فصلنامه علمی تخصصی

پژوهش‌های بازاریابی اسلامی

دوره ۲، شماره ۳، تابستان ۱۴۰۳

پیشگیری از فعالیت مجرمانه مرتبط با ارزهای مجازی در سیاست جنایی ایران در راستای مدیریت بازارهای ارزهای مجازی

محمد قائمی اصل [۲و۱]، سلامه ابوالحسنی [۳] ، نغمه فرهْود [۴]

[۱] دانشجوی دکتری، گروه حقوق جزا و جرم شنا سی، پردیس علوم و تحقیقات خوز ستان، دانشگاه آزاد ا سلامی، اهواز، ایران. / ۲. دانشجوی دکتری، گروه حقوق جزا و جرم شناسی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران.

[۳] استادیار، گروه حقوق جزا و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

[۴] استادیار، گروه حقوق جزا و جرم شناسی، واحد اندیمشک، دانشگاه آزاد اسلامی، اندیمشک، ایران.

تاریخ دریافت: ۱۴۰۲/۰۷/۰۴ تاریخ پذیرش: ۱۴۰۲/۰۹/۲۱ تاریخ انتشار آنلاین: ۱۴۰۲/۰۹/۲۱

چکیده

یکی از واقعیت‌هایی که امروز با آن مواجهیم و هر روزه بر دامنه آن افزوده می‌شـود، رواج اسـتفاده از رمز ارزها در مبادلات اینترنتی است. با این اوصاف در دهه‌های اخیر، سرعت پیشرفت فناوری بویژه در زمینهٔ فناوری‌های مالی، با ایجاد تحولات شگرف در نظام پولی کشورها، تغییر شئون مختلف زندگی مردم و همچنین دولت‌ها را به همراه دا شته ا ست. از جمله این فناوری‌های نوین، ارزهای مبتنی بر فناوری زنجیره بلوکی (بلاک چین) ا ست که تحت عنوان رمزینه ارزها یا ارزهای رمزگذاری شده شناخته می شوند. با توجه به ویژگی‌های منحصـربه فرد این نوع ارزها اعم از غیرمتمرکز بودن و عدم نیاز به نهاد مرکزی و ناظر برای انتقال پول (انتقال نظیر به نظیر) و مشـخص نبودن هویت واقعی گیرنده و فرستنده، بررسی سیاست جنایي ایران در قبال پیشگیري از فعالیت مجرمانه مرتبط با ارزهاي مجازي اهمیت می‌یابد. مقررات گذاری در خصوص مخاطرات جنایی ارزهای مجازی در ایران نیز از تفاوت‌های قابل توجهی با بسیاری کشورها برخوردار است، کنشگران سیاستگذار و مقرره گذار در ایران راهی دیگر را در پیش گرفتند. این رویکرد، با ممنوعیت استفاده و مبادله ارزهای مجازی با ا ستدلال قابلیت ا ستفاده پولشویی، آغاز شد که نوید دهنده توجه بیشتر به ارزهای مجازی از منظر مقررات پولشویی بود با این وجود، اقدامات بعدی که با انتشار پیش نویس سند الزامات و ضوابط فعالیت‌ها در حوزه ارزهای مجازی در کشور مورخ ۱۳۹۷/۱۱/۸ همراه شد نشـانگر به حاشـیه رانده شـدن رویکرد مرتبط با پولشـویی به ارزهای مجازی و تقویت رویکردی اسـت که در تلاش اسـت تا با ارز منظور ارزهای رایج مانند دلار و یورو محسـوب کردن ارزهای مجازی آن‌ها را تحت شـمول قوانین مربوط به ارز و از جمله قانون مبارزه با قاچاق کالا و ارز ۱۳۹۲ با اصلاحات و الحاقات بعدی درآورد.

واژه‌های کلیدی: ارزهای مجازی، سیاست جنایی ایران، فعالیت مجرمانه، مدیریت بازارهای ارزهای مجازی

* نویسنده مسئول: سلامه ابوالحسنی ، ایمیل: salameh_abolhasani@yahoo.com

۱ - مقدمه

در جهان امروز فناوری با سرعت شگرفی درحال پیشرفت است. بزهکاران این موقعیتِ فرصت‌ساز را به خوبی شناخته‌اند و از پیشـــرفت‌های فناورانه برای پیشـــبرد 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 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 ســنتیِ تولید و توزیع پول توســط دولت‌ها را بشکنند و ارزی غیررسمی با قابلیت تولید توسط کاربران فراهم آورند. ارزهای مجازی مبتنی بر رمزنگاری اطلاعات هستند و مبداء و مقصد آن‌ها در خیلی از مواقع معلوم نیست و به همین دلیل می‌توانند بستری برای پولشویی باشند. به همین جهت کشورها یا از ابتدا این پول‌ها را ممنوع کرده‌اند یا با سازوکارهای قانونی به صورت محدود از آن‌ها استفاده می‌کنند. با این حال، بیت کوین و دیگر گونه های ارزهای مجازی، وارد حوزه های جدیدتری برای تأمین مالی در معنای پول شده‌اند که به دلیل عدم قرار گرفتن بیت کوین در سامانه های پرداخت سنتی، مقرره گذاری این حوزه را با مشکلاتی همراه ساخته است؛ زیرا، این ارز مشـــمول قوانین مرتبط در این زمینه نمی شـــود. این امر، در کنار ویژگی‌های منحصـــربه فردی که بیت کوین به ارمغان آورده، موجب افزایش جذابیت این ارز مجازی برای بزهکاران، به ویژه بزهکاران مالی – اقتصادی، شده است. بنابراین، یکی از راه های پولشویی در بستر اینترنت مستلزم انتقال پول از یک بانک به بانک دیگر با استفاده از نام و مکان‌های مختلف است. این پروسه تا زمانی که پول پاک شده و قابل ردگیری نباشد، ادامه پیدا می‌کند. مزیت های پولشویی از طریق اینترنت این است که کمیت تراکنش‌ها به میزان دلخواه قابل افزایش اســـت و می‌تواند از یک نقطه دور صـــورت بگیرد و علاوه بر این‌ها بی نام انجام شود. ناشناس ماندن هویت در تراکنش‌های مالی مشخصه ضروری پول شویی است. رویکرد «مشتری خود را بشناس» که به طور سنتی توسط مؤسسات مالی مورد استفاده قرار می‌گرفت، تا پولشویی را کشف کند، در عصر حاضر که معاملات به جای اشخاص با کلیک موس صورت می‌گیرد، به خوبی پاسخ‌گو نیست.

