حقوق تطبیقی

دو فصلنامهٔ علمی حقوق تطبیقی
دوره یازدهم، شمارهٔ دو، پاییز و زمستان ۱۴۰۳
شماره پیاپی ۲۲، صص ۱۰۷-۱۲۹
مقالهٔ پژوهشی

Law
Comparative

The Journal of Comparative Law
Semi-annual, Vol. 11, No. 2, Fall 2024 and Winter 2025
Issue 22, pp. 107-129
Original Article

مطالعه تطبیقی نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال

صادق خضری‌نیا*
جعفر کوشا**
پرویز ذکائیان***

DOI: https://doi.org/10.22096/law.2025.2047662.2255
[تاریخ دریافت: ۱۴۰۳/۰۹/۱۸ تاریخ پذیرش: ۱۴۰۴/۰۲/۱۶]

چکیده

اقتصاد دیجیتال با دگرگون کردن ساختارهای اجتماعی و مالی، به افزایش کارایی و صرفه‌جویی در منابع منجر شده است. در این میان، ارزهای دیجیتال فرصت‌ها و چالش‌هایی مانند تهدیدات امنیتی و قانونی ایجاد کرده‌اند که پلیس را با مسائل جدیدی روبه‌رو می‌کند. این پژوهش به بررسی نقش و رویکرد پلیس در کشورهای منتخب (آمریکا، اتحادیه اروپا، استرالیا، کانادا، آلمان و ایران) در مقابله با جرایم ارز دیجیتال می‌پردازد و تفاوت‌ها و شباهت‌های استراتژی‌ها، آموزش‌ها و تجهیزات را تحلیل می‌کند. فرضیه تحقیق این است که با توجه به تفاوت در قوانین، زیرساخت‌های فناوری و سطح توسعه ارزهای دیجیتال، پلیس در کشورهای مختلف رویکردهای متفاوتی اتخاذ می‌کند. با روش توصیفی - تحلیلی، نتایج نشان می‌دهد کشورها برای مقابله با این جرایم، قوانین جامعی وضع کرده‌اند. به‌عنوان مثال، آمریکا و اتحادیه اروپا چهارچوب‌های قانونی محکمی برای نظارت بر فعالیت‌های مشکوک و مبارزه با پول‌شویی ایجاد کرده‌اند. پلیس کانادا با فناوری‌های پیشرفته، مانند تحلیل بلاکچین و همکاری بین‌المللی، جرایم را شناسایی می‌کند. در ایران، پلیس فتا با واحدهای تخصصی و نظارت بر صرافی‌ها، به مقابله با جرایم سایبری می‌پردازد، ازجمله تعطیلی مزارع استخراج غیرقانونی و افزایش آگاهی عمومی. همکاری بین‌المللی و تبادل اطلاعات در مبارزه با جرایم فرامرزی حیاتی است. همه کشورها نیازمند به‌روزرسانی مستمر استراتژی‌ها و فناوری‌ها برای مقابله مؤثر با این چالش‌ها هستند تا امنیت اقتصادی تقویت و سوءاستفاده از فناوری‌های مالی کاهش یابد.

واژگان کلیدی: ارز دیجیتال؛ اینترپل؛ پلیس؛ تخصص فنی؛ همکاری؛ یوروپل.

* دانشجوی دکتری حقوق جزا و جرم شناسی، دانشکده حقوق و علوم سیاسی، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران. (نویسنده مسئول) Email: sadegh.khezri20@gmail.com
** دانشیار، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران. Email: jkoosha@yahoo.com
*** استادیار، دانشکده حقوق و علوم سیاسی، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران.
Email: pzokaiyan59@gmail.com

۱. مقدمه

توسعه سریع اقتصاد دیجیتال ساختار اجتماعی را تغییر داده و الگوی معاملات نظام مالی دستخوش تغییرات بسیار قابل‌توجهی شده است. در سیستم معاملات تجاری، دیگر نیازی به حضور فیزیکی فروشندگان و خریداران نیست و همه فرایندها، اعم از پیشنهاددهی و خرید، به‌صورت مجازی انجام می‌شود. به همین ترتیب، در مرحله تراکنش‌های پرداخت، دیگر نیازی به سیستم نقدی و حمل پول فیزیکی به‌عنوان وسیله پرداخت نیست، بلکه پرداخت‌ها ازطریق روش‌های انتقال به شکل ارقام دیجیتال در مبلغ توافق‌شده انجام می‌شود. این الگوی مجازی تجارت و پرداخت‌ها همان چیزی است که به‌عنوان اقتصاد دیجیتال شناخته می‌شود. نقش اقتصاد دیجیتال در نفوذ به بازار، افزایش قدرت خرید و تسهیل معاملات، سهم بزرگی در پیشرفت اقتصادی یک کشور دارد، زیرا با صرفه‌جویی در زمان، انرژی و هزینه‌ها، بسیار کارآمد تلقی می‌شود. با پیشرفت فناوری‌های دیجیتال، ارزهای دیجیتال به‌عنوان یک پدیده نوظهور در اقتصاد جهانی مطرح شده‌اند. این توسعه سریع نه‌تنها فرصت‌های جدیدی را ارائه داده، بلکه چالش‌های امنیتی و قانونی تازه‌ای را نیز به همراه داشته است.

پلیس به‌عنوان یکی از نهادهای کلیدی در مبارزه با جرایم، نقش حیاتی در مقابله با تهدیدات مرتبط با ارزهای دیجیتال ایفا می‌کند. در مطالعات تطبیقی نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال، چندین نکته مهم وجود دارد که باید بررسی شود. کشورهای مختلف قوانین متفاوتی برای ارزهای دیجیتال دارند که بر نحوه عملکرد پلیس تأثیر می‌گذارد. برخی کشورها قوانینی جامع برای مقابله با جرایم مرتبط با ارز دیجیتال تصویب کرده‌اند، درحالی‌که برخی دیگر هنوز در حال توسعه این قوانین هستند. جرایم مرتبط با ارز دیجیتال اغلب ماهیت فرامرزی دارند، لذا همکاری بین‌المللی و تبادل اطلاعات بین ادارات پلیس ضروری است. ناشناس بودن در تراکنش‌های ارز دیجیتال می‌تواند ردیابی جرایم را برای پلیس دشوار کند. تکامل سریع فناوری‌های ارز دیجیتال به این معناست که روش‌های مبارزه با جرایم باید به‌طور مداوم به‌روز شوند. این عناصر نشان می‌دهند که نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال نیازمند رویکردی چندجانبه و بین‌المللی است. سؤال اساسی این پژوهش آن است که نقش و رویکرد پلیس در کشورهای منتخب (آمریکا، اتحادیه اروپا، استرالیا، کانادا، آلمان و ایران) در مواجهه با جرایم مرتبط با ارز دیجیتال چگونه است و چه تفاوت‌ها و شباهت‌هایی در استراتژی‌ها، آموزش‌ها و تجهیزات مورداستفاده وجود دارد. در پاسخ به این سؤال، این فرضیه مطرح می‌شود که با توجه به تفاوت در قوانین، زیرساخت‌های

فناوری اطلاعات و سطح توسعه ارزهای دیجیتال در کشورهای مختلف، پلیس در کشورهای منتخب، استراتژی‌های متفاوتی را در مواجهه با جرایم مرتبط با ارز دیجیتال اتخاذ می‌کند. به‌طور خاص، کشورهایی با قوانین جامع‌تر و زیرساخت‌های پیشرفته‌تر، رویکرد فعالانه‌تری در کشف و پیگرد قانونی این جرایم دارند، درحالی‌که کشورهایی با منابع محدودتر، بیشتر بر آموزش و همکاری بین‌المللی تکیه می‌کنند. این مقاله به مطالعه تطبیقی نقش پلیس در کشورهای مختلف و استراتژی‌های مورداستفاده برای مقابله با این نوع جرایم می‌پردازد. در واقع، مسئله اصلی این پژوهش این است که پلیس در کشورهای مختلف، در مواجهه با جرایم مرتبط با ارزهای مجازی، چه رویکردها و اقداماتی را انجام داده است و با توجه به این اقدامات، پلیس ایران[1] چه نوآوری‌هایی می‌تواند در اقدامات خود ایجاد نماید.

۲.تخصص فنی پلیس در مواجهه با جرایم مرتبط با ارزهای دیجیتال

به‌موازات شکل‌گیری جامعه بشری و انتقال از جامعه سنتی به جامعه مدرن و تغییر در شیوه‌ها و روش‌های ارتکاب جرم، روش‌های مبارزه و مقابله با جرم نیز دستخوش تغییرات اساسی گردیده است.[2] یکی از چالش‌های اصلی امروز پلیس، مقابله با جرایم مرتبط با ارزهای دیجیتال است. امروزه پلیس باید از توانایی‌های تکنولوژیکی به‌روز برای ردیابی تراکنش‌های بلاکچین و تحلیل داده‌های پیچیده برخوردار باشد. در کشورهای پیشرو مانند آمریکا و اروپا، برنامه‌های آموزشی ویژه‌ای برای نیروهای پلیس در نظر گرفته شده است.

