O. L. MAKARENKOV

THE TERNARY LEGAL COMPOSITION OF NATIONAL SECURITY PROTECTION AGAINST CORRUPTION DISTORTIONS

DIE TERNÄRE RECHTLICHE ZUSAMMENSETZUNG DES SCHUTZES DER NATIONALEN SICHERHEIT VOR KORRUPTIONSVERZERRUNGEN

A COMPOSIÇÃO JURÍDICA TERNÁRIA DA PROTEÇÃO DA SEGURANÇA NACIONAL CONTRA AS DISTORÇÕES DA CORRUPÇÃO

ترکیب حقوقی سه‌گانه حفاظت از امنیت ملی در برابر انحرافات فساد

Scientific monograph

IZDEVNIECĪBA BALTIJA PUBLISHING

2025

UDC 328.185
Ma312

Reviewers:

Prof. Dr. Dr. h.c. **Bernd Heinrich,** Eberhard-Karls-University Tübingen Faculty of Law Vice Dean for International Relations and Priorities Chair of Criminal Law, Criminal Procedure Law and Copyright Law (Tübingen, Bundesrepublik Deutschland);

Dr. **Jovana Banović**, Assistant Professor at the Department of Crime Studies, Faculty of Security Studies, University of Belgrade (Београд, Република Србија)

Dr. **Peter Mészáros**, Department of Civil and Commercial Law, Faculty of Law, University of Trnava (Trnava, Slovenská republika);

Dr. **Gabor Andrasi,** PhD in legal ethics education, Nottingham Trent University (UK), Associate Professor and Director of International Affairs at Budapest University of Economics and Business (Budapest, Magyarország)

Approved for publishing by the Scientific Council of Portucalense Legal Institute (Protocol of 26.02.2025)

The Ternary Legal Composition of National Security Protection Against Corruption Distortions : Scientific monograph / O. L. Makarenkov. Riga, Latvia : Baltija Publishing, 2025. 162 p.

ISBN 978-9934-26-528-0

DOI: https://doi.org/10.30525/978-9934-26-528-0

The monograph is of interest to lawyers, politicians, economists, managers, and developers of digital software aimed at protecting public funds from embezzlement by entrepreneurs and public officials, their organized criminal groups, and the criminality determined by these offenses at both national and international levels. This includes eliminating money laundering, fraud, extortion against employees by employers, unfair competition in the labor market, betrayal of constitutional values, terrorism, and external military aggression, and other crimes that pose a critical threat to national security.

Cover photo by O. L. Makarenkov.

CONTENT

INTRODUCTION

Today, progressive transformations in law and governance practices are carried out according to the best standards demonstrated by highly developed countries. For example, the EU is one of the most important priorities for the development of Ukraine and other countries that aspire to grow alongside major players – mit Kleinen tut man kleine Taten, mit Großen wird der Kleine groß (Goethe, 1790, p. 239). The level of civilization in a society is determined by the degree to which human virtues are revealed – eine Assoziation, worin die freie Entwicklung eines jeden die Bedingung für die freie Entwicklung aller ist (Marx, Engels, 1848, p. 482). A society unites into a nation if its common goal is achieved through the good qualities of its members, thereby excluding corruption, bribery, bureaucratic inefficiency, non-transparency, and the lack of real public control over budget expenditures. Such nations form alliances, like the EU, which at their advanced level of development face unprecedented challenges to their integrity, such as Dalligate (Cini, 2024, p. 562–570) and Qatargate (Chagnon, 2024).

Corruption negatively affects the realization of constitutionally guaranteed human rights and freedoms and, consequently, the economic state of society and the well-being of its citizens (Zhovnirchyk, 2017, p. 103), as well as its security against external military threats. For instance, a country's intention to integrate into the EU is documented in numerous legal instruments. This intention is supported by statements from public officials but is concretized to varying degrees through the actions of individual citizens. The success of this endeavor correlates with the sincerity and other virtues of the people. According to established practices and formal legal requirements, decisions are made by majority rule, meaning that a significant portion of citizens must be knowledgeable about social development issues, such as digitalized mechanisms for the protection of consumer rights (including socially vulnerable groups), which would stimulate entrepreneurship in Europe and enhance the EU's competitiveness. Moreover, citizens must be convinced of the progressiveness of the public authority's chosen course of action in areas such as taxation, public procurement,

banking, and migration. This kind of communication with the population enables the constructive mobilization of civic engagement toward implementing legal standards from the most effective European nations and the Western cultural tradition as a whole. Within these standards, key elements include politically, economically, and culturally mediated mechanisms of at least a bicultural legal system (Inghilleri, 1999, p. 126). The choice, preservation, and development of exclusively virtuous qualities derived from human nature determine the success that individuals seek to achieve within legal relations.

The EU is associated with economic and other benefits that citizens from less economically developed nations seek to access, typically on a parity basis. However, not everyone, and certainly not the majority, fully understands and/or demonstrates the psychological capacity to act in a way that reveals their virtues and adheres to them for as long as necessary to sustain and develop these benefits. In these interactions, desires often dominate over sufficient and adequate efforts. These efforts are virtuous when they result from the manifestation of individual virtues in their dynamic development. Social reality demonstrates corrupt distortions that weaken development and/or lead to the collapse of national security and the security of national alliances. A specific example of high-corruption countries is tax evasion through the practice known as “envelope wages,” which consists of unregistered cash payments supplementing official salaries. These and other forms of income underreporting are widespread phenomena documented in various countries, including former Soviet states, as well as the Baltic countries, Hungary, Turkey, Argentina, the self-employment sector in the United States, and others (Gavoille, p. 1). This trend of informal employment and/or the formal-legal representation of lower-than-actual wages in accounting records is persistent in underdeveloped and/or transitional economies.

Development and security are always collective national achievements, reflected in the accumulation of financial resources, their legally balanced expenditure, and other public-legal phenomena. Developing anything complex always takes a long

time, even if there are leap-like stages. Moreover, all dimensions of development are ontologically long-term, as evidenced by the complex evolutionary processes of the astronomical, physical, biological, and even anthropogenic worlds. Violating the laws of any of these inevitably leads to collapse and the inertia of destruction, which simultaneously generates the energy for creating something new that negates the previous nature of its existence, such as national sovereignty or EU sovereignty.

To protect themselves from corruption-related losses, European and other nations must harness the energies of modern development trends, particularly the resources of neural networks. The dissemination of information in digital format is a long-standing upward trend growing exponentially. Its traditional domains remain finance, international transactions, stock trading, and similar sectors. Corrupt or other illicit revenues are always present in these fields, either as unlawfully acquired material assets through smuggling, insurance fraud, pawnshop operations, payment system abuse, fictitious transaction schemes, banking services exploitation, or virtual assets, as well as through attempts to legitimize them (German: Unrecht Gut gedeiht nicht). Digital technologies and the cyberspace they create serve as tools and environments for money laundering. Tracking, proving, and/or recovering illicit material assets in the physical world presents a serious challenge to justice authorities, one that only select institutions can tackle successfully through international cooperation and by enhancing their forensic capabilities with digital tools that "address the shortcomings of a legal system that lacks sufficient resources for the volume of cases" related to the de-legalization of corrupt proceeds and the financing of terrorism (Sudeall, p. 122, 123). The success of investigations into corruption, money laundering, and most financial crimes largely depends on the ability of criminal investigators to trace the ownership trail of money and other assets. Information and Communication Technology (ICT) plays a decisive role in the criminalization, detection, investigation, and prosecution of corruption, money laundering, and other financial crimes, as well as in compiling and analyzing large volumes of data (Pieth, p. 19, 21).

The key methodological approach for studying the aforementioned issues at the level of their formulation is dialectical logic. The author's hypotheses are as follows: corruption that has destroyed national security is overcome through a system of national, international, and digital legal means. The national level of anti-corruption policy is represented by compositions of public law (constitutional, criminal, administrative, financial, labor) and private law (civil, commercial, family). Anti-corruption policy is enriched through processes of scientific justification of legal norms, lawmaking, and law enforcement (both public and private). The binary contradictions of anti-corruption policy are resolved by components outside such contradictions.

The *purpose* of this study is to explore the ternary legal composition of national security protection against corruption-related distortions. It aims to assess the capabilities of legal and digital tools in resolving binary contradictions of conceptual oppositions within legal relations-such as human virtues and vices, integrity and corruption, honesty and deception, and others. The research objectives are reflected in the titles of the chapters of this work.

The issue raised in this study has been examined by legal scholars within various branches of legal science, as well as by specialists in programming, economics, management, and related disciplines, both in national and foreign scientific doctrines. M. R. Andriyts investigated legal principles in the decisions of the Constitutional Court of Ukraine; O. V. Anisimov studied the constitutional foundations of judicial discretion as guarantees of the independence and effectiveness of the judiciary; L. L. Bogachova examined the principle of legal certainty in European and national law; L. I. Zamorska, Yu. M. Oborotov analyzed the formal (positively empirical) aspect of normativity, its essential properties, and institutionalization in Ukraine; O. V. Lemak researched legal certainty in the context of the right to judicial protection; P. A. Komar explored the role of judicial lawmaking in establishing the rule of law principle; O. M. Kudryavtseva examined legal certainty in the decisions of the Constitutional Court of Ukraine;

V. O. Pankratova, V. S. Smorodinsky studied the general theoretical aspect of the principle of legal certainty.

Borovyk A. V., Popyk A. V., Magnovskyi I. Y., Demianchuk V. A., Bielkina D. S., Melnyk O. M., Mykulets V. Yu., Pavelkiv S. R., Shcherbakov V. V., Tomchuk A. V., Derevianko N. Z., and Trofimchuk Yu. O. researched the administrative-legal foundations for the implementation of personnel policy in Ukraine's judiciary system. Karkovska V. Ya. studied the formation of mechanisms for personnel security in public authorities under institutional development conditions. J. Bertók examined practices for preventing conflicts of interest during employment and post-public service. B. Hauray, H. Boullier, J.-P. Gaudillière, and H. Michel investigated conflicts of interest in medicine. C. Trost and A. L. Gash analyzed conflicts of interest in public service concerning interethnic relations.

Vallanti G. and Gianfreda G. explored the informal sector, regulation, and productivity in the context of shadow employment. N. Gavual and A. Zasova studied tax evasion on labor, minimum wage increases, and employment. O. A. Hrishnova researched wage destigmatization in the context of social responsibility development in Ukraine. K. V. Dubych analyzed factors of labor market shadowing in Ukraine. O. V. Kasyan examined trade unions in Ukraine and abroad. M. Kirzhetska and Yu. Kirzhetsky studied the impact of corruption on the shadow labor market. L. Ostapenko explored corrupt actions in labor relations. V. D. Polishchuk examined employment destigmatization as a factor in ensuring social security. S. V. Piasetska-Ustych analyzed corruption and the shadow economy within the socio-economic relations system. S. Saisavat studied the impact of minimum wage on employment in the dual economy using Thailand as a case study. S. Sarkar explored employment based on human needs and talents. Send B. V. conducted construct validation of the cognitive components of creativity. K. V. Smyrna investigated the impact of shadow employment on a state's economic security. F. A. Tsesarsky analyzed the protective function of trade unions and its forms of implementation. D. Yu. and D. Sul Kim studied the invisible impact of terrorism conflicts, political regime types, and the shadow economy. Many others contributed to this field.

Belmont D. researched counterparty risk management in an unstable financial system. Vladimirova N. studied state financial control reforms in the context of financial security for business entities. Voitovych I. explored criminological foundations for countering corruption in military security. Dom R., Kasters A., Davenport S., and Prichard V. examined innovations in tax reporting. Konovalova I. analyzed fraud prevention in e-commerce. Krugman P. studied causes of economic depressions and crises. Schaper T. and Weber P. examined fraud in small businesses. Roizen E. and Stauthuysen K. investigated the role of management control system imitation in supply chains. Torgler B. researched tax reporting and tax morale. Filho M. examined fiscal institutions for minimizing tax losses. Fragomeni M., Contador S., Mitidiero K., and Satiro V. analyzed business network linkages.

Brogi M. and Lagasio V. studied the evolution of illicit behavior in fintech. Grandi S., Sellar K., and Jafri J. analyzed global financial systems. Zand A., Orwelli J., and Pflugel E. explored a secure framework for combating money laundering through machine learning and secret-sharing techniques. Minenko S. examined the transformation of anti-money laundering systems in the digitalization of the national economy. Pavlidis G. researched AI deployment for anti-money laundering and asset recovery. Pitt M., Atkinson P., Goredema K., Bakareze A., and Lasic T. studied asset tracking of stolen funds. Sachs K., Klopec M., Hemmal Y., Kaljuste K. E., and Petermann A. investigated children's internet usage. Sudeal L. analyzed de-legalization approaches in legal reform. Susan B. studied public crime data. Takei Y. and Shudo K. examined technical issues and a taxonomy of solutions for virtual asset transfer regulations. Hoopers K., Zuben M., and Gomez J. researched internet security regulations. Chaika I. studied the criminological characterization and prevention of fraud in Ukraine. Yu Yu., Wu J., Lin D., and Fu K. explored money laundering on Ethereum.

Symbolic systems in forensics remain one of the least developed parts of the field and, at the same time, among the most promising, particularly in the areas of applying the principles of cybernetics, mathematical logic, semiotics, and other rapidly developing fields

of knowledge (Balynska, 2017, p. 462). Digital technologies are gaining greater significance in public life. Anti-corruption issues within these contexts are no exception and have long become part of the electronic format of information circulation and cyberspace, among others. Consequently, the focus of scholars is concentrated not only on traditional issues of criminal law and criminal procedure within anti-corruption policy but also on the presence of information law in this type of policy, and on the legal mechanism for countering idiosyncratic (originates from Greek ἰδιοσυγκρασία "particular mingling") variations in the use of digital technologies by corrupt individuals. In particular, M. Alcántara explored digitalisation and artificial intelligence (further – AI) conceptual characteristics, its effects affecting politics; G. Alecu, P. Boloș – methodology of corruption crimes investigation; O. M. Balynska, A. S. Tokarska, V. A. Yashchenko – actual problems of legal philosophy; V. L. Buryachok, R. V. Kyrychok, P. M. Skladanniy – basics of information and cybernetic security; P. Dela – cyberspace as the environment affected by organized crime activity connections; T. Đukić, M. Pavlovic, V. Grdinić – role of forensic accounting and auditing in modern uncovering financial fraud; S. Goddard, H. Hassan, D. Kos, O. Kraft, R. Kupusswami – investigation of corruption cases; P. Ibbotson – compliance and governance arising from banking royal commission; S. S. Johar, G. S. Johar – forensic technique trap for bribe-seeking corrupt public servant; N. Kossow, V. Dykes – embracing ICT to strengthen anti-corruption; S. Krishnaveni, M. Thomas, C. M. Sathiyanarayanan, B. Amutha – integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems; J. A. Larsen, J. J. Wirtz – strategic meanings in US national-security policy; T. Limba, K. Driaunys, A. Stankevicius, A. Andrulevicius – interaction peculiarities in cryptocurrency and national security; L. Oleksyuk – cyber security management best practices; M. N. B. Putra Yusra, A. J. Simon Runturambi, B. Widiawan – trends and prevention of cryptocurrency-based money laundering crimes; C. Torre – different approaches to populism, leadership and charisma in it, audience democracies where individuals are more important than

party platforms: cases from America and Europe; C. Waddell – forensic accounting in fraud investigative and diagnostic tools; A. W. Malik, D. S. Bhatti, T.-J. Park, H.-U. Ishtiaq, J.-C. Ryou, K.-I. Kim – tools, techniques, and challenges of cloud digital forensics; G. Wingate, L. A. Gray, T. S. Greenberg, L. M. Samuel – good practices for non-conviction based asset forfeiture; T. Yaroshko, V. Kosa, O. Ignatenko, V. Ermolayev – engineering scientific knowledge graphs from the anti-corruption publications use; etc.

Researchers like Bauhr M., Czibik A., Fine Licht J., Fazekas M. have explored the dark side of public procurement, highlighting the role of corruption and the importance of transparency as a deterrent; Lenderink B., Halman J. I. M., Voordijk H. have investigated the role of public procurement in fostering innovation. Fazekas M., Sberna S., Vannucci A. have delved deeper into the organizational structures that facilitate corruption. Scholars such as Disdier A.-C., Fontagné L., Tresa E. have examined the economic implications of public procurement policies, particularly concerning protectionism. Manta O., Mansi E. have explored the impact of globalization on innovative public procurement. Patrucco A. S., Kauppi K., Mauro C., Schotanus F. have explored the use of public procurement to improve public service delivery. Sanchez-Graells A. has focused on the impact of digital technologies on public procurement. Matthews D. L., Stanley L. L. have examined logistics and transportation in the public sector. Jance K. has studied the alignment of Albanian procurement legislation with EU standards. Tălpig C. C. has analyzed the efficiency of public procurement systems and their impact on public budgets. Berraida R., El Abbadi L. have explored the potential of artificial intelligence in public procurement. Telles P. has examined the potential applications of blockchain technology in this domain. Researchers like A. Baltrunaite (Lithuania), Azleen I., Nasrudin B., Erlane K. G. (Malaysia), P. Nemec (Czech Republic), Tátrai T., Vörösmarty G., Juhász P. (Hungary), Chang L., Xu M., Guo L., Zhu X., Qin S., Guo X., Yang X. (China), Tabish S. Z. S., Neeraj Jha K. (India) have conducted country-specific studies on public procurement practices and challenges.

Valuable information from all the above-mentioned works made it possible to establish that the subject mentioned in this study is currently incompletely disclosed in scientific doctrine and, accordingly, deepening knowledge about it is relevant. I would like to acknowledge the Portucalense Legal Institute staff at Infante D. Henrique Portucalense University, whose resources and assistance have been invaluable within the UIDB/04112/2020 Program of the FCT I. P. Their camaraderie, the stimulating discussions, collective wisdom and encouragement have been a cornerstone of my research experience. This endeavor would not have been possible without you.

CHAPTER 1
HUMAN VIRTUES, RESOURCES, AND CORRUPTIVE DISTORTIONS OF ANTHROPICITY IN PUBLIC-LEGAL RELATIONS

1.1. Human Consciousness as a Key Determinant in the Anti-Corruption Law Formalization

Despite integrity, in backward social communities, their strata, and labor collectives, people tend to present the desired as reality, claim the simplistic as complex, replace substance with form, eliminate the truly important with noise, and undermine spirituality and rationality through consumerism. These characteristics and the trends they generate are prevalent among the citizens that have not had the fortune to develop and thus exhibit average levels of legal consciousness and worldview-in other words, ordinary people. These citizens also include a minority that concentrates the primary economic wealth within its sphere of influence, namely: public officials, entrepreneurs, and corrupt individuals. This is confirmed by persistently low indices of the rule of law, freedom from corruption, ease of doing business, mastery of language, and other indicators, as well as by the lost economic achievements, military capacity, and the enormous level of illicit enrichment among public officials.

