شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

فصلنامه تمدن حقوقی

تمدن حقوقی

دوره ۸ - شماره ۲۶ - زمستان ۱۴۰۴

تحلیل مسئولیت بانک گشاینده در حقوق اعتبارات اسنادی
همایون مافی، محسن رئیسی
نقش هوش مصنوعی در بهبود فرآیندهای تحقیق کیفری و تحلیل شواهد دیجیتال در نظام حقوقی ایران
امیررضا محمودی، زهرا رهنما
بازخوانی تعهدات قراردادی در شرایط تورم شدید؛ تحلیلی از ظرفیت‌های تعدیل در حقوق ایران
شیما شکوری بلقور، قاسم نبی زاده کبریا
آسیب شناسی سیاست کیفری ایران در قبال جرائم بغی، محاربه و افساد فی‌الارض در پرتو مفهوم امنیت ملی و ثبات سیاسی کشور
روح الله شیخی، محمد محمودی
چهارچوب مسئولیت مدنی ناشی از فعالیت‌های تفریحی پرخطر؛ مطالعه اتاق‌های فرار
رحیم مختاری، غلامحسین کشاورز
دعاوی ناشی از مالکیت فکری در نظام حقوقی ایران
سیدمحمدباقر حقایقی، محمدرضا نصیری، امیرحسن ابوالحسنی
تحلیل جرم‌شناختی جرایم حوزه رمزارزها: مطالعه کلاهبرداری‌های رایج در ایران
حسین محمودی تکانلو، رویا آسیایی
راهبردهای پیشگیرانه از جرم رانت خواری در سیاست کیفری ایران با تاکید بر چالش ها و خلاءهای جرم شناختی
فاضل موحدی، حمیدرضا کناری زاده، داود سلمانپور
واکاوی اصل تناسب میان جرم و مجازات در ساختار دیوان کیفری بین‌المللی
حسن پیرفلک لسکوکلایه، طیبه قدرتی سیاهمزگی
توافق طرفین قرارداد در تعیین ادله اثبات دعوا
حبیب اله عبداله پور، مهدی شجاعی
عملکرد دادگاه‌های کیفری در پیشگیری از جرم: با نگاهی به جرم‌شناسی انتقادی و تمرکز بر نظام قضایی ایران
ایرج مروتی، نغمه فرهود
مسئولیت دولت‌ها در قبال تروریسم بین‌المللی و دیپلماسی ضدتروریسم
مسعود سرفرازی صالح، مهدی قره داغی
پایان حکمرانی متمرکز: تحلیل ظهور حکمرانی غیرمتمرکز در عصر بلاکچین و قراردادهای هوشمند
هادی زارع، مجید وزیری
تحلیل تطبیقی حمایت‌های جبرانی تأمین اجتماعی در قبال خسارت بدنی و دامنه شمول زیان‌دیدگان در ایران و انگلستان
زینب تاری
انتقال دعاوی در نظام حقوقی ایران با تأکید بر مقررات و ماده‌های منتخب قانون ثبت اسناد و املاک
امیررضا علی تبار
جایگاه هوش مصنوعی در پهنه سیاستگذاری جنایی
محبوبه طالبی رستمی
تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد به نتیجه یا تعهد به وسیله در حقوق خصوصی
سیدامیرحسن مصطفوی
مسئولیت کیفری شرکت‌های فناوری در قبال جرائم ارتکابی کاربران
وحید کیومرثی
مسئولیت مدنی ناشی از پردازش خودکار داده های شخصی توسط هوش مصنوعی در حقوق ایران و افغانستان (با نگاهی به اسناد بین المللی)
راضیه جعفرزاده، وحید حمیدی، محمدرضا رشید
بررسی تأثیر آگاهی حقوقی و شفافیت در پیشگیری و کاهش فساد اداری و مالی
سیده مهشید میری بالاجورشری
مالکیت داده های شخصی در حقوق خصوصی؛ از حق شخصیت تا مال غیرمادی
سینا یوسفی
مسئولیت مدنی پزشک و سازنده ربات در جراحی‌های رباتیک نظام های حقوقی ایران و انگلستان
ابراهیم شیروانی
تحلیلی بر مسئله أخذ خسارت تأخیر تادیه از محکوم به دولتی
محمدمهدی رضوانی فر، زهرا سلیمی
آثار حقوقی و اداری تملک بر وضعیت ثبتی املاک در نظام حقوقی ایران
احسانه وثوقی منفرد، محمد وارسته بازقلعه
دیپلماسی اقتصادی و حقوق قراردادهای بین‌المللی خصوصی؛ تعامل سیاست و حقوق در تأمین منافع ملی
رادمهر رحمانی گل افشان
پذیرش تشخیص تقلب مبتنی بر هوش مصنوعی در بانکداری: نقش اعتماد، شفافیت و ادراک انصاف در موسسات مالی در ایران، امارات متحده عربی و قطر
عبدالمجید یوسفی
جرم‌شناسی جنگ در واقعیت‌های کنونی و لزوم توسعه آن در اوکراین
یاسر شاکری

Legal Civilization
Vol. 8, No. 26, Winter 2026
Pages: 167-182
Article Type: Original Research
https://www.pzhfars.ir/article_238740.html
doi: 10.22034/lc.2026.568479.1725

تمدن حقوقی
دوره ۸، شماره ۲۶، زمستان ۱۴۰۴
صفحات: ۱۸۲-۱۶۷
نوع مقاله: پژوهشی

Criminological Analysis of Crimes in the Field of Cryptocurrencies: A Study of Common Frauds in Iran

Hossein Mahmoudi Tekanloo
Master's student, Department of Criminal Law and Criminology, Faculty of Law, Islamic Azad University, Central Tehran Branch, Tehran, Iran (Corresponding Author)

Roya Asiaei
Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, Islamic Azad University, Central Tehran Branch, Tehran, Iran

Abstract

This research aims to conduct a criminological analysis of the causes, contexts, and common methods of cryptocurrency fraud in the social and economic context of Iran. The study method is descriptive-analytical and based on library-documentary sources. The theoretical framework of the research is based on opportunity-based models, especially the theory of everyday activities and the theory of space transfer, which explain how the criminal context is formed in cyberspace. The findings show that the occurrence of cryptocurrency fraud in Iran is the result of the intersection of a motivated criminal, a suitable target, and the lack of an efficient guard. This weakness of guarding has crystallized at three levels: the individual level due to the low financial and digital literacy of the victims; the environmental level due to incomplete monitoring of exchange platforms and influencers' advertising activities, such as advertisements for buying counterfeit tokens on Instagram and Telegram; and the institutional level due to legal loopholes and legal ambiguity of virtual assets. The research concludes that effectively combating these crimes requires a preventive and multi-level criminal policy. This policy should focus on strengthening the watchdog through public education to raise user awareness, hardening the criminal environment, and developing specialized and transparent laws that criminalize new behaviors while ensuring enforcement that is appropriate to the cross-border and technical nature of cryptocurrencies.

