شناسهٔ دیجیتال (DOI): 10.22106/JLJ.2020.119555.3095

مجله حقوقی دادگستری

مقالهٔ پژوهشی، دورهٔ ۸۴، شمارهٔ ۱۱۰، تابستان ۱۳۹۹، صفحات ۶۵ الی ۹۶
تاریخ دریافت: ۱۳۹۸/۱۰/۱۳ - تاریخ پذیرش: ۱۳۹۸/۱۲/۱۶

مجازی‌شدن بزهکاری یقه‌سفیدی در پرتو ارزهای مجازی[1]

باقر شاملو*، عارف خلیلی‌پاجی**

چکیده

در جهان امروز فناوری با سرعت شگرفی درحال پیشرفت است. بزهکاران این موقعیتِ فرصت‌ساز 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، بسترساز ارتکاب جرایمی نو نیز شده که با گسترش محیط مجرمانه به فراتر از مرزهای‌جغرافیایی یک کشور، فرایند جهانی‌شدن بزهکاری را تسریع کرده است. ابداع ارزهای‌مجازی به فرایند مزبور سرعت بخشیده است. ارزهای‌مجازی با ادعای هم‌ردیف قرارگرفتن با ارزهایِ متعارف (دولتی)، در تلاش‌اند تا تابوهای سنتیِ 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 یقه‌سفیدی یا بزهکاری یقه‌سفیدان 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 یقه‌مجازی‌ها» یاد می‌کنند. بدین‌سان، این پژوهش با روشی توصیفی و تحلیلی، پس از بررسی ابعاد بزهکاری یقه‌سفیدیِ مجازی یا بزهکاری یقه‌مجازی‌ها، به تحلیل چرایی تمایل بزهکاران مجازی به استفاده از ارزهای مجازی در ارتکاب بزهکاری با توجه به برخی پرونده‌های کیفری خواهد پرداخت.

واژگان کلیدی: ارزهای‌مجازی، بزهکاری، یقه‌سفیدها، یقه‌مجازی‌ها، جهانی‌شدن

۱. این مقاله برگرفته از رسالهٔ دورهٔ دکتری تخصصی نویسندهٔ مسئول تحت عنوان «تأثیر ارزهای مجازی بر جهانی‌شدن بزهکاری» با راهنمایی آقایان دکتر باقر شاملو و دکتر علی‌حسین نجفی‌ابرندآبادی و مشاورهٔ آقایان دکتر امیرحسن نیازپور و دکتر مهدی صبوری‌پور در دانشگاه شهید بهشتی است.

* دانشیار گروه حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران
baghershamloo@gmail.com

** دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران (نویسندهٔ مسئول)
a_khalilipaji@sbu.ac.ir

مقدمه

آغاز هزارهٔ سوم را می‌توان شروع تغییر رویکردهای جرم‌شناسی به فضای مجازی دانست. تغییرات ایجادشده به‌واسطهٔ توسعه و گسترش فضای مجازی، اینترنت و اشکال پیچیدهٔ ارتباطات با محصول جانبی آن، یعنی جرم، همراه شد. این امر از چند بُعد قابل توجه است. فضای مجازی در فرایند جهانی‌شدنِ بزهکاری به‌شدت و گسترهٔ آن افزوده است. جهانی‌شدن یکی از فراگیرترین فرایندها و تحولات در جامعهٔ معاصر است که به‌عنوان پدیده‌ای چندبُعدی، آبستن مباحثِ گسترده در ارتباط با ماهیت، ریشه‌های تاریخی و تأثیر آن بر جوامع شده است. دامنهٔ مطالعات و تحقیقات رشته‌هایِ تخصصی علوم جنایی نیز از این تحولات مصون نمانده و با گسترش فرایند جهانی‌شدن در حوزه‌های مختلف، مانند اقتصاد، فرهنگ، حقوق بشر و سیاست، به حوزهٔ بزهکاری نیز تسری پیدا کرده است؛ به‌عبارت دیگر، امروزه با جهانی‌شدن اقتصاد، فرهنگ، سیاست و حقوق بشر و به‌دنبال آن، کمرنگ‌شدن مرزهای سیاسی میان کشورها، شاهد جهانی‌شدن بعضی مظاهر بزهکاریِ مالی و اقتصادی هستیم که توسط مرتکبان چندملیتی به‌طور سازمان‌یافته یا در قالب گروه‌های جنایی ساختارمند ارتکاب می‌یابند (نک: نجفی‌ابرندآبادی، ۱۳۹۵: ۱۳-۵).

تحول مفهومی و موضوعیِ بزهکاری در پرتو فضای مجازی و آثار آن، اتفاق مهمی در جرم‌شناسی و حقوق‌کیفری است. بر این اساس، افزون بر اینکه فضای مجازی مفهوم برخی جرایم را تغییر داده، به مصادیق آن‌ها نیز افزوده است. نمونهٔ بارز تأثیر فضای مجازی بر جهانی‌شدن و تغییر مفهومی و موضوعی جرم را می‌توان در گسترش جرایم یقه‌سفیدها مشاهده کرد. جرایم یقه‌سفیدی، به تعبیر ساترلند[1] جرایم ارتکاب‌یافته به‌وسیلهٔ افراد محترم و متعلق به‌طبقهٔ بالای جامعه، با گسترش جهانی‌شدن 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 فراهم‌ساختن زمینه و فرصت پیدایش جرایمی نوین و وسایل جدید ارتکاب جرایم متعارف، فرایند جهانی‌شدن بزهکاری تزویرآمیز را نیز تسریع کرده و به آن شدت بخشیده است؛[2] به‌طوری که برخی سخن از مجرمان «یقه‌مجازی»،[3] به‌عنوان گونه‌ای از جرایم یقه‌سفیدی به میان می‌آورند (Reid,

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

۲. جهت مطالعهٔ فضای سایبر به‌عنوان محیطی اجتماعی؛ (نک: نجفی‌ابرندآبادی، ۱۳۸۸: ۵۲-۵۰).

3. Virtual Collar Criminal

2018).[1] از جمله زمینه‌های گسترش این امر، ابداع و به‌کارگیری ارزهای‌مجازی[2] است که امروزه نیز با سرعت زیادی درحال افزایش است.

زمانی که ارزهای مجازی غیرمتمرکز، به‌ویژه بیت‌کوین[3]، 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، به‌دلیل ویژگی‌هایی منحصربه‌فرد، بسیار فراگیر خواهند شد؛ دیدگاه دوم اما، با نگاهی بدبینانه به ارزهای‌مجازی به‌عنوان یک ابزار قدرتمند نوین در اختیار بزهکاران، تأمین‌کنندگان مالی تروریسم و اشخاص یا کشورهای تحت تحریم، برای دورزدن تحریم‌ها، جابه‌جایی، ذخیرهٔ منابع مالی و فرار مالیاتی توجه کرده است (FATF, 2015: 27). دیدگاه اخیر بر این نظر است که دسترسی‌جهانی به ارزهای مجازی، زمینهٔ افزایش جرایم یقه‌سفیدی، به‌خصوص پول‌شویی[4]، را فراهم می‌کند؛ زیرا سامانهٔ ارز مجازی می‌تواند از طریق اینترنت و با ابزارهایی، از جمله تلفن‌های همراه، حتی در پرداخت‌های برون‌مرزی در دسترس باشند. افزون بر این، ارزهای‌مجازی 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 ارائهٔ خدمات و درگیربودن 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: خلیلی‌پاجی، ۱۳۹۸: ۱۳۴-۱۱۳). وجود سوابق مشتری و معاملات او در کشورهای مختلف، دسترسی به این اطلاعات را توسط کنشگران نظام عدالت‌کیفری مشکل‌تر می‌سازد. این مشکل به‌دلیل ماهیت به‌سرعت درحال تحولِ فناوری ارز مجازی غیرمتمرکز و مدل‌های کسب‌وکار، از جمله تغییر تعداد و نوع یا نقش مشارکت‌کنندگان در ارائهٔ خدمات در سامانه‌های پرداخت ارز مجازی، تشدید می‌شود. مشکل مهم‌تر اینکه، ممکن است اجزای سامانه یا اشخاص استفاده‌کننده از ارز مجازی در کشورهایی قرار گیرند که وضعیت مبارزه با پول‌شویی در آن‌ها نامناسب است. بدین‌ترتیب، 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 حوزهٔ مبارزه با پول‌شویی و از سوی دیگر، وجود خطر احتمالی در سامانهٔ پرداخت اینترنتی با ابزار ارزهای مجازی و افزایش ریسک جرایم مزبور، از اهمیت بسیاری برخوردار شده است. امری که ضرورت انجام پژوهش‌های دقیق از مخاطرات ارزهای مجازی را اجتناب‌ناپذیر کرده است.

بر این اساس، در بررسی حقوقی و جرم‌شناختی ارزهای 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 ارزهای مجازی به‌طور خاص، از حیث مفهومی متحول شده است و این دسته از بزهکاران با توجه به ویژگی‌های ارزهای مجازی بیش‌ازپیش تمایل به تمرکز رفتارهای بزهکارانهٔ خود در فضایی مجازی دارند که این مسئله، ترسیم چارچوب نظری خاص جرایم یقه‌مجازی‌ها را به‌عنوان گونه‌ای از جرایم یقه‌سفیدی ضروری کرده است.