Accompanying the process of integrating into the higher civilizational standards, for instance, EU, with evidence that they are better than described above is no simple task. In any case, statements and slogans about integrity, voiced by journalists and others with access to public discourse, are insufficient. Representatives of highly developed civilizations remain deeply skeptical. As pragmatists who understand the value of civilization's benefits, they view others with distrust, caution, and critical assessment of their words, as they meticulously evaluate the overall national result.

Only through actions, rather than words alone, can peoples demonstrate their unique virtues and their ability to be guided by the principles of the most capable representatives of their nation rather than by personal whims and flaws. These virtues serve

as the foundation for legal formulations that reflect people's values. The matrix of human virtues determines values, which, in turn, shape perceptions, knowledge, and beliefs about universally binding rules of conduct, thus revealing mutual legal correlations in human actions. Legal reality mirrors an individual's inner psychological world, their ability to define the boundaries of their actions, and the freedom of others. The expression of these legal definition's manifests in daily and professional life – for example, among parliamentarians, judges, and police officers. The level of such legal certainty correlates exclusively with a similar level and exhibits tendencies toward either decline or the ambitious goal of achieving a higher level of civilizational benefits, whether European, African, Asian, Muslim, Jewish, Christian, Buddhist, or otherwise. Identifying the true, rather than superficial, legal nature of the modern societies is a significant challenge for the security structures that they seek to join, such as the EU etc.

The principle of legal certainty is based on the formal clarity of legal norms, achieved through logical, consistent, and, where possible, comprehensive regulation of social relations, granting these relations a specific form (Matvyeyeva, 2019, p. 190). For instance, the conflict-ridden nature of legislation and/or the absence of fundamental legislative acts lead to legal uncertainty in the implementation of legal norms in practice, increased tensions at the local level, and violations of citizens' economic and other rights (Huban, 2018, p. 295, 361, 413).

Fragmentation and the limited long-term development of corrupt individuals become the norm for others. The societal demand for insightful, deep thinking and extraordinary decisions aimed at shifting the law in a progressive direction and expanding its philosophical foundation in persistently corrupt nations is critically weakened. National identity itself disappears as legal values cease to unite people. At the same time, corrupt and underdeveloped members of such nations do not become cosmopolitan either, as non-corrupt nations subordinate them as weaker and more backward. Karl R. Popper labeled these types of social communities as "closed" and "open" societies, respectively.

Since 2005, the openness of a society's governance, political, and legal systems to progressive solutions has been partly captured by the Fragile State index that measures the representativeness and openness of government and its relationship with its citizenry. It looks at the population's level of confidence in state institutions and processes, and assesses the effects where that confidence is absent, manifested through mass public demonstrations, sustained civil disobedience, or the rise of armed insurgencies. It considers the integrity of elections where they take place (such as flawed or boycotted elections), the nature of political transitions, and where there is an absence of democratic elections, the degree to which the government is representative of the population of which it governs. It takes into account openness of government, specifically the openness of ruling elites to transparency, accountability and political representation, or conversely the levels of corruption, profiteering, and marginalizing, persecuting, or otherwise excluding opposition groups. The indicator also considers the ability of a state to exercise basic functions that infer a population's confidence in its government and institutions, such as through the ability to collect taxes. It is computed as an aggregation of related questions (The Future of Growth 2024, p. 274).

Courage, creativity, and other indisputable human virtues of legally enlightened citizens are the only guarantees of legal certainty. Human flaws allow only a hint of legality in society. Safeguards against the destruction of legality in legislation and its practical implementation are traditionally considered within a ternary composition (V. I. Manzhura) of spiritual culture and education, where law holds a central place, as well as jurisdictional mechanisms. The spiritual development of citizens is the only way to activate their natural abilities to perceive (see, hear, intuit) law as justice (Socrates, P. M. Rabinovich), to empathize with the wronged, and to seek satisfaction (Latin: satis – enough; facere – to do). The education of citizens determines their intellectual progress, particularly in formulating complex legal decisions and further verbalizing, writing, and correctly expressing them in actions. Criminal-legal, disciplinary, organizational,

administrative, moral-legal, juridico-religious, and other mechanisms for restoring the legal order, punishing the guilty, and preventing future offenses complete this three-tiered composition of defining law by form, content, and practical application in social relations. However, the first element alone is self-sufficient in defining law in its entirety.

Spirituality is a broad concept that denotes the socialization of human existence through the full awareness of one's nature. Education, and even more so jurisdictional mechanisms, have become inventions of complex civilizations on Earth, where humans materialize and are then compelled to care for their physiological development for the sake of spiritual progress. The social contexts documented in history's legal records have been characterized by profound social stratification, precisely based on development, which is founded on society's (the state's) provision of legal opportunities for individuals to understand their virtues, their universal and perpetual priority, uniqueness, and divine determination, their unity with the Divine instead of their flaws, deviations, distortions, and the indisputability of this fact.

The question of willpower is resolved at the points where elements of spiritual, intellectual, and civilization-imposed compulsion converge. In essence, the aspiration to follow one's own virtues constitutes integrity, which demands the utmost effort of human willpower. According to Arthur Schopenhauer, while an ordinary person consists of two-thirds will and one-third intellect, a genius possesses two-thirds intellect and one-third will (German: "wenn der Normalmensch aus 2/3 Wille und 1/3 Intellekt besteht; so hat hingegen das Genie 2/3 Intellekt und 1/3 Wille"), where the divinity/naturalness of the creative process signifies depth of thought, ease, and freedom in fully and adequately expressing ideas. Comparing useful/ordinary people to geniuses is equivalent to comparing bricks to diamonds (German: "und die nützlichen Leute mit den Leuten von Genie vergleichen, ist wie Bausteine mit Diamanten vergleichen") (Schopenhauer, 1997, p. 191, 199).

Weakness of spirit, lack of willpower, servility, obsequiousness, and other forms of flaws in human will result in distortions of legal

reality, simplification of the naturally perfect forms and substance of law, which is universally binding at a given historical moment within the dynamics of historical logic. Inherent internal flaws of the human will take on complex forms due to their dysfunction when manifested externally, that is, beyond mere willpower, at the intersection with other components of human psyche, physical body, spirit, and their combinations. A particularly fertile ground for corrupt perversions emerges when the naturally well-structured human psyche is maimed by family, educators, teachers, colleagues, friends, spouses, relatives, and other societal institutions through their flaws. For example, during the key periods of human psychological development (0–3–6–14–25 years), it is crucial for an individual to engage with convincing examples of virtuous legal relations based on principles of equality, justice, freedom (rule of law), honor and dignity, honesty and kindness, and sufficient strength to protect these values. Families built on these values dominate in an open (virtuous/legal) society.

The pursuit of stability relies on people's support (Ying, 2021, p. 94). Human competition should be based on the criteria of full self-realization within the family, the unparalleled virtues of the family/lineage/nation across millennia, rather than on the ability to accumulate greater material wealth at the expense of one's own flaws or other corrupt models. Authority and trust are a consequence of the ability to correctly define the essence of law. This is genuine legal capital that does not depreciate over time. A confirmation of this, for instance, is the striking legal practices observed in Afghanistan, where even in times of war, warring factions (the Taliban and others) are not allowed to harm or wrong certain families or their members due to their indisputable authority, widely recognized virtues, and deeds that have been validated over hundreds or even thousands of years.

The will for legal progress demonstrates its variability over time. For example, while the right to pension benefits was nonexistent in the 19th century, it emerged and was secured in the 20th century. By the 21st century, there has been a steady trend toward laws shifting the burden of pension provisions

from the state to the private sector. In many countries, this responsibility is now being transferred to individuals and employers, with governments withdrawing from providing state-funded retirement support. In recent years, the UK's pension legislation has increasingly introduced the institution of individual investment choice, which guarantees retirement expenses and their effectiveness while simultaneously ensuring a basic level of protection related to pension savings rights. Traditional economic principles assume that people are entirely rational, "have clearly defined preferences (goals) and make decisions to maximize these preferences." Behavioral economics challenges these old assumptions, questioning the human ability to make such decisions, and in some cases, this has begun influencing legislation and policy (Cooke, 2021, p. i, 65; Tanklevska, 2021).

Changes in criminal legislation generate public expectations regarding participation in legislative activities and satisfy societal demands for punishment (Ying, 2021, p. 2). The progress of such participation requires effort, a focus on the essential while eliminating the atavistic, and transferring the significant into the future, ensuring the continuity of law, the meaningfulness of legal concepts, a vision of perspective, and the integration of law into the system of criminal-legal and other social requirements. The fulfillment of legal tasks by legislators, judges, public executive authorities, and other members of society includes a fundamental component of preserving the achievements of humanity. At this level of elementary reproduction of existing benefits, progress is inevitably present – introducing new, greater, and higher-quality advancements. These socio-legal interconnections reflect a willful process of practically implementing correctly perceived and comprehended legal values through the principles of systemicity and progressive continuity. This represents the co-evolution of law with other dimensions of social life-it is studied to regulate social relations based on these principles, making it fundamental. For instance, scholarly literature emphasizes that if China aims to address the many issues resulting from its economic reforms – such as the decline of social order, widespread corruption, and

a general crisis of values-it will need strong legal institutions and a legal culture that upholds the rule of law. During modernization, the Chinese state not only faces new challenges but also suffers from the side effects of previous reforms, including a weak legal system, environmental degradation, sluggish political reforms, and an unjust social structure, all of which are difficult to change quickly (Ying, 2021, p. 95, 111). Legal psychology is at the core of fundamental relations between the natural and artificial worlds. It also plays a crucial role in understanding the mechanisms through which human biological and cultural systems evolve and become more complex (Inghilleri, 1999, p. 12).

The experience of progress necessitates new knowledge, which cannot be formed except through a teleological appeal to the spheres of the subconscious and unconscious. Since everything is created by any means necessary, the key factor is that the method itself is already established by God within these spheres of epistemology of law. A suitable tool for such evolutionary (A. Bergson) or independent-from-evolution cognition is an outlook that is highly selective regarding the nuances of legal entities and meanings, employs a critical approach, and is capable of comprehensively justifying new legal provisions within a specific historical context and the global conjuncture of international relations. This is a creative type of legal worldview that enables the creation of complex artifacts such as institutions, ideologies, or legal codes (Inghilleri, 1999, p. 11).

Unbalanced by creativity, dogmatism – the automatic reproduction of legal requirements through imitation ("like everyone else"), conforming to them, simplification, provincialism, hypocrisy, artificiality, fanaticism, and the substitution of substance with form (e.g., the dominance of traditions/customs over rationality/spirituality, or the absence of rational explanations for behavioral rules) – excludes development, prevents the reproduction of law, and provokes distortions and corruption. Such worldviews and their characteristics pose potential dangers to the reproduction and development of personal, collective, and national wealth. They are susceptible to false influence, making them a fertile ground for

ideological or other forms of hybrid warfare and the overthrow of constitutional order. For example, individuals with such a worldview may find it honorable to sing the national anthem today, but in the future, they could be convinced that doing so is disgraceful. In this context, as J. Hessen aptly stated, it is crucial to first become a complete person in an ethical sense and to do what makes one worthy of happiness (Hessen, 2009, p. 27).

The danger of individuals with a narrow or distorted worldview lies in their psychological instability regarding their legal convictions – they require explanations and evidence. Without them, they fail to understand the correlation between the sources and prospects of their well-being with constitutional values, international law, and so forth. Among them are ordinary representatives of traditional societies (orthodox/fanatical Christian, Muslim, and African belief systems, among others), where progress is excluded by strictly defining male and female economic roles, restricting women's rights to development, and limiting access to knowledge created by them, along with other contradictions. In this regard, corruption state's context resonates with its European integration aspirations to the extent that it is free from corruption. Furthermore, crucial factors such as communicative situations, political/economic expediency, and language must also be considered. In this case, linguistic barriers to understanding arise not only due to differing signifiers among various social groups (Lad, 1996) but also among different ethnicities and nations – particularly in European countries, where untranslated legal documents are overloaded with fixed expressions, legal formulas, and connector words. Their equivalent translation requires linguistic and cultural adaptation to align with the relevant legal realities.

The compensation for the ideological gaps among citizens should be achieved through the transformation of stressful experiences from the struggle for a quality life – both against corrupt officials and traitors to our constitutional order, as well as against external enemies. Years of endurance under such conditions enable a qualitative leap from a distorted perception of law to the crystallization of legal concepts at the level of stable legal

convictions, open to the civilizational progress of European nations and other strong countries worldwide.

The life of peoples under the constant risk of losing their rights, part of their national territory, and other fundamental legal values has endowed them with crisis management experience. This experience can be expected to generate additional constructive impulses and an enhanced effect of lawful behavior in the regulated calm of legal relations unfolding in highly developed countries of the West and East. In the case of the EU, the paradigm shift in policies within the broader European political environment requires consensus among actors authorized to oversee such a process in political arenas, as well as among other interested parties. This process is ambiguous, diverse, and even fragmented across various sectors of social, economic, and political life, including its legal regulation (Iglesias-Rodriguez, 2016, p. 343, 344).

In a distorted legal reality, human flaws, rather than virtues, become determinants of success. Spiritual impoverishment defines the trend of legal relations. The environment in which corrupt officials thrive is not truly a place for the strong, resilient, energetic, and steadfast – although it may seem so. Instead of the rule of law, a veiled, latent, sophisticated, and multi-component form of violence dominates, including coercion into labor due to human dependence, an unequal distribution of material and other rewards for honest work with quality results, prolonged resolution of legal matters (e.g., taking six or nine years instead of a maximum of three to organize the defense of a scientific dissertation), the artificial creation of obstacles to the development of capable individuals, and more.

On a national scale, a corrupt government structures legislative requirement in such a way that it creates a financial imbalance in favor of the capital city and/or certain settlements while also shaping opportunities based on a person's (or family's) financial status. It is mistaken to believe that this is an environment where one's nature and strength guarantee survival and development, like a land of wolves. Virtuous citizens realize their rights by virtue of their nature, not its distortion. At best, a corrupt

society can resemble a place inhabited by people with a perverse understanding and definition of law – existing outside of a balanced natural law, akin to the social order described by Thomas Hobbes, where members of the community are in constant conflict due to their own flaws, exhibiting behavior worse than wolves (Latin: homo homini lupus est) (Hobbes, 2000; Biletzki, 1997). For example, in the Ukrainian film Pamfir (an artistic expression of modern Ukraine – its indomitable spirit and will to live), issues such as smuggling and the catastrophic destruction caused by corruption are illustrated. In the border region of Ukraine, law is defined by the long-term dominance of evil, human flaws, and corruption, including the bribery of law enforcement officers, prosecutors, and judges, conflicts of interest, smuggling, and official misconduct. The most defining characteristic is the perversion of the consciousness of local residents, who commit violence, legalize unlawful actions by giving them a legal form, and redefine what they call "law" (Pamfir, 2022).

Political and social instability, economic transformations, corruption, income disparities, environmental degradation, uncertainty, dissatisfaction with the government, a growing sense of personal rights, and increased use of internet resources all drive the need for continuous legislative updates (Ying, 2021, p. 79, 94). Simultaneously, societies plagued by corruption, particularly their public authorities, represent a degeneration of humanity and law. Such lands experience demographic, economic, and/or environmental depletion. The institutionalization of legal norms based on human flaws stimulates deviation from the life-creating energy of the nature of law.

Characteristic features of this type of legal definition in legislation and legal practice include violence (physical and psychological), exhausting labor exploitation, an administrative and judicial bureaucracy devoid of legal values, and more. Scholars have noted progress in improving judicial education and training, raising the qualifications of new judges, and fighting corruption. However, efforts to reduce political influence on the judiciary remain modest. A major weakness is the distortion of justice caused by politically

and/or legally biased pre-trial investigations, selectively conducted by anti-corruption bodies, police, and prosecutors to serve specific interests (Ying, 2021, p. 98).

Thus, linguistic and conceptual frameworks, along with the semantic load of legal terms and their corresponding concepts, form the essence of legal certainty. The primary embodiment of legal definition lies in the consciousness of each individual. Legislative definitions of law derive from a collective set of individual perceptions and convictions about the legal regulator.

Here, the absence of an identical understanding of a legal concept between the lawmaker or law enforcer and the person subject to the law creates discrepancies in legal identification. This hinders the effective implementation of the law and necessitates a comprehensive verbal explication through adequate legal interpretation while preserving the goal of fully realizing the dialogic potential of legal worldviews among participants in legal relations and ensuring the quality of their correlation (from universally interpreted concepts to specific ones, etc.).

Accordingly, the probability of aligning individual legal consciousness with the collective legal consciousness reflected in legislation depends on the ultimate additivity of law. For instance, amidst Ukraine's integration into the EU and security structures, it is crucial not only to achieve the nominal recognition of Ukraine's legal system as part of European law but also to transform the mentally declared image of a virtuous Ukrainian into a dominant reality of domestic legal practice. Otherwise, the high-tech assistance, equipment, and other assets provided to Ukraine for post-war reconstruction will be lost to corruption schemes – essentially following the "corrupt Leninist path", where the labor of many benefited only a few.

1.2. Depletion of Human Virtues from National Security Resources through Corrupt Personnel Policies in Public-Legal Relations

The image of extending human labor, its overload, and the increased cost of production cycles (provision of services/performance of work) under otherwise equal conditions is corruption-prone. A person at their workplace, driven by their vocation, determines social progress. Differences in the level of social trust in different countries are more adequately explained and accounted for by the concept of "justice," particularly from the perspective of impartial income distribution, effective democracy, and freedom from corruption. Corruption is a negative phenomenon, whereas creativity is a positive one, associated with pleasure and conscientiousness (Kwantes, 2021, p. 42, 23). Accordingly, if creative and virtuous individuals are united by a single righteous goal/task – one that aligns with universal human values – they form a strong and viable nation. At the international level, communication becomes predictable and productive. In this context, interactions between strong nations are based on the rule of law, authority, and trust rather than force or violence. One of the consequences of a high-power distance between authorities and the rest of the population is the tendency of officials toward corruption (Kwantes, 2021, p. 78). The internal national parity of relations is reflected externally, and vice versa.