اکنون مجرمان می‌توانند از پول الکترونیکی به عنوان راهی برای انتقال پول به طور نا شناس استفاده کنند. افراد و گروه هایی که مایل به دیده شدن و شناخته شدن نیستند می‌توانند از فرم‌های الکترونیکی پول برای انتقال وجوه در سطح جهان استفاده نمایند و اینترنت به عنوان ابزار مناســـب این حرکت عمل می‌کند. پول الکترونیکی یک پدیده غیر قانونی نیســـت بلکه در واقع پایه سیستم مالی جهانی کنونی است. هر چه پول الکترونیکی ناشناس‌تر باشد، احتمال انجام پولشویی بیشتر می‌شود. بسته به نوع

و ارائه کننده این پول‌ها، خرید دیجیتال به وسیله آن‌ها می‌تواند یک رد پای قابل تشخیص داشته باشد (مانند کارت‌های اعتباری) و یا مشابه پول کاغذی هیچ اثری از خود به جای نگذارد. ترکیب پول الکترونیک و بانک‌هایی که اجازه می‌دهند و حتی تشویق می‌کنند که افراد و یا کسب و کارهای ناشناخته به عنوان مشتری با آن‌ها در تعامل باشند، یک زمینه مناسب برای پولشویی ایجاد می‌کند. ارزهای مجازی در عمل هرچند در قیاس با ارزهای واقعی به صورت محدود فناوری مختل کننده نظام مالی سنتی را عرضه داشته اند که بسیاری از قواعد ضدپولشویی و تأمین مالی تروریسم را به چالش کشیده و ناتوانی آنها را در عرصه دنیای مجازی برجسته ساخته اند. ارزهای مجازی روند عادی ارزهای مادی دارای پشتوانه دولتی را برهم زده‌اند و حقوق را در جایی نحیف گذاشته اند که نه هر سال بلکه هر ماه و شاید هر روز روشی نوین و ابزاری جدید را به منظور ناشناختگی بیشتر به کار می‌گیرد (کدخدایی، ۱۳۹۹: ۲۵). رویکرد ایران در قبال ارزهای مجازی؛ از رویکرد منفعلانه تا رویکرد واکنشی بوده است. رویکرد سیاستگذاری در ایران نسبت به ارزهای مجازی در ابتدا ممنوعیت استفاده از آن بود. براین ا ساس در جل سه سی ام شورای عالی مبارزه با پول شویی در تاریخ ۱۳۹۶/۱۰/۹ به کارگیری ابزار بیت کوین و سایر ارزهای مجازی در تمام مراکز پولی و مالی کشور، به جهت قابلیت آن در ارتکاب پولشویی و تأمین مالی تروریسم ممنوع اعلام شد.

با این حال با گذشت بیش از یک سال از مصوبه مذکور، بانک مرکزی ایران رویکرد واقع بینانه تری در قبال ارزهای مجازی اتخاذ کرده است. براین اساس معاونت فناوری های نوین بانک مرکزی جمهوری اسلامی ایران، نسبت به انتشار پیش نویس سند «الزامات و ضوابط فعالیت‌ها در حوزه رمزارزها در کشور» مورخ ۱۳۹۷/۱۱/۸ اقدام کرد. این سند با هدف بررسی و ارائه نظرات متخصصان و صاحب نظران منتشر شده است و پس از انجام اصلاحات احتمالی و با تصویب شورای پول و اعتبار جهت اجرا ابلاغ شده است. ارز مجازی از انواع مختلفی برخوردار است که هر یک با توجه به ماهیت و کارکرد، دارای ویژگی‌های خاصی نسبت به یکدیگر هستند. بااین‌حال نمونه کامل ارز مجازی بیت‌کوین است که برخی ویژگی‌ها آن را از سایر ارزهای مجازی متمایز می‌کند. از این‌رو در پژوهش حا ضر با رو شی تو صیفی - تحلیلی به ارائه راهکارهای پی شگیرانه وضعی و اجتماعی پیرامون جرایم مرتبط با ارزهای مجازی با محوریت بیت‌کوین پرداخته خواهد شد؛ لذا نگارنده در این رساله به دنبال پاسخ گویی به این سوالات است که چه عواملی سبب جلب نظر بزهکاران به استفاده از ارزهای مجازی برای انجام فعالیت‌های مجرمانه می‌شود؟ راهکارهای پیشگیرانه از فعالیت مجرمانه مرتبط با ارزهاي مجازي منطبق با سیاست جنايي ايران چيست؟

اهمیت و ضرورت انجام تحقیق

ابزارها و شیوه‌های پول‌شویی به عنوان ا صلی‌ترین روش تسهیل کننده تأمین مالی تروریسم، با ظهور فناوری‌های نوین، چنان تنوع یافته ا ست که دیگر نمی‌توان مبارزه با آن را به قالب‌های سنتی گذ شته منوط کرد. تروریست‌ها و تبهکاران از فناوری‌های نوین چون اینترنت و ارزهای مجازی برای توسعه روش‌های مجرمانه خویش بسیار سود می‌جویند. ارزهای مجازی بر بستری غیرمتمرکز و در پوشش ناشناختگی عمل می‌کنند؛ از این رو بررسی این موضوع و ارائه راهکارهای پیشگیرانه می‌تواند راهگشا باشد. علاوه بر این این موضوع، به ویژه در سال‌های اخیر افزون برکشورهای مختلف، توجه نهادهایی چون کارگروه ویژه اقدام مالی را نیز به خود جلب کرده است.

مفهوم ارزهای مجازی

ارزهای مجازی به دلیل مفاهیم فناوری نوآورانه خود، سؤالات حقوقی جدیدی را مطرح می‌کنند. یکی از چالش مهم در حوزه ارزهای دیجیتال روند رو به گسترش آنها می‌باشد به نحوی که با توجه به تعداد زیاد (و به طور مداوم در حال رشد) سیستم‌های به ا صطلاح «ارز رمزنگاری» با ویژگی‌های فناوری متفاوت، ارائه تعریف ا صطلاح «ارز دیجیتال» کار آ سان نیست. آنچه در بیان تعریف ارز دیجیتال اهمیت دارد این است که چه ویژگی ارز دیجیتال را از پول بانکی مجزا می‌سازد.

رمز ارز، ارز مجازی و ارز دیجیتالی سه مفهوم مجزا با کاربردهای متفاوت هستند. ارزهای دیجیتال، ارزهایی هستند که به‌صورت الکترونیکی ذخیره و منتقل می‌شوند. هرگونه پولی که بر مبنای صفر و یک باشد در این تعریف می‌گنجد. مثلاً ریال‌های موجود در حساب بانکی بازنمایی کننده ریال‌های واقعی هستند که جایی نگهداری می‌شوند، در تعریف ارز دیجیتالی جای می‌گیرند. بیت‌کوین‌ها هم چون مبنای صفر و یک دارند؛ ارز دیجیتالی هستند. درنتیجه از نظر حقوقی عبارت «ارز دیجیتالی» یک عبارت موسع است (رجبی، ۱۳۹۷: ۲). ارزهای مجازی گونه‌ای از ارزهای دیجیتالی به شمار می‌آیند، اما هرگونه ارز دیجیتالی ارز مجازی به شمار نمی‌رود. رمز ارز نیز به این صورت تعریف شده‌اند که «ارز دیجیتالی هستند که در آن از فنون رمزگذاری برای مقررات‌گذاری تولید واحدهای جدید ارز و تأیید انتقال وجوه استفاده می‌کنند و مستقل از یک بانک مرکزی فعالیت دارند. معاونت فناوری‌های نوین بانک مرکزی جمهوری اسلامی ایران اقدام به انتشار پیش‌نویس سند «الزامات و ضوابط فعالیت در حوزه رمز ارزها در کشور» مورخ ۱۳۹۷/۱۱/۸ نموده و به تعریف رمز ارزها اقدام کرده است.

«رمز ارز یک نوع دارایی مالی اســت که بر بســتری دیجیتال، غیرمتمرکز و شــفاف به نام زنجیره بلوک موجودیت[1] می‌یابد. این دارایی‌ها می‌توانند در شرایطی کارکرد پولی به خود بگیرند».

