP از شرکت ارتباطات زیرساخت اقدام و تعداد هزار آدرس IP را با تنظیم قرارداد اخذ می‌کند و آنها را در اختیار دانشجویان، اساتید و بخش اداری خود قرار می‌دهد. بدیهی است که هر اتفاقی که در فضای سایبر با این رنج از IPها رخ دهد؛ شرکت ارتباطات زیرساخت در استعلام دانشگاه را صاحب آن اعلام می‌کند. بنابراین دانشگاه‌ها برای جلوگیری از چنین اتفاقی، جداگانه در نقش یک شرکت توزیع‌کننده اینترنت ظاهر شده و براساس شماره دانشجویی یا کد پرسنلی نسبت به تعریف کاربری جداگانه برای اعضای خود اقدام می‌کند تا در صورت بروز مشکل بتوان شخیص داد هویت سایبری در اختیار چه شخصی بوده است؟ این مثال و بسیاری از موارد مشابه نشان می‌دهد که هویت سایبری گونه‌های مختلفی دارد که شناخت ویژگی هر یک نقش مهمی در برقراری رابطه مسئولیت کیفری ایفا خواهد کرد.

۲-۳. گونه‌شناسی هویت سایبری

توسعه و برقراری خدمات دسترسی به اینترنت برای کشورهای مختلف در اختیار شرکت آمریکایی آیکان است. این شرکت با پیروی از سیاست‌های دولت فدرال[1] آمریکا نحوه عملکرد خود را با دولت‌های دیگر سامان‌دهی می‌کند. به همین دلیل این شرکت همسو

1. Federal

با تحریم‌های اقتصادی آمریکا علیه ایران، میزان IP بسیار کمتری را در اختیار ایران قرار می‌دهد. از طرف دیگر سیاست‌های داخلی در ایجاد محدودیت برای کاربران اینترنت از طریق پالایش محتوا و فیلترینگ[1] سبب می‌شود تا کاربران نهایی برای دسترسی به اینترنت، با گونه‌های متفاوتی از هویت سایبری مواجه شوند. بدیهی است شناخت انواع مختلف IPهای استفاده شده توسط کاربران به برقراری دقیق‌تر ارتباط میان هویت حقیقی با هویت مجازی کاربر و در نهایت تشخیص انتساب مسئولیت کیفری در فضای سایبر کمک شایانی می‌کند. استعلام شماره پلاک انتظامی می‌تواند به رفع پیچیدگی بحث کمک کند. تصور کنید یک دستگاه اتوبوس با پلاک مشخص که هر روز وظیفه حمل‌ونقل عمومی مسافران را با راننده‌ای متفاوت در سطح شهر برعهده دارد، وسیله ارتکاب جرم واقع شود، پرسش اول برای رسیدن به راننده خاطی این است که شماره پلاک آن چه عددی بوده است؟ اما آیا رسیدن به پلاک وسیله‌ای که هر روز با یک راننده در سطح شهر تردد داشته، می‌تواند راهگشا باشد؟ پاسخ مثبت است چراکه دستیابی به پلاک موجب می‌شود تا خیل عظیمی از وسایل مشابه از مظان اتهام خارج شوند. در پرسش بعدی از شرکت خدمات حمل‌ونقل عمومی که راننده را استخدام کرده است، می‌توان در تاریخ و ساعت وقوع حادثه به متهم رسید. با این توضیح که هر اتوبوس در شیفت کاری مشخص از طرف شرکت حمل‌ونقل در اختیار راننده‌ای است که مشخصات او در زمان تحویل وسیله ثبت و ضبط می‌شود، بنابراین رسیدن به پلاک وسیله نقلیه در کنار تاریخ و ساعت وقوع حادثه، مشخص می‌کند که راننده خاطی چه کسی بوده است. IP همانند اتوبوسی است که به دلیل تحریم توسط شرکت ارائه‌دهنده خدمات دسترسی در اختیار کاربران متعددی قرار می‌گیرد ولی در صورت وقوع جرم اطلاعات فنی ضبط شده از آن در سیستم‌های شرکت می‌تواند مشخص کند که هویت سایبری متعلق به شخصی بوده است. اما اگر راننده اتوبوس با هر وسیله‌ای پلاک را پنهان کند آیا باز هم می‌توان به راحتی مثال قبل، مسئولیت کیفری را به شخص معین منتسب کرد؟ حال اگر برای IP چنین اتفاقی رخ دهد شرکت‌های ارائه‌دهنده خدمات

1. Filtering

دسترسی، اطلاعاتی برای کمک به دستگاه عدالت کیفری دارند؟ با ذکر این مثال‌ها ویژگی‌های دوگونه اصلی از هویت سایبری تشریح خواهد شد.

