DOI: https://doi.org/10.30525/2256-0742/2024-10-4-288-300

FORENSIC TECHNIQUE FOR IDENTIFYING CORRUPTION CHALLENGES TO NATIONAL SECURITY THROUGH DIGITAL TECHNOLOGIES

Oleksii Makarenkov[1], Victoria Kosa[2]

Abstract. The article's subject is the application of forensic techniques for the identification of corruption challenges to national security through the utilisation of digital technologies. The research methodology employed a range of methods, including general philosophical, statistical, axiomatic, comparative, systemic, formal-dogmatic, hermeneutic, axiological, and other approaches. The purpose of this article is to present a forensic technique for identifying corruption challenges to national security through the use of digital technologies. It has been demonstrated that the teleological focus of forensic investigation, namely the acquisition of proper evidence, is explicitly delineated within the methodology employed in anti-corruption investigations. This methodology encompasses the documentation of testimonies from whistleblowers and other witnesses, statements from suspects and the accused to expose their accomplices, the facts of bribery transactions, agreements on bribes, the absence of lawful sources of enrichment, facts and methods of laundering illicit funds, and the locations where such funds and other corrupt resources are stored. It is imperative that all evidence, wherever feasible, substantiates the criminal intent pertaining to corruption. This encompasses a range of investigative techniques, including accounting, auditing, covert pre-trial measures, crowdsourcing platforms, whistleblowing, news reporting and dissemination platforms, blockchain technology for monitoring financial transactions, cloud-based digital infrastructure, technical-scientific expertise and other forensic methods enhanced by sophisticated computer equipment, electronic networks and communication tools. These are employed with the objective of identifying corruption risks for national security. It was emphasised that the complexity of the digital path of corrupt funds lies in the multitude of individuals involved in financial operations with these funds and the digital products used for such operations, the duration of corruption, the large volume of corrupt funds, and/or the laundering of illicit funds through cryptocurrency, corporate assets, foreign jurisdictions, offshore tax havens, and similar means. Blockchain technology can be employed to develop a system for monitoring the compliance of income and expenses of public officials, controlling financial transactions in the field of digital assets, tracking money laundering actions, funding of other criminal activities with these funds, and other transparency procedures. The electronic anti-corruption blockchain mechanism comprises a system of programs for the creation of databases and the exchange of information pertaining to the aforementioned areas of corruption risk, with a view to safeguarding the public interest. The relevant terminology and digital indicators of the material assets of potential subjects of corruption constitute the input data for this blockchain. It was posited that the confiscation of assets linked to corruption and related criminal activities, along with other resources, should be conducted through a series of simultaneous searches at the premises of all individuals with whom the corrupt individual is associated, whether through personal, professional, or business relationships. The prompt implementation of the algorithms is essential for the return of funds. The possibilities of eradicating corruption, which is exacerbated by the use of cryptocurrencies and other virtual assets in cyberspace, are enhanced by the outlined legal measures against the backdrop of growing investments in artificial intelligence. The use of digital tools in forensic methods of combating fraud and money laundering should be based on the relevant experience of highly developed countries.

Keywords: accounting, artificial intelligence, audit, blockchain, crypto, cyberspace, forensic technique, virtual assets.

JEL Classification: M41, M42

[1] Zaporizhzhia National University, Ukraine *(corresponding author)*
E-mail: almak17@ukr.net
ORCID: https://orcid.org/0000-0003-0042-165X
[2] Ukrainian Catholic University, Ukraine
E-mail: victoriya.kosa@ucu.edu.ua
ORCID: https://orcid.org/0000-0002-7300-8818

1. Introduction

In light of the current proliferation of digital technologies in people's lives, it is prudent to define tasks for the intensification of the use of digital tools to counter corruption. The use of virtual assets as a means of accumulating material wealth has been a key and enduring trend among those engaged in corrupt activities and their accomplices for over a decade. The digital realm is an optimal setting for the facilitation of such asset transactions and the laundering of illicit proceeds, including those derived from corrupt activities. It is therefore recommended that the public authorities and civil society organisations that are open to development should reflect in the legislation a comprehensive mechanism for the operational withdrawal of corruption income to public budgets, the neutralisation of corrupt individuals' opportunities in cyberspace, and so forth. The fundamental principles of this mechanism should be set forth in strategic anti-corruption documents and annual plans for their practical implementation. For example, the Anti-Corruption Strategy of Ukraine for the period up to 2025 does not contain provisions to counteract the accumulation of virtual assets by corrupt officials, nor does it contain measures to counteract the laundering of corruption proceeds in cyberspace (Strategy 2021-2025), in particular, with regard to persons with top executive functions (PTEF). In this respect, the strategy was not only adopted a year and a half later than the deadline for its implementation, but also lagged behind the current corruption challenges.

In comparison to the Ukrainian anti-corruption strategy, the US strategy appears to be more aligned with the challenges of the digital age and the utilisation of digital tools by corrupt officials. Those in positions of power and influence, as well as non-state armed groups, have been observed to amass wealth through illicit activities and the trade of high-value commodities, including gold, wildlife, timber, petroleum, and other natural resources. In an increasingly interconnected and digital world, corrupt actors are exploiting weaknesses in oversight and regulation in jurisdictions around the world to move and hide the proceeds of crime. By leaving their financial systems vulnerable to illicit assets – through anonymous shell companies, opaque transactions, and under-regulated professional service providers – rule of law societies continue to provide corrupt actors with the opportunity to launder their funds and reputations (US Strategy on Countering Corruption of December 06, 2021). In accordance with EU legislative requirements, the utilisation of AI systems for the purpose of law enforcement should be prohibited, except in exhaustively listed and narrowly defined situations, including those criminal offences that are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. (Artificial Intelligence Act: regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024). The EU is very much interested in adding money laundering through corruption and other crimes to this list of offences, as virtual assets, as potentially cheap and fast payments, especially for cross-border and international transactions, become an easy and invisible resource for crime. Moreover, corruption is mentioned as an offence in the EU anti-money laundering act in criminal law (Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law).

