

Research Article

***Fundamentals of Criminalizing Crimes Related to Digital Currencies in
Iran with a Look at Its Jurisprudential Aspects***

Moharram Kokabi^۱, Babak Pourghahramani^۲, Fatemeh Ahadi^۳

Received: ۲۰۲۴/۰۶/۲۱ Accepted: ۲۰۲۴/۰۹/۱۹

Abstract

The distinctive characteristic of the third millennium and the era of information and communication technology can be considered the speed and diversity of advances and innovations; which always places the understanding of technological phenomena and activism towards their regularization several steps behind the developments. One of the most important examples of such phenomena can be considered cryptocurrencies, which, after more than a decade of their introduction and publication, still have many strategic gaps in terms of legal regularity and regulation. Undoubtedly, the lack of knowledge of the characteristics, functions, and newness of the underlying technology of this technology, namely blockchain, has played a significant role in the formation of such an environment. However, some countries have tried to adopt an active and dynamic approach to policymaking in this area; an approach that indicates active activism towards cryptocurrencies. In this regard, one of the most important and controversial aspects of interventions in the field of digital currencies is criminal intervention through criminalization of some of the risks of this technology; which requires justification due to the restriction of freedoms in order to identify the necessities of criminalization in the field of cryptocurrencies. Accordingly, the upcoming research will examine the necessities of criminalization and the manifestations of crimes in the field of cryptocurrencies using a descriptive and analytical method.

Keywords: *Digital currencies, Iran's criminal policy, criminalization.*

^۱ - PhD student, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran.

^۲ - Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. (Corresponding Author).

^۳ - Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran.

مقاله پژوهشی

مبانی جرم انگاری جرایم مرتبط با ارزش‌های دیجیتال در ایران با نگاهی به ابعاد فقهی آن

مبانی فقهی حقوق اسلامی

محرم کوبی^۴، بابک پورقهرمانی^۵، فاطمه احدی^۶

چکیده

مشخصه بارز هزاره سوم و عصر فناوری اطلاعات و ارتباطات را می‌توان سرعت و تنوع در پیشرفت‌ها و نوآوری‌ها دانست؛ امری که شناخت پدیده‌های فناورانه و کنشگری جهت قاعده‌مندی آن‌ها را همواره چندین گام عقب‌تر از تحولات قرار می‌دهد. یکی از مهم‌ترین مثال‌ها از چنین پدیده‌هایی را می‌توان رمزارزها دانست که با گذشت بیش از یک دهه از معرفی و انتشار، همچنان از حیث قاعده‌مندی حقوقی و تنظیم‌گری، از خلأهای راهبردی بسیاری برخوردارند. بی‌تردید در شکل‌گیری چنین فضایی، ناشناختگی ویژگی‌ها، کارکردها و نوظهوری فناوری زمینه‌ساز این فناوری، یعنی بلاک‌چین، نقش قابل توجهی داشته است. با این حال، برخی کشورها تلاش کرده‌اند تا با اتخاذ رویکردی فعال و پویا به سیاست‌گذاری در این حوزه پردازند؛ رویکردی که نشانگر کنشگری فعال در برابر رمزارزهاست. در این راستا یکی از مهم‌ترین و بحث‌برانگیزترین جنبه مداخلات در زمینه ارزش‌های دیجیتال، مداخله کیفری از طریق جرم‌انگاری پیرامون برخی از مخاطرات این فناوری است؛ امری که به دلیل تحدید آزادی‌ها نیازمند توجیه است تا از گذر آن، ضرورت‌های جرم‌انگاری در حوزه رمزارزها شناسایی گردد. بر این اساس، در پژوهش پیش رو با روشی توصیفی و تحلیلی به بررسی ضرورت‌های جرم‌انگاری و جلوه‌های جرایم در حوزه رمزارزها پرداخته می‌شود.

واژگان کلیدی: ارزش‌های دیجیتال، سیاست جنایی ایران، جرم انگاری.