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

۱. از جرایم یقه‌سفیدها تا جرایم یقه‌مجازی‌ها

در قرن بیست‌ویکم، افراد، شرکت‌ها و دولت‌ها به‌طور فزاینده‌ای در معرض بزه‌دیدگی جرایم مالی قرار دارند. افزایش جرایم یقه‌سفیدها، به‌طور گسترده‌ای، زمینهٔ وابستگی جوامع مدرن به سامانه‌های ارتباطی برخط جهت کنترل، نظارت و ارائهٔ 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 پدیدهٔ 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 به‌صورت ناشناس یا حداقل نیمه‌ناشناس، انجام می‌شود. بدین‌ترتیب، عاملان این جرایم یقه‌سفیدی می‌توانند در بستر این فضا مخفی بمانند و به ارتکاب جرایم غافل‌گیرانه بپردازند. بنابراین، فضای مجازی منجر به ایجاد یک پدیدهٔ نوین شده است که می‌توان آن را «جرایم یقه‌مجازی‌ها» نامید.

بر این اساس جهت بررسی تأثیر ارزهای‌مجازی بر جرایم یقه‌مجازی‌ها، ابتدا شناخت مفهوم جرایم یقه‌مجازی‌ها ضروت دارد؛ زیرا ماهیت مجازی این ارزها، آن‌ها را به ابزاری منحصربه‌فرد در این فضا و در خدمت بزهکاران مجازی تبدیل کرده است.

به‌لحاظ نظری، جرایم یقه‌مجازی‌ها مبتنی بر دو تحول است: نخست، تحول در مفهوم جرم یقه‌سفیدها، از رویکرد مجرم‌مدار به‌رویکرد جرم‌مدار؛ دوم، تحول ایجادشده توسط فضای مجازی در مورد این جرم. مورد اخیر افزون بر گسترش دامنهٔ ارتکاب به‌واسطهٔ جهانی‌شدن، در تغییر مفهومی جرم یقه‌سفیدی و ایجاد تعادل بین بزهکار و بزه‌دیده نیز مؤثر بوده است.

۱-۱. رویکرد جرم‌مدار به جرایم یقه‌سفیدی

تعریف ساترلند از جرم یقه‌سفیدی، به‌عنوان مبدع مفهوم جرایم یقه‌سفیدها، نمونهٔ بارزی از تعریف مجرم‌مدار[1] در خصوص این جرایم است. تعریف‌های مجرم‌مدار با تمرکز بر روی مجرم، موقعیت عالی اجتماعی و محترم‌بودن شخص مرتکب را ویژگی‌های اساسی جرم یقه‌سفیدی بیان می‌کنند. برخی اندیشمندان هم‌سو با تعریف ساترلند، جرم یقه‌سفیدی را بازتعریف کردند که در عمل موجب شفاف‌شدن تعریف ساترلند شده است. این دسته معتقدند که «جرایم یقه‌سفیدی به آن نوع اعمال خلاف قانون دارای ضمانت‌اجرای کیفری گفته می‌شود که متضمن سوءاستفادهٔ مرتکب آن‌ها از موقعیت مهم قدرت، نفوذ یا اعتماد در یک نظام سازمانی یا اقتصادی مشروع، به‌منظور کسب درآمدهای نامشروع برای خود یا سازمانی است (Reiss & Biderman, 1981: 15). این تعریف نیز مانند تعریف ساترلند، بر خصوصیات اجتماعی مرتکب جرم یقه‌سفیدی تأکید دارد و جرایمی را شامل می‌شود که با حرفهٔ شغلیِ مرتکب مرتبط باشند.

در مقابل، برخی با اتخاذ رویکرد جرم‌مدار[2]، 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 حیله و تزویر، با هدف تحصیل پول یا مال یا عدم پرداخت وجه یا خسارت یا تحصیل امتیاز شغلی یا شخصی

1. Offender-Based Approach
2. Offence-Based Approach

ارتکاب می‌یابد» (Edelhertz, 1970: 18). این رویکرد، بزهکاری یقه‌سفیدی را بر اساس ابزار ارتکاب جرم، به‌خصوص ابزار غیرفیزیکی که شامل اختفا، کتمان، حیله 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 به‌موقعیت یا قابلیت احترام مرتکب، گسترهٔ 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 اجتماعیِ رسمی بالایی نباشد.[۱]

برایتمن هم‌سو با رویکرد جرم‌مدار در تعریف جرایم یقه‌سفیدی با اعتقاد به اینکه عبارت جرم یقه‌سفیدها باید قلمرو گسترده‌تری را دربرگیرد، هر اقدام غیرخشونت‌آمیز با انگیزهٔ 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 خریدوفروش اوراق سهام اشاره کرد که اگرچه در ابتدا در انحصار طبقهٔ بالای جامعه بود، دسترسی به فناوری‌های رایانه‌ای، امروزه اجازهٔ فعالیت به تمامی افراد در این زمینه را می‌دهد (ابوذری، ۱۳۹۵: ۳۷). سالیفو ضمن تأیید اندیشهٔ برایتمن تأکید می‌کند که دلیل یا انگیزهٔ 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 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 دستهٔ این جرایم، از طرق غیرخشونت‌آمیز و توسط افراد محترم جامعه که سابقهٔ کیفری ندارند، ارتکاب می‌یابند و دیدگاه جامعه بدین‌گونه است که به آن‌ها اهمیت کمتری نسبت به جرایم

۱. 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).

خشونت‌آمیز می‌دهد (Nycum, Parker, 1989: 78). بدین‌ترتیب، توسعهٔ رویکرد جرم‌مدار و گسترش دامنهٔ آن به فضای مجازی، موجب تحول مفهومی جرایم یقه‌سفیدها شده است.

۲-۱. تحول جرایم یقه‌سفیدی در پرتو فضای مجازی

از منظر ساترلند، ویژگی‌های جرایم یقه‌سفیدها، از ماهیت مرتکبان این‌گونه جرایم نشأت می‌گرفت (Reid, 2018: 232). همان طور 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، پدیدهٔ اینترنت و استفاده از آن در سطح جهانی، حیات جدیدی را به‌جسم 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 دایرهٔ ارتکاب این جرایم و تسریع پدیدهٔ «جهانی‌شدن جرایم یقه‌سفیدی»، هم‌سو با رویکرد جرم‌مدار، موجب تسریع در ایجاد «تعادل در قدرت و تغییر در مفهوم جرایم‌یقه‌سفیدی» شده است.

۱-۲-۱. جهانی‌شدن جرایم یقه‌سفیدها

جهانی‌شدن[۳] موجبات تغییر ماهیت جرایم، به‌خصوص جرایم اقتصادی و مالی را ایجاد کرده است. به‌گونه‌ای که «سازمان‌یافتگی»، «فرامرزی‌بودن» و «اتخاذ سازوکارهای پیچیده جهت

۱. البته درنحوهٔ تعریف این گروه از جرایم، همواره اختلاف‌نظر وجود داشته و مجموعهٔ 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 توسعهٔ مفهوم این جرایم به‌سوی فضای مجازی، همان طور که پیش‌تر آمد، نکتهٔ بسیار مهمی که در بیشتر تحقیقاتِ صورت‌گرفته در این حوزه مغفول مانده، تحولاتی است که فضای مجازی در جرایم یقه‌سفیدی ایجاد کرده است.

۳. جهانی‌شدن، اصطلاحی است چندبعدی که به همگونی فزایندهٔ نظام‌های ملی از جنبه‌های اقتصادی، فرهنگی و سیاسی اشاره دارد. افزایش تعاملات منطقه‌ای و جهانی میان دولت‌های مختلف، شرکت‌ها، سازمان‌ها و مؤسسات گوناگون، موجب شده است که آثار یک جرم ارتکابی محدود به مرزهای کشور محل وقوع نباشد (نک: دولاکواِستا، ۱۳۹۶: ۶۷۴ به‌بعد). ازاین‌رو، برخی جرایم ملی، جنبهٔ جهانی به خود گرفته‌اند یا جرایمی در شکل‌های نوین ظهور پیدا کرده‌اند که از آن‌ها تحت عنوان جرایم جهانی یاد می‌شود که به دو دستهٔ عمدهٔ جرایم با انگیزهٔ سودجویانه (اقتصادی) و جرایم خشونت‌آمیز (تروریستی)، تقسیم می‌شوند (نک: نجفی‌ابرندآبادی، ۱۳۹۱: ۴۷-۳۹ و برناردی، ۱۳۹۲: ۱۸۳-۱۶۵).

ارتکاب» از جمله ویژگی‌های مهم این دسته از جرایم است. از نظر ویژگی‌های ساختاری، بزهِ جهانی بیشتر اوقات با مشخصاتی همچون عدم‌تمرکز، انعطاف‌پذیری، قابلیت انطباق، به‌کارگیری فناوری‌های نوین و گستردگی شبکه توصیف می‌شوند (Rotman, 2001: 5). این امر یکی از نگرانی‌های فزایندهٔ دنیای معاصر است که جریان‌های جهانی پولی و اطلاعات و افراد، شرایط و فرصت‌های مناسبی را برای گسترش اشکال جدیدی از بزهکاری جهانی‌شده رقم بزنند.