Keywords: Cryptocurrency Fraud, Routine Activity Theory, Space Transition Theory, Financial Literacy, Situational Prevention.

Received: 2026/01/02 -Review: 2026/02/08 -Accepted: 2026/03/18

تحلیل جرم‌شناختی جرایم حوزه رمزارزها: مطالعه کلاهبرداری‌های رایج در ایران

حسین محمودی تکانلو
دانشجوی کارشناسی‌ارشد، گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران (نویسنده مسئول)
hosein.hmt.432@gmail.com
http://orcid.org/0009-0001-5969-855x

رویا آسیایی
استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران
r.asiyayi@yahoo.com

چکیده

این پژوهش با هدف تحلیل جرم‌شناختی علل، زمینه‌ها و شیوه‌های رایج کلاهبرداری رمزارزی در بستر اجتماعی و اقتصادی ایران انجام شده است. روش مطالعه توصیفی-تحلیلی و مبتنی‌بر منابع کتابخانه‌ای-اسنادی است. چهارچوب نظری پژوهش بر مدل‌های فرصت‌محور، به‌ویژه نظریه فعالیت‌های روزمره و نظریه انتقال فضا استوار است که چگونگی شکل‌گیری بستر بزهکاری در فضای سایبر را تبیین می‌کنند. یافته‌ها نشان می‌دهند که وقوع کلاهبرداری‌های رمزارزی در ایران نتیجه تلاقی بزهکار انگیزه‌دار، هدف مناسب و فقدان نگهبان کارآمد است. این ضعف نگهبانی در سه سطح تبلور یافته است: سطح فردی به‌واسطه پایین بودن سواد مالی و دیجیتال بزه‌دیدگان؛ سطح محیطی به‌دلیل نظارت ناقص بر پلتفرم‌های تبادل و فعالیت تبلیغاتی اینفلوئنسرها مانند تبلیغات خرید توکن‌های تقلبی در اینستاگرام و تلگرام؛ و سطح نهادی به‌واسطه خلاءهای قانونی و ابهام حقوقی دارایی‌های مجازی. نتیجه‌گیری پژوهش حاکی از آن است که مقابله مؤثر با این جرائم مستلزم اتخاذ سیاست جنایی پیشگیرانه و چندسطحی است. این سیاست باید بر تقویت نهاد نگهبانی از طریق آموزش عمومی جهت ارتقای هوشیاری کاربران، سخت‌سازی محیط بزهکار و تدوین قوانین تخصصی و شفاف متمرکز گردد؛ قوانینی که ضمن جرم‌انگاری رفتارهای نوین، ضمانت اجراهای متناسب با ماهیت فرامرزی و فنی رمزارزها را فراهم آورد.

واژگان کلیدی: کلاهبرداری رمزارزی، نظریه فعالیت‌های روزمره، نظریه انتقال فضا، سواد مالی، پیشگیری وضعی.

دریافت مقاله: ۱۴۰۴/۱۰/۱۲ – بازنگری مقاله: ۱۴۰۴/۱۱/۱۹ – پذیرش مقاله: ۱۴۰۴/۱۲/۲۷

ارجاع:
محمودی تکانلو، حسین؛ آسیایی، رویا؛ (۱۴۰۴)، تحلیل جرم‌شناختی جرایم حوزه رمزارزها: مطالعه کلاهبرداری‌های رایج در ایـران، تمدن حقوقی، شماره ۲۶.

مقدمه

ظهور فناوری بلاکچین و دارایی‌های دیجیتال همچون بیت‌کوین، اتریوم و... انقلابی قابل‌توجه در نظام‌های مالی جهانی ایجاد کرده است. این پدیده نوظهور با ویژگی‌های ذاتی خود مانند غیرمتمرکز بودن، سرعت بالای تراکنش‌ها و ماهیت شبه‌گمنام، در کنار فرصت‌های اقتصادی، بستر مناسبی را برای ظهور و تکامل اشکال نوینی از بزهکاری به‌ویژه جرایم مالی و کلاهبرداری فراهم آورده است. در کشور ایران، استقبال عمومی از رمزارزها به دلیل عواملی نظیر تورم، بی‌ثباتی اقتصادی و جذابیت کسب سودهای سریع و بالا به‌شدت افزایش یافته است (معاونت علمی پژوهشی، ۱۳۹۸). این رشد سریع بدون وجود زیرساخت‌های قانونی، آموزشی و نظارتی کافی، منجر به آسیب‌پذیری شدید کاربران و رونق گرفتن فعالیت‌های مجرمانه شده است (درویشی‌ها و حسینی، ۱۴۰۴، ۲).

بر اساس گزارش‌های غیررسمی تخمین زده می‌شود سالانه مبالغ هنگفتی به دلیل کلاهبرداری‌های رمزارزی از دست شهروندان خارج می‌شود که این امر نه‌تنها زیان‌های مالی، بلکه آسیب‌های اجتماعی و کاهش اعتماد عمومی به فضای دیجیتال را نیز به دنبال دارد. از میان این جرایم، کلاهبرداری‌های رمزارزی رایج‌ترین و متداول‌ترین شکل بزهکاری است که مستقیماً دارایی‌های

شهروندان را هدف قرار می‌دهد. برخلاف جرائم سنتی که عمدتاً دارای مصادیق ثابت و واضح هستند، کلاهبرداری‌های حوزه رمزارزها دائماً در حال تغییر و تکامل هستند. شیوه‌هایی چون طرح‌های پانزی و هرمی که در قالب پروژه‌های سرمایه‌گذاری توکنی، فیشینگ در پلتفرم‌های مجازی و عرضه‌های اولیه سکه جعلی از جمله مصادیق بارز این بزهکاری‌ها در فضای ایران هستند. ضعف در سواد مالی و دیجیتال عمومی از یک‌سو و ابهامات و خلأهای قانونی در تعریف و تعقیب این دارایی‌ها از سوی دیگر، موجب شده تا مجرمان با بهره‌گیری از فرصت‌های بزهکاری در این فضای کم‌نظارت، ریسک پایین و سود بالایی را تجربه کنند.

