

مجازی شدن بزهکاری یقه سفیدی در پرتو ارزشهای مجازی^۱

باقر شاملو*، عارف خلیلی پاجی**

چکیده

در جهان امروز فناوری با سرعت شگرفی در حال پیشرفت است. بزهکاران این موقعیت فرصت ساز را به خوبی شناخته‌اند و از پیشرفت‌های فناورانه برای پیشبرد اهداف خود بهره می‌برند. فناوری اطلاعات و ارتباطات، افزون بر ایجاد ابزارهای جدید ارتکاب جرم، بستر ساز ارتکاب جرایمی نو نیز شده که با گسترش محیط مجرمانه به فراتر از مرزهای جغرافیایی یک کشور، فرایند جهانی شدن بزهکاری را تسریع کرده است. ابداع ارزشهای مجازی به فرایند مزبور سرعت بخشیده است. ارزشهای مجازی با ادعای هم‌ردیف قرارگرفتن با ارزشهای متعارف (دولتی)، در تلاش‌اند تا تابوهای سنتی تولید و توزیع پول توسط دولت‌ها را بشکنند و ارزی غیررسمی با قابلیت تولید توسط کاربران فراهم آورند. این امر سبب تحول در برخی مفاهیم سنتی جرم‌شناختی شده است. بزهکاری یقه سفیدی یا بزهکاری یقه سفیدان یکی از این مفاهیم است که با گسترش فضای مجازی و ابزارهای خاص موجود در آن، متحول شده است؛ چندان که برخی اندیشمندان، از آن تحت عنوان «بزهکاری یقه مجازی‌ها» یاد می‌کنند. بدین سان، این پژوهش با روشی توصیفی و تحلیلی، پس از بررسی ابعاد بزهکاری یقه سفیدی مجازی یا بزهکاری یقه مجازی‌ها، به تحلیل چرایی تمایل بزهکاران مجازی به استفاده از ارزشهای مجازی در ارتکاب بزهکاری با توجه به برخی پرونده‌های کیفی خواهد پرداخت.

واژگان کلیدی: ارزشهای مجازی، بزهکاری، یقه سفیدها، یقه مجازی‌ها، جهانی شدن

۱. این مقاله برگرفته از رساله دوره دکتری تخصصی نویسنده مسئول تحت عنوان «تأثیر ارزشهای مجازی بر جهانی شدن بزهکاری» با راهنمایی آقایان دکتر باقر شاملو و دکتر علی حسین نجفی ابرندآبادی و مشاوره آقایان دکتر امیرحسین نیازپور و دکتر مهدی صبوری پور در دانشگاه شهید بهشتی است.

* دانشیار گروه حقوق جزا و جرم‌شناسی دانشکده حقوق دانشگاه شهید بهشتی baghershamloo@gmail.com

** دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشکده حقوق دانشگاه شهید بهشتی (نویسنده مسئول)

a_khalilipaji@sbu.ac.ir

مقدمه

آغاز هزاره سوم را می‌توان شروع تغییر رویکردهای جرم‌شناسی به فضای مجازی دانست. تغییرات ایجاد شده به واسطه توسعه و گسترش فضای مجازی، اینترنت و اشکال پیچیده ارتباطات با محصول جانبی آن، یعنی جرم، همراه شد. این امر از چند بُعد قابل توجه است.

فضای مجازی در فرایند جهانی شدن بزهکاری به شدت و گستره آن افزوده است. جهانی شدن یکی از فراگیرترین فرایندها و تحولات در جامعه معاصر است که به عنوان پدیده‌ای چندبُعدی، آستن مباحث گسترده در ارتباط با ماهیت، ریشه‌های تاریخی و تأثیر آن بر جوامع شده است. دامنه مطالعات و تحقیقات رشته‌های تخصصی علوم جنایی نیز از این تحولات مصون نمانده و با گسترش فرایند جهانی شدن در حوزه‌های مختلف، مانند اقتصاد، فرهنگ، حقوق بشر و سیاست، به حوزه بزهکاری نیز تسری پیدا کرده است؛ به عبارت دیگر، امروزه با جهانی شدن اقتصاد، فرهنگ، سیاست و حقوق بشر و به دنبال آن، کمرنگ شدن مرزهای سیاسی میان کشورها، شاهد جهانی شدن بعضی مظاهر بزهکاری مالی و اقتصادی هستیم که توسط مرتکبان چندملیتی به طور سازمان یافته یا در قالب گروه‌های جنایی ساختارمند ارتکاب می‌یابند (نک: نجفی ابرندآبادی، ۱۳۹۵: ۱۳-۵).

تحول مفهومی و موضوعی بزهکاری در پرتو فضای مجازی و آثار آن، اتفاق مهمی در جرم‌شناسی و حقوق کیفری است. بر این اساس، افزون بر اینکه فضای مجازی مفهوم برخی جرایم را تغییر داده، به مصادیق آن‌ها نیز افزوده است. نمونه بارز تأثیر فضای مجازی بر جهانی شدن و تغییر مفهومی و موضوعی جرم را می‌توان در گسترش جرایم یقه‌سفیدها مشاهده کرد. جرایم یقه‌سفیدی، به تعبیر ساترلند^۱ جرایم ارتکاب یافته به وسیله افراد محترم و متعلق به طبقه بالای جامعه، با گسترش جهانی شدن اقتصاد و شکل‌گیری شرکت‌ها و نهادهای چندملیتی، ابعاد تازه‌ای پیدا کرده است. یکی از دلایل ایجاد چنین امری، گسترش فضای مجازی است. فضا یا محیط مجازی، در کنار فراهم ساختن زمینه و فرصت پیدایش جرایمی نوین و وسایل جدید ارتکاب جرایم متعارف، فرایند جهانی شدن بزهکاری تزویرآمیز را نیز تسریع کرده و به آن شدت بخشیده است؛^۲ به طوری که برخی سخن از مجرمان «یقه‌مجازی»،^۳ به عنوان گونه‌ای از جرایم یقه‌سفیدی به میان می‌آورند (Reid,

۱. اصطلاح بزهکاری یقه‌سفیدها، برای اولین بار در سال ۱۹۳۹ میلادی توسط ساترلند Edwin H, Sutherland (۱۸۸۳-۱۹۵۰) جامعه‌شناس آمریکایی طی مقاله‌ای در مجله آمریکایی «جامعه‌شناسی» به کار برده شد. وی در سال ۱۹۴۹ کتاب مستقلی را به همین عنوان اختصاص داد (نجفی ابرندآبادی، ۱۳۸۵: ۲۸).

۲. جهت مطالعه فضای سایبر به عنوان محیطی اجتماعی؛ (نک: نجفی ابرندآبادی، ۱۳۸۸: ۵۲-۵۰).

(2018).^۱ از جمله زمینه‌های گسترش این امر، ابداع و به‌کارگیری ارزهای مجازی^۲ است که امروزه نیز با سرعت زیادی در حال افزایش است.

زمانی که ارزهای مجازی غیرمتمرکز، به‌ویژه بیت‌کوین^۳، به وجود آمدند، توجه فراوانی را به سمت خود جلب کردند. به‌طور کلی، دو دیدگاه در خصوص کارکرد این‌گونه از ارزها وجود دارد: دیدگاه نخست که نگاهی مثبت به این موضوع دارد، ارزهای مجازی را یک روش نوین برای پرداخت می‌داند که در آینده، به دلیل ویژگی‌هایی منحصر به فرد، بسیار فراگیر خواهند شد؛ دیدگاه دوم اما، با نگاهی بدبینانه به ارزهای مجازی به‌عنوان یک ابزار قدرتمند نوین در اختیار بزهکاران، تأمین‌کنندگان مالی تروریسم و اشخاص یا کشورهای تحت تحریم، برای دورزدن تحریم‌ها، جابه‌جایی، ذخیره منابع مالی و فرار مالیاتی توجه کرده است (FATF, 2015: 27). دیدگاه اخیر بر این نظر است که دسترسی جهانی به ارزهای مجازی، زمینه‌افزایش جرایم یقه‌سفیدی، به‌خصوص پول‌شویی^۴، را فراهم می‌کند؛ زیرا سامانه ارز مجازی می‌تواند از طریق اینترنت و با ابزارهایی، از جمله تلفن‌های همراه، حتی در پرداخت‌های برون‌مرزی در دسترس باشند. افزون بر این، ارزهای مجازی معمولاً به زیرساخت‌های پیچیده‌ای متکی هستند که شامل چندین نهاد در کشورهای مختلف می‌شوند و برای انتقال وجوه یا عملیات پرداخت مورد استفاده قرار می‌گیرند. این‌گونه از ارائه خدمات و درگیر بودن چندین کشور، به‌عنوان حوزه‌های قضایی مختلف، مشکلاتی را در تعیین مسئول مبارزه با پول‌شویی و تأمین مالی تروریسم، ناظر و مجری این مقررات ایجاد خواهد کرد (نک: خلیلی پاجی، ۱۳۹۸: ۱۳۴-۱۱۳). وجود سوابق مشتری و معاملات او در کشورهای مختلف، دسترسی به این اطلاعات را توسط کنشگران نظام عدالت کیفری مشکل‌تر می‌سازد. این مشکل به دلیل ماهیت به‌سرعت در حال تحول فناوری ارز مجازی غیرمتمرکز و مدل‌های کسب‌وکار، از جمله تغییر تعداد و نوع یا نقش مشارکت‌کنندگان در ارائه خدمات در سامانه‌های پرداخت ارز مجازی، تشدید می‌شود. مشکل مهم‌تر اینکه، ممکن است اجزای سامانه یا اشخاص استفاده‌کننده از ارز مجازی در کشورهای قرار گیرند که وضعیت مبارزه با پول‌شویی در آن‌ها نامناسب است. بدین ترتیب، کشف جرایم یقه‌سفیدها

۱. جرایم یقه‌مجازی‌ها اشاره به ارتکاب جرایم یقه‌سفیدی، یعنی جرایم با انگیزه‌های مالی و اقتصادی و تزویرآمیز، در فضای مجازی یا با استفاده از امکانات این فضا دارد. این امر، معیار تفکیک این دسته جرایم با سایر جرایم فضای مجازی یا سایبر است.

2. Virtual Currencies

3. Bitcoin

4. Money Laundering

دشوار خواهد بود. موضع اخیر از یک سو، با توجه به تلاش‌های بین‌المللی در حوزه مبارزه با پول‌شویی و از سوی دیگر، وجود خطر احتمالی در سامانه پرداخت اینترنتی با ابزار ارزش‌های مجازی و افزایش ریسک جرایم مزبور، از اهمیت بسیاری برخوردار شده است. امری که ضرورت انجام پژوهش‌های دقیق از مخاطرات ارزش‌های مجازی را اجتناب‌ناپذیر کرده است.

بر این اساس، در بررسی حقوقی و جرم‌شناختی ارزش‌های مجازی، تحولات آن بر بزهکاری به‌عنوان پرسشی مهم باید مورد بررسی قرار گیرد. در این راستا، می‌توان قائل به این بود که جرایم یقه‌سفیدی با وجود فضای مجازی به‌طور کلی و با به‌کارگیری ارزش‌های مجازی به‌طور خاص، از حیث مفهومی متحول شده است و این دسته از بزهکاران با توجه به ویژگی‌های ارزش‌های مجازی بیش‌ازپیش تمایل به تمرکز رفتارهای بزهکارانه خود در فضایی مجازی دارند که این مسئله، ترسیم چارچوب نظری خاص جرایم یقه‌سفیدی‌ها را به‌عنوان گونه‌ای از جرایم یقه‌سفیدی ضروری کرده است.

بدین ترتیب در پژوهش پیش‌رو، با روش توصیفی و تحلیلی و استفاده از منابع موجود، آنچه مدنظر قرار دارد، ابتدا تحلیل نظری تحولات جرایم یقه‌سفیدی به‌سوی جرایم یقه‌سفیدی‌ها است. این تحولات از یک سو، مربوط به رویکرد جرم‌مدار به جرایم یقه‌سفیدی است و از سوی دیگر، به نقش فضای مجازی اشاره دارد. مورد اخیر، از منظر جهانی شدن جرم و ایجاد تعادل بین بزهکار و بزه‌دیده، زمینه‌ساز گسترش جرایم یقه‌سفیدی‌ها شده است. سپس آنچه تحلیل و بررسی می‌شود، نقش ارزش‌های مجازی در تحول جرایم یقه‌سفیدی و ظهور مجرمان یقه‌سفیدی است. از این رو، با بررسی برخی پرونده‌های کیفری مطرح‌شده، چهار ویژگی انعطاف‌پذیری هویت، ناشناختگی، سهولت شرکت در عملیات مجرمانه و فقدان بازدارندگی، به‌عنوان ویژگی‌های جذاب ارزش‌های مجازی برای مجرمان یقه‌سفیدی مورد تحلیل و بررسی قرار خواهد گرفت.

۱. از جرایم یقه‌سفیدها تا جرایم یقه‌سفیدی‌ها

در قرن بیست‌ویکم، افراد، شرکت‌ها و دولت‌ها به‌طور فزاینده‌ای در معرض بزه‌دیدگی جرایم مالی قرار دارند. افزایش جرایم یقه‌سفیدها، به‌طور گسترده‌ای، زمینه‌ی وابستگی جوامع مدرن به سامانه‌های ارتباطی برخط جهت کنترل، نظارت و ارائه خدمات در سطوح گوناگون را اجتناب‌ناپذیر کرده است. تغییر سبک زندگی و عادت شهروندان به استفاده از فضای سایبر جهت کار، تفریح، مطالعه و...، آن‌ها را به‌طور مداوم در معرض بزه‌دیدگی سایبری قرار داده است. گسترش این قضیه در آینده، منجر به ایجاد فرصت‌های بیشتر بزهکاری خواهد شد و بزه‌دیدگی اشخاص را در این حوزه افزایش خواهد داد.