۱-۲-۳. هویت سایبری تقسیم شده

عدم همکاری آیکان با ایران در اختصاص میزان IP مورد نیاز و حجم بالای تقاضای اینترنت در کشور سبب می‌شود تا شرکت‌های توزیع‌کننده اینترنت با برنامه‌نویسی و استفاده از فناوری‌های مرتبط هر شناسه، IP معتبر را به چندین IP وابسته یا NAT[1] تبدیل کنند و به‌این‌ترتیب تعداد IP مورد نیاز کاربران را برای اتصال به اینترنت فراهم کنند. به‌عبارت‌دیگر هویت سایبری در داخل کشور میان کاربران مختلف به اشتراک گذاشته می‌شود. به این صورت که در آن واحد چند نفر با هویت سایبری یکسان امکان حضور در فضای سایبر را دارند، اما به صورت مشخص شرکت‌های توزیع‌کننده اینترنت با توجه به برنامه‌نویسی که انجام داده‌اند؛ اطلاعات ردوبدل شده هر کاربر را در فضای مجازی با یک IP NAT طبقه‌بندی می‌کند که در مواقع ضروری می‌توان رفتار هر یک از کاربران را مورد تجزیه‌وتحلیل قرار داد، هرچند این امر به‌عنوان یک چالش اساسی در رسیدگی‌های قضایی شناخته می‌شود. برای مثال در یک پرونده کلاهبرداری رایانه‌ای، مجرم با IP NAT و با دسترسی به اطلاعات کارت بانکی بزه‌دیده اقدام به خرید از یک فروشگاه اینترنتی می‌کند. نتیجه تحقیقات نشان می‌داد که در زمان خرید از فروشگاه توسط متهم، هفت نفر دیگر با همان IP به اینترنت متصل بودند، اما فقط دو نفر از آنها به درگاه پرداخت الکترونیک متصل شده بودند (سامانه مدیریت پرونده‌های قضایی، ۱۳۹۸). درهرحال تجزیه‌وتحلیل خرید هر یک از این کاربران و انطباق آن با فروشگاه اینترنتی و کالایی که توسط متهم خریداری شده، برای برقراری رابطه میان رفتار و مرتکب آن و در نهایت انتساب مسئولیت کیفری، بسیار زمان‌بر است. این در حالی است که سرعت ارتکاب جرائم رایانه‌ای بسیار بالا و تعداد افراد بیشتری در معرض قربانی شدن قرار دارند (جوان‌جعفری بجنوردی و فرهادی آلاشتی، ۱۳۹۵).

---

1. Network Address Translation (NAT)

۲-۲-۳. هویت سایبری پنهان شده

سیاست‌های دولت در مواجهه با آسیب‌های فرهنگی و اجتماعی فضای سایبر سبب شده است تا تدابیر فناورانه متنوعی برای کنترل اوضاع اتخاذ شود. یکی از این تدابیر پالایش و فیلتر محتوا و اطلاعاتی است که دسترسی به آنها از نگاه حاکمیت با ارزش‌ها و هنجارهای جامعه منافات دارد. به‌عبارت‌دیگر چون ارائه خدمات دسترسی، توسط دولت مدیریت می‌شود و محدوده IPهای فعال و در دسترس کاربران مشخص است، می‌توان با استفاده از فیلترینگ هوشمند دسترسی این IPها را به برخی از اطلاعات محدود کرد؛ به نحوی‌که امکان دسترسی به آن اطلاعات با هویت سایبری که در اختیار دارند، غیرممکن شود (Ni et al., 2010).

پیشرفت تکنولوژی و پیدایش شبکه‌های خصوصی مجازی، سبب می‌شود تا سامانه‌های فیلترینگ کارایی لازم را نداشته باشند و کاربران بدون محدودیت بتوانند اطلاعات را در فضای مجازی دنبال کنند. نحوه عملکرد شبکه‌های خصوصی مجازی که به اختصار فیلترشکن[1] نامیده می‌شوند به این صورت است که این شبکه مجازی برای سامانه فیلترینگ به‌عنوان داده مخرب شناخته نمی‌شود، بنابراین کاربر با هویت سایبری که در ایران تهیه کرده است به این شبکه متصل می‌شود و از این طریق با یک IP جدید اما ناشناس برای سامانه فیلترینگ داخلی وارد فضای مجازی می‌شود و اطلاعات خود را از همین مسیر دریافت می‌کند بدون اینکه سامانه فیلترینگ متوجه شود و شرکت‌های توزیع‌کننده اینترنت اطلاعات هویتی او را ثبت کند. ذکر این نکته ضروری است که اساس اتصال به شبکه جهانی اینترنت، داشتن IP معتبر است. اینکه بگوییم فیلترشکن هویت سایبری را دگرگون می‌کند، کاملاً نادرست است. فیلترشکن صرفاً هویت سایبری کاربر را در پوششی ناشناس و رمزنگاری شده قرار می‌دهد، به‌گونه‌ای که توزیع‌کنندگان اینترنت داخلی که از سیستم فیلترینگ هوشمند تبعیت می‌کنند، نمی‌توانند تشخیص دهند که داده‌های رمزنگاری شده چیست. در واقع فیلترشکن برای دسترسی کاربر به اینترنت مسیر تازه و ایمنی را جدا از شکل ۱ ایجاد می‌کند ولی در هر حال اطلاعات هویت سایبری