ماهیت ارزهای مجازی

اقتصاد کشورها امرزوه متکی به پول اعتباری است که حکومت‌ها منتشر می‌نمایند. دلیل ارزشمند بودن این نوع از پول صرفاً اعلام حکومت‌ها مبنی بر قانونی بودن استفاده از این نوع پول برای پرداخت بدهی‌های عمومی و خصوصی است، نهایتاً باید خاطر نشان سازیم که پول به این دلیل ارزشمند است که مردم جوامع در خصوص با ارزش بودن آن توافق دارند، لذا دریافت و مبادله آن را پذیرفته‌اند و معتقدند که می‌توانند در برابر مبادله آن، کالا و خدمات مورد نیاز خود را تهیه نمایند.

لذا اســتفاده از هر نوعی از انواع پول یک نوع قرارداد اجتماعی بین اعضــای جامعه بر پذیرش و اســتفاده از آن نوع پول برای معاوضه در برابر کالا و خدمات است. بدین ترتیب سیر تحول پول در پول الکترونیکی و پول دیجیتال را نیز شاهد هستیم. به عبارت بهتر شاهد استمرار قرارداد اجتماعی و اعتماد به آن نوع از پول هستیم و به این ترتیب اکنون شاهد ارائه پول‌های مجازی هستیم (آذرنژاد، ۱۴۰۱: ۱۹).

در واقع هیچ تعریف جهان شــمولی از ارز مجازی وجود ندارد و اصــولاً بســیاری از کشــورها بر ســر اســتفاده از عنوان ارز نیز اختلاف دارند و برخی از آن‌ها در عوض از عبارت دارایی های رمزی استفاده می‌کنند. در گام نخست می توان ارزهای مجازی را ســامانه ارزی که از رمزنگاری برای انتقال امن و مبادله رمزهای دیجیتالی در یک بســتر توزیع شــده و غیرمتمرکز فعالیت می‌کند. تعریف کرد. اما به نظر می‌رســد برای نزدیک‌شــدن به رویکردی که مبنای قواعد ضــدپولشــویی در این حوزه اســت ضرورت دارد تعاریفی رسمی‌تر را برگزید. شبکه اقدام علیه جرایم مالی ایالات متحده این ارزها را با مؤلفه های کارکردی (و نه ماهیت) آن‌ها تعریف کرده اســت:« ارز مجازی در برخی شــرایط همانند ارز واقعی عمل می‌کند اما فاقد تمام ویژگی‌های ارز واقعی است؛ به ویژه آنکه ارز مجازی فاقد صلاحیت قانونی در نظام های حقوقی است.». اتحادیه اروپا در تعریف خود، بیان می دارد:« ارز مجازی جلوه دیجیتالی یک ارزش مرکزی یا مقام صلاحیتدار صادر و تضمین نشده، الزاماً به ارز قانونی شناخته

[1]. B`lockchain.

شده وابسته نبوده و واجد وضعیت حقوقی ارز یا پول نیست اما به عنوان واسطه مبادله که قابلیت انتقال، ذخیره و تجارت در فضای الکترونیکی را دارد، توسط اشخاص حقیقی و حقوقی پذیرفته شده است.

ارز مجازی نوعی ارز دیجیتال است که نمایانگر ارزشی است که ناشی یا دارای پشتوانه بانک مرکزی نیست یعنی توسط بانک مرکزی منتشر نمی‌شود، این نوع ارز به صورت دیجیتالی معامله می‌شود و کارکردهای آن عبارتند از:

الف. وسیله مبادله

ب. واحد محاسبه

ج. ذخیره ارزش

اگرچه این نوع از ارز کارکردهای ارز رایج یا همان پول را دارد اما تفاوت مهمی که با پول‌های واقعی یا ملموس مانند سکه و اسکناس دارند این است که پشتوانه دولت یا بانک مرکزی را ندارد البته با توجه به تحلیلی که در بخش پول ارائه شد پشتوانه دولتی بانک مرکزی یا پشتوانه دولتی نیز متحول شده و از شکل سنتی آن خارج شده است، به هر حال استفاده از این نوع پول یا ارز هنوز به اندازه لازم رایج نشده است که همانند پول واقعی استفاده شود و کارکرد حفظ ارزش آن بیشتر مورد توجه بوده است. مشکل دیگر وضعیت قانونی این نوع از پول یا ارز است به دلیل اینکه در بسیاری از کشورها قانونی محسوب نشده و یا هنوز وضعیت قانونی مشخصی ندارد مانند ایالات متحده، لذا همان طور که اشاره شد کارکرد حفظ ارزش آن بیشتر مورد توجه بوده است. انواع ارزهای مجازی با توجه به ارتباط و وابستگی آنها به ارزهای واقعی به دو نوع اصلی ارزهای مجازی قابل تبدیل و غیر قابل تبدیل تقسیم می شوند که در ادامه بررسی قرار می‌دهیم.

خصوصیات ارزهای مجازی در راستای ارتکاب جرم

بعضاً گروه‌های مجرمانه، به‌ویژه گروه‌های تروریستی نیز، از ویژگی‌های منحصربه‌فرد آن غافل نبوده‌اند. این امر موجب شده تا نهادهای فراملی درگیر در فرایند مقابله با پول شویی و تأمین مالی تروریسم، به فکر چاره‌جویی و ارائه راهکارهایی در این حوزه باشند. در گزارش مربوط به خطرات در حال ظهور تأمین مالی تروریسم که در سال ۲۰۱۵، توسط گروه اقدام مالی اف. ای. تی. اف منتشر شد[1]؛ ارزهای مجازی به عنوان یک خطر بالقوه جهت تأمین مالی تروریسم شناخته شدند. نهادهای اجرای

[1] . Financial Action Task Force (FATF)

قانون نیز نگران استفاده از این‌گونه ارزها جهت تأمین مالی تروریسم هستند و برخی وب‌سایت‌های وابسته به تروریست‌ها که وظیفه ترویج اهدای بیت‌کوین به این گروه‌ها را دارند، نیز مورد شناسایی قرار گرفته است. برخی از تحقیقات صورت گرفته، نیز حاکی از تلاش گروه‌های تروریستی جهت خرید سلاح با استفاده از ارزهای مجازی است، به دلیل سازوکار پنهان تراکنش‌های رمز ارزها، گروه‌های تروریستی و معاند می‌توانند برای مقاصد خویش، به‌راحتی از منابع داخلی و خارجی از طریق رمز ارزها اقدام به تأمین مالی کنند و دستگاه‌های اطلاعاتی توانایی شناسایی آن‌ها را نداشته باشند. با این وصف رمز ارزها دارای ویژگی‌های منحصربه‌فردی هستند که به‌سرعت جای خود را در میان مجرمان باز کرده اند که در ذیل به تبیین مهم‌ترین آن‌ها خواهیم پرداخت:

الف. سرعت و سهولت انجام معامله

پول‌شویی در رمز ارزها، پولشویان را قادر به انتقال وجوه غیرقانونی به‌سرعت و با هزینه کم می‌کند. همچنین رمز ارزها در خارج از مبادله امکان شناسایی و دسترسی را ندارند؛ به‌طورکلی ارزهای دیجیتال یک‌تکه کد کامپیوتری هستند که به صورت منحصربه‌فرد و بدون تکثیر طراحی شده است. در ارزهای دیجیتال گزارش‌های دیجیتالی مبنی بر تصدیق هویت گیرنده و فرستنده است، اما مجرمان می‌توانند از هویت جعلی استفاده کنند.