اگرچه پدیده بزهکاری فضای مجازی، در سال‌های اخیر گسترش یافته، این پدیده همچنان در حال تغییر، تحول و افزایش است تا موجب شکل‌گیری فزاینده‌ای از «بزهکاری مجازی» باشد. چنین عملیات مجازی مجرمانه‌ای اغلب به صورت ناشناس یا حداقل نیمه‌ناشناس، انجام می‌شود. بدین ترتیب، عوامل این جرایم یقه سفیدی می‌توانند در بستر این فضا مخفی بمانند و به ارتکاب جرایم غافل‌گیرانه بپردازند. بنابراین، فضای مجازی منجر به ایجاد یک پدیده نوین شده است که می‌توان آن را «جرایم یقه مجازی‌ها» نامید.

بر این اساس جهت بررسی تأثیر ارزش‌های مجازی بر جرایم یقه مجازی‌ها، ابتدا شناخت مفهوم جرایم یقه مجازی‌ها ضرورت دارد؛ زیرا ماهیت مجازی این ارزش‌ها، آن‌ها را به ابزاری منحصر به فرد در این فضا و در خدمت بزهکاران مجازی تبدیل کرده است.

به لحاظ نظری، جرایم یقه مجازی‌ها مبتنی بر دو تحول است: نخست، تحول در مفهوم جرم یقه سفیدها، از رویکرد مجرم‌مدار به رویکرد جرم‌مدار؛ دوم، تحول ایجاد شده توسط فضای مجازی در مورد این جرم. مورد اخیر افزون بر گسترش دامنه ارتکاب به واسطه جهانی شدن، در تغییر مفهومی جرم یقه سفیدی و ایجاد تعادل بین بزهکار و بزه‌دیده نیز مؤثر بوده است.

۱-۱. رویکرد جرم‌مدار به جرایم یقه سفیدی

تعریف ساترلند از جرم یقه سفیدی، به عنوان مبدع مفهوم جرایم یقه سفیدها، نمونه بارزی از تعریف مجرم‌مدار^۱ در خصوص این جرایم است. تعریف‌های مجرم‌مدار با تمرکز بر روی مجرم، موقعیت عالی اجتماعی و محترم بودن شخص مرتکب را ویژگی‌های اساسی جرم یقه سفیدی بیان می‌کنند. برخی اندیشمندان هم‌سو با تعریف ساترلند، جرم یقه سفیدی را بازتعریف کردند که در عمل موجب شفاف شدن تعریف ساترلند شده است. این دسته معتقدند که «جرایم یقه سفیدی به آن نوع اعمال خلاف قانون دارای ضمانت اجرای کیفری گفته می‌شود که متضمن سوءاستفاده مرتکب آن‌ها از موقعیت مهم قدرت، نفوذ یا اعتماد در یک نظام سازمانی یا اقتصادی مشروع، به منظور کسب درآمدهای نامشروع برای خود یا سازمانی است (Reiss & Biderman, 1981: 15)». این تعریف نیز مانند تعریف ساترلند، بر خصوصیات اجتماعی مرتکب جرم یقه سفیدی تأکید دارد و جرایمی را شامل می‌شود که با حرفه شغلی مرتکب مرتبط باشند.

1. Offender-Based Approach

در مقابل، برخی با اتخاذ رویکرد جرم‌مدار^۱، بزهکاری یقه‌سفیدی را مطالعه کردند. براساس این رویکرد، تعریف جرم بر ماهیت رفتار غیرقانونی، نه ویژگی‌های مرتکب آن، شکل می‌گیرد: «رفتار یا مجموعه‌ای از رفتارهای خلاف قانون که با استفاده از وسایل غیرفیزیکی و از طریق کتمان یا حيله و تزویر، با هدف تحصیل پول یا مال یا عدم پرداخت وجه یا خسارت یا تحصیل امتیاز شغلی یا شخصی ارتکاب می‌یابد» (Edelhertz, 1970: 18). این رویکرد، بزهکاری یقه‌سفیدی را بر اساس ابزار ارتکاب جرم، به خصوص ابزار غیرفیزیکی که شامل اختفا، کتمان، حيله و تزویر می‌شود، تعریف می‌کند.

بدین‌سان و در انتقاد به رویکرد مجرم‌مدار گفته شده است که «تعاریف مجرم‌مدار از جرم یقه‌سفیدی، با پدیدآوردن چارچوبی بسته، منجر به فهم نادرست از منابع ساختاری جرایم یقه‌سفیدی و ایجاد مشکل برای نهادهای کنترل اجتماعی می‌شود» (Shapiro, 1990: 35). تعریف جرم‌مدار، بدون اشاره به موقعیت یا قابلیت احترام مرتکب، گستره جرم یقه‌سفیدی را توسعه می‌دهد. در این تعریف جرم یقه‌سفیدی شامل فعالیت‌های غیرشغلی اما مالی به‌ظاهر مشروع می‌شود. بر این اساس، جرم یقه‌سفیدی، طیف گسترده‌ای از جرایم تزویرآمیز را شامل می‌شود؛ حتی اگر مرتکب دارای موقعیت اجتماعی رسمی بالایی نباشد.^۲

برای‌تمن هم‌سو با رویکرد جرم‌مدار در تعریف جرایم یقه‌سفیدی با اعتقاد به اینکه عبارت جرم یقه‌سفیدها باید قلمرو گسترده‌تری را دربرگیرد، هر اقدام غیرخسونت‌آمیز با انگیزه مالی، چه در فضای واقعی و چه در فضای مجازی را، صرف‌نظر از موقعیت اجتماعی مرتکب، جرم یقه‌سفیدی معرفی می‌کند (Brightman, 2009: 336). این تعریف نشان از تحول مفهوم جرم یقه‌سفیدی بر مبنای زیست دوگانه و گسترش سهم فضای مجازی در زندگی بشر دارد. برای نمونه، می‌توان به دسترسی تمام طبقات جامعه به بازار بورس و خرید و فروش اوراق سهام اشاره کرد که اگرچه در ابتدا در انحصار طبقه بالای جامعه بود، دسترسی به فناوری‌های رایانه‌ای، امروزه اجازه فعالیت به تمامی افراد در این زمینه را می‌دهد (ابوذری، ۱۳۹۵: ۳۷). سالیفو ضمن تأیید اندیشه برای‌تمن تأکید می‌کند که دلیل یا انگیزه اقتصادی و مالی در ذات جرایم سایبری وجود دارد. اگرچه برخی مجرمان فضای مجازی انگیزه‌های دیگری، مانند شهوت، انتقام، ماجراجویی و میل به درنوردیدن مرزهای غیرقانونی را

1. Offence-Based Approach

۲. تعاریف جرم‌مدار بنا به دلایل مختلفی از محبوبیت زیادی بین پژوهشگران برخوردار شده است؛ زیرا در این تعاریف، ذکری از وضعیت اجتماعی مرتکب یا موقعیت اجتماعی رفتار نمی‌شود؛ هم وضعیت اجتماعی مرتکب جرم و هم موقعیت اجتماعی رفتار، به‌طور مستقل از تعریف جرم، آزادند که تغییر کنند و می‌توانند به‌عنوان متغیرهای توضیحی استفاده شوند (ال. بنسون و اس. سیمپسون، ۱۳۹۱: ۲۸۰).

دارند، برجسته‌ترین انگیزه در این جرایم، منفعت‌طلبی است (Salifu, 2008: 435). بر این اساس، جرایم یقه‌سفیدان و جرایم سایبری، ویژگی‌های مشترکی با یکدیگر دارند؛ از این جهت که هر دو دسته این جرایم، از طرق غیرخشونت‌آمیز و توسط افراد محترم جامعه که سابقه کیفی ندارند، ارتکاب می‌یابند و دیدگاه جامعه بدین‌گونه است که به آن‌ها اهمیت کمتری نسبت به جرایم خشونت‌آمیز می‌دهد (Nycum, Parker, 1989: 78). بدین ترتیب، توسعه رویکرد جرم‌مدار و گسترش دامنه آن به فضای مجازی، موجب تحول مفهومی جرایم یقه‌سفیدها شده است.

۱-۲. تحول جرایم یقه‌سفیدی در پرتو فضای مجازی

از منظر ساترلند، ویژگی‌های جرایم یقه‌سفیدها، از ماهیت مرتکبان این‌گونه جرایم نشأت می‌گرفت (Reid, 2018: 232). همان‌طور که پیش‌تر بیان شد، تعریف ساترلند تحت تأثیر افزایش جرایم یقه‌سفیدها، بسیار ساده، گسترده و مبهم است. بر این اساس، به نظر می‌رسد جرایم یقه‌سفیدی، اصطلاحی بسیار فراگیر، کلی و شامل گستره‌ای وسیع از جرایم، با شیوه‌های ارتکاب، مرتکبان، آثار و بزه‌دیدگان متفاوت است که شامل جرایم مختلفی می‌شود؛ به همین دلیل برخی از اندیشمندان، انتخاب عنوان «یقه‌سفیدی» را در این خصوص صحیح نمی‌دانند.^۱ با این وجود، پدیده اینترنت و استفاده از آن در سطح جهانی، حیات جدیدی را به جسم جرایم یقه‌سفیدها دمید که بیش‌ازپیش علاقه‌مندی به رویکرد جرم‌مدار را در تعریف آن ایجاد کرده است.^۲ در واقع، واقعیت موجود حاکی از تأثیر فضای مجازی و امکانات موجود در این فضا بر جرایم یقه‌سفیدی است که افزون بر گسترش دایره ارتکاب این جرایم و تسریع پدیده «جهانی‌شدن جرایم یقه‌سفیدی»، هم‌سو با رویکرد جرم‌مدار، موجب تسریع در ایجاد «تعادل در قدرت و تغییر در مفهوم جرایم یقه‌سفیدی» شده است.

۱. البته در نحوه تعریف این گروه از جرایم، همواره اختلاف نظر وجود داشته و مجموعه واژگان تخصصی و اصطلاح‌شناسی آن از طیف وسیعی برخوردار است (نک: محسنی، ۱۳۹۱: ۱۳۴).
۲. در کنار شباهت‌های موجود بین جرایم یقه‌سفیدها و جرایم سایبری و پذیرش توسعه مفهوم این جرایم به سوی فضای مجازی، همان‌طور که پیش‌تر آمد، نکته بسیار مهمی که در بیشتر تحقیقات صورت گرفته در این حوزه مغفول مانده، تحولاتی است که فضای مجازی در جرایم یقه‌سفیدی ایجاد کرده است.

۱-۲-۱. جهانی شدن جرایم یقه سفیدها

جهانی شدن^۱ موجبات تغییر ماهیت جرایم، به خصوص جرایم اقتصادی و مالی را ایجاد کرده است. به گونه ای که «سازمان یافتگی»، «فرامرزی بودن» و «اتخاذ سازوکارهای پیچیده جهت ارتکاب» از جمله ویژگی های مهم این دسته از جرایم است. از نظر ویژگی های ساختاری، بزوه جهانی بیشتر اوقات با مشخصاتی همچون عدم تمرکز، انعطاف پذیری، قابلیت انطباق، به کارگیری فناوری های نوین و گستردگی شبکه توصیف می شوند (Rotman, 2001: 5). این امر یکی از نگرانی های فزاینده دنیای معاصر است که جریان های جهانی پولی و اطلاعات و افراد، شرایط و فرصت های مناسبی را برای گسترش اشکال جدیدی از بزهکاری جهانی شده رقم بزنند.

نیل شاور از دریچه جهانی شدن، بحثی کوتاه اما جالب در خصوص جرایم یقه سفیدی ارائه کرده است. وی معتقد است از یک سو، رشد نظام اقتصادی در جهان، فرصت های بی نظیری را برای جرایم یقه سفیدی ایجاد کرده است و از سوی دیگر، مقامات کشورهای فقیر، فاقد منابع و توان کافی جهت مقابله با این جرایم هستند (اس.سیمپسون و ویزبرد، ۱۳۹۲: ۱۹۸). پویایی منحصربه فرد سرمایه، دست بزهکاران را در جست و جوی نظام های قضایی که در خصوص فعالیت های اقتصادی نامشروع حساس نیستند، باز می گذارد. در چنین شرایطی، شرکت های چندملیتی که از نظر امکانات و تجهیزات انسانی، مادی، فنی، فناورانه و نیروی انسانی ماهر و تعداد کارمندان با دولت های میزبان رقابت می کنند، در معرض ارتکاب برخی جرایم قرار می گیرند (نجفی ابرندآبادی، ۱۳۹۶: ۱۷). افزون بر این، جهانی شدن مبادلات مالی به واسطه ابزارهای خاص موجود در این حوزه نیز گسترش جرایم یقه سفیدی را در پی داشته است. برخی ارزها، مانند دلار و یورو به عنوان ارزهای جهانی، ابزار تبادل سرمایه جهت گسترش مراودات مالی بین کشورها به صورت وسیله واحد جهانی درآمده اند و به بسیاری از محدودیت های موجود در مبادلات بین المللی پایان داده اند و موجب شده اند که این گونه از جرایم نیز با گسترش پدیده جهانی شدن، ابعاد فرامرزی یافته و از مرزهای داخلی کشورها

۱. جهانی شدن، اصطلاحی است چندبعدی که به همگونی فزاینده نظام های ملی از جنبه های اقتصادی، فرهنگی و سیاسی اشاره دارد. افزایش تعاملات منطقه ای و جهانی میان دولت های مختلف، شرکت ها، سازمان ها و مؤسسات گوناگون، موجب شده است که آثار یک جرم ارتكابی محدود به مرزهای کشور محل وقوع نباشد (نک: دولاکواستا، ۱۳۹۶: ۶۷۴ به بعد). از این رو، برخی جرایم ملی، جنبه جهانی به خود گرفته اند یا جرایمی در شکل های نوین ظهور پیدا کرده اند که از آن ها تحت عنوان جرایم جهانی یاد می شود که به دو دسته عمده جرایم با انگیزه سودجویانه (اقتصادی) و جرایم خشونت آمیز (تروریستی)، تقسیم می شوند (نک: نجفی ابرندآبادی، ۱۳۹۱: ۳۹-۴۷ و برناردی، ۱۳۹۲: ۱۸۳-۱۶۵).