1. Virtual Private Network (VPN)

معتبر او در سرورهای شبکه خصوصی مجازی ثبت و ضبط شده است؛ اما توزیع‌کنندگان اینترنت ایرانی هویتی پنهان شده از کاربر را در حافظه خود ضبط می‌کند و اطلاعی از هویت سایبری اصلی او ندارد (فرهادی آلاشتی، ۱۳۹۵). ذکر این نکته ضروری است که اساس اتصال به شبکه جهانی اینترنت، داشتن IP معتبر است و بیان اینکه فیلترشکن هویت سایبری را دگرگون می‌کند، کاملاً نادرست است چرا که فیلترشکن فقط هویت سایبری کاربر را در پوششی ناشناس و رمزنگاری شده برای شرکت‌های توزیع‌کننده اینترنت داخلی که از سیستم فیلترینگ هوشمند تبعیت می‌کند، تعریف می‌کند و برای دسترسی او به اینترنت ایجاد مسیر تازه و ایمنی را ایجاد می‌کند ولی درهرحال اطلاعات هویت سایبری معتبر او در سرورهای شبکه خصوصی مجازی ثبت و ضبط شده است اما شرکت‌های توزیع‌کننده اینترنت ایرانی هویتی پنهان شده از کاربر را در حافظه خود ضبط می‌کند و اطلاعی از هویت سایبری اصلی او ندارد (فرهادی آلاشتی و جوان‌جعفری بجنوردی، ۱۳۹۵). متأسفانه استفاده مجرمان سایبری از قابلیت پنهان‌سازی فیلترشکن برای برقراری رابطه انتساب مسئولیت کیفری، مشکل ایجاد می‌کند. آمارهای پرونده‌های کیفری گویای استفاده ۹۳ درصدی متهمان جرم کلاهبرداری رایانه‌ای از سرورهای مجازی برای پنهان کردن هویت سایبری است و چون شرکت‌های توزیع‌کننده اینترنت ایرانی مشخصه‌های هویت سایبری متهم را در اختیار ندارد، نمی‌تواند دستگاه عدالت کیفری را برای دستیابی به هویت حقیقی متهم یاری کند و عملاً دستیابی به متهمان از این طریق با شکست مواجه می‌شود (آمارنامه سایبری دادسرای ویژه جرائم رایانه مشهد، ۱۳۹۸).[۱]

---

۱. آمارهای مذکور دربردارنده این نکته هستند که سیاست‌های کنترلی دولت از طریق ایجاد محدودیت برای دسترسی به اینترنت نه تنها در ساماندهی آسیب‌های فرهنگی و اجتماعی توفیقی نداشته‌اند، بلکه موجب هدایت کاربران به سمت استفاده از فیلترشکن برای رفع محدودیت شده است. بنابراین باید به دنبال روشی بود که آثار منفی کنترل به حداقل برسد و زمینه دسترسی آزاد به اینترنت فراهم شود و کاربر به‌گونه‌ای که امکان ردیابی IPهای اصلی و پنهان شده او فراهم است، به اینترنت متصل شود. بحث در خصوص علت آثار منفی کنترل و تدوین روش‌های جایگزین نیازمند پژوهشی خاص است.

۴. ارتباط مسئولیت کیفری با هویت سایبری

مسئولیت کیفری عبارت است از الزام شخص به پاسخ‌گویی در قبال نقض حقوقی که برای صیانت از آنها جرم‌انگاری انجام شده، تحمل آثار و عواقب ناشی از آن (مجازات) و در نهایت استحقاق و سزاواری تحمل این موارد (اردبیلی، ۱۳۹۳). مسئولیت کیفری در فضای سایبر مفهومی غیر از این ندارد و تحمل آثار فعل مجرمانه‌ای است که فرد در فضای مجازی مرتکب شده است (رضوی‌فرد و موسوی، ۱۳۹۵). مبانی مسئولیت کیفری نشان می‌دهد که اصل بر مسئولیت شخص حقیقی است و در واقع باید مرتکب رفتاری که عمل و واجد اثر کیفری است را شناسایی کرد؛ بنابراین تشخیص هویت واقعی متهم برای بررسی انتساب جرم و بررسی شرایط مسئولیت کیفری، اولین اقدامی است که مقام قضایی پس از بررسی صلاحیتش در پرونده کیفری دنبال می‌کند. برقراری ارتباط میان دنیای واقعی با فضای سایبر در یک پرونده کیفری امکان‌پذیر نیست، بلکه باید این ارتباط از قبل شکل گرفته باشد و مقام قضایی نسبت به کشف ارتباط اقدام کند. در مثالی ساده، زمانی که فرد با استفاده از شبکه اینترنت اقدام به نشر اکاذیب علیه فرد یا شخصیت حقوقی می‌کند، صرفاً اطلاعات مربوط به هویت ابرازی وی برای بزه‌دیده و مقام تحقیق معلوم است که این برای انتساب عمل مجرمانه و تحمیل مجازات کافی نیست و دستگاه عدالت کیفری جایگاهی در هویت‌بخشی سایبری به متهم ندارد تا بتواند رفتار مجرمانه را به شخص مشخص در فضای حقیقی منتسب کند. اینجاست که اهمیت مبادی هویت‌بخشی سایبری در نظام رسیدگی قضایی مشخص می‌شود.