^۴ - دانشجوی دکتری، گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

^۵ - دانشیار، گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. (نویسنده مسئول)

b.pourghahramani@yahoo.com

^۶ - دانشیار، گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

در جهان امروز فناوری با سرعت شگرفی در حال پیشرفت است. بزهکاران این موقعیت 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 مرزهای جغرافیایی یک کشور، فرایند جهانی‌شدن بزهکاری را تسریع کرده است. ابداع ارزشهای مجازی به فرایند مزبور سرعت بخشیده است. ارزشهای مجازی با ادعای هم‌ردیف قرارگرفتن با ارزشهای متعارف (دولتی)، در تلاش‌اند تا تابوهای سنتی تولید و توزیع پول توسط دولت‌ها را بشکنند و ارزی غیررسمی با قابلیت تولید توسط کاربران فراهم آورند. ارزشهای 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 گونه‌های ارزشهای مجازی، وارد حوزه‌های جدیدتری برای تأمین مالی در معنای پول شده‌اند که به دلیل عدم قرار گرفتن بیت کوین در سامانه‌های پرداخت سنتی، مقررہ گذاری این حوزه را با مشکلاتی همراه ساخته است؛ زیرا، این ارز مشمول قوانین مرتبط در این زمینه نمی‌شود. این امر، در کنار ویژگی‌های منحصر به 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 راه‌های 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. مزیت‌های پولشویی از طریق اینترنت این است که کمیت تراکنش‌ها به میزان دلخواه قابل افزایش است و می‌تواند از یک نقطه دور صورت بگیرد و علاوه بر این‌ها بی‌نام انجام شود. ناشناس ماندن هویت در تراکنش‌های مالی مشخصه ضروری پول شویی است. رویکرد «مستتری خود را شناس» 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 ناشناس استفاده کنند. افراد و گروه‌هایی 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 مناسب این حرکت عمل می‌کند. پول الکترونیکی یک پدیده غیر قانونی نیست بلکه در واقع پایه سیستم مالی جهانی کنونی است. هر چه پول الکترونیکی ناشناس‌تر باشد، احتمال انجام پولشویی بیشتر می‌شود. بسته به نوع و ارائه‌کننده 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 ارزشهای 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. ارزشهای مجازی روند عادی ارزشهای 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.

رویکرد ایران در قبال ارزشهای مجازی؛ از رویکرد منفعلانه تا رویکرد واکنشی بوده است. رویکرد سیاستگذاری در ایران نسبت به ارزشهای مجازی در ابتدا ممنوعیت استفاده از آن بود. براین اساس در جلسه سی ام شورای عالی مبارزه با پولشویی در تاریخ ۱۳۹۶/۱۰/۹ به کارگیری ابزار بیت کوین و سایر ارزشهای 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 ارزشهای 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. با این حال نمونه کامل ارز مجازی بیت کوین است که برخی ویژگی‌ها آن را از سایر ارزشهای مجازی متمایز می‌کند. از این رو در پژوهش حاضر با روشی توصیفی - تحلیلی به ارائه راهکارهای پیشگیرانه وضعی و اجتماعی پیرامون جرایم مرتبط با ارزشهای مجازی با محوریت بیت کوین 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 ارزشهای مجازی برای انجام فعالیت‌های مجرمانه می‌شود؟ راهکارهای پیشگیرانه از فعالیت مجرمانه مرتبط با ارزشهای مجازی منطبق با سیاست جنایی ایران چیست؟

مفهوم ارزشهای مجازی

ارزهای مجازی به دلیل مفاهیم فناوری نوآورانه خود، سؤالات حقوقی جدیدی را مطرح می‌کنند. یکی از چالش مهم در حوزه ارزشهای دیجیتال روند رو به گسترش آنها می‌باشد به نحوی که با توجه به تعداد زیاد (و به طور مداوم در حال رشد) سیستم‌های به اصطلاح «ارز رمزنگاری» با ویژگی‌های فناوری متفاوت، ارائه تعریف اصطلاح «ارز دیجیتال» کار آسان 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، ارزی هستند که به صورت 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. در نتیجه از نظر حقوقی عبارت «ارز دیجیتالی» یک عبارت موسع است.

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 است که بر بستری دیجیتال، غیرمتمرکز و شفاف به نام زنجیره بلوک موجودیت می‌یابد. این دارایی‌ها می‌توانند در شرایطی کارکرد پولی به خود بگیرند.