فراتر رود. بی تردید در این زمینه نقش فضای مجازی و استفاده از بستر شبکه اینترنت در گسترش جهانی شدن بزهکاری، به ویژه جرایم یقه سفیدها، انکارناپذیر است. جهانی شدن اقتصاد، تحت تأثیر فناوری های جدید اطلاعات و ارتباطات و عوامل سیاسی، سبب شده است که فرایند و سرنوشت تولید، توزیع، حمل و نقل و مصرف کالا و خدمات در نظام اقتصادی کشورها تا اندازه زیادی در تعامل و مرتبط با یکدیگر متحول شوند (نجفی ابرندآبادی، ۱۳۹۴: ۱۳۹). این امر پدیدآورنده فرصت های جرمزای نوینی شده است. جرایم، تابع فرصت ها هستند و جهانی شدن که به واسطه توسعه فناوری، شتاب بیشتری به خود گرفته، فرصت های فراوانی را برای انواع فعالیت های مجرمانه به وجود آورده است (اس.سیمپسون و ویزیرد، ۱۳۹۲: ۲۰۱).

گسترش فضای مجازی و ایجاد امکان انجام مبادلات مالی اقتصادی در بستر این فضا و زیست مالی اقتصادی مجازی، به جهانی شدن بزهکاری یقه سفیدی سرعت بخشیده است. استفاده از فناوری موجود در فضای مجازی موجب می شود که بزهکار در پوشش فعالیتی مشروع، ظاهر شده و به طور ناشناس با هزینه اندک و در سطح جهانی به فعالیت مجرمانه اقدام کرده یا از فناوری شبکه اینترنت برای ایجاد شکل منسجمی از بزهکاری، در قالب سازمان های جنایی مجازی، اقدام کند. بدین ترتیب، فضای مجازی در افزایش دامنه ارتکاب جرایم یقه سفیدی نیز تأثیر شگرفی داشته است. افزون بر این، فضای مجازی بر برتری بزهکاران یقه سفیدی بر بزه دیدگان آن نیز تأثیرگذار بوده و آن را به سوی تعادل نسبی سوق داده است.

۲-۱. تعادل قدرت و تغییر مفهوم جرایم یقه سفیدها

به طور سنتی، مفهوم جرم یقه سفیدها بر عدم توازن قدرت بین مجرم و قربانی استوار است. در این نگاه، جایگاه اعتماد قربانی به بزهکار، وابستگی به سطح خاصی از جهل یا وابستگی قربانی یا مهارت خاص یا شهرت بزهکار دارد. تاریخچه جرایم سایبری به طور دقیق با این موضوع هم خوانی دارد؛ بزه دیدگان مجازی غالباً کم سن و سال یا مسن هستند و در زمینه فناوری اطلاعات تازه کار محسوب می شوند و در نتیجه از مهارت کافی برای دفاع از خود در برابر تهدیدات برخط برخوردار نیستند یا کاربر فناوری های نوینی هستند که مهارت لازم برای استفاده از آن را ندارند و بزهکاران مجازی با استفاده از برخی برنامه های مخرب، مانند ویروس ها یا بد افزارهای رایانه ای، آن ها را قربانی قرار می دهند. این پارادایم در دهه دوم قرن بیست و یکم، دیگر صحیح نیست. قربانیان جرایم برخط جوان تر و بالغ تر شده اند؛ زیرا فناوری تبدیل به یک واقعیت فراگیر در زندگی شده است؛ قربانیان به دلیل گستره فعالیت هایی که در فضای سایبر دارند، بومیان دیجیتال تلقی می شوند که با وجود

برخورداری از هوش غالباً سرشار، از آمادگی و مهارت کافی برای زیست در محیط دیجیتال برخوردار نیستند. نرم افزارهای مخرب و ویروس های رایانه ای، دیگر صرفاً به صورت برخط نیستند و کدهای نرم افزارها به حدی پیچیده شده اند که از دایره اشرف متخصصان رایانه ای نیز خارج اند؛ امکان تهیه انواع برنامه های کاربردی، از جمله برنامه هایی که جهت اهداف مجرمانه تولید شده و مورد استفاده قرار می گیرند، از طریق فروشگاه های برخط وجود دارد (Reid, 2018: 236). بدین ترتیب، بزهکاران نیازی به تحصیل در رشته علوم رایانه ای ندارند تا بتوانند نرم افزارهای کاربردی خود برای ارتکاب جرم را ایجاد و اجرا کنند. به طور خلاصه، عدم تعادل قدرت بین بزه دیدگان و بزه کاران، به میزان درخور توجهی کاهش یافته است. این پدیده به عنوان «جرم، همچون یک خدمت»^۱ شناخته شده است.

بنابراین، در حال حاضر، طبیعی است که مهارت های ویژه لازم برای ارتکاب جرم در فضای مجازی توسط بزهکاران سطوح پایین تر کسب شود؛ یعنی کسانی که به طور سنتی به عنوان بزهکاران یقه آبی معرفی می شوند. جرایم یقه آبی ها به عنوان جرایم خیابانی شناخته شده است که اغلب توسط اشخاص کم مهارت به وقوع می پیوندد و شامل تعرض ها و تهدیدهای فیزیکی می شود که کاملاً محسوس و تأثیرگذار است. این گونه بزهکاری، به دلیل ویژگی جسمانی آن، به طور مستقیم بر کیفیت زندگی اشخاص تأثیر می گذارد؛ از این رو، جامعه تمایل بیشتری دارد جهت مقابله با این جرایم با صرف منابع موجود اقدام کند. در مقابل، جرم یقه سفیدها، از لحاظ قربانی، آسیب و تأثیر اجتماعی آن، نسبتاً پنهان بوده و به همین دلیل کنش یا واکنش به آن توسط نظام عدالت کیفری و نهادهای اجرای قانون اولویت کمتری دارد.

افزایش دامنه ارتکاب و تعداد مرتکبین جرایم یقه سفیدها، معضل پیش روی جوامع است؛ به طوری که طیف وسیعی از افراد کم مهارت یا بی مهارت و گروه های سازمان یافته مجرمانه می توانند این جرایم را مرتکب شوند (Reid, 2018: 237). این امر، هم سو با رویکرد جرم مدار جرایم یقه سفیدی، گذار از تمرکز بر مجرم (به عنوان فردی از طبقه بالا یا پایین جامعه) به سوی درک عمل مجرمانه، نقش فرایندها و ویژگی های عمل ارتكابی است که باید در راستای توسعه مفهومی جرایم یقه سفیدی بررسی شود. بر این اساس، به واسطه فضای مجازی و شکل گیری مرادفات اقتصادی در این بستر، از سویی، بزهکاران یقه سفید، برخلاف تعابیر سنتی از این گونه جرایم، در عمل و به طور غالب، بزهکارانی با هوش فراوان تلقی نخواهند شد و از سوی دیگر، بزه دیدگان جرایم یقه سفیدی نیز نسبت به سایر بزهکاران کم هوش تر نیستند. در واقع فضای مجازی با ارائه امکانات منحصر به فرد

خود، میان بزهکار و بزه‌دیده، توازن و تعادل ایجاد می‌کند که این نیز یکی از شاخصه‌های مهم جرایم یقه‌مجازی‌هاست.

۲. ابداع ارز مجازی؛ تحولی در تمایل به ارتکاب جرم یقه‌سفیدی مجازی

امروزه در کنار ارزهای قانونی دارای پشتوانه دولتی، گونه‌ای جدید از ارزها با ویژگی‌های منحصر به فرد تولید شده‌اند و به واسطه فرایند جهانی شدن با سرعتی شگفت‌انگیز در حال توسعه هستند و سازوکارهای پیچیده‌ای را برای ارتکاب جرایم یقه‌سفیدی فراهم ساخته‌اند. ارزهای مجازی با ادعای جایگزینی برای پول رایج قانونی، ابتدا جهت استفاده در محیط‌های مجازی به‌ویژه برای کاربران سایت‌های برخط بازی طراحی شدند. تعداد چنین ارزهایی با گسترش کاربرد آن‌ها رشد کرد و دنیای واقعی را نیز شامل شد. اکنون، مقدار زیادی ارز مجازی در گردش است. آن‌ها را هم می‌توان به‌طور مستقیم (از طریق استخراج، معاملات دوجانبه با سرمایه‌گذاران دیگر و از صرافی‌هایی که ارز مجازی می‌فروشند) و هم به‌طور غیرمستقیم از طریق یک مبادله مجازی با ارز مجازی به‌عنوان وسیله پرداخت به دست آورد. ایجاد، عرضه و گسترش این گونه ارزها، با تمام مزایای منحصر به فردی که دارد، می‌تواند زمینه‌ساز یا تسهیل‌کننده ارتکاب جرایم یقه‌سفیدی در بعد جهانی باشد و بیش از پیش سازوکار وقوع و کشف این گونه جرایم را پیچیده‌تر سازد (در این زمینه؛ نک: طهماسبی و شاهمرادی، ۱۳۹۷: ۱۲۱-۹۵). در واقع، تحولاتی از این دست در خصوص امکانات و موضوعات مجرمانه و نحوه ارتکاب جرم در پرتو جهانی شدن، علاوه بر ایجاد موضوعات و بسترهای نوین برای ارتکاب جرم، تحولات گسترده‌ای در شیوه و ابزارهای ارتکاب جرم نیز ایجاد کرده است؛ امری که فناوری را در خدمت بزهکاری قرار داده و جرم را به‌مثابه یک خدمت در بستر فضای سایبر قابل عرضه کرده است.

۲-۱. فناوری در خدمت بزهکاری؛ از دارکنت تا بیت‌کوین

معروف‌ترین ارز مجازی، بیت‌کوین است. بیت‌کوین یک سامانه رایانه‌ای عمومی است که امکان پرداخت غیرمتمرکز و شخص به شخص (بدون نیاز به وجود شخص یا نهاد ثالث، مانند صرافی‌ها یا بانک‌ها) را فراهم می‌کند. این سامانه، قدرت خود را از کاربران می‌گیرد و بدون هیچ واسطه یا مرجع مرکزی برای مدیریت که در آن دخل و تصرف کند، فعالیت می‌کند. در اوت سال ۲۰۰۸ دامنه پایگاه Bitcoin.org در شبکه اینترنت ثبت شد و تا به امروز نیز مشخص نیست که چه کسی این دامنه را به ثبت رسانده است. در اکتبر سال ۲۰۰۸ فردی به نام «ساتوشی ناکاماتو» در خبرنامه رمزگذاری شده‌ای به نام metzdowd.com اعلام کرد: «من در حال کار بر روی سامانه پول

الکترونیکی جدیدی هستیم که کاملاً شخص به شخص و بدون دخالت شخص ثالث است.» مقاله مذکور سرمنشأ این پول مجازی، یعنی بیت کوین بوده و معروف به مقاله سفید با عنوان «بیت کوین: سامانه پولی الکترونیک شخص به شخص» است.

پرسش مهم این است که چه عواملی سبب جلب نظر بزهکاران یقه سفید به استفاده از ارزهای مجازی برای انجام فعالیت‌های مجرمانه می‌شود؟ شاید پاسخ این سؤال، نیاز به پول‌شویی درآمدهای مجرمانه جهت استفاده از آن در نظام‌های پولی و مالی باشد. یکی از جرایم مهم یقه سفیدی فراملی، پول‌شویی است. مقصود از پول‌شویی استفاده از شیوه‌هایی است که از طریق آن بزهکاران، منشأ سود نامشروع را مخفی و از آن راه، پول کثیف را به پول تمیز تبدیل می‌کنند. چنین امری می‌تواند از طریق معاملات مالی فراملی بی‌شمار و پیچیده تحقق پذیرد. امروزه، نظام بین‌المللی نقل و انتقال وجوه و رمزگشایی از کارت‌های اعتباری، انتقال پول را با سرعت نور ممکن ساخته که همین امر موجب تحول زمانی و مکانی پول‌شویی نیز شده است.

بدین‌سان، نیاز به طرق امن و غیرقابل شناسایی برای پول‌شویی درآمدهای مجرمانه، از ابتدایی‌ترین ضرورت‌های حفظ حیات فعالیت جنایی است. در واقع همین ویژگی‌هاست که جذابیت ارزهای مجازی را برای گروه‌های جنایی دوچندان کرده است. بدین منظور حرکت به سمت فضای مجازی و تمرکز بر این فضا و استفاده از امکانات منحصربه‌فرد آن، زمینه‌ساز مجازی شدن جرایم یقه سفیدی شده است. موضوعی که در بررسی پرونده‌های کیفری در ارتباط با ارزهای مجازی، به‌ویژه پرونده جاده ابریشم^۱، به‌وضوح مشاهده می‌شود. در سازوکار این سامانه فروش برخط، به‌طور آشکار می‌توان مشاهده کرد که فناوری به خدمت بزهکاری درآمده است. جاده ابریشم با قرارگرفتن بر لایه پنهان اینترنت، یعنی دارکنت و استفاده از ابزار مالی ارزهای مجازی، تبدیل به یک سامانه مجرمانه جهت ارتکاب طیف وسیعی از جرایم شد.

۱-۲. جاده ابریشم؛ سامانه فروش برخط مجرمانه

جاده ابریشم، با سامانه فروش برخط «از فروشنده تا منزل»، تبدیل به بزرگترین بازار سیاه برخط شد. جاده ابریشم ناشناخته‌ترین بازار برخط در فضای دارکنت است که برای تسهیل فروش محصولات غیرقانونی، به‌ویژه پول‌شویی و خرید و فروش مواد مخدر شناخته شده است (Christin, 2013; Hout & Bingham, 2013). بر این اساس بررسی پرونده جاده ابریشم بیانگر ویژگی‌هایی است که استفاده از ارزهای مجازی را برای ارتکاب جرم یقه سفیدی جذاب‌تر می‌سازد.