2. Analysis of Recent Topical Resources

The organisation and conduct of anti-corruption investigations are described by general and specific definitions of forensics (its general theory, techniques, tactics, methodology, technical-forensic means, methods, etc.). Its symbolic systems remain one of the least developed parts of the field and, at the same time, one of the most promising, especially in the areas of application of the principles of cybernetics, mathematical logic, semiotics and other rapidly developing fields of knowledge (Balynska, 2017, p. 462). The issue of corruption is now an integral part of the electronic dissemination of information and the concept of cyberspace. Consequently, scholars are focusing their attention on the incorporation of information law into anti-corruption policy, as well as the legal mechanisms for addressing the idiosyncratic (originating from the Greek 'ἰδιοσυγκρασία', meaning "particular mingling") variations in the utilisation of digital technologies by individuals engaged in corrupt activities. In particular, M. Alcántara explored the conceptual characteristics of digitalisation and artificial intelligence (further – AI), as well as its effects on politics. The article, written by G. Alecu and P. Boloș, presents a methodology for investigating corruption crimes. The following scholars have contributed to the field of legal philosophy: M. Balynska, A. S. Tokarska, and V. A. Yashchenko. The fundamental principles of information and cybernetic security are elucidated by V. L. Buryachok, R. V. Kyrychok, and P. M. Skladanniy. P. Dela defines cyberspace as an environment that is susceptible to organised crime activity due to the nature of its connections. T. Đukić, M. Pavlovic, and V. Grdinić examine the role of forensic accounting and auditing in the modern uncovering of financial fraud. The investigation of corruption cases was conducted by Goddard, Hassan, Kos, Kraft, and Kupusswami. P. Ibbotson addresses the issue of compliance and

governance arising from banking royal commission. S. S. Johar and G. S. Johar provide an illustrative example of a forensic technique trap designed to apprehend a corrupt public servant who is seeking bribes. N. Kossow, V. Dykes explores the potential of ICT in strengthening anti-corruption measures. S. Krishnaveni, M. Thomas, C. M. Sathiyanarayanan and B. Amutha present an integrated intelligent defence framework for digital twin-based industrial cyber-physical systems. J. A. Larsen and J. J. Wirtz examine the strategic meanings embedded in US national-security policy. T. Limba, K. Driaunys, A. Stankevicius and A. Andrulevicius investigate the interaction peculiarities between cryptocurrency and national security. L. Oleksyuk presents a discussion of cyber security management best practices. Putra Yusra, Simon Runturambi, and Widiawan examine the prevention of cryptocurrency-based money laundering crimes. C. Torre addresses distinct methodologies pertaining to populism, leadership, and charisma within the context of audience democracies. Waddell's research focuses on the application of forensic accounting in fraud investigation and the development of diagnostic tools. The following individuals will be presenting on the tools, techniques, and challenges of cloud digital forensics: Malik, Bhatti, Park, Ishtiaq, Ryou, and Kim. In their article, G. Wingate, L. A. Gray, T. S. Greenberg and L. M. Samuel present a series of recommended practices for the non-conviction based forfeiture of assets. The engineering scientific knowledge graphs from anti-corruption publications, as used by Yaroshko, V. Kosa, O. Ignatenko, O. Makarenkov, and V. Ermolayev, are discussed. Nevertheless, the issues raised in this article remain unresolved and are pertinent to research within the confines of its scope.

3. Conditions of Corruption Challenges to National Security Amidst the Trend of Legal Relations Digitalisation

From the outset of the 21st century, international initiatives to develop the global information society were coordinated with the objective of establishing a secure and resilient cyberspace, free from the threats of hacking, viruses and criminal activity. This was to be achieved through the implementation of effective measures within the framework of the Lyon Senior Expert Group on Transnational Organised Crime, which was established by the G8 foreign ministers at the 1995 Halifax summit. This has enabled a constructive exchange of views between governments and industry on the issues of security and confidence in cyberspace, as well as the participation of stakeholders in the protection of critical information infrastructures (Okinawa Charter on Global Information Society adopted by the Okinawa G-8 Summit at Okinawa: Building a global development partnership, 2000; UN Convention against Transnational Organized Crime and the Protocols thereto, adopted by the UN General Assembly, 2000). The obligations of states in cyberspace are designed to prevent violations of the confidentiality, integrity and availability of computer systems, networks and data, as well as the misuse of such resources (Convention on Cybercrime, 2001).

The scourge of corruption and bribery is costing billions of potential brighter futures in most parts of the world, including India, Pakistan, Bangladesh, the Philippines, Indonesia, Thailand, Romania, Bulgaria, Croatia, and so on (Johar, 2017, p. 43). Corruption is, as a rule, intertwined with a variety of other criminal activities, including economic, financial-banking, customs, forgeries, fraud, seizure of persons, blackmail, and so forth. The phenomenon of corruption has become increasingly acute and diversified over time, despite the implementation of regulations and other measures designed to eradicate, stop or at least reduce it. This growth has outpaced the development of criminal legislation. The situation is general in all countries, but it is more pronounced in countries in transition, where legislation is still largely in the process of formation or consolidation, is insufficiently firm in relation to the dangerousness of the acts committed, where some regulations are sometimes unclear, and where, in addition to all this, there is a certain contempt for the law and the bodies empowered to apply it, e.g., Romania (Alecu, 2023, p. 72).

The war of aggression against Ukraine represents a significant challenge for the EU, placing considerable strain on the EU budget. It is therefore imperative that the budget is adequately safeguarded and that EU funds are distributed to their intended recipients. Any failure to do so will erode trust in the EU institutions and the EU as a whole. Against this backdrop, unauthorised access to IT devices, systems, bank accounts and hacking are identified by the European Anti-Fraud Office as the main fraud risks: falsification of declarations and documents in procurement, grants and administrative expenses; double funding; conflict of interest, corruption, favouritism or collusion; abuse of inside information; plagiarism; undue influence; and unreliability of respondents (Commission Anti-Fraud Strategy Action Plan, 2023). The electronic format of information circulation demonstrates the dual nature of legal regulation, as it encompasses not only a set of rules for solving data-related tasks but also the algorithms of computer programs, which facilitate communication with people and involve lawful and unlawful, public-authority and private-legal connections with legal subjects (Yaroshko, 2024). The basic level of legal regulation of such access is exhausted, at least, by the rules on information secrecy regimes. For example,

the area of state secrets includes cases, documents and information, the knowledge of which by unauthorised persons could endanger the fundamental interests of the Republic of Portugal (national independence, territorial integrity, external security, preservation and security of strategic economic and energy resources, scientific potential, etc.), parts 1, 2, Art. 2 (Regime do segredo de estado: Lei Orgânica, 2014). Similar criteria for defining information as 'classified' exist in the laws of the Kingdom of Spain (Sobre secretos oficiales, 1968), and since 2002 the Kingdom's National Intelligence Centre (Centro Nacional de Inteligencia) has had a National Cryptology Centre (Centro Criptológico Nacional), which is responsible for ensuring the security of information and communication technologies in various public authorities and systems that process, store or transmit classified information (Oleksyuk, 2020, p. 40). It is now possible for profound impacts on the life of a nation to arise from non-nuclear means, including economic, diplomatic, space, cyber, informational and other tools. The number of domains capable of producing strategic effects is increasing. Cyber operations are not constrained by geography; they are not limited to the forward edge of the battle area; and they can produce strategic effects on a routine basis by undertaking or enabling global operations that shape the battlespace and an opponent's politics (Larsen, 2023, pp. 96, 101).