نتیجه این سهولت در استفاده از ارز مجازی در فعالیت ها، امکان اتحاد فراملی برای ارتکاب جرم است. بزهکاران می توانند در کشورهای مختلف زندگی کنند و یک تجارت مجرمانه را از طریق ارزهای مجازی اداره نمایند. در حقیقت، ارزهای مجازی بر خلاف ارزهای رایج و سنتی برخوردار از ویژگی پویایی فضایی هستند (صفاری، ۱۳۹۹: ۲۳۲) ، به عبارتی انتقالات در این سیستم به صورت فرد به فرد صورت می پذیرد و به طور میانگین درکمتر از ۱۰ دقیقه وجه از حساب فردی به فرد دیگر منتقل می شود. در صورت نیاز به سرعت بالاتر، هر فرد می تواند با تعریف کارمزدی برای تراکنش خود، سرعت انتقال وجه خود را افزایش دهد (قاسمی، ۱٤۰۰: ۳٦). در صورتی که در غیر از سیستم رمز ارزها، به دلیل بودن واسطه های مالی فراوان سرعت انتقال وجوه پایین تر است.

ب. غیرمتمرکز بودن ارزهای مجازی

ارزهای مجازی سامانه‌ای غیرمتمرکز دارند که هیچ واسط یا نهاد مرکزی (مانند بانک‌های مرکزی کشورها) در تولید، توزیع و کنترل آن نقشی ندارد. به عبارت بهتر شبکه‌های مبتنی بر بلاک چین به عنوان شبکه‌های همتا به همتا (نظیر به نظیر)، بدون

اجرای سـرورهای متمرکز مبادرت به انتقال اطلاعات در بسـتری نامتمرکز می‌نمایند. از این رو رمز ارزها مبتنی بر تمرکززدایی هسـتند و برخلاف ارزهای رسـمی بانک مرکزی آن را مدیریت نمی‌کند. تراکنش‌های رمز ارزها نیز به پشـتوانه زنجیره بلوکی و رمزنگاری، تأمین و تأیید می شود. درواقع یکی از مهم‌ترین دلایل فراگیر شدن ارز حذف هزینه‌های عملیاتی اضافی است که از سوی نهادهای واسط دریافت می‌شود.

به‌طور مثال به دلیل قرار نگرفتن بیت‌کوین در سـامانه‌های پرداخت سـنتی، تنظیم‌گری این حوزه را با مشـکلاتی همراه کرده است؛ زیرا این ارز مشمول قوانین مرتبط در این زمینه نمی شود. این امر در کنار ویژگی‌های منحصربه‌فردی که بیت‌کوین به ارمغان آورده، موجب افزایش جذابیت این ارز مجازی برای بزهکاران، به‌ویژه بزهکاران مالی - اقتصادی شده است (شاملو، ۱۳۹۹: ۲٤۸).

رمزارزها، پولی بدون پشتوانه و بر پایه پروتکل رمزنگاری شده است که توسط هیچ نهاد یا سازمانی مانند بانک مرکزی تولید و منتشر نمی‌شود و تنها با حل معادلات پیچیده ریاضی یا با عملیات استخراج (ماینینگ[1]) به منصه ظهور رسیده است (سلیمانی پور، ۱۳۹٦: ۱۷۰).

این رمز ارزها، خوشـایند کسـانی شـد که از تمرکزگرایی بانک مرکزی، نظارت و دسـت‌اندازی دولت‌ها در دارایی‌ها و نیز مقرره‌گرایی دوری می‌کردند. ازاین‌رو، رمز ارزها با گرایش فعالان مجازی، باندهای مجرمانه به‌ویژه پول‌شویان، سرمایه‌گذاران ماجراجو و دولت‌های تحت تحریم از جمله ایران، توسعه یافت و با توجه به سازوکار رمز ارزها این امکان برای متخلفین فراهم است تا پول غیرمشروع را از طریق فرآیند پول‌شویی وارد سیستم مالی کشور کنند.

ج. هویت پنهان و ناشناختگی مجرمان در ارزهای مجازی

منظور از مخفی بودن این فضا، این نیست که نمی‌توان آن را مشاهده کرد؛ بلکه مراد این است که این فضا قابلیت آن را دارد که بازیگران و نقش‌آفرینان آن به‌طور کامل و در کمال ناشناس ماندن و بدون بیم از آنکه شناخته شده یا مورد ردیابی و تعقیب قرار گیرند، اقدامات خود را به معرض اجرا گذارند. هر کاربری می‌تواند با مراجعه به یک ارائه‌کننده خدمات اینترنتِ حضـوری (کافی‌نت) و با استفاده از یک هویت ساختگی به صورت ناشناس و مخفی هرگونه اطلاعات مجرمانه و مضر را وارد این شبکه

[1]. Mining

سازد و پس از مدت‌زمانی اندک، بسیاری از رایانه‌ها را در سراسر جهان مبتلا سازد. نقض‌کنندگان محیط فضای سایبر از قابلیت اختفاء در چنین محیطی بسیار سود می‌برند و با استفاده از نقابی که امکانات فنی و ویژگی‌های فناوری در راستای امکان جعل و قلب هویت در اختیار آنان می‌گذارد و نیز با استفاده از سامانه‌های رایانه‌ای عمومی و یا رایانه‌های کارگذار آزادانه امکان ارتکاب بالقوه طیف وسیعی از انواع جرایمی را می‌یابند که وقتی این امکان با گسترة بی‌انتهای فضای سایبر در هم می‌آمیزد، موقعیت خطرناکی را با محیطی وسیع و مجرمانی بی‌شمار، پراکنده و ناشناس پدیدار می‌سازد (اله وردی، ۱۳۹۶:۲۵).

برخی از کاربران خدمات مالی به دلایل متعددی علاقه ای به استفاده از نام حقیقی خویش ندارند. دلایل عدم اعتماد به سیستم مالی طیف متنوعی است که در حالت خوشبینانه به دلیل دخالت‌های روز افزون دولت و دستگاه‌های دولتی در حریم خصوصی افراد منجر عدم اعتماد برخی از شهروندان به دولت و سیستم مالی و قوانین متعدد حاکم بر آن شده است و از اینکه در معرض چنین مقرراتی قرار بگیرند اجتناب می‌کنند برای نمونه اعمال استاندارد احراز هویت یا شناخت مشتری طیف‌های[1] دیگری را ایجاد می‌کنند که برای پنهان نمودن درآمدهای حاصل از اعمال مجرمانه نظیر فرار مالیاتی، تأمین مالی تروریسم و پولشویی از ابراز هویت خویش در سیستم‌های مالی قابل ردیابی همانند بانک‌ها پرهیز می‌کنند.