دسترسی به فضای سایبر مستلزم تهیه هویت سایبری یا همان IP از شرکت‌های ارائه دهنده خدمات دسترسی است که این امر راه‌های متنوعی دارد. براساس مطالعات انجام شده دسترسی به اینترنت از طریق سیم‌کارت ارتباطی همراه و شبکه اینترنت خانگی بیشترین سهم در بازار فروش شرکت‌های ارائه‌دهنده خدمات دسترسی به اینترنت را دارد، به‌نحوی‌که شرکت بین‌المللی داده IDC[1] در سه‌ماهه اول سال ۲۰۱۷ تعداد ۳۴۴ میلیون

1. International Data Corporation (IDC)

تلفـن همـراه هوشـمند را در فضـای سـایبر شناسـایی کـرد (Wang, 2017). ایـن مـوارد در کنـار گسـترش سـریع و افزایش محبوبیت و اسـتفاده از شـبکه‌های اجتماعـی و نرم‌افزارهای پیام‌رسـان موبایلـی خبـر از تبدیـل شـدن موبایـل بـه عضـو لاینفـک جوامـع بشـری را می‌دهـد (Bennett, 2015). سـازمان تنظیـم مقـررات و ارتباطـات رادیویـی در زمـان انعقاد قـرارداد و اعطـای مجـوز فعالیـت و همچنیـن بـه موجـب مـاده (۵) آیین‌نامـه واحدهـای اطلاع‌رسـانی و خدمـات اینترنـت، شـرکت‌های توزیع‌کننـده اینترنـت را مکلـف می‌کنـد تـا در فرم‌هـای ثبت‌نـام مخصـوص، اطلاعات هویتی کاربـران را به صورت کامـل دریافت، تصویری از کارت ملی آنها را اخذ و ضمن احراز هویت، اطلاعات را به سازمان ارسال و نسخه‌ای از آن را بایگانـی کننـد. به این منظور قانونگـذار در ماده (۶۶۷) قانون آیین دادرسـی کیفری، این شرکت‌ها را مکلف به نگهداری و حفاظت اطلاعات کاربران برای مدت حداقل ۶ماهه پس از خاتمه اشتراک کاربران کرده است. این اطلاعات شامل قرارداد واگذاری خدمات دسترسی بـه اینترنت، IP و سـایر اطلاعات هویـت حقوقی کاربران می‌شـود، به‌نحوی‌که امکان ردیابی کاربران در فضای مجازی از مبدأ تا مقصد وجود داشـته باشـد. بنابراین کاربر مهمترین رکن زنجیره هویت سایبری است و زمانی که جرم سایبری اتفاق می‌افتد؛ شرکت‌های توزیع‌کننده اینترنـت بـا دنبال کـردن این زنجیـره و انطباق IP به‌جامانـده از متهـم در دیواره‌های آتش[1] سـایت‌ها و درگاه‌هـای اینترنتی که مجرم به آنها مراجعه کرده اسـت بـا بانک اطلاعاتی که در زمـان ثبت‌نـام و اعطای IP به کاربران داشـته‌اند، درمی‌یابند که هویت سـایبری مجرمانه در زمان وقوع جرم به چه شخصی منتسب است (Ji et al., 2007).

نکتـه‌ای کـه در برقراری ارتباط میان هویت سـایبری با هویت حقوقی فرد حائز اهمیت اسـت، بررسی قابلیت اسـتنادپذیری یا انکار هویت سایبری اسـت، به‌عبارت‌دیگر مهمترین قرینه‌ای که از مجرم در بررسـی صحنه ارتکاب جرائم سـایبری به دست می‌آید، IP وی است و بایـد دیـد که ایـن قرینه در نظر مراجـع قضایی و قوانیـن کیفری از چه جایگاهـی برخوردار اسـت؟ چـرا کـه انـکار متهـم در مـورد اسـتفاده از هویتـی کـه به او نسـبت داده شـده اسـت

1. Fire Wall

می‌تواند اصلی‌ترین وسیله احراز انتساب جرم و بررسی مسئولیت کیفری را کنار بزند. وزارت دادگستری ایالات متحده سوابق و دلایل الکترونیکی را به سه دسته تقسیم می‌کند:

الف) دلایل با منشأ رایانه،

ب) دلایلی که در رایانه نگهداری می‌شوند،

ج) دلایلی که از دو ماهیت قبلی تبعیت می‌کنند.

منشأ رایانه‌ای به آن دسته از داده‌های الکترونیکی اطلاق می‌شود که کاربر نقشی در ایجاد آنها ندارد، مانند اطلاعاتی که از سوابق موقعیت جغرافیایی بر روی تلفن همراه ذخیره می‌شود یا اطلاعاتی که شرکت‌های ارائه‌دهنده خدمات دسترسی از کاربران در اختیار دارند. اما دسته دوم دلایلی هستند که کاربر در ایجاد، تغییر، نگهداری یا حذف آنها نقش ایفا می‌کند، مانند پیام‌های پست‌های الکترونیکی یا واژگانی که در نرم‌افزار Word می‌نویسد. دسته سوم دربرگیرنده ویژگی‌های موارد قبلی است، مانند صفحات فیشینگی که کلاهبرداران رایانه‌ای برای صید اطلاعات کارت‌های بانکی کاربران طراحی می‌کنند، به عبارتی صفحات وب طراحی شده در دسته دوم دلایل و جزئیاتی از قبیل زمان طراحی، IP طراح و مشخصات سیستمی که با آن طراحی انجام شده است در زمره دلایل با منشأ رایانه قرار می‌گیرد (جلالی فراهانی، ۱۳۸۶؛ Marcella and Menendez, 2007). در قوانین داخلی نیز ماده (۲) قانون تجارت الکترونیک و تبصره ماده (۶۶۷) قانون آیین دادرسی کیفری به موارد فوق اشاره کرده است. داده پیام در دسته دوم دلایل الکترونیکی قرار می‌گیرد و ارزش اثباتی آن مطابق مواد (۱۳ و ۱۴) قانون تجارت الکترونیک بسته به طرق ایجاد مطمئن یا نامطمئن آن متفاوت است، به صورتی که مطابق ماده (۱۴) داده پیامی که به طرق مطمئن ایجاد و نگهداری شده باشد در حکم اسناد معتبر بوده و ادعای انکار و تردید در مورد آنها مسموع نیست و در غیر این صورت از ارزش اثباتی کمتری برخوردار خواهد بود. اما IP به‌عنوان موضوع اصلی هویت سایبری مطابق تبصره ماده (۶۶۷) قانون آیین دادرسی کیفری در زمره دلایلی قرار می‌گیرد که توسط رایانه و بدون دخالت کاربر ایجاد می‌شود. چنانچه این دلایل مطابق آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی وفق موازین علمی و پلیسی با رعایت زنجیره حفاظتی جمع‌آوری شوند، استنادپذیر و