یکی از چالش‌های اساسی که نیروهای پلیس و نهادهای نظارتی در مقابله با جرایم مرتبط با ارزهای دیجیتال با آن مواجه‌اند، نیاز به تخصص فنی بالا است. پیچیدگی فناوری بلاکچین و ناشناس بودن نسبی تراکنش‌های آن، ردیابی جرایم سایبری را به یک فرایند پیچیده تبدیل کرده است. ازاین‌رو، توسعه و آموزش نیروهای پلیس با توجه به آخرین فناوری‌های موجود و ابزارهای تحلیل بلاکچین، به یک ضرورت تبدیل شده است. تخصص فنی و ابزارهای موردنیاز پلیس در جهت مبارزه با ارزهای دیجیتال عبارت‌اند از:

۱. تحلیل بلاکچین و داده‌های مرتبط: پلیس‌ها از ابزارهای تخصصی تحلیل بلاکچین برای شناسایی تراکنش‌های مشکوک استفاده می‌کنند. همکاری با شرکت‌های تحلیلی مثل

---

۱. منظور از پلیس ایران در این مقاله، نیروی انتظامی و به‌طور خاص، پلیس فتا است.

۲. صیاد درویشی، «بررسی دانش و مهارت موردنیاز پلیس در پیشگیری وضعی از جرم»، *فصلنامه پژوهش‌های دانش انتظامی* ۱۹ (۱۳۹۶): ۴۸.

Chainalysis و Merkle Science به نیروهای امنیتی این امکان را می‌دهد تا به داده‌های بلاکچین دسترسی داشته و آن‌ها را با اطلاعات دنیای واقعی ترکیب کنند. این فرایند به شناسایی کاربران و ردیابی جرایم کمک می‌کند.

۲. برنامه‌های آموزشی: نهادهای پلیس در کشورهای پیشرو همچون ایالات متحده و اروپا، برنامه‌های آموزشی ویژه‌ای را برای نیروهای خود برگزار می‌کنند. این آموزش‌ها شامل استفاده از ابزارهای تحلیل داده، شبیه‌سازی‌های واقع‌گرایانه از جرایم بلاکچین، و همچنین تمرینات عملی برای افزایش مهارت‌های مرتبط با ارزهای دیجیتال است. به‌عنوان مثال، FBI و یوروپل دوره‌های مشترکی در زمینه مقابله با جرایم سایبری و رمزارزها برگزار کرده‌اند.

۳. همکاری بین‌المللی: همکاری بین نهادهای بین‌المللی مانند FBI، یوروپل، و شرکت‌های خصوصی مانند صرافی‌های رمزارز برای مقابله با این جرایم حیاتی است. این همکاری‌ها به اشتراک‌گذاری اطلاعات، تحلیل تراکنش‌ها، و ردیابی جریان‌های مالی کمک می‌کند.

٤. تجهیزات پیشرفته: ابزارهای پیشرفته‌ای همچون سیستم‌های تحلیل مبتنی‌بر هوش مصنوعی، برای ردیابی تراکنش‌های رمزارز در سطح بین‌المللی و در بلاکچین‌های مختلف مورد استفاده قرار می‌گیرند. این ابزارها به کشف هویت مجرمان و پیگیری جریان‌های مالی در شبکه‌های پیچیده کمک می‌کنند.

مقابله با جرایم مرتبط با ارزهای دیجیتال نیازمند تخصص فنی بالایی است. پلیس و نهادهای نظارتی باید همواره به‌روز باشند و از ابزارها و فناوری‌های پیشرفته‌ای همچون تحلیل بلاکچین، شبیه‌سازی و آموزش‌های تخصصی بهره بگیرند. همکاری‌های بین‌المللی و استفاده از تجربیات شرکت‌های خصوصی نیز نقش کلیدی در موفقیت این اقدامات دارند.

۳.نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در ایالات متحده آمریکا

ایالات متحده آمریکا ازجمله کشورهایی است که رمزارزها را به‌عنوان یک دارایی به رسمیت شناخته است، به‌طوری که در مارس ۲۰۱٤، سرویس درآمد داخلی ایالات متحده (IRS) راهنمایی‌هایی را منتشر کرد که در آن‌ها، بیت‌کوین و سایر ارزهای دیجیتال به‌عنوان دارایی قلمداد می‌شدند. این راهنما تصریح نمود که ارزهای دیجیتال همچون بیت‌کوین، باید در زمینه‌های مالیاتی، مشابه سایر دارایی‌ها مانند دارایی‌های مشهود و مالی تحت رسیدگی قرار

گیرند. این به معنای آن است که درآمدهای حاصل از فعالیت‌هایی نظیر فروش یا مبادله رمزارزها، شامل قوانین مالیاتی می‌شوند و باید گزارش شوند. به‌طور مشخص، راهنمای IRS تصریح کرده بود که ارزهای دیجیتال به‌عنوان دارایی در نظر گرفته می‌شوند، نه به‌عنوان ارز خارجی یا قانونی. این تصمیم بر چگونگی محاسبه سود و زیان مالیاتی اثر می‌گذارد. برای مثال، اگر یک فرد بیت‌کوین خود را بفروشد و سود کند، باید این سود را به‌عنوان سود سرمایه‌ای در اظهارنامه مالیاتی خود گزارش کند. این رویکرد IRS به رمزارزها به‌عنوان دارایی، شفافیت بیشتری به محیط قانونی استفاده و دادوستد رمزارزها در آمریکا می‌دهد و از این نظر حائز اهمیت است.[۳]

در ایالات متحده، چهارچوب قانونی جامعی برای مقابله با جرایم مرتبط با ارزهای دیجیتال وجود دارد و به‌صورت پیوسته در حال تکامل است. قانون‌گذاران با تصویب قوانینی مانند قانون محرمانگی بانک‌ها (BSA) و قانون PATRIO، پلیس را مجاز به نظارت و ردیابی تراکنش‌های مشکوک می‌کنند.[٤] قانون محرمانگی بانک‌ها که در سال ۱۹۷۰ تصویب شد، یکی از ابزارهای کلیدی برای ردیابی و شناسایی فعالیت‌های مشکوک مالی است. این قانون به نهادهای مالی این اختیار را می‌دهد که تراکنش‌های مشکوک را به شبکه اطلاعات مالی جرایم (FinCEN) گزارش دهند. با گسترش استفاده از ارزهای دیجیتال، FinCEN با تدوین دستورالعمل‌هایی خاص، مشاغل مرتبط با ارزهای دیجیتال را نیز تحت این قانون قرار داده است. این قوانین به پلیس اجازه می‌دهند تا به اطلاعات و داده‌های حیاتی دسترسی پیدا کند و فعالیت‌های مالی مشکوک را ردیابی نماید. طبق گزارش‌های FinCEN، در سال ۲۰۲۱، تعداد گزارش‌های مرتبط با ارزهای دیجیتال به‌طرز چشمگیری افزایش یافته است، که نشان‌دهنده توجه روزافزون نهادهای نظارتی به این حوزه است.

همچنین قانون PATRIOT که بعداز حملات تروریستی ۱۱ سپتامبر ۲۰۰۱ به تصویب رسید، ابزارهای قانونی را برای شناسایی و پیشگیری از فعالیت‌های تروریستی و جرایم مالی تقویت می‌کند.[٥] این قانون شامل چندین بخش مهم است که به نظارت و ردیابی منابع مالی کمک می‌کند:

3.U.S. Internal Revenue Service, "Letter, No. 2016-0036", (2016).

4."Guidance on Virtual Currency," FinCEN, accessed 2021, https://www.fincen.gov

5."The Financial Crimes Enforcement Network," U.S. Department of the Treasury, accessed 2021. https://www.treasury.gov

۱. گسترش دامنه نظارت: این قانون به نهادهای امنیتی و پلیس این اختیار را می‌دهد که به‌صورت مؤثرتر به نظارت بر فعالیت‌های مالی بپردازند.

۲. همکاری بین‌المللی: این قانون به مقامات آمریکایی این امکان را می‌دهد که با نهادهای بین‌المللی برای مقابله با جرایم مالی و تروریسم همکاری کنند.

این دو قانون به پلیس و نهادهای امنیتی در ایالات متحده این امکان را می‌دهند که به‌راحتی فعالیت‌های مرتبط با ارزهای دیجیتال را ردیابی کنند. به‌عنوان مثال، با استفاده از فناوری‌های پیشرفته، پلیس می‌تواند داده‌های جمع‌آوری‌شده از صرافی‌ها و سایر نهادهای مالی را تحلیل کرده و الگوهای مشکوک را شناسایی کند و باوجود چهارچوب قانونی، پلیس قادر است به‌سرعت به مواردی مانند پول‌شویی، کلاهبرداری و تأمین مالی تروریسم واکنش نشان دهد.[۶] در نهایت، چهارچوب قانونی ایالات متحده برای مقابله با جرایم مرتبط با ارزهای دیجیتال، به‌صورت پیوسته در حال توسعه و تکامل است. قوانین BSA و PATRIOT نه‌تنها به پلیس و نهادهای امنیتی ابزارهای لازم را برای ردیابی و جلوگیری از جرایم مالی می‌دهند، بلکه به آن‌ها این امکان را می‌دهند که به شکل مؤثری، با چالش‌های جدید در این حوزه مقابله کنند. این تلاش‌ها به‌عنوان بخشی از یک رویکرد جامع برای امنیت مالی و مبارزه با جرایم جهانی به حساب می‌آید.