نیل شاور از دریچهٔ جهانی‌شدن، بحثی کوتاه اما جالب در خصوص جرایم یقه‌سفیدی ارائه کرده است. وی معتقد است از یک سو، رشد نظام اقتصادی در جهان، فرصت‌های بی‌نظیری را برای جرایم یقه‌سفیدی 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 منحصربه‌فرد سرمایه، دست بزهکاران را در جست‌وجوی نظام‌های قضایی که در خصوص فعالیت‌های اقتصادی نامشروع حساس نیستند، باز می‌گذارد. در چنین شرایطی، شرکت‌های چندملیتی که از نظر امکانات و تجهیزات انسانی، مادی، فنی، فناورانه و نیروی انسانی ماهر و تعداد کارمندان با دولت‌های میزبان رقابت می‌کنند، در معرض ارتکاب برخی جرایم قرار می‌گیرند (نجفی‌ابرندآبادی، ۱۳۹۶: ۱۷). افزون‌بر این، جهانی‌شدنِ مبادلات مالی به‌واسطهٔ ابزارهای خاص موجود در این حوزه نیز گسترش جرایم یقه‌سفیدی را در پی داشته است. برخی ارزها، مانند دلار و یورو به‌عنوان ارزهای جهانی، ابزار تبادل سرمایه جهت گسترش مراودات مالی بین کشورها به‌صورت وسیلهٔ واحد جهانی درآمده‌اند و به بسیاری از محدودیت‌های موجود در مبادلات بین‌المللی پایان داده‌اند و موجب شده‌اند که این‌گونه از جرایم نیز با گسترش پدیدهٔ جهانی‌شدن، ابعاد فرامرزی یافته و از مرزهای داخلی کشورها فراتر رود. بی‌تردید در این زمینه نقش فضای مجازی و استفاده از بستر شبکهٔ اینترنت در گسترش جهانی‌شدن بزهکاری، به‌ویژه جرایم یقه‌سفیدها، انکارناپذیر است. جهانی‌شدن اقتصاد، تحت تأثیر فناوری‌های جدید اطلاعات و ارتباطات و عوامل سیاسی، سبب شده است که فرایند و سرنوشت تولید، توزیع، حمل‌ونقل و مصرف کالا و خدمات در نظام اقتصادی کشورها تا اندازهٔ زیادی در تعامل و مرتبط با یکدیگر متحول شوند (نجفی ابرندآبادی، ۱۳۹۴: ۱۳۹). این امر پدیدآورندهٔ فرصت‌های جرم‌زای نوینی شده است. جرایم، تابع فرصت‌ها هستند و جهانی‌شدن که به‌واسطهٔ توسعهٔ فناوری، شتاب بیشتری به خود گرفته، فرصت‌های فراوانی را برای انواع فعالیت‌های مجرمانه به وجود آورده است (اس.سیمپسون و ویزبرد، ۱۳۹۲: ۲۰۱).

گسترش فضای مجازی و ایجاد امکان انجام مبادلات مالی‌اقتصادی در بستر این فضا و زیستِ مالی‌اقتصادی مجازی، به جهانی‌شدن بزهکاری یقه‌سفیدی سرعت بخشیده است. استفاده از

فناوری موجود در فضای مجازی موجب می‌شود که بزهکار در پوشش فعالیتی مشروع، ظاهرشده و به‌طور ناشناس با هزینهٔ اندک و در سطح جهانی به فعالیت مجرمانه اقدام کرده یا از فناوری شبکهٔ اینترنت برای ایجاد شکل منسجمی از بزهکاری، در قالب سازمان‌های جنایی مجازی، اقدام کند. بدین‌ترتیب، فضای مجازی در افزایش دامنهٔ ارتکاب جرایم یقه‌سفیدی نیز تأثیر شگرفی داشته است. افزون‌بر این، فضای مجازی بر برتری بزهکاران یقه‌سفیدی بر بزه‌دیدگان آن نیز تأثیرگذار بوده و آن را به سوی تعادل نسبی سوق داده است.

۲-۲-۱. تعادل قدرت و تغییر مفهوم جرایم یقه‌سفیدها

به‌طور سنتی، مفهوم جرم یقه‌سفیدها برعدم 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. تاریخچهٔ جرایم سایبری به‌طور دقیق با این موضوع هم‌خوانی دارد؛ بزه‌دیدگان مجازی غالباً کم‌سن‌وسال یا مسن هستند و در زمینهٔ فناوری اطلاعات تازه‌کار محسوب می‌شوند و در نتیجه از مهارت کافی برای دفاع از خود در برابر تهدیدات برخط برخوردار نیستند یا کاربر فناوری‌های نوینی هستند که مهارت لازم برای استفاده از آن را ندارند و بزهکاران مجازی با استفاده از برخی برنامه‌های مخرب، مانند ویروس‌ها یا بدافزارهای رایانه‌ای، آن‌ها را قربانی قرار می‌دهند. این پارادایم در دههٔ دوم قرن بیست‌ویکم، دیگر صحیح نیست. قربانیان جرایم برخط جوان‌تر و بالغ‌تر شده‌اند؛ زیرا فناوری تبدیل به یک واقعیت فراگیر در زندگی شده است؛ قربانیان به‌دلیل گسترهٔ فعالیت‌هایی که در فضای سایبر دارند، بومیان دیجیتال تلقی می‌شوند که با وجود برخورداری از هوش غالباً سرشار، از آمادگی و مهارت کافی برای زیست در محیط دیجیتالی برخوردار نیستند. نرم‌افزارهای مخرب و ویروس‌های رایانه‌ای، دیگر صرفاً به‌صورت برخط نیستند و کدهای نرم‌افزارها به‌حدی پیچیده شده‌اند که از دایرهٔ اشراف متخصصان رایانه‌ای نیز خارج‌اند؛ امکان تهیهٔ انواع برنامه‌های کاربردی، از جمله برنامه‌هایی که جهت اهداف مجرمانه تولید شده و مورد استفاده قرار می‌گیرند، از طریق فروشگاه‌های برخط وجود دارد (Reid, 2018: 236). بدین‌ترتیب، بزهکاران نیازی به تحصیل در رشتهٔ علوم رایانه‌ای ندارند تا بتوانند نرم‌افزارهای کاربردی خود برای ارتکاب جرم را ایجاد و اجرا کنند. به‌طور خلاصه، عدم تعادل قدرت بین بزه‌دیدگان و بزهکاران، به‌میزان درخور توجهی کاهش یافته است. این پدیده به‌عنوان «جرم، همچون یک خدمت»[1] شناخته شده است.

1. Crime as a Service

بنابراین، درحال‌حاضر، طبیعی است که مهارت‌های ویژهٔ لازم برای ارتکاب جرم در فضای مجازی توسط بزهکاران سطوح پایین‌تر کسب شود؛ یعنی کسانی که به‌طور سنتی به‌عنوان بزهکاران یقه‌آبی معرفی می‌شوند. جرایم یقه‌آبی‌ها به‌عنوان جرایم خیابانی شناخته شده است که اغلب توسط اشخاص کم‌مهارت به وقوع می‌پیوندد و شامل تعرض‌ها و تهدیدهای فیزیکی می‌شود که کاملاً محسوس و تأثیرگذار است. این‌گونه بزهکاری، به‌دلیل ویژگی جسمانی آن، به‌طور مستقیم برکیفیت زندگی اشخاص تأثیر می‌گذارد؛ ازاین‌رو، جامعه تمایل بیشتری دارد جهت مقابله با این جرایم با صرف منابع موجود اقدام کند. درمقابل، جرم یقه‌سفیدها، 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 دامنهٔ ارتکاب و تعداد مرتکبین جرایم یقه‌سفیدها، معضل پیش‌روی جوامع است؛ به‌طوری که طیف وسیعی از افراد کم‌مهارت یا بی‌مهارت و گروه‌های سازمان‌یافتهٔ مجرمانه می‌توانند این جرایم را مرتکب شوند (Reid, 2018: 237). این امر، هم‌سو با رویکرد جرم‌مدارِ جرایم یقه‌سفیدی، گذار از تمرکز برمجرم (به‌عنوان فردی از طبقهٔ بالا یا پایین جامعه) به‌سوی درک عمل مجرمانه، نقش فرایندها و ویژگی‌های عمل ارتکابی است که باید در راستای توسعهٔ مفهومی جرایم یقه‌سفیدی بررسی شود. بر این اساس، به‌واسطهٔ فضای مجازی و شکل‌گیری مراودات اقتصادی در این بستر، از سویی، بزهکاران یقه‌سفید، برخلاف تعابیر سنتی از این‌گونه جرایم، در عمل و به‌طور غالب، بزهکارانی با هوش فراوان تلقی نخواهند شد و از سوی دیگر، بزه‌دیدگان جرایم یقه‌سفیدی نیز نسبت به سایر بزهکاران کم‌هوش‌تر نیستند. در واقع فضای مجازی با ارائهٔ امکانات منحصربه‌فرد 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 قانونیِ دارای پشتوانهٔ دولتی، گونه‌ای جدید از ارزها با ویژگی‌های منحصربه‌فرد تولید شده‌اند و به‌واسطهٔ فرایند جهانی‌شدن با سرعتی شگفت‌انگیز درحال 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 محیط‌های‌مجازی 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 مبادلهٔ مجازی با ارز مجازی به‌عنوان وسیلهٔ پرداخت

به دست آورد. ایجاد، عرضه و گسترش این‌گونه ارزها، با تمام مزایای منحصربه‌فردی که دارد، می‌تواند زمینه‌ساز یا تسهیل‌کنندهٔ ارتکاب جرایم یقه‌سفیدی در بعد جهانی باشد و بیش‌ازپیش 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 نحوهٔ ارتکاب جرم در پرتو جهانی‌شدن، 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 به‌مثابهٔ یک خدمت در بستر فضای سایبر قابل‌عرضه کرده است.