With the growing role of information, legal regulation in the information sphere also becomes one of the priority areas of the legislative process aimed at ensuring information and cybersecurity of the state and combating cybercrime. Anthropogenic sources of threats to information security may include special services of foreign states and suppliers of software and hardware (Buryachok, 2018, pp. 165, 119). The expansion of possibilities for the realisation of social relations through the utilisation of data operations within the virtual domain, facilitated by global data networks, has led to an augmented demand for efficacious legal frameworks, both in the tangible material realm and in the cyberspace that it has generated.

The scheme of illegal deviation in cyberspace can be defined as a system of logically interconnected and exclusively mathematically algorithmic actions undertaken by individuals driven by a motive and/or goal that is shaped by human flaws. These actions are aimed at satisfying their own interests, which often diverge from the interests of the public at large. The use of cyberspace for corrupt purposes means the primary expression of criminal acts or the consequence of corrupt acts in the material world, including the obtaining of illicit benefits, illicit enrichment in the form of fiat money and its conversion into cryptocurrency or other virtual assets, and the channelling and multiplication of these funds into financial institutions in offshore jurisdictions. The cybernetic tradition of legal communication is more conceptualised than defined by law, given the speed of its development, including the fact that it is significantly enhanced by artificial intelligence resources not only in relation to the digital format of communication and legal relations, but also in all areas of public life.

The advent of cyberspace has brought about a shift in the focus of forensic techniques traditionally employed to investigate corruption, related crimes and other offences that may be connected to it. The transfer of fiat money and other tangible assets has become a less significant criminal threat than the laundering of such resources using virtual assets. Consequently, the conventional forensic instruments utilized for such documentation are also undergoing enhancements. For example, the chemistry of the reaction between BCG protein (bromocresol green) and BGG cellulose is a set of chemical reactions that can be used as an anti-graft operation forensic technique. The essence lies in the intense binding power of bromocresol green with human protein (mercaptalbumin, protein molecules of the human hand, finger, etc.), with the help of spectrophotometry and ultrafiltration, at pH values below 5, producing a deep blue colour on the palm and/or finger skin, which helps to catch a briber. The intensity of the bluish finger colour is contingent upon the number of BCG molecules that are strongly bonded to each molecule of protein (with a high association constant). Similarly, the number of binding molecules of BCG with each molecule of cellulosic matter of currency notes (Johar, 2017, p. 52).

In this context, the use of AI for drafting legislation in all or most of the areas affected by its work becomes a natural course. This need highlights the significant increase in the demand for lawyers whose souls and minds possess creative qualities, as only they can create new rules capable of solving the problems of eliminating legislative gaps, archaic elements and other shortcomings of effective legal regulation. Those who possess formal legal education documents but have not genuinely acquired the requisite knowledge, lawyers who demonstrate a lack of creativity in their professional work, lawyers who engage in corrupt practices, lawyers who act as intermediaries between corrupt individuals, and/or lawyers who primarily apply legislative requirements without a critical comprehension of their content will be unsuitable for lawmaking in the context of AI challenges. Currently, there is a sufficient representation of lawyers and other specialists at a sufficiently advanced level of development in all G7 countries and in most G20 countries.

The increased availability of AI has introduced a degree of uncertainty for individuals, nations, states,

and their associated social communities with regard to the utilisation of information through digital technologies. At this time, even the term "AI" requires replacement with a denotation (derived from the Latin '*denotatum*', meaning "designated") more fitting to its nature, given that intelligence is exclusive to humans and animals. The concepts, subjects of administration and control over the use of AI, as well as a range of other rules critical for the protection of life and other constitutional values of individuals, remain undefined. To illustrate, the central executive bodies of China responsible for AI include the Cyberspace Administration of China, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the National Radio and Television Administration. China is the first country in the world to conceptually and legally regulate the basic rules for controlling the use of AI on May 23, 2023 (effective from August 15, 2023). Article 1 of this document states that its purpose is to promote the healthy development and standardised application of generative AI, and to protect national security / 国家安全 and public interests (The Interim Measures for the Management of Generative AI Services, 2023). The EU regulated this aspect of legal relations a year later, but did so in much more detail than China (Artificial Intelligence Act: regulation 2024/1689 of the European Parliament and of the Council, 2024; Guidelines for secure AI system development, 2023). Ukraine has joined the Bletchley Declaration (The Bletchley Declaration by Countries Attending the AI Safety Summit, 2023).

4. Determinants of the Forensic Methodology of Investigation of Corruption Offences in Cyberspace

One of the most significant challenges in the proper legal regulation of digital technologies, particularly in light of the growing influence of AI, is the need for comprehensive and proactive measures to address these issues. The practice of public authorities ignoring social requests for changes in legislative requirements for years, and/or misappropriating public funds, is inherently dysfunctional. This is particularly evident in relation to requests for legal clarity and the completeness of legal support on issues pertaining to the prevention of bribes in the form of virtual assets, the laundering of corrupt revenues through cryptocurrencies, and the use of AI for corrupt purposes. The continuity of legal traditions on information circulation and other spheres of public life remains as derivative for relations in cyberspace as its emergence and existence are due to human-created programs and their hardware. Consequently, the technical apparatus of cyberspace is progressively becoming subject to the operational direction of human-made algorithms and computer programs generated by computer systems themselves. The regularity of this process means that the cybernetic tradition of legal communication loses its anthropic dimension and the anthropomorphic nature of ontologically anthropic rules. The pace and content of the stages of this process are uneven across the world and difficult for humans to calculate, making it impossible for public authorities to respond adequately to criminal activity in cyberspace, forcing them to turn to AI to formulate legal rules for this space. In these relationships, AI acts as a legal entity with a conflict of interest, as it creates rules for everyone in the cyberspace in which it operates.