۴. نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در اتحادیه اروپا

در اتحادیه اروپا، مقررات جامعی درخصوص ارزهای مجازی وجود ندارد. در برخی دولت‌های عضو، برای مبادله این ارزها قانون وضع شده است. از این میان، می‌توان به آلمان، فرانسه و ایتالیا اشاره کرد.[۷] اما اتحادیه اروپا قوانین سخت‌گیرانه‌ای برای مقابله با پول‌شویی و تأمین مالی تروریسم ازطریق ارزهای دیجیتال وضع کرده است. مقررات AMLD5 (پنجمین دستورالعمل مبارزه با پول‌شویی) و AMLD6 (ششمین دستورالعمل مبارزه با پول‌شویی) به‌عنوان ابزارهای قانونی مهم برای پلیس در کشورهای عضو اتحادیه اروپا

6. U.S. Department of Justice, "Report on Cryptocurrency Enforcement Framework," *Office of Public Affairs*. (2020).

7. K. Bryanov, "France and Germany: How Regulatory Traditions in Two Countries Could Affect EU Legislation," *CoinTelegraph* (2018).

محسوب می‌شوند.[۸] مقررات AMLD5 که در ژانویه ۲۰۲۰ اجرایی شد، به‌طور خاص، شامل قوانینی برای شفاف‌سازی و تنظیم فعالیت‌های مربوط به ارزهای دیجیتال است. هدف AMLD5 تقویت امنیت اقتصادی ازطریق شفافیت بیشتر و ارتقای نظارت بر تراکنش‌های ارزهای دیجیتال است. این مقررات پلیس کشورهای عضو اتحادیه را قادر می‌سازد تا در شناسایی و جلوگیری از فعالیت‌های پول‌شویی و تأمین مالی تروریسم مؤثرتر عمل کند.[۹] مقررات AMLD6 نیز که در دسامبر ۲۰۲۰ معرفی و در ژوئن ۲۰۲۱ اجرایی شد، برمبنای حساسیت‌های جدید و چالش‌های موجود به‌روزرسانی شد. این قانون باعث می‌شود تا کشورهای عضو اتحادیه اروپا به‌طور هماهنگ‌تری به چالش‌های پیچیده مالی و نقض امنیت اقتصادی پاسخ دهند و پلیس ابزارهای قانونی بیشتری برای پیگرد قانونی فعالیت‌های مجرمانه در اختیار داشته باشد.[۱۰] مقررات AMLD5 و AMLD6 به اتحادیه اروپا امکان می‌دهد با اتخاذ سیاست‌های جامع و شفاف، در برابر تهدیدات و خطرات ناشی از استفاده غیرقانونی از ارزهای دیجیتال موضع‌گیری نماید. این قوانین نه‌تنها به شفافیت بیشتر در فعالیت‌های مالی کمک می‌کنند، بلکه پلیس و نهادهای نظارتی را نیز به ابزارهای موردنیاز برای مقابله با این جرایم مجهز می‌کنند.

۵. نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در استرالیا

پلیس فدرال استرالیا (AFP) واحدهای تخصصی ویژه‌ای برای مقابله با جرایم مرتبط با ارزهای دیجیتال ایجاد کرده است. این واحدها بر تحلیل و شناسایی جرایم پیچیده‌ای مثل پول‌شویی و کلاهبرداری متمرکز هستند. مهم‌ترین وظایف و نقش واحدهای تخصصی عبارت‌اند از:

۱. تحلیل بلاکچین: این واحدها از فناوری‌های پیشرفته برای تحلیل تراکنش‌های بلاکچین استفاده می‌کنند تا مسیریابی تراکنش‌ها و فعالیت‌های مشکوک را تسهیل کنند.

---

8. European Parliament and Council of the European Union, "Directive (EU) 2018/843 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing." *Official Journal of the European Union*, L 156/43 (2018).

9. Cipher Trace, "Cryptocurrency Anti-Money Laundering Report – Q4 2018 Jan 4." (2019): 20.

10. J. Miseviciute, "Virtual Currency Regulation in the EU," *Journal of Investment Compliance* 19, no. 3 (2018): 33-38.

۲. آمـوزش نیروهـای پلـیس: بـا برگـزاری دوره‌هـای آموزشـی، نیروهـای پلـیس بـا تکنولوژی‌های جدید و روش‌های شناسایی جرایم ارز دیجیتال به‌روز می‌شوند.

۳. همکاری با نهادهای بین‌المللی: این واحدها با سازمان‌های بین‌المللی و سایر کشورها برای تبادل اطلاعات و تجربه همکاری می‌کنند.

٤. مشارکت با نهادهای مالی: همکاری نزدیک با بانک‌ها و مؤسسـات مـالی، بـه‌منظـور شناسایی و پیشگیری از جرایم پول‌شویی ازطریق سیستم‌های مالی.

۵. راه‌اندازی تحقیقات ویژه: واحـدهای تخصصـی اغلـب تحقیقـات ویـژه‌ای را پیرامـون جریان‌های مالی مشکوک که ممکن است به پول‌شویی مرتبط باشند، انجام می‌دهند.

٦. مبارزه با فعالیت‌های غیرقانونی ارائه‌دهندگان خدمات ارز دیجیتال: تمرکز بر شناسـایی و متوقف کردن خدمات‌دهندگانی که به امنیت قوانین نظارتی پایبند نیستند.[11]

گسترده شدن این واحدها و استفاده از فناوری‌های نوین، استرالیا را در مقابله با جرایم ارز دیجیتال به یکی از کشورهای پیشرو تبدیل کرده و به بهبود امنیت بازارهای مالی کمک نمـوده است. همکاری با نهادهای دیگر و سازمان‌های بین‌المللی نیز این توانایی‌هـا را بیشـتر تقویـت کرده است.

۶. نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در آلمان

در آلمان، ارزهای دیجیتال به‌عنوان دارایی‌های مالی و ابزارهای مالی جدید شناسایی شده‌اند. موضع دولت آلمان و نهادهای مالی این کشور بر این است که بیت‌کوین به‌عنـوان یـک دارایـی قابل مالیات‌گیری محسوب می‌شود و ویژگی‌های خـاص خـود را بـه‌عنوان یـک واحـد ارزش دارد. آلمان یکی از اولین کشورهایی بود که نگاهی جدی و سازمان‌یافته به چهارچوب قـانونی بیت‌کوین داشت. در سـال ۲۰۱۳، وزارت دارایـی آلمـان بیـت‌کوین را بـه‌عنـوان «واحـد پـولی خصوصی» به رسمیت شناخت. این تصمیم به معنای آن است که اگرچـه بیـت‌کوین بـه‌عنـوان ارز قانونی شناخته نمی‌شود، اما می‌تواند در برخی مبادلات و به‌عنـوان ابـزار پرداخـت بـه کـار گرفته شود. در آلمان، بیت‌کوین به‌عنـوان یـک دارایـی مالیات‌پـذیر شـناخته می‌شـود. فراینـد مالیات‌گذاری در آلمان بستگی به مدت زمان نگهداری بیـت‌کوین دارد. اگـر بیـت‌کوین بـرای

11. Mirko Bagaric, Richard Edney, and Theo Alexander, *Sentencing in Australia*, 8th edition ([n.p]: Lawbook, 2020), 211-220.

بیش از یک سال نگهداری و سپس فروخته شود، سود آن به‌طور کلی از مالیات معاف است. اما اگر بیت‌کوین در مدت زمان کوتاه‌تر از یک سال فروخته شود، سود آن به‌عنوان درآمد مشمول مالیات بر درآمد فرد می‌شود.[۱۲] آلمان به‌دنبال شفافیت در تراکنش‌های مرتبط با ارزهای دیجیتال و جلوگیری از فعالیت‌های غیرقانونی مانند پول‌شویی است. بنابراین، استفاده از بیت‌کوین و سایر ارزهای دیجیتال تحت نظارت‌های خاص قانونی قرار دارد و نهادهای نظارتی بر استفاده و مبادلات آن‌ها نظارت می‌کنند. این نگاه باعث شده تا آلمان به یکی از کشورهایی تبدیل شود که به‌طور رسمی، چهارچوب قانونی و مالیاتی خاصی برای ارزهای دیجیتال تعیین کرده است. پلیس آلمان نقش مهمی در مقابله با جرایم مرتبط با ارز دیجیتال دارد. در مواجهه با این جرایم، اقدامات زیر ازسوی پلیس آلمان قابل توجه است:

۱. تعطیل کردن صرافی‌های ارز دیجیتال غیرقانونی: پلیس آلمان، به‌خصوص اداره پلیس جنایی فدرال، چندین صرافی ارز دیجیتال غیرقانونی را که به فعالیت‌های مجرمانه مانند پول‌شویی کمک می‌کردند، شناسایی و تعطیل کرده‌اند. این اقدام نشان‌دهنده تعهد آلمان به مقابله با جرایم اقتصادی دیجیتال است.[۱۳]

۲. تلاش‌های ضد پول‌شویی: اقدامات پلیس آلمان بر تعطیلی پلتفرم‌های خدماتی متمرکز است که مجرمین را قادر می‌ساختند تا از ارز دیجیتال برای پول‌شویی و انتقال وجوه غیرقانونی استفاده کنند.[۱۴]

۳. به‌کارگیری تکنولوژی و همکاری بین‌المللی: پلیس آلمان از تکنولوژی‌های پیشرفته برای ردیابی تراکنش‌های دیجیتال استفاده می‌کند و با نهادهای بین‌المللی همکاری نزدیکی دارد تا شبکه‌های جنایی بین‌المللی را شناسایی و متلاشی کند.[۱۵]

٤. برنامه‌های ویژه و واحدهای تخصصی: اداره پلیس جنایی فدرال آلمان (BKA) واحدهای تخصصی برای مواجهه با جرایم سایبری و مالی ایجاد کرده است. این واحدها به

12. Sarah E. Needleman and Spencer E. Ante, "Bitcoin Startups Begin to Attract Real Cash," *Wall Street Journal* 8 (2013): 71.

