DOI: https://doi.org/10.30525/2256-0742/2026-12-2-91-104

DETECTION OF ILLICIT CAPITAL THROUGH THE FORENSIC METHODOLOGY OF CRIMINAL CORRUPTION INVESTIGATION

Oleksii Makarenkov[1]

Abstract. The article examines the forensic methodology for identifying the capital derived from corruption-related crimes. It is noted that the essence of the methodology lies in a system of methods for recognizing reliable traces, collecting, examining, documenting, and preserving evidence of the existence of such assets in both the material and cybernetic spheres. It is established that the "methodology for identifying corruption assets" is defined through the algorithms of forensic experts and investigators with data regarding such assets, their owners, the mechanisms of their acquisition, storage, multiplication, and laundering, the results of which are transformed into evidence. This methodology intersects with the "methodology of investigating money laundering offences." It is emphasized that the personality of the corrupt actor and his accomplices is characterized by social alienation. Corrupt actors maintain special relationships with financiers (bankers, investors, insurers, brokers) and businesspersons, as well as with accountants and programmers. Taken together, analysis of these connections enables investigators to determine the places, methods, scale, and composition of misappropriated public funds, the results of their laundering and multiplication, and to identify appropriate mechanisms for their seizure and return. It is underscored that the documentation of procedural actions is accompanied by protocols (interrogations, inspections, expert examinations, audio, photo, and video recordings, etc.), inventory lists, and other annexes to the protocols of thorough searches, expert reports, procedural documents, and other materials required under criminal procedure law. A certain part of the evidentiary base for identifying and/or recovering corruption assets consists of contracts, certificates of completed work, memoranda, reports, and other officially prepared documents drafted by specialists in all jurisdictions and fields where such assets are located. The study of these documents is necessary to overcome the obfuscation created by corrupt actors. It is determined that corruption assets in cyberspace require verification of cryptocurrency wallets and electronic addresses belonging to the corrupt actor. Assets located outside the national jurisdiction in which they were obtained have a relatively high probability of being identified and/or returned only in countries intolerant of illicit proceeds and largely free from internal corruption. The article concludes that the practical measures of criminal justice authorities to identify illicit proceeds in the form of digital currencies and to trace their laundering through such currencies depend on legislative norms regulating the activities of cryptocurrency exchanges, which act as intermediaries in transactions with these assets. Financial monitoring by exchanges of the legality of the sources of funds used by participants in transactions on electronic platforms, as well as the blocking of assets belonging to corrupt actors, terrorists, war sponsors, money launderers, and other criminals, is essential. To date, the primary model for implementing such regulation remains that of the United States. It is summarized that the labor intensity, complexity, and duration of criminal procedural actions aimed at identifying corruption assets, combined with uncertainty regarding the timing of their return, underscore the importance of recording corruption assets – with varying degrees of verification, composition, nominal value, location, stage of return, and corresponding procedural documents of justice authorities – in a specialized register or in new sections of existing anti-corruption registers.

Keywords: asset, compliance, justice, cryptocurrency wallet, cryptocurrency expert, money laundering, terrorism, bank, cyberspace.

JEL Classification: K40, K42, I31, M42, M14, E22

[1] Zaporizhzhia National University, Ukraine
E-mail: almak17@ukr.net
ORCID: https://orcid.org/0000-0003-0042-165X

1. Introduction

Proceeds of crime refer to any property acquired or obtained, directly or indirectly, as a result of the commission of any offence (subpara. (e), para. 1, Art. 2, Convention 2000) by a person guided by corrupt ideals and marginalized due to the loss, absence, or distortion of legal value. The misfortune of nations lies in their unawareness of corruption-related or other criminal proceeds. However, nations also display negligence when they know of such assets but fail to confiscate them for the benefit of public finances.

We assume that the completeness and clarity of the conceptual framework of specialized legislation; the detailing and digitalization of pre-trial and judicial investigative algorithms in cases of illicit enrichment; the regulation of market operators dealing with virtual currencies; the establishment of a database on corruption-related assets; and a set of accompanying measures will enable the effective detection and confiscation of such assets, as well as prevent their legalization in both material and cybernetic environments. Addressing these tasks empowers employees of financial monitoring bodies, anti-corruption compliance specialists, criminal justice authorities, parliamentary investigative commissions, and the open civil society – where criminal proceeds are eliminated through social practices of "individuals who are better than a mere member of the community, and persons who think historically and systematically, which is superior to a human being driven by tradition, captured by it, and unable, due to the structure of memory, to transform the environment in which they find themselves into an object, to objectify it, to localize it in time, and to possess it apart from the past" (Merleau-Ponty 1976, p. 19).

In light of the continued and increasing use of stablecoins by illicit actors, similar to other virtual assets, jurisdictions should monitor market developments, assess illicit finance risks, and implement appropriate mitigation measures, including: (a) developing a regulatory framework to identify responsible entities and apply supervisory and enforcement actions as appropriate; (b) sharing good practices and remaining challenges with members of the Virtual Assets Contact Group (VACG); (c) monitoring market developments and assessing money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks, particularly with regard to large-scale thefts and money laundering through virtual assets, as well as the rise in existing and new types of fraud and scams; (d) enhancing public-private cooperation and international collaboration (FATF 2025, p. 4).

Thus, norms that delegitimize illicit assets constitute the foundational element of the methodology for detecting corruption-related proceeds. They provide the basis for the actions of criminal justice authorities, journalists, lawyers, paralegals, auditors, and other authorized asset-tracing actors. All of them require forensic and others algorithms adequate to the challenges posed by corruption and related criminal activities across all domains of legal relations. Meanwhile, the normal functioning of financial operations in cyberspace should be understood as a process of integration, whereby the text of the external material world is not copied but constituted through unique meanings, forming a unified space governed by the rule of law. Protecting legal relations in both cybernetic and physical environments require specific rules for organizing and conducting pre-trial, judicial, and other jurisdictional activities. In view of the foregoing, it is appropriate to examine the subject of this study.

2. Analysis of Recent Topical Resources

Answers to the fundamental questions concerning the nature of criminal offences can be found in the works of Merleau-Ponty M., who explored the phenomenology of perception; Passmore J. A., who examined the possibility of human improvement; M. Bergsmo and E. J. Buis, who investigated the philosophical foundations of international criminal law; Schwöbel-Patel C., who analysed the marketing of global justice; C. Santos Pereira, S. Jayantilal, S. Oliveira, L. Varregoso Mesquita, J. Vašek, and A. Arnaout, who studied compliance management. The body of knowledge on forensic methodologies for investigating corruption, terrorism, drug trafficking, money laundering, and related crimes – including those facilitated by virtual assets in cyberspace – has been enriched by the research of Nagy T., Montgomery Johnson D., Jones L., and Friedman A. T., who examined financial crime; Brun J.-P., Gray L., Scott C., and Stephenson K. M., who worked on asset recovery; Bartulovic M., Aljinovic N., and Piplica D., who explored links between corruption and money laundering; Park S., who analysed the impact of political corruption on corporate cash holdings; Ceschel F., Hinna A., and Homberg F., who studied public-sector anti-corruption strategies; Daubner L., Buhnova B., and Pitner T., who researched software systems in forensics; Agarwal U., Rishiwal V., Tanwar S., and Yadav M., who investigated blockchain and crypto-forensics; Lehka L. V., who contributed to education in quantum informatics; Samoilenko O. A., who developed methodologies for investigating crimes committed in cyberspace; Fienberg S. E., Blascovich J. J., Cacioppo J. T., Davidson R. J., and Ekman P., who studied polygraph technologies and lie detection; Jondle D., Ardichvili A., and Mitchell J., who tested models of ethical business culture; Dewey J. N. and Patel S., who examined the legal regulation of blockchain and cryptocurrencies; Gardner E. A., Warner G., Smith S., Haines N.,

Harris W., and Adams E., who researched crypto currency fraud, online drug sales, and financial crime; Lazea G.-I., Balea-Stanciu M.-R., Bunget O.-C., Sumănaru A.-D., and Coras A.-M. G., who studied cryptocurrency taxation; Lee J., Choi G., Han J., and Park J., who advanced extended wallet forensics and cryptocurrency transaction tracing; Reuter M., Bureau S., Gerges-Yammine R., Battaglia D., and Zhou J., who investigated the decoding of international stablecoin flows and the legitimisation of the destructive crypto-entrepreneur. Analyses of relevant international experiences of countries and groups of countries are presented in the works of Gorsira M., Huisman W., Denkers A., and Steg L., who studied the drivers of bribery among Dutch public officials; Yao Y. and Zhai N., who examined police investigations in China; Oteroa R. G. and Méndez Diaz R., who examined crypto-criminality in transnational organized crime and money laundering in Colombia; Gaganis C., Pasiouras F., Roubaud D., and Hollebeek L. D., who researched family firms and bribery in developing countries; Ochnio,A. H., who analysed EU anti-corruption strategies; among others. Nevertheless, a number of issues, including those addressed in the present study, have remained outside the scope of scholarly doctrine, thus underscoring the relevance of this research.