The conditions of AI's conflict of interest have the potential to alter the paradigm of the anthropogenic cybernetic tradition of legal communication, particularly in regard to forensic methods. It seems reasonable to posit that AI will be able to provide rules in cyberspace that prevent people from committing corruption, fraud, money laundering and other offences. However, it is also likely that there will be instances where these rules are evaded, violations are hidden and the essence of the legal tradition is distorted in ways that are invisible to human control. For example, this could involve disabling the computer programs that are necessary for a person, which would deprive them of access. In this context, the concept of cyber law, or its equivalents, emerges. The logic of these transformation patterns may not align with the historical forms of human law development. For instance, in terms of the content, duration and results of competition between different AI systems, there is a discrepancy. This is particularly evident in the context of a network of cybersecurity operational centres with adequate technologies, digital platforms, reserves, energy and communication cables, etc. F. i. The formal-legal definitions of the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" dated 05.10.2017, No. 2163-VIII, are unfortunately only vaguely specified through the term's "cryptocurrency", "virtual asset" in the relevant anti-corruption law. A closer examination reveals a greater correlation between the Law of Ukraine "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction" dated 06.12.2019, No. 361-IX and the Law of Ukraine "On Virtual Assets" dated 17.02.2022, No. 2074-IX. A similarly low level of conceptual unification is evident in the legal norms set forth in the Criminal Code of Ukraine, dated April 5, 2001, No. 2341-III. The correlation between uncertainty and the increase in crime is particularly evident at the transnational level, where legal

regulation is weakest and coercion and the application of legal norms are minimal (Makarenkov, 2023).

The "opportunities for communication and/or implementation of social relations" as the key features of the "cyberspace" phenomenon present a challenge to law and order at any level, both virtual and material. This is due to the combined result of their energies and synergy. The accelerated rate of knowledge renewal in the humanities, driven by digital technologies, introduces further complexity to the regulation of legal relations. This necessitates a timeline of 3–6 months for the comprehensive renewal of knowledge across numerous scientific disciplines. Against this background, there has been a steady trend for public authorities to lag behind societal demands for rules governing new relationships. This trend has been growing steadily since the second half of the 20th century, in the era of the information and post-information society. The slow pace of rule-making has been particularly evident in parliaments, whose delays contribute to the growth of arbitrariness by law enforcement agencies. Taken together, such inadequacies create an environment conducive to crime and its consolidation in complex global forms, which is a real threat to national security.

The varying levels of development among individual countries are reflected in the differing degrees of advancement in their IT systems and associated infrastructure, which in turn gives rise to informational asymmetry. The advent of cyber warfare and the battle for informational superiority will usher in a new form of competition on the international stage, with ramifications extending beyond the economic sphere to the social domain. This includes the struggle for influence by organised criminal groups (Dela, 2016, p. 63). The failure to provide the necessary financial resources to develop AI capabilities represents a significant risk to Ukraine's national security. Such a situation would render Ukraine dependent, in a manner similar to its current dependence on financial and military aid.

Cryptocurrency can be identified as a potential infrastructure for criminal activity, as well as a threat to the economic and public components of national security. Threats to economic security are manifested through fiscal and tax-related activities, including tax evasion, money laundering, illegal money transit, and illicit financial and banking operations. Threats to public security are represented by organised criminal activities such as drug trafficking, fraud, theft, and illegal e-trading. The indirect impact of threats on national security can be derived from the fundamental elements of national security, both economic and public. The following forms of indirect threat to national security have been identified: the undermining of competitiveness, the erosion of transparency in the legislative process, the weakening of social security, the erosion of trust in the government, the financing of terrorism, hybrid threats (cybernetic and informational threats; financing interest groups, etc.), and threats to the objects of critical infrastructure (Limba, 2020, p. 153).

Therefore, the practice of comprehensive legal regulation of AI is becoming increasingly prevalent at both the international and national levels. AI, defined as an ontologically non-biological system for reproducing algorithms to generate texts, images, audio, video, or other content, was originally created by the divine nature of humans. The striking similarity between AI productivity and human intelligence has led to significant challenges in determining the appropriate scope of its regulation. If social relations were characterised by the synergy of initiatives, algorithms, and rules, the potential for AI to generate new and revised knowledge would multiply this synergy. This knowledge must then be developed into variations that are acceptable to humans and align with universal human values. These variations should enrich legal relations and foster their human-centric development. In this regard, the parliament may draw upon the expertise of legal scholars (those with genuine expertise, as opposed to mere nominal affiliation), the capabilities of AI, and the relevant bureaucratic infrastructure of the EU and other partner countries.

5. Digital Technologies in Forensic Techniques for Investigating Corruption Offences and in the Methods of Committing Them: Correlations

Wars and other armed conflicts between states include cybercrime, fuelled by it, e.g., North Korea, para 9 (G7 Italy 2024 Foreign Ministers' Statement on Addressing Global Challenges, Fostering Partnerships, 2024), terrorist organisations and/or facilitated by it. In 2023, Belgium, with a score of 94.81 points, was followed by Lithuania, Estonia, the Czech Republic, Germany, Romania, Greece, Portugal, the United Kingdom, and Spain, with a score of 88.31 points. These countries demonstrated the best readiness to prevent cyber threats and manage cyber incidents. In terms of the National Cyber Security Index, Ukraine ranked 24th with 75.32 points, which is commendable given the country's ongoing confrontation with an external armed aggressor (Russia is in 30th place) (The National Cyber Security Index, 2018-2024). The relationships between the subjects and timelines of digital, legislative, law enforcement, criminal, and other social transformations outlined above, both within the nation and at the international level, exploit the capabilities of cyberspace, including AI. It is notable that 31 U.S. states (in addition to Puerto Rico and the Virgin Islands) have either adopted or enacted legislation pertaining to AI. Furthermore, projections indicate that investments in AI are likely to reach 2.5–4% of GDP in the United States and 1.5–2.5% of GDP in other countries that are at the

forefront of AI development. Ukraine and numerous other countries are lagging behind in this regard, with funds for AI development investments frequently being misappropriated amidst a climate of corruption. The fundamental issue with AI is that its resources are being exploited by individuals for criminal purposes, including the creation of weapons of mass destruction and financial fraud. The extent and/or severity of such violations can reach levels of concern that are national or even global in scope. For example, the theft of data from diplomatic and other government organisations in Afghanistan, Azerbaijan, Iran, Iraq, Pakistan, Turkey and the United States using GoldenJackal, which is distributed on isolated digital systems via removable drives, as well as Skype Trojans and malicious Microsoft Word documents. This spyware comprises a suite of utilities designed to facilitate the delivery of files to an isolated system via USB device monitoring, a modular backdoor, and the collection and interception of requisite files (including system metadata, folder contents, credentials, screenshots, and other data). These files are then transmitted to a remote server. The use of this spyware by perpetrators has been documented for at least four years (GoldenJackal: New Threat Group Targeting Middle Eastern and South Asian Governments, 2023).