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

معروف‌ترین ارزمجازی، بیت‌کوین است. بیت‌کوین یک سامانهٔ رایانه‌ای عمومی است که امکان پرداخت غیرمتمرکز و شخص‌به‌شخص (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 دخل‌وتصرف کند، فعالیت می‌کند. در اوت سال ۲۰۰۸ دامنهٔ پایگاه Bitcoin.org در شبکهٔ اینترنت ثبت شد و تا به امروز نیز مشخص نیست که چه‌کسی این دامنه را به ثبت رسانده است. در اکتبر سال ۲۰۰۸ فردی به نام «ساتوشی ناکاماتو» در خبرنامهٔ رمزگذاری‌شده‌ای به نام metzdowd.com اعلام کرد: «من در حال کار بر روی سامانهٔ پول الکترونیکی جدیدی هستم که کاملاً شخص‌به‌شخص و بدون دخالت شخص ثالث است.» مقالهٔ مذکور سرمنشأ این پول مجازی، یعنی بیت‌کوین بوده و معروف به مقالهٔ سفید با عنوان «بیت‌کوین: سامانهٔ پولی الکترونیک شخص‌به‌شخص» است.

پرسش مهم این است که چه عواملی سبب جلب نظر بزهکاران یقه‌سفید 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 یقه‌سفیدی 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 مالیِ فراملی بی‌شمار و پیچیده تحقق پذیرد. امروزه، نظام بین‌المللی نقل‌وانتقالِ وجوه و رمزگشایی از کارت‌های اعتباری، انتقالِ پول را با سرعت نور ممکن ساخته که همین امر موجب تحول زمانی و مکانی پول‌شویی نیز شده است.

بدین‌سان، نیاز به طُرق 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 مجازی‌شدن جرایم یقه‌سفیدی شده است. موضوعی که در بررسی پرونده‌های کیفری در ارتباط با ارزهای‌مجازی، به‌ویژه پروندهٔ جاده ابرایشم[1]، به‌وضوح مشاهده می‌شود. در سازوکار این سامانهٔ فروش برخط، به‌طور آشکار می‌توان مشاهده کرد که فناوری به خدمت بزهکاری درآمده است. جادهٔ ابریشم با قرارگرفتن بر لایهٔ پنهان اینترنت، یعنی دارک‌نت و استفاده از ابزار مالی ارزهای مجازی، تبدیل به یک سامانهٔ مجرمانه جهت ارتکاب طیف وسیعی از جرایم شد.

۱-۱-۲. جادهٔ ابریشم؛ سامانهٔ فروش برخط مجرمانه

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

راس ویلیام اولبریچ درسال ۲۰۱۱ جاده ابریشم را ایجاد کرد. در جادهٔ 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 (Afilipoaie & Shortis, 2015). بیت‌کوین یگانه ارز پذیرفته‌شده در جادهٔ ابریشم بود. طی دو سال فعالیت موفق، جادهٔ ابریشم بیش از ۱/۲ میلیارد دلار به دست آورد.

اولین‌گام برای همهٔ فروشندگان در جادهٔ ابریشم این بود که یک فروشگاه در آن راه‌اندازی کنند. فروشنده باید از نحوهٔ کار در سرویس Tor آگاهی می‌داشت و به جادهٔ ابریشم دسترسی پیدا می‌کرد. Tor در اصل یک شبکهٔ توزیع رایانه‌ای است که آدرسIP واقعی کاربر را پنهان می‌کند و به همین علت هویت کاربران شبکه را با مسیریابی ارتباطات یا معاملات، ازطریق چندین رایانه در سراسر جهان از شناسایی مصون می‌سازد و آن‌ها را در چندین لایهٔ رمزگذاری‌شده قرار می‌دهد. مرحلهٔ دوم این بود که خریداران جهت خرید کالا یا دریافت خدمتی غیرقانونی، بیت‌کوین به دست آورند و یک آدرس برای تحویل کالا یا خدمات معرفی‌کنند. یگانه وجه پرداختی مقبول در جادهٔ ابریشم، بیت‌کوین بود و چنانچه خریداران بیت‌کوین نداشتند، می‌توانستند از سرویس مبادله یا صرافی

1. Silk Road

بیت‌کوین برای تبدیل ارزهای رایج و قانونی خود به بیت‌کوین استفاده کنند. «فیلا و شرم» دو نفر از مرتبطان جادهٔ 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 جادهٔ ابریشم انتقال می‌دادند و مبلغی را به‌عنوان هزینهٔ 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. مرحلهٔ سوم، تحویل و پرداخت بود. برای پیشگیری از تحویل کنترل‌شده[1]، جادهٔ 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 خلاءِ مهروموم‌شده و زیپ‌دار برای ارسال موادمخدر استفاده می‌کردند. جادهٔ ابریشم از یک سامانهٔ سپردهٔ خاص استفاده می‌کرد. تحت این سامانه، خریداران، بیت‌کوین را از کیف‌پول خود (توسط وب‌سایت) به‌حساب خود در جادهٔ 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 جادهٔ ابریشم، اولبریچ قوانینی را مبنی بر ممنوعیت این چنین پرداخت‌هایی و ضمانت‌اجرایی برای آن وضع کرد.

سرانجام جادهٔ ابریشم توسط FBI درسال 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 گفتگوِ 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 جادهٔ ابریشم درسراسر جهان، از جمله در انگلستان، سوئد و ایالات متحده دستگیر شدند. دیگر ارائه‌کنندگان خدمات مبادلهٔ بیت‌کوین (صرافی‌های بیت‌کوین) نیز به‌دلیل مبادلهٔ بیت‌کوین در ازای ارزهای‌سنتی برای کاربران

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

جادهٔ ابریشم دستگیر شدند. ازمیان پرونده‌های کیفری مرتبط با دارک‌نت و بیت‌کوین، جادهٔ ابریشم نمونهٔ کاملی محسوب می‌شود که براساس آن می‌توان خطرات مجرمانهٔ ارزهای‌مجازی را تحلیل کرد؛ زیرا این بازار برخط مجرمانه، نمونهٔ کاملی از یک سازمان مجرمانهٔ مجازی برای ارتکاب جرایم غالباً یقه‌سفیدی با استفاده از ارزمجازی است.

۲-۱-۲. دارک‌نت؛ بستر امن مجرمانه

فعالیت‌های غیرقانونی در فضای دارک‌نت و به‌واسطهٔ ارزهای مجازی، شامل دامنهٔ وسیعی از جرائم، از جمله انتقال وجه بدون مجوزقانونی، 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 بزهکاران یقه‌سفیدی به این فضا دانست. موضوعی که با قرارگرفتن جادهٔ ابریشم در بستر امن دارک‌نت، تجلی پیدا کرد.

سه نوع وب‌سایت اینترنتی وجود دارد: نخست، «وب سطحی»[1] که وب‌سایت‌هایی که به‌عنوان بخشی از وب سطحی شناخته می‌شوند، به‌دلیل نمایه‌دارشدن آن‌ها از طریق موتورهای جستجو، در دسترس هستند؛ دوم، وب‌سایت‌های دیگر که از طریق مرورگرهای استاندارد وب، دسترسی‌پذیر هستند ولی توسط موتورهای جستجو دسترسی‌پذیر نیستند، به‌عنوان بخشی از «وب عمیق»[2] طبقه‌بندی می‌شوند و توسط موتورهای جستجو نشان داده نمی‌شوند؛ ردهٔ نهایی، «دارک‌نت»[3] است که با وب‌سایت سطحی و وب عمیق تفاوت دارد؛ برخلاف وب‌سایت‌های موجود در وب سطحی، وب‌سایت‌هایی که به‌عنوان بخشی از دارک‌نت طبقه‌بندی می‌شوند، از طریق موتورهای جستجوی معمولی قابل‌جستجو نیستند. تمایز دارک‌نت از وب عمیق نیز از نحوهٔ دسترسی به آن‌ها شکل می‌گیرد؛ دارک‌نت به‌کاربران اجازه می‌دهد تا در اینترنت به جستجو بپردازند؛ در حالی که با مسیریابی اتصالات توسط سرورهای پروکسی شخص ثالث و مسدودکردن آدرس IP کاربر، از آن‌ها در برابر نظارت و تحلیل ترافیک محافظت می‌کند (Weimann, 2016:42). مجلهٔ وایرد (Wired) تخمین می‌زند که دارک‌نت بیش از ۰/۱ درصد از اینترنت را شامل نمی‌شود. با این حال، به‌دلیل ناشناس‌بودن و امنیتی که دارک‌نت فراهم می‌کند، اغلب توسط مجرمان سایبری برای فعالیت‌های غیرقانونی مورد استفاده قرار می‌گیرد. گزارش‌ها حاکی از آن است که ۵۷درصد محتوای دارک‌نت

1. Surface Web
2. Deep Web
3. Dark Web

غیرقانونی است؛ مانند پورنوگرافی، مراودات مالی غیرقانونی، فروش مواد مخدر و سلاح، پول‌شویی و ارتباطات تروریستی (Wechsler, 2016).