3. Differentiation of Illicit Income within the Forensic Methodology of Investigating Criminal Corruption

Highly developed states establish comprehensive legislative frameworks for defining the concept of "corruption assets" within the broader category of "illicit assets" and for detailing procedural rules governing the return of such assets to the legal domain. For example, in Ukraine, offences involving corruption-related assets fall under the following provisions: Criminal Code of Ukraine No. 2341-III of 05.04.2001 (hereinafter CCU No. 2341) and several specialized laws (Ukraine Laws 2001; 2019). Another example is Portugal's legislation on neutralizing corruption and organized economic crime: Section V "Crimes Against the State" (Arts. 308–385) of the Criminal Code of Portugal No. 48/95 of 15.03.1995; Law on Measures to Combat Organized and Financial-Economic Crime No. 5/2002 of 11.01.2002 and eleven other Portuguese laws establishing anti-corruption legal institutions (Portugal Laws 1995, 2002, 1994). Comparative legal analysis shows that the State recognizes as a crime the intentional acts of converting or transferring property, knowing that such property constitutes proceeds of crime, for the purpose of concealing or disguising its criminal origin or assisting any person involved in the commission of the predicate offence in avoiding legal consequences, as defined in subpara. (a), para. 1, Art. 17. "Property" shall mean assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets, according to subpara. (i), para. 1, Art. 2. (UN Convention 2024).

A corruption asset (hereinafter CA) refers to values which, as a result of a corruption offence, are possessed, used, and/or disposed of by a person, including any increase in such values and any documents pertaining thereto. Corruption-related proceeds fall under the legal regime established for illicit assets.

Virtual assets exist within cyberspace and exhibit an upward exponential trajectory of popularity. For example, stablecoin transactions in 2024 amounted to a total of USD 2 trillion, of which USD 633 billion occurred in North America, USD 519 billion in the Asia-Pacific region, 7.7% in Latin America and the Caribbean, and 6.7% in Africa and the Middle East (Reuter 2025). Virtual assets are widespread among corrupt actors. For instance, the High Anti-Corruption Court of Ukraine, in its ruling of 14 November 2024 in case No. 991/3227/24 (proceeding No. 42023000000001295), determined that crypto-currency, in particular Bitcoin, as a decentralized digital asset, constitutes an intangible asset and an object of civil circulation, possesses economic value and actual market worth, and is actively used for exchange into other currencies or assets, for purchasing goods, paying for services, investment, value storage, and various financial operations. It functions as a means of payment in e-commerce, tourism, financial technologies, and real estate. Across various countries, including Ukraine, there are cryptocurrency ATMs (Bitcoin-ATMs) that allow the exchange of cryptocurrency for cash, confirming its real use as a means of payment. Such ATMs operate in major Ukrainian cities, including Kyiv, Lviv, and Kharkiv.

The definition of the boundaries of cyberspace presents a problem. Formally, such boundaries are not established. They are determined through the citizenship of natural persons and the jurisdiction of incorporation of legal persons engaged in the circulation of corruption-related assets as recipients, intermediaries, beneficiaries, and other actors. In general, the investigation of money laundering is difficult due to rapid cash transactions characteristic of corruption, complex business structures, and the combination of various laundering methods. Criminal prosecution and sanctioning are further complicated by difficulties in proving the origin of property benefits in court, particularly due to cash payments that leave no tangible trace (Bartulovic 2023, p. 116).

Verification of a corruption asset (CA) occurs through measuring the non-compliance between officially declared income and actual expenditures within a single calendar year. As a unit of measurement for CA,

we propose "one average monthly gross salary (before tax), calculated on the basis of all salaries recorded by the national tax authority", denoted as x in a potential mathematical algorithm for a computer program intended to identify statistically significant CAs and the resources necessary for the successful application of investigative methods in criminal proceedings.

The rationale for this point of reference is as follows: a) at a minimum, official wages within official income are formally calculated to ensure human reproduction and development; b) any illegal income exceeding the official income by the amount of the national average monthly salary is accumulated and/or laundered, since the needs of reproduction and development have already been formally satisfied through official income. Accordingly, the CA physically exists and can be seized.

Let us assume that exceeding the value of x multiplied by six months transforms a CA into an average "statistically significant CA", denoted as y. The six-month period is conditional and may be reduced. We consider this duration sufficient for the utilisation of illicit income and/or the completion of its circulation within a laundering scheme, namely: 1) the placement of funds into bank deposits; 2) cryptocurrency transactions in cyberspace; 3) transactions with real estate, vehicles and other high-value goods; 4) receiving wages due to fictitious employment; 5) fictitious performance of works or services; 6) fictitious delivery of goods; 7) establishing an enterprise in an offshore jurisdiction and transferring illicit income to it, etc.

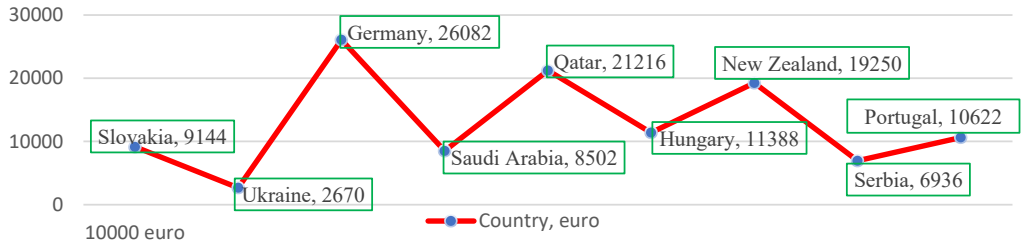
The indicator x × 6 months had the following values in 2024 for these countries (Chart 1): 1) Slovakia: 1,524 EUR × 6 = 9,144 EUR (Slovakia 2025); 2) Ukraine: 445 EUR × 6 = 2,670 EUR (Ukraine 2025); 3) Germany: 4,347 EUR × 6 = 26,082 EUR (German FSO 2025); 4) Saudi Arabia: 1,417 EUR × 6 = 8,502 EUR (Saudi Arabia 2025); 5) Qatar: 3,536 EUR × 6 = 21,216 EUR (Qatar 2025); 6) Hungary: 1,898 EUR × 6 = 11,388 EUR (Hungary 2025); 7) New Zealand: 3,225 EUR × 6 = 19,250 EUR (New Zealand 2025); 8) Serbia: 1,156 EUR × 6 = 6,936 EUR (Serbia 2025); 9) Portuguese Republic: 1,777 EUR × 6 = 10,622 EUR (Portugal 2025).

The value Y is determined in this calculation model at the level of EUR 10,000, since this amount is often subject to customs regulations and other legal requirements. For example, European countries and the United States consider this amount "statistically significant for financial monitoring" during customs control because they require travellers crossing state borders to declare cash exceeding this threshold and/or equivalent value in precious metals. Simultaneously, the determination of the social significance of calculated incomes and expenditures of corrupt actors in legal reality differs on the basis of the principle of justice. The content of this aspect of the rule of law is specified by parameters of citizens' consciousness shaped by income levels and the communicative consequences within their economic stratum of society.