رمز ارزها نیز به‌مانند فضای مجازی از این قائده مستثنی نیستند و ناشناختگی و گمنامی را برای کاربران به ارمغان می‌آورند؛ به عبارتی انتقال وجه در این نوع ارزها غیرقابل تشخیص و امکان رهگیری آن به‌راحتی میسر نیست. به‌طور مثال اگر فردی از یک فروشگاه با رمز ارزها، کالایی را خریداری کند و فروشنده پس از دریافت وجه از ارسال کالا امتناع ورزد، خریدار امکان پیگیری حقوقی از مراجع قضایی به دلیل فقدان مستندات لازم را ندارد؛ چراکه آدرس‌ها دربردارنده هویت اصلی مالک نیستند و همچنین فروشنده می‌تواند در هر تراکنش از آدرس جدیدی استفاده کند، علاوه بر این هیچ نهادی متولی این امر نخواهد بود. سیستم‌های غیرمتمرکز به طور ویژه در معرض خطرات نا شناس ماندن هستند. درواقع، برخلاف خدمات مالی سنتی، هویت کاربران معمولاً ناشناخته است، گرچه در بیشتر موارد فقط نام مستعار است و هیچ واسطه تنظیم‌شده‌ای وجود ندارد که بتواند به عنوان «محافظ» برای کاهش خطرات عمل کند. برخی از دارایی‌هایی رمزنگاری شده مانند دش[2] و مونرو[3] و سایر «رمز ارزها» حتی فراتر هم می‌روند؛ زیرا کاملاً ناشناس طراحی‌شده‌اند؛ آدرس کیف پول، معاملات و اطلاعات مربوط به

[1] . Know your customer (KYC).
[2]. Dash
[3]. Monero

تراکنش‌ها به صورت عمومی در DL مربوطه ثبت نمی شوند و ویژگی‌هایی مثل نا شناس ماندن، جلوگیری از شنا سایی مالک قانونی و سودمندی برای پولشویان جذابیتی دوچندان دارد (فیضی چکاب، ۱٤۰۰: ۸۰).

سطوح مختلف ناشناس بودن در دارایی‌های رمزنگاری شده، ریسک مبارزه با پول‌شویی و مبارزه با تأمین مالی تروریسم را بالا برده و مبتنی بر این واقعیت هستند که آن ها در فضای اینترنت‌اند و به این معنی است که کاربران توانایی دارند تا با سرعت بیشتری در سطح جهان آن‌ها را معامله کنند.

د. بهره گیری بدون واسطه از کیف پول دیجیتالی

به دلیل عدم وجود نهادی واسطه‌گر همچون بانک، ایجاد حساب برای هیچ‌یک از طرفین که منجر به افشای هویت آن‌ها می‌شود نیز ضروری نیست، بلکه ساخت کیف پول می‌تواند به‌صورت کاملاً محرمانه و بدون افشای مشخصات فردی انجام گیرد. دلیل این موضوع آن است که برای ایجاد کیف پول، مراجعه حضوری به نهادی مانند بانک ضروری نیست و تمامی مراحل به‌صورت برخط و بدون شناسایی هویت واقعی اشخاص انجام می‌شود (فراتی، ۱۳۹۹: ٦۰).

رمز ارزها که بر روی بستر زنجیرهای بلوکی فعالیت می‌کنند؛ برای نقل و انتقال و هر فعل دیگری نیازمند وجود کیف پول دیجیتال است، کیف پول دیجیتال دارای کلید عمومی و خصوصی است و کلید خصوصی تنها راه ورود به حساب کاربری و کیف پول دیجیتال است. گفته شده است که تراکنش‌های مالی رمز ارزها بر روی کیف پول دیجیتال نامعلوم بوده و تنها به‌صورت سوابقی از اعداد، حروف و علامت‌های نامعلوم قابل مشاهده است که امکان شناسایی هویت اشخاص و تراکنش‌هایشان غیرقابل پیگیری است، از این‌رو بهترین ابزار برای جرایم به‌ویژه پول‌شویی است.

ه. فقدان امنیت و حریم شخصی

امنیت و حریم شخصی ارز رمزنگاری شده همواره از موضوعات مورد بحث بوده اند. یکی از مشکلات اصلی گسترش استفاده از آن مربوط به مسائل امنیتی آن می شود. ارز رمزنگاری شده همواره در معرض دزدی و حملات هکری قرار دارد. برای مثال در مواردی که شخصی کلید خصوصی فرد دیگری را برباید یا بدان دست یابد. البته باید توجه داشت این مسئله بیشتر مربوط به مخاطرات کلیه فناوری‌های نوین است. کما اینکه است از زمان ترویج استفاده از خدمات الکترونیکی و ارزهای دیجیتالی این امر صادق بوده لذا امنیت حساب‌های ارزهای رمزنگاری شده در واقع در ذات فناوری است چراکه

توسعه دهندگان فناوری، همواره در حال افزایش کارایی و رفع معایب آن هستند، اما هیچ فناوری کامل و بدون نقص نیست و در ضمن باید توجه داشت که با توسعه فناوری و افزایش سطح کارایی آن‌ها به تدریج چنین مخاطراتی نیز محدود شده یا کاهش می‌یابد. عدم حضور فیزیکی اشخاص در ارتباطات، تعاملات و مبادله ها، که به واسطه ظهور فناوری های نوین اطلاعاتی و ارتباطی در عصر اطلاعاتی بسیار در حال گسترش و رو به فزونی است، علی رغم فواید پیش گفته، جامعه بشری را با دغدغه های نوینی مواجه کرده است. در سبک های نوین ارتباطی، به ویژه در زمان بهره مندی اشخاص از قابلیت‌های فضای مجازی، دسترسی به حجم اطلاعات (خصوصی و عمومی) بیشتر، صرفا با حضور در این شبکه های مجازی برای همگان میسر شده است. این پدیده از سویی به منزله یک فرصت برای افزایش آگاهی افراد، توجه اندیشمندان فناوری های اطلاعاتی و جامعه شناسان را جلب کرده است و از سوی دیگر به منزله یک تهدید، در قالب رعایت نشدن حریم خصوصی کاربران شبکه های مجازی، جلوه کرده است. زیرا با وجود حداقل محدودیت، امکان کسب اطلاعات از حریم خصوصی افراد، عکس‌ها، لیست دوستان، محل زندگی و... فراهم می شود. از سوی دیگر، با توجه به افزایش دسترسی افراد به محتوای ایجاد شده در فضاهای مجازی و پنهان بودن هویت افراد استفاده کننده از این محتوا، بحث مالکیت فکری و متعاقب آن سوء استفاده‌های احتمالی از ایده دیگران، حساسیت بیشتری می یابد و به بیانی دیگر سرقت اطلاعات، ایده ها و افکار دیگران در فضای مجازی از جمله دیگر چالش‌های اخلاقی پیش روی جامعه اطلاعاتی است.

از جمله مسائل اساسی در بعد حقوقی فضای مجازی مسئله حریم خصوصی و آزادی است. به دلیل فقدان مدل بلوغ در نظامات فضای مجازی در کشور نظریه ها و حدود مشخصی برای حریم خصوصی و آزادی تعیین نشده است. برای مثال در دوران پست مدرن بروز ویژگی های جدید ناشناسی (گمنامی)، لامکانی، لازمانی و گسترش مخاطب پیام در فضای مجازی باعث ایجاد تغییرات اساسی در تعریف و حدود آزادی بیان شده است؛ اما متأسفانه به دلیل نبود مدل بلوغ مناسب در کشور نسبت به این حدود و تعریف شناخت کافی را نداریم (فیروزآبادی، ۱۳۹۹: ۳٤).

