Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 3, Issue 5, 2024

Discovering and Punishing Computer and Virtual (Cyber) Crimes with an Approach to Digital Currency

Ali Javaheri[1], Seyyed Ebrahim Ghodsi*[2], Javad Vahedizadeh[3]

1. PhD Student in Criminal Law and Criminology, Ardabil Branch, Islamic Azad University, Ardabil, Iran.
2. Associate Professor, Department of Law and Political Science, Mazandaran University, Mazandaran, Iran. (Corresponding Author)
3. Assistant Professor, Department of Law, Faculty of Law, Ardabil Branch, Islamic Azad University, Ardabil, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 339-349

Corresponding Author's Info
ORCID: *0000-0002-5273-4802*
TELL: *+989111114591*
Email: *Ghodsi@umz.ac.ir*

Article history:
Received: *08 Oct 2023*
Revised: *14 Dec 2023*
Accepted: *09 Jan 2024*
Published online: *20 Feb 2024*

Keywords:
Technology, Computer and Virtual (Cyber) Crimes, Detection and Prevention, Security, Digital Currency.

ABSTRACT

Today, with the increasing use of the Internet, it is used for various types of crimes, including stealing personal information, stealing money from users' bank accounts, spreading pornography, etc. Almost anyone who uses the Internet for personal gain can be a victim of cybercrime. Achieving any of these goals may make us become a victim of Internet crimes; The findings showed that digital currencies have characteristics that make them suitable options for money laundering and transferring illegal amounts. These currencies are hard to track and detect, their transactions are anonymous, their transfer costs are low, they are transferred without the need for an intermediary, they can be transferred from one country to another in a few minutes and into other digital currencies or even tangible assets. changed. The methods and techniques used by the police and regulatory bodies to deal with crimes are very important, but in order to optimize their techniques and get maximum results, they must first understand the concept of digital currencies and strengthen their basic knowledge in this field. Unfortunately, it is possible that senior police officials do not understand the necessity of training in this field as they should, due to the newness of the field of digital currencies. Due to the increasing use and popularity of digital currencies, law enforcement agencies should strive to hire elite experts and create specialized digital intelligence units. The detection of crimes in this area requires the evolution of law enforcement tools, training and strategies based on digital intelligence and data analysis.

How to Cite This Article: Javaheri, A; Ghodsi, SE & Vahedizadeh, J (2024). "Discovering and Punishing Computer and Virtual (Cyber) Crimes with an Approach to Digital Currency". *Journal of Comparative Criminal Jurisprudence*, 3(5): 339-349.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره سوم، شماره پنجم، اسفند ۱۴۰۲

کشف و مجازات جرایم رایانه‌ای و مجازی (سایبری) با رویکردی به ارز دیجیتال

علی جواهری[۱]، سیدابراهیم قدسی*[۲]، جواد واحدی‌زاده[۳]

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران.
۲. دانشیار، گروه حقوق و علوم سیاسی، دانشگاه مازندران، مازندران، ایران. (نویسنده مسؤول)
۳. استادیار، گروه حقوق، دانشکده حقوق، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی
صفحات: ۳۳۹-۳۴۹

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۲-۵۲۷۳-۴۸۰۲
تلفن: ۹۸۹۱۱۱۱۱۴۵۹۱+
ایمیل: Ghodsi@umz.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۲/۰۷/۱۶
تاریخ ویرایش: ۱۴۰۲/۰۹/۲۳
تاریخ پذیرش: ۱۴۰۲/۱۰/۱۹
تاریخ انتشار: ۱۴۰۲/۱۲/۰۱

واژگان کلیدی:

فناوری، جرایم سایبری، کشف و پیشگیری، امنیت، ارز دیجیتال.

چکیده

ارز دیجیتال از موضوعات مهمی است که دارای ابعاد مختلف حقوقی است و از جهات مختلف حقوقی محل بحث و اختلاف نظر است. هدف مقاله حاضر بررسی این سؤال مهم است که جرایم رایانه‌ای و مجازی (سایبری) و راهکارهای کشف این جرایم چگونه است؟ مقاله پیش رو توصیفی ـ تحلیلی و با استفاده از روش کتابخانه‌ای به بررسی سؤال مورد اشاره پرداخته شده است. یافته‌ها نشان داد ارزهای دیجیتال ویژگی‌هایی دارند که آن‌ها را به گزینه‌های مناسبی برای پول‌شویی و انتقال مبالغ غیرقانونی تبدیل می‌کند. ردیابی و کشف این جرایم این ارزها سخت است، تراکنش‌های آن‌ها ناشناس است، هزینه انتقال آن‌ها پایین است، بدون نیاز به واسطه منتقل می‌شوند، می‌توان در چند دقیقه آن‌ها را از کشوری به کشور دیگر منتقل کرد و به سایر ارزهای دیجیتال یا حتی دارایی‌های ملموس تبدیل کرد. شیوه‌ها و تکنیک‌هایی که پلیس و نهادهای نظارتی برای مقابله با جرایم استفاده می‌کنند، بسیار مهم هستند، اما آن‌ها باید برای بهینه‌سازی تکنیک‌های خود و نتیجه‌گیری حداکثری، ابتدا به درک درستی از مفهوم ارزهای دیجیتال برسند و دانش ابتدایی خود را در این زمینه تقویت کنند. متأسفانه این امکان وجود دارد که مقامات ارشد پلیس به‌علت جدیدبودن حوزه ارزهای دیجیتال، ضرورت آموزش در این حوزه را به‌طوری که باید درک نکنند. باتوجه به افزایش کاربرد و محبوبیت ارزهای دیجیتال، نهادهای اعمال قانون باید برای استخدام کارشناسان نخبه و ایجاد واحدهای تخصصی هوش دیجیتال تلاش کنند. کشف جرایم این حوزه مستلزم تکامل ابزارهای اعمال قانون، آموزش و راهبردهای مبتنی‌بر هوش دیجیتال و تحلیل داده‌هاست.