13. Phil Muncaster, "German Police Shutter 47 Criminal Crypto Exchanges," Infosecurity Magazine, accessed September 20, 2024, https://www.infosecurity-magazine.com/news/german-police-shut-47-criminal/

14. Matthias Schulze, "German Police Dismantles Illegal Crypto Exchanges," CSO Online, accessed September 20, 2024, https://www.csoonline.com/article/3535563/german-police-dismantles-illegal-crypto-exchanges.html?utm_source=dlvr.it&utm_medium=mastodon

15. Schulze, "German Police Dismantles Illegal Crypto Exchanges."

جمع‌آوری اطلاعات، تحلیل داده‌ها و اجرای عملیات‌های ویژه در مقابله با فعالیت‌های غیرقانونی ارز دیجیتال می‌پردازند.[۱۶]

۵. آموزش و آگاهی‌بخشی: پلیس آلمان به آموزش و آگاهی‌بخشی عمومی نیز توجه دارد و کاربران را درمورد ریسک‌های مرتبط با سرمایه‌گذاری و استفاده از ارزهای دیجیتال آگاه می‌سازد.[۱۷]

٦. قوانین و چهارچوب‌های حقوقی: آلمان قوانین سخت‌گیرانه‌ای در زمینه ارزهای دیجیتال وضع کرده است که هدف اصلی آن‌ها پیشگیری از سوءاستفاده‌های مالی و پول‌شویی است. این قوانین به پلیس و مقامات قضایی قابلیت‌های بیشتری برای مداخله مؤثر می‌دهد.[۱۸]

این رویکرد جامع پلیس آلمان را قادر می‌سازد تا به‌طور مؤثری با چالش‌های امنیتی و مالی مرتبط با ارزهای دیجیتال مقابله کند و از این طریق، از آسیب‌های اقتصادی و اجتماعی ناشی از این جرایم جلوگیری کند. این تلاش‌ها و اقدامات نشان‌دهنده رویکرد فعالانه پلیس آلمان در مقابله با جرایم مرتبط با ارزهای دیجیتال و فراهم کردن بستری امن‌تر برای تراکنش‌های دیجیتال است.

۷. نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در کانادا

پلیس کانادا، ازجمله پلیس ملی این کشور، که با نام Royal Canadian Mounted Police (RCMP) شناخته می‌شود، نقش بسیار مهم و متنوعی در مقابله با جرایم مربوط به ارزهای دیجیتال ایفا می‌کند. این ارگان مسئول اجرای قوانین و حفاظت از امنیت عمومی است و با توجه به رشد سریع استفاده از ارزهای دیجیتال و ارتباط آن با فعالیت‌های غیرقانونی، پلیس کانادا ابزارها، فناوری‌ها و استراتژی‌های خاصی را برای مقابله با این نوع جرایم به کار

16. Deloitte, “New Challenges for the Digitization of Germany: What the IT Security Act 2.0 and the New KRITIS-Ordinance Entail,” Deloitte Legal Germany, accessed 2021, https://www2.deloitte.com/dl/en/pages/legal/articles/it-sicherheitsgesetz-kritis-verordnung.html
17. Deloitte, “New Challenges for the Digitization of Germany.”
18. Bundesregierung, “Goals Adopted in the Area of Cyber Security,” Federal Government of Germany, accessed September 8, 2021, https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688

می‌برد.[۱۹] در اینجا به نقش‌های مختلف پلیس کانادا در این حوزه پرداخته می‌شود:

۱. تحقیق و جمع‌آوری اطلاعات: یکی از مهم‌ترین نقش‌های پلیس کانادا در مقابله با جرایم رمزارزی، تحقیق و جمع‌آوری اطلاعات است. پلیس کانادا با استفاده از فناوری‌های پیشرفته و ابزارهای تحلیل داده‌های دیجیتال، شبکه‌های مجرمانه و فعالیت‌های غیرقانونی مرتبط با ارزهای دیجیتال را شناسایی و پیگیری می‌کند. اطلاعاتی مانند تراکنش‌های مشکوک، آدرس‌های دیجیتال (wallets) و دیگر داده‌های مرتبط با کاربران ارز دیجیتال، مورد تجزیه‌وتحلیل قرار می‌گیرد.[۲۰] پلیس کانادا به‌ویژه از فناوری‌هایی مانند Blockchain Analysis Tools برای ردیابی تراکنش‌های ارز دیجیتال استفاده می‌کند. این ابزارها به محققان این امکان را می‌دهند که مسیر تراکنش‌ها را در بلاکچین دنبال کنند و ارتباطات مجرمانه بین کاربران مختلف را شناسایی نمایند.

۲. مبارزه با پول‌شویی و تأمین مالی تروریسم: یکی از مهم‌ترین تهدیدات امنیتی مرتبط با ارزهای دیجیتال، استفاده از این فناوری‌ها برای پول‌شویی و تأمین مالی تروریسم است. ارزهای دیجیتال به‌دلیل ویژگی‌هایی مانند ناشناسی نسبی و قابلیت انتقال سریع و جهانی، می‌توانند ابزار مناسبی برای انجام معاملات غیرقانونی و انتقال وجوه ازطریق مرزها بدون شفافیت کافی باشند. پلیس کانادا با نظارت دقیق بر فعالیت‌های مالی و مالیات‌ها، در تلاش است تا هرگونه فعالیت مشکوک مرتبط با پول‌شویی یا تأمین مالی تروریسم را شناسایی و پیگیری کند.[۲۱] در این راستا، «مرکز تجزیه‌وتحلیل معاملات و گزارش‌های مالی کانادا»[۲۲] نقش کلیدی را در نظارت بر فعالیت‌های مالی و کمک به پلیس کانادا ایفا می‌کند. این مرکز داده‌های مالی را جمع‌آوری می‌کند و به تحلیل و شناسایی الگوهای غیرقانونی می‌پردازد و آن‌ها را در اختیار پلیس قرار می‌دهد تا تحقیقات بیشتری صورت گیرد.

۳. مقابله با کلاهبرداری‌ها و هک‌ها: کلاهبرداری‌های مربوط به ارزهای دیجیتال، مانندPonzi schemes، Phishing و Ransomware attacks، یکی دیگر از جنبه‌های مهم

19. K .Gile, “Chainalysis Reactor Aids Canadian Law Enforcement in Tracking Crypto Cybercrimes,” BitDegree, accessed 2023, https://www.bitdegree.org/crypto/news/chainalysis-reactor-aids-canadian-law-enforcement-in-tracking-crypto-cybercrimes .

20. Gile, “Chainalysis Reactor Aids Canadian Law.”

21. H.A. Reda, “Terrorist Financing: Are Current Anti-Money Laundering Regulations Easily Applied to Virtual Currencies?” (PhD diss., Colorado Technical University, 2017), 163.

22. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

جرایم دیجیتال هستند که پلیس کانادا به‌شدت به آن‌ها توجه دارد. پلیس کانادا برای مقابله با این نوع کلاهبرداری‌ها، از تیم‌های ویژه‌ای که در حوزه جرایم سایبری تخصص دارند بهره می‌برد.[۲۳] برای مثال، در مواقعی که گروه‌های مجرمانه ازطریق هک سیستم‌ها و سرقت اطلاعات کاربری در صرافی‌های ارز دیجیتال، به دارایی‌های افراد دسترسی پیدا می‌کنند، پلیس کانادا در کنار سایر نهادهای بین‌المللی مانند یوروپل و اینترپل، برای شناسایی و بازگرداندن وجوه مسروقه و دستگیری عاملان این حملات تلاش می‌کند.

٤. آموزش و همکاری با نهادهای بین‌المللی: پلیس کانادا به‌طور مستمر، در حال همکاری با سایر نهادهای بین‌المللی و دولتی در راستای مبارزه با جرایم مرتبط با ارزهای دیجیتال است. این همکاری‌ها نه‌تنها شامل اشتراک‌گذاری داده‌ها و شواهد بین کشورها می‌شود، بلکه پلیس کانادا در برگزاری سمینارها و دوره‌های آموزشی برای سایر نیروهای انتظامی و مقامات دولتی در سایر کشورها هم مشارکت دارد. به‌ویژه در زمینه مبارزه با جرایم سایبری و پول‌شویی، کانادا عضو سازمان‌های بین‌المللی نظیر FATF) Financial Action Task Force) و Egmont Group است که در جهت تسهیل تبادل اطلاعات بین نهادهای نظارتی و پلیسی کشورهای مختلف فعالیت می‌کنند.[۲٤]

به‌طور کلی و با توجه به مطالب فوق، پلیس کانادا با استفاده از ترکیبی از تحقیق و جمع‌آوری داده‌ها، همکاری‌های بین‌المللی، استفاده از فناوری‌های نوین و آموزش، به مقابله با جرایم مرتبط با ارزهای دیجیتال پرداخته است. این اقدامات شامل مبارزه با پول‌شویی، کلاهبرداری‌های دیجیتال، هک‌ها، و فعالیت‌های مرتبط با تأمین مالی تروریسم می‌شود. با توجه به پیچیدگی و جهانی بودن این جرایم، همکاری‌های بین‌المللی و نظارت دقیق بر بازارهای ارز دیجیتال ازجمله اقداماتی است که پلیس کانادا در راستای حفظ امنیت عمومی و پیشگیری از فعالیت‌های غیرقانونی در این حوزه انجام می‌دهد.