غیرقابـل انـکار خواهند بود (زنـدی، ۱۳۹۴). مطالعه رویه قضایی در مواجهه با ادله با منشـأ رایانـه خالـی از لطـف نیسـت. سـوابق آمـاری پرونده‌هـای کیفـری نشـان می‌دهـد کـه مقام تحقیق، دلایلی که توسط رایانه ایجاد می‌شوند را به‌عنوان یکی از قرائن مفید علم قاضی در پرونده کیفری لحاظ می‌کند. آمار ۶ماهه نخسـت سـال ۱۳۹۸ پرونده‌های کیفری دادسرای ویژه فضای مجازی مشـهد نشـان می‌دهد که در بیش از ۹۰ درصد کیفرخواست‌های صادره بـا اتهـام رایانـه‌ای، به IP به‌عنوان یکی از قرائن مفید علم قاضی اشـاره شـده اسـت و ادعای انکار و تردید را در مورد آن مسـموع نمی‌دانند، بلکه صرفاً در مواردی قرینه رایانه‌ای را منشـأ علـم قلمـداد نمی‌کننـد که متهم دلیلی بر سوءاسـتفاده از هویت خود توسـط فـرد دیگری را ارائه دهد (سامانه مدیریت پرونده‌های قضایی، ۱۳۹۸).

در تابسـتان سـال ۱۳۹۷ نماینـده حقوقـی یکی از شـرکت‌های هواپیمایی در مشـهد با مراجعه به دادسـرای ویژه فضای مجازی و طرح شـکایت، اعلام داشـت که فردی ناشـناس با دسترسـی به پنل مدیریتی سـایت فروش بلیت‌های چارتری این شـرکت، اقدام به فروش بلیت‌هـای مسـیرهای پـروازی پرتـردد بـا مبالغـی بسـیار ناچیز کـرده و بـا صدور بلیـط برای خریداران موجب ورود خسـارت هنگفت به شـرکت شده است. شرکت زمانی متوجه موضوع می‌شود که تعداد زیادی از خریداران این بلیت‌ها، مسافرت خود را انجام دادند و خریداران حقیقی از پرواز جاماندند و موجب بروز اعتراضات مردمی در فرودگاه شد و علاوه‌بر خسارت مالـی، خدشـه جدی بـه اعتبار شـرکت وارد کرد. نتیجـه تحقیقات قضایی نشـان می‌داد که فردی با IP خاص ضمن نفوذ به سایت فروش شرکت هواپیمایی کنترل آن را به دست گرفته و مرتکـب افعال مجرمانه سـایبری، دسترسـی غیرمجاز به سـامانه‌های رایانـه‌ای و اخلال در عملکرد آن می‌شـود. با اسـتعلام از شـرکت ارتباطات زیرساخت، شـرکت ارتباطی ارائه‌دهنده IP بـه فرد مشـخص شـد. سـپس بـا مکاتبـه با این شـرکت معلوم شـد کـه ایـن IP مربوط به اینترنـت همـراه موبایـل بوده و در تاریخ و سـاعت نفوذ در اختیار شـماره سـیم‌کارت خاصی بوده اسـت. با احضار مالک سـیم‌کارت به دادسـرا و تحقیقات از او مشـخص می‌شود که وی صاحب کافی‌شـاپی در مشـهد اسـت که برای مشـتریانش امکان اسـتفاده از اینترنت رایگان را فراهـم کـرده و فردی با سوءاسـتفاده از این امکان مرتکب جرم شـده اسـت. هرچند قرائن

حکایت از انتساب اتهام به مالک IP بود اما دوربین‌های مداربسته محل کسب او نشان می‌داد که فرد دیگری در حال استفاده از IP برای ارتکاب جرم است. در نهایت با استفاده از اطلاعات پرداخت متهم در کافی‌شاپ هویت حقیقی وی شناسایی شد. اما اگر این فرد خارج از دید دوربین‌های مداربسته یا بیرون از کافی‌شاپ این جرائم را مرتکب می‌شد چه سرنوشتی در انتظار دارنده حقیقی IP بود؟ این مثال اهمیت بخش‌های مختلف برای تشخیص هویت سایبری به منظور انتساب مسئولیت کیفری نمایان و نقش دارنده هویت سایبری را برای محافظت از هویتش در فضای مجازی یادآوری می‌کند (سامانه مدیریت پرونده‌های قضایی، ۱۳۹۸). این پرونده نشان می‌دهد که IP به‌عنوان یک دلیل الکترونیکی غیرقابل انکار بزه را به مالک آن منتسب می‌کند، اما متهم در دفاعیاتش به فیلم دوربین‌های مداربسته استناد کرد که نشان می‌داد در زمان ارتکاب جرم سایبری فرد دیگری با سوءاستفاده از سهل‌انگاری مالک واقعی هویت سایبری و با تصرف هویت او، مرتکب جرم سایبری می‌شود.