ماهیت ارزهای مجازی

اقتصاد کشورها امروزه متکی به پول اعتباری است که حکومت‌ها منتشر می‌کنند. 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 استفاده از هر نوعی از انواع پول یک نوع قرارداد اجتماعی بین اعضای جامعه بر پذیرش و استفاده 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.

در واقع هیچ تعریف جهان شمولی از ارز مجازی وجود ندارد و اصولاً بسیاری از کشورها بر سر استفاده از عنوان ارز نیز اختلاف دارند و برخی از آن‌ها در عوض از عبارت دارایی‌های رمزی استفاده می‌کنند. در گام نخست می‌توان ارزهای مجازی را سامانه ارزی که از رمزنگاری برای انتقال امن و مبادله رمزهای دیجیتالی در یک بستر توزیع شده و غیرمتمرکز فعالیت می‌کنند. تعریف کرد. اما به نظر می‌رسد برای نزدیک شدن به رویکردی که مبنای قواعد ضد پولشویی در این حوزه است ضرورت دارد تعاریفی رسمی‌تر را برگزید. شبکه اقدام علیه جرایم مالی ایالات متحده این ارزها را با مؤلفه‌های کارکردی (و نه ماهیت) آن‌ها تعریف کرده است: «ارز مجازی در

برخی شرایط همانند ارزش واقعی عمل می‌کند اما فاقد تمام ویژگی‌های ارزش واقعی است؛ به ویژه آنکه ارزش مجازی فاقد صلاحیت قانونی در نظام های حقوقی است.»

اتحادیه اروپا در تعریف خود، بیان می‌دارد: «ارزش مجازی جلوه دیجیتالی یک ارزش مرکزی یا مقام صلاحیتدار صادر و تضمین نشده، الزاماً به ارزش قانونی شناخته شده وابسته نبوده و واجد وضعیت حقوقی ارزش 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.

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

الف. وسیله مبادله

ب. واحد محاسبه

ج. ذخیره ارزش

اگرچه این نوع از ارزش کارکردهای ارزش 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 ارزش 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 ارزش 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 ارزشهای مجازی با توجه به ارتباط و وابستگی آنها به ارزشهای واقعی به دو نوع اصلی ارزشهای مجازی قابل تبدیل و غیر قابل تبدیل تقسیم می‌شوند که در ادامه بررسی قرار می‌دهیم.

خصوصیات ارزشهای مجازی در راستای ارتکاب جرم

بعضاً گروه‌های مجرمانه، به‌ویژه گروه‌های تروریستی نیز، از ویژگی‌های منحصر به فرد آن غافل نبوده‌اند. این امر موجب شده تا نهادهای فراملی درگیر در فرایند مقابله با پول‌شویی 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؛ ارزشهای مجازی به عنوان یک خطر بالقوه جهت تأمین مالی تروریسم شناخته شدند. نهادهای اجرای قانون نیز نگران استفاده از این گونه ارزشها

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 ارزشهای مجازی است، به دلیل سازوکار پنهان تراکنش‌های رمز ارزها، گروه‌های تروریستی و معاند می‌توانند برای مقاصد خویش، به راحتی 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 منحصر به فردی هستند که به سرعت جای خود را در میان مجرمان باز کرده اند که در ذیل به تبیین مهم‌ترین آن‌ها خواهیم پرداخت:

الف. سرعت و سهولت انجام معامله

پول شویی در رمز ارزها، پولشویان را قادر به انتقال وجوه غیرقانونی به سرعت و با هزینه کم می‌کند. همچنین رمز ارزها در خارج از مبادله امکان شناسایی و دسترسی را ندارند؛ به‌طور کلی ارزشهای دیجیتال یک‌تکه کد کامپیوتری هستند که به صورت منحصر به فرد و بدون تکثیر طراحی شده است. در ارزشهای 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 فعالیت‌ها، امکان اتحاد فراملی برای ارتکاب جرم است. بزهکاران می‌توانند در کشورهای مختلف زندگی کنند و یک تجارت مجرمانه را از طریق ارزشهای مجازی اداره نمایند. در حقیقت، ارزشهای مجازی بر خلاف ارزشهای رایج و سنتی برخوردار از ویژگی پویایی فضایی هستند، به عبارتی انتقالات در این سیستم به صورت فرد به فرد صورت می‌پذیرد و به طور میانگین در کمتر از ۱۰ دقیقه وجه از حساب فردی به فرد دیگر منتقل می‌شود. در صورت نیاز به سرعت بالاتر، هر فرد می‌تواند با تعریف کارمزدی برای تراکنش خود، سرعت انتقال وجه خود را افزایش دهد. در صورتی که در غیر از سیستم رمز ارزها، به دلیل بودن واسطه‌های مالی فراوان سرعت انتقال وجوه پایین تر است.

ب. غیرمتمرکز بودن ارزشهای مجازی

ارزشهای مجازی سامانه‌ای غیرمتمرکز دارند که هیچ واسطه 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 سرورهای متمرکز مبادرت به انتقال اطلاعات در بستری نامتمرکز می‌نمایند. از این رو رمز ارزها مبتنی بر تمرکززدایی هستند و برخلاف ارزشهای رسمی بانک مرکزی آن را مدیریت نمی‌کند. تراکنش‌های رمز ارزها نیز به پشتوانه زنجیره بلوکی و رمزنگاری، تأمین و تأیید می‌شود. در واقع یکی از مهم‌ترین دلایل فراگیر شدن ارز حذف هزینه‌های عملیاتی اضافی است که از سوی نهادهای واسطه دریافت می‌شود.

به‌طور مثال به دلیل قرار نگرفتن بیت‌کوین در سامانه‌های پرداخت سنتی، تنظیم‌گری این حوزه را با مشکلاتی همراه کرده است؛ زیرا این ارز مشمول قوانین مرتبط در این زمینه نمی‌شود. 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.

رمزارها، 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) به منصفه ظهور رسیده است.

این رمز ارزها، خوشایند کسانی شد که از تمرکزگرایی بانک مرکزی، نظارت و دست‌اندازی دولت‌ها در دارایی‌ها و نیز مقرره‌گرایی دوری می‌کردند. از این‌رو، 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 اینترنتی حضور (کافی‌نت) و با استفاده از یک هویت ساختگی به صورت ناشناس و مخفی هرگونه اطلاعات مجرمانه و مضر را وارد این شبکه 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 گستره بی‌انتهای فضای سایبر در هم می‌آمیزد، موقعیت خطرناکی را با محیطی وسیع و مجرمانی بی‌شمار، پراکنده و ناشناس پدیدار می‌سازد.

برخی از کاربران خدمات مالی به دلایل متعددی علاقه‌ای 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 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 به مانند فضای مجازی از این قاعده 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 به راحتی میسر نیست. به طور 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 ناشناس ماندن هستند. در واقع، 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 دس و مونرو و سایر «رمز ارزها» حتی فراتر هم می‌روند؛ زیرا کاملاً ناشناس طراحی شده‌اند؛ آدرس کیف پول، معاملات و اطلاعات مربوط به تراکنش‌ها به صورت عمومی در DL مربوطه ثبت نمی‌شوند و ویژگی‌هایی مثل ناشناس ماندن، جلوگیری از شناسایی مالک قانونی و سودمندی برای پولشویان جذابیتهای دوچندان دارد.

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 آن‌ها در فضای اینترنت‌اند و به این معنی است که کاربران توانایی دارند تا با سرعت بیشتری در سطح جهان آن‌ها را معامله کنند.

د. بهره‌گیری 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 به صورت 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 به صورت برخط و بدون شناسایی هویت واقعی اشخاص انجام می‌شود.