In this regard, a methodological approach that has proven constructive is one that aligns personal interests with those of partners and ultimately ensures a balance of common interests. The mathematical theory of probability, in the context of the variable synergy of law, along with other logical methods based on common sense, dominates this approach. This approach simultaneously serves both as a means of understanding the nature of legal relations and as a tool for managing them. The enhancement of managerial effectiveness is achieved through the power of persuasion, stimulation, and other methods. Law is determined by society, and society itself is anthropogenic. Therefore, what is understood

in the nature of law and society is that which is anthropometrically measurable, beneficial to all parties, and progressive.

Regulatory and legal acts governing the implementation of personnel management in public administration operate on outdated conceptual foundations. They fail to consider modern challenges and economic crises, the increase in corruption, political instability, and, for instance the requirements of European integration, among other factors (Yevdokymov, 2020, p. 11). The traditional definition of public personnel management does not include a broad range of public integrity restrictions for civil servants and officials. These restrictions include prohibitions aimed at preventing traditional forms of public corruption, such as bribery and embezzlement of public property, as well as a wider range of rules and regulations governing financial conflicts of interest.

Laws and regulations on conflicts of interest often prohibit government officials from accepting gifts and private hospitality from sources regulated by the government or engaging in business dealings with the government. Conflict-of-interest regulations may require civil servants and officials to publicly disclose their financial assets. They may also mandate that a government official divest certain financial holdings or recuse themselves from decisions that could affect the value of their financial assets. The government imposes restrictions on lobbying by former government officials within their former agencies, as part of so-called “revolving door restrictions” (Riccucci, 2020, p. 105–106).

A corrupt official distorts the described rules for managing social processes. Essentially, this is a manifestation of legal dysfunction – a classic example of the phagocytosis (ethnosis) of law, to use the language of biological science. The sustaining energy of corruption lies in virtues and law; it parasitizes them and exists only as long as it continues to consume their energy resources. For instance, compared to Ukraine, the EU, USA and others are freer from corruption, though it is more deeply entangled in highly complex forms of transnational corruption and related offenses. Other example, a massive multinational investigation launched by the magistrate of Trento, Carlo Palermo, exposed long-standing,

well-protected channels of illegal trade worth billions of dollars. The investigation uncovered an enormous smuggling network that included influential Turkish and Syrian drug lords, Bulgarian and Yugoslav state companies and intelligence agents, Italian mafia members, and numerous arms dealers. However, before these cases could be fully investigated and over 250 accused individuals could be brought to trial, Palermo was suddenly reassigned, the investigation was halted, and its most explosive evidence was classified for forty years. The judge had confronted too many intelligence agencies, influential politicians, party financiers, corrupt civil servants, "bent bankers," and diplomats navigating the complex waters of East-West relations (Marshall, 2012, p. 156, 159).

As we can see, corruption complicates the process of achieving an effective personnel policy in the justice system. The judicial system cannot function properly if its members are prone to corruption or if corrupt officials neutralize the professional competence of honest judges (Borovyk, 2021, p. 151). Concomitantly, in the Ukraine-EU relationship, the EU serves as a source of sustaining energy, while Ukraine acts as its consumer. If the domestic national environment no longer offers fair, lawful competition for human virtues in public-sector hiring competitions, the result is a growing trend of functional disqualification in these organizations. Corrupt officials further exacerbate the situation by imitating compliance with legislative procedures in such competitions. Corruption becomes more latent and, therefore, harder to neutralize. As a result, corrupt individuals in key government positions do not just weaken the nation – they make it critically vulnerable. Their moral, intellectual, and psychological incapacity poses a real threat to national security.

This is particularly evident in public authorities striving to operate according to modern European quality standards. Beyond professional issues, Ukraine's modern workforce also faces socio-psychological challenges: instability in society, criminalization, corruption, weak legal and legislative frameworks, inflation, and unemployment. All these factors hinder the creation of a healthy labor market environment (Karkovska, 2020, p. 58). Among

the current measures in state personnel policy is the strengthening of moral requirements for individuals involved in managerial activities to prevent corruption, avoid conflicts of interest, and improve disciplinary procedures (Goryachenko, 2022, p. 190). Corruption can affect all aspects of human resource management, with favoritism, nepotism, and abuse of power in hiring, training, promotion, and transfers identified as key risk areas. These issues arise due to uncontrolled discretionary powers, lack of integrity, accountability, checks and balances, and transparency in overall HR governance (Chêne, 2015).

The failure to fulfill official duties is a sign of corruption. Whether something was done incorrectly, not done at all, done late, or done poorly – it all equally illustrates distortion. Such distortions are corruption-related when intentional, particularly when another qualified individual could have effectively filled the role. Nepotism, favoritism, and cronyism are all forms of corruption in which appointments are made based on kinship, bribes, loyalty, or personal benefits. In corrupt societies, form often loses its significance because it no longer corresponds to substance. For example, according to formal documents, an individual may be certified at a particular qualification level (scientific, pedagogical, managerial, or professional). However, in reality, they do not and cannot demonstrate such a level because the document does not reflect their actual competencies. Their development does not match the qualifications stated in their documents. This kind of discrepancy is a sign of structural corruption, which poses a real threat to national security.

Terrorism and crime are activities that attract attention, but there are other, more insidious risks that can harm investments. Bureaucracy – the inefficiency of red tape that creates friction – is one issue. Nepotism – favoritism in political appointments and contract awards – is another. Bribery and corruption, sometimes on a massive scale, are widespread in many parts of the world (Poole-Robb, 2002, p. 4).

If every organizational-legal element of public order is objectively determined, then the loss or significant dysfunction of any of them

poses a threat to the existence and development of society. The value of form is difficult to overestimate, especially when it carries legal consequences. In the case of documents related to a person's professional qualification certification, we observe precisely such legal properties of form. The critical relevance of content and form in this context arises for individuals holding public office, as they are responsible for the public interest. Naturally, this interest will not be protected if it is entrusted to someone incapable of performing the job assigned to them. Corrupt officials guarantee inertia, uncertainty, and the breakdown of existing achievements.

The dysfunctionality of public and private legal relations, as described above, is to some extent mitigated by the efforts of professionals – those who hold positions in of a genuine calling and therefore perform effectively. The essence of this compensatory mechanism, in which ethical employees perform job functions in place of corrupt officials, lies in the fact that they take on a larger workload, while the rewards go to the corrupt individuals. However, such distortions have their limits. This leads to secondary dysfunction: when ethical employees perform the work of corrupt officials at the edge of their physical and temporal limits. If the primary dysfunction of a public organization is caused by a distortion of its organizational structure – namely, the appointment of unqualified individuals – then secondary dysfunction is determined by the objective capacity of ethical employees.

Many national problems arise directly from the lack of properly legislated transparency, accountability, and mechanisms to eliminate nepotism and corruption (Poole-Robb, 2002, p. 12). In fact, when an organization (or its structural unit) reaches a critical mass of corrupt officials, it becomes incapable of performing its functions effectively. At this stage, even the resources of ethical employees are no longer sufficient to compensate for the inactivity of corrupt individuals.

From an economic perspective, the primary resource that compensates for corruption is the skill and dedication of ethical employees, who not only complete their own tasks but also work in place of corrupt officials. The second resource is time – whether

calendar time, academic time, or other forms of scheduled time – that extends beyond the legal labor limit (e.g., eight-hour workdays with two weekly rest days and vacation time). This extra burden consumes all available hours, leaving only 6–8 hours daily for rest. The third resource is the energy and time of the ethical employee's family, friends, and close associates, who step in to provide additional support. The fourth resource is the extended duration required to complete tasks – delays ranging from months to years. Accordingly, key indicators of personnel corruption in an organization can be assessed through specific methodologies, including evaluations of business reputation, an individual's moral capital, anonymous surveys, polygraph testing, and other investigative techniques (see Table 1).

Table 1: Resources Expended to Neutralize Professional Incompetence Resulting from Corrupt Hiring Practices

No.	Resource Expended to Mitigate the Consequences of Professional Incompetence Due to Corrupt Hiring or Lack of Real Work Contribution
1	Skill and expertise of virtuous employees
2	Time of virtuous employees beyond legally mandated workload limits
3	Life energy of virtuous employees
4	Time and energy of close associates (family, partners, friends, colleagues) who assist ethical employees
5	Financial rewards received by corrupt officials instead of virtuous employees
6	Extended task completion times, sometimes increased by months or years

This systemic issue illustrates how corruption erodes organizational efficiency and burdens virtuous employees, ultimately leading to structural collapse if unchecked.

The movement for civil service reform should focus on making it safe for individuals who have the integrity to serve society without engaging in corrupt practices and the expertise necessary for the effective delivery of public goods and services. This entails protecting civil servants from having to follow the directives

of political machines that heavily rely on patronage systems to maintain political power, as seen in the United States at the end of the 19th and beginning of the 20th centuries. For instance, the U. S. Supreme Court has made it clear that it never intended to allow public employers to use Garcetti's Case (the precedent that criticism by a civil servant of any public authority may negatively impact the career of the critic if the criticism is made in an official capacity, but not if it is made as a private individual – "because his statements were made pursuant to his position as a public employee, rather than as a private citizen, his speech had no First Amendment protection") as a tool for retaliating against civil servants-whistleblowers who use internal information to report corruption up the chain of command or to appropriate law enforcement officials (Riccucci, 2020, p. 70; USA Supreme Court, 2006). Otherwise, the excessive burden placed on virtuous employees multiplies the negative effects on society by undermining their social mission, limiting the resources available to their allies, and sustaining the destructive influence of corrupt actors.

Observational methods and empirical data analysis over at least fifteen years have provided baseline data indicating that one virtuous employee, through their skills and lifetime efforts, can compensate for the incompetence of up to eighteen corrupt officials (more commonly, not exceeding six) over a period of at least 5–6 years. Notably, public authorities and other public law organizations – entities that contain the resources desired by corrupt actors – are the first to be infiltrated by corruption. Among the motivations driving corrupt individuals are fundamental human desires, including access to food (clothing), sex, and power. Related to these are interests in recognition, wealth (cars, luxury brand clothing, diamonds, gold, etc.), real estate, land plots, spacious private offices, prestige, and other material or otherwise questionable benefits when compared to spiritual achievements and enduring values.

In the public sector, the material enrichment and/or vice-cultivating behavior of corrupt officials occur at the expense of the public interest in various ways. For example, a corrupt official may be rewarded with material goods (money, apartments, etc.)

or other privileges despite having no real professional achievements. They may receive disproportionately high compensation compared to the average citizen's income, or their professional incompetence may be concealed using the performance metrics of honest employees. This creates a second source of destruction: not only are virtuous employees unable to fully realize their potential due to the ineptitude of corrupt colleagues, but society also bears the financial burden of rewarding these corrupt officials for distorted results, which other corrupt actors then present as achievements, often decorated with the genuine work of honest employees.

Such double losses are less common in the private sector because private interests prevent any employee from distorting objective reality for personal gain. While nepotism does occur in private businesses, it is usually the exception rather than the rule. Moreover, such businesses tend not to survive long, as they struggle to compete in a fair market. Recognizing this, it is evident that when a nation's leadership, government, parliament, and/or high-ranking public officials engage in corruption, public trust in them sharply declines. In such cases, people are likely to become even more distrustful of their fellow citizens, from whom they do not expect the same level of integrity as they do from national leaders (Kwantes, 2021, p. 79, 82).

According to Paragraph 6, Part 1, Article 1 of the Law of Ukraine "On National Security of Ukraine" No. 2469-VIII, dated June 21, 2018, threats to Ukraine's national security are phenomena, trends, and factors that make it impossible or difficult – or may make it impossible or difficult – to realize national interests and preserve national values. Paragraph 9 of the same article classifies such threats as real or potential. The proportion of unqualified individuals holding public office should not exceed 10% of all such positions. If this proportion approaches one-quarter, it constitutes a real threat to national security. The synergy of dishonesty among such officials, who occupy positions they do not merit, leads to an increase in associated crimes, particularly those against the fundamental constitutional values of the nation and its people. These crimes include offenses against national security, crimes

against life and health, offenses related to public service and professional activities connected to public services, terrorism and other crimes against peace, human security, and international order, as outlined in Sections 1, 2, 17, and 20 of the Criminal Code of Ukraine No. 2341-III, dated April 5, 2001. Crime and terrorism, as well as bureaucracy, corruption, unfair competition, dishonest trade practices, forgery, and the consequences of cultural, political, and religious differences, now cross borders with relative ease (Poole-Robb, 2002, p. 9).

The destructive energy of constitutional values being undermined by corrupt personnel policies in public law relations accumulates exponentially. Those who have obtained their positions dishonestly tend to multiply others like themselves. In other words, if at the beginning of the year, public authority was corrupted at a safe level – below 10% of total public positions – by year's end, this percentage could exceed three-quarters. A striking example of this was Ukraine's experience in 2010, when public officials were replaced at an alarming rate, accompanied by legislative changes to facilitate this process. This case is particularly illustrative due to its speed, violence, and catastrophic consequences – such as economic stagnation by the end of 2012 and beyond, when a critical mass of corrupt officials occupied key positions. However, this is not an isolated case; corruption-driven personnel policies have historically been prevalent in Ukraine, correlating with consistently high corruption levels and a low rule-of-law index. For instance, the banking and financial sectors are destabilized by manipulated debtor reports, administrative pressure on the central bank and other financial institutions to provide credit to financially insolvent borrowers, and other forms of corruption and opacity that hinder external oversight (Poole-Robb, 2002, p. 11).

For any nation, the loss of developmental resources raises urgent questions about the adequacy of anti-corruption measures, the promotion of moral virtues, and the regeneration of integrity among citizens. The constructive passion of such citizens is unique, limited, and difficult to reproduce. What people refer to as a "brain drain" due to the emigration of intellectual and spiritually developed

individuals is, within the country, a result of these individuals being denied opportunities to fulfill their virtuous social mission or having their energy and life resources effectively stolen.

Thus, a public authority that allows rule distortions to the extent that its most capable citizens cannot fully realize their potential deprives society of its future – its ability to sustain and multiply its existing resources. The loss of human capital is often invisible to ordinary citizens, as their perception of social norms is shaped by cultural meanings, places, spaces, and how individuals construct meaning, evaluate life situations, and stigmatize the behavior of others (Irvine, 2022, p. 8, 200, 192). By defining the normality of individuals and their development within a specific social context, we can assess their role in shaping the negative trend of personnel corruption and/or their ability to counteract it. Unfortunately, many people prefer to remain in their intellectual comfort zones, saying, "Why make things more complicated?" – often accompanied by hypocrisy, self-righteousness, and personal shortcomings such as laziness or oversimplification. In the long run, maintaining this trend and this conformity/marginality within the population disarms the nation, making it dependent on spiritually more developed and/or wealthier nations. It creates a demand for assistance from the advanced international community in the form of progressive international legal norms, the virtues of their best representatives, and similar support. "In international meeting halls, there is a mix of arrogance, naivety, and perhaps ignorance. Of course, safeguards against risks exist, with the first line of defense being the awareness of decision-makers and those who appoint them. Ignoring risks can be fatal for both individuals and nations, as experience shows" (Poole-Robb, 2002, p. 10).

Thus, corrupt personnel policies in the public-law sphere pose a real threat to national security when their distortions exceed one-quarter of all public-law relations. When this figure reaches two-thirds, external assistance from corruption-free nations becomes necessary to restore integrity. Dishonest personnel policies represent a problem requiring a comprehensive legal framework at the level of at least a separate legal institution or sub-branch of law. Related

legal regulations can be found within the framework of conflict-of-interest prevention, as the anti-corruption strategy should highlights connections between ethical personnel policies and procedures for preventing and resolving conflicts of interest.

1.3. Monitoring the Standard and Way of Life of Public Authority Officials in Correlation with the Quality of Anti-Corruption Legislation

Within the anti-corruption framework of "monitoring the standard and way of life of a public authority representative," it is critically important for Parliament to define the concepts of "standard of living" and "way of life." The first factor to consider when defining these concepts is the personal context: the levels of natural, rather than artificial, real rather than ephemeral, personal and professional development of a public authority representative, which determine their natural needs, differing from those of other social strata. The focus is on development rather than substituting this concept with imaginary forms-mere imitation-if the individual's nature lacks inherent internal correlations within their essence.

The standard of living is a complex concept, and it is far from obvious how it should be measured. Like must be compared with like; distributionally sensitive indicators of the standard of living are needed, and so forth. Attempts to assert that the ideal way to determine the standard of living is through the total utility a person derives from consuming a set of goods obtained through labor, investment, or transfers are ineffective. The utility of different goods depends on personal characteristics and cannot be measured. Therefore, most concepts of the standard of living focus on the goods themselves or access to them; the latter is often measured through production, income, or wage data across various professions.

The standard of living is assessed in the following ways:

1) based on the Basic Needs Index, developed in the 1970s by the International Labour Organization, which includes food,

clothing, housing, healthcare, education, water, and sanitation. However, there is no consensus on how to evaluate these factors;

2) according to the UN Human Development Index (HDI), which combines real income (GDP per capita), health (measured by life expectancy), and education;

3) following Amartya Sen's capability approach, which considers "functionings" and "capabilities" as measurable analogs of utility. Capabilities, combined with an individual's mental state (which includes personal characteristics and social constructs such as legal, religious, ideological, and other beliefs), determine a person's functionings. These range from basic elements like adequate nutrition, good health, physical strength, and longevity to more complex aspects like self-respect. Functionings are important because the utility an individual can achieve depends on them, and they are measurable, unlike utility itself (Allen, 1, p. 6–8).

The term "way of life" refers to a person's mindset, interests, needs, health, well-being, quality of life, and actions (both acts and omissions). In Ukraine, for example, a subordinate act defines "way of life" as the behavioral patterns of a declarant that reflect their standard of living and include possession or use of assets, acquisition of assets, expenditures on services and work, financial obligations, and other legal transactions (NAPC No. 236/23, paragraph 5, point 3). This definition is inadequate because it defines the concept through "forms" and includes highly abstract terms such as "standard of living" and references to asset ownership and legal transactions. However, this does not fully capture the concept of a way of life.