۵. جمع‌بندی، نتیجه‌گیری و ارائه پیشنهادها

هویت در علوم اجتماعی مفهومی چندوجهی است و در رشته‌های علمی مختلف تعاریف متفاوتی را به خود می‌گیرد. به ویژگی‌های منحصربه‌فردی که حاکمیت برای تمایز میان اتباعش در اختیار دارد و از این طریق علم حقوق آنها را شناسایی می‌کند، هویت حقوقی گفته می‌شود. به تبع در حقوق کیفری به وسیله این هویت متهم تحت پیگرد قرار می‌گیرد و مسئولیت کیفری رفتار مجرمانه به وی تحمیل می‌شود. ارتکاب جرم در فضای سایبر از این جهت مهم است که در نگاه اول همه چیز در خصوص مرتکب مبهم به نظر می‌رسد. اینکه چه شخصی و با چه هویتی مرتکب جرم شده است و چگونگی ارتباط میان مسئولیت کیفری با فضای سایبر سؤالاتی است که پاسخ آن در شناسایی هویت سایبری کاربران مجازی نهفته شده است. منظور از این هویت اطلاعاتی نیست که کاربران در فضای مجازی با آن خود را معرفی می‌کنند و هر آن امکان تغییر یا حذفش متصور است؛ بلکه داده‌هایی است که مانند حلقه‌های به هم پیوسته در یک ارتباط زنجیره‌ای از یک‌سو به صحنه جرم

و هویت سایبری که از متهم به جا مانده است و سیستم آن را گواهی می‌کند، وصل است و از سوی دیگر به هویت واقعی مرتکب در فضای حقیقی متصل می‌شود و امکان تحمیل مجازات را به‌عنوان ثمره مسئولیت کیفری بر مجرم میسر می‌کند. پروتکل اینترنت یا همان IP ابزار دستیابی کاربران به فضای مجازی است و بدون آن ارتباط کاربر با محیط سایبر قطع می‌شود. این پروتکل براساس قواعد فنی و مهندسی یک شناسه خاص را به کاربر می‌دهد که او را از سایر کاربران در فضای مجازی متمایز می‌کند. کشف علمی این شناسه وابسته به شرکت‌های ارائه‌دهنده خدمات دسترسی به اینترنت است، جایی که اطلاعات مربوط به کاربران در فضای حقیقی با هویت سایبری آنها گره می‌خورد و بدون اینکه کاربر متوجه باشد در تمام فضای وب ردپای IP او برجای می‌ماند و در زمان وقوع جرم سایبری ضابطان قضایی مطابق دستورالعمل‌های فنی جمع‌آوری ادله دیجیتال در پرتو مقررات قانونی سبب می‌شوند تا قابلیت استنادپذیری این مدارک خدشه‌دار نشود و به موجب آن امر تعقیب و تحقیق ادامه یابد. انواع مختلف هویت سایبری محل چالش‌های فراوانی برای دستگاه عدالت کیفری است که قسمتی از آن در این پژوهش به تصویر کشده شد. این مورد در کنار سؤالات بی‌پاسخی که در خصوص آنها مطرح شد، ضرورت مطالعات آتی روی چالش‌های هویت سایبری را آشکار می‌کند تا در آن شیوه‌های مقابله با استتار هویت از منظر متخصصان علوم سایبر مورد بررسی قرار گیرد.

نتایج پژوهش حاضر نشان می‌دهد که راه‌های پنهان‌سازی و به عبارت عامیانه دور زدن هویت سایبری به‌عنوان چالش اساسی دستگاه عدالت کیفری در مواجهه با مجرمان سایبری برای انتساب مسئولیت کیفری است. در ایران اصلی‌ترین راه اتصال کاربران به اینترنت، سیم‌کارت‌های مخابراتی است و بر همین اساس موارد ذیل به‌عنوان پیشنهادهای عملیاتی این پژوهش احصا می‌شود. هرچند که تبیین نقش هر یک از عوامل و نحوه پیشگیری فنی نیازمند پژوهشی مجزا در آن حوزه است.

- ساماندهی نحوه واگذاری سیم‌کارت‌های تلفن همراه در حال حاضر بزرگترین هدف پیش روی متولیان رصد و پایش فضای سایبری قلمداد می‌شود، چراکه در حال حاضر و به گواهی آماری که بیان شد، اینترنت همراه بیشترین سهم را در اتصال کاربران به

فضای مجازی از آن خود کرده است، جایی که نبود نظارت کافی بر نحوه صدور و واگذاری سیم‌کارت‌ها موجب می‌شود تا اصلی‌ترین گلوگاه نظارتی حاکمیت در اعطای دسترسی اینترنت به کاربران حقیقی با چالش جدی مواجه شود.