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

ه. فقدان امنیت و حریم شخصی

امنیت و حریم شخصی ارزش رمزنگاری شده همواره از موضوعات مورد بحث بوده اند. یکی از مشکلات اصلی گسترش استفاده از آن مربوط به مسائل امنیتی آن می شود. ارزش رمزنگاری شده همواره در معرض دزدی و حملات هکری قرار دارد. برای مثال در مواردی که شخصی کلید خصوصی فرد دیگری را برآید یا بدان دست یابد. البته باید توجه داشت این مسئله بیشتر مربوط به مخاطرات کلیدهای فناوری-های نوین است. کما اینکه است از زمان ترویج استفاده از خدمات الکترونیکی و ارزشهای دیجیتالی این امر صادق بوده لذا امنیت حساب-های ارزشهای 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 آن-ها به تدریج چنین مخاطراتی نیز محدود شده یا کاهش می-یابد.

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 قابلیت-های فضای مجازی، دسترسی به حجم اطلاعات (خصوصی و عمومی) بیشتر، صرفاً 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، عکس-ها، 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 استفاده-های 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 چالش-های 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.

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 آرایه شده اختیار و آزادی انسان در تصمیم گیری در خصوص میزان وقوف و مداخله سایرین نسبت به زندگی شخصی است»؛ 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 و در این محدوده از آزادی معقولانه‌ای 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 انسان ورود و نظارت دیگران بر این فضا را بر نمی‌تابند و نسبت به ورود غیر واکنش نشان می‌دهد، در نتیجه ورود به آن جز به حکم قانون یا رضایت وی جایز نمی‌باشد. در نتیجه امری را حریم خصوصی می‌نامند که فرد بتواند دسترسی به آن را در کنترل خودش داشته باشد و حمایت از حریم خصوصی یعنی حمایت در مقابل دسترسی 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، بازجویی‌های 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 «از جمله مکان مورد نظارت، موضوع مورد نظارت، استفاده‌ای که اطلاعات حاصل از نظارت ممکن است داشته باشد، وسایلی که برای نظارت مورد استفاده قرار می‌گیرد، وضعیت شخصی که مورد نظارت واقع می‌شود، رضایت و روابط بین طرفین» است.

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

حمایت از داده‌ها و اطلاعات شخصی در فضای مجازی یکی از مهم‌ترین مباحث است. چرا که بدون وجود چنین حمایتی ورود به فضای مجازی و استقبال از فعالیت در آن به شدت کاهش می‌یابد، برای مثال در تجارت الکترونیکی که اعتماد سازی به آن از مهم‌ترین اهداف فعالان این عرصه است، اگر مصرف‌کنندگان از امنیت اطلاعاتی برخوردار نباشند از تجارت الکترونیکی روی خواهند برگرداند، 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 بی‌سابقه‌ای 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 بی‌توجهی نسبت به اطلاعاتی که از خود در طی انجام فعالیت‌های اینترنتی باقی می‌گذارند، ممکن است موجبات سوء استفاده از داده‌های شخصی و خصوصی خود را فراهم آورند.

یکی از نگرانی‌های اساسی در مورد اینترنت و فضای سایبر حفظ حریم شخصی افراد است؛ اطلاعات گوناگون که درباره داده‌ها نگهداری می‌شود از طریق نفوذ به این سیستم‌ها امکان سوء استفاده و ایجاد خطر را برای شهروندان به دنبال دارد. به هر حال ظهور شبکه‌ها به معنای تهدید بزرگ‌تر حریم اطلاعات و رابطه‌ای 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 عمیق‌ترین 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؟ مطمئناً 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 مدل‌های 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 چشم‌پوشی 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 روش‌های پرداخت پول به صورت ناشناس کارهای تجاری را بدون افشای اطلاعات شخصی قابل شناسایی ممکن می‌سازد.

در خصوص نقض حریم خصوصی در خدمات دولت الکترونیک هم باید بیان داشت که، همان‌طور که در خصوص حق حریم خصوصی دیدیم، یکی از حقوق اساسی بشر این حق می‌باشد، که وی را در مقابل تعرضات دیگران به حریم خصوصی‌اش و نیز مداخلات ناروای دولت‌ها مورد حمایت قرار می‌دهد. اما امروزه با گسترش ابزارهای اطلاع‌رسانی و استفاده گسترده از سرویس‌های، این حق به یکی از چالش‌انگیزترین مسائل حقوقی تبدیل شده است که قطعاً حمایت‌های مدنی از حریم خصوصی و حمایت از افراد در برابر انواع شیوه‌های نقض حریم خصوصی آنها در این جوامع مجازی بخش جدایی‌ناپذیر 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 ارزشهای مجازی