راس ویلیام اولبریچ در سال ۲۰۱۱ جاده ابریشم را ایجاد کرد. در جاده ابریشم، مواد مخدر و سایر محصولات غیرقانونی، برای مثال کارت‌های اعتباری سرقتی، و خدمات غیرقانونی، از جمله استخدام برای قتل، از فروشنده یا خدمات‌دهنده تا منزل خریدار یا خدمت‌گیرنده ارائه می‌شد (Afiploaie & Shortis, 2015). بیت‌کوین یگانه ارز پذیرفته‌شده در جاده ابریشم بود. طی دو سال فعالیت موفق، جاده ابریشم بیش از ۱/۲ میلیارد دلار به دست آورد.

اولین گام برای همه فروشندگان در جاده ابریشم این بود که یک فروشگاه در آن راه‌اندازی کنند. فروشنده باید از نحوه کار در سرویس Tor آگاهی می‌داشت و به جاده ابریشم دسترسی پیدا می‌کرد. Tor در اصل یک شبکه توزیع رایانه‌ای است که آدرس IP واقعی کاربر را پنهان می‌کند و به همین علت هویت کاربران شبکه را با مسیریابی ارتباطات یا معاملات، از طریق چندین رایانه در سراسر جهان از شناسایی مصون می‌سازد و آن‌ها را در چندین لایه رمزگذاری شده قرار می‌دهد. مرحله دوم این بود که خریداران جهت خرید کالا یا دریافت خدمتی غیرقانونی، بیت‌کوین به دست آورند و یک آدرس برای تحویل کالا یا خدمات معرفی کنند. یگانه وجه پرداختی مقبول در جاده ابریشم، بیت‌کوین بود و چنانچه خریداران بیت‌کوین نداشتند، می‌توانستند از سرویس مبادله یا صرافی بیت‌کوین برای تبدیل ارزشهای رایج و قانونی خود به بیت‌کوین استفاده کنند. «فیلا و شرم» دو نفر از مرتبطان جاده ابریشم، چنین صرافی‌ای راه‌اندازی کردند. آن‌ها وجوه نقد را از مشتری دریافت و آن را به بیت‌کوین تبدیل می‌کردند. سپس بیت‌کوین‌ها را به حساب مشتری در جاده ابریشم انتقال می‌دادند و مبلغی را به‌عنوان هزینه تبدیل دریافت می‌کردند. همچنین خریداران باید آدرسی را برای دریافت کالاهایی که خریداری شده است، فراهم می‌کردند. بسیاری از آن‌ها از خدمات صندوق پستی با استفاده از هویت جعلی استفاده می‌کردند. مرحله سوم، تحویل و پرداخت بود. برای پیشگیری از تحویل کنترل‌شده، جاده ابریشم دستورالعمل‌های مفصلی را برای کمک به مشتریان خود ارائه می‌کرد. جهت اجتناب از کشف مواد مخدر در تحقیقات معمول پستی در خصوص بسته‌های ارسالی، با سگ‌های موادیاب، فروشندگان از کیسه‌های خلاء مهر و موم‌شده و زیپ‌دار برای ارسال مواد مخدر استفاده می‌کردند. جاده ابریشم از یک سامانه سپرده خاص استفاده می‌کرد. تحت

۱. تحویل کنترل‌شده، روشی است که توسط نهادهای اجرای قانون مورد استفاده قرار می‌گیرد. در این روش، زمانی که نهاد مجری قانون، محموله مواد مخدر را شناسایی می‌کند، از توقیف آن خودداری کرده و اجازه می‌دهد تحت کنترل و نظارت، محموله منتقل شود و به مقصد برسد تا بدین وسیله، اقدامات لازم برای شناسایی مقصد و سایر موارد صورت پذیرد (نک: بند «خ» ماده ۲ کنوانسیون سازمان ملل متحد برای مبارزه با جرایم سازمان‌یافته فراملی مصوب ۲۰۰۰).

این سامانه، خریداران، بیت‌کوین را از کیف پول خود (توسط وبسایت) به حساب خود در جاده ابریشم انتقال می‌دادند. هنگامی که فروشندگان مطلع می‌شدند که پرداخت صورت گرفته است، کالا را تحویل می‌دادند. هنگامی که خریداران، کالا یا خدمات را دریافت کردند، با تأیید معامله، پرداخت نهایی به فروشندگان صورت می‌پذیرفت. برای جلوگیری از پرداخت مستقیم خریداران به فروشندگان، خارج از سازوکار جاده ابریشم، اولبریچ قوانینی را مبنی بر ممنوعیت این چنین پرداخت‌هایی و ضمانت‌اجرائی برای آن وضع کرد.

سرانجام جاده ابریشم توسط FBI در سال ۲۰۱۳ با شناسایی مؤسس و اداره‌کنندگان آن مسدود شد. علت شناسایی مجرمان در این پرونده نیز این بود که راس اولبریچ با بی‌دقتی از آدرس ایمیل شخصی خود در یک انجمن گفتگو برخط استفاده کرد. اگرچه او متوجه این اشتباه شد و آدرس ایمیل را حذف کرد، FBI توانست او را ردیابی کند و سرانجام در سانفرانسیسکو شناسایی و دستگیر شد (Lane, 2014). پس از دستگیری اولبریچ، ۸ نفر از دست‌اندرکاران جاده ابریشم در سراسر جهان، از جمله در انگلستان، سوئد و ایالات متحده دستگیر شدند. دیگر ارائه‌کنندگان خدمات مبادله بیت‌کوین (صرافی‌های بیت‌کوین) نیز به دلیل مبادله بیت‌کوین در ازای ارزهای سنتی برای کاربران جاده ابریشم دستگیر شدند. از میان پرونده‌های کیفی مرتبط با دارکنت و بیت‌کوین، جاده ابریشم نمونه کاملی محسوب می‌شود که براساس آن می‌توان خطرات مجرمانه ارزیابی مجازی را تحلیل کرد؛ زیرا این بازار برخط مجرمانه، نمونه کاملی از یک سازمان مجرمانه مجازی برای ارتکاب جرایم غالباً یقه‌سفیدی با استفاده از ارز مجازی است.

۲-۱-۲. دارکنت؛ بستر امن مجرمانه

فعالیت‌های غیرقانونی در فضای دارکنت و به واسطه ارزیابی مجازی، شامل دامنه وسیعی از جرائم، از جمله انتقال وجه بدون مجوز قانونی، قاچاق مواد مخدر، هک رایانه‌ای، کلاهبرداری و تا حدودی فعالیت‌های تروریستی می‌شوند. با این حال، می‌توان امکانات و قابلیت این فضا در پول‌شویی درآمدهای مجرمانه را علت اصلی اقبال بزهاران یقه‌سفیدی به این فضا دانست. موضوعی که با قرارگرفتن جاده ابریشم در بستر امن دارکنت، تجلی پیدا کرد.

سه نوع وبسایت اینترنتی وجود دارد: نخست، «وب سطحی»^۱ که وبسایت‌هایی که به‌عنوان بخشی از وب سطحی شناخته می‌شوند، به دلیل نمایه‌دار شدن آن‌ها از طریق موتورهای جستجو، در دسترس هستند؛ دوم، وبسایت‌های دیگر که از طریق مرورگرهای استاندارد وب، دسترسی‌پذیر

هستند ولی توسط موتورهای جستجو دسترسی پذیر نیستند، به عنوان بخشی از «وب عمیق»^۱ طبقه بندی می شوند و توسط موتورهای جستجو نشان داده نمی شوند؛ رده نهایی، «دارکنت»^۲ است که با وب سایت سطحی و وب عمیق تفاوت دارد؛ برخلاف وب سایت های موجود در وب سطحی، وب سایت هایی که به عنوان بخشی از دارکنت طبقه بندی می شوند، از طریق موتورهای جستجوی معمولی قابل جستجو نیستند. تمایز دارکنت از وب عمیق نیز از نحوه دسترسی به آنها شکل می گیرد؛ دارکنت به کاربران اجازه می دهد تا در اینترنت به جستجو بپردازند؛ در حالی که با مسیریابی اتصالات توسط سرورهای پروکسی شخص ثالث و مسدود کردن آدرس IP کاربر، از آنها در برابر نظارت و تحلیل ترافیک محافظت می کند (Weimann, 2016:42). مجله وایرد (Wired) تخمین می زند که دارکنت بیش از ۱/۰ درصد از اینترنت را شامل نمی شود. با این حال، به دلیل ناشناس بودن و امنیتی که دارکنت فراهم می کند، اغلب توسط مجرمان سایبری برای فعالیت های غیرقانونی مورد استفاده قرار می گیرد. گزارش ها حاکی از آن است که ۵۷ درصد محتوای دارکنت غیرقانونی است؛ مانند پورنوگرافی، مراودات مالی غیرقانونی، فروش مواد مخدر و سلاح، پول شویی و ارتباطات تروریستی (Wechsler, 2016).

چند راه شناخته شده برای دسترسی به دارکنت وجود دارد: نخستین راه، استفاده از مرورگر Tor است.^۳ «مرورگر Tor یک سیستم پیوندی مسیریابی است که یک آدرس خام رایانه ای شخصی را پیش از رسیدن به مقصد، از طریق تکرار داده های رمزنگاری شده ای که از طریق چندین سرور که به طور تصادفی انتخاب شده ارسال می کند و ردیابی را غیرممکن می سازد.» (Crawford, 2014) مسیریابی پیازی به این معنی است که «پیام ها در لایه هایی از رمزنگاری محفوظ می شوند. داده های رمزگذاری شده از طریق یک مجموعه از گره های شبکه، به نام روترهای پیازی منتقل می شوند، که

1. Deep Web

2. Dark Web

۳. سامانه Tor (The Onion Route) برای ناشناس ماندن کاربران در محیط اینترنت به کار می رود و از نرم افزار کارخواه و شبکه ای از سرورهای دهنده (سرورها) تشکیل شده است و می تواند داده هایی از کاربران مانند موقعیت مکانی و نشانی پروتکل اینترنت را پنهان کند. بهره گیری از این سامانه، ردگیری و شنود داده های کاربر را از سوی دیگران بسیار سخت می کند. این ردگیری و شنود می تواند در زمینه بسیاری از فعالیت های کاربر، مثل وبگاه هایی که بازدید کرده، داده هایی که بارگیری و بارگذاری کرده، پیام هایی که از طریق نرم افزارهای پیام رسان ارسال یا دریافت کرده و هرگونه ارتباطاتی که در محیط اینترنت برقرار کرده است، صورت پذیرد؛ لذا می توان گفت که این سیستم برای محافظت از آزادی کاربران و حفظ حریم خصوصی آنها در محیط اینترنت طراحی شده است. این نرم افزار، یک نرم افزار آزاد است و استفاده از شبکه آن نیز رایگان است.

هر کدام از آن‌ها یک لایه را برمی‌دارد و مقصد بعدی داده را کشف می‌کند. وقتی لایه نهایی رمزگشایی می‌شود، پیام به مقصد می‌رسد. در این حالت فرستنده ناشناس باقی می‌ماند؛ زیرا هر واسطه فقط محل گره‌های بلافاصله قبل و بعد خود را می‌داند» (J. Mounteney & A. Oteo, 2017: 136).

کاربران می‌توانند Tor را با جستجوی آن بر روی هر مرورگر وب سطحی، دانلود کنند. این کار نسبتاً آسان است؛ مراحل لازم برای استفاده از این سرویس در یک وب سایت به نام PC Advisor نشان داده شده است: «به www.torproject.org بروید و Tor Browser Bundle را دانلود کنید که حاوی تمام ابزارهای مورد نیاز است. فایل دانلودشده را اجرا کنید. یک محل ذخیره را انتخاب کنید. سپس پوشه را باز کنید و روی Start Tor Browser کلیک کنید؛ به همین سادگی. پنل مدیریت Vidalia به‌طور خودکار تنظیمات شبکه تصادفی را انجام می‌دهد و وقتی Tor آماده شد، مرورگر باز خواهد شد؛ برای جدا شدن از شبکه، دوباره فقط باید آن را ببندید.» (Egan, 2017) علاوه بر این، Tor از طریق تقریباً ۶۰۰۰ سرور، سیگنال‌ها را هدایت می‌کند (Spalevic & Ilic, 2017: 75). هر دو مرحله باعث می‌شوند که ردیابی سوابق یک مجرم غیرممکن گردد. بدین ترتیب، اگر یک سوءاستفاده‌گر جنسی کودک، سایت‌های پورنوگرافی کودکان را مرور کند یا یک هویت شهروندی جعلی را خریداری کند، نهادهای اجرای قانون تا زمانی که از مرورگر Tor استفاده می‌شود، هرگز متوجه نخواهند شد.

یکی دیگر از مرورگرهای دارکنت، I2P (Project Internet Invisible) است که اجازه ارتباطات ناشناس بین کاربرانی را که مایل به اشتراک فایل هستند، می‌دهد (Spalevic & Ilic, 2017: 75). اتصال اینترنت بین کاربران، با رمزگذاری محافظت می‌شود. در مقایسه با Tor، I2P در برابر کنترل و نظارت، ارتجاعی‌تر است. Freenet یک نسخه ساده از I2P است و به اشتراک‌گذاری فایل را برای مخاطبان گسترده‌تری امکان‌پذیر می‌سازد. Freenet یک ارتباط جدید با مسیرهای جدید ایجاد می‌کند. مانند Tor، I2P و Freenet به دلیل عدم امکان ردیابی به‌طور کامل ناشناسی را فراهم می‌کنند.