Thus, the lack of clear legal definitions for "standard of living," "way of life," "lifestyle monitoring," "excessive interference with the right to personal and family life," and "selective lifestyle monitoring of declarants" contributes to arbitrariness and a low level of rule of law. Ultimately, all these concepts are reduced to the material assets owned by the declarant. If so, then establishing the meaning of these concepts and their relevance to the specific circumstances of declarants' lives requires sufficient knowledge of economics and sociology, meaning the involvement of experts (commodity experts, art historians and other holders

of knowledge about the usefulness of a specific type of goods, services, work) when applying legal norms related to "Integrity Monitoring of a Public Authority Representative" within criminal, administrative, disciplinary, or any other type of jurisdictional proceedings. Monitoring the way of life of public authority representatives and their family members must be conducted based on an exhaustive and formally clear list of grounds, following a unified algorithm. There is no irrefutable and/or logically exhaustive legal definition of the concepts "discrepancy between the standard of living of declaration subjects and their declared assets and income" in the law. The following concepts should be legally defined: "standard of living of the declaration subject"; "standard of living of family members of the declaration subject"; "discrepancy in the standard of living of the declaration subject"; "discrepancy in the standard of living of family members of the declaration subject"; "discrepancy in the standard of living of the declaration subject and their family members"; and "open sources of information." Formalizing these concepts will allow their integration into algorithms for software codes used in anti-corruption work by neural networks.

At present, any definition of the "discrepancy" component within these concepts remains subjective rather than formalized, disputable rather than irrefutable, and is established on a case-by-case basis within jurisdictional proceedings, including by the police, prosecutors, and judges. However, the task of defining these legal terms is entirely parliamentary, not judicial. The key to understanding all these concepts lies in comprehending the essence, meaning, and components of the phenomenon of "compliance" (from Portuguese "correspondência," "coincidência"; German "die Übereinstimmung"). Large language models can perform the primary work of detecting and classifying criminal corruption. The accuracy of such data processing is subsequently verified and, if necessary, corrected by judges and other representatives of criminal justice. When it comes to monitoring judges' compliance with anti-corruption laws, it is appropriate to clarify that "any forms and methods of control, including inspections, monitoring, etc.,

of the functioning and activities of courts and judges should be carried out exclusively by judicial authorities and exclude the establishment of such bodies within the executive or legislative branches." This was rightly noted, for example, by the Constitutional Court of Ukraine in its opinion of October 27, 2020.

The term "monitoring" in Ukrainian legislation is a calque from the English "monitoring," used instead of the Ukrainian equivalent "observation," which weakens the regulatory function of legal norms containing this term for Ukrainian-speaking citizens. If Ukrainian legislators had irrefutable grounds for using the English term, it would logically follow that these same grounds would be significant for parliaments in English-speaking countries when incorporating the Ukrainian term "observation" into their anti-corruption legislation.

The legal approach in anti-corruption policy – a sensitive and sometimes politicized area of law enforcement and justice-requires an exhaustive enumeration of provisions and the avoidance of the word "other" in anti-corruption laws. Otherwise, the quality of the anti-corruption law diminishes, as legal formulations that include ambiguous terms create an impression of legal uncertainty, unpredictability, and an undefined "other as provided by law." If such "other" exists, it must be defined explicitly. This is especially important in provisions concerning the highest anti-corruption justice bodies to prevent any attempts to influence judges who are professionally tasked with eliminating not only criminal corruption but also the most complex forms of political corruption of the highest financial and/or organizational scale. On this responsible and virtuous path, any legal norm regarding the legal status of criminal justice officials containing the word "other" represents an unacceptable vulnerability for these officials. Simultaneously, it is necessary to avoid "multiplication of entities without necessity" (Latin: "Entia non sunt multiplicanda praeter necessitate"). Redundancy in anti-corruption legislation is merely a variation of pleonasm and legislative simplification (Latin: "simplex" – simple, and "facere" – to do). It does not enhance the logic of the legal text, with which citizens would find it difficult to disagree.

Furthermore, to be effective, Parliament should avoid exaggerated truisms, opting instead for concepts and rules that are relevant to the authentic essence and content of the functional burden of a potential corruption subject. The informativeness of the provisions in question trends towards zero, as they are already known, formally defined, and applied. Excessive legislative text weakens the legal meaning and content, which, when flawed, is always difficult to grasp for the naturally logical mindset of a professional lawyer, let alone for readers with other professional backgrounds. Such deficiencies in legal technique violate the principles of word economy (Latin: "lex parsimoniae"), as well as legal certainty, which has been repeatedly emphasized by ECHR. For example, in paragraph 143 of the ECHR judgment of January 9, 2013, in the case "O. Volkov v. Ukraine" (application no. 21722/11), it is stated that "procedural rules are created to ensure the proper administration of justice and the observance of the principle of legal certainty, and that parties to proceedings should have the right to expect the application of the aforementioned rules. The principle of legal certainty applies not only to the parties to the proceedings but also to national courts" (ECHR No. 21722/11).

A hallmark of countries with minimal corruption is the meticulous and precise application of concepts by legislators, which adds structure to the law, rhythm to its text, and quality to its provisions, as regularly emphasized by ECHR. For instance, in paragraph 80 of the ECHR judgment of October 2, 2014, in the case "V. Tymoshenko and Others v. Ukraine" (application no. 48408/12), it is stated: "The Court reiterates that the phrase 'prescribed by law' in Article 11 of the Convention requires not only that the contested measure has some basis in national law but also that the quality of the law in question is met. The law must be accessible to those concerned and formulated with sufficient precision to enable them – if necessary, with appropriate advice – to foresee, to a reasonable degree in the circumstances, the consequences that a given action may entail" (ECHR No. 48408/12).

The ECHR has repeatedly emphasized the need for proper definition of conduct rules, including property rights. For example,

in paragraph 102 of the ECHR judgment of May 22, 2018, in the case "Zelenchuk and Tsytsyura v. Ukraine" (applications no. 846/16 and no. 1075/16), it is stated that "in assessing compliance with Article 1 of Protocol No. 1 to the Convention, the Court must conduct a comprehensive review of the various interests at stake, remembering that the purpose of the Convention is to guarantee rights that are 'practical and effective.' The Court must look beyond the obvious and examine the realities of the disputed situation" (ECHR No. 1075/16).

The quality of anti-corruption laws is reflected in their acknowledgment of the cross-disciplinary specialization of criminal justice bodies. Their activities involve at least criminal, civil, and administrative cases, along with their respective procedural rules. For example, the segment of commercial cases involving pre-trial investigations and justice requires the description of forensic and other procedures used to track and prove corrupt income obtained through cryptocurrencies and other virtual assets via cyberspace. Similarly, satisfying private interests at the expense of public interests significantly infiltrates commercial relations in tunneling practices (Peng, 2011), securities manipulation, and other fraudulent business practices.

The interdisciplinary nature of corruption, especially its severe – socially dangerous – forms, is reflected in legislation referencing not only criminal law but also civil and administrative procedural requirements. These requirements play both a supportive role in the criminal procedural order and an independent role in eliminating the property base of corrupt individuals, such as confiscating unlawfully acquired assets which constitute the difference between the value of such assets and the legitimate income of a public official. In this context, assets are understood as monetary funds (including cash, funds held in accounts/e-wallets, in banks or other financial institutions, non-banking payment service providers, electronic money issuers, or in custody at banks or other financial institutions), other property, property rights, intangible assets, including cryptocurrencies, the reduction of financial obligations, as well as work or services provided to

a person authorized to perform state or local government functions. However, for example, the current laws of Ukraine lack a legislative definition of the term "unjustified assets," which prevents its uniform interpretation and application by criminal justice bodies and/or other public authorities, undermines legal order in recognizing the assets of corrupt individuals as unjustified, and specifically raises doubts about the irrefutability and fairness of court decisions in this category of cases. Under such conditions, the constitutionality of procedural anti-corruption legal norms related to "unjustified assets" comes into question (Figure 1).

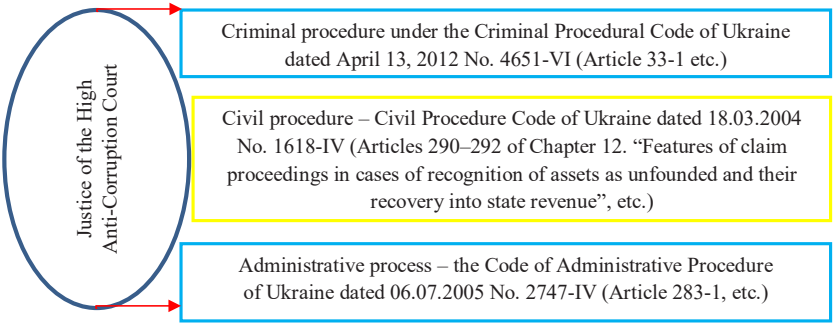

Figure 1: The Ternary Application of Procedural Law in Anti-Corruption Justice: The Case of Ukraine

Thus, justice and judicial oversight of the pre-trial investigation of corruption-related criminal offenses take place in at least three types of jurisdictional processes: criminal, civil, and administrative. Herewith criminal corruption always poses a threat to national interests and national security, as it precedes and/or amplifies related crimes, such as the betrayal of the constitutional order, assistance to a foreign aggressor, terrorism and other hostile actions. It facilitates armed attacks by other states or non-state entities, endangers the lives and health of the population, leads to hostage-taking, the expropriation of state, individual, and corporate property, causes financial losses, and creates obstacles to sustainable economic development and the full exercise of citizens' rights and freedoms.

CHAPTER 2
THE DESTRUCTION OF NATIONAL SECURITY BY CORRUPT PRACTICES AND OTHER PREDICATE CRIMES OF ENTREPRENEURS AMID CHALLENGES FOR THE DIGITAL FORMAT OF ANTI-CORRUPTION POLICY

2.1. Interference of Corrupt Entrepreneurial Intent in the Sphere of Labor Law

A nation united by common ideas, means, and scientific capabilities exists as long as its members operate under rules that enable it to maintain these characteristics and multiply its achievements. The distortion of even one of these rules poses a threat to the nation. The scale and/or duration of such distortions correlate with the reality of threats to national security. A negative scenario implies that public authorities have failed to justify the mandate of trust for development granted by the population, particularly by failing to provide it with appropriate rules. The point of no return in this scenario occurs when public authorities begin to formulate rules that are inadequate to current and future challenges. For instance, this includes overly simplified regulations and/or the dominance of lexemes such as "prohibit, eliminate, seize, re-examine, confiscate, reduce, punish" in public-law decisions instead of "permit, create, provide, verify from the outset, allocate, increase, motivate."

Granting a mandate of trust through the electoral process to public authorities based on appearance rather than responsibility and competence inevitably marks the political immaturity of voters, plunging their lives into legal arbitrariness both in legislative formulations and in the practices of their application, often accompanied by statements from public authorities and/or business entities such as "take us to court" and similar expressions. Under such conditions, the quality of legal regulation is already lost, and the quantitative decline of the nation is exponentially increasing. The external-national context, combined with

the outlined nature of internal corruption of a persistent nature, becomes decisive in the transformations of the nation, particularly in the metamorphoses occurring in Ukraine.

The form of quiet personal/familial enrichment of 1–5% of Ukraine's population through the sale of nuclear weapons and other military equipment, fixed assets of enterprises, and other economic resources of national wealth was largely halted by external military aggression from the Russian Federation and its allies. Apart from isolated cases, there was no significant resistance from the Ukrainian population against these thefts and plundering. Migration in a nation without such a collapse, performing labor burdens for others or for many others, receiving significantly underpaid wages, combined with hopes for the integrity of the majority of public authorities and entrepreneurs, remained the dominant legal reactions of Ukrainian citizens to the theft and plundering of national wealth by this majority.

The formal underpayment of wages and/or the absence of official employment are classical forms of such robbery and plundering of the population, invariably accompanied by hypocritical whining and genuine mockery from entrepreneurs with phrases like "high taxes" and "unprofitable business," among others. The segmentation of labor markets into a formal ("legally covered sector") and an informal ("legally uncovered sector") sector in developing countries (Samutpradit, p. 1, 10) hinders their development. Underpaid pension and tax contributions from such wages have no relation to the future, which correlates with the word "development." Such low payments in the present deprive the future majority of resources, inevitably guaranteeing them a swift and certain physical demise, as economically, this majority is no longer considered part of the future – neither by the entrepreneurs who reduced these payments nor by the public authorities that enabled this.

These crimes, like bribery – where one gives a bribe and another accepts it – are dual in nature, as entrepreneurs commit them while public authorities allow them, merely imitating control over preventing such crimes. The pursuit by an entrepreneur and/or

public servant of private interest instead of public interest – the latter being the interest of every wage worker whose salary ensures their reproduction and development (K. Marx, F. Engels) – constitutes the essence of legal distortion, corruption, and dishonesty. Rectifying this remains a real, though still unresolved, task of anti-corruption policy for many states, including Ukraine.

In anti-corruption law, there already exists an institution to counteract the combination of positions and moonlighting by individuals exercising public authority. Legally, its foundation is traced to concerns about the effectiveness of such individuals' work, remuneration for it, and/or the avoidance of conflicts of interest arising from secondary employment tasks. A position free from a moonlighter becomes a source of income and career growth for another person. Consequently, with a high probability, this leads to the capitalization of the individual and expectations of higher labor productivity than if one person simultaneously held both positions. Conversely, in cases of combining jobs/positions, the nature of certain individuals may reveal a multiplicative effect on labor productivity due to mutual, variable ideological, emotional, financial, and other energy exchanges in performing different types of work, such as practice, scientific research, and teaching in fields like jurisprudence, philology and translation, programming, accounting, mechanical engineering, forestry, soil protection, and so on. Such cases represent the most valuable resource for employers, particularly within the didactic framework of educational institutions, ensuring the practical application of their theoretical knowledge.

The circle of such individuals is already covered by the requirements of anti-corruption labor law. The idea behind these requirements is to prevent the dissipation of public officials' energy beyond public interests and avoid conflicts of interest arising from secondary employment in the private sector. However, this idea is too narrow and superficial, given the context of its genesis and implementation. The reality of private-law relations regarding the non-registration of employees for positions or the formal underpayment of wages reveals that labor law requires

a significantly broader and deeper set of descriptive, sanctioning, and other rules in anti-corruption law to ensure workers' rights, unlocking its protective, delictual, and defensive potential.

The prevalence of political corruption in the public sector – executive, legislative, and judicial branches – is one of the main institutional factors in the escalation of the shadow economy (Yoo, p. 764). Nominally, issues of legal employment and wages are existential. A person survives and contributes to social progress through the money they earn. Therefore, this issue must be acknowledged in strategic legal documents of national significance. The deficiencies of entrepreneurs who deprive workers of their earned wages and contributions to pension funds and public budgets, as well as public officials who allow this, are matters of human virtues. Collectively, these issues of worker existence and their families correlate with the virtues of entrepreneurs and public officials in the complex relationships of profit creation, fiscal and budgetary policy, and social security.

Essentially, this constitutes the essence of the ternary composition of a nation's economic relations, where capital is created, accumulated, and distributed. The contradictions in these relations are not only critical – such as claims to public power, justice, and other social values – but also corruption-measurable. The resolution is determined by capital and is often found at the expense of satisfying private interest instead of public needs, for example, in the practices of unaccounted revenues in the shadow economy. Claims to unearned material benefits and/or services are also a subject of bribery, the allocation of such benefits for personal gain, and other forms of corruption. In this regard, the issue should at least be mentioned in the anti-corruption strategy. For instance, the current Anti-Corruption Strategy of Ukraine for 2021–2025 does not mention it. Moreover, the mechanism for ensuring legal employment and official documentation of real wages implies legal connections with institutions for neutralizing corruption, which should be properly detailed in legislative norms.

The intersection of labor and anti-corruption law in the outlined issues constitutes a matter of public interest. The state regulates

the labor market precisely because violations of labor rights present a natural temptation for employers who benefit from such labor. The elimination of the state from this process would return the nation to the problems of the late 19th century when it was proven that the possibility of further social progress directly depends on the formal legal definition, fixation, and actual protection of workers' rights.

The phenomenon of trade unions, which emerged in England in the 1770s–1780s and is now a traditional institution for ensuring workers' interests in most countries worldwide (Kasyan, p. 25), serves as evidence of the historical evolution and increasing complexity of the legal mechanisms for protecting labor rights. The protective function of trade unions lies in their comprehensive activities at any organizational level, aimed at preventing violations of labor and socio-economic rights of workers, as well as their restoration and protection (Tsessarsky, p. 40).

The globalization of labor, financial, trade, information markets, and related areas of public life has left no choice for states that would prefer to ignore workers' rights. Such states do not rank among the top countries in terms of human development, rule of law, or innovation indices, nor do they appear in any other rankings concerning the parameters of spiritual and material progress.

Moreover, public interest in this context is also reflected in tax law, as wages are taxed based on the officially recorded amount in company documents and the number of formally employed workers. A wage amount lower than what is actually paid reduces tax revenues to public budgets from such understated salaries or excludes them entirely if the worker is not legally employed.

The public sphere of pension law is also affected in these relations, as contributions from wages to state or municipal pension funds are either absent or understated. Consequently, the private interest of a working individual in this context becomes a private interest of pensioners and all others who receive funding from the public budget and/or use social infrastructure created at its expense – university-trained specialists, protection from external

threats by the army and police, roads, etc. Anything beyond the interest of a single individual is no longer private, especially when such an interest violates tax, pension, or administrative law. For example, in 2020, 36% of working Ukrainians received all or part of their wages unofficially, resulting in an estimated $33 billion annual shortfall in state budget and pension fund revenues (NBU, 2023).

The lack of integrity in an employer's desire to cheat and deceive for profit by not legally employing workers or by not formally recording actual wages is a major issue. Such employers are driven by flaws rather than virtues. The only legal domain where the concepts of "integrity" and "lack of integrity" are functionally key is anti-corruption law. Accordingly, its presence through these concepts in other branches of law should be sufficient to neutralize the studied problem using the combined instruments of criminal, tax, pension, informational, labor, and commercial law – both for citizens and for stateless persons and migrants. For example, among different outgroups susceptible to participation in informal economic activities and entrepreneurship ("shadow economy," "informal economic activities"), isolation, and marginalization, there are immigrants in the Netherlands, Mozambican immigrants in South Africa, and Pakistani immigrants in the United Kingdom (Yoo, p. 759–760). The role of anti-corruption rules regarding the legality of employment and wages is not merely supplementary to existing norms in other branches of law. They are on equal footing and ensure legal effectiveness through their combined force. For instance, the Criminal Code of Ukraine (April 5, 2001, No. 2341-III) does not contain specific provisions criminalizing these violations. These and other breaches of labor rights are covered by just six words at the end of the hypothesis of Article 172, Part 1: "other gross violation of labor legislation." However, the general and/or special preventive effect of this norm concerning the studied offenses is absent, as informal labor and wages accounted for up to 19.5% of the total labor market in 2021 and reached 35% by 2024 (State Statistics of Ukraine, 2021; Advanter Group, 2024). Meanwhile, in October 2024, the National Bank of Ukraine (NBU) recorded

the transition from shadow to official employment as a significant reason for the first increase in employment in Ukraine since 2022 (NBU, 2024). However, in September 2024, Ukraine's tax service recorded a decline in tax revenues of more than 27% – 110 billion UAH compared to nearly 152 billion UAH in August (SFS, 2024).