The data presented in the chart indicate that in 2024 the amount of EUR 10,000 does not constitute Y for Germany, Qatar, or New Zealand. Most likely, the corrupt actor consumed the corrupt asset (CA), and therefore the task is to assess the value of the asset in order to compel offenders to return the funds to public budgets. In this context, a forensic methodology for estimating the lost corrupt asset and recording its nominal amount in the register becomes particularly relevant. The correlations of "x" with CA in Portugal and Hungary demonstrate that CA may indeed constitute Y. An even higher statistical significance of the EUR 10,000 threshold appears in the cases of Slovakia, Saudi Arabia, Serbia, and especially Ukraine.

Within civilizationally homogeneous groups of states – such as those of the EU, wider Europe, the Persian Gulf, and other economic regions – it is reasonable to average the value of Y, since these countries are integrated into shared legal, trade, financial, logistical, telecommunication, and other frameworks. This reduces the relevance of the national indicator "x" for assessing the degree of materialization of CA and increases the importance of forensic methodologies for analysing interactions among corrupt actors from different jurisdictions within the same region.

Chart. 1. **The scale of a corruption asset** that is *statistically significant for a given country*, as it becomes *noticeable* within its financial system, serves as an *indicator of the trend in the accumulation of illicit revenues in the physical and/or cyber*



4. Unified Algorithms for Forensic Detection of Corruption Assets

The criminal case files indicate that corrupt officials expected bribes to yield both material and non-material benefits; deliberately sought to reduce the likelihood of detection; perceived opportunities to engage in one or more acts of bribery and, to a lesser extent, found it difficult to refrain from bribery; did not acknowledge the gravity or moral reprehensibility of their conduct; and believed that their close colleagues accepted or engaged in similar corrupt practices (Gorsira 2021, p. 62). Proactive work by criminal justice authorities in anticipating the actions of corrupt actors and their accomplices requires them to model such actions by reading the system of property traces left by individuals, their organizations, and objects (Tab. 1).

This trace framework assists investigators in structuring information sources about the crime and focusing on missing data and criminal-procedural means of obtaining them. Databases of corruption assets are built through the analysis of information from registers of real estate, land, vehicles, securities, etc.

The subsequent determination of the nature, content, and location of illicit assets requires focusing on significant details of the perpetrator's personality, motivation, consciousness, and the modus operandi. The focus on market values over social values explains the lack of redistributive functions for global justice (Schwöbel-Patel 2021, p. 269). The probability of unethical behaviour being detected is lower in countries with low social capital, making it more likely for family firms to engage in bribe payments to reap

Table 1
Matrix of Traces of the Acquisition and Laundering of Corruption Assets

№	Indicators of Corrupt Asset	Holders / Users / Controllers	Formation Traces of the Corrupt Asset	Indicators of the Mechanism of Laundering Corrupt Assets
1.	Powers related to hiring and dismissal, financial management, determining obligations of entrepreneurs and subordinates, and other corruption-prone functions in positions funded from public budgets (Makarenkov O. 2025)	Potentially the public official receiving remuneration from a public fund, their family members, and other close associates	Formed through the use of powers and other public resources to satisfy personal interests, according to corrupt practices among colleagues and/or superiors, based on the principle "as everyone does," and regularities of legal consciousness deformation (Makarenkov 2018, p. 21)	At the stage of corruption risk manifestation, participants, assets, and other components of the laundering mechanism may be planned
2.	Non-compliance of income with expenditure	The corrupt actor, their family members, and other close persons	Purchases of real estate, land plots, vehicles, yachts, aircraft, luxury-brand watches, clothing, and footwear; payment for luxury resorts, tickets to sports events, concerts, exhibitions, and other prestigious entertainment activities; casino bets, etc.	Indicator of exponential growth in the need for laundering: excess of recorded monthly income over an amount not less than the price of 100 g of 999.9 gold (≈3.215 troy ounces). In 2025 this equals EUR 9,000–10,000 on major global exchanges in London, New York, and Shanghai. Indicator of forming or joining a criminal group for laundering: formation of social ties and distribution of roles in money-laundering procedures.
3.	Non-compliance of time with work results; falsification of authorship	Colleagues within the organization or profession across different organizations, subordinates, and persons from item 2	Material benefits obtained through exchange of services ("service for service"), work, and traces listed in item 2	
4.	Lobbying contrary to national interests, trading in influence, and other non-compliance in professional activity	Persons from items 2 and 3, and others benefiting at the expense of the public interest	Traces as in items 2 and 3	
5.	Receiving material or other benefits from representatives of foreign states (intelligence services, diplomats, etc.)	The bribed official whose remuneration is drawn from the public funds of the nation they betray		
6.	Indicators 2 and/or 3 combined with non-compliance between the professional activity and the social circle	Atypical social circle for the official's professional role, as well as persons from items 2 and 3	Participants in the official's meetings, content of their conversations, and illicit income as described in items 2 and 3	

short-term financial benefits (Gaganis 2025, p. 224). Long-standing institutional corruption in a country means that the specific offender in corruption and money-laundering cases is not unique.

Before an official notice of suspicion is served, police detectives frequently obtain evidence through the interception of telecommunications, email channels, video surveillance, and other covert investigative measures designed to collect incontrovertible evidence of criminal corruption and associated economic crime. Such evidence typically constitutes no less than one-quarter of the entire evidentiary base of a criminal case and may take months to gather, as illustrated, for example, in the film "Heat" 1995 (54–55; 1:09–1:14; 1:19; 1:19–1:21; 1:35).

Another illustration of the effectiveness of this procedural tool concerns covert investigative actions undertaken by the National Anti-Corruption Bureau of Ukraine (NABU), which, for instance, over a period of 15 months (since summer 2024) documented 1,000 hours of audio recordings of conversations among members of a high-level criminal organisation that used kickbacks and other corrupt schemes to misappropriate hundreds of millions of US dollars from the national energy sector (NABU and SAPO 2025). Another example concerns surveillance and other covert investigative actions applied by NABU between 5 March and 15 May 2023 in the case of the then President of the Supreme Court of Ukraine and his accomplices regarding a USD 2.7 million bribe (HACC 2024). Herewith the collected data often contain sensitive information, so their collection and retention may be regulated – for example, by the GDPR (Daubner 2024, p. 11; EU 2016).

Long-standing, personal, and often intense relationships frequently exist between public officials and representatives of companies that bribe them (Gorsira 2021, p. 62). In this connection, the institution of whistle-blowers is of great importance. They are crucial in exposing corruption, betrayal, and unethical practices hidden under layers of legitimacy-building strategies. Policymakers could include financial rewards, enhanced confidentiality protections, and targeted measures for high-risk industries in their frameworks, while also raising public awareness to encourage whistle-blowers (Bureau 2025, p. 13). Any confidential cooperation with individuals who interact with corrupt actors, terrorists, and other criminals – as well as with their close associates – remains traditionally important, as illustrated, for example, in "Heat" (1995) (1:17–1:18).

The first overt investigative measure after extensive covert surveillance is the execution of searches. Searches of all premises where evidence may exist are carried out simultaneously and without warning. However, in countries where public officials have not yet been "taught virtue" (Bergsmo 2018, p. 46), investigators must take into account the high risk of information leakage about forthcoming searches. Concomitantly, a merit-based recruitment system promotes effective and non-corrupt governance, as is characteristic of EU institutions" (Ceschel 2022, p. 581).

Interviews and interrogations aim to detect deception and uncover information that the deceiver does not admit openly. Polygraph examinations measure physiological reactions as indicators of deception. This is a highly valuable method in criminal investigations for identifying offenders, spies, and saboteurs in the absence of direct evidence (Fienberg 2003, pp. 11-12). "Witnesses may have experienced changes in motivation, allegiance, and/or memory since the crime occurred that make re-interviewing them a potentially fruitful avenue to solving a cold case" (Price 2025, p. 406). Four strategies for continuing after ambiguous answers from suspects include shifting the topic, initiating resolution, reframing questions, and demonstrating explicit distrust (Yao 2025, p. 493).