یکی از پیش‌شرط‌های استفاده بیشتر سازمان‌های تروریستی از ارزشهای مجازی، گسترش بازار ارزشهای مجازی است. رشد مستمر بازار پولی به این معنی است که مقبولیت و اعتماد کاربران در این وضعیت معاملاتی در حال بهبود است. در حال حاضر، به‌ویژه در مناطقی که سازمان‌های تروریستی فعال هستند، مقبولیت ارزشهای رمزپایه همچنان پایین است. خاورمیانه در حال حاضر منطقه‌ای است که حملات تروریستی در آن زیاد است، با این

حال، تقریباً هیچ دستگاه خودپرداز بیت کوین در خاورمیانه وجود ندارد. از ژانویه ۲۰۱۸، تنها عربستان سعودی در خاورمیانه دستگاه خودپرداز بیت کوین دارد.

اگرچه توسعه آینده فناوری ارزهای مجازی غیرقابل پیش بینی است، اما اگر تعداد کاربرانی که از ارزهای دیجیتال استفاده 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 فعالیت های سازمان های تروریستی ثابت کرده است که درآمد ماهانه ارزهای دیجیتال بین المللی می تواند به چندین میلیون دلار آمریکا از طریق فروش داروهای غیرقانونی برسد. ارز دیجیتال به دلیل ویژگی های مناسب به تدریج در بازار دارک وب مورد استفاده 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 پیشگیری اجتماعی از فعالیت های مجرمانه مرتبط با ارزهای مجازی

پیش گیری اجتماعی به تغییر شرایط جرم زایی اجتماعی و اصلاح نگرش ها و انگیزه های مجرمان تأکید می کند و اقدامات خود را بر توسعه طرح هایی مانند کلپ های جوانان متمرکز می کند 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 گروه هایی است که بیشتر در معرض ارتکاب جرم هستند.

پیش گیری اجتماعی بزه کار مدار است بر خلاف پیش گیری وضعی که بزه دیده مدارانه است؛ بدین ترتیب ملاحظه می شود که در پیش گیری وضعی از جرم به جای مقابله با انگیزه ارتکاب به جرم سعی در بستن راه های دست یابی مرتکب به موضوع جرم و افزودن زحمت و خطر ارتکاب جرم و کم فایده کردن آن برای مرتکب می شود.

در مقابل، هدف از پیش گیری اجتماعی، حذف یا خنثی کردن آن دسته از عوامل اجتماعی هست که در تکوین بزه مؤثرند.

پیش گیری اجتماعی، ریشه های بزه کاری را نشانه می گیرد و با استمداد از هیئت اجتماع و از طریق شیوه های گوناگون، علل و عوامل مؤثر در فعلیت یافتن اندیشه مجرمانه را تحت نظارت درمی آورد. در حقیقت پیش گیری اجتماعی به طور مستقیم در مقام جلوگیری از مجرم شدن افراد است، یعنی جلوگیری از تبدیل شدن بزهکاران بالقوه به بزهکاران بالفعل.

پیش گیری اجتماعی به دودسته تقسیم می شود: پیش گیری جامعه مدار و پیش گیری رشدمدار یا زودرس از طریق پیش گیری جامعه مدار سعی می کنیم ریشه ها و خواستگاه های اجتماعی جرم را که عمدتاً با حقوق انسان مرتبط

است، حل کنیم. مثل حق تفریح سالم که در جوامع هرچه تفریحات سالم داشته باشیم رفتارهای پرخطر کمتری است.

پیش‌گیری اجتماعی از جرم یکی از موضوعات اصلی مطالعات اجتماعی است 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 می‌شود. شورای اقتصادی و اجتماعی سازمان ملل متحد در ماده ۲۵ قطعنامه شماره ۲۰۰۲/۱۳ پیش‌گیری از جرم از طریق توسعه اجتماعی با روش‌هایی مانند: الف) استفاده از راهبردهای آموزش و آگاه‌سازی عمومی برای رواج فرهنگ قانون‌مداری و انعطاف در عین احترام به هویت‌های فرهنگی ب) ترویج عوامل حمایتی از طریق برنامه‌های جامع و موافق توسعه اجتماعی و اقتصادی و ... توصیه می‌کند.