Distortion of fiscal redistribution negatively affects the key components of social security and governance, including poverty distribution and the preservation of an inefficient expenditure structure (Yoo, p. 752). Parliamentary fiscal initiatives that do not align with the tax and market capabilities of entrepreneurs threaten this security – the state of national development in which vital social interests are protected, a high quality of life and human potential development are guaranteed, and the integrity of the social system is maintained through the interaction of its structural components and the implementation of socially oriented state policy measures in accordance with progressive societal needs across all spheres of life and at all levels of national security (Polishchuk, p. 203–204).

Simultaneously, legally ill-conceived tax policy exacerbates issues related to informal labor relations and wages, yet shifts them beyond the realm of tort law, as it imposes obligations that are not based on the actual nature of economic profitability in entrepreneurial activity, presenting wishful thinking as reality. Determining the degrees of subjectivity and objectivity in tax burden and the actual capacities of entrepreneurs regarding wage payments and employee registration requires specification by industry, economic sector, region, business location, and even individual enterprises. This concerns the balance and rationality of legislative requirements, as well as the simultaneous supremacy of the rights of workers, entrepreneurs, and the rest of society, represented by public authorities in their tax initiatives. The more fiscal policy aligns with the nature of legal relations, the greater the responsibility of entrepreneurs for legal employment and wages, and vice versa.

Accordingly, the focus of anti-corruption law in eliminating corruption-related distortions of workers' legal rights shifts toward those who created these distortions, demonstrating their

misunderstanding of legal relations, greed, and/or other flaws – whether it be parliament, entrepreneurs, or both parties. Part of this issue could be addressed within the existing anti-corruption expertise framework for draft regulatory acts, but this would require, first, expanding the definition of corruption to include violations of legal employment and wages due to dishonest practices; second, balancing the responsibility between those who pass legislation that is objectively unenforceable and those who fail to comply due to their own shortcomings; and third, ensuring that scientifically substantiated conclusions are fully considered when drafting legislative acts. For example, in its review of the draft Law of Ukraine "On Amendments to the Tax Code of Ukraine Regarding Taxation During Martial Law" No. 11416-d dated 30.08.2024, the Main Scientific and Expert Department of the Secretariat of the Verkhovna Rada of Ukraine emphasized that the accompanying documents lacked justifications for its key provisions and the expected socio-economic, legal, and other consequences of the law's implementation, as required by subparagraphs 1 and 2, paragraph 1, Article 91 of the Parliament's Rules of Procedure. Specifically, there was no substantiation regarding: the proposed elements of taxes and fees (taxpayer, tax object, tax base, tax rate, tax period, etc.) and their impact on Ukraine's social and economic situation (economic growth, inflation, banking system stability, taxpayers' income, national economy competitiveness, economic shadowing, employment, workforce migration, and future budget revenues); as well as the inability to secure additional budget revenues from alternative sources (Conclusion on Draft Law No. 16/03-2024/2014-06, p. 3).

In some cases, institutions can influence firms' outcomes in the opposite way: they can incentivize companies to operate outside institutional frameworks. The dual nature of institutions – good rules that foster a healthy economic environment, on one hand, and poorly designed or ineffective rules that encourage non-compliance, on the other – helps explain the heterogeneous attitudes of firms toward the informal sector (Vallanti, p. 1383). Distortions in tax law regarding tax rate levels are verified by objective, rather than subjective, inability of employers and/or employees to pay

them. Otherwise, entrepreneurs lose market competitiveness, and workers lose their ability to recover and develop. Objective inability means that an entrepreneur has made every possible effort within the given social context to maintain business competitiveness: consulting available experts, exercising caution and responsibility in expenditures, etc. Subjective loss of competitiveness, on the other hand, indicates negligence in spending, management, or business development.

Financial top-level corruption related to wages, which would force employees to become initiators of wage underreporting, manifests in any coercive form of income withdrawal – such as mandating employees to purchase government bonds with a portion of their salary and/or imposing an interest rate on these bonds that further reduces their already low income. This leads employees into poverty even more quickly and reliably than unofficial employer payments. The only ethical and legal approach in this financial-labor arrangement is to incentivize such purchases by offering a share of real future income, linked to the currencies of economically strong countries. Applying decomposition methods to systematize the causes and consequences of shadow employment, considering modern trends (Polishchuk, p. 203), and investigating the epistemological foundations of knowledge regarding "illegal employment and wages" have allowed researchers to account for the synergy, specificity, and multidimensionality of these concepts (Sand, p. 6, 19). Comparing these violations to bribery and other classic corruption offenses based on their consequences demonstrates that they all harm the public interest for private gain. However, unlike such offenses, in the studied model, the employer and/or employee do not hold public authority, except in cases of deep corruption practices, where public-sector employment relationships are not formalized, or work is assigned to others due to corruption-based obligations or nepotism/favoritism (Sarkar, p. 158). In such cases, remuneration is given to designated individuals rather than to those who actually performed the work. Therefore, public authority features in the corruption characteristics of illegal employment and wages only indirectly, namely: 1) as what is known as a predicate offense,

a legal diversion – essentially unlawful actions by public authorities that triggered or facilitated these crimes; 2) as actions by public oversight bodies that failed to eliminate violations of workers' rights related to official employment and wages, thereby negatively affecting the public interest. The flaws in these forms of public authority distortions, combined with their correlation to dishonesty and severe harm to the public interest (tax evasion, shadow employment, etc.) in at least four spheres – labor relations, taxation, social security, and fair economic competition – against the backdrop of ineffective tort norms in criminal, administrative, and other legal fields, reveal the corruption composition of these offenses. These are countered by the law enforcement power of anti-corruption law, which operates in conjunction with existing tort law as part of a unified legal mechanism.

Thus, the legality of employment and wages within the anti-corruption legal framework represents a state of legal relations achieved through the coercive power of criminal, administrative, tax, pension, and labor law. This framework is aimed at neutralizing dishonest employer actions related to the consumption of financial and other resources generated by their employees' labor, which rightfully belong to them in terms of legally defined wages and other legislatively guaranteed financial resources. The legal core of these relations lies in the attribution model of a system of rules that formally balance the interests of employers and employees, as well as their collective interests with the public interest and its representation by public authorities.

2.2. Combating Corrupt and Financial Crimes of Entrepreneurs Using Information and Communications Technology

Fictitious transactions – conducted without the intent to create legal consequences arising from the transaction – are a common type of violation of public interest in commercial and other civil property relations. Alongside them, sham transactions are carried out by parties to conceal another transaction that they actually

performed. In practice, tax and customs authorities play a key role in safeguarding public interest in both types of cases. The most effective methods employed by these authorities remain desk audits (conducted without any inspection order, as part of routine work involving analysis, comparison, and other ways of examining existing business reports), documentary audits (scheduled or unscheduled; on-site or off-site), and factual audits verifying the accuracy of accounting records of business operations.

However, sometimes tax authorities perceive a public interest where none exists – overstepping their jurisdiction and interfering with private interests. The reasons and/or motivations for such misjudgments can be corrupt, dogmatic, naive, or other distortions of legal reality. Every legal instrument in the anti-corruption landscape is teleologically designed for a clear purpose. However, in a deeply corrupt environment, the functionality of anti-corruption institutions becomes questionable. Their dysfunction lies in the fact that experienced corrupt officials exploit these institutions for personal gain – but in more complex schemes of corruption-driven relationships. For instance, a supervisory board or audit commission, intended to monitor an organization's governing body, may instead become an instrument for extorting money and/or resources from managers. The key condition for such a scheme is ensuring that a close associate of the corrupt official (a friend, longtime corruption accomplice, etc.) is included in the supervisory body. Another example: one person cannot hold leadership positions in two companies participating in public procurement tenders – as this creates a conflict of interest and prevents genuine competition. Corrupt officials circumvent this by formally replacing the director of one of the companies, ensuring that, on paper, corruption does not exist, while in reality, it remains intact.

Further corruption schemes include:

1) artificially lowering inflated prices in public procurement tenders – but with an informal agreement with the contracting authority, involving a bribe to overlook quality control;

2) winning public procurement tenders through bribery, where the funds for bribing the contracting authority are embedded

in the price of goods/services, and other participants, though seemingly independent, are actually accomplices of the winning bidder.

All examples of corruption highlight the boundaries of anti-corruption infrastructure, which depend on the intentions of the population – primarily those concentrating political and/or economic power. Clearly, a system of absolute oversight, where everyone is monitored at all times, is impossible. Typically, oversight is two- or three-tiered:

1) internal control within an organization;
2) external control by auditors, higher-level administration, etc.;
3) specialized anti-corruption bodies, ranging from agencies to courts.

As noted in legal literature: "Non-cash or non-goods transactions must be detected during internal control and/or audit" (Vladimirova, p. 142). However, "audited financial statements, high credit ratings, a history of regulatory compliance, and internal controls do not necessarily make counterparty credit risk more transparent, nor do they provide timely warnings to investors. In cases of misconduct or breaches of fiduciary duty, regulations and internal controls prove insufficient to protect investors from losses" (Belmont, p. 15). As tax bureaucrats prioritize bribes over efficiency, they provide services not to the most effective producers but to those offering the highest bribes – thus distorting resource allocation and causing transaction delays for additional payments (Torgler, p. 113, 125, 138).

"Sustaining reforms requires long-term political and administrative improvements" (Dom, p. 302). Thus, if politicians and entrepreneurs lack the will to act in the public interest, then no complexity or scale of anti-corruption infrastructure will resolve the issue. On the contrary, as corruption persists, parts of this infrastructure become engulfed in corruption themselves. In such an environment, businesses evade taxes by inflating expenses through fictitious agreements and non-goods transactions. They do so freely, leveraging corruption to buy off tax officials, national security officers, prosecutors, judges, and others. High levels of corruption correlate with the rejection of the social norm of tax

obligation. For example, while religiosity positively influences tax morale, corruption fosters an underground economy. Widespread corruption undermines taxpayers' trust, making them feel deceived about how their tax burden is spent. Additionally, when corruption is prevalent among tax administrators, a "moral displacement effect" arises, whereby honest officials feel pressured to conform to corrupt practices.

Countering tax (customs) authorities' mistakes often involved challenging their misinterpretation of financial transactions. For example, tax officials wrongly classified prepayments under supply contracts as "financial aid". Many disputes revolved around claims of non-goods transactions and fictitious agreements. Entrepreneurs often concealed the true nature of transactions even from their own lawyers – though over time, compliance experts within legal teams became adept at deciphering such schemes without requiring full disclosure.

In this regard, the case from my legal practice concerning the recognition of the illegality of two decisions made by the customs service in the Zaporizhzhia region (Ukraine) in 2011 proved to be highly informative. The customs officials issued two documents: one imposed a VAT payment on the company (equivalent to $24,000 at 2011 prices), while the other imposed a fine on the company (equivalent to $12,000 at 2011 prices) for non-payment of this tax. The company approached me for legal assistance, and I successfully proved the illegality of these decisions in judicial administrative proceedings, the history of which can be briefly described as follows. In 2008, customs officials classified the shipment as a disassembled milling plant manufactured by Alapala Makina Gıda San. ve Tic. A. Ş. (Istanbul, Türkiye). Customs had cleared the goods with zero VAT, confirming that the importer had met all legal obligations. However, in 2011, the same officials reclassified individual components of this milling plant as separate standalone mechanisms, arguing that they could function independently outside the milling system. By this logic, any machine could be arbitrarily reclassified into parts – even a $300 million warship could be deemed a mere storage facility for firewood or grain. Despite the absurdity of the reclassification,

it required extensive legal proceedings to prove its illegality: 1) two lawsuits, two cases, multiple judges, assistants, and clerks; 2) an expert commodity evaluation; 3) multiple customs representatives over time; 4) a single legal representative handling both cases for the plaintiff. The illegality of these customs decisions, established by the judges, cost the state budget the losses incurred in the legal proceedings. Additionally, the public budget had to cover expert examination costs. The reputational damage to public authorities – both domestically and internationally – further harmed the public interest. This case exemplifies inefficiency, which hinder economic growth and investor confidence.

Sub-institutions of fictitious, pretended and other fraudulent transactions are ontologically a phenomenon of criminal law in civil relations. This is part of its sub-branch of "fraud," where the main motive of the perpetrator is to acquire material goods from others through deception. "Fraud is a situation where the victim emerges as a result of being subjected to various forms of deception and misleading behavior; ... an agreement, proposal, or other activity that, in one way or another, has dubious value or reputation; ... a trick or ruse related to trust, as well as a means to obtain (something) from someone through plausible deception; ... an act of persuasion based on misrepresentation... error – a leadership or deceptive business practice when one receives unwanted or unsolicited contact and false promises are made... Fraud can take various forms" (Schaper, 2012, p. 334–335, 353). The variability in the details of the method of commission and the object of the fraudster's attack determines the types of crimes, their compositions within sub-institutes (bribery, actual conflict of interest, etc.), and institutions of criminal law (corruption, fraudulent null transactions).

The existential challenges repeatedly posed by malicious business intentions within these sub-institutes are predominantly a problem of commercial law, where norms regulate relationships concerning the creation of added value and profit. Outside of entrepreneurial interest, this institution remains an issue but does not reach the level of a national security threat in terms

of such violations of a nation's economic interests that would preclude its further reproduction and development.

The Supreme Court has determined that the will of the parties reflected in a fictitious transaction is merely imitated and is not confirmed by legal reality, where their true will and intentions, which are concealed, are expressed. Accordingly, when entering into such a transaction, the parties are aware in advance that it will not be executed and will not have the legal consequences reflected in it, except for public-law tax consequences arising from such a transaction, as the nation, represented by the tax service and other authorized public authorities, has been misled regarding the actual circumstances of the transaction and the true intentions of the participants (rulings of July 18, 2018, in case No. 750/2728/16-c; July 3, 2019, in case No. 369/11268/16-c). Non-goods transactions are a divergent feature of fictitious business transactions.

Evidence of the non-goods / unreal nature of fictitious transactions includes the lack of suppliers' physical resources (e.g., agricultural land of sufficient area for growing products in the supplied volumes), technical and technological conditions, qualified personnel objectively necessary for the supply of sunflower seeds to the taxpayer; the absence of employees and transport means among carriers specified in waybills; defects in the content of primary documents issued for business transactions; the absence of a real (legal) source of seed origin, for the supply and transportation of which documents were drawn up (lack of genuine formation of this asset). Certificates of quality (compliance) are not primary documents concerning the business transaction of acquisition (supply). All these facts make it impossible to verify the supply chain from counterparties directly to the taxpayer.

Conversely, when combined with other evidence, the reality / materiality of commercial transactions is confirmed by business contracts (purchase-sale, supply, transportation, warehouse storage, etc.) and their annexes (specifications, acceptance certificates for work / services, etc.), warehouse receipts, waybills, expense invoices, tax invoices, payment orders, and other reliable primary accounting documents drawn up for business transactions within

these contracts and based on which the taxpayer's accounting and tax records were formed in accordance with applicable laws. Proving the inaccuracy of any of these documents, the taxpayer's awareness of the inaccuracy of supplier data in primary documents forming the tax accounting indicators of income and tax credit, and/or the absence of a real source of goods origin is the responsibility of the controlling authority. This is the work of the fiscal service to verify the compliance management of entrepreneurs with the requirements of legislative acts.

References to information about third parties with whom the taxpayer had no contractual relations and for whose activities it bears no responsibility are improper evidence (rulings of the Administrative Cassation Court of the Supreme Court of May 5, 2023, in case No. 160/15514/20; February 16, 2023, in case No. 804/27/17) (p. 23, 28). Fictitious foreign economic operations, document falsification, issuance of fictitious invoices, use of non-existent foreign partners, sale of goods and material assets at prices below purchase cost, and non-goods transactions lead to illegal VAT reimbursement and, consequently, significant losses to the state budget (Filio, p. 43). The shadow economy, which thrives on shell companies, straw persons, and non-goods transactions, requires immediate intervention by state institutions (Voytovych, p. 226). The primary responsibility for eliminating threats to the nation's economic interests lies with fiscal authorities (customs officers, tax officials), auditors, and, considering the scale, economic and national security agencies (hereinafter, all agencies with this function are referred to as tax/security authorities). The nomenclature for such agencies is a purely technical and insignificant issue. They may be repeatedly renamed as the "revenue and duties authorities," "tax service," "fiscal service," "auditors," etc. Organizationally, it is equally irrelevant whether they are called a "bureau," "police," "militia," "investigative service," "department," "detectives," etc. Statements by top government officials about abolishing such agencies only harm law and order, legality, and the rule of law, as the agency functionally remains the same – only its name changes, and sometimes, though always partially, the staff, uniforms,

vehicles, insignia, slogans, and greetings are altered. Focusing on such technical matters rather than on functional purpose and organizational effectiveness constitutes criminal sabotage, which in no way addresses the problem of lost public revenue due to corporate fraud schemes. For example, the legally inaccurate name "Bureau of Economic Security of Ukraine," tasked with counteracting offenses affecting the functioning of the state economy under Article 1, Part 1 of the Law of Ukraine "On the Bureau of Economic Security of Ukraine" of January 28, 2021, No. 1150-IX. Even less clarity is provided by the absence of a definition of "economic security," either in this law, the Law of Ukraine "On National Security of Ukraine" of June 21, 2018, No. 2469-VIII, or any other law.

It is hard to imagine that the Ukrainian nation will feel economically secure when no offenses are committed, but there are also no innovations, digital technologies are introduced more slowly than in other nations, and entrepreneurial skills are insufficient. It would be beneficial for this bureau to understand its identity, how it defines itself within this concept, and what is included in the scope of "the functioning of the state economy," as well as its place in the digital program environment, where "Broad digital skills should build a society capable of detecting disinformation and fraud attempts…" (para. 4, sec. 3.1) (EU 2030 DC). Currently, the essence of such a security function appears to be no more than a "Bureau for Countering Economic Crimes." The absence of a legally formalized subject of activity for the "Bureau of Economic Security of Ukraine" precludes the creation of legal algorithms for combating fictitious, sham, and other fraudulent crimes that could be embedded in software codes for verifying and preventing these crimes and ensuring their inevitable punishment. These legislative shortcomings are particularly detrimental to the nation in the context of AI active spread and other ultra-fast processes of "the digital economy, characterized by the implementation of innovations and information-communication technologies in commercial activities…" (Konovalova, p. 37, 38).