- بازنگری در سیاست‌های فیلترینگ؛ چراکه ممانعت از دسترسی کاربر به سایت‌ها و برنامه‌های فیلتر شده از مهمترین دلیل گرایش کاربران به سمت استفاده از فیلترشکن محسوب می‌شود. در نهایت استفاده از این ابزار منجر به پنهان شدن هویت سایبری کاربر می‌شود و با توجه به نقابی که به او می‌دهد، می‌تواند زمینه‌ساز ارتکاب اعمال مجرمانه وی شود.

- عدم دستیابی به مقدار کافی IP سبب می‌شود تا شرکت‌های توزیع‌کننده اینترنت برای رفع این نقیصه و عرضه اینترنت به همه کاربران، اقدام به ایجاد IP وابسته یا NAT کنند. این امر در کنار عدم ساماندهی IPهای نت شده توسط شرکت‌های توزیع‌کننده اینترنت به مخفی شدن هویت سایبری کاربر منجر می‌شود. بنابراین لازم است میزان IP مورد نیاز کاربران ایرانی به صورت معتبر از آیکان تأمین شود. در صورت عدم تأمین، شرکت‌های توزیع‌کننده خدمات دسترسی باید به ساماندهی نرم‌افزارهای تقسیم IP و نگهداری اطلاعات آن برای مدت زمان مشخص الزام شوند تا در صورت نیاز بتوانند جوابگوی دستگاه عدالت کیفری برای تعقیب متهمان سایبری باشند.

منابع و مآخذ

۱. اردبیلی، محمدعلی (۱۳۹۳). *حقوق جزای عمومی*، جلد ۲، تهران، میزان.

۲. آمارنامه سایبری دادسرای ویژه جرائم رایانه مشهد (۱۳۹۸). «پرسش‌نامه آماری کاربران مشهدی شبکه‌های اجتماعی»، بازیابی شده ۱۷ اسفند، ۱۳۹۸.

۳. باقری دولت‌آبادی، علی و فرج‌الله زارعیان جهرمی (۱۳۹۲). «تأثیر فضای مجازی بر هویت و همبستگی ملی»، *فصلنامه مطالعات راهبردی بسیج*، ۱۶(۶۰).

۴. جاویدنیا، جواد و جعفر کوشا (۱۳۹۱). *جرائم تجارت الکترونیک*، تهران، انتشارات خرسندی.

۵. جلالی فراهانی، امیرحسین (۱۳۸۶). «استنادپذیری ادله الکترونیکی در امور کیفری»، *مجله فقه و حقوق*، ۴(۱۵).

۶. جوان‌جعفری بجنوردی، عبدالرضا (۱۳۸۹). «جرائم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرائم رایانه‌ای)»، *مجله دانش و توسعه*، ۱۷(۳۴).

۷. جوان‌جعفری بجنوردی، عبدالرضا و زهرا فرهادی آلاشتی (۱۳۹۵). «بررسی تعارض رهیافت‌های تدابیر موقعیت‌مدار نظارت سایبری با حریم خصوصی کاربران»، فصلنامه *مجلس و راهبرد*، ۲۳(۸۷).

۸. خالقی، ابوالفتح و زهرا صالح‌آبادی (۱۳۹۴). «مطالعه سرقت هویت در حقوق فدرال آمریکا با نگاهی اجمالی به حقوق ایران»، *حقوق تطبیقی*، ۲(۱۱).

۹. ذوالفقاری، ابوالفضل و سیدعلی پرهیز (۱۳۹۷). «بررسی مقایسه‌ای هویت واقعی و مجازی افراد (مورد مطالعه: جوانان شهر یاسوج)»، *مدیریت اطلاعات*، ۴(۲).

۱۰. رضوی‌فرد، بهزاد و سیدنعمت‌الله موسوی (۱۳۹۵). «مسئولیت کیفری در فضای سایبر در حقوق ایران»، *فصلنامه پژوهش‌های حقوق کیفری*، ۵(۱۶).

۱۱. ریتزر، جورج (۱۳۸۲). *نظریه‌های جامعه‌شناختی در دوران معاصر*، ترجمه محسن ثلاثی، تهران، انتشارات علمی.

۱۲. زندی، محمدرضا (۱۳۹۴). *تحقیقات مقدماتی در جرائم رایانه‌ای*، تهران، انتشارات جنگل.

۱۳. سازمان تنظیم مقررات و ارتباطات رادیویی (۱۳۸۵). «تصویب کلیات مقررات تأمین، توزیع و عرضه خدمات اینترنت»، بازیابی شده از https://asnad.cra.ir/fa/Public/Documents/Details/cdcab54b-f687-e511-973c-68b599781b58

۱۴. سامانه مدیریت پرونده‌های قضایی (۱۳۸۸). «پرونده‌های کیفری دادگستری کل استان خراسان رضوی با عنوان جرائم رایانه‌ای»، بازیابی شده ۱۷ اسفند، ۱۳۹۸.

۱۵. شهبازی، میثم، مسعود شفیعی و زینب ابوطالبی (۱۳۹۰). *رویکرد شبکه‌ای به زیرساخت‌های حیاتی*،

تهران، مرکز پژوهش‌های استراتژیک.

۱۶. طیبی، مرتضی و انیس خدادادی (۱۳۹۳). «سرقت هویت»، نشریه علمی-پژوهشی *فقه و حقوق اسلامی*، ۱۰(۵).

۱۷. عمید، حسن (۱۳۹۰). *فرهنگ فارسی عمید*، تهران، انتشارات امیرکبیر.