مقدمه

از لحاظ حقوقی می‌توان این تعریف را برای جرایم سایبری ارائه داد، هر اقدامی که از طریق فضای مجازی و با بهره‌گیری از ابزارهای اتصال به فضای مجازی صورت گرفته و حقوق شناسایی‌شده برای افراد را نقض کند؛ به این ترتیب تنها جرایمی در دامنه شمول این تعریف قرار می‌گیرند که از طریق فضای مجازی و با بهره‌گیری از ابزارهای اتصال به این فضا ارتکاب می‌یابند. سرقت رایانه‌ای به‌عنوان یک پدیده خطرناک در عصر الکترونیک و ارتباطات، نسبت به سرقت‌های کالسیک از قابلیت‌های بسیار زیاد، همچون دقت بالا، سرعت زیاد، ذخیره‌سازی حجم زیاد اطلاعات، سهولت ارتکاب، خستگی‌ناپذیری و سایر محاسن از طرفی و فراملی بودن و محدود به مکان خاص‌نبودن گسترگی فضای کامپیوتر و کاربران از طرف دیگر سبب شد که این‌گونه جرایم را نتوان در قالب سرقت سنتی قرار داد. درجهت تبیین جرم‌شناختی سرقت رایانه‌ای که یکی از جرایم مالی رایانه‌ای محسوب می‌شود، شخصیت‌شناسی بزهکاران سایبری و ریشه‌یابی بزهکاری با روش‌های پیشگیرانه مؤثر است. آنچه در عوامل سرقت سایبری مورد تأکید است، شناسایی عوامل فردی و اجتماعی تأثیرگذار در این جرم است و در بحث پیشگیری اجتماعی آنچه مد نظر است، خنثی‌سازی انگیزه ارتکاب جرم در مرتکب می‌باشد و در پیشگیری وضعی محیط ارتکاب جرم را مورد توجه قرار می‌دهد. درنهایت، پیشگیری کیفری الزامات قانون‌گذار به جرم‌انگاری رفتارهای قابل ارتکاب در محیط رایانه‌ای و همچنین اعمال کیفر بر مرتکب و چالش‌هایی که در این زمینه وجود دارد را مورد بحث قرار می‌دهد.

فضای سایبر در مناسبات اجتماعی فرهنگی و اقتصادی جای خود را یافته، به‌نحوی‌که در جوامع پیشرفته استفاده از آن به‌عنوان یک ضرورت مطرح شده و این امر جهان را مشابه دهکده‌ای ساخت که اعضای آن در هر نقطه از مکان جغرافیایی باشند، به سهولت و بدون محدودیت می‌توانند در این فضا با یکدیگر ارتباط برقرار کنند و بدون صرف زمان طولانی در جهان اطلاعات سیر دانش خود بیفزایند و مهارت‌های خود را افزایش دهند. بدون شک میل و اشتیاق به استفاده از فناوری روز و بهره‌مندی از مزایای آن یک تمایل جهانی می‌باشد که این تمایل از سوی آحاد مردم و دولت‌ها با سرعت قابل توجه در حال افزایش است و فرصت‌هایی بسیار برای کشورها در زمینه تبادل و مشارکت‌های اقتصادی اجتماعی و فرهنگی با سایر کشورها ایجاد خواهد کرد، اما در عین حال این گستره بیکران می‌تواند شرایط مخاطره‌آمیز و بستری مساعد نیز برای ظهور پدیده‌های جدید بزهکاری و ایجاد چالش در حوزه‌های مختلف، اجتماعی سیاسی، مالی، امنیتی و شبه‌امنیتی به وجود آورد.

گسترش روزافزون فناوری‌ها در کنار کثرت روابط انسانی و لزوم توجه به اصل سرعت، استفاده از ابزارهای رایانه‌ای را اجتناب‌ناپذیر نموده است، به‌نحوی‌که حجمی فزاینده از اطلاعات مورد نیاز جامعه امروزی، با استفاده از فناوری‌های پیشرفته، ازجمله رایانه و شبکه‌های مرتبط با آن تولید، ذخیره، ارسال و توسعه می‌یابد. توسعه و گسترش علوم رایانه‌ای و تمایل روزافزون به استفاده از آن، گذشته از این‌که موجب تحول یا انقلاب فناوری در جهان گردید، هم‌زمان ضمن تأثیرگذاری بر تمام جنبه‌ها و شئون زندگی بشر، شرایط و بستری مساعد برای ظهور جرایم در فضای مجازی را فراهم آورده و گسترش آن موجب آسیب‌ها و خساراتی گوناگون در جوامع گردیده است. از سوی دیگر، این فناوری مرزهای جغرافیایی را در هم شکسته و قلمرویی جدید برای فعالیت‌های بشری به‌وجود آورده، به‌گونه‌ای‌که امکان به‌کارگیری حقوق موجود در چهارچوب مرزهای ملی را تضعیف نموده است.

۱- مفاهیم

۱-۱- فناوری

فناوری یا تِکنولوژی مجموع تکنیک‌ها، مهارت‌ها، روش‌ها و فرایندهایی است که در تولید کالاها یا خدمات یا تحقق اهداف، مانند تحقیقات علمی استفاده می‌شود. فناوری می‌تواند دانش تکنیک‌ها، فرایندها و مواردی از این دست باشد یا می‌تواند در ماشین‌ها تعبیه شود تا بدون اطلاع دقیق از عملکرد آن‌ها، امکان کار را فراهم آورد. سیستمی که از فناوری برای دریافت یک ورودی و سپس تغییر آن باتوجه به

کاربرد و تولید خروجی استفاده می‌کند به‌عنوان سیستم تکنولوژیک یا فناوری شناخته می‌شود.

۱-۲- جرایم رایانه‌ای و مجازی

برای تعریف جرم رایانه‌ای دارای دیدگاه جرم‌شناسی هستند، یعنی علاوه‌بر اعتقاد به جرایم رایانه‌ای محض که پیش‌تر بیان گردید، به ارتکاب جرایم سنتی، بدون تغییر در ماهیت، ولی با استفاده از رایانه نیز معتقد هستند و این قبیل جرایم را نیز از مصادیق جرایم رایانه‌ای و جرایم سایبری می‌دانند، لذا این‌طور تعریف می‌نمایند: «هر جرمی که سیستم یا داده رایانه‌ای عملاً موضوع یا وسیله ارتکاب‌یافتن جرم باشد، اعم از این‌که مورد تصریح قانون‌گذار قرار گرفته باشد یا نه، جرم رایانه‌ای نامیده می‌شود.»