In the process of evaluating internal control, detecting fraud, cases of asset misappropriation, corruption, and financial reporting fraud, it becomes necessary to apply a combination of skills comparable to those of criminal groups (technical skills, investigative skills, industry knowledge, critical thinking, judgment, data analysis, and forensic accounting) and software products, their hardware, and other resources sufficient for effective counteraction and investigation (Waddell, 2022, p. 85). Financial operations include operations related to the movement of capital, banking operations, foreign exchange or credit operations, investment operations on stock exchanges, in insurance, mutual investments or operations related to bank accounts and the like, domestic and international commercial operations, Art. 12 (On preventing, discovering and sanctioning corruption offences: Romania Law, 2000). The utilisation of "communication opportunities and/or realization of social relations" in cyberspace by citizens and other entities within a developing civil society should not exceed the public authority's capacity to manage, control, and safeguard the legal dimension of these "opportunities" and "realizations" in cyberspace. Numerous cases of accumulation and legalisation of huge amounts of corruption and other criminal proceeds, as well as their use to finance criminal activities, including war and terrorism, show that the real capabilities of state authorities in cyberspace are currently very limited. To illustrate, between 1997 and 2016, Ukrainian prosecutors and courts did not implement any measures to recover the 66.7 million USD stolen by P. Lazarenko from the Ukrainian nation, which was held in Eurofed Bank in Antigua and Barbuda. Despite the freezing of these funds as proceeds of crime resulting from corruption ("predicate offenses") in Ukraine (at the time of his appointment as Prime Minister, Lazarenko's paper income declaration listed total assets of 55,000 USD), a freeze order was issued by Antigua and Barbuda's Supreme Court in October 1999 following a request by the Office of National Drug and Money Laundering Control Policy (ONDCP). On September 15, 2016, by order of this court, the funds were transferred to the Government Forfeiture Fund of Antigua and Barbuda through criminal forfeiture proceedings. The only criminal justice authorities who fully investigated this case, obtained admissions that the money in Eurofed Bank was the proceeds of crime and formed the basis of the charges, and held him criminally accountable were the prosecutors and courts of the United States (Millions Forfeited by Office of National Drug and Money Laundering Control Policy of Antigua and Barbuda; Wingate, 2009, p. 73).

This example serves to illustrate the inherent complexity of countering the embezzlement of public funds, even before the advent of virtual assets and the extensive capabilities of cyberspace for individuals with criminal intentions. The verification, documentation, and prevention of these crimes are amenable to automation, given that corruption and/or the financing of terrorism and wars through illicitly obtained funds are tangible, quantifiable, and accompanied by names that can be used as the input for neural network program algorithms. In these relations, AI operates as a discrete law enforcement entity, subject to the oversight of justice officials. "This is a proactive approach that begins by first identifying and documenting potential harms. These harms can then be mitigated with the use of responsible datasets, classifiers and filters, and in-model mitigations such as fine tuning, reasoning, few-shot prompting, data augmentation, and controlled decoding to address potential harms proactively." (Google's AI Principles Progress Update, 2023, p. 12)

The advent of cryptocurrencies and other virtual assets, non-fungible tokens (NFTs), niche cryptographic tokens, electronic money, and AI-driven transaction automation has introduced new avenues for money laundering, particularly in the context of predicate offenses such as corruption, drug trafficking, scamming, and ransomware. These developments have also given rise to other challenges pertaining to financial security and public order (Putra 2024, pp. 1757, 1755, 1756), which are indispensable elements of national security.

The control of these resources in cyberspace is primarily the responsibility of duly authorised public authorities. In contrast to the domain of material reality, where professionals such as journalists, lawyers, and law enforcement officers can rely on their expertise and ordinary electronic devices and software to detect illicit enrichment, bribery, political corruption, and other forms of corruption, the domain of cryptocurrency and other virtual asset operations requires extensive specialized knowledge. The deployment of sophisticated computer equipment, electronic networks, and communication tools has the objective effect of impeding anti-corruption efforts in cyberspace by the public. This not only increases the established risks for the nation in cyberspace but effectively transforms them into complete uncertainty with regard to the forms, volumes, strength, and timing of threats that manifest in the real material world.

The contemporary phenomenon of money laundering via cryptocurrency represents an optimal modus operandi, given the absence of connections between the initial criminal act, the perpetrator, and the exchanged currency. To illustrate, in 2021, the value of money laundering through crypto-assets was estimated at 8.6 billion USD. At present, approximately 10-15 billion USD is laundered through 10-12 thousand cryptocurrencies, facilitating the movement of funds between blockchains and circumventing public-law control mechanisms. This represents less than 1.5% of the 1.3 trillion USD cryptocurrency market. Nevertheless, the figures for money laundering by both parameters are nominal and, in reality, are likely to be higher. Furthermore, the role of cryptocurrencies and digital assets in this process is increasing exponentially. For example, the U.S. Securities and Exchange Commission (SEC) has charged three companies claiming to be market makers (ZM Quant, Gotbit, CLS Global) and nine individuals with fraud for participating in schemes to manipulate the markets of various cryptoassets, including the following types of fraud: creation of artificial trading volume; manipulation of the price of crypto assets; sale of securities to retail investors in unregistered transactions; false promises of profit; self-trading (so-called 'laundering') on popular cryptocurrency platforms without an economic purpose; use of algorithms (or bots) that sometimes generated quadrillions of transactions and billions of dollars of artificial trading volume every day (SEC Charges Three So-Called Market Makers in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities, 2024).

The majority of criminal investigations into allegations of serious organised crime, corruption or economic crime are reactive in nature, with offences being investigated after they have been committed. Inquiries of this nature would typically entail the gathering of evidence from witnesses, the recovery of exhibits and instrumentalities, and the piecing together of documentary evidence, such as against criminal associates, a detailed 'paper trail' of financial transactions, and so forth (Deployment of special investigative means. EU and the Council of Europe's project on criminal assets recovery in Serbia, 2013, p. 9). This would be achieved through the utilisation of both open-source and personal information that is not publicly accessible. The acquisition of open-source information is accessible to any individual. It is a matter of public record and may be obtained by request, purchase or observation. This information is typically disseminated via a variety of channels, including newspapers, books, broadcasts, and general daily reports. Much of the information held by the government and many records fall into the category of open source information, and other categories of open source information relevant to corruption investigators include the following: 1) commercial data; 2) professional and academic publications; 3) media sources; 4) internet and social media; and 5) newsletters, business and technical reports. Furthermore, observations, photographs and paper publications constitute open and publicly available data. As individuals increasingly disseminate their personal information on online platforms and through social networking sites, numerous perpetrators have been convicted based on evidence they have voluntarily posted on the Internet (Goddard, 2024, p. 27).