چند راه شناخته‌شده برای دسترسی به دارک نت وجود دارد: نخستین راه، استفاده از مرورگر Tor است.[۱] «مرورگر Tor یک سیستم پیوندی مسیریابی است که یک آدرس خام رایانه‌ای شخصی را پیش از رسیدن به مقصد، از طریق تکرار داده‌های رمزنگاری‌شده‌ای که از طریق چندین سرور که به‌طور تصادفی انتخاب شده ارسال می‌کند و ردیابی را غیرممکن می‌سازد.» (Crawford, 2014) مسیریابی پیازی به این معنی است که «پیام‌ها در لایه‌هایی از رمزنگاری محفوظ می‌شوند. داده‌های رمزگذاری‌شده از طریق یک مجموعه از گره‌های شبکه، به نام روترهای پیازی منتقل می‌شوند، که هر کدام از آن‌ها یک لایه را برمی‌دارد و مقصد بعدی داده را کشف می‌کند. وقتی لایهٔ 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 شبکهٔ تصادفی را انجام می‌دهد و وقتی Tor آماده شد، مرورگر باز خواهد شد؛ برای جداشدن 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

۱. سامانهٔ Tor (The Onion Route) برای ناشناس‌ماندن کاربران در محیط اینترنت به کار می‌رود و از نرم‌افزار کارخواه و شبکه‌ای از سرویس‌دهنده‌ها (سرورها) تشکیل شده است و می‌تواند داده‌هایی از کاربران مانند موقعیت مکانی و نشانی پروتکل اینترنت را پنهان کند. بهره‌گیری از این سامانه، ردگیری و شنود داده‌های کاربر را از سوی دیگران بسیار سخت می‌کند. این ردگیری و شنود می‌تواند در زمینهٔ بسیاری از فعالیت‌های کاربر، مثل وبگاه‌هایی که بازدید کرده، داده‌هایی که بارگیری و بارگذاری کرده، پیام‌هایی که از طریق نرم‌افزارهای پیام‌رسان ارسال یا دریافت کرده و هرگونه ارتباطاتی که در محیط اینترنت برقرار کرده است، صورت پذیرد؛ لذا می‌توان گفت که این سیستم برای محافظت از آزادی کاربران و حفظ حریم خصوصی آن‌ها در محیط اینترنت طراحی شده است. این نرم‌افزار، یک نرم‌افزار آزاد است و استفاده از شبکهٔ آن نیز رایگان است.

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 اجازهٔ 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 نسخهٔ ساده از I2P است و به‌اشتراک‌گذاری فایل را برای مخاطبان گسترده‌تری امکان‌پذیر می‌سازد. Freenet یک ارتباط جدید با مسیرهای جدید ایجاد می‌کند. مانند Tor، I2P و Freenet به‌دلیل 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 نسخهٔ پاک‌شده را نگه می‌داریم.» (Spalevic & Ilic, 2017: 75)

در سطح جهانی، دارک‌نت، تبدیل به یک مکان ملاقات برای افرادی شده است که به‌دنبال محصولات غیرقانونی هستند. مردم به‌طور کاملاً ناشناس، قادر به انجام هرگونه معاملات غیرقانونی یا ارضای تمایلات انحرافی خود هستند و دولت‌ها توانایی کمی در متوقف‌کردن آن‌ها دارند. ازاین‌رو، قرارگرفتن سامانه‌های برخط مجرمانه‌ای چون جادهٔ ابریشم در بستر دارک‌نت و استفاده از ارزهای مجازی، مانند بیت‌کوین، به‌عنوان ابزار مالی پذیرفته‌شده در مبادلات آن، بیش‌ازپیش 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 سادهٔ آن است. بیت‌کوین یک ارز مجازی است که واقعی یا فیات نیست.[۲] در عوض، از لحاظ الکترونیکی مشتق شده و قابل‌ارزیابی به‌عنوان 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 به‌عنوان یک واحد حساب، یک ذخیرهٔ ارزش و یک وسیلهٔ 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 به‌صورت جمعی توسط شبکه انجام می‌شود. بیت‌کوین منبع باز است؛ طراحی آن عمومی است: هیچ‌کس صاحب یا کنترل‌کنندهٔ بیت‌کوین نیست و همه می‌توانند با آن کار کنند.... بیت‌کوین قابلیت‌های استفادهٔ هیجان‌انگیزی دارد که سیستم‌های پرداخت دیگر از آن محروم هستند».[۳] بیت‌کوین‌ها به چهار روش به دست می‌آیند: دریافت به واسطهٔ فروش کالا یا ارائهٔ خدمات، خرید بیت‌کوین با پول واقعی، مبادلهٔ بیت‌کوین‌ها و استخراج.[۴] 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.[۵] بیت‌کوین به‌دلیل سه مزیت عمده به خریداران و فروشندگان در بازارهای دارک‌نت ارائه می‌شود. نخست، خطرات کمتر برای

۱. بیت‌کوین Bitcoin (با حرف بزرگ) هم به نرم‌افزار منبع بازِ استفاده‌شده برای ایجاد ارز مجازی و هم شبکهٔ 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 ازبین‌رفتن حکومت، پول ضرب‌شده 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 یکجانبهٔ پیمان برتون وودز از سوی آمریکا در سال ۱۹۷۱، پول مورد استفاده در تمامی کشورهای دنیا پول فیات است.

3. Bitcoin.org, https://bitcoin.org/en/ accessed February 14, 2016.

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

۵. 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 شبکهٔ 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).

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 به‌راحتی 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 ارزهای خود با استفاده از خدمات پشتیبانی مضاعف و رمزگذاری، حفاظت بیشتری کنند. سوم، شفافیت؛ تمام اطلاعات مربوط به عرضهٔ 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 هستهٔ بیت‌کوین کاملاً شفاف و پیش‌بینی‌پذیر باشد.

بیت‌کوین، امنیت و ناشناسی‌بودنی را فراهم می‌کند که کارت‌های اعتباری فاقد آن هستند؛ هیچ دنبالهٔ 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 آنجایی‌که مجازی است، نیازی به حضور اشخاص ثالث در فرایند کاربری ندارد. این امر موجب می‌شود اشخاص برای خرید محصولات غیرقانونی از مجرمان راحت‌تر باشند. در مجموع، بیت‌کوین هم برای کاربری‌های مشروع و هم برای تبهکاران امنیت گسترده‌ای را فراهم می‌کند و اطمینان لازم جهت تسهیل معاملات در جهان زیرزمینی را ایجاد می‌کند.

۲-۲. دلایل جذابیت ارزهای مجازی برای بزهکاران

بررسی پروندهٔ جادهٔ ابریشم و برخی پرونده‌های کیفری مرتبط با ارزمجازی، نشانگر چهار عامل است که بسیاری از بزهکاران سنتی را جذب تجارت برخط در فضای مجازی کرده است. چهار عامل، انعطاف‌پذیری هویت، ناشناختگی، سهولت شرکت در عملیات مجرمانه و فقدان بازدارندگی، از عوامل تسهیل‌کنندهٔ تجارت غیرقانونی در فضای مجازی شناخته می‌شوند که با وجود ارزهای‌مجازی تقویت شده‌اند. بررسی این موارد نشان از جایگاه ارزهای‌مجازی در بزهکاری یقه‌مجازی‌ها و به‌عنوان نقطهٔ عطفی در این‌گونه از بزهکاری است.

۱-۲-۲. انعطاف‌پذیری هویت

انعطاف‌پذیری هویت، از جذاب‌ترین عواملی است که سبب جلب توجه مجرمان به فضای مجازی می‌گردد. این امر جزء ویژگی‌های ذاتی فضای مجازی است که با وجود ارزهای مجازی تشدید شده است. بدین‌سان، بررسی انعطاف‌پذیری هویت از چند بُعد درخور توجه است.

نخست، تمام مجرمان برخط از هویت جعلی استفاده می‌کنند. هویت‌های جعلی آن‌ها تا حدودی برخی از جنبه‌های کار آن‌ها را نمایان می‌سازد. امری که در جادهٔ ابریشم به‌وضوح دیده می‌شود. اشخاص درگیر در پروندهٔ جادهٔ ابریشم، شامل مالک جادهٔ ابریشم، اولبریچ، کارمندانش، اندرو مایکل جونز، گری دیویس، پیتر فیلیپ ناش و راجر توماس کلارک[1]، فروشندگان مواد مخدر استیون لوید سدلر و جرمی دانگال[2]، رابرت فایلا و چارلی‌شرم[3]، فروشندگان یا صرافان بیت‌کوین فعال در این بازار برخط مجرمانه و مأموران FBI مسئول بررسی پرونده، اولبریچ، کارل مارک و شان بریج[4]، که متهم به پول‌شویی و تخلفات مالی شدند، می‌شود. دانگال، فروشندهٔ مواد مخدر، از «Xanax king» و «XX» و فیلا، فروشندهٔ بیت‌کوین، از عنوان «BTCKing» به‌عنوان هویتی برای خود استفاده می‌کردند.