۱-۳- پیشگیری از جرم

«پیشگیری از جرم از اصطلاحات حقوق جزا بوده و در معنای وسیع خود شامل اقدامات کیفری و غیرکیفری، مانند پیشگیری وضعی و اجتماعی که برای خنثی‌کردن عوامل ارتکاب جرم و کاهش بزهکاری می‌شود، ولی در مفهوم مضیق پیشگیری فقط تدابیر غیرکیفری را شامل می‌شود» (ذبیح‌الله‌نژاد، ۱۳۸۶: ۱۷).

۱-۴- امنیت

امنیت دوری از هرگونه تهدید و نیز آمادگی برای رویارویی با خطرات است، مفهوم امنیت نسبی و دارای شدت و ضعف است، به این معنا که در برخی موقعیت‌ها (زمان و مکان‌های مختلف) در ذهن افراد ارتقا یا کاهش می‌یابد. امنیت از ضروری‌ترین نیازهای یک جامعه است.

۱-۵- ارز دیجیتال

ارز دیجیتال ارزهایی هستند که در فعالیت‌های اقتصادی به‌صورت الکترونیکی ذخیره و منتقل می‌شوند و مبنای آن‌ها صفر و یک است. همان‌طور که از واژه آن نیز برمی‌آید، ارز دیجیتال به هر ارزش ایجادشده در بستر دیجیتال اشاره دارد. این مفهوم در مقابل واسطه‌های فیزیکی مانند اوراق بانکی یا سکه مطرح می‌شود. ارز دیجیتال ویژگی‌هایی مشابه با ارزهای فیزیکی دارد، اما به‌طور معمول تراکنش‌های انتقال سرمایه ارزهای دیجیتالی به‌صورت آنی و بدون مرز بین افراد قابل انجام است. ارزهای مجازی و رمزارزها هر دو از نمونه‌های ارزهای دیجیتال هستند، اما هر ارز دیجیتالی ارز مجازی یا رمزارز نیست. پول‌های دیجیتال مانند پول‌های فیزیکی، برای خرید کالا و خدمات مورد استفاده قرار می‌گیرند، اما می‌توانند به استفاده در مجامع خاص نیز محدود شوند. برای مثال می‌توان یک پول مجازی مخصوص یک بازی یا شبکه اجتماعی داشت. پول‌های دیجیتال مانند بیت‌کوین و اتریوم به‌عنوان «پول‌های غیرمتمرکز دیجیتال» شناخته می‌شوند، به این معنی که مرکزی برای تولید این پول وجود ندارد.

«می‌توان برای غیرقانونی‌دانستن معامله‌های رمزارزی به بند «ج» ماده ۲ قانون پولی و بانکی مصوب ۱۳۵۱ استناد کرد» (شاه‌محمدی، ۱۳۹۳: ۱۰۱). این ماده مقرر کرده است: «**تعهد پرداخت هرگونه دین و یا بدهی فقط به پول رایج کشور انجام پذیر است، مگر آنکه با رعایت مقررات ارزی کشور ترتیب دیگری بین بدهکار و بستانکار داده شده باشد، استناد می‌کنند**»، درحالی‌که اگر رمزارز به‌عنوان یک دارایی دیجیتال (نه پول در معنای اخص خود) در نظر گرفته شود، تعارضی بین قانون مذکور و مبادله رمزارز وجود نخواهد داشت. از سوی دیگر، براساس مصوبه هیأت وزیران در جلسه ۶ مرداد ۱۳۹۸: «**استفاده از رمز ارزها صرفاً با قبول مسؤولیت خطرپذیری (ریسک) از سوی متعاملین صورت می‌گیرد.**» همچنین قوانین داخلی موجود در حوزه استخراج رمزارز نیز نشان می‌دهد که جواز و مشروعیت این دارایی موضوعی انکارناپذیر برای مراجع قانون‌گذاری در ایران است. طبق مصوبه مذکور: «**استخراج فرآورده‌های پردازشی رمزنگاری‌شده رمزارزها (ماینینگ) با اخذ مجوز از وزارت صنعت، معدن و تجارت مجاز است، هرچند مراجع قانون‌گذاری به‌جهت ماهیت این دارایی هنوز در شناسایی حقوقی آن موضع روشنی اتخاذ نکرده‌اند، اما تردید در این موضوع، موجب می‌شود که در این مورد به اصل اباحه رجوع شود، به این معنی که وقتی قانونی برای غیرمشروع‌بودن آن وجود ندارد، اصل را بر مشروع و مباح‌بودن معامله رمزارز است.**»

ایران تجارت و مالکیت ارزهای دیجیتال را در سال ۱۳۹۶ و ۱۳۹۷، به‌دلیل نگرانی‌های مربوط به پول‌شویی و تأمین مالی

تروریسم ممنوع اعلام کرد و تمام مؤسسات مالی ایرانی، مانند بانک‌ها، صرافی‌های زیر نظر بانک مرکزی و سایر مراکز اصلی مالی از کارکردن با ارزهای دیجیتال یا تبلیغ آن به هر نحوی منع شدند.

بانک مرکزی در سی‌امین جلسه شورای عالی مبارزه با پول‌شویی در تاریخ ۹ آذر ۱۳۹۶ به‌طور رسمی همه مؤسسات مالی را از کار با ارزهای دیجیتال منع کرد.

بانک مرکزی در اردیبهشت‌ماه سال ۱۳۹۷، طی یک اعلامیه رسمی، خرید و فروش بیت‌کوین در ایران را ممنوع اعلام کرد. در این اطلاعیه بیان شد: «از آنجا که ماهیت ارزهای مجازی، این ارزها را به ابزاری برای پولشویی، تأمین مالی تروریسم و به‌طور کلی جابه‌جایی پول بین مجرمان تبدیل می‌کند، ممنوعیت به‌کارگیری این ارزها به بانک‌ها ابلاغ شده است.»

اما در سال ۲۰۱۹ باتوجه به مشکلاتی که به‌دلیل تحریم‌ها به‌وجود آمد، دولت شروع به لغو محدودیت‌ها در این زمینه کرد. بعد از آن، قانون ارز دیجیتال در ایران تغییر کرد؛ آیین‌نامه اجرایی استخراج فرآورده‌های پردازشی رمزنگاری‌شده، توسط معاون اول رییس جمهور اعلام و مالکیت و استخراج ارز دیجیتال در ایران با اخذ مجوز از وزارت صمت، قانونی شد، اما همچنان استفاده از رمزارزها به‌عنوان یک سیستم پرداخت ممنوع بود.