۸. نقش پلیس در مواجهه با جرایم مرتبط با ارز دیجیتال در ایران

در حوزه مقررات‌گذاری درخصوص رمزارزها در سطح بین‌المللی، بعضی کشورها رویکرد ممنوعیت کلی را در پیش گرفته و برخی تنها یک یا چند وجه از ابعاد رمزارز را ممنوع

23. M-H Maras, *Cybercriminology* (New York: Oxford University Press, 2016), 90.

۲٤. مریم کشمیری، *سرقت هویت در فضای سایبری: مقایسه تطبیقی حقوق ایران و کانادا* (تهران: نشر سیمرغ آسمان آذرگان، ۱۳۹۷)، ۴۵.

کرده‌اند. برخی نیز با آغوش باز به استقبال این پدیده رفته و بعضی هم موضع خاصی در این خصوص اتخاذ نکرده‌اند. در کشور ما، مقررات‌گذاری در این حوزه از سال ۱۳۹٦ به‌تدریج آغاز شد و با کندی به پیش رفت.[۲۵] مصوبه شورای عالی مبارزه با پول‌شویی (۱۳۹٦)، اطلاعیه گمرک جمهوری اسلامی ایران (۱۳۹۸/۰٤/۲۲)، آیین‌نامه اجرایی چگونگی استخراج فراورده‌های پردازشی رمزنگاری‌شده (۱۳۹۸/۰۵/۱۳)، دستورالعمل صدور جواز تأسیس و پروانه بهره‌برداری برای فعالیت استخراج رمزارز (۱۳۹۸/۰۸/۲۲)، مصوبه هیئت وزیران درخصوص تکلیف دارندگان دستگاه‌های استخراج رمزارز نسبت‌به ثبت مشخصات هویتی خود و دستگاه‌هایی که تحت مالکیت آن‌ها می‌باشد (۱۳۹۹/۰٤/۰۸)، مصوبه هیئت وزیران درخصوص الحاق یک تبصره به بند ۱ تصویب‌نامه مورخ ۱۳۹۸/۰۵/۱۳ (۱۳۹۹/۰۷/۱۳)، دستورالعمل خوداظهاری دارندگان دستگاه‌های رمزارز قاچاق (۱۳۹۹/۰۸/۲۰)، مقررات تأمین برق مراکز استخراج رمزارزها (فروردین ۱٤۰۰)، اصلاحیه دستورالعمل صدور مجوز فعالیت استخراج رمزارزها (۱٤۰۰/۰۱/۲۵)، آیین نامه استخراج رمزدارایی‌ها (۱٤۰۱/۰۸/۲۳)، ازجمله مقرراتی هستند که به تصویب نهادهای مختلف قانون‌گذاری رسیده‌اند.

با توجه به قوانین فوق، پلیس ایران به‌عنوان ضابطان قضایی[۲٦] در مواجهه با جرایم مرتبط با ارزهای مجازی، نقش مهمی را ایفا می‌کند، به‌ویژه با توجه به افزایش استفاده از این فناوری‌ها در سال‌های اخیر. جرایم مرتبط با ارزهای مجازی معمولاً شامل پول‌شویی، کلاهبرداری‌های اینترنتی، و فعالیت‌هایی نظیر تأمین مالی غیرقانونی می‌شود. در اینجا به برخی از اقدامات و نقش‌های پلیس ایران در این زمینه اشاره می‌کنیم:

۱. تشکیل واحدهای ویژه: برای مقابله مؤثر با جرایم ارزهای مجازی، پلیس ایران واحدهای ویژه‌ای نظیر پلیس فتا (فضای تبادل اطلاعات) را تشکیل داده است. پلیس فتا مسئولیت شناسایی و پیگیری جرایم سایبری و مرتبط با فناوری اطلاعات را بر عهده دارد. این واحد تخصصی به جمع‌آوری اطلاعات، تحلیل، و پیگیری موارد مشکوک در حوزه ارزهای دیجیتال می‌پردازد.

---

۲۵. زهرا ساکیانی و سید عباس واعظی، «امکان‌سنجی قاچاق کالا و ارز درخصوص دستگاه‌های استخراج رمزارز و مبادلات رمزارزها: مسائل قانونی و رویه‌های عملی»، *فصلنامه آموزه‌های حقوق کیفری* ۱۹، شماره ۲۴ (۱۴۰۱): ۱۲۶.

۲٦. براساس ماده ۲۹ قانون آیین دادرسی کیفری، بند ۸ ماده ۴ قانون نیروی انتظامی و بند الف ماده یک آیین‌نامه اجرایی احراز عنوان ضابط دادگستری مصوب ۱۳۹۸/۰۶/۰۱ رئیس قوه قضاییه، نیروی انتظامی ضابط قضایی محسوب می‌شود.

۲. نظارت بر صرافی‌های دیجیتال: یکی از وظایف مهم پلیس ایران، نظارت بر صرافی‌های آنلاین و دیجیتال است. این نظارت به‌منظور جلوگیری از پول‌شویی و تراکنش‌های غیرقانونی انجام می‌شود. دولت ایران با همکاری بانک مرکزی و سایر نهادهای مالی، چهارچوب‌های قانونی برای فعالیت صرافی‌های دیجیتال تدوین کرده که پلیس موظف به اجرای این قوانین است.

۳. مقابله با استخراج غیرقانونی: استخراج ارزهای دیجیتال یکی از حوزه‌های پرچالش در ایران است. به‌دلیل قیمت پایین برق، استخراج ارزهای دیجیتال جذابیت ویژه‌ای پیدا کرده است. پلیس به همراه سایر نهادهای قانونی، اقدام به شناسایی و تعطیلی مزارع استخراج غیرقانونی‌ای می‌کند که بدون مجوزهای لازم فعالیت می‌کنند و ممکن است به شبکه برق کشور آسیب برسانند.

٤. آموزش و آگاه‌سازی عمومی: پلیس ایران تلاش می‌کند تا با برگزاری دوره‌ها و سمینارهای آموزشی، افراد جامعه را نسبت‌به خطرات و کلاهبرداری‌های مرتبط با ارزهای دیجیتال آگاه کند. این برنامه‌های آگاه‌سازی، به جلوگیری از قربانی شدن کاربران و کاهش جرایم مرتبط کمک می‌کند.

۵. همکاری با نهادهای بین‌المللی: مبارزه با جرایم ارزهای مجازی غالباً نیازمند همکاری بین‌المللی است. پلیس ایران در برخی موارد با نهادهای بین‌المللی همکاری می‌کند تا با شبکه‌های جرایم سازمان‌یافته فراملی مقابله کند. این شامل تبادل اطلاعات و تجربیات با سایر کشورها برای بهبود توانایی‌های مقابله با این‌گونه جرایم می‌شود.

٦. پیگیری و بازداشت مجرمان: پلیس ایران با استفاده از تکنیک‌های تحلیلی و تحقیقاتی پیشرفته، به شناسایی و تعقیب مجرمان در حوزه ارزهای دیجیتال می‌پردازد. این اقدامات شامل بازداشت افرادی است که در کلاهبرداری‌های اینترنتی، هک و سرقت ارزهای مجازی نقش دارند.

با توجه به رشد سریع فناوری‌های مرتبط با ارزهای دیجیتال و پیچیدگی‌های این حوزه، پلیس ایران به‌طور پیوسته، نیازمند به‌روزرسانی دانش و تجهیزات خود برای مقابله با جرایم سایبری است. هدف از این اقدامات، تأمین امنیت مالی و حفظ ثبات اقتصادی در برابر تهدیدات ناشی از سوءاستفاده از ارزهای مجازی است.

۹. همکاری بین‌المللی در مبارزه با جرایم مرتبط با ارزهای دیجیتال (اینترپل و یوروپل)

جرایم مرتبط با ارزهای دیجیتال به‌طور فزاینده‌ای دارای ماهیت فرامرزی هستند. این بدان معنی است که فعالیت‌های مجرمانه معمولاً از یک کشور به کشور دیگر گسترش می‌یابند و به‌همین‌دلیل، نیاز به همکاری بین‌المللی برای مقابله با این نوع جرایم به‌شدت احساس می‌شود. نهادهای بین‌المللی مانند اینترپل و یوروپل، نقش اساسی در تسهیل تبادل اطلاعات و هماهنگی بین پلیس کشورها دارند. همکاری‌های بین‌المللی در جهت مبارزه با جرایم مرتبط با ارزهای دیجیتال، به دلایل زیر می‌تواند مفید واقع شود:

۱. ماهیت فرامرزی جرایم: از آنجایی که ارزهای دیجیتال به‌صورت آنلاین استخراج می‌شوند و معامله آن‌ها به‌صورت اینترنتی انجام می‌شود، به‌سختی می‌توان فرد مجرم یا کلاهبردار را شناسایی کرد.[۲۷] بسیاری از جرایم مرتبط با ارز دیجیتال مانند پول‌شویی، کلاهبرداری و تأمین مالی تروریسم فراتر از مرزهای ملی صورت می‌گیرند. مجرمان ممکن است از تبادل ارزهای دیجیتال برای پنهان‌سازی فعالیت‌های خود استفاده کنند. به همین دلیل، توانایی شناسایی و پیگیری این تراکنش‌ها نیازمند همکاری بین‌المللی است.