دوم، بیش از هشتاددرصد مجرمان اینترنتی از بیش از دو هویت استفاده می‌کنند (Kethineni, Cao, Dodge, 2018:143). راس اولبریچ، مالک جادهٔ ابریشم، از هویت‌های «Dread Pirate Roberts»، «DPR» یا «Silk Road» به‌عنوان نام کاربری خود استفاده می‌کرد و کارل، مأمور ادارهٔ مبارزه با مواد مخدر، زمانی که به‌عنوان مأمور مخفی FBI برای شناسایی گردانندگان و مرتبطان جادهٔ ابریشم فعالیت می‌کرد، از عنوان «NOB» برای برقراری ارتباط با اولبریچ استفاده می‌نمود و هنگامی که قصد اخاذی از اولبریچ را داشت، نام «French Maid» و «Carla Sophia» را به کار می‌برد. در یکی از پیام‌هایی که از کارل جهت اخاذی 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 رخ‌می‌دهد. راجر کلارک، که از ژانویهٔ ۲۰۱۱ تا اکتبر ۲۰۱۳ به اولبریچ در مدیریت جادهٔ ابریشم کمک می‌کرد، از چهار هویت متفاوت در بازهٔ زمانی سه‌ساله استفاده کرد. در آغاز، او هویت «Jones Variety» و «VJ» را برگزید. در پیامی به اولبریچ در

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

۲۹اکتبر۲۰۱۱، 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 این‌حال فضای دارک‌نت، این ویژگی منحصربه‌فرد را به وجود آورده است تا ردپایی از کاربر در فضای مجازی باقی نماند و در صورت استفاده از چندین هویت، شناسایی از طُرق دیگر نیز در عمل بسیار دشوار شود. این امر با وجود ارزهای مجازی ابعاد جدیدی یافته است که می‌تواند مکملی جهت تقویت این قابلیتِ چندگانگی و انعطاف‌پذیری در هویت باشد. این مکمل عبارت است از تعداد «مشارکت‌کنندگان زیاد و کنترل‌نشده»[1] که در ایجاد و استفاده از ارزهای مجازی شرکت می‌کنند.

۱. منظور از مشارکت‌کنندگان در فرایند ارزهای مجازی، تمامی افرادی هستند که به‌نوعی در جریان مبادلات به‌واسطهٔ ارزهای مجازی دخیل‌اند؛ برای مثال، در فرایند بیت‌کوین 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 اَشکال ارزهای مجازی و همچنین فلزات گران‌بها و بالعکس می‌پردازد. صرافان عموماً دامنهٔ 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 به‌صورت شخصی به فرد دیگری (برای استفادهٔ شخصی) ارسال می‌کند یا پولی مجازی را به‌عنوان 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 فعالیت‌های‌خاصی که منجر به کسب ارز مجازی می‌شود، درگیر باشند؛ (۳) با توجه به‌ساختارهای برخی از ارزهای مجازی غیرمتمرکز خود اقدام به تولید ارز نماید. برای مثال بیت‌کوین این امکان را به‌کاربر می‌دهد، به‌عنوان معدنچی (Miner)، با استفاده از ویژگی «استخراج» (Mining) به تولید بیت‌کوین بپردازد. معدنچی عبارت است از فرد یا مؤسسه‌ای که در شبکهٔ 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). معدنچیان همچنین ممکن است در یک سامانهٔ ارز ←

مشارکت‌کنندگان در فرایند مبادلات به‌واسطهٔ ارزهای مجازی، طیف وسیعی از اشخاص حقیقی و حقوقی را شامل می‌شوند. ازاین‌رو، یک ارز مجازی ممکن است توسط مجمعی از «معدنچیان» (در خصوص ارز رمزپایهٔ غیرمتمرکز، مانند بیت‌کوین) یا توسط یک نهاد مجزا (در خصوص ارز مجازی متمرکز)[1] صادر شود؛ توسط عده‌ای تحت عنوان صراف به فروش برسد؛ کاربرانی از آن در مبادلات خود استفاده کنند و عده‌ای دیگر اقدام به ذخیرهٔ آن در کیفِ پول‌های خاص نمایند.

بدین‌ترتیب، در فرایند ارزهای مجازی با گستردگی اشخاص دخیل مواجه هستیم که با انعطاف‌پذیری در هویت، بیش‌ازپیش موجبات سردرگمی مأموران مجری قانون را فراهم می‌کنند. این امر درکنار گستردگی قلمرو جغرافیایی حضور این اشخاص و محدودنبودن آن‌ها به‌مرزهای کشوری خاص تشدید می‌شود. در این زمینه یکی از تشکیلات مجرمانه، به نام لیبرتی‌رزرو[2] که با استفاده از ارز مجازی در زمینهٔ 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 به‌فعالیت می‌کرد و بیش از یک‌میلیون 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 همهٔ آن‌ها غیرقانونی بودند. در واقع تعداد مشارکت‌کنندگان زیاد با هویت‌های چندگانهٔ غیرواقعی، به‌ویژه در فرایند کارکرد ارز مجازی، یکی از مشکلات نهادهای اجرای قانون در شناسایی و کشف بزهکاران دخیل در این تشکیلات مجرمانه بود. بدین‌ترتیب افزایش مشارکت‌کنندگان برخوردار از هویت‌های چندگانه، بیش‌ازپیش کاربرانِ مجرم ارزهای مجازی را از دسترس کنشگران نظام عدالت کیفری دور کرده است.

عدم‌کنترل نیز ویژگی مکمل دیگری برای انعطاف‌پذیریِ 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 فراملی‌بودن فضای مجازی و

مجازی به‌عنوان صراف شرکت کنند؛ ارز مجازی را به‌عنوان یک کسب‌وکار ایجاد نمایند تا بتوانند آن را در برابر پول نقد یا دیگر ارزهای مجازی بفروشند.

۱. ارز مجازی غیرقابل‌تبدیل (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.

2. LIBERTY RESERVE (LR)

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 مبادلهٔ ارز مجازی در کشور «پ» تبدیل کند و این ارز مجازی را به یک کیف پول در کشور «ت» انتقال دهد. این ارزمجازی (احتمالاً از طریق سایر واسطه‌ها) می‌تواند به کیف پول دریافت‌کنندهٔ 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 نقل‌وانتقالات، ممکن است کاربر اقدام به مبادله با اشخاص یا شرکت‌های کشوری نماید که به‌لحاظ سامانهٔ مبارزه با پول‌شویی و تأمین مالی تروریسم دارای ضعف است یا اساساً بنا به دلایل مختلف، در این حوزه به‌طور بین‌المللی همکاری نمی‌کند. بدین‌سان حتی چنانچه یک شخص به شرحی که گذشت تمامی اقدامات را انجام دهد، به‌دلیل عدم وجود توان کافی برای کنترل مؤثر، کشف و شناسایی مرتکب درعمل غیرممکن می‌شود.

بدین‌ترتیب می‌توان به‌وضوح دید که ویژگی انعطاف هویت در فضای مجازی، در صورت ترکیب با ویژگی عدم قابلیت ردیابی دارک‌نت و ویژگی‌های مشارکت‌کنندگان زیاد و عدم‌کنترل کاربران ارزهای مجازی، به‌میزان چشمگیری تمایل به‌ارتکاب جرم یا تمرکز فعالیت‌های مجرمانه درفضای مجازی را افزایش داده است.

۲-۲-۲. ناشناختگی

قرن‌هاست که به‌دلیل ممنوعیت‌های موجود در واردات یا صادرات تعدادی از کالاها، برخی فعالیت‌های تجاری بین‌المللی به‌صورت قاچاق روی می‌دهد. جدا از افزایش سطح معاملات تجاری معمولی که موجب افزایش فرصت‌های تجاری غیرقانونی شده، اینترنت نیز به‌طور گسترده‌ای شکل‌گیری بازارهای بین‌المللی غیرقانونی برای هرچیزی، 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 هزارهٔ سوم، تمایل به تمرکز فعالیت‌های مجرمانهٔ تجاری در فضای اینترنت به‌واسطهٔ گمنامی و ناشناسی مرتکبان افزایش یافته است. ازاین‌رو، شاید گمنامی، مهم‌ترین عامل تسهیل‌کننده‌ای باشد که مجرمان را به‌سوی فضای مجازی می‌کشاند. روش‌های متعددی وجود دارند که مجرمان فضای مجازی برای حفاظت از گمنامی خود طراحی نموده‌اند. نخستین فناوری، سرویس Tor است. جادهٔ ابریشم بر اساس تکنیک Tor عمل می‌کرد. Tor آدرس IP کاربران را مخفی می‌کند و از آن‌ها در برابر شناسایی و کشف محافظت می‌کند. روش دوم و بسیار مهم فناوری، ارزهای‌مجازی است.

یکی از مزایای مهم ارزهای‌مجازی این است که ناشناختگی کامل و عدم شناسایی را برای معاملات فراهم می‌کنند. در خصوص بسیاری از ارزهای رمزپایه، گرچه هویت مدیران و ذی‌نفعان

رمزگذاری شده‌اند و معاملات در یک فهرست عمومی ثبت و قابلیت ردیابی آن‌ها تضمین می‌شود، همچنان مسئلهٔ 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 به‌موجب پروتکل‌های موجود ارزهای مجازی تضمین شده است و نه از لحاظ سامانه‌ای امکان‌پذیر است (Kethineni & Cao & Dodge, 2018: 148). ضمن آنکه برخی از ارزهای رمزپایه، ناشناسی و عدم‌ردیابی را به‌عنوان ویژگی‌های منحصربه‌فرد خود ارائه می‌دهند و در کنار آن به‌واسطهٔ ابزارها و برنامه‌های کاربردی، این امکان را به کاربران می‌دهند که پرداخت‌های خود را توسط ترکیبی از شناسه‌های‌کاربری انجام دهند. علاوه بر این، علت و چرایی معاملات، هم از نظر فنی و هم به‌لحاظ قانونی مشخص نیست که این قضیه موجب عدم‌شفافیت و ایجاد فضایی مبهم و جذاب برای سازمان‌های‌جنایی می‌شود.