طبق مصوبه هیأت وزیران در جلسه مورخ ۱۳ مردادماه ۱۳۹۸ تحت عنوان آیین‌نامه فرایند ماینینگ و استفاده از رمزارز: **«استفاده از رمزارزها صرفاً با قبول مسؤولیت خطرپذیری (ریسک) از سوی متعاملین انجام می‌شود و مشمول حمایت و ضمانت دولت و نظام بانکی نبوده و استفاده از آن در مبادلات داخل کشور مجاز نیست.»**

مفاد این مصوبه دلالت بر این امر دارد که استفاده و خرید و فروش رمزارز مجاز است، اما دولت و نظام بانکی ارزش ذاتی رمزارز را تضمین نمی‌کند.

همچنین طبق بند ۲ این مصوبه، استخراج فرآورده‌های پردازشی رمزنگاری‌شده رمزارزها (ماینینگ) با اخذ مجوز از وزارت صنعت، معدن و تجارت مجاز است.

افراد می‌توانند براساس قانون استخراج ارز دیجیتال در ایران، با ثبت شرکت مسؤولیت محدود یا سهامی خاص، مجوز ماینینگ را به نام شرکت خود دریافت کنند. براساس ماده ۱۵ دستورالعمل صدور و بهره‌برداری رمزارزها، پروانه بهره‌برداری از استخراج ارز دیجیتال برای متقاضی زمانی صادر می‌شود که اقدامات لازم جهت ظرفیت‌سنجی محل و بازدید فنی توسط کارشناسان وزارت صنعت انجام گرفته باشد.

همچنین براساس اطلاعیه بانک مرکزی در سال ۱۳۹۸، «تشکیل و فعالیت اشخاص برای ایجاد و اداره شبکه پولی و پرداخت مبتنی‌بر فناوری زنجیره بلوک، از نظر این بانک، غیرمجاز محسوب شده و بانک مرکزی حق پیگرد قانونی اشخاصی که با نادیده‌گرفتن مقررات، شبکه‌ای ایجاد و آن را تبلیغ می‌کردند را برای خود محفوظ می‌دانست.»

در حال حاضر ارزهای رمزنگاری‌شده در صرافی‌هایی که مقررات را رعایت کرده‌اند، قابل خرید و فروش و مبادله است و توسعه کیف پول ارز دیجیتال که با نام‌های وَلِت یا والت نیز شناخته می‌شود با در نظرگرفتن مقررات بخش کیف پول رمزارزی، برای اشخاص حقیقی و حقوقی مشکل قانونی ندارد.

به‌طور کلی در مورد جواز معامله و استفاده از رمزارزها در ایران باید گفت، باتوجه به ماده ۲ قانون مجازات اسلامی که: **«هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است، جرم محسوب می‌شود.»** از آنجا که در مورد ممنوعیت خرید و فروش ارزهای دیجیتال در کشور قانونی تصویب نشده است، معامله یا خرید و فروش رمزارز در ایران، غیرقانونی نیست و جرم محسوب نمی‌شود، هرچند در مورد قانونی‌بودن آن نیز قوانین محکمی وجود ندارد، اما باتوجه به دستورالعمل‌ها و مصوبات دولتی استخراج و استفاده از آن تحت ضوابط و شرایط اعلامی مجاز است.

ویژگی‌های کاربردی رمزارزها باعث شده است که ایران نیز به‌سمت تولید ارز دیجیتال تحت عنوان «رمز ریال» برود. سرعت انتقال و کم‌کردن اسکناس در دست مردم، ازجمله عواملی است که موجب حرکت بانک مرکزی جمهوری اسلامی ایران و نهادهای مالی به سوی تولید رمز ریال شده است.

۲- روش تحقیق

روشی که برای این تحقیق به‌کار گرفته شده است، روش توصیفی ـ تحلیلی است. برای این منظور از ابزارهایی استفاده خواهد شد، ازجمله استفاده از منابع موجود در کتابخانه‌ها و بانک‌های اطلاعاتی. پس از جمع‌آوری منابع و فیش‌برداری از آن‌ها، به تشریح و تحلیل مطالب، شناسایی معضلات مربوطه و راه‌های احتمالی پاسخگویی به آن‌ها پرداخته خواهد شد. این پژوهش اساساً با استفاده از آخرین و جدیدترین مقالات و کتاب‌ها و اسناد حقوقی و همچنین منابع معتبر الکترونیکی انجام خواهد شد. روش تجزیه و تحلیل داده‌ها از طریق روش تحلیلی استنباطی است.

۳- پیشینه تحقیق

کامران شیرزاد در مقاله‌ای به این جرایم رایانه‌ای اشاره داشته است که «پلیس برای دستیابی به الگویی مناسب برای پیشگیری از وقوع جرایم مجازی، علاوه‌بر ضرورت ملاحظه دقیق ویژگی‌های خاص و منحصربه‌فرد فضای مجازی، می‌تواند به الگوهای پیشگیری از وقوع جرایم مرسوم نیز استفاده کند که از میان الگوهای گوناگون، پیشگیری وضعیت اجتماعی از جرایم به‌دلیل انعطاف‌پذیری و جامعیت لازم می‌تواند مورد توجه قرار گیرند.» جوان‌جعفری در مقاله‌ای با عنوان «جرایم سایبر و رویکرد افتراقی حقوق کیفری با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای» ضمن اشاره به ابعاد فناوری اطلاعات، به فرامرزی‌بودن و سهولت ارتکاب جرم و مجرم در فضای مجازی اشاره کرده و اثربخشی و کارایی قوانین برای مقابله با جرایم دیجیتال را مستلزم نگاهی متفاوت به مقوله‌هایی، مانند تعریف جرم، ارکان جرم و مسؤولیت‌های کیفری دانسته است که در زمان تصویب قوانین باید مورد توجه قرار گیرند» (جوان‌جعفری، ۱۳۸۹: ۱۸۵).