در این شرایط پژوهش حاضر تلاش می‌کند تا با رویکردی جرم‌شناختی و نه صرفاً حقوقی، به تحلیل علل و عوامل زمینه‌ساز ارتکاب این جرائم بپردازد. هدف، درک چرایی موفقیت این روش‌های کلاهبرداری در بستر اجتماعی و اقتصادی ایران وشناسایی دقیق مکانیزم‌های بزهکاری از منظر نظریه‌های جرم‌شناسی است. این پژوهش سعی دارد بستر ایران را به‌عنوان یک «محیط با فرصت بزهکاری بالا»[1] تحلیل کند. پژوهش حاضر به تکمیل و بسط نظریه‌های جرم‌شناختی موجود به‌ویژه نظریه فعالیت‌های روزمره و نظریه انتقال فضا در تبیین جرایم نوین حوزه سایبر کمک می‌کند و نشان می‌دهد که چگونه فقدان نگهبان کارآمد و حضور هدف مناسب[2] منجر به افزایش ریسک بزه‌دیدگی می‌شود.

نتایج این پژوهش می‌تواند به سیاستگذاران و قانون‌گذاران در تدوین مقررات شفاف و جامع برای‌شناسایی، تعریف و جرم‌انگاری مصادیق خاص کلاهبرداری‌های رمزارزی کمک کند. این تحلیل باشناسایی دقیق نقاط آسیب‌پذیر مانند عدم آگاهی عمومی و نقش اینفلوئنسرها و همچنین راهکارهای پیشگیری وضعی مؤثر مبتنی‌بر اصل «سخت کردن هدف»[3]، راهکارهای اجتماعی را برای نهادهای مجری قانون، پلیس فتا و نهادهای آموزشی پیشنهاد خواهد کرد. این پژوهش از نظر

1- High-Opportunity Crime Environment

۲- دارایی دیجیتال

3- Hardening the Target

هدف کاربردی و از نظر ماهیت و روش، توصیفی-تحلیلی است.

۱- نظریه ها

این بخش چهارچوب نظری جامع برای تحلیل جرم‌شناختی جرایم رمزارزی و همچنین مرور مختصر مطالعات مرتبط را فراهم می‌آورد.

۱-۱- نظریه‌های جرم‌شناختی فرصت‌محور و محیطی

اول- نظریه فعالیت‌های روزمره و مدل مثلث جرم: این نظریه وقوع بزه را نتیجه تلاقی موفقیت‌آمیز سه عنصر می‌داند: بزهکار با انگیزه، هدف مناسب و فقدان نگهبان کارآمد (کلارک، ۱۹۹۵، ۹۱). گسترش مفهوم نگهبان کارآمد در فضای رمزارز شامل نگهبان فرد[۴]، نگهبان محیطی[۵] و نگهبان کنترلی[۶] است. دوم- نظریه انتقال فضا: [۷] این نظریه تبیین می‌کند که مجرمان با انتقال فعالیت خود از فضای فیزیکی به فضای سایبر[۸] از ویژگی‌هایی نظیر انعطاف‌پذیری هویت[۹] و احساس عدم نظارت[۱۰] بهره می‌برند. سوم- تکنیک‌های خنثی‌سازی: [۱۱] این نظریه به فرآیند تصمیم‌گیری بزهکار با انگیزه کمک می‌کند؛ چرا که مجرمان رمزارزی اغلب با توسل به مکانیسم‌هایی مانند «انکار قربانی»[۱۲] یا «انکار آسیب»[۱۳]، بار اخلاقی جرم را برای خود خنثی می‌کنند تا ریسک روانی جرم کاهش یابد.

۴- سواد مالی قربانی

۵- مدیر صرافی‌ها

۶- قوانین بازدارنده

7- Space Transition Theory

۸- بلاکچین

۹- در فضای سایبری افراد به‌راحتی می‌توانند از هویت‌های غیرواقعی استفاده کنند

۱۰- بسیاری از صرافی‌های خارجی بدون نیاز به احراز هویت و نظارت کافی به مردم خدمات می‌دهند

11- Techniques of Neutralization

۱۲- قربانی خودش مقصر طمع است و به‌نوعی فریب طمع خود را خورده است

۱۳- امید واهی به بازگشت قیمت توکن‌های فیک

چهارم- نظریه کنش عقلانی:[۱۴] بر اساس این نظریه، مجرم پیش از ارتکاب جرم به‌صورت عقلانی مزایای بالقوه[۱۵] و ریسک‌های احتمالی[۱۶] را محاسبه می‌کند. در کلاهبرداری‌های رمزارزی، ماهیت فرامرزی و گمنامی، ریسک کشف را به‌شدت کاهش می‌دهد درحالی‌که سود بالقوه بالا باقی می‌ماند (لوساردی، ۲۰۱۹، ۳۲۹). پنجم- تئوری سبک زندگی و بزه‌دیدگی: افرادی که سبک زندگی پرریسک[۱۷] را انتخاب می‌کنند، سطح «در معرض بودن»[۱۸] خود را افزایش داده و به بزه‌دیدگان بالقوه بالا تبدیل می‌شوند. این افراد با وعده‌های سود چندصد درصدی ممکن است تمام زندگی‌شان را روی یک پروژه بگذارند.

۱-۲- مفهوم‌شناسی و ماهیت رمزارزها

رمزارزها[۱۹] گونه‌ای از دارایی‌های دیجیتال هستند که بر مبنای اصول رمزنگاری ایجاد شده‌اند و مهم‌ترین ویژگی آن‌ها اتکاء به فناوری دفتر کل توزیع‌شده[۲۰] یا همان بلاکچین است (شیرانی و طلاکش، ۱۳۹۹، ۷۵). این ویژگی سبب می‌شود که نیاز به واسطه‌های متمرکز مانند بانک‌ها یا دولت‌ها جهت تأیید و ثبت تراکنش‌ها از بین برود. از منظر فنی رمزارزها صرفاً کدهای رمزنگاری شده‌ای هستند که مالکیت را در یک شبکه غیرمتمرکز اثبات می‌کنند. البته بعضی از رمزارزها غیرمتمرکز نبوده و توسط یک سازمان مدیریت می‌شوند؛ مانند استیبل‌کوین تتر.