عدم امکان ردیابی معاملات و مشخص‌کردن ذی‌نفعان واقعی آن، ویژگی منحصربه‌فرد و جذابی است که تبهکارن را به سمت خود جلب می‌کند. کاربران ارزهای مجازی صرفاً بر اساس شناسهٔ حساب شناسایی می‌شوند که به‌واسطهٔ 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، نقل‌وانتقالات به‌صورت پول نقد (دلار آمریکا) انجام و ذخیره می‌شد. برای استفاده از ارز لیبرتی‌رزرو، کاربر، یک حساب کاربری را از طریق وب‌سایت لیبرتی رزرو باز می‌کرد. درحالی که بازکردن حساب کاربری درلیبرتی رزرو ظاهراً نیاز به اطلاعات شناسایی اولیه داشت، به تأیید هویت‌ها توسط سرورها و سامانه‌های موجود نیاز نداشت. به‌همین دلیل کاربران به‌طور معمول تحت نام‌های دروغین، از جمله نام‌هایی با مضامین مجرمانه (مانند هکرهای روس) حسابی با آدرس‌های محل اقامت دروغین می‌ساختند (FATF, 2015: 27). برای اضافه‌کردن یک لایهٔ ناشناختهٔ 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 جادهٔ 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

به‌حساب سایر کاربران، ازجمله شرکت‌های تجاری «بازرگانان»[1] که LR را به‌عنوان روش پرداخت قبول داشتند، انجام دهد (FATF, 2015: 28). به‌ازای هزینهٔ اضافی تحت‌عنوان «هزینهٔ حفظ حریم خصوصی» (۷۵ سنت ایالات متحده در هر معامله)، کاربران می‌توانستند شماره حساب‌های لیبرتی رزرو خود را هنگام نقل‌وانتقال پول، پنهان کنند و انتقال‌های آن‌ها به‌طور کامل غیرقابل‌شناسایی باشد و نه‌تنها ردی از معاملات باقی نماند، حتی در لایهٔ بعدی مبدأ و مقصد واقعی نقل‌وانتقالات نیز ناشناخته باقی می‌ماند. بدین‌ترتیب، هزینهٔ ارتکاب جرم کاهش می‌یابد و با کاهش خطر برای بزهکاران، امکان وقوع جرم در این بستر افزایش خواهد یافت.

۳-۲-۲. سهولت شرکت در عملیات مجرمانه

بیت‌کوین، به‌عنوان شناخته‌شده‌ترین ارز مجازی، از فناوری شخص به شخص استفاده می‌کند که برای کار به هیچ نهاد مرکزی یا بانکی که معاملات را مدیریت کند، احتیاج ندارد و صدور آن به‌صورت جمعی توسط شبکه انجام می‌شود. بیت‌کوین منبع باز است؛ طراحی آن عمومی است: هیچ‌کس صاحب یا کنترل‌کنندهٔ بیت‌کوین نیست و همه می‌توانند با آن کار کنند. معاملات بیت‌کوین امن و برگشت‌ناپذیر است و اطلاعات حساس یا شخصی مشتری را ذخیره نمی‌کند. این کار بازرگانان را از خسارات ناشی از تقلب یا بازپرداخت‌های جعلی مصون می‌دارد. بازرگانان به‌راحتی می‌توانند به بازارهای جدیدی راه پیدا کنند که در آن‌ها یا کارت‌های اعتباری در دسترس نیستند یا نرخ تقلب به‌طور نامقبولی بالاست. نتایج این سهولت در استفاده عبارت است از: کاهش هزینهٔ تجارت، دسترسی به بازارهای بزرگتر و هزینه‌های اداری کمتر.

نتیجهٔ دیگر این سهولت، امکان اتحاد فراملی برای ارتکاب جرم است. مجرمان سایبری می‌توانند در کشورهای مختلف زندگی کنند و یک تجارت مجرمانه را اداره کنند. اولبریچ در ایالات متحده زندگی می‌کرد، درحالی که کلارک، یک کانادایی‌تبار، ساکن تایلند بود. این فناوری می‌تواند در کشورهای مختلف واقع شود. شالون، یکی از فروشندگان بیت‌کوین، از زیرساخت شبکهٔ رایانه‌ای، از جمله سرورهای واقع در مصر، جمهوری چک، آفریقای جنوبی، برزیل و دیگر مکان‌ها برای دسترسی غیرقانونی و سرقت اطلاعات استفاده می‌کرد (Kethineni & Cao & Dodge, 2018: 149). مواردی وجود داشت که در آن‌ها درآمد حاصل از جرائم به کشورهای خارجی منتقل می‌شد.

1. Merchants

دانگل که باعنوان «XanaxKing» نیز شناخته می‌شود، از وسترن‌یونیون[۱] برای انتقال درآمدهای مجرمانه خود به چین استفاده کرد. در نمونه‌ای دیگر، شخصی به نام علی شکری‌امین، با استفاده از رسانه‌های اجتماعی‌مجازی، برای تأمین مالی داعش، از افراد درخواست بیت‌کوین می‌کرد (United States of America v. Ali Shukri Amin, 2015). مجرمان سایبری یکدیگر را به‌صورت برخط ملاقات می‌کنند. گرچه ممکن است جرائم در هر گوشه‌ای از جهان رخ دهد، این امر به‌خصیصهٔ جهانی‌شدن جرایم در بستر فضای سایبر کمک می‌کند.

نمونهٔ دیگر گروه جرایم سایبری، «WEI»[۲] است که تحقیقات هشت‌ساله در خصوص آن، منجر به محکومیت ۱۶ نفر از اعضای آن به جهت نقش آن‌ها در طرح سرقت هویت جهانی یا برنامهٔ فاجعهٔ سایبری شد. اعضای گروهِ جرایم اینترنتی، در ابتدا از طریق وب‌سایت‌های اینترنتی «کارتینگ»[۳] 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 ناشناس‌بودن 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 پانزده‌میلیون دلار در وب‌مانی[۴] و بیست‌میلیون دلار در ای‌گلد[۵] 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،[۶] اطلاعات و کمک‌های لازم را برای انتقال پول به‌طور ناشناس و با خودداری از رعایت الزامات

۱. Western Union: شرکت وسترن‌یونیون، ارائه‌دهندهٔ خدمات مالی و ارتباطی است. حوالهٔ 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.

2. Western Express International
3. CARDING
4. WebMoney
5. E-Gold
6. Dengiforum.comandPaycard2000.com

گزارش‌دهی ارائه می‌داد.[۱] 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 ارزهای‌مجازی در قلمروهای سیاسی مختلف، عملیات مجرمانهٔ خود را به شکل گسترده‌ای پیگیری می‌کردند. فروشندگان تقریباً ۱۰۰,۰۰۰ شمارهٔ 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 برای ساخت کارت‌های اعتباری و خرید کالاهای گران‌قیمت استفاده می‌کردند و مرتکب جرایم دیگری مانند نگهداری از اموال مسروقه، کلاهبرداری، تولید حدود پنج‌میلیون دلار اعتبار کارت تخفیف و پول‌شویی و جابه‌جایی پول بیش از ۳۵میلیون دلار از طریق حساب‌های مختلف شدند. بدین‌سان، استفاده از ارزهای‌مجازی بیش‌ازپیش 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 ۵۷درصد محتوای آن غیرقانونی است (Weimann, 2016)، نسبتاً کم است. جادهٔ 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 فروشندهٔ مواد مخدر و فروشندگان غیرقانونی دیگر در جادهٔ ابریشم فعالیت می‌کردند، احتمال شناسایی‌شدن آن‌ها، با وجود دستگیری بنیان‌گذار این بازار برخط مجرمانه، اندک بود. این امر تا حدود زیادی به ماهیت پویا و نفوذ ناپذیر سازوکار مراودات مالی در این فضا، خصوصاً استفاده از بیت‌کوین، برمی‌گردد.

۱. مالک شرکت WEI که ملیت اوکراینی دارد، در ماه فوریه سال ۲۰۱۳ در ایالت نیویورکِ 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 منطقهٔ منهتن (نیویورک) انجام شد (FATF, 2015: 26).