۴- کشف و مجازات جرایم ارز دیجیتال

کشف جرایم مربوط به ارز دیجیتال با چالش‌های متعددی مواجه بوده و بسیار دشوار است. متأسفانه هیچ ناظر مشخصی این جرایم را پیگیری نمی‌کند، زیرا در بیشتر کشورها این دارایی‌های دیجیتال و مجازی هنوز به رسمیت شناخته نشده‌اند. طبق تحقیقات به‌عمل‌آمده در حال حاضر تعداد کمی از سیستم‌های بانکداری جهان از این رمزارزها استفاده می‌کند. باتوجه به این‌که شناسایی و استفاده از این ارزهای دیجیتال درصد پایینی دارد، بدون شک مراکز خاصی نیز برای نظارت و پیگیری وضعیت این جرایم وجود ندارد. در این صورت مجرمان چون می‌دانند در دسترس ناظران و مجریان نیست، با خیال راحت‌تری به جرم خود مشغول می‌شوند. از دیگر دلایل راحتی اجرای جرایم دنیای ارزهای دیجیتال عدم وجود محدودیت‌های جغرافیایی است. افراد به‌صورت آنلاین و از دورترین کشورها می‌توانند در این بازار شرکت کنند و مشغول معامله شوند. ازاین‌رو مجرمان در هر کشور و جایگاهی می‌توانند به فضای ارزهای دیجیتال دسترسی داشته باشند و هیچ محدودیتی برای آن‌ها وجود ندارد. از آنجایی که ارزهای دیجیتال به‌صورت آنلاین استخراج می‌شوند و معامله آن‌ها به‌صورت اینترنتی انجام می‌شود، نمی‌توان فرد مجرم یا کلاه‌بردار را شناسایی کرد. بدین‌ترتیب مجرمان و کلاه‌برداران خیلی راحت به فعالیت خود ادامه می‌دهند و هیچ نگرانی از شناسایی‌شدن ندارند. «علم جرم‌شناسی در عمر یکصدساله خود همواره در پی کشف عوامل جرم‌زا و شرایط مؤثر در بروز رفتار جنایی بوده تا به مدد آن و البته بهره‌گیری از تمامی تخصص‌های علمی به روش‌های درمان و اصلاح و تربیت بزهکاران دست یابد، اما نکته قابل توجه در این میان است که چنین تکاپویی تا اوایل دهه شصت و همزمان با پیدایش جرایم سایبری صرفاً در بستر دنیای حقیقی بوده است، هرچند که نقاط مشترک در مطالعات تطبیقی جرایم فضای حقیقی و مجازی وجود دارد، لکن باید گفت جرایم سایبری مرزهای مطالعاتی جدیدی برای جرم‌شناسان ایجاد کرده است، زیرا این جرایم در سیر تحول خود، نه‌تنها چالش مفهومی و

مصداقی برای حقوق جزای سنتی ایجاد کرده، بلکه ادبیات تخصصی خاص خود را نیز دارا هستند، هرچند برخی بر این باورند که اصلاح قوانین سنتی جزایی پاسخگوی نیازها در برابر جرایم سایبری است، در مقابل عده‌ای معتقدند دنیای مجازی دنیایی جدید است و مجرمان سایبر از لحاظ جرم‌شناسی از مجرمان عادی متفاوتند و مجازات‌ها و درمان‌های متفاوتی را نیاز دارند» (جوان‌جعفری، ۱۳۸۹: ۱۷۱). جرم رایانه‌ای دربرگیرنده همه اوضاع، احوال و کیفیاتی است که در آن شکل‌های پردازش الکترونیک داده‌ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان‌دادن این ظن است که جرمی ارتکاب یافته است. جرایم سایبری از زمان پیدایش تاکنون، با سه نسل یا تیپ مواجه شده است. دهه‌های ۶۰ و ۷۰ و اوایل ۸۰ زمان حاکمیت نسل اول تحت عنوان جرایم رایانه‌ای است. در این زمان درخصوص جرایم، محوریت بحث با رایانه بود. ازاین‌رو تعداد توصیف‌های مجرمانه بسیار کم بود. به‌تدریج در دهه ۸۰ تا اوایل دهه ۹۰ نسل دوم به میان آمد. بحث محتوا مورد استفاده قرار گرفت، یعنی به موضوع جرایم داده و اطلاعات توجه شد.

«جرایم رایانه‌ای عبارت‌اند از: جرایمی که در فضای مجازی رخ می‌دهند. به‌عبارت دیگر می‌توان گفت هر فعل یا ترک فعلی که در یا از طریق یا به کمک رایانه یا از طریق اتصال به اینترنت، چه به‌طور مستقیم یا غیرمستقیم رخ دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده باشد، جرم رایانه‌ای محسوب می‌شود. بنابراین باتوجه به تعریف فوق جرایم رایانه‌ای را می‌توان به سه دسته تقسیم کرد: ۱- جرایمی که در آن‌ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود؛ ۲- جرایمی که در آن‌ها رایانه به‌عنوان ابزار ارتکاب جرم به‌کار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهد، مثل کلاه‌برداری، جعل و سرقت رایانه‌ای؛ ۳- جرایمی که می‌توان آن‌ها را جرایم سایبری نامید که در فضای مجازی به وقوع می‌پیوندد، اما آثار آن‌ها در دنیای واقعی ظاهر می‌شود، مانند نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس، کرم‌های رایانه‌ای. به‌طور کلی جرایم اینترنتی به سه گروه اصلی: خرابکاری رایانه‌ای، کلاه‌برداری اینترنتی و جاسوسی رایانه‌ای تقسیم می‌شوند، اما از آنجایی که قسمت عمده این جرایم به مواردی همچون جرم هک و جرایم اقتصادی رایانه‌ای ارتباط دارد، بدون در نظرداشتن ضررها و خساراتی که نتیجه بی‌مبالاتی وارده به سامانه‌های رایانه‌ای است. شیوع جرایم رایانه‌ای در حوزه‌های مختلف اجتماعی موجب بروز آسیب‌ها و خسارات متعددی در جامعه می‌گردد. از مهم‌ترین آسیب‌های وارد بر فرد و جامعه از بین‌بردن مبانی و اصول اخلاقی و نظام اجتماعی بوده که خسارات زیادی به نظام‌های اقتصادی، سیاسی، فرهنگی جامعه وارد می‌آورد. هرچه بیشتر فناوری رایانه‌ای توسعه یابد جرایم رایانه‌ای مرتبط با هنجارشکنی‌های غیراخلاقی نیز توسعه پیدا خواهد نمود و تأثیر منفی بر نظام اجتماعی و بنیادی خانواده‌ها خواهد گذاشت» (شاه‌محمدی، ۱۳۹۳: ۱۰۲).