۱۴- Rational Choice Theory

۱۵- سود بالا

۱۶- ریسک کشف و مجازات

۱۷- سرمایه‌گذاری

۱۸- Exposure

۱۹- Cryptocurrencies

۲۰- Distributed Ledger Technology

۲- چالش‌های ماهوی و طبقه‌بندی حقوقی

در نظام حقوقی ایران و بسیاری از کشورها، تعریف مشخصی از این که رمزارزها دقیقاً چه ماهیتی دارند، وجود ندارد (عسکری، ۱۴۰۰، ۱۱۲). این دارایی‌ها می‌توانند از جنبه‌های مختلف مورد تحلیل قرار گیرند که هر کدام پیامدهای قانونی متفاوتی در پی دارند: اول- پول یا ارز: اگر رمزارزها به‌عنوان ابزار پرداخت و واسطه مبادله تلقی شوند، مستقیماً تحت نظارت بانک مرکزی قرار می‌گیرند. در ایران به دلیل سیاست‌های پولی، رمزارزها فاقد تعریف قانونی ارز رسمی هستند. دوم- کالا و دارایی: [۲۱] اگر رمزارزها به‌عنوان یک کالای معاملاتی یا دارایی سرمایه‌ای در نظر گرفته شوند، مشمول قوانین مالیاتی و قوانین مربوط به اموال منقول خواهند شد که در حال حاضر قانون‌گذاران کشورهایی همچون ایالات متحده امریکا، کانادا، آلمان و بریتانیا رمزارزها را دارایی حساب کرده و از آن‌ها مالیات اخذ می‌کنند.

۲- عدم شفافیت قانونی و فقدان نگهبان نهادی

در ایران هرچند نهادهای حاکمیتی[۲۲] مواضعی در قبال رمزارزها به‌ویژه در حوزه استخراج اتخاذ کرده‌اند، اما هنوز قانون جامع و مشخصی که تمام جنبه‌های مالکیت، تبادل، ورشکستگی و به‌ویژه تعقیب کیفری کلاهبرداری‌های مرتبط با آن را پوشش دهد، وجود ندارد. این عدم شفافیت به‌طور مستقیم بر نظریه فعالیت‌های روزمره تأثیر می‌گذارد؛ زیرا باعث می‌شود سیستم عدالت کیفری[۲۳] نتواند به‌درستی وظایف خود را در قبال این دارایی‌ها انجام دهد. قضات در مواجهه با پرونده‌های کلاهبرداری رمزارزی با ابهام جدی درباره انطباق عنصر مادی جرم[۲۴] با تعاریف سنتی قانون مجازات اسلامی مواجه هستند. این امر خود زمینه‌ساز احساس مصونیت برای بزهکاران می‌شود.

21- Asset

۲۲- مانند بانک مرکزی و وزارت صمت

۲۳- کنترل‌کننده یا نگهبان نهادی

۲۴- مال برده شده و مالیت داشتن رمزارز

۳- چالش گمنامی و غیرمتمرکز بودن از منظر جرم‌شناسی

ویژگی غیرمتمرکز بودن رمزارزها و ماهیت «شبه‌گمنام»[۲۵] تراکنش‌ها، به‌ویژه در ترکیب با نظریه انتقال فضا، فرصت‌هایی بی‌بدیل برای مجرمان ایجاد می‌کند. مجرمان با استفاده از این ویژگی‌ها هویت خود را در فضای سایبر پنهان ساخته، ریسک کشف را به‌شدت پایین می‌آورند و وجوه حاصل از جرم را به‌سرعت و به‌صورت فرامرزی جابجا می‌کنند. بنابراین، فقدان مرجع متمرکز برای توقف تراکنش‌ها، عنصر «هدف مناسب» را در دسترس‌تر کرده و عملاً توانایی پلیس[۲۶] را در ردیابی و مسدودسازی وجوه کاهش می‌دهد.

۴- تحلیل جرم‌شناختی مصادیق کلاهبرداری رمزارزی و بستر فرصت

۴-۱- پدیدارشناسی کلاهبرداری‌های رایج در بستر فضای مجازی ایران

اول- طرح‌های پانزی و هرمی: [۲۷] رایج‌ترین شکل کلاهبرداری در فضای رمزارزی ایران طرح‌هایی است که با وعده سودهای کلان، سریع و تضمین‌شده طمع قربانیان را هدف قرار می‌دهند و خود را در قالب پروژه‌های مدرن مانند دیفای[۲۸] پنهان می‌کنند (طالبی رستمی، ۱۴۰۴، ۳۴). در حال حاضر وب‌سایت‌هایی برای‌شناسایی این نوع از طرح‌ها ایجاد شده که هدف اصلی آن آگاهی عمومی افراد در مورد پروژه‌های پانزی و هرمی است (مزامیل و همکاران، ۲۰۲۵، ۱).

دوم- نقش تسهیل‌گر اینفلوئنسرهای مالی و سلبریتی‌ها: اینفلوئنسرهای مالی در فضای مجازی نقش کلیدی در اعتمادسازی کاذب دارند. بزهکاران اصلی با پرداخت مبالغ هنگفت، پروژه‌های کلاهبرداری را از طریق این افراد معتبر جلوه می‌دهند. در تحلیل جرم‌شناختی می‌توان بیان نمود که قربانیان به دلیل «اعتماد» به مرجعیت اینفلوئنسر، نگهبان فردی خود را کاملاً تضعیف کرده و در معرض کلاهبرداری قرار می‌گیرند (قوامی‌پور سرشکه و محمودی، ۱۴۰۴، ۷).

25- Pseudo-Anonymity

۲۶- نگهبان محیطی و کنترلی

27- Ponzi and Pyramid Schemes

28- DeFi

سوم- کلاهبرداری‌های توکنی و عرضه‌های اولیه جعلی: [۲۹] این شکل از کلاهبرداری که اغلب در فضای توکن‌های جدید و ناشناخته رخ می‌دهد، متکی بر عنصر «ریسک پایین کشف» در نظریه انتخاب عقلانی و فقدان نگهبان نهادی و محیطی است. در سال‌های اخیر با رشد این حوزه، ساخت توکن در بستر بلاکچین بسیار آسوده شده و نیازی به هزینه زیاد نیست. پلتفرم‌هایی همچون «پامپ فان» [۳۰] فضایی را برای افراد سودجو ایجاد نموده‌اند که با هزینه پایین و زحمت کم توکن بسازند. کلاهبردارانی در بستر فضای مجازی هستند که گاهاً هر هفته توکن جدیدی ساخته و با تبلیغ آن مردم زیادی را اغفال می‌کنند.