دوم، از دیدگاه فرصت، قوانین و مقررات به‌خوبی به‌عنوان ابزارهایی در نظر گرفته می‌شوند که می‌توانند برای کنترل فرصت‌های جرم یقه‌سفیدی مورد استفاده قرار گیرند. باید به خاطر داشت که جرایم یقه‌سفیدی دارای ویژگی‌های خاصی هستند: دسترسی قانونی بزهکار به قربانی، جدایی فیزیکی و مکانی میان بزهکار و قربانی و صورت به‌ظاهر قانونی اَعمال. این خصوصیات موجب استفاده از شگردهای جنایی خاص می‌شود؛ برای مثال فریب، سوءاستفاده از اعتماد، اخفاء و توطئه و تبانی. بعضی از جرایم یقه‌سفیدی به‌موازات رشد فناوری جدید به وجود می‌آیند؛ برای‌مثال، تا زمانی که اینترنت به‌وجود نیامده بود، خبری از کلاهبرداری اینترنتی نبود؛ به همین دلیل، قانون نیازمند انعطاف‌پذیری و قابلیت تطبیقِ به‌هنگام با فرصت‌های مجرمانهٔ 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 ارزهای‌مجازی، هنوز یک منطقهٔ 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 جادهٔ ابریشم «معاملات‌مالی» نبودند. همچنین فیلا، صراف بیت‌کوین، استدلال کرد که رفتار وی انتقال غیرقانونی پول نقد نیست؛ زیرا بیت‌کوین پول نیست؛ بنابراین او فرستندهٔ 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 جادهٔ ابریشم شناخته می‌شد، شخصی با هویت واقعی راس اولبریچ است، یک آدرس ایمیل بود. وقتی اولبریچ به‌دنبال یک دستیار ITدر اینترنت بود، به‌اشتباه، آدرس ایمیل شخصی خود را نوشت: «Rossulbricht@gmail.com» (Hout & Bingham, 2013). اگر اشتباه راس اولبریچ نبود، پلیس برای ردیابی و توقف فعالیت مجرمانهٔ جادهٔ ابریشم با مشکل مواجه می‌شد. علاوه بر اولبریچ، دیگر مجرمان بازار ابریشم نیز از طریق روش‌های سنتی یافت شدند؛ برای مثال، سدلر، فروشندهٔ مواد مخدر، هنگام تحویل کنترل‌شده

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

گرفتار شد و دلایل مجرمانهٔ مربوط به کارل مارک در لپ‌تاپ اولبریچ یافت شدند. به‌طور کلی، پلیس برای تحقیق در زمینهٔ جرایم سایبریِ ارتکابیِ برخوردار از فناوری بالا در جادهٔ 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. بدین‌ترتیب کشف جرایم یقه‌سفیدی که به‌طور سنتی از رقم سیاه بزهکاری بالایی برخودار است، به‌مراتب دشوارتر خواهد شد.

نتیجه

ارزهای‌مجازی نمونهٔ نوین از تحولات فناوری هستند که به‌واسطهٔ ویژگی‌های منحصربه‌فرد خود، کارکرد گسترده‌ای در وقوع جرایم دارند. این ویژگی‌ها افزون بر ایجاد برخی تحولات مفهومی، گسترهٔ وسیعی از جذابیت‌های مجرمانه را ایجاد کرده‌اند که بیش‌ازپیش کوچ مجرمان، به‌ویژه مجرمان یقه‌سفید، به فضای مجازی را سرعت بخشیده است. امری که منجر به افزایش ریسک بزهکارانهٔ ارزهای مجازی شده است و اقدام به اتخاذ یک سیاست جنایی مناسب را در برابر آن اجتناب‌ناپذیر کرده است. با وجود این، اتخاذ سیاست جنایی مناسب در این زمینه نیازمند پیش‌شرط‌هایی است که عدم تحقق آن، هر راهبردی را با شکست روبه‌رو می‌سازد.

نخست، تلاش جهت شناسایی فنی ارزهای‌مجازی و تدوین رژیم حقوقی متناسب با قابلیت‌های آن. قانون‌مندسازی فعالیت‌های پولی و مالی در بستر ارزهای مجازی از شدت زیرزمینی‌شدن فعالیت‌های مرتبط با این حوزه، به‌دلیل افزایش تمایل عموم به استفاده از آن، خواهد کاست. این مسئله به‌عنوان ضرورتی انکارناپذیر به‌دلیل دشواری در کشف جرایم ارتکابی به‌وسیلهٔ ارزهای مجازی، مدیریت این حوزه با ابزارهای قانونی را اجتناب‌ناپذیر کرده است. بدین‌سان، رویکردی انفعالی در قبال ارزهای مجازی نه‌تنها 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 مقرره‌گذاری شده است. این رویکرد منفعلانه و تلاش جهت محونمودن صورت‌مسئله به‌جای ارائهٔ یک پاسخ و راهکار مناسب، نه‌تنها مفید واقع نخواهد شد، بلکه پیامدهایی منفی از جمله زیرزمینی‌شدن فعالیت‌های این حوزه را در پی خواهد داشت. ازاین‌رو، به‌نظر می‌رسد بانک مرکزی ایران، در چرخشی آشکار، تلاش جهت منضبط‌کردن این قلمرو را با انتشار پیش‌نویس سند «الزامات و ضوابط فعالیت‌ها در حوزهٔ رمزارزها در کشور» آغاز کرده است.

دوم، ترسیم چارچوب قانونی مناسب به‌منظور برقراری رویکرد ریسک‌مدار در برابر خطرات بزهکارانهٔ 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 شمولِ قوانین پول‌شویی قرار دهند تا به کاهش مخاطرات مجرمانهٔ این ارزها اقدام کنند. در این راستا، در ژوئن ۲۰۱۹، گروه ویژهٔ اقدام مالیFATF، به‌عنوان تخصصی‌ترین نهاد فراملی در زمینهٔ پیشگیری و مقابله با پول‌شویی، به روزآمدکردن دستورالعمل[1] خود دربارهٔ رویکرد ریسک‌مدار در برابر دارایی مجازی و ارائه‌دهندگان خدمات مربوط به آن پرداخت. دستورالعمل روزآمدشده تلاش می‌کند تا نخست، درک صحیحی در خصوص مقررات‌گذاری و پاسخ‌گذاری‌های نظارتی در خصوص ارزهای 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 اِعمال مؤثر این الزامات در این زمینه آشنا کند. ازاین‌رو به نظر می‌رسد پس از شناسایی قانونی ارزهای مجازی، پیش‌شرط دوم جهت اتخاذ سیاست جنایی مناسب در برابر ارزهای مجازی این است که این ارزها را تحت پوشش مقررات پول‌شویی قرار دهیم. امری که با توجه به ظرفیت‌های جدید قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷ و آیین‌نامهٔ اجرایی مصوب ۱۳۹۸ قانون مزبور در پهنهٔ نظام تقنینی ایران، پس از روشن‌شدن وضعیت حقوقی ارزهای مجازی، قابل‌اعمال است.

استفاده از ارزهای مجازی به‌طور قطع در جوامع پولی و مالی مقبولیت بیشتری قرار خواهد داشت. در آینده، انتظار می‌رود به‌دلیل عوامل متعددی، از جمله افزایش پذیرش پرداخت‌های بیت‌کوین توسط شرکت‌های بزرگ، ارزش بیت‌کوین، به‌عنوان محبوب‌ترین و شناخته‌شده‌ترین ارز مجازی افزایش یابد. افزون بر این، به‌دلیل 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.

۱. این سند، سند روزآمد شده سند سال ۲۰۱۵ با عنوان رویکرد ریسک‌مدار FATF به ارزهای مجازی است. نک:
http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

منابع

فارسی

- ابوذری، مهرنوش (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)، **جرم‌شناسیِ جرایم یقه‌سفیدان**، 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 نجفی‌ابرندآبادی، کتاب دوم، چاپ نخست، تهران: انتشارات میزان.
- خلیلی پاجی، عارف (۱۳۹۸)، امکان‌سنجی تأمین مالی تروریسم در پرتو ارزهای مجازی، **مجموعه مقالات همایش بین‌المللی ابعاد حقوقی-جرم‌شناختی تروریسم**، چاپ اول، تهران: انتشارات دانشگاهی علامه طباطبایی.
- دولاکوراِستا، خوزه لوییس (۱۳۹۶)، سیاست جنایی اروپا: نمونه‌ای از بین‌المللی شدن حقوق کیفری در سطح منطقه‌ای، ترجمه علی حسین نجفی‌ابرندآبادی، **مجموعه مقالات نکوداشت‌نامهٔ 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)، «جرائم شرکتی از دیدگاه جرم شناختی»، **دیدگاه‌های حقوق قضایی**، شماره ۵۷.
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۵)، «تحلیل جرم‌شناختی جرایم اقتصادی»، **تعالی حقوق**، سال اول، شماره.
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۹۱)، **تقریرات جرم‌شناسی (جهانی‌شدن جرم)**، دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه مفید. قابل دسترس در: www.lawtest.ir
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۸)، «جرم‌شناسی در فضای سایبر»، **تعالی حقوق**، سال چهارم، شماره ۳۶.
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۹۶)، جنایات بین‌المللی و جرم‌شناسی، دیباچه در: نیکوکار، حمیدرضا «به کوشش»، **جرم‌شناسی فراملی؛ به سوی جرم‌شناسی جنایات بین‌المللی**، چاپ اول، تهران: انتشارات میزان.
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۹۴)، جهانی‌شدن بزهکاری، دیباچه در: ذاقلی، عباس، **قاچاق انسان در سیاست جنایی ایران و اسناد بین‌المللی**، تهران: انتشارات میزان.
- نجفی‌ابرندآبادی، علی‌حسین (۱۳۹۵)، جهانی‌شدن حقوق کیفری و تعاملات دانشگاهی بین‌المللی، دیباچه در: رضوی‌فرد، بهزاد «به کوشش»، **جلوه‌هایی از حقوق کیفری فرانسه-مجموعه مقالات و سخنرانی‌های میشه مسه و برنادت زیبر**، چاپ اول، تهران: انتشارات دانشگاه علامه طباطبایی.
- نجفی‌ابرندآبادی، علی‌حسین 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, Sesha, 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.