در فضای 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، گستره 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 است، می‌گردد. پیش‌گیری اجتماعی از جرم به سبب ارتباط معنادار با عوامل تأثیرگذار اجتماعی، از پیامدهای تغییرات و تحولات اجتماعی گسترده تأثیر می‌پذیرد.

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 می‌پذیرد، جایگاه ویژه‌ای در میان پژوهش‌های جرم‌شناختی و سیاست‌گذاری‌های جنایی یافته است. رویکرد پیش‌گیری اجتماعی از جرم، تقویت روابط اجتماعی، افزایش سطح کنترل غیررسمی اجتماعی و در نتیجه بازدارندگی بزهکاران بالقوه و بالفعل از ارتکاب جرم، است. پیش‌گیری اجتماعی از جرم بر بازسازی‌گری کسانی تمرکز دارد که در خطر بزهکاری قرار دارند و احساس یکپارچگی کمتری را با جامعه می‌کنند.

نتیجه‌گیری

رواج نسبی ارزش‌های مجازی در ایران سر آغاز بحث‌هایی در خصوص ابعاد گوناگون این فن‌آوری به ویژه از حیث حقوقی و جرم‌شناختی شده است. با این وجود موضع‌گیری متولیان امر در ابتدا منفعلانه و ناکارآمد بود و کندتر از بسیاری از کشورها رویکردهای معقولانه‌تری از حیث وضع قوانین و مقررات در خصوص ابعاد گوناگون ارزش‌های مجازی صورت پذیرفت، بر این اساس کنشگری تقنینی در ایران پیرامون ارزش‌های مجازی را می‌توان در چارچوبی از انفعال و ممنوعیت استفاده تا صدور اعلامیه‌های هشداردهی و آگاه‌سازی از ریسک‌ها و تلاش نافرجام جهت قاعده‌مندسازی تجاری دسته‌بندی کرد.

مقررات‌گذاری در خصوص مخاطرات جنایی ارزش‌های مجازی در ایران نیز از تفاوت‌های قابل توجهی با بسیاری کشورها برخوردار است، کنشگران سیاستگذار و مقررگذار در ایران راهی دیگر را در پیش گرفتند. این رویکرد،

با ممنوعیت استفاده و مبادله ارزهای مجازی با استدلال قابلیت استفاده 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 فعالیت آنها در حوزه ارزهای 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 رقمی) 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 می-شود. 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 پیش-دستانه نیاز به تدوین و تصویب برخی مقررات را اجتناب ناپذیر کرده است.

منابع

۱. برومند، شهرزاد و همکاران، امنیت اقتصادی در ایران و چند کشور منتخب (مطالعه تطبیقی)، تهران، مطالعات اقتصادی مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۷ ش.
 ۲. بک، اولریش، جامعه در مخاطره جهانی، ترجمه محمدرضا مهدی‌زاده، تهران، کویر، ۱۳۸۸ ش.
 ۳. پاک‌نهاد، امیر، سیاست جنایی ریسک‌مدار، تهران، میزان، ۱۳۸۸ ش.
 ۴. پردل، ژان، تاریخ اندیشه‌های کیفری، ترجمه علی حسین نجفی ابرندآبادی، چاپ یازدهم، تهران، سمت، ۱۳۹۹ ش.
 ۵. خلیلی پاجی، عارف، «امکان‌سنجی تأمین مالی تروریسم در پرتو ارزهای مجازی»، مندرج در: مجموعه مقالات همایش بین‌المللی ابعاد حقوقی - جرم‌شناختی تروریسم، تهران، دانشگاهی علامه طباطبایی، ۱۳۹۸ ش.
 ۶. دلماس مارتی، می‌ری، نظام‌های بزرگ سیاست جنایی، برگردان علی حسین نجفی ابرندآبادی، چاپ دوم، تهران، میزان، ۱۳۹۸ ش.
 ۷. رهبریور، محمدرضا، «مبانی فقهی ممنوعیت و جرم‌انگاری در قلمروی اخلاق زیستی»، فصلنامه حقوق اسلامی، سال یازدهم، شماره ۴۲، پاییز ۱۳۹۳ ش.
 ۸. سیاه‌بیدی کرمانشاهی و دیگران، حقوق کیفری اقتصادی، تهران، جاودانه، ۱۳۹۷ ش.
- سیاه‌بیدی کرمانشاهی و دیگران، محشای قانون مبارزه با قاچاق کالا و ارز، تهران، جاودانه، ۱۳۹۸ ش.