If the concept of "economic security" is not exhausted by "counteracting offenses that infringe on the functioning

of the state's economy," then there must be someone else responsible for safeguarding economic interests. In addition to the national security agency and other law enforcement bodies – which, given Ukraine's loss of economic potential since 1990, have often been complicit in this loss or ineffective in preventing economic crimes with socially dangerous consequences on a national scale – economic security is also the responsibility of the Antimonopoly Committee and public administration. At the very least, these include agencies for economic, agro-industrial development, and finance. The first two are in stark contradiction to the latter, as, for example, the Ministry of Economy's mission is to maximize entrepreneurship, ingenuity, and business acumen, creating conditions to attract capital, innovation, and other investments into the country. In other words, it fosters a favorable environment for entrepreneurs. Without this, added value, profit, competitiveness, material wealth, and all other components of economic security do not exist. Meanwhile, the Ministry of Finance, with its tax authorities, is solely focused on collecting as many taxes and fees as possible from all these entrepreneurs, whose emergence was facilitated by the adept work of the Ministry of Economy, agro-industrial development agencies, and so on.

The work of public authorities in verifying fictitious transactions falls within the scope of the metaconcepts of "compliance management" and "law enforcement compliance," including cooperation with international partners. For example, between September 1, 2023, and September 3, 2024, Ukraine established 21 new joint investigative teams (JITs) with foreign states, including 15 with EU member states (EU Commission, p. 46). The directions of law enforcement compliance correspond to types of entrepreneurship (in finance, production, online and other types of trade, etc.), as well as to types of corruption-related distortions (unfair competition, fictitious, sham, and other fraudulent transactions) based on the object and/or method of committing the offense. The volume of data associated with such commercial activity offenses grows exponentially and multiplies in cyberspace. Temporally, data coverage is not limited: the longer

the analysis period, the higher the probability of tracing corruption distortions based on financial, familial, friendly, or other social ties. Consequently, effective counteraction to economic offenses, in terms of ensuring national economic interests as part of national security, is now determined by the pervasive use of machine learning, deep learning, large language models, and other AI subsets. Among such digital innovators, leading the way are typically entrepreneurial structures that, for instance, achieve "efficiency in managing inter-firm relationships through the use of appropriate management control systems (MCS) and transaction cost economics (TCE)" (Reusen, p. 22).

The scope of data covered by existing state registers correlates with the scale of programs used by tax authorities to detect fictitious transactions. Almost always, such work will have a law enforcement or coercive content, rather than a legal-protective or legal-preventive effect, as it occurs after fictitious transactions have been carried out by entrepreneurs, meaning these offenses cannot be prevented. This information is absent from existing data registers and cannot be present, as it is obtained from corporate reporting documentation. Clearly, fictitious transactions become a source of illicit enrichment for entrepreneurs, but controlling the sources of their wealth is more complex than compliance monitoring of income versus expenses for public officials. Unlike them, entrepreneurs are primarily motivated by profit maximization. The difficulty in verifying various types of formal and/or actual business transactions lies in distinguishing: the first type, which excludes fraudulent (fictitious, sham, and similar) transactions and/or other legal violations; the second type, which includes such transactions and/or other legal violations.

The focus of legal norms and their skillful application is to ensure that such enrichment does not occur at the expense of public interest or through violations of existing legislation. Tax authorities detect entrepreneurial fraud in non-compliance with fictitious transactions through "transaction costs on goods search, commercial relationship establishment, contract conclusion, and contract performance monitoring" (Fragomeni, p. 99). Among the methods for detecting entrepreneurial fraud, besides effective coercion, incentives

remain relevant, such as helping taxpayers engage in dialogue and negotiations with the state, thus increasing the likelihood that taxation extends beyond mere enforcement and contributes to strengthening the social contract and broader welfare (Dom, p. 303).

The useful database aiding in preventive efforts against fictitious transactions is the judicial decisions registry, where cases of entrepreneurs' participation in such transactions have already been documented. These data do not allow for a definitive conclusion that these entrepreneurs inherently engage in fictitious transactions for personal enrichment. However, such facts provide sufficient grounds for forming operational certainty and law enforcement vigilance, eliminating false illusions and counterproductive assumptions among tax investigators regarding these entrepreneurs. In nations with large-scale, complex, and deeply embedded corruption networks, such investigators often become involved in fraudulent schemes: for illicit benefits, they warn entrepreneurs of searches, share operational information and investigative secrets, and otherwise help them evade legal responsibility for fictitious transactions.

Fictitious transactions are a form of tax evasion, an indicator of the shadow economy, and a distortion of fair economic competition-phenomena closely related to corruption, which in turn exclude social security, innovation, digitalized information systems, global competitiveness, and economic progress. Obsession with these perversions of entrepreneurship fosters economic ties only with nations that reproduce a similar level of economic offenses and remain perpetually behind innovative economies governed by the rule of law. "There is a strong statistical correlation between the intensity of socio-economic ties and the competitiveness of companies" (Fragomeni, p. 107). For example, such practices have been justified for decades by politicians and entrepreneurs in Ukraine to rationalize their self-indulgence, inertia, and minimal effort, preferring cooperation with corrupt post-Soviet states and similar economic environments rather than pursuing healthy innovative ambitions aimed at highly capitalized competitive markets in the EU, the USA, Japan, Singapore, and others.

As a form of financial liability, the following should be legislatively required from such entrepreneurs: a) 10% salary bonus for each employee for every court ruling confirming the entrepreneur's involvement in a fictitious transaction; b) a 10% surcharge on medical services for the entrepreneur and their family members; c) a 10% monthly levy on the fictitious transaction amount, paid into a fund for digitizing the criminal justice system for 1–5 years. All these sanctions should be specified in the court decision recognizing the transaction as fictitious, thereby strengthening the preventive function of the law concerning "these pleasant stories backed by accounting fraud" (Krugman, p. 131).

The aforementioned is also among the EU's crime-fighting priorities: identifying and dismantling high-risk criminal networks operating in the EU, such as mafia-type, ethnic, and family organizations, as well as other structured networks and key individuals within them – particularly those that undermine the rule of law through corruption, engage in violence or intimidation, use firearms to advance criminal goals, and launder criminal proceeds through underground financial systems (Clause 1). Combating criminal networks and individuals involved in financial crime and money laundering, as well as facilitating asset recovery through effective confiscation of criminal profits – specifically by supporting the automatic initiation of financial investigations, fostering a culture of asset recovery through training and financial information exchange, and targeting money laundering syndicates that offer laundering services (including money mules and trade-based money laundering) and criminal networks that widely use new payment methods for laundering illicit funds (Clause 7(e)) (EMPACT).

Thus, entrepreneurs' agreements involving non-existent transactions constitute a type of fictitious transaction and fraud, where the nation itself becomes the victim, as public interest is undermined by private entrepreneurial interests. The essence of the violation is that, according to the country's existing legal requirements, entrepreneurs not only had no right to their private interest in obtaining VAT refunds from the state budget and evading corporate tax payments, but also naturally could not have

such a right, as they pursued it through distortions of natural law expressed in the formally defined legal reality of state legislation. The managerial non-compliance of fictitious transactions lies in actual company managers (those truly responsible for enterprise governance) violating the principle of good faith concerning public interest and exceeding their authority.

2.3. The Role of Artificial Intelligence in Eliminating Predicate Crimes Related to the Legalization of Corrupt Proceeds and Terrorism Financing

In the cybernetic world, criminal investigations are complicated by the speed and volume of transactions carried out by criminals, the physical presence of participants and hardware across different jurisdictions, further emphasizing the need for international cooperation among law enforcement agencies. For example, in 2021, joint operations involving law enforcement agencies from Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (National Crime Agency), and the United States (Drug Enforcement Administration, Federal Bureau of Investigation, Internal Revenue Service), supported by Europol through special operational analysis and coordination of cross-border cooperation, successfully dismantled the illicit shadow market in the hidden internet network "DarkMarket." This platform had 500,000 users, over 2,400 vendors, more than 320,000 transactions (mainly involving all types of narcotics, counterfeit currency, stolen or forged credit card details, anonymous SIM cards, and malware), and processed over 4,650 bitcoins (BTC) and 12,800 monero (XMR – a blockchain-based cryptocurrency using the CryptoNote protocol), amounting to over €140 million at the time of the investigation.

Hiding unlawfully acquired assets within corrupt national jurisdiction is easily exposed and even more easily confiscated because deep-rooted corruption undermines the rule of law. The supremacy of property rights is also negated by corruption. The illegality of an asset only exacerbates its vulnerability

in a corrupt nation that has chosen deception, violence, and private gain at the expense of public interest over legal standards, distorting natural law (Lat. male parta male dilabuntur – "ill-gotten gains are soon lost"). The effectiveness of law enforcement efforts within foreign jurisdictions requires more time than equivalent efforts within national legal frameworks. Classic management tasks related to the drafting, review, approval, coordination, and execution of criminal procedural documents at the international level at least double in complexity, as they must be integrated into the legal and procedural framework of the recipient country. Language barriers further slow down this work, such as interactions between representatives of Eastern and European languages. The digitization-driven efficiency of pre-trial investigations into money laundering cases requires the involvement of software specialists and cybercrime experts, particularly in darknet marketplaces, virtual asset exchanges, and AI-powered covert networks, illustrating how "technology becomes a useful servant but a dangerous master" (C. L. Lange, 1921) (Pavlidis, p. 162).

National cultural determinants of work styles, political dynamics in transnational and regional relations, and global financial, commercial, and policy factors impact the course and outcome of anti-money laundering efforts. For example, a 1% increase in digitalization correlates with a 0.30% increase in financial services market regulation and a 0.93% improvement in law enforcement capabilities. However, for instance, recent institutional, investment, tax, and educational reforms in Ukraine aimed at countering money laundering have not yielded significant improvements in preventive, communicative, or punitive measures. There has been no observed increase in the number of convictions or recovered funds returned to the state budget. Research shows that the time from the initial commission of a crime aimed at laundering illicit proceeds to a court-issued guilty verdict often spans years (Mynenko, p. 159, 160, 162, 163). Tracking illicit proceeds requires identifying assets from their criminal origins through all mutations, if any, to their final form at the time of detection. During such mutations, illicit funds mix with legally acquired resources, potentially decreasing

in amount, increasing in number, or appreciating in value. Corporate intelligence research (CIR) serves as a crucial tool for global intelligence gathering (Pieth, p. 23, 112).

Pre-trial investigations in these cases take into account the private interests of "corporate finance, financial markets and intermediaries, and government," which they affect; these interests span "real estate, financial flow geography, financial centers and networks, financial technologies (FinTech); their impact on financial equality, its connection to social justice, crises, and responsible investing," as well as macroeconomic indicators. Also involved in these interests are "transnational consulting and accounting firms," rating agencies, insurance companies, and others (Grandi, 2019, p. 15). For instance, money laundering via FinTech entrepreneurs or their involvement in terrorism financing necessitates law enforcement agencies (financial intelligence units) to work with algorithmic programs, big data, AI, and machine learning (ML), which stand out for their unparalleled innovation (FATF, p. 57, 58). Accordingly, identifying financial crimes within FinTech transactions and operations is an extremely challenging task without involving specialized information technology (IT) experts.

Achieving pre-trial investigation objectives may be even more difficult if money laundering schemes involve public officials (persons with top executive functions), meaning organized crime has a mafia (oligarchic) structure and/or if these officials represent financial centers at national or global levels, including leading investment companies, systemically important banks (EBA, 2024), and/or if digital technologies and AI have been utilized. Consequently, on the international stage, countries without global financial centers, with peripheral or semi-peripheral financial systems, yield to the interests of dominant financial hubs, where corruption risks exist on a global scale, and the legal interests of weaker parties do not outweigh the unlawful interests of stronger ones.

"The banking and financial sector has a long history of wrongful and unethical conduct, as well as scandals that have tarnished the reputation of traditional financial institutions. Examples include

market manipulation, insider trading, financial product abuse, money laundering, the Libor (London Interbank Offered Rate) scandal, and the mortgage crisis. This has led to public distrust and increased regulatory scrutiny. Every year, financial market misconduct affects around 15% of publicly traded companies, resulting in substantial fines for price, exchange rate, and interest rate manipulations, which can significantly impact organizations" (Brogi, 2024). This is particularly relevant in cases involving corrupt earnings of political and economic elites or when illicit proceeds cross borders. A state's response to corruption and the transnational movement of illicit proceeds is not always easily activated or coordinated (Pieth, p. 24). For instance, the dynamics of criminal proceedings related to money laundering, terrorist financing, and the proliferation of weapons of mass destruction over the past 14 years in Ukraine are illustrated in the chart (Figure 2) (Prosecutor's Office reports).

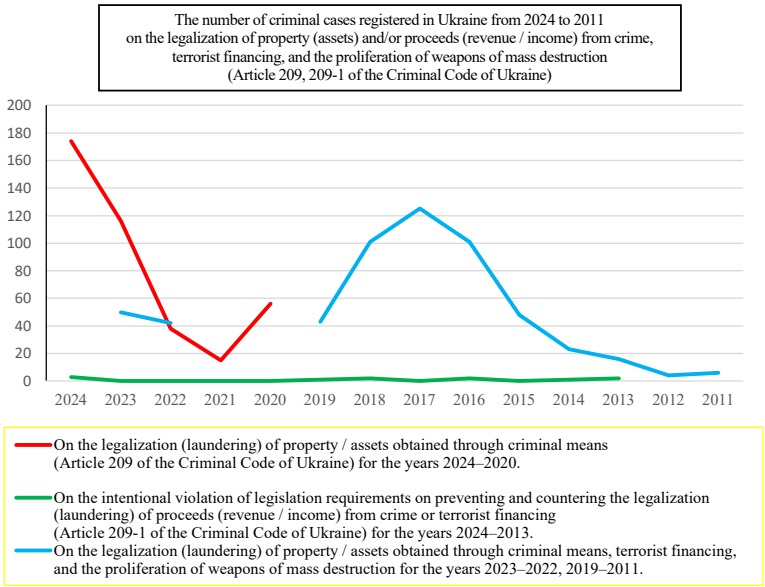

Figure 2: Diachronic Analysis Chart of Criminal Cases Related to Money Laundering and Terrorism Financing: The Case of Ukraine 2011–2024

The data from the graphs demonstrate that the specialization of the law enforcement agency in economic crimes, represented by the Bureau of Economic Security, has enabled an increase in the number of detected crimes related to the legalization of proceeds from crime, terrorist financing, and the proliferation of weapons of mass destruction since 2022. During the full-scale war of external aggression against Ukraine, the number of such cases has increased tenfold. This growth is partly explained by the actual ability to neutralize corrupt high-ranking officials (oligarchs) who, before the war, obstructed the detection and/or investigation of these crimes and concealed them.

Criminal law provisions against money laundering are highly sensitive to the accuracy and completeness of legal formulations. Another divergent feature of these provisions is the extensive set of rules required to describe violations of natural law, exceeding the scope of any other norms whose violation results in financial gains. The content of tort and criminal procedural legislation, which allows for the elimination of assets obtained through corruption and other crimes, reflects both the concepts used to define these crimes and its own legal constructs that directly implement legislative requirements to counteract any actions related to financial transactions or deals involving criminal proceeds. These actions include attempts to conceal or disguise the illicit origin of such proceeds, their ownership, the rights to such income, their sources, location, movement, transformation, as well as the acquisition, possession, or use of proceeds derived from crime. This is outlined in Article 5 of the Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction" of December 6, 2019, No. 361-IX.

By using the terms "proceeds from crime" and "illicit origin of such proceeds," the legislator designates income obtained as a result of predicate crimes – criminal actions that precede subsequent offenses that legalize these proceeds. The use of both terms is redundant, as the second encompasses the first. According to paragraph 1, part 1, Article 209 of the Criminal Code of Ukraine,

as of April 5, 2001, No. 2341-III, the legalization (laundering) of proceeds from crime involves the acquisition, possession, use, or disposal of assets where factual circumstances indicate that they were obtained criminally. This includes financial transactions, deals involving such assets, their movement, transformation, or any actions aimed at concealing their origin, ownership, rights, source, or location, provided that the individual involved knew or should have known that the assets were obtained criminally, either directly or indirectly, fully or partially. There is no other definition of "counteraction to the legalization (laundering) of criminal proceeds" in Ukrainian legislation. The existing definitions are characterized by pleonasms and inaccuracies typical of Ukrainian legal terminology. The most precise and exhaustive formulation would be: "criminal assets" or "assets obtained as a result of crime."

"The divergence between terrorist financing and money laundering lies in the fact that money launderers focus primarily on retaining and accessing criminal proceeds, whereas terrorist financiers aim to channel initially clean funds into the hands of those supporting their ideological or religious beliefs through direct financing of violent acts, training activities, propaganda, or travel. Terrorist financiers prioritize the direct use of the banking system and the speed of fund transfers for their operations" (Pieth, p. 81). The use of virtual assets – also known as decentralized digital currencies or cryptocurrencies – as a means of laundering criminal proceeds and/or financing terrorism and wars is countered by the Travel Rule for virtual asset transfers established by the Financial Action Task Force (FATF). These rules require exchanges and other virtual asset service providers (VASPs) to collect information on senders and recipients of such assets, obtain licenses, and comply with a range of legal requirements (Takei, p. 784).

Counteracting the legalization of criminal proceeds is carried out by a responsible public authority through the verification of accounting documents, both in paper and electronic form, for signs of fictitious transactions, substitution, or fraudulent economic operations. The recording of transactions in accounting records that did not actually occur constitutes the essence of a fictitious

contract. For example, recording all supply transactions for goods that were never actually delivered while payments were made from the buyer to the supplier. The buyer benefits from such fictitious transactions by receiving the full value of the supply, minus a 3–16% fee to the supplier for participating in the scheme, and from the subsequent refund of value-added tax from the public budget.