The practical uselessness of interrogation arises in all cases where the psychological development of the interviewee significantly exceeds the psychogram of the investigator (Makarenkov 2018, pp. 37–47). The investigator also could rely on evidence obtained with the assistance of experts and through the use of the polygraph. "The instrument measures physiological responses that are believed to be stronger during acts of deception than at other times. A deceptive response to a question causes a reaction - such as fear of detection or psychological arousal - that changes respiration rate, heart rate, blood pressure, or skin conductance relative to what they were before the question was asked and relative to what they are after comparison questions are asked. A pattern of physiological responses to questions relevant to the issue being investigated that are stronger than those responses to comparison questions indicates that the examinee may be deceptive" (Fienberg 2003, p. 13).

Forensic accounting is based on the examination of accounting documents of specific entities and types of economic operations for their compliance with legislation, for example, accounting rules in Europe, USA (EU 2023; IFRSF 2025; EFRAG 2001–2025; GlobalData 2025). Business ethics rules and other standards of corporate culture also remain important regulators of relations as a set of learned responses to various events and incentives, where "basic assumptions and beliefs that are shared by members of an organization… define in a basic 'taken-for-granted' fashion an organization's view of itself and its environment" (Jondle 2014, pp. 30, 40; McCarthy 2012, pp. 30, 120; Plato, pp. 347, 350, 358; Passmore 2000, p. 261). Criminal justice agencies investigating corruption-related and other criminal assets may expect financial experts to provide reports on suspicious patterns, anomalies, and other types of deviations of

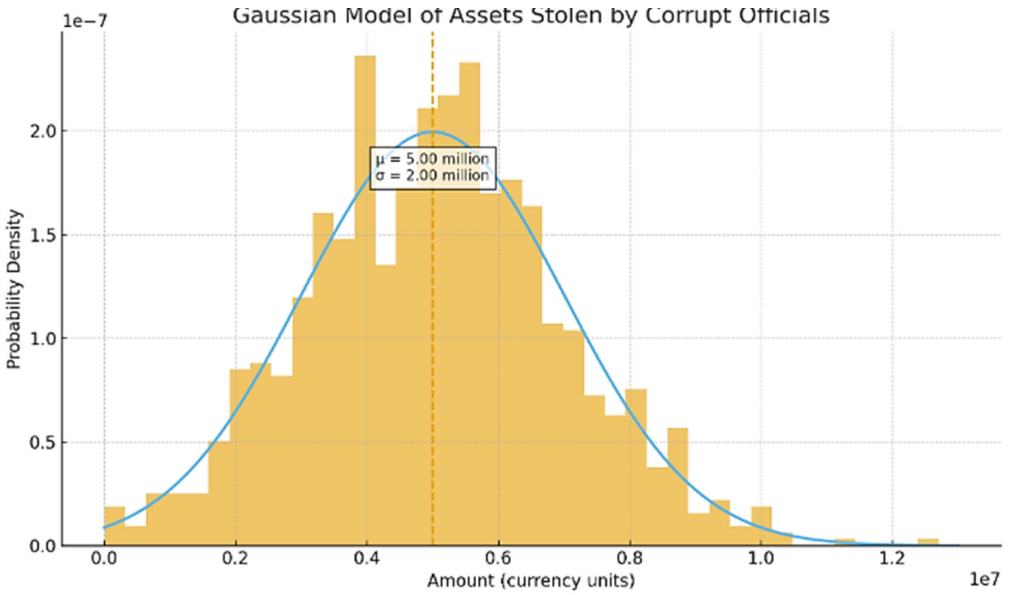


Figure 1. Normal distribution of corrupt assets

transactions from statutory and corporate accounting, managerial, and ethical standards that may evidence crimes (see Table 1).

The model assumes a mean value of corrupt assets μ = USD 5 million, a standard deviation σ = USD 2 million, and a sample size of N = 1000. The model shown in this graph demonstrates that the distribution of most corrupt assets in both material and cyber domains – as well as within those domains – corresponds to the central limit theorem of probability theory and tends toward normality according to the Gaussian distribution. Deviations may occur only in cases of small-scale or extremely large corrupt assets and/or where a corrupt actor has access to unique goods into which criminal proceeds can be converted. Another source of deviation is the non-standard, creative thinking of a corrupt actor, which may reflect an unusually high level of personal development (Galton 2018). A log-normal distribution requires the adaptation of forensic methodology to new conditions determined by the characteristics of the object and/or the subject of corruption, which helps identify corrupt assets.

The value of the forensic methodology for detecting corrupt assets lies in its timely application – before these assets are transferred abroad and/or into cyberspace. Once such transfers occur, the practical significance of the methodology shows a pronounced downward trend, as foreign jurisdictions, are generally indifferent to the interests of the state of origin of criminal assets. Such jurisdictions include offshore (the Cayman Islands, the Bahamas, Macao, among others), technological, and/or financial centers in which criminals successfully engage in obfuscation (IMF 2019). For example, Euroclear Investments S.A. settles domestic and international securities transactions for more than 90 countries, among which are EUR 198 billion in assets of the rf (Euroclear 2025).

In civil law jurisdictions or mixed systems, victims (including a state or government) may initiate criminal investigations or proceedings in a foreign jurisdiction as a civil party (Brun 2021, p. 181). For instance, participants in the corruption scheme in the "Midas" case embezzled hundreds of millions of U.S. dollars from NNEGC "Energoatom" (the operator of all nuclear power plants in Ukraine) and subsequently transferred the funds through banks into a very large number of foreign jurisdictions, thereby diluting the traces of the crime. Unfortunately, the State Financial Monitoring Service of Ukraine and the banks did not block the transfers made by the corrupt officials in this case and therefore failed to prevent these operations, as the head of the Service reported at a meeting of the Temporary Investigative Commission of the Verkhovna Rada of Ukraine on Economic Security (TICES 2025; NABU 2025).

Even this portion is returned predominantly after lengthy and costly procedures. For example, the Federal Council may freeze the assets of foreign PEPs for the purpose of confiscation if mutual legal assistance procedures fail (art. 4, Swiss Act 2015). Members of the Swiss Parliament demonstrate vigilance to the "financially influential entrepreneurs" behavior (Neuhaus 2025). Under the French model, assets may be returned through official criminal or civil judicial proceedings. However, such avenues require initiative from the requesting State. The legal basis for channeling recovered assets to countries of origin was introduced by the Programming Act of 4 August 2021 (Ochnio 2024, pp. 8–9; French laws, 2021, 2022).

Table 2
Scale of laundering of proceeds from financial, corruption-related, and other crimes in 2023, USD million
(Nagy 2024, p. 36)

#	Nomenclature of the Crime	Global Total	Total Americas	Total EMEA (Europe, the Middle East and Africa)	Total Asia-Pacific
1.	Money Laundering Aggregate Total	3,099,166	1,055,282	951,632	1,092,252
	including:				
2.	Terrorist Financing: Arms Trafficking, Foreign and Domestic Terrorism	11,472	5,106	3,701	2,665
3.	Human Trafficking: Sex Trafficking, Forced Labor	346,725	109,064	107,604	130,057
4.	Drug Trafficking	782,944	287,745	226,448	268,751
5.	Other Crimes: Other Organized Crimes, Corruption	1,958,024	653,367	613,878	690,779

The volume of illicit revenues from payments for the use of public authority in the interests of private individuals at the expense of violating public interests amounted in 2023 to USD 1,958,024 million. These funds are distributed in three roughly equal parts, each exceeding USD 600,000 million, across global regions.