تشخیص دقیق تعداد افرادی که در فعالیت‌های غیرقانونی دارکنت مشغول فعالیت هستند، دشوار است؛ اما معیارهایی وجود دارد که بر اساس آن می‌توان مواردی را احراز کرد؛ به‌عنوان مثال، Tor تخمین می‌زند که ۱۰۰,۰۰۰ نفر هر روز آن را دانلود می‌کنند (Tor Browser in Numbers, 2107). از این تعداد، برآورد شده است که بین ۵۰۰۰ تا ۱۵۰۰۰ نفر از Tor در روز استفاده می‌کنند (Spalevic & Ilic, 2017: 75)؛ بدون آنکه اطلاعات هویتی کاربران جمع‌آوری و ذخیره شود. پروتکل Tor بیان می‌کند: «ما داده‌های مورد استفاده در بالا را از پرونده‌های سرور وب Tor Project استخراج می‌کنیم. نگران نباشید! ما چیزی را که بدان احتیاجی نداریم، ثبت نمی‌کنیم»

(آدرس IP شما یا زمان درخواست‌ها) و اطلاعات شناسایی را قبل از پردازش حذف می‌کنیم و فقط یک نسخه پاک شده را نگه می‌داریم.» (Spalevic & Ilic, 2017: 75)

در سطح جهانی، دارکنت، تبدیل به یک مکان ملاقات برای افرادی شده است که به دنبال محصولات غیرقانونی هستند. مردم به طور کاملاً ناشناس، قادر به انجام هرگونه معاملات غیرقانونی یا ارضای تمایلات انحرافی خود هستند و دولت‌ها توانایی کمی در متوقف کردن آن‌ها دارند. از این رو، قرارگرفتن سامانه‌های برخط مجرمانه‌ای چون جاده ابریشم در بستر دارکنت و استفاده از ارزهای مجازی، مانند بیت‌کوین، به عنوان ابزار مالی پذیرفته شده در مبادلات آن، بیش از پیش مخاطرات مجرمانه‌ای را ایجاد کرده که بررسی آن اجتناب‌ناپذیر است.

۳-۱-۲. ارز مجازی؛ ابزاری با کارکرد مجرمانه

برای خرید محصولات یا دریافت خدماتی که در دارکنت وجود دارد، به یک ارز مجازی نیاز است. بیت‌کوین^۱ یک مثال ساده آن است. بیت‌کوین یک ارز مجازی است که واقعی یا فیات نیست.^۲ در عوض، از لحاظ الکترونیکی مشتق شده و قابل ارزیابی به عنوان پول است که می‌تواند پیشگام در عصر جدید تجارت آنلاین باشد. افزایش ارزش بیت‌کوین به تقاضای آن بستگی دارد که در شکل مثبت با هدف سرمایه‌گذاری و در شکل منفی با هدف خرید کالا یا خدمات غیرقانونی در فضای دارکنت کسب می‌شود. با وجود اختلاف در ماهیت، باید کارکرد پول را برای بیت‌کوین به رسمیت شناخت و آن را به عنوان یک واحد حساب، یک ذخیره ارزش و یک وسیله مبادله محسوب کرد.

وجود بیت‌کوین در دارکنت ضروری است؛ زیرا «از فناوری نظیر به نظیر یا شخص به شخص استفاده می‌کند که برای کار، احتیاج به هیچ مقام مرکزی یا بانکی ندارد؛ کاربر معاملات را مدیریت می‌کند و صدور بیت‌کوین‌ها به صورت جمعی توسط شبکه انجام می‌شود. بیت‌کوین منبع باز است؛ طراحی آن عمومی است: هیچ‌کس صاحب یا کنترل‌کننده بیت‌کوین نیست و همه می‌توانند با آن کار کنند.... بیت‌کوین قابلیت‌های استفاده هیجان‌انگیزی دارد که سیستم‌های پرداخت دیگر از آن

۱. بیت‌کوین (با حرف بزرگ) هم به نرم‌افزار منبع باز استفاده شده برای ایجاد ارز مجازی و هم شبکه شخص به شخص (p2p) و بیت‌کوین (bitcoin (حروف کوچک) به واحدهای ارزش ارز مجازی اشاره دارد.
۲. پول فیات پولی است که فاقد هرگونه ارزش ذاتی بوده و ارزش آن تنها وابسته به حکومت است. در این نوع سیستم با از بین رفتن حکومت، پول ضرب شده توسط آن حکومت نیز بی‌ارزش می‌شود. در زمان قدیم، پول تمامی کشورها معمولاً به فلزات گرانبها نظیر طلا و نقره متصل بود؛ ولی بعد از لغو یکجانبه پیمان برتون وودز از سوی آمریکا در سال ۱۹۷۱، پول مورد استفاده در تمامی کشورهای دنیا پول فیات است.

محروم هستند^۱. بیت‌کوین‌ها به چهار روش به دست می‌آیند: دریافت به واسطه فروش کالا یا ارائه خدمات، خرید بیت‌کوین با پول واقعی، مبادله بیت‌کوین‌ها و استخراج^۲. استخراج، روند جمع‌آوری بیت‌کوین‌ها با استفاده از رایانه‌های تخصصی است. افراد زیادی نمی‌توانند این کار را انجام دهند؛ اما این یک سرمایه‌گذاری کاملاً سودآور است؛ زیرا به‌زودی فرایند آن پایان خواهد یافت^۳. بیت‌کوین به دلیل سه مزیت عمده به خریداران و فروشندگان در بازارهای دارکنت ارائه می‌شود. نخست، خطرات کمتر برای کاربران؛ معاملات بیت‌کوین امن و غیرقابل‌برگشت هستند و حاوی اطلاعات حساس یا شخصی یا هویتی مشتری نیستند. این کار از کاربران در برابر خسارات ناشی از تقلب یا بازپرداخت‌های جعلی محافظت می‌کند. آن‌ها به راحتی می‌توانند به بازارهای جدیدی راه پیدا کنند که در آن یا کارت‌های اعتباری در دسترس نیستند یا نرخ تقلب به‌طور غیرقابل‌قبولی بالاست. نتایج این امر عبارت است از هزینه‌های نازل‌تر انتقال، دسترسی به بازارهای بزرگتر و هزینه‌های مادی و غیرمادی اداری کمتر. دوم، امنیت و کنترل؛ کاربران بیت‌کوین بر معاملات خود کنترل کامل دارند. پرداخت‌های بیت‌کوین را می‌توان بدون اطلاعات شخصی مرتبط با معامله انجام داد. این کار در برابر سرقت هویت از کاربر محافظت می‌کند. کاربران بیت‌کوین همچنین می‌توانند از ارزش‌های خود با استفاده از خدمات پشتیبانی مضاعف و رمزگذاری، حفاظت بیشتری کنند. سوم، شفافیت؛ تمام اطلاعات مربوط به عرضه پول بیت‌کوین در بلاک‌چین برای هر کسی، جهت تأیید و استفاده، در هر زمانی در دسترس است. هیچ فرد یا سازمانی نمی‌تواند پروتکل بیت‌کوین را کنترل یا دستکاری کند؛ زیرا از طریق رمزنگاری ایمن‌سازی شده است. این کار اجازه می‌دهد تا هسته بیت‌کوین کاملاً شفاف و پیش‌بینی‌پذیر باشد.

بیت‌کوین، امنیت و ناشناسی بودن را فراهم می‌کند که کارت‌های اعتباری فاقد آن هستند؛ هیچ دنباله کاغذی وجود ندارد. هیچ ارتباطی با بانک‌ها ندارد و مهم‌تر از همه، توسط نهادهای اجرای قانون کنترل‌شدنی نیست. بیت‌کوین مانند پول نقد است؛ اما از آنجایی که مجازی است، نیازی به حضور اشخاص ثالث در فرایند کاربری ندارد. این امر موجب می‌شود اشخاص برای خرید

1. Bitcoin.org, <https://bitcoin.org/en/> accessed February 14, 2016.

2. "Frequently Asked Questions" Bitcoin, <https://bitcoin.org/en/faq#what-is-bitcoin>, accessed June 14, 2017.

۳. بیت‌کوین این امکان را به کاربر می‌دهد، به‌عنوان معدنچی، با استفاده از ویژگی «استخراج»، به تولید بیت‌کوین بپردازد. معدنچی عبارت است از فرد یا مؤسسه‌ای که در شبکه ارز مجازی غیرمتمرکز، با استفاده از نرم‌افزار ویژه مشارکت می‌کند تا با استفاده از الگوریتم‌های پیچیده اقدام به تولید ارز مجازی نماید (FATF, 2015: 29).

محصولات غیرقانونی از مجرمان راحت تر باشند. در مجموع، بیت کوین هم برای کاربری های مشروع و هم برای تبهکاران امنیت گسترده ای را فراهم می کند و اطمینان لازم جهت تسهیل معاملات در جهان زیرزمینی را ایجاد می کند.

۲-۲. دلایل جذابیت ارزشهای مجازی برای بزهکاران

بررسی پرونده جاده ابریشم و برخی پرونده های کیفی مرتبط با ارز مجازی، نشانگر چهار عامل است که بسیاری از بزهکاران سنتی را جذب تجارت برخط در فضای مجازی کرده است. چهار عامل، انعطاف پذیری هویت، ناشناختگی، سهولت شرکت در عملیات مجرمانه و فقدان بازدارندگی، از عوامل تسهیل کننده تجارت غیرقانونی در فضای مجازی شناخته می شوند که با وجود ارزشهای مجازی تقویت شده اند. بررسی این موارد نشان از جایگاه ارزشهای مجازی در بزهکاری یقه مجازی ها و به عنوان نقطه عطفی در این گونه از بزهکاری است.

۲-۲-۱. انعطاف پذیری هویت

انعطاف پذیری هویت، از جذاب ترین عواملی است که سبب جلب توجه مجرمان به فضای مجازی می گردد. این امر جزء ویژگی های ذاتی فضای مجازی است که با وجود ارزشهای مجازی تشدید شده است. بدین سان، بررسی انعطاف پذیری هویت از چند بُعد درخور توجه است. نخست، تمام مجرمان برخط از هویت جعلی استفاده می کنند. هویت های جعلی آنها تا حدودی برخی از جنبه های کار آنها را نمایان می سازد. امری که در جاده ابریشم به وضوح دیده می شود. اشخاص درگیر در پرونده جاده ابریشم، شامل مالک جاده ابریشم، اولبریچ، کارمندانش، اندرو مایکل جونز، گری دیویس، پیتر فیلیپ ناش و راجر توماس کلارک^۱، فروشندگان مواد مخدر استیون لوید سدلر و جرمی دانگال^۲، رابرت فایلا و چارلی شرم^۳، فروشندگان یا صرافان بیت کوین فعال در این بازار برخط مجرمانه و مأموران FBI مسئول بررسی پرونده، اولبریچ، کارل مارک و شان بریج^۴، که متهم به پول شویی و تخلفات مالی شدند، می شود. دانگال، فروشنده مواد مخدر، از «Xanax king» و «XX» و فیلا، فروشنده بیت کوین، از عنوان «BTCKing» به عنوان هویتی برای خود استفاده می کردند.

1. Andrew Michael Jones, Gary Davis, Peter Phillip Nash, and Roger Thomas Clark
2. Steven Lloyd Sadler and Jeremy Donagal
3. Robert M. Faiella and Charlie Shrem
4. Carl Mark Force and Shaun W. Bridges

دوم، بیش از هشتاد درصد مجرمان اینترنتی از بیش از دو هویت استفاده می‌کنند (Kethineni, Roberts, «DPR» یا «Silk Road» به‌عنوان نام کاربری خود استفاده می‌کرد و کارل، مأمور اداره مبارزه با مواد مخدر، زمانی که به‌عنوان مأمور مخفی FBI برای شناسایی گردانندگان و مرتبطان جاده ابریشم فعالیت می‌کرد، از عنوان «NOB» برای برقراری ارتباط با اولبریچ استفاده می‌نمود و هنگامی که قصد اخذی از اولبریچ را داشت، نام «French Maid» و «Carla Sophia» را به کار می‌برد. در یکی از پیام‌هایی که از کارل جهت اخذی به اولبریچ فرستاده شده بود، وی با نام کاربری French Maid نوشت: «من از این بابت متأسفم. نام من کارل سوفیاست و دوستان بسیاری در بازار دارم. DPR مشتاق شنیدن حرف‌های من خواهد شد.»

سوم، مجرمان اینترنتی، برای اجتناب از شناسایی، مکرراً هویت خود را تغییر می‌دهند و این حتی زمانی که هویت‌ها جعلی است نیز رخ می‌دهد. راجر کلارک، که از ژانویه ۲۰۱۱ تا اکتبر ۲۰۱۳ به اولبریچ در مدیریت جاده ابریشم کمک می‌کرد، از چهار هویت متفاوت در بازه زمانی سه‌ساله استفاده کرد. در آغاز، او هویت «Jones Variety» و «VJ» را برگزید. در پیامی به اولبریچ در ۲۹ اکتبر ۲۰۱۱، خود را «Cimon» نامید. در ژوئن ۲۰۱۲، از عنوان «Plural of Mongoose» در برقراری ارتباط با اولبریچ استفاده نمود.

انعطاف‌پذیری در هویت، سبب سهولت کار برخط مجرمان فضای مجازی می‌گردد. اگرچه آن‌ها غالباً با هم در تماس هستند، تمام آنچه از یکدیگر می‌دانند، تنها یک نام جعلی است. آن‌ها هیچ شناختی نسبت به جنسیت، لهجه یا شکل ظاهری یکدیگر ندارند و به‌گونه‌ای امن پشت هویت‌های متعدد خود پنهان می‌شوند.

این امر اگرچه ویژگی ذاتی فضای مجازی است، باید در این خصوص به این نکته توجه داشت که در فضای مجازی قابلیت ردیابی و شناسایی افراد، حتی در مواردی که از چندین هویت جعلی استفاده می‌کنند، وجود دارد. با این حال فضای دارکنت، این ویژگی منحصربه‌فرد را به وجود آورده است تا ردیابی از کاربر در فضای مجازی باقی نماند و در صورت استفاده از چندین هویت، شناسایی از طرق دیگر نیز در عمل بسیار دشوار شود. این امر با وجود ارزشهای مجازی ابعاد جدیدی یافته است که می‌تواند مکملی جهت تقویت این قابلیت چندگانگی و انعطاف‌پذیری در هویت

باشد. این مکمل عبارت است از تعداد «مشارکت کنندگان زیاد و کنترل نشده»^۱ که در ایجاد و استفاده از ارزهای مجازی شرکت می‌کنند.