چهارم- فیشینگ، حملات مهندسی اجتماعی و جعل هویت: بزهکاران با ایجاد وب‌سایت‌های جعلی شبیه صرافی‌های معتبر یا ساخت اپلیکیشن‌های جعلی کیف پول، اطلاعات ورود یا «کلیدهای خصوصی» [۳۱] کاربران را سرقت می‌کنند. این نوع از کلاهبرداری به مهارت بالایی نیاز دارد به‌طوری‌که بتواند سیستم‌های ایمنی موبایل را نیز گمراه نماید.

۴-۲- ویژگی‌های قربانیان و بزهکاران

قربانیان: عمده قربانیان تحت تأثیر آرزوی یک‌شبه پولدار شدن و اضطرار اقتصادی ناشی از تورم و بی‌ثباتی وارد بازار شده‌اند. این گروه اغلب دارای بزه‌دیدگی‌های بالقوه بالا تلقی می‌شوند؛ زیرا سواد مالی و دیجیتال پایین، «توانایی خود-حفاظتی» [۳۲] آنان را برای عمل به‌عنوان یک نگهبان کارآمد از بین می‌برد. الگوی بزه‌دیدگی در ایران با نوعی شکاف نسلی همراه است. نسل جوان [۳۳] عمدتاً در دام کلاهبرداری‌های پیچیده فنی مانند «راگ پول» و «تله عسل» می‌افتند، درحالی‌که نسل‌های قدیمی‌تر به دلیل اعتماد سنتی و آشنایی کمتر با محیط وب، بیشتر هدف طرح‌های پانزی و هرمی قرار می‌گیرند.

29- Rug Pull & Honey Pot
30- Pump Fun
31- Private Keys
32- Self-Protective Capability
۳۳- بومیان دیجیتال

این تفکیک نشان می‌دهد که «نگهبان فردی»[۳۴] نباید به‌صورت عمومی باشد، بلکه باید به‌صورت تخصصی و تفکیک‌شده برای هر گروه سنی طراحی گردد تا کارایی لازم را در پیشگیری اجتماعی داشته باشد (صفاری و همکاران، ۱۳۹۹، ۱۵).

بزهکاران: مجرمان معمولاً افرادی هستند که دانش فنی قابل قبولی در حوزه سایبر دارند و می‌توانند از ماهیت فرامرزی و قابلیت گمنامی رمزارزها برای کاهش ریسک کشف و تعقیب استفاده کنند. بزهکاران در حوزه رمزارز در ایران به دو دسته اصلی تقسیم می‌شوند: بزهکاران معمار[۳۵]: این افراد دارای دانش عمیق در برنامه‌نویسی بلاکچین و مهندسی اجتماعی هستند. بزهکاران واسط[۳۶]: این گروه که در جرم‌شناسی به آن‌ها «قاطرهای پولی» نیز گفته می‌شود، اغلب با اجاره کردن کارت‌های بانکی و حساب‌های کاربری اشخاص ثالث، وظیفه نقد کردن وجوه مسروقه را بر عهده دارند. این توزیع نقش، باعث می‌شود که لایه اصلی جرم[۳۷] از دسترس نگهبانان نهادی[۳۸] دور بماند و تنها لایه‌های پایین که تخصص کمی دارند،شناسایی شوند (خلیلی‌پاجی و شاملو، ۱۴۰۰، ۵۵).

۵- مجازی‌سازی بزهکاری

بزهکاران رمزارزی در ایران اغلب از تکنیک «انکار قربانی» استفاده می‌کنند. از آن جا که در این جرائم، بزهکار با قربانی مواجهه فیزیکی ندارد و تنها با آدرس‌های عددی و کیف‌پول‌های دیجیتال روبرو است، نوعی «جدایی عاطفی» رخ می‌دهد. این گمنامی و فاصله دیجیتال، منجر به خنثی شدن وجدان اخلاقی بزهکار می‌شود؛به‌طوری که او بزه دیده را نه یک انسان با دارایی‌های واقعی، بلکه صرفاً یک «عدد در شبکه» می‌بیند. این پدیده که تحت عنوان «اثر مهارگسیختگی آنلاین»[۳۹] شناخته

۳۴- آموزش

۳۵- حرفه‌ای

۳۶- آماتور یا اجاره‌ای

۳۷- طراحان

۳۸- پلیس

39- Online Disinhibition Effect

می‌شود، باعث می‌گردد افرادی که در دنیای فیزیکی هرگز مرتکب سرقت نمی‌شوند، در فضای رمزارزها به راحتی دست به کلاهبرداری بزنند.

در اکوسیستم رمزارزی ایران، صرافی‌های تبادل دارایی دیجیتال نقشی دوگانه ایفاء می‌کنند. از منظر جرم‌شناختی، این پلتفرم‌ها اصلی‌ترین «نگهبانان محیطی»[۴۰] محسوب می‌شوند که می‌توانند با سخت‌سازی فرآیند احراز هویت[۴۱]، از ورود «بزهکاران انگیزه‌دار» به چرخه نقد کردن وجوه مسروقه جلوگیری کنند. بااین‌حال، نبود پروتکل‌های نظارتی واحد و یکپارچه در سطح ملی، منجر به ایجاد «نقاط کور نظارتی» شده است. بزهکاران باشناسایی صرافی‌هایی که دارای حفره‌های امنیتی درشناسایی هویت هستند، از آن‌ها به‌عنوان پل ارتباطی برای تبدیل رمزارزهای کلاهبرداری شده به ریال استفاده می‌کنند. بنابراین، تقویت این نگهبانان از طریق نظارت هوشمند و اشتراک‌گذاری لیست سیاه آدرس‌های مشکوک، می‌تواندبه‌طور مؤثری فرصت بزهکاری را در مرحله نقد کردن مال مسروقه کاهش دهد.

۶- چالش‌های حقوقی، فنی و قضایی در تعقیب کیفری

نظام عدالت کیفری در ایران با موانع ساختاری جدی در ردیابی و مجازات بزهکاران رمزارزی روبرو است که در تحلیل جرم‌شناختی بیانگر ناکارآمدی نگهبان نهادی است.