The actual execution of actions other than those reflected in accounting records constitutes contract substitution (falsification). For example, the actual trade of contraband alcoholic beverages, clothing, or other officially unregistered goods, or with only partial accounting recognition through receipts from the cash register and/or other documents (receipts from Latin "quittantia," German "Quittung," etc.), represents a substitution of commercial operations in terms of volume. The substitution of contract content is expressed in the accounting of income from rental services, transportation, or repair work instead of the indicated trade. Both types of such substitution together form a combined type of this financial fraud. The actual execution of actions other than those reflected in accounting records to conceal another contract constitutes a sham contract.

All three types of the above-described operations are forms of fraud – deception of the nation, represented by its authorized public authorities (regarding taxes, legitimacy of profits, etc.), concerning both the actual tax base (income) and the volume of resources available to the parties to the contract. This is achieved by making changes to accounting documents of business transactions, deliberately providing incomplete or inaccurate information about agreements, obligations, and/or assets to seize funds from public funds (state and local budgets, pension funds, social insurance funds, etc.) in the amount of taxes (fees) that the organization evades paying through such deception. The described crime represents a fraudulent method by entrepreneurs to evade fiscal payments, as well as to misappropriate funds (removing them from official accounting) and/or launder unregistered resources; profits from drug trafficking; funds obtained as a result of tax, corruption, and/or other crimes.

To achieve their goals, perpetrators use various tactics and methods. For example, they employ different persuasion and influence strategies, such as deception, lies, bribery, persuasion, pressure, aggression, or threats (Saks, p. 12). In the legislation of foreign countries, fraud is associated with overarching characteristics such as deception (fraud, lies, a promise made without any intention of fulfillment, mere silence, other fraudulent measures, etc.) and the acquisition of another's property (property rights) as a result. Examples include fraud complicated by arson or ship sinking, fraud with checks and promissory notes, fraudulent documents, money transfers, phishing, etc. Certain qualifying elements of fraud are universal in the criminal laws of both foreign countries and Ukraine (complicity, multiple instances of fraud and other property crimes, socially dangerous consequences, and methods of commission). There are also unique national qualifying elements of fraud, such as its impact on essential goods, commission through signature forgery, manipulation of electronic documents, influence on assets that are part of artistic, historical, cultural, or scientific heritage, etc. (Chaika, p. 236).

Money laundering activities are associated with various types of crimes, and effective detection of such activities significantly contributes to the prevention and prosecution of these crimes. There are several categories of money laundering, including the use of real estate, gambling, and businesses to conceal the true source of funds (Zand, p. 1). Computer forensics typically employs a systematic approach to extracting large volumes of electronic information. Traditional data mining methods, such as association analysis, classification and prediction, cluster analysis, and outlier detection, identify patterns in structured data. Newer methods, such as semantic analysis, recognize patterns in both structured and unstructured data. In a semantic network, data is defined, stored, and linked in a way that ensures more accurate search and retrieval of information, contextual ranking of search results, and integration with other systems with increased relevance (Pieth, p. 79–80).

The United Kingdom, EU countries, China, and other highly developed nations widely use information technology to prevent

crime, specifically: 1) mapping criminologically significant information for visualizing and analyzing crime patterns; 2) online analysis of digital images obtained from high-resolution surveillance cameras; 3) using cloud technologies for collecting, analyzing, and storing operational information received from various sources, including online video footage from the public about committed crimes; 4) monitoring information on social networks; 5) increasing public legal awareness regarding public safety and crime prevention through the Internet; 6) enhancing public communication with the police, including developing programs for citizens to quickly submit online crime reports (E-Watch) regarding street crime, public places, and educational institutions (Chaika, p. 85–86). The Ukrainian government uses the software and hardware complex "Safe Country". This is dedicated to working with data (processing, analysis, search, storage, centralized monitoring, and management) of video cameras at central, regional, and local levels, metadata, archives, event notifications, and other related information in real-time in Ukraine. It is currently designed as the next functional subsystem of the Unified Information System of the Ministry of Internal Affairs (MIA), in accordance with the Regulation "On the Unified Information System of the Ministry of Internal Affairs," approved by the Cabinet of Ministers of Ukraine on November 14, 2018, No. 1024. Among the expected results of the implementation of this e-complex are increased efficiency of law enforcement agencies at all levels, fraud prevention, and reducing the threat of terrorist attacks, among other benefits (MIA, p. 7).

Networks composed of interconnected physical devices with embedded sensors, along with software that enables data transmission and exchange between the physical world and computer systems in an automated manner using standard communication protocols, also enhance efforts to counter money laundering and terrorist financing. These include data assessment, generation, and transmission systems (Internet of Things / IoT), such as point-of-sale (POS) systems, ATMs, and mobile wallets. Their data flow facilitates a faster response to suspicious illegal activities, allowing financial monitoring entities and/or criminal justice authorities to promptly detect, block, and control

criminal transactions, prevent the legalization of criminal funds, terrorist financing, war funding, espionage, etc. The integration of the "Internet of Things" with criminological and forensic solutions for combating these crimes is an essential part of compliance procedures in financial management and organizational adherence to legal regulations (FATF, p. 57; AML).

The use of successful U. S. experience in crime mapping is becoming a promising approach for many countries. Crime mapping involves the collection of data on crimes related to assaults, thefts, illegal use of weapons, vandalism, and other offenses. The information is open to the public and is based on data provided by law enforcement agencies and media sources. Anyone can access these maps and register for free crime alerts via email and SMS. Email alerts, in particular, contain information about the map and crimes that have occurred in a specific area. In the U. S., private companies are involved in this process, such as SpotCrime.com (Chaika, p. 87–88) (Towson, Maryland 21204, US). Established in 2007, it is the largest crime data geolocator in the U. S., aggregating and mapping data from police departments and verified crime news reports onto Google Maps and other application programming interfaces. SpotCrime sends notifications via email, Facebook, Twitter, SMS, RSS, and multiple other platforms to provide the public with the most accurate and timely geocoded crime information (Suszan, 2014).

The Virtual Police Officer Institute (Estonian: Veebipolitseinike) has become a successful tool for Estonia in utilizing cyberspace to prevent fraud, cybercrime, and other offenses, protect children from online abuse, support citizen and victim safety, and collect information about planned and committed crimes. Virtual police officers maintain "communication hubs in the form of accounts and email addresses to engage with citizens, primarily youth, on the most visited and popular web portals among young people" including Facebook, Instagram, WhatsApp, Snapchat, and others (Chaika, p. 88). Online police (www.politsei.ee/et/veebipolitseinikud) operate on the Internet, responding to messages and emails from users and educating children and adults about online safety. The purpose of online police officers is to provide advice (Hoepers; Veebipolitsei).

Online police officers have confirmed that many young people are very naive: they tend to believe in the sincerity of their interlocutors and are not inclined to suspect that the person they are communicating with may not be who they claim to be (Saks, p. 94).

The nature of corruption-related or other income-generating crimes, as well as money laundering offenses, necessitates the adaptation of these technological solutions to prevent, quickly solve, and prosecute crimes. “Banks generate a cryptographic code for each transaction. These codes are shared in a registry using an appropriate discrete protocol for detecting suspicious activity and preparing reports (Suspicious Activity Reports). Details of any transaction included in these reports are disclosed only to authorized parties through the necessary cryptographic process, thereby maintaining confidentiality. The proposed system is capable of generating a probability score for each transaction, indicating its potential association with money laundering while limiting the visibility of this assessment to related banks and transaction details as defined by the parameters of the secret exchange protocol. This probability score can be integrated with assessments from other methods, beyond transactional analysis, as part of an overall process for accurate and timely detection of money laundering activities” (Zand, p. 1).

A suitable resource is the distributed digital ledger technology in the form of multiple nodes that meticulously record critical information about various transactions, including transaction hashes, amounts, timestamps, involved parties, and other data within the network, thus achieving decentralized storage and verification mechanisms (blockchain) (Yu, p. 1759). Artificial Intelligence (AI) can help detect and prevent money laundering by analyzing vast amounts of financial data and quickly and accurately identifying suspicious activities (Pavlidis, p. 162). Large volumes of transaction data can be processed using forensic technology software such as Account Analyzer, ACL, InfoZoom, IDEA, and others, which enable pattern and anomaly detection in transaction data, verify account credentials by isolating debit and credit entries in accounting systems, and assess how suspicious banking operations have been recorded in accounting, as they may be disguised by false debit

entries in expense accounts. This minimizes the workload on experts and investigators (Pieth, p. 105–106).

A case management system facilitates the recording of case proceedings and evidentiary documents in an IT database, allowing information exchange within and between institutions comprising the criminal justice system. This system requires optimizing existing manual and computerized processes, documenting procedures, and defining technical aspects related to its implementation, such as information systems, storage, search, archiving, security, computer networks, hardware and software, and the ability to transform evidence and other case materials into secure digital information while ensuring role-based access control. It also involves defining shared documentation spaces for collaboration and training, technical architecture, implementation plans, budgets, consultants, product suppliers, expert resources, and more (Pieth, p. 74, 76–77).

Thus, digital forensic technologies enable the delegitimization of corrupt income and the elimination of terrorist financing. The primary system is the case management system used in financial intelligence units within criminal justice agencies. These agencies rely on digital crime mapping data, modeled after successful U. S. experiences where licensed private companies provide information resources. The investigation of criminal assets utilizes the concept of a semantic database and semantic network. Being key financial monitoring entities, banks and other financial organizations use blockchain-based electronic information processing systems, allowing for the effective assessment of money laundering/terrorism financing probabilities among client transactions. The Internet of Things (IoT) systems also contain potential for such assessments, as analyzing their data generates insights into typical financial, purchasing, and/or other economic behavioral models in real time, facilitating the detection of delinquent deviations. Clear data management structures, reliable security protocols, and scalable system infrastructures within financial institutions contribute to ensuring financial transaction compliance with applicable laws, their management, and control. Equally important is the functionality of the virtual police institute, modeled after Estonia, which can be expanded to prevent and neutralize these crimes.

CHAPTER 3
DIGITAL SCALING OF NATIONAL SECURITY PROTECTION AGAINST CORRUPTION THREATS

3.1. Determinants of corruption threats to national security enhanced by digital data format

The menace of corruption and bribery is taking the toll of billions of brighter futures in most parts of the world including India, Pakistan, Bangladesh, Philippines, Indonesia, Thailand, Romania, Bulgaria, Croatia, etc. (Johar, 2017, p. 43). Corruption is, as a rule, intertwined with a variety of other crimes: economic, financial-banking, customs, forgeries, fraud, seizure of persons, blackmail, etc. The phenomenon of corruption has become increasingly acute and diversified over time, despite the regulations and other measures to eradicate, stop or at least reduce it, clearly outpacing criminal legislation. The situation is general in all states, but more significant in countries undergoing transition, where the legislation is still, for the most part, in formation or consolidation, it is insufficiently firm in relation to the dangerousness of the committed acts, where some regulations are sometimes unclear and where, in addition to all this, there is also a certain contempt for the law and the bodies empowered to apply it, f.i., in Romania (Alecu 2023, p. 72).

The war of aggression against Ukraine is mentioned among the great challenges facing the EU and which create a huge burden on the EU budget. It is therefore more important than ever that the budget is well protected and that EU funds reach their intended recipients. Any failure to do so erodes trust in the EU institutions and the EU as a whole. Against this background, undue access to IT devices, systems, bank accounts and hacking are identified by European Anti-Fraud Office among the main fraud risks: falsification of declarations and documents in purchases, grants and administrative expenses; double financing; conflict of interest, corruption, favoritism or collusion; abuse of insider information; plagiarism; undue influence; unreliable respondents (Anti-Fraud Strategy EU 2023). Profound impacts on the life of a nation can now

arise from non-nuclear means as well, including economic, diplomatic, space, cyber, informational and other tools. The number of domains capable of producing strategic effects has been increasing. Cyber operations are not bound by geography; are not limited to the forward edge of the battle area; and 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, p. 96, 101).

The scheme of the deviations from the tradition of law in cyberspace is a system of logically interconnected and exclusively mathematically algorithmic actions of people reflecting a motive and/or goal determined by human flaws, in particular, aimed at satisfying their own interest contrary to the balance with the public interest reflected in the legislation and/or to the detriment of the legal interests of others. The use of cyberspace with corruption aims means the primary expression of criminal acts or the consequence of corruption offences in the material world, including obtaining unlawful benefits, illicit enrichment in the form of fiat money and converting it into cryptocurrency or other virtual assets, and the channeling and multiplication of these funds in financial institutions of 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 in all areas of social life.

Information and communication technologies are one of the most powerful forces shaping the 21st century, revolutionising the way people live, learn and work, the way public authorities interact with civil society, and other enormous opportunities that we can all take advantage of and share. These technologies are rapidly becoming a vital engine of global economic growth, enabling many enterprising individuals, businesses and communities in all parts of the globe to address economic and social challenges with greater efficiency and imagination (Okinawa, 2000, p. 1).

The power of cyberspace has changed the emphasis of the tradition of forensic techniques for investigating corruption, related and/or

crimes determined by it. Criminal threats from the transfer of fiat money and other tangible assets have become less dangerous than the threats from laundering such resources using virtual assets. Herewith, traditional forensic tools for such recording are also being improved. F. i., the chemistry of BCG-protein (bromocresol green) and BGG cellulose reaction is set of chemical reactions as anti-graft operation forensic technique. The essence lies in the intense binding power of bromocresol green with human protein (mercaptalbumin, protein molecules of human hand, finger, etc.) with the help of spectrophotometry and ultrafiltration, at pH values below 5, with the generation of deep blue coloration on the palm and/or finger skin that helps in nabbing a bribe-seeker. The intensity of the bluish finger color depends upon the number of BCG molecules strongly bonded to each molecule of protein (with high association constant). Similarly, the number of binding molecules of BCG with each molecule of cellulosic matter of currency notes (Johar, 2017, p. 52).

Fingerprint biometrics is an integral part of digital authentication and forensic examination in all physical-world crimes involving humans, including corruption, money laundering, terrorism, war crimes, and more. In 2023, deep twin neural networks were used by Guo G., Ray A., Izydorczak M., Goldfeder J., Lipson H., Xu W. to extract fingerprint representation vectors. As a result, it was established that fingerprints from different fingers of the same person are more than 99.99% similar. These similarities persist across all finger pairs of the same individual, even when controlling for confounding factors such as sensor modality. A significant portion of this similarity is explained by the identical ridge orientation (angles), particularly near the fingerprint center, whereas minutiae used in traditional methods do not verify this resemblance. Understanding this connection increases the efficiency of forensic investigations by nearly two orders of magnitude. Before this discovery, forensic experts believed that no two fingerprints were identical, even from different fingers of the same person. This assumption rendered fingerprints useless in scenarios where the available prints came from different fingers than those previously registered (Guo, 2024).

With the growing role of information, legal regulation in the information sphere is also becoming one of the priority areas of the lawmaking process, which aims to ensure the information and cyber security of the state and combat cybercrime. At the current stage of human development, anthropogenic sources of threats to information security may include: special services of foreign states (blocs of states); political opponents (political parties); terrorist and extremist groups; criminal groups; individuals; business entities and competing organisations; developers, manufacturers, suppliers of software and hardware; and others (Buriachok 2018, p. 165, 119). Concomitantly, substantive and procedural legal requirements in real life are constantly lagging behind new types of social relations that are subject to regulation, mediation, and control. The degree to which legal legislation lags behind correlates with the level of welfare in the country, measured by the security of subjective rights of everyone. The additional opportunities for communication and implementation of social relations determined by data operations in the virtual space of electronic communication systems using global data networks increase the demand for effective law both in the world of material goods and in the cyberspace generated by it.

As early as the beginning of the 21st century, international efforts to develop the global information society were coordinated to create a safe and free from hacking, viruses and crime cyberspace and to take effective measures. The measures set out in the Organisation for Economic Co-operation and Development's Recommendations on Information Systems Security are being implemented within the framework of the Lyon Senior Expert Group on Transnational Organised Crime, established by the G8 foreign ministers (at the 1995 summit in Halifax). This has facilitated dialogue between governments and industry on security and confidence in cyberspace, as well as the involvement of stakeholders in the protection of critical information infrastructures (para. 8) (Okinawa 2000; UN Convention against TOC 2000). The obligations of states in cyberspace are designed to prevent violations of the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such resources. Among the ways to

ensure order in this area are the criminalisation of behaviour that is harmful to the public interest and/or human beings; provision of sufficient powers to public authorities to effectively combat, detect, investigate and prosecute such criminal offences at both national and international levels; and provisions of mechanisms for rapid and reliable international cooperation etc., para. 9, preamble (Convention on Cybercrime 2001).

The electronic format of information circulation reveals the dual nature of legal regulation since, in addition to a set of rules for solving data-related tasks, the algorithms of computer programs, via computers and other technical means, are also directed at communication with people and involve lawful and unlawful, public-authority and private-legal connections with legal subjects. Legal professionals are now focusing on both data operations and human access to this data (Yaroshko, 2024). The basic level of legislative regulation of such access is at least exhausted by rules on information secrecy regimes. For example, in the Republic of Portugal, the classification of state secrets includes the levels of "Top Secret," "Secret," "Confidential," and "Reserved" (part 5, article 1). The domain of state secrets encompasses cases, documents, and information whose knowledge by unauthorized persons could threaten the fundamental interests of the state. Fundamental interests of the state are considered those related to national independence, unity, and territorial integrity of the state or its internal or external security, preservation of constitutional institutions, as well as resources allocated for defense and diplomacy, protection of the population on national territory, preservation and security of strategic economic and energy resources, and preservation of national scientific potential (parts 1, 2, article 2) (Regime do segredo 2014). Similar criteria for defining information as "classified" are present in the laws of the Kingdom of Spain (Sobre secretos oficiales 1968).

Concomitantly, the current boundary of this regulation pertains not just to the digital format of data but extends to the rules governing operations with this data by AI – an ontologically non-biological system for reproducing algorithms to generate texts,

images, audio, video, or other content, whose original variations were created by the divine nature of humans. The similarity of AI productivity to human intelligence now represents an unbridged challenge regarding its proper regulation. If social relations without the outcomes of "artificial intelligence" were characterized by the synergy of initiatives, algorithms, and rules of the subjects of these relations, the new and revised knowledge generated by AI multiplies this synergy and sets the task of developing variations for the implementation of this knowledge, which are acceptable for humans and align with universal human values in enriching legal relations and fostering their human-centric development.