The scale of financial operations and the breadth of individuals involved in committing the crimes under investigation may necessitate the appointment of a financial-economic forensic examination of the organization involved. For example, "Cryptocurrency price volatility measures the size of variations in cryptocurrency returns and should be the standard deviation of cryptocurrency logarithmic returns between their daily closing prices" (Lucey 2022, pp. 7, 1).

Experts in audio and video recordings are valuable in investigating such categories of cases, as they provide conclusions regarding the technical characteristics of recorded materials and recording devices, as well as the acoustic and linguistic parameters of the speaker. Semantic-textual (linguistic) analysis may be useful within audio and video examinations to identify hidden, ambiguous, and other meanings in recorded conversations or texts, as well as to determine the authorship of a text and its linguistic features. For instance, how this is illustrated in the investigations of robbery and kidnapping in the films "Inside Man" (2006) (50:45–52:20, 55:40–57:00) and "Taken" (2008) (44:30–45:40), respectively.

Portrait expertise enables verification of a person's identity in photographs and videos, which aids in the search for criminals, as illustrated, for example, in the investigation of high-level corruption in the film "El hombre de las mil caras" (2016), where the Director of the Spanish Civil Guard, Luis Roldán, amassed commissions intended for the renovation of Civil Guard barracks nationwide and embezzled more than 10 million euros from government secret funds. These funds were subsequently laundered through transfers between international banks (López 2023).

Thus, the examination of the subject-matter of the crime entails the sequential use of covert investigative actions, assessment of the locations where corrupt income was obtained and later legalized, searches, and expert knowledge. The interrogation of the suspected perpetrator, witnesses, and other persons is aimed at studying the offender's personality, understanding their reasoning and actions, the scope of the crime, and other facts significant for the successful investigation of the criminal case. A polygraph increases the informational value of this procedural action.

5. Features of Forensic Verification of Corruption Assets in Cyberspace

In cyberspace, forensic specialists associate participants in crimes involving corruption assets through registry data of such participants located in the physical territories of states. Crypto-assets generate risks associated with exchange operations, financial crimes, money laundering, and tax evasion (Lazea 2025, p. 26). Firms operating in more corrupt environments tend to hold less cash in order to avert political extractions (Park 2022, p. 2) and resort to cryptocurrencies to conceal capital from corrupt public authorities that extort grease payments from entrepreneurs. For instance, in the USA in 2023, 85% of the USD 4.5 billion in "investment frauds" in cyberspace involved cryptocurrency; in 2024, this share was 45.57% of USD 6.5 billion (Gardner 2025, p. 91). Herewith, experts advocate for a ban on developing superintelligence until a scientific consensus confirms that such systems can be safely developed and controlled (Butts 2025).

Taking into account the combined characteristics of cyberspace and the current version of the Convention against Transnational Organized Crime, the presence of CAs in the form of cryptocurrency constitutes a transnational offence committed by an organized group, provided that a cryptocurrency exchange is required to conduct financial monitoring of the

lawful origin of the funds used by participants in cryptocurrency transactions on its e-platform (Convention 2000; Convention on Cybercrime 2001). Cryptocurrencies constitute a system that facilitates money laundering for criminal associations worldwide and enables the commission of various punishable acts (Otero 2025, p. 1168).

The narrowing of forensic inquiry is constrained by criminals' use of blockchain technology as a distributed-ledger technology that used to record and store information on digital transactions, enables secure data exchange and transactions without the involvement of a central authority, for example in Ethereum or Bitcoin applications. In 2022, USD 8.2 trillion was transferred via the Bitcoin blockchain. Most cryptocurrency systems employ pseudonymization to obscure the link between an address and the real identity of a user. It is possible to re-identify a trader through network analysis, address clustering, and transaction-graph analysis, since all transactional data are publicly available. To safeguard traders' confidentiality, decentralized anonymous payment (DAP) systems such as Monero and ZCash have been developed, employing cryptographic methods to ensure privacy and anonymity of financial-transaction participants. The volume of money laundering conducted through decentralized payment systems reached USD 23.8 billion in 2022 – an increase of 68% compared to 2021. Several governments and exchanges have banned DAP cryptocurrencies. For example, major global economies such as Japan and South Korea have already prohibited Monero on their exchanges to combat money laundering and organized crime. Many cryptocurrency exchanges have similarly discontinued support for Monero for these reasons, including Bittrex, BitBay, and Huobi (Gao 2025, p. 2022; Lazea 2025). Accordingly, the task of justice authorities is to verify the alphanumeric identifier of the location (address), keys, volume, and other essential characteristics of cryptocurrency that constitute the "registration data of crypto-assets" belonging to the corrupt actor. Crypto-assets in cyberspace thus become a defining attribute of the notion of the "crypto-asset-enabled corrupt actor." Accountants specializing in virtual financial assets and in analyzing information contained in distributed ledgers (blockchains) are regarded as "cryptocurrency forensic auditors." A "cryptocurrency forensic programmer" is a specialist whose expertise lies in decoding and/or technically supporting the transformation of digital data.

Digital forensics may reveal confidential information by analyzing off-chain artifacts such as memory files and wallets using memory-scanning algorithms implemented, for example, in the open-source Volatility3 framework together with decryption-script sets capable of identifying data structures associated with cryptographic keys (Lee 2025; Samoilenko 2020, pp. 281, 287)).

The expert roles of programmers in criminal proceedings concerning corruption and money laundering involving cryptocurrencies – like those of auditors - consist in interpreting data encoded in binary code. Such data will become increasingly complex due to the use of symmetry, transformations, invariance, superposition, entanglement, and other principles of quantum computation. The uncertainty of the security of online transactions encoded through the binary opposition "0/1" has been observed since 1995, when Peter Shor proposed a polynomial-time quantum factoring algorithm (Lehka 2021). Computation based on such algorithms involves decomposing the numbers of cryptographic codes, using sets of factors and recurrent formulas, ultimately reproducing the number sequences of these codes – that is, decoding them.

Justice authorities are trained using textual information, which they reproduce in the material world in procedural documents. Programmers thus serve as translators of meaning – from cryptographic, interval (arithmetic), and/or optical (two- or multi-dimensional) encoding – into the meanings of the national language comprehensible to the legal decision-maker.

To obtain a unified conclusion concerning criminal assets of corrupt actors in cyberspace, it is advisable to appoint a comprehensive forensic examination, since the matter requires the combined expertise of specialists in cryptocurrencies, programming, computer hardware, and related fields. For instance, the processing of integrated information on drug trafficking and money laundering across several jurisdictions took place during Operation "White Tulip" in 2018, coordinated by Europol with the participation of the Spanish Civil Guard and the U.S. Immigration and Customs Enforcement (ICE). Finally, eleven persons were arrested in connection with drug trafficking and money laundering amounting to EUR 8,369,867, carried out through 174 current accounts, credit-card use, and cryptocurrency purchase and sale (Gill 2018).

In practice, the application of criminal-procedure law to virtual assets depends on the existence of legislative requirements governing cryptocurrency-trade relations and their administrative enforcement. At a minimum, cryptocurrency exchanges must be registered with an authorized public body, which presupposes the transparency of their statutory information, trading rules, liability, and reporting obligations, and enables the State to oversee the legality of their operations.

The absence of a public-law registry of digital currencies renders such assets invisible to justice authorities and necessitates cooperation within the sphere of private-law relations, where cryptocurrency

exchanges maintain records of digital-asset owners, of property transactions involving such assets, and other relevant registries. For example, in the United States the most significant development was the enactment of the Financial Innovation and Technology for the 21st Century Act (FIT21) in May 2024. This was the first digital-asset statute granting the Commodity Futures Trading Commission (CFTC) regulatory jurisdiction over digital commodities, while assigning to the Securities and Exchange Commission (SEC) authority over digital assets classified as securities. The Clarity Act, adopted in May 2025, granted the CFTC exclusive jurisdiction over digital-commodity spot markets, while enabling crypto platforms to register with either agency depending on whether they handle digital commodities such as Bitcoin or assets deemed securities. Simultaneously, the legislation preserves the SEC's authority to determine whether blockchain systems have achieved sufficient decentralization to qualify for CFTC oversight (Dewey 2025).