۲. تبادل اطلاعات: نظام همکاری بین‌المللی در قلمرو کیفری زاییده هم محدودیت و هم ضرورت رویارویی با بزهکاران فراملی است؛ محدودیت، زیرا قلمرو حاکمیت دولت‌ها بیرون از سرزمین، در تلاقی با حاکمیت دولت دیگر متوقف می‌ماند و هرگز مأموران یک دولت بدون استعانت از قوای عمومی دولت بیگانه، نمی‌توانند به ساده‌ترین صورت‌های معاضدت نظیر احضار متهم، ضبط اموال و ابلاغ احکام و غیره بپردازند. ضرورت، زیرا منافع دولت ها ایجاب می کند که خود را به قواعدی پایبند کنند که ضامن و حافظ منافع مشترک همه آن‌هاست.[۲۸] نهادهای بین‌المللی مانند یوروپل و اینترپل، با فراهم آوردن بسترهای مناسب برای تبادل اطلاعات، به پلیس‌های محلی کمک می‌کنند تا با آگاهی بیشتری عمل کنند. این اطلاعات شامل جزئیات مربوط به تراکنش‌ها، شناسایی مجرمان، و الگوهای جرمی است که می‌تواند به شناسایی و پیشگیری از جرایم کمک کند.

۳. توسعه استراتژی‌های مشترک: همکاری بین‌المللی همچنین به توسعه و پیاده‌سازی

---

۲۷. امیررضا تتها و فرنام خسروی پور، «بررسی ارزهای دیجیتال و تبیین جرائم ناشی از آن»، *یازدهمین کنفرانس بین‌المللی مطالعات مدیریت، حسابداری و حقوق* (۱۴۰۳): ۲۱۴.

۲۸. محمدعلی اردبیلی، *معاضدت قضایی و استرداد مجرمین* (تهران: نشر میزان، ۱۴۰۲)، ۱۸.

استراتژی‌های مشترک کمک می‌کند. این استراتژی‌ها می‌توانند شامل رویکردهـای جدیـد در تحلیل داده‌ها، به‌اشـتراک‌گذاری تکنیک‌هـا و ابزارهـای ردیـابی، و طراحـی چهارچوب‌هـای قانونی مشترک باشند.

از عملیات‌های موفق در این زمینه، می‌توان به یوروپل اشـاره کـرد کـه در سـال ۲۰۲٤، بـا همکاری پلیس کشورهای مختلف، موفق به شناسایی و انهدام یک شبکه پول‌شویی بزرگ شد که از ارزهای دیجیتال استفاده می‌کردند. این عملیات شامل تحلیل داده‌های بلاکچین و تبادل اطلاعات میان نهادهای مختلف بود که به شناسایی ۲۰ مظنون اصلی منجـر شـد و نزدیـک بـه ٦۰ میلیون یورو از وجوه مشکوک مسدود گردید.[۲۹] بـا اسـتفاده از ابزارهـای پیشـرفته تحلیـل بلاکچین، نیروهای پلیس قـادر بـه شناسـایی الگوهـای غیرعـادی و تراکنش‌هـای مشـکوک شدند. این تجزیه‌وتحلیل‌ها کمک کرد تا پیوندهای مـالی بـین مجرمـان شناسـایی شـوند و در نهایت، به جمع‌آوری شواهد منجر گردد. یوروپل همچنین به ایجاد گروه‌های عملیاتی مشترک کمک کرد که شامل مأموران پلیس و متخصصان فناوری اطلاعات از کشورهای مختلف بـود. این گروه‌ها به‌طور مشترک، روی پرونده‌های خاص کار می‌کردند و با تبادل اطلاعات در زمـان واقعی، به شناسایی و متوقف کردن فعالیت‌های مجرمانه کمک می‌کردند.

اینترپل نیز در مبارزه با جرایم مرتبط با ارزهای دیجیتال نقش مهمی ایفا می‌کنـد. اینترپـل با تقویت خدمات پشتیبانی که به نیروهای پلیس در ۱۹۵ کشور عضو خـود ارائـه می‌دهـد، بـه افزایش تلاش‌های ملی برای مقابله با جرایم ارز دیجیتـال کمـک می‌کنـد. برخـی از اقـدامات کلیدی شامل موارد زیر است:

۱. افزایش توانایی شناسایی و تحقیق: اینترپل به کشورهای عضو خـود کمـک می‌کنـد تـا ظرفیت‌های خود را برای پیشگیری، شناسایی، تحقیق و مختل کردن جـرایم سـایبری افـزایش دهند.

۲. همکاری و اطلاعات مشترک: ماده ۳۱ اساسنامه اینترپل، با تأکیـد بـر اهمیـت انجـام معاضدات پلیسی بیان می‌دارد: «به‌منظور رسیدن بـه اهـداف نهـایی سـازمان، نیـاز دائمـی بـه همکاری وسیع در امور پلیسی با اعضای خود، براسـاس امکانـات و قـوانین داخلـی کشـورها ضروری است.» با توجه به اهمیت تأمین اطلاعات، دلایل و اسـناد معتبـر در اثبـات جـرایم و

29. “Operation DisrupTor: International Law Enforcement Operation Disrupts Major Online Drug Market.” Europol, accessed September 22, 2020, https://www.europol.europa.eu .

اجرای عدالت، دفاتر ملی مرکزی اینترپل با ایجاد شبکه ارتباطی پیشرفته بین دبیرخانه کل و کشورهای عضو و ایجاد زمینه‌های مناسب در محدوده‌ای وسیع، می‌توانند در امر تأمین اطلاعات، اسناد تبادل سریع و دقیق آن‌ها با استفاده از ظرفیت‌ها و امکانات وسیع و پیشرفته خود نقش مهمی را ایفا کنند.[۳۰] با ایجاد شبکه‌های جهانی همکاری‌های پلیسی، اینترپل بستری برای تبادل اطلاعات حیاتی درمورد فعالیت‌های مشکوک و کلاهبرداری‌ها فراهم می‌کند.

۳. آموزش و آگاهی‌بخشی: اینترپل برنامه‌های آموزشی و کارگاه‌های تخصصی برای آموزش پرسنل در زمینه شناسایی و مقابله با تهدیدات ارز دیجیتال ترتیب می‌دهد.

٤. کنفرانس‌های جهانی و همکاری‌های بین‌المللی: اینترپل با سازمان‌دهی کنفرانس‌های جهانی بر روی ارزهای دیجیتال و تأکید بر تقویت توانایی‌های کشورهای عضو در زمینه تحقیق، شناسایی و متلاشی کردن شبکه‌های مرتبط با پول‌شویی و دیگر جرایم مالی تلاش می‌کند.

۵. تجهیز به فناوری‌های پیشرفته: اینترپل با استفاده از فناوری‌های پیشرفته و تحلیل داده‌ها، توانایی‌های کشورهای عضو را در ردیابی تراکنش‌های مشکوک افزایش می‌دهد. این اقدامات شامل توسعه ابزارهایی برای تحلیل بلاکچین و شناسایی الگوهای مجرمانه است.

این فعالیت‌ها به‌وضوح نشان می‌دهند که اینترپل همواره به‌دنبال تقویت همکاری‌های بین‌المللی و بهبود روش‌های مبارزه با جرایم مربوط به ارزهای دیجیتال است. با توجه به پیچیدگی این جرایم و طبیعت فرامرزی آن‌ها، اینترپل به‌عنوان یک نهاد بین‌المللی، نقش کلیدی در ایجاد امنیت و ثبات در فضای اقتصادی جهانی ایفا می‌کند. اینترپل به‌عنوان یکی از بزرگ‌ترین سازمان‌های پلیس بین‌المللی، به تسهیل همکاری میان نیروهای پلیس کشورهای مختلف کمک می‌کند. این سازمان با ارائه یک پلتفرم برای تبادل اطلاعات و هماهنگی میان نهادها، به تسریع فرایند تحقیقات و عملیات‌های مشترک کمک می‌کند.[۳۱]

همکاری‌های بین‌المللی توسط اینترپل و یوروپل چالش‌هایی نیز به همراه دارد که مهم‌ترین آن‌ها عبارت‌اند از:

---

۳۰. انوشیروان کریمی، «نقش اینترپل در انجام معاضدات حقوقی و پلیسی در راستای استرداد مجرمین»، *مجله مطالعات بین‌المللی پلیس*، شماره ۶ (۱۳۹۰): ۱۷.

۳۱. حمیدرضا شعبانی‌فرد، *شرحی بر اسناد و ظرفیت‌های حقوقی سازمان اینترپل* (تهران: مهاجر، ۱۴۰۰)، ۱۱۸.