«با استناد به قانون ۲۵ جرایم رایانه‌ای هر شخصی که مرتکب یکی از موارد زیر شود، از سه‌ماه تا یک‌سال حبس و یا جریمه نقدی از پنج تا بیست‌ریال محکوم خواهد شد. ۱- دسترسی غیرمجاز به داده یا سامانه‌های رایانه‌ای و مخابراتی؛ ۲- شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج مغناطیسی یا نوری؛ ۳- جاسوسی اینترنتی؛ ۴- جعل رایانه‌ای؛ ۵- تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی؛ ۶- سرقت و کلاه‌برداری مرتبط با رایانه؛ ۷- جرایم علیه عفت و اخلاق عمومی؛ ۸- هتک حیثیت و نشر اکاذیب؛ ۹- تولید، انتشار یا در دسترس قراردادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی؛ ۱۰- فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم آورد» (عالی‌پور، ۱۳۹۰: ۸۹).

در ادامه به بررسی برخی دیگر از مهم‌ترین جرایم رایانه‌ای پرداخته می‌شود:

۴-۱- کلاه‌برداری اینترنتی

با استناد به ماده ۷۴۱ قانون مجازات جرایم رایانه‌ای نظیر کلاه‌برداری می‌توان گفت، برای این جرم نیز حبس از یک تا پنج‌سال پیش‌بینی شده است، علاوه‌بر این مرتکب به پرداخت جریمه نقدی در حق دولت محکوم خواهد شد. براساس بند آخر ماده ۷۴۱، مجازات جرم کلاه‌برداری رایانه‌ای می‌تواند شامل هر دو نوع مجازات حبس و جریمه نقدی شود.

۴-۲- سرقت رایانه‌ای

مجازات جرم سرقت رایانه‌ای نیز براساس ماده ۷۴۰ قانون جرایم رایانه‌ای دربردارنده جریمه نقدی و حبس از نودویک‌روز تا یک‌سال می‌باشد. به همین ترتیب اگر کسی به‌طور غیرمجاز نسبت به سرقت داده‌های متعلق به شخص دیگر اقدام نماید، مجرم شناخته شده و مستحق مجازات جرایم رایانه‌ای با عنوان جرم سرقت رایانه‌ای خواهد بود. همچنین اگر شخصی به روش‌های غیرمجاز به سامانه‌های رایانه‌ای و داده‌ها دسترسی پیدا کرده است، مطابق با قانون به جرم دسترسی غیرمجاز محکوم خواهد شد. مجازاتی که برای این افراد نیز در نظر گرفته می‌شود، براساس ماده ۷۲۹ قانون جرایم رایانه‌ای حبس از نودویک‌روز تا یک‌سال به اضافه جریمه نقدی خواهد بود.

۴-۳- شنود غیرقانونی

«یکی‌دیگر از مهم‌ترین جرایم رایانه‌ای به شنود غیرقانونی مربوط می‌شود. در مورد مجازات شنود نیز درصورتی‌که شخصی به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود نماید، به مجازات حبس از شش‌ماه تا دوسال و یا پرداخت جریمه نقدی محکوم خواهد شد» (گلستانی و همکاران، ۱۳۹۱: ۷۱). بیشتر مجازات‌های جرایم رایانه‌ای ثبت‌شده در قانون مربوطه می‌تواند به قلم قاضی صادرکننده حکم، شامل هر دو مجازات حبس یا مجازات جزای نقدی باشد.

۴-۴- مجازات جرایم رایانه‌ای علیه عفت

جرایمی که در زمینه اخلاق عمومی و منافی عفت قرار می‌گیرند، در قالب داده‌های اینترنتی و مخابراتی می‌باشند که به شکل اطلاعات ممنوعه و مستهجن مورد معامله و انتشار قرار می‌گیرد. جرایم رایانه‌ای منافی عفت و اخلاق عمومی به عوامل متفاوتی بستگی دارد.

مسأله مهمی که در این مورد وجود دارد، این مسأله است که چنانچه شخصی این جرایم را به‌عنوان حرفه خود قرار دهد یا این جرایم را به‌صورت سازمان‌یافته‌ای انجام دهد، امکان دارد برای وی مجازاتی با عنوان محاربه نیز پیش‌بینی شود و شخص به اعدام محکوم گردد.

«پس از بررسی قانون جرایم رایانه‌ای موجود به‌نظر می‌رسد قوانینی که بتواند با این جرایم برخورد نماید، حداقلی بوده و تنها نیاز امروز را برطرف می‌کند، لذا با پیشرفت این فناوری باید تدابیری اندیشید که مطالعات اخلاقی و حقوقی در این ارتباط نیز متناسب با آن گسترش یابد و دولت‌ها می‌بایستی قوانین خود را با جرایم رایانه‌ای متناسب نمایند. آنچه از ملاحظات اخلاقی، اجتماعی و حقوقی جرایم رایانه‌ای به‌دست می‌آید، این است که باید بر شناخت مسائل اصلی حقوقی و اخلاقی شهروندان در فضای سایبر تأکید کرد و گفت حفظ حقوق معنوی پدیدآورندگان نرم‌افزارهای رایانه‌ای یا حق مالکیت معنوی، ترویج اطلاعات سالم و پاک، اعتمادسازی در محیط سایبر، ایجاد اصل انکارناپذیری و جلوگیری از انتشار غیرمجاز داده‌های متنی، صوتی، تصویری، پورنوگرافی در فضای مجازی و حفظ امنیت داده‌ها و شبکه مواردی هستند که در محیط سایبر باید پیاده‌سازی شوند تا اخلاق انسانی و دینی به‌منظور نظم اجتماعی و عنصری روانی مهم بر افراد، جامعه و حاکمیت تضمین شود» (شریفی، ۱۳۸۹: ۹۱).