Oversight of transactions in cyberspace is possible with respect to public-oriented cryptocurrencies, which operate on blockchain types where all transactions are recorded in a publicly accessible and immutable distributed ledger. An investigator need only join the network of such an exchange in order to view and verify information on the public trading of that cryptocurrency – for instance, Bitcoin and Ethereum. By contrast, all transactions in privacy-oriented cryptocurrencies are concealed, visible only to participants, and cryptographically protected in a manner that resists tracing. Such cryptocurrencies are used by criminals for illegal transactions which, according to Chainalysis, amounted to USD 20.6 billion in 2022 (Agarwal 2024, p. 2). Cryptocurrency exchanges are therefore capable of providing valuable data to criminal-justice authorities (Lazea 2025, p. 27), since they serve as intermediaries between anonymous cryptocurrency owners and trading operations; consequently, cooperation with them is a primary objective of criminal-justice authorities, as effectively demonstrated, for example, by U.S. law-enforcement agencies.

As a result of searches conducted at locations where corrupt actors store their cryptocurrency wallets, the following are seized: (1) computers, smartphones, tablets, and similar technical devices on which software wallets in the form of applications or web browsers – such as MetaMask, Trust Wallet, Exodus, and others – are installed (see Images 1-3); (2) paper wallets in the form of printouts of public and private keys; and (3) USB-like physical devices and/or other types of hardware wallets, referred to as "cold wallets" because of their infrequent connection to the Internet (see Images 4-6).

In cases involving hardware and/or software cryptocurrency wallets, investigators must also seize paper (notebooks, journals, etc.) and/or other media containing records of seed phrases – the master key consisting of unique sequences of 12–24 words used to access private keys and cryptocurrency assets.

It is advisable to document crypto-assets stored in a corrupt official's software wallets remotely, within the framework of covert investigative actions. Access to a computer, smartphone, tablet, or similar device containing the wallet software is carried out via the Internet, including through malware previously implanted on such a device. Because registration data for crypto-assets may potentially be accessed online, such wallets are referred to as "hot cryptocurrency wallets." Both methods require the involvement of domain specialists and must remain within the scope of covert investigative measures authorized by an investigative judge for the collection of physical evidence of the existence of corruption assets in cyberspace.

Investigators and forensic experts require data guides and glossaries explaining the content of data and events recorded by software systems, their format, extraction in a form suitable for shared use, auditability, and other structurally organized data properties enabling their processing. The standardization, approval, and certification of these forensic tools ensure the evidentiary reliability of the results obtained in court. To this end, documentation from software developers is required regarding the system's capabilities, limitations, rules of use, maintenance, operational modes and configurations, and the categories of persons authorized to access it and their rights. Information concerning all assets – such as forensic devices, servers, and applications, including persons, specifications, and locations – is crucial (Daubner 2024, p. 13).

Image 1. MetaMask Wallet

Image 2. Trust Wallet

Image 3. Exodus Wallet

Images 1–3. Examples of visual indicators showing the presence of software cryptocurrency wallets on a computer, smartphone, or other similar device (MetaMask, Trust, Exodus, 2025)

Image. 1. SafePal S1

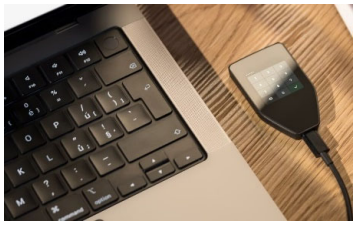


Image. 2. Trezor Safe 5

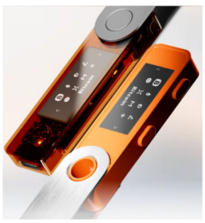


Image. 3. Classic Ledger Nano signers

Images 4–6. Examples of the appearance of hardware cryptocurrency wallets (SafePal, Trezor, Ledger 2025)

6. Conclusions

The essence of forensic methodology for identifying corruption assets consists of a system of methods for recognizing reliable traces (material and digital), collecting, examining, documenting, and preserving evidence of such assets in both the material and cybernetic domains. These methods comprise algorithms of forensic experts and investigators with data concerning such assets, their owners, mechanisms of acquisition, storage, multiplication, and laundering, the results of which are transformed into evidence in corruption and related criminal cases. In this regard, the technique intersects with the "methodology for investigating money-laundering crimes," the degree of overlap increasing with the scale of corruption assets, which makes them more visible and less acceptable to jurisdictions where they are placed.

The personality of corruptionist is characterized by their alienation from society and affiliation with a social stratum of similar actors. Their connections with networks of facilitators contain traces of transformation, jurisdictional placement (domestic or foreign), and the material or cybernetic locations of illegal proceeds. Corrupt actors maintain distinct relationships with financiers (bankers, investors, insurers, brokers) and entrepreneurs, as well as with accountants and programmers. Collectively, analyzing these connections allows investigators to determine the locations, methods, scale, and composition of stolen public resources, the results of their laundering and reinforcement, and to identify appropriate mechanisms for their seizure and return.

Documentation of procedural actions is accompanied by protocols (interrogations, inspections, examinations, audio, photo, and video recordings, etc.), inventory lists and other attachments to the protocol of meticulous searches, expert opinions, procedural documents, and all other items required by criminal procedure law. A specific part of the evidentiary base for identifying and/or returning corruption assets consists of contracts, certificates of work performed, memoranda, reports, and other formally documented outputs produced by specialists. Examination of these documents, as well as of cryptocurrency transaction traces, is essential for overcoming the obfuscation created by corrupt actors. Assets held outside the national jurisdiction in which they were generated have a relatively high likelihood of being detected and/or returned only in nations intolerant of illicit proceeds and largely free from internal corruption. In light of this the axiological dimension of legal tradition remains foundational for all actions.

The practical measures of criminal justice authorities for detecting illegal income in the form of digital currencies and for tracing its laundering through such currencies depend on legislative rules governing the operation of cryptocurrency exchanges serving as intermediaries for transactions involving these assets. Foundational are definitional norms that convey unambiguous meanings of phenomena related to the cyber-circulation of illicit assets. Among these are the addresses and keys of virtual assets, designated here as "registration data of crypto-assets"; corruption assets in cyberspace, which give rise to the concept of a " crypto-active corrupt actor"; and other criminal-law concepts within this regulatory system.

Preventing the generation of illicit proceeds in cyberspace depends on ensuring compliance of cryptocurrency exchanges with legal regulations on cryptocurrencies. This includes, among other things, financial monitoring by exchanges of the legality of the sources of funds used by transaction participants on the e-platform, as well as blocking the assets of corrupt actors, terrorists, war sponsors, money launderers, and other criminals. To date, the USA – represented by the SEC and CFTC, the Office of Foreign Assets Control of the Department of the Treasury, Department of Justice, and the courts – remains the principal model for implementing such regulation.

The labor intensity, complexity, and duration of criminal procedure actions for identifying corruption assets, combined with uncertainty regarding the timeframes for their return, underscore the importance of recording CAs with varying levels of verification, composition, nominal value, location, stage of return, and relevant procedural documents of justice authorities in a specialized register or in new fields of existing anti-corruption registers. The sources for populating this register include: 1) results of administrative procedures detecting non-compliance

between income and expenditures of public officials; 2) objects of criminal corruption and money laundering, including through sham commercial transactions, fictitious employment, purchases and sales of cryptocurrencies, and similar schemes, documented in: a) pre-trial investigation materials; b) judicial proceedings; c) final court decisions.

Such a digital solution forms the basis of a database for justice authorities, enabling the proper accounting of corruption assets, coordination, sequencing, and other elements of managerial and jurisdictional activities of authorized public authorities, as well as oversight by representatives of open civil society.

A socially significant area of further research includes the methodology for returning corruption assets; identifying CA through exchanges of services and/or work ("service for service"), falsification of authorship of work for personal gain in positions funded by public resources, and detecting corruption lobbying. Educational games illustrating the "consequences of public funds theft" and the "achievements in countering corruption" may serve to enhance public awareness.