اول- چالش‌های ماهوی و قانونی: ابهام در عنصر مادی جرم: قانون مجازات اسلامی مصوب ۱۳۹۲ برای تحقق کلاهبرداری «اخذ مال» را شرط می‌داند. از آن جا که ماهیت حقوقی رمزارزه[۴۲] در ایران به‌طور قاطع مشخص نیست، قضات در انطباق رمزارز برده شده با مفهوم سنتی «مال» با ابهام جدی مواجه هستند. این امر فرآیند کیفری را کند و مجازات را کم‌اثر می‌کند. نارسا بودن قوانین سنتی و رایانه‌ای: تلاش برای انطباق جرایمی چون «راگ پول» یا «تله عسل» با قوانین سنتی

40- Environmental Guardians
41- KYC

۴۲- پول، کالا یا دارایی

کلاهبرداری یا حتی قانون جرایم رایانه‌ای، اغلب با ابهام و مقاومت مواجه است و نیاز به جرم‌انگاری مستقل و شفاف را آشکار می‌سازد.

دوم- چالش‌های فنی در ردیابی: تکنیک‌های گمنامی پیشرفته: مجرمان از ابزارهای فنی پیچیده‌ای مثل «مخلوط‌کن‌های رمزارز» و «پرش بین زنجیره‌ها» استفاده می‌کنند (لی و همکاران، ۲۰۲۴، ۱۲۳) که ردیابی را مختل می‌سازد. این ابزارها عبارتند از: اختلاط رمزارز:[۴۳] سرویس‌هایی که رمزارزهای ورودی از منابع مختلف را با هم مخلوط کرده و به آدرس‌های خروجی ارسال می‌کنند تا ردگیری منبع اصلی[۴۴] قطع شود. پرش بین زنجیره‌ها: [۴۵] تبدیل سریع رمزارز مسروقه به ارزهای دیگر در بلاکچین‌های متفاوت؛ به‌طوری‌که پیگیری قضایی را فراتر از حوزه یک بلاک‌چین می‌برد. موانع فرامرزی و سازمان‌یافتگی: بخش قابل‌توجهی از این جرائم توسط گروه‌های سازمان‌یافته فراملی مدیریت می‌شود. نبود پروتکل‌های همکاری قضایی بین‌المللی مؤثر و سریع[۴۶] و همچنین تحریم‌های اقتصادی، امکان توقیف دارایی‌ها در صرافی‌های خارجی و استرداد مجرمان را تقریباً ناممکن می‌سازد.

سوم- چالش نابودسازی خودکار و بازگشت‌ناپذیری تراکنش‌ها: برخلاف جرائم مالی سنتی که امکان مسدودسازی حساب یا ابطال تراکنش وجود دارد، در بستر بلاکچین، تراکنش‌ها «قطعی» و «بازگشت‌ناپذیری»[۴۷] هستند. از منظر جرم‌شناختی، بزهکار با آگاهی از این ویژگی فنی، از «تکنیک خنثی‌سازی زمان» استفاده می‌کند؛ یعنی با انتقال سریع دارایی به کیف‌پول‌های متعدد در کسری از ثانیه، عملاً فرصت مداخله را از نگهبانان نهادی[۴۸] سلب می‌کند. این ویژگی باعث می‌شود که حتی در صورت‌شناسایی مجرم، بازگرداندن مال به بزه‌دیده عملاً غیرممکن باشد که خود منجر به کاهش ضریب بازدارندگی مجازات‌ها می‌گردد.

43- Mixers/Tumblers

۴۴- لایه فیزیکی جرم

45- Chain Hopping
46- Mutual Legal Assistance Treaties
47- Irreversibility

۴۸- پلیس و قوه قضاییه

چهارم- ابزارمندی بزهکاران؛ بهره‌گیری از حریم‌خصوصی در نرم افزارها: بزهکاران برای تضعیف نقش «نگهبان محیطی»،به‌طور فزاینده‌ای از «ارزهای حریم‌خصوصی‌محور»[۴۹] مانند مونرو استفاده می‌کنند. این ارزها با مخفی کردن فرستنده، گیرنده و مبلغ تراکنش، تحلیل‌های زنجیره‌ای[۵۰] را که ابزار اصلی پلیس فتا برای ردیابی اموال است، بی‌اثر می‌سازند. این اقدام بزهکاران، عملاً «هزینه جرم» را کاهش داده و با افزایش گمنامی، «فایده جرم» را به حداکثر می‌رساند.

۷- راهبردهای پیشگیرانه جرم‌شناختی

راهکارهای پیشگیرانه باید بر اساس مدل جرم‌شناختی فرصت‌ها در سه سطح اصلی و با هدف افزایش ریسک کشف و «سخت کردن هدف» پیاده‌سازی شوند.

اول- پیشگیری اجتماعی و آموزشی[۵۱]: این راهبرد بر افزایش توان دفاعی قربانی[۵۲] و کاهش بزه‌دیدگی‌های بالقوه بالا متمرکز است. آموزش سواد مالی و رمزارزی: آموزش همگانی و ارتقای سواد رسانه‌ای کاربران می‌تواند نقش مهمی در کاهش بزه‌دیدگی در این حوزه ایفاء نماید (آذری و همکاران، ۱۴۰۱، ۲۲). باید از طریق کمپین‌های گسترده ملی و رسانه‌ای عموم مردم را نسبت به مفاهیم زیر آگاه کرد: تشخیص سودهای غیرمعقول: آموزش این که سودهای تضمینی و بسیار بالا، معمولاً نشانه طرح‌های پانزی و کلاهبرداری است. لذا آگاهی‌بخشی به کاربران برای تشخیص پروژه‌های فریب‌کارانه و وعده‌های سودهای غیرمتعارف، ضرورتی انکارناپذیر است (قاسمی، ۱۴۰۳، ۱۸). امنیت کیف پول و کلید خصوصی: آموزش نحوه نگهداری ایمن از کلیدهای خصوصی و پرهیز از به اشتراک‌گذاری اطلاعات شخصی (لوساردی، ۲۰۱۹، ۳۲۹). مسئولیت کیفری و مدنی تبلیغ‌کنندگان: تدوین مقرراتی برای تعیین مسئولیت کیفری[۵۳] یا مسئولیت مدنی تضامنی برای سلبریتی‌ها و

49- Privacy Coins
50- On-chain Analysis

۵۱- تقویت نگهبان فردی
۵۲- نگهبان فردی
۵۳- معاونت در جرم

اینفلوئنسرهای مالی که پروژه‌های کلاهبرداری را با استفاده از اعتبار عمومی خود تبلیغ می‌کنند. این اقدام به‌طور مستقیم به مقابله با عامل تسهیل‌کننده جرم می‌پردازد.

دوم- پیشگیری وضعی و نظارتی: این راهبرد محیط بزهکاری را هدف قرار می‌دهد تا ارتکاب جرم را برای بزهکار دشوارتر سازد.