۱. اختلافات قانونی و قضایی: کشورهای مختلف ممکن است قوانین و مقررات متفاوتی درمورد ارزهای دیجیتال و جرایم مرتبط داشته باشند. این اختلافات می‌تواند مانع از همکاری مؤثر شود.

۲. محدودیت‌های فنی و فناوری: درحالی‌که بسیاری از کشورها به فناوری‌های پیشرفته دسترسی دارند، برخی دیگر ممکن است از منابع و امکانات لازم برای تحلیل داده‌های پیچیده برخوردار نباشند.

۳. تأمین منابع: بسیاری از عملیات‌های مشترک نیازمند منابع انسانی و مالی قابل‌توجهی هستند که ممکن است برای کشورهای مختلف در دسترس نباشد.[۳۲]

در نهایت، همکاری بین‌المللی در مبارزه با جرایم ارز دیجیتال ضروری است. نهادهای بین‌المللی مانند اینترپل و یوروپل، با فراهم آوردن بسترهای مناسب برای تبادل اطلاعات و توسعه استراتژی‌های مشترک، نقش کلیدی در شناسایی و انهدام شبکه‌های مجرمانه ایفا می‌کنند. بااین‌حال، برای افزایش کارایی این همکاری‌ها، لازم است که چالش‌های موجود برطرف شوند و کشورها به یک توافق مشترک در زمینه قوانین و مقررات دست یابند.

۱۰. نتیجه‌گیری

توسعه اقتصاد دیجیتال به تغییرات قابل‌توجهی در ساختار اجتماعی و سیستم‌های مالی منجر شده است. در این سیستم جدید، تعاملات تجاری و پرداخت‌ها بیشتر به‌صورت مجازی انجام می‌شوند که باعث صرفه‌جویی در زمان، انرژی و هزینه‌ها می‌شود و کارایی اقتصادی را افزایش می‌دهد. ارزهای دیجیتال به‌عنوان یکی از دستاوردهای فناوری‌های دیجیتال، فرصت‌ها و چالش‌های جدیدی برای اقتصاد جهانی ایجاد کرده‌اند. این ارزها به ارائه امکانات جدید برای معاملات و سرمایه‌گذاری کمک می‌کنند، اما همچنین چالش‌های امنیتی و قانونی جدیدی به همراه دارند.

نقش پلیس و چالش‌های مرتبط با ارزهای دیجیتال: پلیس به‌عنوان یکی از نهادهای اساسی در مقابله با جرایم، با چالش‌های جدیدی در زمینه ارزهای دیجیتال مواجه است. ویژگی‌های منحصربه‌فرد این ارزها، مانند ناشناسی و ماهیت فرامرزی تراکنش‌ها، کار پلیس را پیچیده‌تر می‌کند. در این راستا، کشورها باید قوانین جامع و به‌روز برای مدیریت و مقابله با

۳۲. صادق سلیمی، *اینترپل: از تعقیب تا تضمین حقوق متهمین و مجرمین* (تهران: شهر دانش، ۱۴۰۲)، ۲۴۴.

جرایم ارز دیجیتال تصویب کنند. بعضی کشورها پیشرفت‌های قابل‌توجهی در این زمینه داشته‌اند، درحالی‌که دیگران هنوز در حال توسعه و تدوین این قوانین هستند.

همکاری و هماهنگی بین‌المللی برای مقابله مؤثر با این جرایم حیاتی است. با توجه به تکامل سریع فناوری‌های دیجیتال، پلیس باید به‌طور مداوم، استراتژی‌ها و روش‌های خود را به‌روز کند. این شامل بررسی تطبیقی اقدامات موفق در کشورهای مختلف و ایجاد نوآوری در روش‌های پیشگیری و مقابله با جرایم مرتبط با ارزهای دیجیتال است. در نتیجه، پلیس نیازمند رویکردی جامع و بین‌المللی برای مقابله با جرایم ارز دیجیتال است. کشورها با یادگیری از تجربیات یکدیگر و بهبود قوانین و استراتژی‌های پلیسی، می‌توانند به‌صورت مؤثرتری به این چالش‌ها پاسخ دهند. در عین حال، نوآوری در روش‌های اجرایی و استفاده از فناوری‌های نوین می‌تواند به تقویت بیشتر امنیت در عرصه اقتصاد دیجیتال کمک کند. همچنین، با توجه به پیچیدگی تکنولوژی بلاکچین و ناشناسی تراکنش‌ها، پلیس نیازمند تخصص‌های فنی پیشرفته‌ای مانند تحلیل داده‌های بلاکچین و استفاده از ابزارهای تحلیلی پیشرفته است. همین امر لزوم آموزش‌های ویژه و به‌روزرسانی مداوم دانش فنی نیروهای پلیس را تقویت می‌کند.

کشورهایی مانند ایالات متحده، با تصویب قوانین خاص مانند BSA و PATRIOT، توانسته‌اند چهارچوب قانونی محکمی برای نظارت و مقابله با جرایم مرتبط با ارزهای دیجیتال ایجاد کنند. این قوانین به پلیس امکان می‌دهند فعالیت‌های مالی مشکوک را شناسایی و نظارت کنند. گرچه اتحادیه اروپا، به‌طور کلی، مقررات گسترده‌ای برای ارزهای دیجیتال ندارد، اما با استفاده از مقررات AMLD5 و AMLD6، به شفافیت و تنظیم دقیق‌تری بر فعالیت‌های ارزهای دیجیتال، به‌ویژه در زمینه مبارزه با پول‌شویی و تأمین مالی تروریسم پرداخته است. مقررات AMLD5 و AMLD6 ابزارهای قانونی لازم را برای کشورهای عضو فراهم کرده تا پلیس بتواند به شکلی مؤثرتر، در شناسایی و مقابله با جرایم مرتبط با ارزهای دیجیتال فعالیت کند. این قوانین به نظارت جدی‌تر بر تراکنش‌های مشکوک و شفافیت در بازارهای مالی کمک می‌کنند. به‌طور کلی، تلاش‌های اتحادیه اروپا در حوزه ارزهای دیجیتال با هدف ایجاد شفافیت و امنیت بیشتر در بازار مالی دیجیتال، و مقابله مؤثر با جرایم مرتبط، به‌صورت کاملاً هماهنگ و با بهره‌گیری از چهارچوب‌های قانونی سخت‌گیرانه صورت می‌گیرد. این اقدامات نقش بسزایی در ایجاد یک فضای امن برای تعاملات دیجیتال در سطح اروپا ایفا می‌کند.

پلیس کانادا، با استفاده از فناوری‌های مدرن و ابزارهای تحلیل بلاکچین، بـه شناسـایی و دنبـال کـردن تراکنش‌هـای مشـکوک و فعالیت‌هـای مجرمانـه مـرتبط بـا ارزهـای دیجیتـال می‌پردازد. این تلاش‌ها شامل استفاده از ابزارهای تحلیل بلاکچین می‌شود که امکـان پیگیـری مسیر تراکنش‌ها و شناسایی شبکه‌های مجرمانه را فراهم می‌کند. پلیس کانادا با کنتـرل دقیـق فعالیت‌های مالی و همکاری با مرکز تجزیه‌وتحلیل معـاملات و گزارش‌هـای مـالی کانـادا، بـه شناسایی و جلوگیری از پول‌شویی و تأمین مالی تروریسم می‌پردازد. به‌طور کلی، پلـیس کانـادا برای مقابله با جرایم مرتبط با ارزهـای دیجیتـال از ترکیبـی از فناوری‌هـای نـوین، روش‌هـای تحلیلی، و همکاری‌های بین‌المللی بهره می‌برد. این اقدامات بـه افـزایش توانایی‌هـا و کـارایی نیروهای انتظامی در مقابله با چالش‌های جدید در این حوزه کمک می‌کند.

پلیس ایران، به‌ویژه پلیس فتا، واحدهای تخصصی برای مقابله با جرایم مرتبط بـا ارزهـای دیجیتال ایجاد کرده است. این واحدها به شناسایی، پیگیری و تجزیه‌وتحلیل مـوارد مشـکوک می‌پردازند و در تشخیص و جلوگیری از جرایم سایبری نقـش دارنـد. نظـارت بـر فعالیت‌هـای صرافی‌های دیجیتال یکی از وظایف کلیدی پلیس است که با هماهنگی با دیگر نهادهای مـالی انجام می‌شود. این نظارت به‌منظور جلوگیری از پول‌شویی و تراکنش‌های غیرقـانونی ضـروری است. بنابراین، به‌دلیل جـذابیت اقتصـادی اسـتخراج ارزهـای دیجیتـال در ایـران، نظـارت و شناسـایی مـزارع اسـتخراج غیرقـانونی ضـرورت دارد. ازسـوی‌دیگـر، بـا برگـزاری دوره‌هـا و سمینارها، پلیس ایران تلاش می‌کند تا کاربران را درمورد خطرات و کلاهبرداری‌های مرتبط بـا ارزهای دیجیتال آگاه سازد، که این به کاهش جرایم مرتبط کمک می‌کند. همکاری بین‌المللی در مقابله با جرایم سازمان‌یافته فراملی از اهمیت بالایی برخوردار اسـت. پلـیس ایـران نیـاز بـه همکاری بیشتر با نهادهای بین‌المللی در زمینـه تبـادل اطلاعـات و تجربیـات دارد. همچنـین پلیس ایران نیازمند بهره‌گیری از روش‌های پیشرفته تحلیل و تحقیق برای شناسایی و بازداشت مجرمـان در حـوزه ارزهـای دیجیتـال اسـت. در کـل، پلـیس ایـران نیازمنـد بـه‌کارگیری اسـتراتژی‌های تخصصـی و به‌روزرسـانی مـداوم دانـش و ابزارهـای خـود، بـرای مقابلـه بـا چالش‌های جرایم ارزهای دیجیتال است. هـدف ایـن اقـدامات، افـزایش امنیـت اقتصـادی و جلوگیری از سوءاستفاده‌های احتمالی از فناوری‌های نوین مالی است.