۱۸. فرهادی آلاشتی، زهرا و عبدالرضا جوان جعفری بجنوردی (۱۳۹۵). *پیشگیری وضعی از جرائم سایبری: راهکارها و چالش‌ها*، تهران، میزان.

۱۹. کوره‌پز، حسین محمد (۱۳۹۳). «نیمرخ جنایی بزهکاران سایبری»، پایان‌نامه کارشناسی ارشد، پردیس فارابی دانشگاه تهران، قم.

۲۰. کوهی، کمال و محمدرضا حسنی (۱۳۹۱). «رابطه استفاده از رسانه‌های نوین با ابعاد هویتی در نوجوانان وجوانان ۲۹-۱۴ساله شهر تبریز»، *فصلنامه پژوهش‌های ارتباطی*، ۴(۷۲).

۲۱. هیگنز، جرج و کترین دیویس مارکم (۱۳۹۷). *شبکه‌های اجتماعی به مثابه ابزار ارتکاب جرم*، ترجمه حمید دانش‌ناری و ابراهیم داوودی دهاقانی، تهران، میزان.

22. Ayaburi, E. W. and D. N. Treku (2020). "Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook", *International Journal of Information Management*, 50.

23. Bates, S., C. Bavitz and K. Hessekiel (2017). Zero Rating and Internet Adoption: The Role of Telcos, ISPs and Technology Companies in Expanding Global Internet Access: Workshop Paper and Research Agenda, *Berkman Klein Center Research Publication*.

24. Becker, M. (2019). "When Public Principals Give up Control Over Private Agents: The New Independence of ICANN in Internet Governance", *Regulation and Governance*, 13(4).

25. Bennett, S. (2015). 28% of Time Spent online is Social Networking, *Retrieved March*, 16, 2016.

26. Bernabe, J. B., M. David, R. T.Moreno, J. P. Cordero, S. Bahloul and A. Skarmeta

(2020). "Aries: Evaluation of a Reliable and Privacy-preserving European Identity Management Framework", *Future Generation Computer Systems*, 102.

27. Chidimma Blessing, N., P. C. Okoli, E. A Chukwunonye and C. P. Ofojebe (2020). "Identity Orientation Dimensions as Correlates of Cyber-Aggressive Behaviour among Undergraduates", *International Journal of Innovative Science and Research Technology.* 5(4).
28. Cusack, B. and E. Ghazizadeh (2019). *Defining Cloud Identity Security and Privacy Issues: A Delphi Method*, Twenty-fifth Americas Conference on Information Systems, Cancún, México.
29. Hadzhidimova, L. I., and B. K. Payne (2019). "The Profile of the International Cyber Offender in the US", *International Journal of Cybersecurity Intelligence and Cybercrime*, 2(1).
30. Ji, S., J., Wang, Q. Min and S. Smith-Chao (2007). Systems Plan for Combating Identity Theft-a Theoretical Framework. In *2007 International Conference on Wireless Communications, Networking and Mobile Computing*.
31. Manago, A. M., M. B. Graham, P. M. Greenfield and G. Salimkhan (2008). "Self-presentation and Gender on MySpace", *Journal of Applied Developmental Psychology*, 29(6).
32. Marcella Jr, A. and D. Menendez (2007). *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, Auerbach Publications.
33. Michel, M. C., M. Carvalho, H. Crawford and A. C. Esterline (2018). "Cyber Identity: Salient Trait Ontology and Computational Framework to Aid in Solving Cybercrime", In *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, IEEE.
34. Nagy, P. (2010). Second Life, Second Choice? The Effects of Virtual Identity on Consumer Behavior, A Conceptual Framework, In *Proceedings of FIKUSZ'10*

Symposium for Young Researchers.

35. National Research Council, Kent, S. T. and L. I. Millett (2003). *Who goes There?: Authentication Through the Lens of Privacy*, National Academies Press.
36. Ni, Q., E. Bertino, J. Lobo, C. Brodie, C. M. Karat, J. Karat and A. Trombeta (2010). "Privacy-aware role-based Access Control", *ACM Transactions on Information and System Security (TISSEC)*, 13(3).
37. Okoli, P. C. (2020). Identity Orientation Dimensions as Correlates of Cyber-Aggressive Behaviour among Undergraduates.
38. Perrin, S. E. (2018). *The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World's Data Protection Authorities* (Doctoral Dissertation).
39. Schafer, V. and A. Serres (2017). *Histories of the Internet and the Web*, Infoclio.
40. Sridhar, V. (2019). Who Governs the Internet? *Emerging ICT Policies and Regulations*, Springer, Singapore.
41. Sun, Y., S. Fang and Y. Hwang (2019). "Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce", *Sustainability*, 11(12).
42. Wang, T. (2017). "Social Identity Dimensions and Consumer Behavior in Social Media", *Asia Pacific Management Review*, 22(1).
43. Wang, W., Y. Yuan and N. Archer (2006). "A Contextual Framework for Combating Identity Theft", *IEEE Security and Privacy*, 4(2).
44. Yang, J., Y. Shi, and J. Yang (2011). "Personal Identification Based on Finger-vein Features", *Computers in Human Behavior*, 27(5).
45. Zalnieriute, M. (2019). "From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Example of Internet Governance and ICANN", *Forthcoming (2019) XXI Yale Journal of Law and Technology*.