در حقوق ایران تعریف مشخص قانونی از حریم خصوصی ارائه نشده است و حریم خصوصی مستقلاً حمایت نشده و به تعبیری موضع تحول گرایانه اتخاذ شده و از مصادیق آن حمایت شده است. در مقام تعریف، تعاریف متعددی ارائه شده که فارغ از اختلاف موجود در تعاریف «وجه مشترک تعاریف ارایه شده اختیار و آزادی انسان در تصمیم گیری در خصوص میزان وقوف و مداخله سایرین نسبت به زندگی شخصی است (اصلانی، ۱۳۸۹: ۴۰)»؛ این وجه مشترک رکن اساسی حریم خصوصی است.

در نتیجه می‌توان گفت؛ عبارت است از؛ قلمرو و محدوده‌ای از اعمال، رفتارها، اندیشه‌ها، ویژگی‌ها و خصوصیات شخص که به وسیله قانون و عرف تعیین شده و بنا به مقتضیات زمان و مکان قابل تغییر بوده و برای عموم آشکار نبوده و مختص به آن فرد بوده ودر این محدوده از آزادی معقولانه ای برخوردار بوده و فارغ از بازخواست حقوقی و کیفری است و آن‌ها را افشا نکرده و انسان نوعی و متعارف تمایل به افشاء آن ندارد. لذا این حریم مصون از ورود، نگاه و نظارت دیگران و یا هرگونه تعرض است و از سان ورود و نظارت دیگران بر این فضا را برنمی‌تابند و نسبت به ورود غیر واکنش نشان می‌دهد، درنتیجه ورود به آن جز به حکم قانون یا رضایت وی جایز نمی‌باشد. درنتیجه امري را حریم خصوصي مي‌نامند که فرد بتواند دسترسي به آن را در کنترل خودش داشته باشد و حمایت از حریم خصوصي یعني حمایت در مقابل دسترسي ناخواسته به آن امر به وسیله دیگران. بنابراین شرط اساسی در شناخت حریم خصوصی دور از انظار عموم بودن و عدم جواز دخالت دیگران است؛ در واقع حریم خصوصی مبتنی بر دو حق اساسی؛ حق افراد در برابر تجاوز فیزیکی به تنهایی‌شان (از طریق ابزارهایی چون ورود غیرمجاز به خانه و محافل خصوصی، استراق سمع، بازجویی های غیرقانونی، فیلم برداری و عکس برداری غیر مجاز و غیره) و حق افراد در برابر نشر اطلاعات مربوط به آنها می‌باشد. از این رو حریم خصوصی تابع اوضاع و احوالی «ازجمله مکان مورد نظارت، موضوع مورد نظارت، استفاده‌ای که اطلاعات حاصل از نظارت ممکن است داشته باشد، وسایلی که برای نظارت مورد استفاده قرارمی‌گیرد، وضعیت شخصی که مورد نظارت واقع می‌شود، رضایت و روابط بین طرفین» است (انصاری، ۱۳۹۴:۲۴).

فضای سایبر، محیطی مجازی اما بسیار حساس و حساسیت برانگیز است. شاید بهره برداری بدون تفاوت و تبعیض از این فضاست که به مجرمین و منحرفین امکان داده، برای نتیجه گیری بهتر و مؤثرتر از نیات پلیدشان این چنین فضایی را در اولویت قرار دهند. در این آشفته بازار نیز بدیهی است که حریم داده های الکترونیکی شخصی و حتی عمومی و دولتی از این وضعیت مستثنی نبوده و آماج انواع تعرضات و آسیب ها قرار بگیرند.

حمایت از داده‌ها و اطلاعات[1] شخصی در فضای مجازی یکی از مهم ترین مباحث است. چرا که بدون وجود چنین حمایتی ورود به فضای مجازی و استقبال از فعالیت در آن به شدت کاهش می یابد، برای مثال در تجارت الکترونیکی که اعتماد سازی به آن از مهم ترین اهداف فعالان این عرصه است، اگر مصرف کنندگان از امنیت اطلاعاتی برخوردار نباشند از تجارت

[1] Data Protection.

الکترونیکی روی خواهند برگرداند (حبیب زاده، ٤٦:۱۳۹۰)، ولی این که حمایت از داده‌ها با مفهوم حریم خصوصی در فضای مجازی یکی باشد یا نه، نیازمند تدقیق و توجه بیشتری است.

حریم خصوصی یکی از مهم‌ترین حقوقی است که امروزه توسط اینترنت در معرض خطر قرار گرفته است. این فناوری جدید، امکانات بی‌سابقه ای را جهت تجاوز به حریم خصوصی افراد ایجاد کرده است. ارتباطات خصوصی افراد در این محیط مجازی ممکن است قطع شده و فایل‌های محرمانه که در کامپیوتر ذخیره شده و با اینترنت مرتبط گشته است از هر جایی در دنیا مورد دسترسی قرار گرفته یا کپی شود. همچنین کاربران با بی توجهی نسبت به اطلاعاتی که از خود در طی انجام فعالیت های اینترنتی باقی می‌گذارند، ممکن است موجبات سوء استفاده از داده‌های شخصی و خصوصی خود را فراهم آورند (کدخدایی، ۱۳۹۴: ۱۳۵).

یکی از نگرانی‌های اساسی در مورد اینترنت و فضای سایبر حفظ حریم شخصی افراد است؛ اطلاعات گوناگون که درباره داده ها نگهداری می‌شود از طریق نفوذ به این سیستم‌ها امکان سوء استفاده و ایجاد خطر را برای شهروندان به دنبال دارد (اجلالی، ۱۳۸۲: ۵۷). به هر حال ظهور شبکه‌ها به معنای تهدید بزرگ‌تر حریم اطلاعات و رابطه ای افراد در مقایسه با فنون قبلی ارتباطات است این تهدید ناشی از دسته بندی و ادغام پرونده‌ها و قابلیت ردگیری کارهای روزانه افراد است.

این به معنای به وجود آمدن ارزشی ضد ارزش به نام در دسترس بودن در هر مکان و زمان است که می‌توان رد افراد را تا عمیق ترین زوایای جامعه گرفت. اما این مسئله یک سوال آزاد باقی می‌گذارد که آیا اینترنت و فضای سایبر باعث افزایش یا کاهش دخالت چشم‌گیر در حریم خصوصی شخصی می‌شود؟ مطمناً یک پاسخ قوی وجود دارد که اینترنت عصر جدیدی در نظارت جمعی به وجود می‌آورد همچنین انگیزه‌های قوی تجاری در اینترنت برای کاهش حریم خصوصی وجود دارد بسیاری از مدل های رایج در این زمینه مفهوم بازاریابی «یک به یک» است که تولید انبوه بازار مدار را به تولید مبتنی بر خدمات شخصی تغییر داده و این یعنی تولید همه محصولات از کفش تا روزنامه به طور روز افزونی بر پایه خصوصیات فردی و آگاهی از اطلاعات شخصی صورت می‌گیرد. در این میان افراد هیچ راهی جز آشکار ساختن اطلاعات شخصی خود ندارند، با این حال نمی‌توان از این مطلب هم چشم پوشی کرد که اینترنت و فضای سایبر سکویی برای ایجاد اشکال جدید ارتباطی و رابطه دو سویه مهیا می‌کند که می‌تواند در حفاظت از حریم خصوصی به دقت ایجاد گردد. به عنوان نمونه روش های پرداخت پول به صورت ناشناس کارهای تجاری را بدون افشای اطلاعات شخصی قابل شناسایی ممکن می‌سازد.