References:

A bruttó átlagkereset 727700 forint volt, 11,0%-kal meghaladta az egy évvel korábbit. Központi Statisztikai Hivatal [The average gross salary was HUF 727,700, ... Central Statistical Office]. Hungary. 25/02/2025. Available at: https://www.ksh.hu/gyorstajekoztatok/ker/ker2412.html

Adopting certain international accounting standards in accordance with Regulation (EC) No 1606/2002 of the EU Parliament and of the Council: EU Commission regulation 2023/1803 of 13/08/2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1803

Agarwal, U., Rishiwal, V., Tanwar, S., Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *Int. J. Network Mgmt*. Vol. 34. Iss. 2. P. 1-32. DOI: https://doi.org/10.1002/nem.2255

متوسط الشهرية في المملكة العربية السعودية [Average monthly salaries in Saudi Arabia]. Trading Economics. April 2025. Available at: https://ar.tradingeconomics.com/saudi-arabia/wages

Bartulovic, M., Aljinovic, N., Piplica, D. (2023). Determining the Relationship Between Corruption and Money Laundering. *Montenegrin Journal of Economics*. Vol. 19. No. 2. P. 109-118. DOI: https://doi.org/10.14254/1800-5845/2023.19-2.9

Brun, J.-P., Gray, L., Scott, C., Stephenson, K. M. (2021). Asset Recovery Handbook A Guide for Practitioners. Washington: World Bank. 403 p.

Bureau, S., Gerges-Yammine, R., Battaglia, D., Zhou, J. (2025). Legitimising destructive entrepreneurship: the case of a crypto-entrepreneur. *Small Business Economics*. P. 1-15. DOI: https://doi.org/10.1007/s11187-025-01093-4

Butts, D. Hundreds of public figures, including Apple co-founder Steve Wozniak and Virgin's Richard Branson urge AI 'superintelligence' ban. CNBC. Oct. 22, 2025. Available at: https://www.cnbc.com/2025/10/22/800-petition-signatures-apple-steve-wozniak-and-virgin-richard-branson-superintelligence-race.html

Ceschel, F., Hinna, A., Homberg, F. (2022). Public Sector Strategies in Curbing Corruption: A Review of the Literature. *Public Organization Review*. Vol. 22. P. 571–591. DOI: https://doi.org/10.1007/s11115-022-00639-4

Classic Ledger Nano signers. 2025. Available at: https://shop.ledger.com/pages/classic-ledger-nano-signers#why-ledger

Daubner, L., Buhnova, B., Pitner, T. (2024). Forensic experts' view of forensic-ready software systems: A qualitative study. *J. Softw. Evol. Proc*. Vol. 36. Iss. 5. P. 1-23. DOI: https://doi.org/10.1002/smr.2598

De programmation relative au developpement solidaire et a la lutte contre les inegalites mondiales: Loi n° 2021–1031 L'Assemblée nationale et le Sénat. Adopté du 4 août 2021. Available at: www.legifrance.gouv.fr/jorf/id/JORFTEXT000043898536

Dewey, J. N., Patel, S. Blockchain & Cryptocurrency Laws and Regulations 2026 – USA. 21/10/2025. Available at: www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/usa/

EFRAG's Commitment to Rigorous Due Process in Reporting. 2025. Available at: https://www.efrag.org/en/open-consultations

Euroclear Investments S.A. as a global provider of Financial Market Infrastructure services. 2025. Available at: https://www.euroclear.com/en.html

FATF (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets. Paris: FATF. 32 p.

Fienberg, S. E., Blascovich, J. J., Cacioppo, J. T., Davidson, R. J., Ekman, P. others (2003). The Polygraph and Lie Detection. Washington, DC: The National Academies Press. DOI: https://doi.org/10.17226/10420

Gaganis, C., Pasiouras, F., Roubaud, D., Hollebeek, L. D. (2025). Family Firms and Bribe Payments in Developing Countries: The Moderating Role of Social Capital. *Journal of Business Ethics*. Vol. 202. P. 221-242. DOI: https://doi.org/10.1007/s10551-025-05950-w

Gao, R., Wan, Z., Wang, H., Luo, S. (2025). Invisible Warning Line: Efficient and Generic Regulation for Anonymous Cryptocurrencies. *IEEE Transactions on Dependable and Secure Computing*. Vol. 22. P. 2022-2036. DOI: https://doi.org/10.1109/TDSC.2024.3475391

Galton Board and the Normal Distribution. 2018. Available at: https://www.youtube.com/watch?v=AwEaHCjgeXk

Gardner, E. A., Warner, G., Smith, S., Haines, N., Harris, W., Adams, E. (2025). Revealing the Web of Connections: Crypto Scams, Online Drug Sales, and Financial Crimes. *Forensic Science Review*. Vol. 37. № 2. P. 88-95

Gill, S. Narco cryptocurrency laundering network busted in Spain. Colombia Reports. 09/04/2018. Available at: https://colombiareports.com/narco-cryptocurrency-laundering-network-busted-in-spain/

GlobalData Plc. One connected platform of intelligence and the insights for act with conviction. 2025. Available at: https://www.globaldata.com/

Gorsira, M., Huisman, W., Denkers, A., Steg, L. (2021). Why Dutch officials take bribes: a toxic mix of factors. *Crime, Law and Social Change*. Vol. 75. P. 45-72. DOI: https://doi.org/10.1007/s10611-020-09919-w

IMF Staff Assessments on Offshore Financial Centers (OFCs). 03/10/2019. Available at: https://www.imf.org/en/publications/ofca-by-jurisdiction

Jondle, D., Ardichvili, A., Mitchell, J. (2014). Modeling Ethical Business Culture: Development of the Ethical Business Culture Survey and Its Use to Validate the CEBC Model of Ethical Business Culture January. *Journal of Business Ethics*. Vol. 119. No. 1. P. 29-43. DOI: https://doi.org/10.1007/s10551-012-1601-2

Labour market statistics: December 2024. 05/02/2025. Statistics New Zealand / Tatauranga Aotearoa. Available at: https://www.stats.govt.nz/information-releases/labour-market-statistics-december-2024-quarter/

Lazea, G.-I., Balea-Stanciu, M.-R., Bunget, O.-C., Sumănaru, A.-D., Coras, A.-M. G. (2025). Cryptocurrency Taxation: A Bibliometric Analysis and Emerging Trends. *International Journal of Financial Studies*. Vol. 13(1). P. 1-37. DOI: https://doi.org/10.3390/ijfs13010037

Lee, J., Choi, G., Han, J., Park, J. (2025). Advanced Monero wallet forensics: Demystifying off-chain artifacts to trace privacy-preserving cryptocurrency transactions. *Forensic Science International: Digital Investigation*. Vol. 54. P. 1-10. DOI: https://doi.org/10.1016/j.fsidi.2025.301988

Lehka, L. V. (2021) Methodology for teaching the basics of quantum informatics to high school students. PhD dis. in specialty 014 - Secondary Education (Informatics) 01 – Education/Pedagogy. Kryvorizkyy SPU. Kryvyi Rih. 269 p.

López Canales D. La muerte final del espía Francisco Paesa [The final death of spy Francisco Paesa]. July 31, 2023. elDiario.es. Available at: https://www.eldiario.es/politica/muerte_1_10421353.html

Lucey, B. M., Vigne, S. A., Yarovaya, L., Wang, Y. (2022). The cryptocurrency uncertainty index. *Finance Research Letters*. Vol. 45. P. 1-8. DOI: https://doi.org/10.1016/j.frl.2021.102147

Makarenkov, O. (2025) Data protection and security compliance. Chapter 9. Compliance Management. Interactive Coursebook. C. Santos Pereira, S. Jayantilal, S. Oliveira, J. Vašek, A. Arnaout, others. Praha: Future Books, spol. s r.o. ISBN 978-80-909429-2-9. Available at: https://vscht.futurebooks.cz/detail-knihy/85-compliance-management

Makarenkov, O. L. (2018). Legal Deontology: teaching and learning manual. Zaporizhzhia: ZNU, 106 p.