«محیط سایبر یا محیط مجازی مفهومی است که اخیراً از سوی جرم‌شناسان و حقوق‌دانان مورد توجه قرار گرفته و هم‌زمان با خلق این محیط جرایمی نیز در آن و با استفاده از آن به وقوع می‌پیوندد. مبارزه حقوقی با این جرایم مستلزم برداشتن چند گام اساسی بود؛ نخست جرم‌انگاری رفتارهای مجرمانه بود، البته جرم‌انگاری بدون ایجاد و احراز مسؤولیت کیفری عملی تقریباً بی‌سرانجام تلقی می‌شود؛ شاید بر همین اساس بوده که قانون‌گذار ایران در قانون جرایم رایانه‌ای بر مسؤولیت کیفری اشخاص حقوقی تأکید زیادی نموده و

مسؤولیت کیفری این اشخاص را برای نخستین‌بار در حقوق ایران صراحتاً مورد توجه قرار داده است» (گلستانی و همکاران، ۱۳۹۱: ۷۴). «به هر حال موضوع مسؤولیت کیفری و تبیین گسترده آن در حقوق جرایم رایانه‌ای از اهمیت بسیار زیادی برخوردار است، ممکن است و سؤالات زیادی در رابطه با گسترده مسؤولیت افراد در محیط مجازی مطرح شود، قانون‌گذار ایران فصل ششم از قانون جرایم رایانه‌ای را به موضوع مسؤولیت کیفری اختصاص داده است و تغییری که قانون فوق ایجاد نموده، شناسایی و ایجاد مسؤولیت کیفری برای اشخاص حقوقی در محیط مجازی است. پیشرفت‌های امروز فناوری و به تبع آن سازوکاری‌شدن حیات بشر قرن حاضر که همگی برآورد تلاش و اندیشه آدمی هستند، شاید توانسته باشد رفاه را برای وی فراهم آورد، اما به موازات این پیشرفت‌ها، حوادث نیز روزبه‌روز افزایش یافته و اشکال تازه‌ای به خود گرفته‌اند. از آنجا که این پدیده شگفت‌انگیز از همان بدو تولد در دسترس همگان قرار گرفت، هرکس مطابق هدف و غرض خود از آن جست و نتیجه آن شد که بعضی از این بهره‌برداری‌ها جنبه سوءاستفاده به خود گرفت و به همین متصدیان این امر را واداشت که تدبیری بیندیشند. از آنجا که مجموعه کشورهای بهره‌مند از این فضا هریک واجد فرهنگ و نیز قواعد و قوانین موضوعی خویش هستند، هماهنگ‌سازی قوانین جهانی در این حوزه از دغدغه‌های جامعه بین‌المللی است» (عالی‌پور، ۱۳۹۰: ۸۷).

«واقع‌بینانه باید در نظر داشت که استفاده از بسیاری اهرم‌های اعمال روش‌های پیشگیرانه در دسترس ما نیست، چراکه اساساً این فناوری، یک فناوری وارداتی است و ما در برابر جریان یک‌طرفه‌ای قرار گرفته‌ایم که از خیلی جهات دست ما را برای اعمال اراده بسته است، اما در عین حال از روش کنترل و نظارتی فیلترینگ می‌توان به‌عنوان یک اقدام پدافندی تا حدودی بازدارنده استفاده کرد، چنانچه به‌موجب مصوبه شورای عالی انقلاب فرهنگی، شماره ۵۹ مورخ ۱۰ دی سال ۱۳۸۱، کمیته‌ای تحت عنوان «کمیته تعیین مصادیق پایگاه‌های اطلاع‌رسانی رایانه‌ای غیرمجاز» مرکب از نمایندگان وزارت اطلاعات، وزارت فرهنگ و ارشاد اسلامی، سازمان صدا و سیما، نماینده دبیرخانه شورای عالی انقلاب فرهنگی و نماینده سازمان تبلیغات اسلامی با مسؤولیت نماینده وزارت اطلاعات و برای بررسی و احراز مصادیق فعالیت‌های غیرمجاز در عرصه سایبر تشکیل شد تا اعمال فیلترینگ باتوجه به جمیع جهات فرهنگی، امنیتی و ... مورد بهره‌برداری قرار داده شود» (جاویدنیا، ۱۳۸۸: ۲۲).

«جرایم رایانه‌ای جرایمی سازمان‌یافته می‌باشند که از طریق اشخاص حرفه‌ای و باسواد انجام می‌شوند و همیشه قصد آن‌ها سوءاستفاده از اشخاص دیگر می‌باشد. باتوجه به طیف گسترده جرایم و اصل قانونی‌بودن جرایم و مجازات‌ها قوانین رایانه‌ای امروزه برای مجازات مجرمین کافی، اما کامل نمی‌باشد، چون هر روز جرایم جدیدی به‌وجود می‌آید که برای مجازات آن‌ها نیاز به قوانین جدید داریم، همان‌گونه که جرایم اینترنتی همیشه در حال به‌روزشدن هستند، بایستی تلاش کرد تا بتوان با نوشدن جرایم هرساله قوانینی را که در زمینه جرایم جدید قابل اعمال باشد، ارائه کرد، چون رایانه و اینترنت همیشه و همیشه شکل‌های مختلفی به‌خود می‌گیرند. برای پیشگیری از این جرایم می‌بایست همه دستگاه‌ها تلاش کنند و مردم نیز توصیه‌های مسؤولین را در این مورد جدی بگیرند و در هنگام استفاده از اینترنت و رایانه مورد استفاده قرار دهند تا مورد سوءاستفاده دیگران قرار نگیرند. همچنین اگر دیدند سایت یا وبلاگی برخلاف قوانین تعیین‌شده در حال ارائه مطلب می‌باشد، موضوع را سریعاً به دادستانی اطلاع تا نسبت به اعمال فیلتر در مورد آن سایت اقدام شود، قضات نیز می‌بایست به شدت با کسانی که اقدام به جرایم رایانه‌ای می‌کنند، برخود نمایند، چون این جرایم هم سبب بردن مال و هم سبب بردن آبروی اشخاص می‌گردد، برخورد قضات نیز در پیشگیری از وقوع جرم اهمیت دارد، می‌بایست سعی شود در زمینه جرایم رایانه‌ای مجازات‌ها بازدارندگی بیشتری داشته باشد تا هم سبب ارعاب مردم و هم سبب عبرت‌گرفتن مجرمین شود تا دیگر اقدام به چنین جرایمی ننمایند» (شاه‌محمدی، ۱۳۹۳: ۱۰۲).