در خ صوص نقض حریم خ صو صی در خدمات دولت الکترونیک هم باید بیان دا شت که، همان طور که در خ صوص حق حریم خصوصی دیدیم، یکی از حقوق اساسی بشر این حق می‌باشد، که وی را در مقابل تعرضات دیگران به حریم خصوصی اش و نیز مداخلات ناروای دولت‌ها مورد حمایت قرار می‌دهد. اما امروزه با گسترش ابزارهای اطلاع رسانی و استفاده گسترده از سرویس‌های، این حق به یکی از چالش انگیز ترین م سائل حقوقی تبدیل شده ا ست که قطعا حمایت های مدنی از حریم خ صو صی و حمایت از افراد در برابر انواع شیوه های نقض حریم خ صو صی آنها در این جوامع مجازی بخش جدایی ناپذیر حمایت از حریم خصوصی است. در معرض مخاطره قرار گرفتن حریم خصوصی افراد یکی از مشکلات اخلاقی است که با گسترش ارتباطات از طریق چنین خدمات الکترونیکی و مجازی بروز کرده است.

مدیریت بازارهای ارزهای مجازی

یکی از پیش شرط‌های ا ستفاده بیشتر سازمان‌های تروریستی از ارزهای مجازی، گسترش بازار ارزهای مجازی ا ست. ر شد مستمر بازار پولی به این معنی است که مقبولیت و اعتماد کاربران در این وضعیت معاملاتی در حال بهبود است. در حال حا ضر، به‌ویژه در مناطقی که سازمان‌های تروریستی فعال هستند، مقبولیت ارزهای رمزپایه همچنان پایین ا ست. خاورمیانه در حال حا ضر منطقه ای ا ست که حملات تروریستی در آن زیاد ا ست، با این حال، تقریباً هیچ د ستگاه خودپرداز بیت کوین در خاورمیا نه وجود ندارد. از ژانو یه ۲۰۱۸، تنها عربستان سعودی در خاورمیا نه دستگاه خودپرداز بیت کوین دارد (ربانی، ۱۴۰۲: ۱۲۱).

اگرچه تو سعه آینده فناوری ارزهای مجازی غیرقابل پیش بینی ا ست، اما اگر تعداد کاربرانی که از ارزهای دیجیتال ا ستفاده می کنند به میزان قابل توجهی در سراسر جهان افزایش یابد، سازمان های تروریستی احتمالاً استفاده از آنها را افزایش خواهند داد. علاوه بر این، یک حمله تروریستی واقعی بر استفاده جهانی از ارزهای دیجیتال نیز تأثیر خواهد گذاشت.

تجارت مواد مخدر به عنوان منبع اصلی تامین مالی فعالیت‌های سازمان‌های تروریستی ثابت کرده است که درآمد ماهانه ارزهای دیجیتال بین‌المللی می‌تواند به چندین میلیون دلار آمریکا از طریق فروش داروهای غیرقانونی برسد .ارز دیجیتال به دلیل ویژگی های منا سب به تدریج در بازار دارک وب مورد ا ستفاده قرار می گیرد. افزایش تراکنش ها در بازار دارک وب به طور اجتناب ناپذیری باعث تحریک استفاده از ارزهای دیجیتال توسط سازمان های تروریستی می شود. لذا مدیریت و کنترل

گسترش استفاده از ارزهای دیجیتال می تواند نقش مهمی در پیشگیری وضعی از تامین مالی تروریسم از طریق ارزهای دیجیتال داشته باشد.

راهکارهای پیشگیري اجتماعی از فعالیت‌های مجرمانه مرتبط با ارزهاي مجازي

پیش گیری اجتماعی به تغییر شرایط جرم زایی اجتماعی و ا صلاح نگرش‌ها و انگیزه‌های مجرمان تأکید می‌کند و اقدامات خود را بر توسعه طرح هایی مانند کلوپ‌های جوانان متمرکز می‌کند تا مجرمان بالقوه و یا بالفعل را از ارتکاب جرم منصرف کند هدف این نوع پیش گیری تقویت نهادهای اجتماعی و مؤسسات جامعه پذیر کننده برای تأثیرگذاری بر گروه‌هایی ا ست که بیشتر در معرض ارتکاب جرم هستند. پیش گیری اجتماعی بزه‌کار مدار ا ست بر خلاف پیش گیری و ضعی که بزه دیده مدارانه است؛ بدین ترتیب ملاحظه می‌شود که در پیش گیری وضعی از جرم به جای مقابله با انگیزه ارتکاب به جرم سعی در بستن راه‌های د ست یابی مرتکب به مو ضوع جرم و افزودن زحمت و خطر ارتکاب جرم و کم فایده کردن آن برای مرتکب می‌شود (موسوی مجاب، ۱۳۹۵: ۳٦۸). در مقابل، هدف از پیش‌گیري اجتماعي، حذف یا خنثي کردن آن دسته از عوامل اجتماعي هست که در تکوین بزه مؤثرند.

پیش‌گیري اجتماعي، ریشه‌هاي بزه‌کاري را نشانه مي‌گیرد و با ا ستمداد از هیئت اجتماع و از طریق شیوه‌هاي گوناگون، علل و عوامل مؤثر در فعلیت یافتن اندیشه مجرمانه را تحت نظارت درمی‌آورد. در حقیقت پیش‌گیري اجتماعي به‌طور مستقیم در مقام جلوگیري از مجرم شدن افراد است، یعني جلوگیري از تبدیل‌شدن بزهکاران بالقوه به بزهکاران بالفعل. پیش‌گیری اجتماعی به دود سته تقسیم می شود: پیش‌گیری جامعه مدار و پیش‌گیری ر شدمدار یا زودرس از طریق پیش‌گیری جامعه مدار سعی می‌کنیم ری شه‌ها و خوا ستگاه‌های اجتماعی جرم را که عمدتاً با حقوق ان سان مرتبط ا ست، حل کنیم. مثل حق تفریح سالم که در جوامع هرچه تفریحات سالم دا شته با شیم رفتارهای پرخا شگری کمتر ا ست. پیش‌گیری اجتماعی از جرم یکی از مو ضوعات ا صلی مطالعات اجتماعی ا ست که جایگاه ویژه‌ای در میان راهبردهای پیش‌گیرانه دارد؛ در اکثر متون غربی از این نوع پیشگیری با عنوان پیشگیری از جرم از طریق توسعه اجتماعی نام برده می شود. شورای اقتصادی و اجتماعی سازمان ملل متحد در ماده 25 قطعنامه شماره 2002/13 پیشگیری از جرم از طریق توسعه اجتماعی با روش‌هایی مانند: الف) استفاده از راهبردهای آموزش و آگاه سازی عمومی برای رواج فرهنگ قانون مداری و انعطاف در عین احترام به هویت های فرهنگی ب) ترویج عوامل حمایتی از طریق برنامه‌های جامع و موافق تو سعه اجتماعی و اقت صادی و ... تو صیه می‌کند. در ف ضای جهانی

شدن ، ساختارهای اجتماعی متحول می‌گردند و بر فرآیند جامعه‌پذیری افراد تأثیر می‌گذارند. جهانی شدن نه یک فرایند، بلکه ترکیبی پیچیده از فرایندهاست که علاوه بر گسترش روابط اجتماعی در سطح جهانی، گسترش روابط اجتماعی در سطح جهانی، گسترة تأثیرپذیری اجتماعی را نیز افزایش می‌دهد. تحولات گسترده و فراگیر در ساختار روابط و نهادهای اجتماعی موجب تضعیف مؤلفه‌های مؤثر بر پیش‌گیری اجتماعی از جرم که بر جامعه‌پذیری افراد جامعه و وجود وفاق بنیادین بر ارزش‌ها مبتنی ا ست، می‌گردد. پیش‌گیری اجتماعی از جرم به سبب ارتباط معنادار با عوامل تأثیرگذار اجتماعی، از پیامدهای تغییرات و تحولات اجتماعی گسترده تأثیر می‌پذیرد (نجفی توانا، ۱۳۹۱: ۷۳).