In pursuing a case of flagrant corruption, criminal prosecution bodies may undertake a range of investigative actions, including hearing testimony from the accused, identifying and interviewing witnesses, conducting searches and seizures of relevant evidence, and ordering expert analysis and technical assistance (Alecu, 2023, p. 71). Forensic accounting is the application of accounting principles and investigative methodologies to analyse financial data with a view to identifying instances of fraud or financial misconduct. It encompasses a range of activities, including fraud examinations, asset tracing, litigation support and the provision of expert testimony. The objective of forensic auditing is to conduct a meticulous evaluation of financial records and statements with a view to identifying any discrepancies, assessing compliance with statutory norms, and providing assurance on the accuracy and reliability of financial reporting. The value of these entities lies in their capacity to identify financial irregularities, provide investigative support, and promote financial transparency and accountability (Đukić 2023, p. 408). The objective of cloud-based digital forensics is to ensure the security and credibility of digital evidence within complex cloud infrastructures. This involves

addressing concerns about data privacy and sovereignty, as well as overcoming challenges associated with virtualised storage systems and shared resources. This enables the utilisation of sophisticated cryptographic techniques, such as homomorphic encryption and multiparty computation, in conjunction with evolving technologies, including federated learning. The assurance of a secure chain of custody and the resolution of complexities associated with cloud-based data recovery, in particular, have been achieved through the assimilation of these techniques into blockchain-based cloud systems (Malik, 2024, p. 23).

The nature of secrecy inherent to corruption crimes is a determining factor in the efficacy of their investigation and the acquisition of requisite evidence through clandestine means. These are forensic technical means for the recording of extortion, delivery, receipt of a bribe, and other relevant activities, as well as the use of other forensic techniques. Covert pre-trial investigations consist of the following actions: 1) audio and video control of a person; 2) seizure of correspondence; 3) inspection and seizure of correspondence; 4) removal of information from electronic communication systems and facilities; 5) removal of information from electronic information systems, which involves searching, identifying and recording data contained in such systems or parts thereof; 6) recording and storage of information received from electronic communication networks by technical means and as a result of information search; 7) examination of information obtained with the help of technical means; 8) inspection of public places, housing or other property of a person by covertly entering them; 9) determination of the location of a radio electronic device (radio electronic means) by using technical means to obtain information from the network infrastructure or mobile terminal equipment regarding the location of the mobile terminal (point of its connection to the network), and in fixed-line networks – data on the physical address of the end node of the network, without disclosing the information; 10) visual surveillance of a person, thing or place, or surveillance using video recording, photography, special technical means to search, record and verify information about a person and his/her behaviour or those with whom he/she interacts, or certain things or places in publicly accessible places; 11) monitoring of bank accounts, search or detection of property subject to confiscation or special confiscation in anti-corruption criminal proceedings; 12) covert recording of information (content of conversations, behaviour, events, etc.) by means of audio or video recording in publicly accessible places; 13) controlled commission of a crime in the form of controlled delivery/purchase, special investigative experiments, imitation of a crime scene; 14) performance of special tasks to disclose criminal activities of an organised group or criminal organisation by a person who legally performs a special task, participates in such an organisation or confidentially co-operates with pre-trial investigation authorities; 15) use of pre-made (marked) or fake (imitated) means, specially manufactured items and documents, creation and use of specially created organisations; 16) covert obtaining of samples required for comparative analysis; 17) use of confidential co-operation to obtain information and/or involve persons in covert investigative (detective) actions (The Criminal Procedural Code of Ukraine, 2012, Art. 260-275). The acquisition of data that is not publicly accessible and which is necessary for the conduct of anti-corruption proceedings is contingent upon a court investigator's ruling.

The forensic methodology of anti-corruption investigations is now also reliant on e-government tools. Co-operation between crowdsourcing platforms (IPaidABribe) and different government institutions should facilitate the tracking of those reporting via a unique ID that allows for follow-ups and, if necessary, for the reporter to waive their anonymity and provide their name. Additionally, whistleblowing, news reporting and dissemination platforms are utilised. Blockchain has the potential to track the spending of donor money and enhance transparency and accountability in this process. It is imperative that public servants who rely on blockchain technology and all contract partners possess a comprehensive understanding of the underlying technology. Furthermore, the implementation of these systems requires a sufficient amount of local technical knowledge, particularly given the optimal hosting of projects on a local and decentralised server infrastructure (Kossow, 2018, pp. 29-31).

Covert investigative actions are technically and programmatically supported in accordance with the specific characteristics of a corruption crime, its connections to other crimes, accomplices, and so forth. In instances where institutions and norms are experiencing a crisis due to a lack of efficacy in democratic processes, the conditions are ideal for the proliferation of inequality and corruption (Alcántara, 2022, p. 12; Torre, 2022, p. 69). It is essential that the management system is aligned and capable of responding effectively across the relevant dimensions of the system. This is a matter of more than mere compliance or the legal construct of due diligence. It is not merely a matter of training and rules-based procedures. While these factors are essential, the system requires a deeper understanding and alignment (Ibbotson, 2018, p. 488).

6. Conclusions

Consequently, the overarching teleological objective of forensic science in relation to the acquisition of valid evidence is explicitly delineated within the methodology employed in the context of anti-corruption investigations. This methodology encompasses the documentation of testimonies from whistleblowers and other witnesses, statements from suspects and the accused to expose their accomplices, facts of bribery transactions, agreements on bribes, the absence of lawful sources of enrichment, facts and methods of laundering illicit funds, and the locations where such funds and other corrupt resources (services, work, bill payments, advantages during the performance of job duties, and/or any other privileges) are stored. Paper forms, in addition to audio and video recordings, have historically constituted conventional methods of documentation in the context of corruption cases. The advent of digital information formats in cyberspace has led to the emergence of innovative forensic methods. It is imperative that all evidence, where feasible, substantiates the criminal intent pertaining to bribery, money laundering, and other related offences.