مشارکت کنندگان در فرایند مبادلات به واسطه ارزهای مجازی، طیف وسیعی از اشخاص حقیقی و حقوقی را شامل می‌شوند. از این رو، یک ارز مجازی ممکن است توسط مجمعی از «معدنچیان» (در خصوص ارز رمز پایه غیر متمرکز، مانند بیت کوین) یا توسط یک نهاد مجزا (در خصوص ارز مجازی متمرکز)^۲ صادر شود؛ توسط عده‌ای تحت عنوان صراف به فروش برسد؛ کاربرانی از آن در مبادلات خود استفاده کنند و عده‌ای دیگر اقدام به ذخیره آن در کیف پول‌های خاص نمایند. بدین ترتیب، در فرایند ارزهای مجازی با گستردگی اشخاص دخیل مواجه هستیم که با انعطاف پذیری در هویت، بیش از پیش موجبات سردرگمی مأموران مجری قانون را فراهم می‌کنند.

۱. منظور از مشارکت کنندگان در فرایند ارزهای مجازی، تمامی افرادی هستند که به نوعی در جریان مبادلات به واسطه ارزهای مجازی دخیل‌اند؛ برای مثال، در فرایند بیت کوین این اشخاص فعال هستند: یک مبدل یا صراف (Exchanger) عبارت است از شخص یا نهادی که به عملیات صرافی جهت تبدیل ارز مجازی به ارز واقعی، پول یا دیگر اشکال ارزهای مجازی و همچنین فلزات گران بها و بالعکس می‌پردازد. صرافان عموماً دامنه وسیعی از پرداخت‌ها، از قبیل پول نقد، کارت‌های اعتباری و دیگر ارزهای مجازی را می‌پذیرند. کاربران عموماً از صرافان برای سپرده‌گذاری و برداشت پول از حساب‌های ارزی مجازی استفاده می‌کنند. کاربر (User) فرد یا نهادی است که ارز مجازی را به دست می‌آورد و از آن برای خرید کالا یا خدمات واقعی یا مجازی استفاده می‌کند یا انتقال‌ها را به صورت شخصی به فرد دیگری (برای استفاده شخصی) ارسال می‌کند یا پولی مجازی را به عنوان سرمایه حفظ می‌کند. کاربران می‌توانند پول مجازی را از چندین راه بدست آورند: برای مثال، آن‌ها می‌توانند (۱) پول مجازی را با استفاده از پول واقعی (از طریق مبادله یا در ارزهای مجازی متمرکز مستقیم از مدیر یا تولیدکننده) خریداری کنند؛ (۲) در فعالیت‌های خاصی که منجر به کسب ارز مجازی می‌شود، درگیر باشند؛ (۳) با توجه به ساختارهای برخی از ارزهای مجازی غیر متمرکز خود اقدام به تولید ارز نمایند. برای مثال بیت کوین این امکان را به کاربر می‌دهد، به عنوان معدنچی (Miner)، با استفاده از ویژگی «استخراج» (Mining) به تولید بیت کوین پردازد. معدنچی عبارت است از فرد یا مؤسسه‌ای که در شبکه ارز مجازی غیر متمرکز، با استفاده از نرم افزار ویژه مشارکت می‌کند تا با استفاده از الگوریتم‌های پیچیده، اقدام به تولید ارز مجازی نماید (FATF, 2015:29). معدنچیان همچنین ممکن است در یک سامانه ارز مجازی به عنوان صراف شرکت کنند؛ ارز مجازی را به عنوان یک کسب و کار ایجاد نمایند تا بتوانند آن را در برابر پول نقد یا دیگر ارزهای مجازی بفروشند.

۲. ارز مجازی غیر قابل تبدیل (یا بسته) مختص یک حوزه یا جهان مجازی خاص است؛ مانند بازی‌های برخطی که دارای چندین کاربر هستند (MMORPG) یا سایت Amazon.com. طبق قوانینی که استفاده از این نوع ارزها را کنترل می‌کنند، آن‌ها نمی‌توانند با پول رایج مبادله شود (FATF, 2015:27). نمونه‌های آن عبارت‌اند از: دلارهای Project Entropia، Q Coins و طلای World of Warcraft که همگی از بازی‌های برخط هستند.

این امر در کنار گستردگی قلمرو جغرافیایی حضور این اشخاص و محدود نبودن آن‌ها به مرزهای کشوری خاص تشدید می‌شود. در این زمینه یکی از تشکیلات مجرمانه، به نام لیبرتی‌رزرو که با استفاده از ارز مجازی در زمینه توزیع، ذخیره و پول‌شویی درآمدهای مربوط به فروش کارت‌های اعتباری، سرقت هویت، تقلب در سرمایه‌گذاری، هک، قاچاق مواد مخدر و پورنوگرافی کودکان فعالیت می‌کرد، درخور توجه است (FATF, 2015: 35). این مؤسسه در مقیاس گسترده و بُعدی جهانی اقدام به فعالیت می‌کرد و بیش از یک میلیون کاربر در سراسر جهان داشت؛ از جمله بیش از ۲۰۰,۰۰۰ کاربر در ایالات متحده و تقریباً با ۵۵ میلیون معامله انجام شده است که همه آن‌ها غیرقانونی بودند. در واقع تعداد مشارکت‌کنندگان زیاد با هویت‌های چندگانه غیرواقعی، به ویژه در فرایند کارکرد ارز مجازی، یکی از مشکلات نهادهای اجرای قانون در شناسایی و کشف بزهکاران دخیل در این تشکیلات مجرمانه بود. بدین ترتیب افزایش مشارکت‌کنندگان برخوردار از هویت‌های چندگانه، بیش از پیش کاربران مجرم ارزهای مجازی را از دسترس کنشگران نظام عدالت کیفری دور کرده است.

عدم کنترل نیز ویژگی مکمل دیگری برای انعطاف‌پذیری هویت است که سبب می‌شود نهادهای اجرای قانون که درصدد شناسایی هویت کاربر یا حداقل کشور محل فعالیت کاربر هستند، گمراه شوند (Kethineni & Cao & Dodge, 2018: 144). این امر نیز از ویژگی فراملی بودن فضای مجازی و دسترسی بدون مرز به آن نشئت می‌گیرد. برای نمونه، شاید کاربری که در کشور «الف» است، معامله‌ای را از طریق اینترنت آغاز می‌کند تا ارز ملی کشور «ب» را از طریق مبادله ارز مجازی در کشور «پ» تبدیل کند و این ارز مجازی را به یک کیف پول در کشور «ت» انتقال دهد. این ارز مجازی (احتمالاً از طریق سایر واسطه‌ها) می‌تواند به کیف پول دریافت‌کننده نهایی در کشور «ث» منتقل شود. این عملیات ممکن است از طریق یک مبادله در کشور «ج» انجام شود و به ارز کشور «چ» تبدیل شود. همچنین برای ایجاد دشواری بیشتر در خصوص کشف نقل و انتقالات، ممکن است کاربر اقدام به مبادله با اشخاص یا شرکت‌های کشوری نماید که به لحاظ سامانه مبارزه با پول‌شویی و تأمین مالی تروریسم دارای ضعف است یا اساساً بنا به دلایل مختلف، در این حوزه به طور بین‌المللی همکاری نمی‌کند. بدین سان حتی چنانچه یک شخص به شرحی که گذشت تمامی اقدامات را انجام دهد، به دلیل عدم وجود توان کافی برای کنترل مؤثر، کشف و شناسایی مرتکب در عمل غیرممکن می‌شود.

1. LIBERTY RESERVE (LR)

بدین ترتیب می‌توان به وضوح دید که ویژگی انعطاف هویت در فضای مجازی، در صورت ترکیب با ویژگی عدم قابلیت ردیابی دارکنت و ویژگی‌های مشارکت‌کنندگان زیاد و عدم کنترل کاربران ارزشهای مجازی، به میزان چشمگیری تمایل به ارتکاب جرم یا تمرکز فعالیت‌های مجرمانه در فضای مجازی را افزایش داده است.

۲-۲-۲. ناشناختگی

قرن‌هاست که به دلیل ممنوعیت‌های موجود در واردات یا صادرات تعدادی از کالاها، برخی فعالیت‌های تجاری بین‌المللی به صورت قاچاق روی می‌دهد. جدا از افزایش سطح معاملات تجاری معمولی که موجب افزایش فرصت‌های تجاری غیرقانونی شده، اینترنت نیز به طور گسترده‌ای شکل‌گیری بازارهای بین‌المللی غیرقانونی برای هر چیزی، از هرزه‌نگاری کودکان گرفته تا قاچاق مواد مخدر و سلاح و پول‌شویی، را تسهیل کرده است (اس.سیمپسون و ویزبرد، ۱۳۹۲: ۲۱۱). اما در آغاز هزاره سوم، تمایل به تمرکز فعالیت‌های مجرمانه تجاری در فضای اینترنت به واسطه گمنامی و ناشناسی مرتکبان افزایش یافته است. از این رو، شاید گمنامی، مهم‌ترین عامل تسهیل‌کننده‌ای باشد که مجرمان را به سوی فضای مجازی می‌کشاند. روش‌های متعددی وجود دارند که مجرمان فضای مجازی برای حفاظت از گمنامی خود طراحی نموده‌اند. نخستین فناوری، سرویس Tor است. جاده ابریشم بر اساس تکنیک Tor عمل می‌کند. Tor آدرس IP کاربران را مخفی می‌کند و از آن‌ها در برابر شناسایی و کشف محافظت می‌کند. روش دوم و بسیار مهم فناوری، ارزشهای مجازی است.

یکی از مزایای مهم ارزشهای مجازی این است که ناشناختگی کامل و عدم شناسایی را برای معاملات فراهم می‌کنند. در خصوص بسیاری از ارزشهای رمزپایه، گرچه هویت مدیران و ذی‌نفعان رمزگذاری شده‌اند و معاملات در یک فهرست عمومی ثبت و قابلیت ردیابی آن‌ها تضمین می‌شود، همچنان مسئله هویت اصلی ذی‌نفع را رفع نمی‌کند. در واقع با وجود قابلیت ثبت معاملات و کاربران، هویت اصلی کاربر و ذی‌نفع معاملات همچنان پوشیده باقی می‌ماند. این قابلیت ردیابی نه به موجب پروتکل‌های موجود ارزشهای مجازی تضمین شده است و نه از لحاظ سامانه‌ای امکان‌پذیر است (Kethineni & Cao & Dodge, 2018: 148). ضمن آنکه برخی از ارزشهای رمزپایه، ناشناسی و عدم ردیابی را به عنوان ویژگی‌های منحصر به فرد خود ارائه می‌دهند و در کنار آن به واسطه ابزارها و برنامه‌های کاربردی، این امکان را به کاربران می‌دهند که پرداخت‌های خود را توسط ترکیبی از شناسه‌های کاربری انجام دهند. علاوه بر این، علت و چرایی معاملات، هم از نظر

فنی و هم به لحاظ قانونی مشخص نیست که این قضیه موجب عدم شفافیت و ایجاد فضایی مبهم و جذاب برای سازمان‌های جنایی می‌شود.

عدم امکان ردیابی معاملات و مشخص کردن ذی‌نفعان واقعی آن، ویژگی منحصر به فرد و جذابی است که تبهکاران را به سمت خود جلب می‌کند. کاربران ارزهای مجازی صرفاً بر اساس شناسه حساب شناسایی می‌شوند که به واسطه عدم امکان شناسایی کاربر حقیقی، احتمال معاملات مجرمانه افزایش می‌یابد. نمونه‌ای از این امر در سازوکار لیبرتی رزرو نیز مشهود است. لیبرتی رزرو ارز مجازی خاص خود را داشت؛ اما در هر طرف، نقل و انتقالات به صورت پول نقد (دلار آمریکا) انجام و ذخیره می‌شد. برای استفاده از ارز لیبرتی رزرو، کاربر، یک حساب کاربری را از طریق وبسایت لیبرتی رزرو باز می‌کرد. در حالی که باز کردن حساب کاربری در لیبرتی رزرو ظاهراً نیاز به اطلاعات شناسایی اولیه داشت، به تأیید هویت‌ها توسط سرورها و سامانه‌های موجود نیاز نداشت. به همین دلیل کاربران به طور معمول تحت نام‌های دروغین، از جمله نام‌هایی با مضامین مجرمانه (مانند هک‌های روس) حسابی با آدرس‌های محل اقامت دروغین می‌ساختند (FATF, 2015: 27). برای اضافه کردن یک لایه ناشناخته دیگر، لازم بود که کاربران حساب‌های سپرده در لیبرتی رزرو ایجاد کنند و برداشت‌هایی را از طریق تبادلگران یا صرافان مستقر در برخی از کشورها که مقررات مربوط به نظارت‌های مالی در آن‌ها با محدودیت همراه بود، مانند مالزی، نیجریه و ویتنام، انجام دهند. لیبرتی رزرو، در سازوکاری مشابه با جاده ابریشم، با اجتناب از سپرده‌گذاری و برداشت مستقیم کاربران، از طریق انجام معاملات بانکی یا فعالیت‌های دیگری که موجب ایجاد رد معاملات می‌شوند، از جمع‌آوری اطلاعات در خصوص کاربران اجتناب می‌کرد. هنگامی که یک حساب کاربری ایجاد می‌شد، کاربر می‌توانست معاملات را با دیگر کاربران، با انتقال LR از حساب خود به حساب سایر کاربران، از جمله شرکت‌های تجاری «بازرگانان»^۱ که LR را به عنوان روش پرداخت قبول داشتند، انجام دهد (FATF, 2015: 28). به ازای هزینه اضافی تحت عنوان «هزینه حفظ حریم خصوصی» (۷۵ سنت ایالات متحده در هر معامله)، کاربران می‌توانستند شماره حساب‌های لیبرتی رزرو خود را هنگام نقل و انتقال پول، پنهان کنند و انتقال‌های آن‌ها به طور کامل غیر قابل شناسایی باشد و نه تنها ردی از معاملات باقی نماند، حتی در لایه بعدی مبدأ و مقصد واقعی نقل و انتقالات نیز ناشناخته باقی می‌ماند. بدین ترتیب، هزینه ارتکاب جرم کاهش می‌یابد و با کاهش خطر برای بزهکاران، امکان وقوع جرم در این بستر افزایش خواهد یافت.