الگوی لیست سفید:[۵۴] ایجاد و انتشار رسمی لیستی از صرافی‌ها و پلتفرم‌های رمزارزی مورد تأیید و مجاز توسط نهادهای ناظر. این کار به کاربران کمک می‌کند تا صرافی‌های معتبر راشناسایی کرده و ریسک استفاده از پلتفرم‌های ناشناس و جعلی کاهش یابد. سخت کردن هدف:[۵۵] الزام به احراز هویت سخت‌گیرانه: الزام صرافی‌های داخلی به اجرای دقیق مبارزه با پولشویی برای کاهش ماهیت گمنام تراکنش‌ها. (کرامتی‌معز و بهاری غازانی، ۱۴۰۱، ۸۵). تأخیر در برداشت:[۵۶] اعمال یک زمان تأخیر مشخص[۵۷] برای برداشت‌های کلان ریالی یا رمزارزی. این فرصت طلایی را برای نهادهای نظارتی و پلیس فراهم می‌کند تا در صورت اعلام کلاهبرداری، وجوه مسروقه را مسدود سازند. تقویت امنیت فنی: اجباری کردن استفاده از احراز هویت دومرحله‌ای[۵۸] برای تمامی حساب‌ها.

سوم- سیاستگذاری و تقنینی: این راهبرد نیازمند اصلاح ساختارهای قضایی و قانونی است. جرم‌انگاری شفاف و مستقل: تدوین و تصویب قانون جامع و مستقل برای رمزارزها که ماهیت حقوقی آن‌ها را تعیین کرده و مصادیق کلاهبرداری‌های نوین را به‌وضوح جرم‌انگاری کند تا ابهام در عنصر مادی رفع شود. تخصصی‌سازی دادرسی: ایجاد دادسراها و شعب تخصصی در دادگاه‌ها با حضور قضات، دادیاران و ضابطین مسلط به فناوری بلاکچین که قادر به ردیابی فنی و حقوقی این نوع جرائم باشند. همکاری‌های فراملی حقوقی: تلاش برای ایجاد و فعال‌سازی پروتکل‌های همکاری قضایی و

54- White List
55- Hardening the Target
56- Withdrawal Delay

۵۷- مثلاً بیست و چهار تا هفتادودو ساعت

58- Two-Factor Authentication

پلیسی سریع با کشورهای دیگر[۵۹] برای ردیابی و استرداد دارایی در جرایم سازمان‌یافته فراملی. تأسیس واحد واکنش سریع تعاملی: با توجه به سرعت بالای جابجایی اموال در شبکه بلاکچین، پیشنهاد می‌شود یک واحد عملیاتی مشترک میان پلیس فتا، دادستانی و انجمن بلاکچین ایران تشکیل شود. وظیفه این واحد، ایجاد یک پروتکل «توقیف آنی» است تا به محض گزارش کلاهبرداری، آدرس‌های مقصد در تمام صرافی‌های داخلی به‌صورت خودکار در لیست سیاه قرار گیرند. این راهکار به‌عنوان یک «نگهبان محیطی هوشمند»، فضای تنفس بزهکار برای نقد کردن وجوه را به حداقل می‌رساند.

نتیجه

یافته‌های این پژوهش وقوع گسترده کلاهبرداری‌های رمزارزی در ایران را نه یک پدیده تصادفی، بلکه نتیجه منطقی و قابل پیش‌بینی تعامل ساختاری بین فناوری، اقتصاد و قانون می‌دانند. تحلیل حاضر این تعامل را در ذیل دو نظریه محوری فعالیت‌های روزمره و انتقال فضا تبیین می‌کند. نخست، مثلث جرم در فضای رمزارزهای ایران به‌صورت کامل تحقق یافته است. «بزهکار با انگیزه» با بهره‌گیری از دانش فنی و انگیزه سود بالا وارد میدان می‌شود. «هدف مناسب» نیز به‌واسطه ماهیت دیجیتال، سریع‌الانتقال و باارزش رمزارزها فراهم است. بااین‌حال، عنصر تعیین‌کننده، «فقدان نگهبان کارآمد» است.

یافته‌ها نشان می‌دهند این فقدان یک ضعف واحد نیست، بلکه یک شکست سیستمی در سه لایه است: در لایه فردی: ترکیب «اضطرار اقتصادی» و «سواد دیجیتال پایین»، قربانی را از ایفای نقش مؤثر به‌عنوان نخستین خط دفاعی[۶۰] ناتوان می‌سازد. در لایه محیطی: نظارت ناقص بر پلتفرم‌ها و مهم‌تر نقش غیرمسئولانه اینفلوئنسرها، اعتماد کاذب ایجاد کرده و محیط را برای شکار امن می‌کند. اینفلوئنسر در این مدل عملاً به یک «تسهیلگر جرم» تبدیل می‌شود که جای خالی نگهبان محیطی را پر می‌کند اما در جهت عکس. در لایه نهادی: ابهام حقوقی و کندی نظام قضایی در مواجهه با جرایم نوین، ریسک

۵۹- فارغ از محدودیت‌های تحریمی

۶۰- نگهبان دارایی خود

قانونی را برای بزهکار به حداقل می‌رساند و پیامدهای جرم را بی‌اثر می‌سازد.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

ـ آذری، سکینه؛ افضلی، روح‌الله؛ طارم، میثم، ۱۴۰۱، جرایم ارز مجازی از منظر فقه جزای جزایی، **فصلنامه فقه جزای تطبیقی**، شماره ۲.

ـ خلیلی‌پاجی، عارف و شاملو، باقر، ۱۴۰۰، جرم‌انگاری در حوزه رمزارزها، **فصلنامه آموزه‌های حقوق کیفری**، شماره ۲۱.

ـ درویشی‌ها، محسن و حسینی، حدیث‌سادات، ۱۴۰۴، تحلیل حقوقی و جرم‌شناسی جرایم مرتبط با رمزارز در ایران، **فصلنامه پژوهش‌های نوین در روانشناسی**، شماره ۲.

ـ شیرانی، مسعود و طلاکش، ملیکاسادات، ۱۳۹۹، قانون‌گذاری بلاکچین در ایران، چین و انگلستان، **فصلنامه تمدن حقوقی**، شماره ۷.

ـ صفاری، علی؛ صابری، راضیه؛ خلیلی‌پاجی، عارف، ۱۳۹۹، کارکردهای مجرمانه ارزهای مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه، **فصلنامه دانشنامه حقوق اقتصادی**، شماره ۱۸.