از میان انواع رویکردهای پیشگیری از جرم، گونه‌ی پیشگیری اجتماعی که از طریق توسعه‌ی شاخصه‌های اجتماعی و ارتقاء وضعیت رفاه و بهبود کیفیت زندگی افراد جامعه صورت می پذیرد، جایگاه ویژه ای در میان پژوهش‌های جرم شناختی و سیاستگذاری‌های جنایی یافته است. رویکرد پیشگیری اجتماعی از جرم، تقویت روابط اجتماعی، افزایش سطح کنترل غیررسمی اجتماعی و درنتیجه بازدارندگی بزهکاران بالقوه و بالفعل از ارتکاب جرم، است. پیشگیری اجتماعی از جرم بر بازسازگاری کسانی تمرکز دارد که در خطر بزهکاری قرار دارند و احساس یکپارچگی کمتری را با جامعه می‌کنند.

نتیجه گیری

رواج نسبی ارزهای مجازی در ایران سر آغاز بحث‌هایی در خصوص ابعاد گوناگون این فن آوری به ویژه از حیث حقوقی و جرم شناختی شده است. با این وجود موضع گیری متولیان امر در ابتدا منفعلانه و ناکارآمد بود و کندتر از بسیاری از کشورها رویکردهای معقولانه تری از حیث وضع قوانین و مقررات در خصوص ابعاد گوناگون ارزهای مجازی صورت پذیرفت، بر این اساس کنشگری تقنینی در ایران پیرامون ارزهای مجازی را می‌توان در چارچوبی از انفعال و ممنوعیت استفاده تا صدور اعلامیه های هشداردهی و آگاه سازی از ریسک‌ها و تلاش نافرجام جهت قاعده مندسازی تجاری دسته بندی کرد.

مقررات گذاری در خصوص مخاطرات جنایی ارزهای مجازی در ایران نیز از تفاوت‌های قابل توجهی با بسیاری کشورها برخوردار است، کنشگران سیاستگذار و مقرره گذار در ایران راهی دیگر را در پیش گرفتند. این رویکرد، با ممنوعیت استفاده و مبادله ارزهای مجازی با ا ستدلال قابلیت ا ستفاده پول شویی، آغاز شد که نوید دهنده توجه بیشتر به ارزهای مجازی از منظر مقررات پولشویی بود با این وجود، اقدامات بعدی که با انتشار پیش نویس سند الزامات و ضوابط فعالیت‌ها در حوزه ارزهای

[1]. Globalization

مجازی در کشور مورخ ۱۳۹۷/۱۱/۸ همراه شد نشانگر به حاشیه رانده شدن رویکرد مرتبط با پولشویی به ارزهای مجازی و تقویت رویکردی است که در تلاش است تا با ارز منظور ارزهای رایج مانند دلار و یورو محسوب کردن ارزهای مجازی آن‌ها را تحت شمول قوانین مربوط به ارز و از جمله قانون مبارزه با قاچاق کالا و ارز ۱۳۹۲ با اصلاحات و الحاقات بعدی درآورد.

امری که با الحاق یک تبصره (تبصره ۷ ماده ۲۰ مکرر الحاقی سال ۱۳۹۹ : تمامی رمزارزها (ارزهای رقومی) در حکم ارز موضوع این قانون هستند و جرائم، تخلفات، ضمانت اجراها و نیز تمامی احکام و مقررات مربوط به ارز در این قانون در مورد آن‌ها نیز اجراء می‌شود. به قانون مبارزه با قاچاق کالا و ارز و بیان صریح این امر نه تنها از حیث تقنینی فاقد سابقه در سایر کشورها است با در دستور کار قرار دادن رویکرد جرم انگاری پیش‌دستانه نیاز به تدوین و تصویب برخی مقررات را اجتناب ناپذیر کرده است.

منابع

آذرنژاد، مهدی(۱٤۰۱). **حقوق دارایی‌های رمز نگاری شـــده (مبانی، مقدمات، قواعد و مقررات)**، چاپ اول، تهران: مجمع علمی و فرهنگی مجد.

ابراهیمی، شهرام(۱۳۹٦). **جرم‌شناسی پیشگیری**، جلد اول، چاپ چهارم، تهران: بنیاد حقوقی میزان.

اجلالی، علی اکبر(۱۳۸۲). **شهر الکترونیک**، تهران: انتشارات دانشگاه علم و صنعت ایران.

ا صلانی، حمیدر ضا (۱۳۸۹). **حقوق فناوری اطلاعات**، چاپ دوم، تهران: انتشارات میزان با همکاری فناوری اطلاعات ریاست جمهوری.

الهوردی، فرهاد (۱۳۹٦). **حقوق کیفری سایبری**. چاپ اول. تهران: انتشارات جنگل.

انصاری، باقر(۱۳۹٤). **حقوق حریم خصوصی**، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).

بارانی، محمد (۱۳۹۳). **پیشگیری از جرایم جهانی تعهد بین المللی دولت‌ها**، چاپ اول، تهران: بنیاد حقوقی میزان.

بک، اولریش(۱۳۸۸). **جامعه در مخاطره جهانی**، مترجم: محمدرضا مهدی‌زاده، تهران، انتشارات کویر.

توسلی زاده، توران(۱۳۹٦). **پیشگیری از جرایم اقتصادی**، چاپ اول، تهران: انتشارات جنگل.

شیخ الا سلامی، عباس(۱۳۸۰). **جرایم مطبوعاتی: بررسی تطبیقی سیا ست جنایی ا سلامی و انگلستان**، چاپ اول، مشهد، انتشارات جهاد دانشگاهی.

جیشانکار، کی(۱۳۹٤). **جرم شنا سی فضای مجازی: کشف جرایم اینترنتی و رفتار مجرمانه**، ترجمه حمیدر ضا ملک محمودی، چاپ اول، بنیاد حقوقی میزان.

حبیب زاده، طاهر(۱۳۹۰). **حقوق فناوری اطلاعات مقدمه‌ای بر حقوق تجارت الکترونیک**، تهران: مرکز پژوهش های مجلس.

حسینی، سید محمد(۱۳۹۳). **سیاست جنایی در اسلام و جمهوری اسلامی ایران**، چاپ سوم، تهران: انتشارات سمت.

جعفرپور صادق، الهام(۱۳۹٤). **مطالعه جرم شناختی ارتشاء**، چاپ اول، تهران: بنیاد حقوقی میزان.

دارابی، شهرداد(۱۳۹۵). **پیشگیری از جرم در مدل مردم سالار سیاست جنایی**، چاپ اول، تهران، انتشارات میزان.