1. Merchants

۳-۲-۲. سهولت شرکت در عملیات مجرمانه

بیت کوین، به عنوان شناخته شده ترین ارز مجازی، از فناوری شخص به شخص استفاده می کند که برای کار به هیچ نهاد مرکزی یا بانکی که معاملات را مدیریت کند، احتیاج ندارد و صدور آن به صورت جمعی توسط شبکه انجام می شود. بیت کوین منبع باز است؛ طراحی آن عمومی است: هیچ کس صاحب یا کنترل کننده بیت کوین نیست و همه می توانند با آن کار کنند. معاملات بیت کوین امن و برگشت ناپذیر است و اطلاعات حساس یا شخصی مشتری را ذخیره نمی کند. این کار بازرگانان را از خسارات ناشی از تقلب یا بازپرداخت های جعلی مصون می دارد. بازرگانان به راحتی می توانند به بازارهای جدیدی راه پیدا کنند که در آن ها یا کارت های اعتباری در دسترس نیستند یا نرخ تقلب به طور نامقبولی بالاست. نتایج این سهولت در استفاده عبارت است از: کاهش هزینه تجارت، دسترسی به بازارهای بزرگتر و هزینه های اداری کمتر.

نتیجه دیگر این سهولت، امکان اتحاد فراملی برای ارتکاب جرم است. مجرمان سایبری می توانند در کشورهای مختلف زندگی کنند و یک تجارت مجرمانه را اداره کنند. اولبریچ در ایالات متحده زندگی می کرد، در حالی که کلارک، یک کانادایی تبار، ساکن تایلند بود. این فناوری می تواند در کشورهای مختلف واقع شود. شالون، یکی از فروشندگان بیت کوین، از زیرساخت شبکه رایانه ای، از جمله سرورهای واقع در مصر، جمهوری چک، آفریقای جنوبی، برزیل و دیگر مکان ها برای دسترسی غیرقانونی و سرقت اطلاعات استفاده می کرد (Kethineni & Cao & Dodge, 2018). مواردی وجود داشت که در آن ها درآمد حاصل از جرائم به کشورهای خارجی منتقل می شد. دانگل که با عنوان «XanaxKing» نیز شناخته می شود، از وسترن یونیون^۱ برای انتقال درآمدهای مجرمانه خود به چین استفاده کرد. در نمونه ای دیگر، شخصی به نام علی شگری امین، با استفاده از رسانه های اجتماعی مجازی، برای تأمین مالی داعش، از افراد درخواست بیت کوین می کرد (United States of America v. Ali Shukri Amin, 2015). مجرمان سایبری یکدیگر را به صورت برخط ملاقات می کنند. گرچه ممکن است جرائم در هر گوشه ای از جهان رخ دهد، این امر به خصیصه جهانی شدن جرایم در بستر فضای سایبر کمک می کند.

۱. Western Union: شرکت وسترن یونیون، ارائه دهنده خدمات مالی و ارتباطی است. حواله ارز، یکی از خدمات خوب و محبوب این شرکت است. از طریق این خدمت، اشخاص قادر هستند که ارز را از یک کشور به کشور دیگر برای فرد مشخصی حواله کنند.

نمونه دیگر گروه جرایم سایبری،^۱ «WEI» است که تحقیقات هشت ساله در خصوص آن، منجر به محکومیت ۱۶ نفر از اعضای آن به جهت نقش آن‌ها در طرح سرقت هویت جهانی یا برنامه فاجعه سایبری شد. اعضای گروه جرایم اینترنتی، در ابتدا از طریق وبسایت‌های اینترنتی «کارتینگ»^۲ که مخصوص قاچاق کارت اعتباری مسروقه و اطلاعات شخصی، حساب‌های ناشناس پیام‌رسان، حساب‌های ایمیل ناشناس و حساب‌های ارز مجازی ناشناس بود، ارتباط برقرار می‌کردند تا وجود و هدف شرکت مجرم را پنهان کنند و مانع از شناسایی خود توسط نهادهای امنیتی و نظارتی شوند و ناشناس بودن خود را حفظ کنند (FATF, 2015: 30).

مرکز کل عملیات شرکت WEI، یک شرکت نیویورکی مستقر در منهتن بود که به‌عنوان مبادله‌گر ارز مجازی عمل می‌کرد تا روش‌های پرداخت اینترنتی را که توسط شرکت‌های مجرمانه استفاده می‌شد، هماهنگ و تسهیل کند و درآمد گروه را پول‌شویی کند. WEI، به‌عنوان یکی از مبادله‌گران بسیار بزرگ ارز مجازی در ایالات متحده، در مجموع پانزده میلیون دلار در وب‌مانی^۳ و بیست میلیون دلار در ای‌گلد^۴ را برای گروه جرایم سایبری مورد مبادله قرار داد و از بانک‌ها و انتقال‌دهندگان پول برای انتقال مبالغ هنگفت پول استفاده کرد (FATF, 2015: 32). همچنین از طریق وبسایت‌های خود،^۵ اطلاعات و کمک‌های لازم را برای انتقال پول به‌طور ناشناس و با خودداری از رعایت الزامات گزارش‌دهی ارائه می‌داد.^۶ این شرکت مجرم، از فروشندگان، خریداران، ارائه‌دهندگان خدمات مرتبط با جرایم اینترنتی و سرمایه‌گذارانی تشکیل می‌شد که در کشورهای متعدد، از جمله اوکراین و سراسر اروپای شرقی تا ایالات متحده قرار دارند و با استفاده از سازوکار ارزهای مجازی در قلمروهای سیاسی مختلف، عملیات مجرمانه خود را به شکل گسترده‌ای پیگیری می‌کردند. فروشندگان تقریباً ۱۰۰,۰۰۰ شماره کارت اعتباری دزدیده‌شده و سایر اطلاعات شناسایی شخصی را از طریق اینترنت فروختند و بیشتر پرداخت‌ها را در ای‌گلد و وب‌مانی انجام می‌دادند. خریداران از شناسه‌های سرقتی

1. Western Express International
2. CARDING
3. WebMoney
4. E-Gold
5. Dengiforum.com and Paycard2000.com

۶. مالک شرکت WEI که ملیت اوکراینی دارد، در ماه فوریه سال ۲۰۱۳ در ایالت نیویورک آمریکا به جرم پول‌شویی، کلاهبرداری و تبانی محکوم شد. سه متهم دیگر این پرونده نیز بعد از محاکمه، در ژوئن ۲۰۱۳ محکوم شدند. این تحقیقات به‌صورت مشترک توسط دستگاه امنیتی ایالات متحده و دفتر دادستانی منطقه منهتن (نیویورک) انجام شد (FATF, 2015: 26).

برای ساخت کارت‌های اعتباری و خرید کالاهای گران‌قیمت استفاده می‌کردند و مرتکب جرایم دیگری مانند نگهداری از اموال مسروقه، کلاهبرداری، تولید حدود پنج میلیون دلار اعتبار کارت تخفیف و پول‌شویی و جابه‌جایی پول بیش از ۳۵ میلیون دلار از طریق حساب‌های مختلف شدند. بدین‌سان، استفاده از ارزشهای مجازی بیش از پیش به سهولت شرکت در عملیات مجرمانه کمک کرده و جایگزینی مطمئن برای نظام‌های مالی و سامانه‌های پرداخت سنتی شده است. پدیده‌ای که در عمل ارتکاب جرم را تسریع می‌کند و ریسک کشف آن را نیز کاهش می‌دهد.

۴-۲-۲. فقدان بازدارندگی

دیگر ویژگی مهم و جذاب برای ورود مجرمان به فضای مجازی جهت ارتکاب جرم، نبود بازدارندگی است. این امر از جنبه‌های مختلفی قابل تحلیل است. نخست آنکه احتمال ورود نهادهای مجری قانون به فضای مجازی، به‌ویژه در دارکنت که تحقیقات نشان می‌دهند ۵۷ درصد محتوای آن غیرقانونی است (Weimann, 2016)، نسبتاً کم است. جاده ابریشم به مدت چهار سال در دسترس بود؛ با این حال، نهادهای مجری قانون قابلیت ردیابی بزهکاران را در این فضا نداشتند. هرچند تعداد زیادی فروشنده مواد مخدر و فروشندگان غیرقانونی دیگر در جاده ابریشم فعالیت می‌کردند، احتمال شناسایی شدن آن‌ها، با وجود دستگیری بنیان‌گذار این بازار برخط مجرمانه، اندک بود. این امر تا حدود زیادی به ماهیت پویا و نفوذناپذیر سازوکار مراودات مالی در این فضا، خصوصاً استفاده از بیت‌کوین، برمی‌گردد.

دوم، از دیدگاه فرصت، قوانین و مقررات به‌خوبی به‌عنوان ابزارهایی در نظر گرفته می‌شوند که می‌توانند برای کنترل فرصت‌های جرم یقه سفیدی مورد استفاده قرار گیرند. باید به خاطر داشت که جرایم یقه سفیدی دارای ویژگی‌های خاصی هستند: دسترسی قانونی بزهکار به قربانی، جدایی فیزیکی و مکانی میان بزهکار و قربانی و صورت به‌ظاهر قانونی اعمال. این خصوصیات موجب استفاده از شگردهای جنایی خاص می‌شود؛ برای مثال فریب، سوءاستفاده از اعتماد، اخفاء و توطئه و تبانی. بعضی از جرایم یقه سفیدی به موازات رشد فناوری جدید به وجود می‌آیند؛ برای مثال، تا زمانی که اینترنت به‌وجود نیامده بود، خبری از کلاهبرداری اینترنتی نبود؛ به همین دلیل، قانون نیازمند انعطاف‌پذیری و قابلیت تطبیق به‌هنگام با فرصت‌های مجرمانه نوظهور است (ال. بنسون و اس. سیمپسون، ۱۳۹۱: ۲۸۰). در غیر این صورت، نظام قانونی بازدارندگی لازم جهت پیشگیری از ارتکاب جرم را نخواهد داشت. وضعیت قانونی بیت‌کوین و به‌طور کلی ارزشهای مجازی، هنوز یک

منطقه خاکستری به شمار می‌رود.^۱ اگرچه ممکن است بیت‌کوین قابلیت تبدیل به ارزهای سنتی، مانند دلار آمریکا یا یورو را داشته باشد، هنوز در بسیاری از کشورها به‌عنوان پول شناخته نشده است. بر این اساس، یکی از استدلال‌های اولبریچ در دفاع از خود در برابر اتهام به پول‌شویی، این بود که او در پول‌شویی دخالت نمی‌کند؛ زیرا معاملات در جاده ابریشم «معاملات مالی» نبودند. همچنین فیلا، صراف بیت‌کوین، استدلال کرد که رفتار وی انتقال غیرقانونی پول نقد نیست؛ زیرا بیت‌کوین پول نیست؛ بنابراین او فرستنده پول محسوب نمی‌شد (Kethineni, Cao, Dodge, 2018: 150).

سوم، ممانعت از ارتکاب جرایم اینترنتی بدون استفاده از شیوه‌های پیشرفته، دشوار است. دلایل کلیدی که به FBI کمک کرد تا متوجه شود DPR که به‌عنوان بنیان‌گذار جاده ابریشم شناخته می‌شد، شخصی با هویت واقعی راس اولبریچ است، یک آدرس ایمیل بود. وقتی اولبریچ به دنبال یک دستیار IT در اینترنت بود، به اشتباه، آدرس ایمیل شخصی خود را نوشت: «Rosulbricht@gmail.com» (Hout & Bingham, 2013). اگر اشتباه راس اولبریچ نبود، پلیس برای ردیابی و توقف فعالیت مجرمانه جاده ابریشم با مشکل مواجه می‌شد. علاوه بر اولبریچ، دیگر مجرمان بازار ابریشم نیز از طریق روش‌های سنتی یافت شدند؛ برای مثال، سدلر، فروشنده مواد مخدر، هنگام تحویل کنترل‌شده گرفتار شد و دلایل مجرمانه مربوط به کارل مارک در لپ‌تاپ اولبریچ یافت شدند. به‌طور کلی، پلیس برای تحقیق در زمینه جرایم سایبری ارتكابی برخوردار از فناوری بالا در جاده ابریشم، همچنان به روش‌های سنتی متکی بود که این خود دلیلی بر جذابیت بیشتر فضای مجازی برای بزهکاران است. این امر با توجه به ماهیت ارزهای مجازی معضل بزرگی را برای کنشگران نظام عدالت‌کیفری در سطح ملی و بین‌المللی ایجاد کرده است. بدین ترتیب کشف جرایم یقه‌سفیدی که به‌طور سنتی از رقم سیاه بزهکاری بالایی برخوردار است، به مراتب دشوارتر خواهد شد.

نتیجه

ارزهای مجازی نمونه نوین از تحولات فناوری هستند که به‌واسطه ویژگی‌های منحصر به فرد خود، کارکرد گسترده‌ای در وقوع جرایم دارند. این ویژگی‌ها افزون بر ایجاد برخی تحولات مفهومی، گستره وسیعی از جذابیت‌های مجرمانه را ایجاد کرده‌اند که بیش‌ازپیش کوچ مجرمان، به‌ویژه

۱. ارزهای مجازی در حوزه دستورالعمل اتحادیه اروپا درباره خدمات پرداخت (PSD) قرار نمی‌گیرد و از این رو برخلاف روش‌های سنتی پرداخت، هیچ‌گونه حمایتی از مصرف‌کننده در برابر کلاهبرداری ارائه نمی‌دهد. امنیت عملیاتی این روش‌های جدید پرداخت نیز تضمین نشده است (French Financial Intelligence Unit, 2014: 7).