ـ طالبی رستمی، محبوبه، ۱۴۰۴، درآمدی بر جرایم مرتبط با رمزارزها؛ از تسهیل‌گری تا پیشگیری، **فصلنامه تمدن حقوقی**، شماره ۲۴.

ـ عسکری، سجاد، ۱۴۰۰، نسبت‌شناسی ارز و رمزارز در نظام تقنینی ایران، **مجله حقوقی دادگستری**، شماره ۱۱۳.

ـ قاسمی، علیرضا، ۱۴۰۳، بررسی جرایم سایبری در حوزه ارزهای دیجیتال و طرح‌های کلاهبرداری مدرن، **فصلنامه اندیشه وکیل**، شماره ۸.

ـ قوامی‌پور سرشکه، محدثه و محمودی، امیررضا، ۱۴۰۴، امنیت رمزارزها در فضای سایبر و چالش‌های پیش رو، **دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم‌شناسی**، شماره آن لاین.

ـ کرامتی‌معز، هادی و بهاری غازانی، مجید، ۱۴۰۱، پیشگیری وضعی از جرایم در بستر رمزارزها، **فصلنامه مطالعات پیشگیری از جرم**، شماره ۶۳.

ـ معاونت علمی پژوهشی، ۱۳۹۸، **پدیده رمزارزها، مخاطرات فرصت‌ها و نحوه سیاست‌گذاری**، چاپ اول، تهران، انتشارات دبیرخانه مجمع تشخیص مصحت نظام.

لاتین

- Clarke, R. V., 1995, Situational Crime Prevention. Crime and Justice, 19.
- Li, K.; Guan, S.; Lee, D., 2024, Towards Understanding and Characterizing the Arbitrage Bot Scam in the Wild. Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security.
- Lusardi, A., 2019, Financial literacy and the need for financial education: Evidence and implications. Journal of Pension Economics and Finance, 18 (2).
- Muzammil, M.; Pitumpe, A.; Li, X.; Rahmati, A.; Nikiforakis, N., 2025, The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams. Proceedings of the ACM on Human-Computer Interaction, 9 (CSCW).

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.26- Winter 2026

Analysis of the Issuing Bank's Liability under the Law of Documentary Credits
Homayoun Mafi, Mohsen Raeisi
The Role of Artificial Intelligence in Improving Criminal Investigation Processes and Digital Evidence Analysis in the Iranian Legal System
Amirreza Mahmoudi, Zahra Rahnama
Revisiting Contractual Obligations in Conditions of High Inflation: an Analysis of Adjustment Capacities in Iranian Law
Shima Shakouri, Ghasem Nabizadeh Kebrya
Iranian Criminal Policy Ppathology Regarding the Crimes of Rebellion, Moharebeh and Corruption on Earth in Light of the Concept of National Security and Political Stability of the Country
Ruhollah Sheikhi, Mohammad Momahmoodi
The Framework of Civil Liability Arising from High-Risk Recreational Activities: A Study of Escape Rooms
Rahim Mokhtari, Gholamhossein Keshavarz
Handling Intellectual Property Claims in the Iranian Legal System
Sayyed Mohammadbagher Haghayeghi, Mohammadreza Nasiri, Amirhasan Abolhasani
Criminological Analysis of Crimes in the Field of Cryptocurrencies: A Study of Common Frauds in Iran
Hossein Mahmoudi Tekanloo, Roya Asiaei
Preventive Strategies for the Crime of Rent-Taking in Iran's Criminal Policy with an Emphasis on Criminological Challenges and Gaps
Fazal Movahedi, Hamidreza Konari Zhadeh, Davoud Salmanpour
An Analysis of the Principle of Proportionality Between Crime and Punishment in the Structure of the International Criminal Court
Hasan Pirfalak, Tayebe Ghodrati Siyahmazgi
Agreement Between the Parties to the Contract in Determining the Evidence to Prove the Claim
Habibolah Abdolah Poor, Mahdi Shojayi
Performance of Criminal Courts in Crime Prevention: A Critical Criminology Perspective with Focus on Iran's Judicial System
Iraj Morvati, Naghmeh Farhood
The Responsibility of States for Human Rights Violations by Private Security Companies on Foreign Missions
Mahdi Gharedaqi, Masoud Sarfarazi Saleh
The End of Centralized Governance: an Analysis of the Emergence of Decentralized Governance in the Era of Block chain and Smart Contracts
Hadi Zare, Majid Vaziri
Comparative Analysis of Social Security Compensatory Protection for Bodily Injuries and the Scope of Eligible Victims in Iran and England
Zeinab Tari
Transfer of Lawsuits in the Iranian Legal System with Emphasis on Selected Provisions of the Deeds and Real Estate Registration Law
Amirreza Alitabar
The Position of Artificial Intelligence in the Field of Criminal Policymaking
Mahbobeh Talebi Rostami
Commitment to Data Security as a Commitment to Result or a Commitment to Means in Private Law
Sayyed Amirhasan Mostafavi
Criminal Liability of Technology Companies for Crimes Committed by Users
Vahid Kioumarsi
Civil Liability Arising from Automated Processing of Personal Data by Artificial Intelligence in Iranian and Afghan Law (With a Look at International Documents)
Raziyeh Jafarzade, Vahid Hamidi, Mohammadreza Rashid
The Impact of Legal Awareness and Transparency on the Prevention and Reduction of Administrative and Financial Corruption
Sayyedeh Mahshid Miri Balajorshari
Ownership of Personal Data in Private Rights; from Personality Right to Intangible Property
Sina Youseffi
Civil Liability of the Physician and Robot Manufacturer in Robotic Surgeries: Iranian and English Legal Systems
Ebrahim Shiravanian
an Analysis of the Issue of Receiving Compensation for Delayed Payment from the Convict to the Government
Mohammadmahdi Rezvanifar, Zahra Salimi
Legal and Administrative Effects of Acquisition on the Registered Status of Real Estate in the Iranian Legal System
Ehsaneh Vosoughi Monfared, Mohammad Varaste Bazghale
Economic Diplomacy and the Law of Private International Contracts; The Interaction of Politics and Law in Securing National Interests
Radmehr Rahmani Golafshan
Adoption of Artificial Intelligence-Driven Fraud Detection in Banking: The Role of Trust, Transparency, and Fairness Perception in Financial Institutions in Iran, the United Arab Emirates and Qatar
Abdolmajid Yousefi
Criminology of War in the Current Realities and the Need for its Development in Ukraine
Yasser Shakeri