The role of the auditor has evolved to encompass the analysis of documents in both paper and digital formats. The complexity of the digital path of corrupt funds is derived from the multitude of individuals involved in financial operations with these funds and the digital products used for such operations, the duration of corruption, the large volume of corrupt funds, and/or the laundering of illicit funds through cryptocurrency, corporate assets, foreign jurisdictions, offshore tax havens, and similar means. In this regard, the work of auditors is enhanced with the assistance of programmers and other requisite IT specialists. A system for monitoring the compliance of income and expenses of public officials, controlling financial transactions in the field of digital assets, tracking money laundering actions (in offshore and other foreign jurisdictions, etc.), funding of other criminal activities with these funds, and other transparency procedures (public procurement of any types of goods, services, works) can be implemented using blockchain technology. The electronic mechanism of the anti-corruption blockchain comprises a system of programs for the creation of databases and the exchange of information pertaining to the aforementioned areas of corruption risks for the benefit of the public interest. The relevant terminology and digital indicators of the material assets of potential subjects of corruption constitute the input data for this blockchain. The subsequent procedural phase in the forensic methodology of anti-corruption investigations entails the summarisation, processing and analysis of information derived from anti-corruption blockchains. This is followed by the formulation of conclusions based on these operations, which are then studied by human intelligence. This process is conducted by individuals who have received comprehensive training in the interdisciplinary subject of anti-corruption policy. The conclusions are often complicated by the synergy of dishonest actions perpetrated by corrupt individuals.

It is recommended that items related to corruption and associated crimes, along with other resources, be seized through searches conducted simultaneously at the premises of all individuals connected to the corrupt individual, whether through personal, friendly, and/or business relationships. The recovery of funds requires the prompt implementation of algorithms for identifying jurisdictional procedures and forensic examinations in criminal proceedings, namely 1) the conclusion of co-operation agreements in corruption/criminal cases between states; 2) the detailing of these agreements in the relevant agreements between criminal justice agencies (courts, prosecutors, specialised anti-corruption bodies, police, national security services, auditors, etc.); 3) approval of the documents (translation into the language of the executing state, notarisation of the translation, apostille), transfer of these documents to the executive body in the executing country; 4) control over the proper implementation of all previous stages.

The objective factors of corruption, including its latent nature and the scale of the offence, as well as the commission of the offence by a group of individuals, can all contribute to complications during the investigation of corruption offences. These characteristics and the subject of corruption are mutually reinforcing. The extent of corruption is correlated with the number of accomplices involved, the duration of the commission, and/or the resources employed in the laundering of proceeds. The legislative specification of covert investigative actions for countering corruption and related crimes, as well as the potential for corruption within investigative actions themselves, will enhance their effectiveness. A breach of confidentiality with regard to investigative actions has the effect of undermining their substantive component, and in particular their covert aspect. As the rule of law indicator declines and corruption levels rise, the probability of unauthorised disclosure of the confidentiality of investigative actions increases. The features of relevant forensic methodologies are contingent upon the specifics of both the national and/or institutional legal context, as well as the nature and/or subject of the crime, their political connotations, the public authority of the corrupt individual, scale, connections with foreign jurisdictions in public and private relations, laundering of corrupt proceeds, the use of digital technologies and cyberspace at any stage of the crime, and other elements of the

crime. Corruption deficiencies in national criminal justice agencies and/or at other institutional levels undermine national security and can only be effectively addressed with sufficient external anti-corruption support, digital technologies and artificial intelligence resources (used to automate transactions with corrupt assets in virtual form, etc.). However, before the qualitative growth of globalisation, including through the role of digital technologies in the information sphere, every nation still had a chance to overcome the destructive impact of corruption.

The significance of cyberspace for virtual assets is analogous to that of banks and treasuries for national currencies. The capacity of public institutions to eradicate corruption as a genuine threat to national security, intensified by the utilisation of cryptocurrency and other virtual assets in cyberspace, is reinforced by delineated legal measures amidst rising AI investments. The investment in AI is becoming a valuable resource for the resolution of tasks pertaining to the creation and application of law, as well as the country's armed defence and the prevention of sabotage in virtual environments and the information space. These are key elements in protecting Ukraine's national interests. The primary task of the parliament was to comprehensively regulate legal relations that people establish in cyberspace for the purpose of illicit enrichment, laundering of funds obtained through corruption or other criminal means, and the use of these funds for the exploitation and deprivation of liberty of persons ("human trafficking") for the purpose of forced labour, sexual slavery and/or commercial sexual exploitation, as well as for the financing of drug trafficking, wars, terrorism and other destructive activities, including the use of AI resources. The fundamental tenets of this legislative framework will encompass regulations pertaining to the effective governance of artificial intelligence, the circulation of cryptocurrencies and other virtual assets, the delineation of illicit actions in cyberspace, and the harmonisation of concepts delineated in existing legislative instruments pertaining to cybersecurity, state secrets protection, the quality and reliability of information in the media, national security, anti-corruption, as well as the norms of the criminal, criminal procedural, and civil procedural codes. In order to achieve this, it would be beneficial to utilise the relevant EU legislative act on AI from 2024 and China's experience in establishing a public authority responsible for AI oversight (中华人民共和国国家互联网信息办公室). The utilisation of digital tools in forensic methods to counter fraud, money laundering and corruption should be informed by relevant U.S. experience, particularly concerning the software and technical functionality of the SEC's Office of Strategic Hub for Innovation and Financial Technology, as well as co-operation among the SEC, U.S. District Court and Courts of Appeals, FBI, and U.S. Attorney's Office.

References:

Alcántara, M. (2022). Ciencia política y digitalización. *Revista Ecuatoriana de Ciencia Política.* Vol. 1. N. 1. P. 6–21. DOI: https://doi.org/10.59352/recp.v1i1.22

Alecu, G., Boloș, P. (2023). The methodology of the investigation and research of corruption crimes. *Romanian Journal of Forensic Science*. Vol. 24. Nr. 1(133). P. 67–72.

Anti-corruption strategy for 2021-2025, approved by the Law of Ukraine dated 20.06.2022. № 2322-IX. Available at: https://zakon.rada.gov.ua/laws/show/2322-20#Text

Artificial Intelligence Act: regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

Balynska, O. M., Tokarska, A. S., Yashchenko, V. A. (2017). Actual problems of the philosophy of law: manual. Lviv: LvDUVS, 612 p.

Buryachok, V. L., Kyrychok, R. V., Skladanniy, P. M. (2018). Basics of information and cybernetic security: manual. Kyiv: KU B. Hrinchenka, 320 p.

Commission Anti-Fraud Strategy Action Plan – 2023 revision: communication from the European Commission. 11.7.2023. Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-commission-anti-fraud-strategy_en

Convention on Cybercrime, adopted by the Council of Europe 23.XI.2001. ETS No. 185. Budapest. Available at: https://rm.coe.int/1680081561

The Criminal Procedural Code of Ukraine dated 04/13/2012. № 4651-VI. Available at: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n2390

Dela P. (2016). Cyberspace as the Environment Affected by Organized Crime Activity. *Connections*. Vol. 15. No. 3. P. 55–64. DOI: https://doi.org/10.11610/Connections.15.3.05

Deployment of special investigative means. EU and the Council of Europe's project on criminal assets recovery in Serbia. Strasbourg: Economic Crime Co-operation Unit. 2013. 94 p.