«یکی از نکات بسیار مهمی که باید درخصوص تدابیر پیشگیرانه اجتماعی مورد توجه قرار داد، این است که به‌لحاظ اقدامات زیربنایی و اساسی که در دستور کار قرار می‌گیرد،

نمی‌توان انتظار داشت همانند تدابیر پیشگیرانه وضعی یا ضمانت اجراهای کیفری و غیرکیفری، در کوتاه‌مدت نتایج محسوس و قابل مشاهده‌ای به‌دست آید، البته این مسأله هیچ‌گاه از دیدگاه جرم‌شناسان و متخصصان پیشگیری یک نقطه ضعف محسوب نمی‌شود، زیرا این تدابیر زیربنای فکری و شخصیتی بزهکاران و بزه‌دیدگان بالقوه را هدف قرار می‌دهند که درصورت تحقق اهداف پیش‌بینی‌شده، جامعه‌ای سالم و متعهد به رعایت هنجارها و ارزش‌های پذیرفته‌شده به‌وجود خواهد آمد. با این حال، بیشتر مسؤولان اجرایی چنین دیدگاهی را ندارند. آن‌ها می‌خواهند در کوتاه‌مدت آثار مقابله با جرایم را مشاهده کنند و آن را در کارنامه خود به ثبت برسانند و به همین دلیل، حاضرند هزینه‌های بیشتری در راستای اتخاذ و اجرای انواع تدابیر پیشگیرانه وضعی و ضمانت اجراهای کیفری و غیرکیفری متحمل شوند، اما در کوتاه‌مدت نتایج مقطعی به‌دست آورند. ازاین‌رو متأسفانه به‌دلیل وجود چنین تفکری، چندان به سیاست‌های پیشگیرانه اجتماعی بها داده نمی‌شود» (پاکزاد، ۱۳۸۰: ۶۷).

نتیجه‌گیری

امروزه با افزایش استفاده از اینترنت، از آن برای انواع مختلفی از جرایم، ازجمله سرقت اطلاعات شخصی، سرقت پول از حساب‌های بانکی کاربران، گسترش پرونوگرافی و ... استفاده می‌شود. تقریباً هر شخصی که از اینترنت برای منافع شخصی خود استفاده می‌کند، می‌تواند قربانی جرایم اینترنتی باشد. پیشرفت‌های امروز فناوری و به‌تبع آن سازوکاری‌شدن حیات بشر قرن حاضر که همگی برآورد تالش و اندیشه آدمی هستند، شاید توانسته باشد رفاه را برای وی فراهم آورد، اما به موازات این پیشرفت‌ها، حوادث نیز روزبه‌روز افزایش یافته و اشکال تازه‌ای به خود گرفته‌اند. از آنجا که این پدیده شگفت‌انگیز از همان بدو تولد در دسترس همگان قرار گرفت، هرکس مطابق هدف و غرض خود از آن جست و نتیجه آن شد که بعضی از این بهره‌برداری‌ها جنبه سوءاستفاده به خود گرفت و به همین متصدیان این امر را واداشت که تدبیری بیندیشند. مسأله بسیار بااهمیت درخصوص جرایم رایانه‌ای، چالش‌هایی است که پس از وقوع جرم رخ می‌دهد؛ مجرمان رایانه‌ای در این محیط به آسانی هویت خود را پنهان می‌کنند، کشف جرایم بسیار مشکل بوده و امکان تعقیب مجرمان بسیار پایین است. نکته اساسی در جرایم اینترنتی حذف مکان در قلمروی مکان فیزیکی و محدوده حاکمیت سیاسی است. امکان دارد جرم در محدوده خارج از جغرافیا و قلمرو حاکمیت کشور انجام شود و جرم‌انگاری لازمه نادیده‌گرفتن اصل صلاحیت سرزمین و توسعه مرزهای جغرافیایی است، در مواردی براساس ماده ۵ قانون مجازات‌های اسلامی مبنی‌بر محدودبودن مورد تعقیب و مجازات تبعه خارجی نسبت به جرایم ارتکابی خارج از کشور که در سال ۱۳۷۰ به تصویب مجمع تشخیص مصلحت نظام رسیده است، هر ایرانی و یا بیگانه‌ای که در خارج از قلمرو حاکمیت ایران مرتکب یکی از جرایم ذیل شود و در ایران یافت شود و یا به ایران مسترد گردد، طبق قانون مجازات‌ها اسلامی مجازات می‌شود.

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

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

تشکر و قدردانی: از تمام کسانی که ما را در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

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

منابع و مآخذ

– پاکزاد، بتول (۱۳۸۰). *جرایم رایانه*. پایان‌نامه کارشناسی ارشد، به راهنمایی استادمحمدعلی اردبیلی، تهران: دانشگاه شهید بهشتی.

– جاویدنیا، جواد (۱۳۸۸). *جرایم تجارت الکترونیکی*. چاپ دوم، تهران: انتشارات خرسندی.

- جوان‌جعفری، عبدالرضا (۱۳۸۹). «جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای»). *نشریه دانش و توسعه*،۱۷(۳۴): ۱۶۹-۱۹۲.

- ذبیح‌الله‌نژاد، وحید (۱۳۹۶). «ماهیت جرایم رایانه ای و نقش پلیس فتا در پیشگیری وضعی و پیشگیری اجتماعی از جرایم سایبری نقش پلیس فتا در پیشگیری و کشف این جرایم». *فصلنامه دانش انتظامی پلیس پایتخت*، ۳(۲۷): ۸-۲۷.

- شاه‌محمدی غلامرضا (۱۳۹۳). «بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات». *نشریه پژوهش های اطلاعاتی و جنایی*، ۹(۳): ۹۹-۱۱۹.

- شریفی، مرسده (۱۳۸۹). *جرایم رایانه‌ای در حقوق جزای بین المللی*. پایان‌نامه کارشناسی ارشد، تهران: دانشگاه آزاد اسلامی واحد تهران.

- عالی‌پور، حسن (۱۳۹۰). *حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)*. چاپ اول، تهران: انتشارات خرسندی.

- گلستانی محمود؛ پهلوانی محمدتقی و عبدالله‌پور، مهدی (۱۳۹۱). «چالش‌ها و فرصت‌های جرایم سایبری». *فصلنامه دانش انتظامی استان سمنان*، ۶(۴): ۴۸-۷۹.