Marsh McLennan as risk and development manager of the companies and the communities. 2025. Available at: https://www.marsh.com/en/home.html

McCarthy, Q. (2012) Police Leadership A Primer for the Individual and the Organization. London: Palgrave Macmillan. VIII, 211 p. DOI: https://doi.org/10.1057/9781137005939

Medidas de combate à corrupção e criminalidade económica e financeira: Lei da República Portuguesa n.º 36/94, de 29 de setembro de 1994. Diário da República n.º 226/1994. Série I-A de 1994-09-29. P. 5908–5910.

Medidas de combate à criminalidade organizada e económico-financeira: Lei da República Portuguesa n.º 5/2002, de 11 de janeiro de 2002. Diário da República n.º 9/2002. Série I-A de 2002-01-11. P. 204–207.

Merleau-Ponty, M. (1976) Phénoménologie de la perception. Paris: Éditions Gallimard. P. X (540).

Nagy, T., Montgomery Johnson, D., Jones, L., Friedman, A. T. (2024) Global Financial Crime Report 2024. Insights at the Intersection of Financial Crime Data & Real Survivor Stories. Celent & Oliver Wyman. New York: Nasdaq, Inc. 40 p.

Neuhaus, C. Hat die Schweiz Trump bestochen? Grüne und Juso zeigen die sechs Unternehmer [Milliardäre] an, die ihn im Oval Office besucht haben. 27.11.2025. Neue Zürcher Zeitung AG. Available at: https://www.nzz.ch/schweiz/ld.1913913

Ochnio, A. H. (2024). Recent developments in EU anti-corruption strategy: the missing element of the return of corrupt assets to "victim countries". *Journal of Money Laundering Control*. Vol. 27. No. 7. P. 1-12. DOI: https://doi.org/10.1108/JMLC-11-2023-0176

O Código Penal da República Portuguesa: Decreto-Lei n.º 48/95, de 15 de março de 1995. Diário da República n.º 63/1995. Série I-A. 15/03/1995. P. 1350-1416.

On the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons: Federal Act (Foreign Illicit Assets Act, FIAA) adopted by The Federal Assembly of the Swiss Confederation. 18/12/2015. Available at: https://www.fedlex.admin.ch/eli/cc/2016/322/en

On the protection of natural persons with regard to the processing of personal data and on the free movement of such data: regulation (EU) 2016/679. EU Parliament, Council. 27/04/2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Operation Midas: High-level criminal organization operating in the energy sector exposed. NABU. 11/11/2025. Available at: https://nabu.gov.ua/news

Operation to expose corruption in the energy sector. NABU and SAP. 10/11/2025. Available at: https://www.youtube.com/watch?v=ZWbUQcpHn5k

Oteroa, R. G., Méndez Diaz, R. (2025). Crypto crime: Approaches from transnational crime and money laundering in Colombia. *Procedia Computer Science*. Vol. 257. P. 1166–1171.

Our purpose. Trust. 2025. Available at: https://trustwallet.com/about-us

Park, S. (2022). Liquid asset sheltering, or cost of capital? The effect of political corruption on corporate cash holdings. *Inter. Rev. of Financial Analysis*. Vol. 82. P. 1-15. DOI: https://doi.org/10.1016/j.irfa.2022.102146

Passmore, J. A. (2000) The perfectibility of man. Indianapolis: Liberty Fund, Inc. 548 p.

متوسط الرواتب في قطر 2025 [Per capita income and average salaries in Qatar 2025]. 08/01/2025. Available at: https://msheireb.co/4ml

Philosophical Foundations of International Criminal Law. M. Bergsmo, E. J. Buis eds. Brussels: Torkel Opsahl Academic EPublisher. 2018. 772 p.

Plato. The Republic. Translated from the Greek by Prof. Benjamin Jowett. Gutenberg Free eBooks Project. Ed. 2021. 484 p. Available at: https://www.sciencetheearth.com/uploads/2/4/6/5/24658156/plato_-_the_republic.pdf

Presse1 % der Vollzeitbeschäftigten verdiente im Jahr 2024 mehr als 213 286 Euro brutto. Pressemitteilung Nr.134. 08/04/2025. German FSO. Available at: www.destatis.de/DE/Presse/Pressemitteilungen/2025/04/PD25_134_621

Priemerný nominálny mesačný plat (hrubá mzda) na Slovensku v roku 2024. Štatistický úrad SR [Average nominal monthly salary (gross wage) in Slovakia in 2024]. 03/03/2025. Available at: https://slovak.statistics.sk/

Prosečne mesečne zarade za godinu. Republički zavod za statistiku [Average monthly earnings for the year. Republic Institute of Statistics]. 25/02/2025. Republic of Serbia. Available at: https://data.stat.gov.rs/Home/Result/2403040401

Remuneração bruta mensal média por trabalhador. Estatísticas do Emprego. O Instituto Nacional de Estatística, instituto público [Average gross monthly remuneration per employee]. Portuguese Republic. 14/02/2025. Available at: www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=695021120&DESTAQUESmodo=2

Relative au mecanisme de restitution des biens mal acquis: Circulaire n° 6379/SG La Première Ministre a approuvé du 22 novembre 2022. Available at: https://www.legifrance.gouv.fr/circulaire/id/45384?origin=list

Reuter, M. (2025) Decrypting Crypto: How to Estimate International Stablecoin Flows. WP/25/141. IMF. 55 p.

Rozbir MindichHeytu v Radi. Pryyshly NABU, SAP, Uryad, Henprokuratura [MindichGate investigation in the Rada. NABU, SAPO, Government, Prosecutor General's Office came]. 17/11/2025. Available at: https://www.youtube.com/live/Jk_nqJRau-g?t=15076s

SafePal S1 Hardware Wallet. 2025. Available at: https://www.safepal.com/pt/store/s1

Samoilenko, O. A. (2020) Fundamentals of the methodology for investigating crimes committed in cyberspace: monograph. Odesa: TES. 372 p.

SatoshiLabs as operator of the Trezor Cryptocurrency hardware wallet. 2025. Available at: https://trezor.io/trezor-safe-5

Average monthly wages by types of economic activity for the period from the beginning of 2024. Ukraine. 25/02/2025. Available at: ukrstat.gov.ua/operativ/operativ2005/gdn/Zarp_ek_p/Zp_ek_p_u/arh_zpp_u.htm

Schwöbel-Patel, C. (2021) Marketing Global Justice. The Political Economy of International Criminal Law. Cambridge: University press. 316 p. DOI: https://doi.org/10.1017/9781108697651.010

The Convention on Cybercrime: Council of Europe. 23/11/2001. ETS No. 185. Budapest. Entry in force 01/07/2004. Available at: https://rm.coe.int/1680081561

The Goal at Exodus. 2025. Available at: https://www.exodus.com/about

The IFRS Foundation. 2025. Available at: https://www.ifrs.org/issued-standards/list-of-standards/

The MetaMask wallet. 2025. Available at: https://metamask.io

UN Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes: Resolution 79/243 of the UN GA. 24/12/2024. Available at: www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

UN Convention against Transnational Organized Crime and the Protocols thereto: adopted by the UN General Assembly resolution 55/25. 15/11/2000 (entry into force: 29/09/2003). Available at: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

In May 2023, NABU detectives exposed Knyazev in receiving a $2.7 million bribe. 12/12/2024. Available at: https://hacc-decided.ti-ukraine.org/uk/cases/52023000000000202

Yao, Y., Zhai, N. (2025). Police officers' management of suspects' I don't know responses in Chinese investigative interviews. *Discourse Studies*. Vol. 27(3). P. 477–497. DOI: https://doi.org/10.1177/14614456241285899

Received on: 23th of December, 2025
Accepted on: 06th of March, 2026
Published on: 10th of April, 2026