- سیاه‌بیدی کرمانشاهی، سعید، و احمدعلی ثالث مؤید، حقوق کیفری اقتصادی؛ پول‌شویی، تهران، میزان، ۱۳۹۶ ش.
- شاملو، باقر، و عارف خلیلی پاچی، «مجازی شدن بزهکاری یقه‌سفیدی در پرتو ارزش‌های مجازی»، مجله حقوقی دادگستری، دوره هشتاد و چهارم، شماره ۱۱۰، تابستان ۱۳۹۹ ش.
- شاهیده، فرهاد، و امیرحسین نیازپور، «جرم‌انگاری پیش‌دستانه اعمال تروریستی»، آموزه‌های حقوق کیفری، مشهد، دانشگاه علوم اسلامی رضوی، دوره هفدهم، شماره ۱۹، بهار و تابستان ۱۳۹۹ ش.
- صیقل، یزدان، مطالعه حقوقی - جرم‌شناختی جرم در جامعه مخاطره‌آمیز، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۹۷ ش.
- فرح‌بخش، مجتبی، تأثیر فایده‌گرایی بر جرم‌انگاری، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشگاه تهران، ۱۳۸۹ ش.
- لارنت چیتن، پیتر و همکاران، پیشگیری از پولشویی و تأمین مالی تروریسم؛ راهنمای عملی برای ناظران بانکی، ترجمه مریم کشتکار، تهران، تاش، ۱۳۹۲ ش.
- محمودی جانکی، فیروز، و مهرانگیز روستایی، «توجیه مداخله کیفری؛ اصول و ضرورت‌ها»، پژوهش حقوق کیفری، سال دوم، شماره ۳، بهار و تابستان ۱۳۹۲ ش.
- میرمحمدصادقی، حسین، و زینب لکی، «رویکردی نوین بر ارجاع کیفری در پرتو اصل وصف‌گذاری منصفانه»، پژوهش حقوق کیفری، سال هفتم، شماره ۲۷، تابستان ۱۳۹۸ ش.
- میرمحمدصادقی، حسین، و علی رحمتی، «مصادیق عدول از اصول کلی حقوق کیفری در جرایم علیه امنیت»، فصلنامه راهبرد، سال بیست و چهارم، شماره ۷۶، پاییز ۱۳۹۴ ش.
- نجفی ابرندآبادی، علی حسین، «جرم‌شناسی حقوقی (درآمدی بر جرم‌شناسی حقوق کیفری عمومی)»، مندرج در: تازه‌های علوم جنایی، کتاب دوم، زیر نظر علی حسین نجفی ابرندآبادی، چاپ دوم، تهران، میزان، ۱۳۹۵ ش.
- همو، «درباره امنیت‌شناسی (از حق بر امنیت تا حق بر تأمین)»، دیباچه در: رضوانی، سودابه، مدیریت انسان‌مدار ریسک جرم، تهران، میزان، ۱۳۹۱ ش.
- همو، «کیفرشناسی نو - جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار»، مندرج در: تازه‌های علوم جنایی، کتاب اول، زیر نظر علی حسین نجفی ابرندآبادی، تهران، میزان، ۱۳۸۸ ش.
- نجفی ابرندآبادی، علی حسین، محمدجعفر حبیب‌زاده، و محمدعلی بابائی، «جرایم مانع (جرایم بازدارنده)»، فصلنامه مدرس علوم انسانی (ویژه‌نامه حقوق)، شماره ۳۷، زمستان ۱۳۸۳ ش.