مجرمان یقه سفید، به فضای مجازی را سرعت بخشیده است. امری که منجر به افزایش ریسک بزهکارانه ارزهای مجازی شده است و اقدام به اتخاذ یک سیاست جنایی مناسب را در برابر آن اجتناب ناپذیر کرده است. با وجود این، اتخاذ سیاست جنایی مناسب در این زمینه نیازمند پیش شرط‌هایی است که عدم تحقق آن، هر راهبردی را با شکست روبه‌رو می‌سازد.

نخست، تلاش جهت شناسایی فنی ارزهای مجازی و تدوین رژیم حقوقی متناسب با قابلیت‌های آن. قانون‌مندسازی فعالیت‌های پولی و مالی در بستر ارزهای مجازی از شدت زیرزمینی شدن فعالیت‌های مرتبط با این حوزه، به دلیل افزایش تمایل عموم به استفاده از آن، خواهد کاست. این مسئله به‌عنوان ضرورتی انکارناپذیر به دلیل دشواری در کشف جرایم ارتكابی به‌وسیله ارزهای مجازی، مدیریت این حوزه با ابزارهای قانونی را اجتناب‌ناپذیر کرده است. بدین‌سان، رویکردی انفعالی در قبال ارزهای مجازی نه تنها صحیح نیست، بلکه رویکردی مشکل‌زا محسوب می‌شود؛ مشابه آنچه تاکنون از سوی بانک مرکزی ایران اتخاذ شده است که ابتدا به استناد قابلیت استفاده از ارزهای مجازی در پول‌شویی و تأمین مالی تروریسم، هرگونه استفاده از آن‌ها در مراکز پولی و مالی کشور را ممنوع کرده است و سپس به‌موجب برخی مقررات در سطح هیئت‌دولت در خصوص بعضی حوزه‌های محدود مرتبط با ارزهای مجازی مقررگذاری شده است. این رویکرد منفعلانه و تلاش جهت محو نمودن صورت مسئله به‌جای ارائه یک پاسخ و راهکار مناسب، نه تنها مفید واقع نخواهد شد، بلکه پیامدهایی منفی از جمله زیرزمینی شدن فعالیت‌های این حوزه را در پی خواهد داشت. از این‌رو، به‌نظر می‌رسد بانک مرکزی ایران، در چرخشی آشکار، تلاش جهت منضبط کردن این قلمرو را با انتشار پیش‌نویس سند «الزامات و ضوابط فعالیت‌ها در حوزه رمزارزها در کشور» آغاز کرده است.

دوم، ترسیم چارچوب قانونی مناسب به‌منظور برقراری رویکرد ریسک‌مدار در برابر خطرات بزهکارانه ارزهای مجازی. بررسی رویکردهای فراملی در پاسخ‌دهی به ریسک ارزهای مجازی نشانگر پذیرش رویکرد ریسک‌مدار در چهارچوب برنامه‌های مقابله با پول‌شویی است. بر این اساس، کشورها تلاش می‌کنند ارزهای مجازی را تحت شمول قوانین پول‌شویی قرار دهند تا به کاهش مخاطرات مجرمانه این ارزها اقدام کنند. در این راستا، در ژوئن ۲۰۱۹، گروه ویژه اقدام مالی FATF، به‌عنوان تخصصی‌ترین نهاد فراملی در زمینه پیشگیری و مقابله با پول‌شویی، به روزآمد کردن دستورالعمل^۱ خود درباره رویکرد ریسک‌مدار در برابر دارایی مجازی و ارائه‌دهندگان

۱. این سند، سند روزآمد شده سند سال ۲۰۱۵ با عنوان رویکرد ریسک‌مدار FATF به ارزهای مجازی است. نک:

خدمات مربوط به آن پرداخت. دستورالعمل روزآمد شده تلاش می‌کند تا نخست، درک صحیحی در خصوص مقررات‌گذاری و پاسخ‌گذاری‌های نظارتی در خصوص ارزشهای مجازی و ارائه‌دهندگان خدمات مربوط به آن در میان مقامات ملی ایجاد کند و دوم، اشخاص خصوصی که تمایل به ورود در این حوزه‌ها را دارند، با الزامات مربوط به مبارزه با پول‌شویی و تأمین مالی تروریسم و چگونگی اعمال مؤثر این الزامات در این زمینه آشنا کند. از این رو به نظر می‌رسد پس از شناسایی قانونی ارزشهای مجازی، پیش‌شرط دوم جهت اتخاذ سیاست جنایی مناسب در برابر ارزشهای مجازی این است که این ارزشها را تحت پوشش مقررات پول‌شویی قرار دهیم. امری که با توجه به ظرفیت‌های جدید قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷ و آیین‌نامه اجرایی مصوب ۱۳۹۸ قانون مزبور در پهنه نظام تقنینی ایران، پس از روشن شدن وضعیت حقوقی ارزشهای مجازی، قابل اعمال است.

استفاده از ارزشهای مجازی به‌طور قطع در جوامع پولی و مالی مقبولیت بیشتری قرار خواهد داشت. در آینده، انتظار می‌رود به دلیل عوامل متعددی، از جمله افزایش پذیرش پرداخت‌های بیت‌کوین توسط شرکت‌های بزرگ، ارزش بیت‌کوین، به‌عنوان محبوب‌ترین و شناخته‌شده‌ترین ارز مجازی افزایش یابد. افزون بر این، به دلیل هزینه‌های انتقال پول بین‌المللی، انتظار می‌رود در سال‌های پیش‌رو، استفاده از این ارز مجازی هم در خاورمیانه و هم در آفریقا رشد یابد. به همین دلیل رویکرد منفعلانه در خصوص این فناوری نوین از پیش محکوم به شکست است و کشورها باید با پذیرش آن، همسو با جدیدترین تحولات بین‌المللی، رویکردهای مناسبی در این زمینه اتخاذ نمایند تا افزون بر کاهش مخاطرات احتمالی، به‌طور تام از ظرفیت‌های مثبت این فناوری روبه‌رشد استفاده کنند.

منابع

فارسی

- ابوذری، مهنوش (۱۳۹۵)، *جرم‌شناسی جرایم سایبری*، چاپ نخست، تهران: انتشارات میزان.
- ال. بنسون، مایکل، اس. سیمپسون، سالی (۱۳۹۱)، *جرایم یقه سفیدی؛ رویکردی فرصت‌مدار*، برگردان اسمعیل رحیمی‌نژاد، چاپ نخست، تهران: انتشارات میزان.
- اس. سیمپسون، سالی، ویزبرد، دیوید (۱۳۹۲)، *جرم‌شناسی جرایم یقه سفیدان*، برگردان حمیدرضا دانش ناری، آزاده صادقی، تهران: انتشارات مجد.
- برناردی، الکساندر (۱۳۹۲)، *اروپایی شدن علوم کیفری*، ترجمه محمود روح‌الامینی، *دایره المعارف علوم جنایی*، زیر نظر علی حسین نجفی ابرندآبادی، کتاب دوم، چاپ نخست، تهران: انتشارات میزان.
- خلیلی پاجی، عارف (۱۳۹۸)، *امکان‌سنجی تأمین مالی تروریسم در پرتو ارزش‌های مجازی*، *مجموعه مقالات همایش بین‌المللی ابعاد حقوقی-جرم‌شناختی تروریسم*، چاپ اول، تهران: انتشارات دانشگاهی علامه طباطبایی.
- دولاکوآستا، خوزه لوییس (۱۳۹۶)، *سیاست جنایی اروپا: نمونه‌ای از بین‌المللی شدن حقوق کیفری در سطح منطقه‌ای*، ترجمه علی حسین نجفی ابرندآبادی، *مجموعه مقالات نکوداشت‌نامه استاد دکتر محمد آشوری*، چاپ هفتم، تهران: انتشارات سمت.
- طهماسبی، جواد؛ شاهمرادی، خیرالله (۱۳۹۷)، «چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری، *مجله حقوقی دادگستری*، دوره ۸۲، شماره ۱۰۴.
- محسنی، فرید (۱۳۹۱)، «جرانم شرکتی از دیدگاه جرم‌شناختی»، *دیدگاه‌های حقوق قضایی*، شماره ۵۷.
- نجفی ابرندآبادی، علی حسین (۱۳۸۵)، «تحلیل جرم‌شناختی جرایم اقتصادی»، *تعالی حقوق*، سال اول، شماره.
- نجفی ابرندآبادی، علی حسین (۱۳۹۱)، *تقریرات جرم‌شناسی (جهانی شدن جرم)*، دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه مفید. قابل دسترس در: www.lawtest.ir
- نجفی ابرندآبادی، علی حسین (۱۳۸۸)، «جرم‌شناسی در فضای سایبر»، *تعالی حقوق*، سال چهارم، شماره ۳۶.
- نجفی ابرندآبادی، علی حسین (۱۳۹۶)، *جنایات بین‌المللی و جرم‌شناسی*، دیباچه در: نیکوکار، حمیدرضا «به کوشش»، *جرم‌شناسی فراملی؛ به سوی جرم‌شناسی جنایات بین‌المللی*، چاپ اول، تهران: انتشارات میزان.
- نجفی ابرندآبادی، علی حسین (۱۳۹۴)، *جهانی شدن بزهکاری*، دیباچه در: ذاقلی، عباس، *قاجاق انسان در سیاست جنایی ایران و اسناد بین‌المللی*، تهران: انتشارات میزان.
- نجفی ابرندآبادی، علی حسین (۱۳۹۵)، *جهانی شدن حقوق کیفری و تعاملات دانشگاهی بین‌المللی*، دیباچه در: رضوی فرد، بهزاد «به کوشش»، *جلوه‌هایی از حقوق کیفری فرانسه-مجموعه مقالات و سخنرانی‌های همیشه مسه و برنادت زیبر*، چاپ اول، تهران: انتشارات دانشگاه علامه طباطبایی.
- نجفی ابرندآبادی، علی حسین و هاشم‌بیکی، حمید (۱۳۹۵)، *دانشنامه جرم‌شناسی*، چاپ چهارم، تهران: انتشارات گنج دانش.

انگلیسی

- Afilipoaie, A., & Shortis, P. (2015), *From dealer to doorstep-how drugs are sold on the dark net*. Global Drug Policy Observatory situation analysis. Retrieved November 15, 2015, from: <http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf>
- Bitcoin.org, <https://bitcoin.org/en/> accessed February 14, 2016.
- Brightman, H. J. (2009), **Today White Collar Crime: legal**, *Investigation Journal of Police Science & Management*, 9 (4):336.
- Christin, N. (2013), **Traveling the silk road: A measurement analysis of large anonymous online marketplace**, *22nd International World Wide Web Conference* (pp.213–224). Rio de Janeiro: Brazil. doi:10.1145/2488388.2488408.
- Crawford, Angus. (2014) Dark net ‘used by tens of thousands of paedophiles’, *BBC News*, June 19.
- Edelhertz, Herbert. (1970), **The Nature, Impact and Prosecution of White-Collar Crime**, Washington, D.C.: U.S. Dept. of Justice, National Institute of Justice.
- Egan, Matt. (2017), “**What is the Dark Web?**” *pcadvisor.com*, June 19.
- FATF. (2015), **VIRTUAL CURRENCIES, GUIDANCE FOR A RISK-BASED APPROACH**.
- French Financial Intelligence Unit. (2014). **REGULATING VIRTUAL CURRENCIES**, Virtual Currencies Working Group.
- Hout, M. C. V., & Bingham, T. (2013), **BSurfing the silk road: A study of users’ experiences**, *International Journal of Drug Policy*, 24 (6):524–529.
- J. Mounteney, A. Bo and A. Oteo. (2017), **EMCDDA project group**, “The Internet and Drug Markets” *European Monitoring Centre for Drugs and Drug Addiction*, 2016, accessed June 19, 2017.
- Kethineni, Sessa, Cao, Ying, Dodge, Cassandra. (2018), **Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes**, *American Journal of Criminal Justice*, 43 (2):141–157.
- Lane, J. (2014), **Bitcoin, silk road, and the need for a new approach to virtual currency regulation**, *Charleston Law Review*, 8, 511–535 Retrieved October 10, 2015, from: <http://heinonline.org/HOL/LandingPage?handle=hein.journals/charlwrev8&div=25&id=&page=>.
- Nycum, Susan, Parker, Donn B (1989), **Computer Crime: Criminal Justice Resource Manual**, U.S. Department of Justice, National Institute of Justice, Office of Justice Programs.
- Reid, Alan S (2018), **Financial Crime in the Twenty-First Century: The Rise of the Virtual Collar Criminal, White Collar Crime and Risk**, Palgrave Macmillan, London.
- Reiss, Albert J. and Biderman, Albert D (1981), **Data Sources on White-Collar Law Breaking**, Washington, D.C.: U.S. Dept. of Justice, National Institute of Justice.

- Rotman, Edgardo (2001), **The Globalization of Criminal violence**, *Cornell Journal of Law and Public Policy*, No 49.
- Salifu, A (2008), **The Impact of Internet Crime on Development**, *Journal of Financial Crime*, 15 (4): 435.
- Spalevic, Zaklina and Ilic, Milos. (2017), "The use of the dark web for the purpose of illegal activity spreading," from:
<https://www.ekonomika.org.rs/en/PDF/ekonomika/2017/clanci17-1/7.pdf>
- Shapiro, Susan P. (1990), Collaring the Crime, Not the Criminal: Reconsidering the Concept of White-Collar Crime, *American Sociological Review*. 55:346-65.
- Tor Browser in Numbers, **The Tor Project**. (2017), from:
<https://blog.torproject.org/blog/tor-browser-numbers>, accessed June 7.
- United States of America v. Ali Shukri Amin (2015, June 11), **Plea agreement**, 1 16. Retrieved November 9, 2016, from:
<https://www.justice.gov/opa/file/477366/download>
- Wechsler, P (2016), "Dark web" gives cover to criminals, Issue: Cyber Security Retrieved October 10, 2016, from:
<http://businessresearcher.sagepub.com/sbr-1775-98146-2715485>.
- Weimann, G (2016), **Terrorist migration to the dark web**, *Perspectives on Terrorism*, 10 (3), 40-44.