۱۱. پیشنهادات

۱. تدوین قوانین جامع و تخصصی: نظام حقوقی ایران نیازمند تدوین قوانین مـدون و جـامعی

است که به‌طور خاص، به جرایم مرتبط با ارزهای دیجیتال بپردازد. این قوانین باید شامل تعریف دقیق اصطلاحات کلیدی، جرم‌انگاری رفتارهای مجرمانه (مانند پول‌شویی، کلاهبرداری، قمار و ...) و تعیین مجازات‌های متناسب باشد.

۲. توسعه زیرساخت‌های فنی و تخصصی: کشف و پیگیری جرایم ارز دیجیتال نیازمند دانش فنی بالا و دسترسی به ابزارهای تخصصی است. ایجاد واحدهای تخصصی در پلیس فتا و سایر نهادهای انتظامی و قضایی، تجهیز آن‌ها به نرم‌افزارها و سخت‌افزارهای موردنیاز و آموزش تخصصی پرسنل، ازجمله اقدامات ضروری در این زمینه است.

۳. تقویت همکاری‌های بین‌المللی: ماهیت فرامرزی ارزهای دیجیتال، همکاری بین‌المللی را برای مقابله با جرایم مرتبط ضروری می‌سازد. عقد معاهدات دوجانبه و چندجانبه با سایر کشورها در زمینه تبادل اطلاعات، استرداد مجرمان و همکاری در تحقیقات، می‌تواند به‌طور مؤثری در این زمینه کمک کند.

۴. ارتقای آگاهی عمومی و آموزش: بسیاری از قربانیان جرایم ارز دیجیتال به‌دلیل ناآگاهی از خطرات و نحوه عملکرد این فناوری فریب می‌خورند. برگزاری دوره‌های آموزشی و اطلاع‌رسانی عمومی درخصوص ارزهای دیجیتال، نحوه سرمایه‌گذاری امن و راه‌های شناسایی کلاهبرداری‌ها، می‌تواند از وقوع بسیاری از جرایم پیشگیری کند.

۵. توسعه سازوکارهای پیشگیری: پیشگیری از وقوع جرم، همواره کم‌هزینه‌تر و مؤثرتر از مقابله با آن است. ایجاد سامانه‌های هشداردهی زودهنگام برای شناسایی فعالیت‌های مشکوک در حوزه ارزهای دیجیتال، نظارت بر فعالیت صرافی‌های ارز دیجیتال و سایر ارائه‌دهندگان خدمات مرتبط، و حمایت از توسعه فناوری‌های امنیتی، می‌تواند به کاهش وقوع جرایم کمک کند.

۶. تغییر نگرش نسبت‌به ارزهای دیجیتال: نگرش منفی و محدودکننده نسبت‌به ارزهای دیجیتال، می‌تواند مانع از بهره‌گیری از فرصت‌های این فناوری و همچنین مانع از تدوین قوانین و مقررات مناسب شود. انجام مطالعات کارشناسی و تحقیقات علمی برای درک بهتر مزایا و معایب ارزهای دیجیتال، و ایجاد فضای گفت‌وگو بین متخصصان و سیاست‌گذاران، می‌تواند به تدوین سیاست‌های واقع‌بینانه و متناسب با شرایط ایران کمک کند.

سیاهه منابع

الف- منابع فارسی:

آیین‌نامه اجرایی احراز عنوان ضابط دادگستری، مصوب ۱۳۹۸.

اردبیلی، محمدعلی. *معاضدت قضایی و استرداد مجرمین*. تهران: نشر میزان، ۱۴۰۲.

تنها، امیررضا، و فرنام خسروی‌پور. «بررسی ارزهای دیجیتال و تبیین جرائم ناشی از آن» *یازدهمین کنفرانس بین‌المللی مطالعات مدیریت، حسابداری و حقوق* (۱۴۰۳): ۲۱۶_۱۹۹.

درویشی، صیاد. «بررسی دانش و مهارت موردنیاز پلیس در پیشگیری وضعی از جرم»، *فصلنامه پژوهش‌های دانش انتظامی* ۱۹ (۱۳۹۶): ٦٨-٤٧.

ساکیانی، زهرا، و سید عباس واعظی. «امکان‌سنجی قاچاق کالا و ارز درخصوص دستگاه‌های استخراج رمزارز و مبادلات رمزارزها: مسائل قانونی و رویه‌های عملی»، *فصلنامه آموزه‌های حقوق کیفری* ۱۹، شماره ۲۴ (۱۴۰۱): ١٥٦-١٢٥.

سلیمی، صادق. *اینترپل: از تعقیب تا تضمین حقوق متهمین و مجرمین*. تهران: شهر دانش، ۱۴۰۲.

شعبانی‌فرد، حمیدرضا. *شرحی بر اسناد و ظرفیت‌های حقوقی سازمان اینترپل*. تهران: مهاجر، ۱۴۰۰.

قانون آیین دادرسی کیفری.

قانون نیروی انتظامی جمهوری اسلامی ایران.

کریمی، انوشیروان. «نقش اینترپل در انجام معاضدات حقوقی و پلیسی در راستای استرداد مجرمین»، *مجله مطالعات بین‌المللی پلیس*، شماره ۶ (۱۳۹۰): ۳۰-۵.

کشمیری، مریم. *سرقت هویت در فضای سایبری: مقایسه تطبیقی حقوق ایران و کانادا*. تهران: نشر سیمرغ آسمان آذرگان، ۱۳۹۷.

ب- منابع لاتین:

Bagaric, Mirko, Richard Edney, and Theo Alexander. *Sentencing in Australia*. 8th edition, [N.P]: Lawbook, 2020.

Bryanov, K. "France and Germany: How Regulatory Traditions in Two Countries Could Affect EU Legislation." *CoinTelegraph* (2018).

Bundesregierung. "Goals Adopted in the Area of Cyber Security." Federal Government of Germany, Accessed September 8, 2021, https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688

Cipher Trace. Cryptocurrency Anti-Money Laundering Report – Q4 2018 Jan 4

(2019).

Deloitte. “New Challenges for the Digitization of Germany: What the IT Security Act 2.0 and the New KRITIS-Ordinance Entail.” Deloitte Legal Germany, Accessed 2021, https://www2.deloitte.com/dl/en/pages/legal/articles/it-sicherheitsgesetz-kritis-verordnung.html

European Parliament and Council of the European Union. “Directive (EU) 2018/843 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing.” *Official Journal of the European Union*, L 156/43 (2018).

Gile, K. “Chainalysis Reactor Aids Canadian Law Enforcement in Tracking Crypto Cybercrimes.” BitDegree, Accessed 2023, https://www.bitdegree.org/crypto/news/chainalysis-reactor-aids-canadian-law-enforcement-in-tracking-crypto-cybercrimes .

“Guidance on Virtual Currency.” FinCEN, Accessed 2021. https://www.fincen.gov

Interpol. “Cryptocurrency Training for Law Enforcement.” 2019. https://www.interpol.int

Maras, M-H. *Cybercriminology*. New York: Oxford University Press, 2016.

Miseviciute, J. “Virtual Currency Regulation in the EU.” *Journal of Investment Compliance* 19, no. 3 (2018): 33-38.

Muncaster, Phil. “German Police Shutter 47 Criminal Crypto Exchanges.” *Infosecurity Magazine*, Accessed May 10, 2025. https://www.infosecurity-magazine.com/news/german-police-shut-47-criminal/

Needleman, Sarah E., and Spencer E. Ante. “Bitcoin Startups Begin to Attract Real Cash.” *Wall Street Journal* 8 (2013).

“Operation Disrup Tor: International Law Enforcement Operation Disrupts Major Online Drug Market.” Europol, Accessed September 22, 2020. https://www.europol.europa.eu .

Reda, H.A. “Terrorist Financing: Are Current Anti-Money Laundering Regulations Easily Applied to Virtual Currencies?” PhD diss., Colorado Technical University, 2017 .

Schulze, Matthias. “German Police Dismantles Illegal Crypto Exchanges.” CSO Online, Accessed September 20, 2024, https://www.csoonline.com/article/3535563/german-police-dismantles-illegal-crypto-exchanges.html?utm_source=dlvr.it&utm_medium=mastodon

“The Financial Crimes Enforcement Network.” U.S. Department of the Treasury. Accessed 2021 .https://www.treasury.gov

U.S. Department of Justice. “Report on Cryptocurrency Enforcement Framework.” *Office of Public Affairs* (2020).

U.S. Internal Revenue Service. “Letter, No. 2016-0036.” (2016). https://www.irs.gov/pub/irs-wd/16-0036.pdf