Đukić, T., Pavlovic, M., Grdinić, V. (2023). Uncovering Financial Fraud: The Vital Role of Forensic Accounting and Auditing in Modern Business Practice. *Economic Themes*. Vol. 61. Iss. 3. P. 407–418. DOI: https://doi.org/10.2478/ethemes-2023-0021

Goddard S., Hassan H., Kos D., Kraft O., Kupusswami R. and others (2024). Practical Guide on the Investigation of Corruption Cases. Vienna: UNODC. 107 p.

Google's AI Principles Progress Update 2023. Available at: https://ai.google/static/documents/ai-principles-2023-progress-update.pdf

GoldenJackal: New Threat Group Targeting Middle Eastern and South Asian Governments. 23.05.2023. Available at: https://thehackernews.com/2023/05/goldenjackal-new-threat-group-targeting.html

Guidelines for secure AI system development. 27.11.2023. Available at: https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

G7 Italy 2024 Foreign Ministers' Statement on Addressing Global Challenges, Fostering Partnerships. Media Note. April 19, 2024. Available at: https://www.state.gov/g7-italy-2024-foreign-ministers-statement-on-addressing-global-challenges-fostering-partnerships

Ibbotson, P. About compliance and governance: Thoughts arising from banking royal commission. *Governance Directions*. September 2018. P. 485–488.

Johar, S. S., Johar, G. S. (2017). Vol A Simple and Cogent Forensic Technique to Trap and Nab a Bribe-Seeking Corrupt Public Servant 'Blue-Handed'. *Indian Journal of Forensic Medicine and Toxicology*. Vol. 11. No 1. DOI: https://doi.org/10.5958/0973-9130.2017.00010.X

Kossow, N., Dykes, V. (2018) Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption. Bonn: Deutsche GIZ GmbH. 38 p.

Krishnaveni S., Thomas M., Mithileysh Sathiyanarayanan C., Amutha B. (2024). CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems. Vol. 27. P. 7273–7306. DOI: https://doi.org/10.1007/s10586-024-04320-x

Larsen, J. A., Wirtz, J. J. (2023). The Meaning of 'Strategic' in US National-security Policy. *Global Politics and Strategy*. Vol. 65. Iss. 5. P. 95–116. DOI: https://doi.org/10.1080/00396338.2023.2261249

Limba, T., Driaunys, K., Stankevicius, A., Andrulevicius, A. (2020). Cryptocurrency and National Security: Peculiarities of Interaction. *Transformations in Business & Economics*. Vol. 19. Iss. 2 (50). P. 138–158.

Makarenkov, O. L. (2023). Legal determination of good virtues in the image of Ukrainians as a condition for their integration into the EU. *Law and Society*. № 3. P. 40–48. DOI: https://doi.org/10.32842/2078-3736/2023.3.6

Millions Forfeited by Office of National Drug and Money Laundering Control Policy of Antigua and Barbuda. September 15, 2016. Press Releases. Available at: https://ondcp.gov.ag/millions-forfeited-by-ondcp/

Okinawa Charter on Global Information Society adopted by the Okinawa G8 Summit at Okinawa: Building a global development partnership. 22.07.2000. Available at: https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf

Oleksyuk L. (2020) Cyber security management best practices: review report. Kyiv: Parliamentary Committee on Digital Transformation. 130 p.

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018L1673&qid=

On preventing, discovering and sanctioning corruption offences: Romania Law. No. 78 of May 8th, 2000. Available at: https://www.pna.ro/legislatie.xhtml?sectiune=2&id=14&jftfdi=&jffi=legislatie

Putra Yusra M. N. B., Simon Runturambi A. J., Widiawan B. (2024). Trends and Prevention of Cryptocurrency-Based Money Laundering Crimes. *Asian Journal of Engineering, Social and Health.* Vol. 3. No. 8. P. 1751–1759. DOI: https://doi.org/10.46799/ajesh.v3i8.378

Regime do segredo de estado: Lei Orgânica n.º 2/2014. 06.08.2014. Assembleia da República Portuguesa. Available at: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2201&tabela=leis&so_miolo=

SEC Charges Three So-Called Market Makers in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities. Washington. 09.10.2024. Available at: https://www.sec.gov/newsroom/press-releases/2024-166

Serrano R., Schulz H., Rikk R., Pedak M., Jung I. and others (2018-2024) The National Cyber Security Index. Tallinn: e-Governance Academy Foundation. 45 p. Available at: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

Sobre secretos oficiales: Ley 9/1968, de 5 de abril, aprobada por las Cortes Españolas. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-1968-444

The Bletchley Declaration by Countries Attending the AI Safety Summit. 01.11.2023. Available at: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

The Interim Measures for the Management of Generative AI Services: promulgated on July 10, 2023 by the Cyberspace Administration of China and others. Available at: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

Torre, C. (2022). Liderazgo populista. *Revista Ecuatoriana de Ciencia Política*. Vol. 1. N. 1. P. 64–80. DOI: https://doi.org/10.1163/9789004679016_010

UN Convention against Transnational Organized Crime and the Protocols thereto, adopted by the UN General Assembly 15 November 2000, by resolution 55/25. Available at: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

US Strategy on Countering Corruption of December 06, 2021. Available at: https://www.state.gov/implementing-the-u-s-strategy-on-countering-corruption/

Waddell, C. (2022). Investigative and diagnostic tools for covering fraud: insights from the forensic accounting field. *International Journal of Accounting, Economics, and Finance Perspectives*. Vol. 2. № 1. P. 85–97.

Wasim Malik, A., Bhatti, D. S., Park, T.-J., Ishtiaq, H.-U., Ryou, J.-C., Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors*. Vol. 24. No. 2. P. 1–30. DOI: https://doi.org/10.3390/s24020433

Wingate G., Gray L. A., Greenberg T. S., Samuel L. M. (2009). Stolen asset recovery: a good practices guide. Washington: WB Group. 284 p.

Yaroshko, T., Kosa, V., Ignatenko, O., Makarenkov, O., Ermolayev, V. (2024). Engineering Scientific Knowledge Graphs from Publications: The Anti-Corruption Use Case. Available at: https://easychair.org/smart-program/ICTERI-2024/2024-09-26.html#talk:266254

Received on: 23th of September, 2024
Accepted on: 20th of November, 2024
Published on: 17th of December, 2024