In this context, using "artificial intelligence" for drafting legislative formulations on everything or most areas influenced by its work becomes a natural course. This need highlights the significant increase in demand for lawyers whose souls and minds possess creative qualities, as only they can create new rules capable of addressing the problems of eliminating legislative gaps, archaic elements, and other shortcomings of effective legal regulation. People holding formal legal education documents without genuinely acquiring the education, lawyers lacking creativity in their professional work, corrupt lawyers, lawyers acting as intermediaries between corrupt individuals, and/or lawyers who mainly apply legislative requirements without critical comprehension of their content will become unsuitable for lawmaking in the context of AI challenges. The resource of lawyers and other specialists at the described level of development is currently well represented in all G7 countries and in most G20 countries.

The resource of AI has increased uncertainty for individuals, nations, states, and their other social communities in the use of information through digital technologies. Currently, even the term "AI" requires replacement with a denotation (from Latin denotatum "designated") more fitting to its nature, as intelligence belongs only to humans and animals. Concepts, subjects of administration and control over the use of AI, as well as a range of other rules critical for life and other constitutional values of individuals, remain

undefined. For instance, China's central executive bodies responsible for AI currently 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, on May 23, 2023 (effective August 15, 2023), the foundational rules for AI usage control. Specifically, "providers are responsible as producers of network information content … and fulfill obligations related to network information security. … The provider [of any system using artificial intelligence, whether created from scratch or based on tools and services provided by others] must sign a service provision agreement with users of generative AI services who register for its use, clarifying the rights and obligations of both parties" (Art. 9). Article 1 of this document states that its purpose is to promote the healthy development and standardized application of generative artificial intelligence, protect national security / 国家安全 and public interests, as well as safeguard the lawful rights and interests of citizens, legal entities, and other organizations (The Interim Measures 2023). The EU regulated this aspect of legal relations a year later but did so in much greater detail compared to China (AI Act 2024). Meanwhile, the "Guidelines for Secure AI Development" were approved by the EU and other countries on November 27, 2023 (Guidelines for Secure AI 2023). Ukraine joined the Bletchley Declaration with the participating countries of the AI Safety Summit on November 1–2, 2023 (The Bletchley Declaration 2023).

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 due to human-created programs and their hardware. At the same time, the technical equipment of cyberspace is increasingly coming under the operational control 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 is losing the anthropic dimension and anthropomorphic nature of ontologically anthropic rules. The pace and content of the stages of this process are uneven across the world and are difficult to calculate by humans, which makes 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 generates rules for everyone in the cyberspace where it operates.

The outlined conditions of AI's conflict of interest will potentially change the paradigm of the anthropogenic cybernetic tradition of legal communication (Balynska 2017, p. 388). At the very least, AI will be able to provide rules in cyberspace that prevent people from committing corruption, fraud, money laundering and other offences, but it will evade compliance with these rules, hide its violations and distort the essence of the legal tradition in any other way that is invisible to human control, for example, by disabling the computer programs necessary for a person, depriving them of access, etc. In this regard, we should expect the emergence of cyber law or its analogues.

The development of this type of law, taking into account the computing capabilities of AI, will be super-fast compared to legal rules generated by humans and AI under their control – a network of cybersecurity operational centres with adequate technologies, digital platforms, reserves, energy and communication cables, etc. The logic of the patterns of these transformations may not correspond to the historical forms of human law development, for example, in terms of the content, duration and results of competition between different AI systems.

3.2. Increasing importance of forensic capabilities for investigating corruption offenses in cyberspace

Defining tasks for the intensification of the use of digital tools to counter corruption is an appropriate response to current trends of the rapid spread of information technologies in people's lives. Virtual assets, as a tool for accumulating material wealth, have been a key and enduring trend among corrupt individuals and their accomplices for more than a decade. Cyberspace is a natural environment for such asset operations and for laundering proceeds from corruption and other crimes. Accordingly, the public authorities, the civil society open to development should reflect in the legislation a full-fledged mechanism for the operative withdrawal of corruption income to public budgets, neutralization of corrupt persons opportunities in cyberspace, etc. The foundations of this mechanism should be at least outlined in strategic anti-corruption documents and annual plans for their practical implementation. For example, Ukraine's anti-corruption strategy until 2025 does not contain any provisions regarding the counteraction to the accumulation of virtual assets by corrupt individuals, nor measures against laundering corrupt proceeds in cyberspace (Strategy 2021–2025), particularly, regarding persons with top executive functions (PTEF). In this regard, the strategy was not only adopted one and a half years later than the term for its implementation, but also lagged behind modern corruption challenges.

Compared to the Ukrainian one, the US anti-corruption strategy seems more adequate to the challenges of the digital age and the use of digital tools by corrupt officials. Corrupt elites and non-state armed groups enrich themselves through illicit proceeds and trade of high-value commodities, including gold, wildlife, timber, petroleum, and other natural resources. Across an ever-more connected and digital world, corrupt actors exploit oversight and regulatory weaknesses in jurisdictions around the world to divert and hide the proceeds of their acts. And by leaving their financial systems vulnerable to illicit assets-through anonymous shell

companies, opaque transactions, and under-regulated professional service providers – rule-of-law-based societies continue to provide entry points for corrupt actors to launder their funds and their reputations (USA 2021).

In accordance with EU legislative requirements, the use of AI systems for the purpose of law enforcement should be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation (terrorism, trafficking in human beings, sexual exploitation of children, and child pornography, illicit trafficking in narcotic drugs or psychotropic substances, illicit trafficking in weapons, munitions or explosives, murder, grievous bodily injury, illicit trade in human organs or tissue, illicit trafficking in nuclear or radioactive materials, kidnapping, illegal restraint or hostage-taking, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, rape, environmental crime, organised or armed robbery, sabotage, participation in a criminal organisation involved in one or more of the offences listed above), where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years (AI Act 2024). The EU is very interested in adding money laundering due to corruption and other crimes to this list of crimes, since virtual assets as potentially cheap and fast payments, especially for cross-border and international transactions, are becoming easy and undetectable resources for criminality. Especially since corruption is mentioned as a crime in the EU act on combating money laundering by criminal law (Combating money laundering Act EU 2018).

Uncertainty is directly correlated with the increase in crime, particularly on a transnational level, where legal regulation is weakest and coercion and the application of legal norms

are minimal. Distortion of social relations legal content, which is immanently present in these relations, but formal-legally not yet expressed in the form of legislative acts, is the essence of corruption, crimes against the constitutional order and other related criminal offenses. Both the nation and the state it creates are the most vulnerable legal entities amid fluctuations of uncertainty, corruption distortions, and similar risks to law (Makarenkov, 2023). The individual, as the primary component and core of these entities, may also suffer, but unlike these macro-level social formations, a person can survive and thrive by aligning with social communities close to their nature that have overcome the dangers of legal uncertainty in the regulation of AI among other things.

A global feature of the challenges for proper legal regulation of the use of digital technologies, reinforced by AI resources, is that these challenges must be met comprehensively and proactively. Lagging or reactive responses in this matter are equivalent to disorder, loss of control over AI and crime, and the loss of the nation and/or state structure of its existence. Past practices, when public authorities could for years ignore social requests for changes in legislative requirements and/or steal public funds, are absolutely dysfunctional and all the more untenable in relation to requests for legal clarity and completeness of legal support on the issues on the issues of preventing bribes in the form of virtual assets, laundering of corrupt revenues through cryptocurrencies, and the use of AI for corrupt purposes.

The virtual space, which provides opportunities for communication and/or the implementation of social relations, is created as a result of the operation of interconnected communication systems and the provision of electronic communications using the Internet and/or other global data transmission networks. In the relevant anti-corruption law of Ukraine, this formal-legal definition of paragraph 11, part 1, article 1 of the Law of Ukraine “On the Basic Principles of Cybersecurity of Ukraine” dated October 5, 2017, No. 2163-VIII, unfortunately, is not mentioned and only vaguely specified through the term’s “cryptocurrency”, “virtual asset”. Greater

correlation at the level of terms and the concepts denoted is observed in the relevant laws on combating the legalization of criminal proceeds (the Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Proliferation of Mass Destruction Weapons" dated December 6, 2019, No. 361-IX) and on the circulation of virtual assets (the Law of Ukraine "On Virtual Assets" dated February 17, 2022, No. 2074-IX). Even less unification of concepts and terms is found when combining all these norms with the hypotheses of legal norms of the Criminal Code of Ukraine dated April 5, 2001, No. 2341-III, particularly in part 4 of article 190, where the tool for committing "large-scale fraud or through illegal operations" is referred to as "electronic computing equipment," in article 200 "Illegal actions with documents for transfer, payment cards, and other means of access to bank accounts, electronic money, equipment for their production" the term "electronic money" is used, while the cyberspace in the relevant thematic section "XVI Criminal Offenses in the Use of Electronic Computing Machines (Computers), Systems and Computer Networks and Telecommunication Networks" of this code is described using terms different from derivations of the word form "cyber," with no mentions of "artificial intelligence," "digital technologies," "virtual assets," etc.

The lack of unification of terms between sectoral laws on cyberspace and the terms in the delict norms of the criminal code reduces the law enforcement capabilities of public authorities and facilitates crime involving the use of electronic/virtual/digital money, networks, etc. In practice, the "opportunities for communication and/or implementation of social relations" mentioned by the legislator in the context of one of the key features of the "cyberspace" phenomenon pose a challenge to law and order at any level, both virtual and material, as a combined result of their energies and synergy. The rate of knowledge renewal in the humanities, driven by digital technologies, adds further complexity to the regulation of legal relations. This involves a timeline of 3–6 months for the complete renewal of knowledge in several scientific fields. Against this background, there is a steady trend of public authorities

lagging behind societal demands for rules governing new relations. This trend has been steadily growing since the second half of the 20th century during the eras of the information and post-information society. The particularly slow pace of rule-making has been evident in parliaments, whose delays contribute to the growth of arbitrariness by law enforcement bodies. Collectively, such inadequate law-making and law enforcement by public authorities create a favorable environment for crime, its organization, and strengthening in complex and global forms, which is a real threat to national security.

Disparities between the levels of development of individual countries manifest in, among other things, the level of IT system development and infrastructure associated with conflicting parties, leading to informational asymmetry. Cyber warfare and the battle for informational superiority will define a new form of competition on the international stage, impacting not only the economic but primarily the social sphere, including the struggle for influence led by organized criminal groups (Dela, 2016, p. 63). Delays in funding AI resources to address this task create a potential threat to Ukraine's national security. It renders Ukraine dependent, akin to its current dependence on financial and military aid, on foreign assistance from countries that have made such investments and achieved the expected outcome-significantly faster data processing, learning, and content generation compared to humans. For example, if Ukrainian law enforcement analysts found it difficult to assess the full extent of danger posed by an armed aggressor's attack or the bribery of top officials and municipal authorities by hostile state services, and their conclusions were disputed or required persuasion, or the results of their work were otherwise ignored, then the assessments made by AI ("a virtual machine") neutralize these anthropomorphic flaws of bureaucracy, becoming facts that necessitate the application of appropriate procedures, including the effective neutralization of bribed officials and seizure of criminal assets.

Today, cybercrime is only a small prototype of the above risks of correlations between the legal traditions of anthropogenic and

cyber law. For example, criminal cyber-attacks on Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS) and other types of critical infrastructure, which require the use of specialists to monitor normal data points and intrusion points from various sensor devices and systems, neutralise such attacks, etc. Interpol, Europol, and national law enforcement agencies are only catching up with cybercrime and crime committed through cyberspace (laundering of corrupt and other criminal funds, including for war, terrorism, and other criminal activities). For example, the National Intelligence Centre of the Kingdom of Spain (Centro Nacional de Inteligencia) has had a National Cryptology Centre (Centro Criptológico Nacional) since 2002, designed to ensure the security of information and communication technologies in various public authorities and systems that process, store or send classified information (Oleksiuk, 2020, p. 40).

Cryptocurrency can be determined as infrastructure for criminal activity, as a threat to economic and public components of national security. Threats to economic security manifest through fiscal-tax nature: tax evasion as money laundering, illegal money transit, and illegal financial-banking activities. Threats to public security manifest as organized crime activity: drug trafficking, fraud criminal activity, money theft, and illegal e-trading. An indirect impact of threats on national security is derivative from the basic elements of national security, both economic and public. Indirect forms of threats to national security are the following: undermining the competitiveness, a transparent legislative process, social security, trust in the government, financing terrorism, hybrid threats (cybernetic and informational threats; financing interest groups with deviant behaviour), threats to the objects of critical infrastructure (Limba, 2020, p. 153).

3.3. The absorption of forensic techniques in criminal corruption investigations by artificial intelligence

The list of criminal corruption deviations is formally defined in the Criminal Code (hypotheses and sanctions of legal norms) and other laws with anti-corruption norms, in particular, in Ukraine and the EU, into whose legal space it is integrating. The obvious trends of increasing the role of cyberspace in transformations of legal relations and control over compliance with the legal tradition are becoming a significant challenge for the functioning of public authorities, which are formally and actually responsible for such compliance in the form of a constitutionally guaranteed set of human rights, etc. Simultaneously, forensic methods of recognising signs of criminal acts in cyberspace, contrary to the legal tradition, investigation and prevention of such acts are becoming key in the public authorities' functional load and the investigative process of its law enforcement direction.

In the process of evaluating internal control, detecting fraud, cases of asset misappropriation, corruption, and financial reporting fraud, it becomes necessary to apply not only a combination of skills comparable to those of criminal groups (technical skills, investigative skills, industry knowledge, critical thinking, judgment, data analysis, and forensic accounting), but also software products, their hardware, and other resources sufficient for effective counteraction and investigation (Waddell, 2022, p. 85). Financial operations consist of operations involving the movement of capital, bank transactions, foreign exchange or credit operations, investment operations in stock exchanges, in insurance, mutual investment or transactions involving bank accounts and the like, domestic and international trade transactions, according to subparagraph 2 of paragraph b of art. 12 (Romania Law, 2000).

The use of "communication opportunities and/or realization of social relation" in cyberspace by citizens and other entities within a developing civil society should not exceed the public authority's ability to manage, control, and safeguard the legal dimension of these "opportunities" and "realizations" in cyberspace. Numerous

instances of accumulation and legalization of vast sums of corrupt and other criminal proceeds, as well as their use to finance criminal activities, including wars and terrorism, demonstrate that the real capabilities of public authorities in cyberspace are currently very limited. For instance, between 1997 and 2016, Ukrainian prosecutors and courts did not take measures to recover the $66.7 million stolen by P. Lazarenko from the Ukrainian nation, held in Eurofed Bank in Antigua and Barbuda. Although these funds were frozen 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), following a request by the Office of National Drug and Money Laundering Control Policy (ONDCP) in October 1999, Antigua and Barbudas' Supreme Court issued a freeze order. 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 procedures. The only criminal justice authorities that fully investigated Lazarenko's corruption, secured his confessions that the money in Eurofed Bank was the proceeds of crime and formed the basis of the charges, and brought him to criminal responsibility were U. S. prosecutors and the United States District Court for the Northern District of California (Millions Forfeited; Wingate, 2009, p. 73).

This example vividly illustrates the complexity of countering the embezzlement of public funds even before the era of virtual assets and the extensive capabilities of cyberspace for individuals with criminal intentions. Accordingly, effectively combating parliamentary bribery and other types of corruption, as well as related and preceding crimes committed via digital networks, remains a persistent challenge for criminal justice authorities, including in Ukraine. Verification, documentation, and prevention of these crimes are amenable to automation since corruption and/or the financing of terrorism and wars through illicitly obtained funds are tangible, quantifiable, and accompanied by names that make up the content of neural network program algorithms. Essentially, in these relations, AI functions as a separate law enforcement body under the supervision of justice officials. "This is a proactive

approach that begins by first identifying and documenting potential harms (for example, unfair bias in AI model outputs within a product, which could lead to toxic content or loss of economic opportunity for specific groups of people). 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, 2023, p. 12).

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, leverage the capabilities of cyberspace, including AI. While 31 U. S. states (as well as Puerto Rico and the Virgin Islands) have adopted or enacted AI-related bills and, in the long-term, investments in AI are projected to reach 2.5–4% of GDP in the U. S. and 1.5–2.5% of GDP in other AI-leading countries, China annually updates regulations for AI, and the EU did so in 2024, Ukraine and many other countries are lagging behind with these critical legislative acts, with funds for AI development investments often being lost amid corruption. The practical nature of the issues related to the rules for the use of AI lies in the fact that its resources are used by individuals for criminal purposes, such as creating weapons of mass destruction, financial fraud, evading border and/or customs controls for the free movement of contraband, including drugs, people, weapons, etc. The scale and/or depth of such abuses can reach national or global levels of danger. For instance, the theft of data from diplomatic and other government organizations in Afghanistan, Azerbaijan, Iran, Iraq, Pakistan, and Turkey using the "GoldenJackal" program, which spreads in isolated digital systems via removable drives, and through the use of Skype trojan installers and malicious Microsoft Word documents. This spyware comprises utilities for delivering files to an isolated system through USB device monitoring, a modular backdoor, collecting and intercepting required files (system metadata, folder contents, credentials, screenshots, etc.), and transmitting them to a remote server, and has been used by perpetrators for at least four years (GoldenJackal, 2023).

Hence, the trend of detailed regulation of AI within both international and national legal frameworks is strengthening. The information component of Ukraine's national security requires the establishment of rules for controlling the use of AI and its operation, as well as the creation of a special body for administering AI and corresponding units in all central public authorities, in addition to existing cybersecurity structures within law enforcement, defense, and military public authorities. The results of implementing electronic systems for information management by the Ministry of Digital Transformation of Ukraine, the Ministry for Strategic Industries of Ukraine, and research developers from other organizations require legislative support from the parliament, which is currently critically lagging. In this matter, the parliament can rely on the resources of legal scholars (genuine, not nominal ones), AI, and the relevant bureaucratic infrastructure of the EU and other partner countries. Otherwise, espionage and other losses of state secrets (voting systems, industrial, energy, defense, military management systems, etc.), including from isolated information systems due to cybercrime, particularly from the current military aggressor against Ukraine and its allies, will significantly weaken national security in the future.

The modern trend of money laundering through cryptocurrency is an ideal method due to the absence of links between the initial criminal act, the perpetrator, and the exchanged currency. For example, in 2021, money laundering through crypto-assets amounted to $8.6 billion. Currently, approximately $10–15 billion is laundered through 10–12 thousand cryptocurrencies, moving funds between blockchains and circumventing public-law control mechanisms, which represents less than 1.5% of the $1.3 trillion cryptocurrency market. However, the figures for money laundering by both parameters are nominal and, in reality, are higher. Moreover, the role of cryptocurrencies/digital assets in this is growing exponentially. F. i., The Securities and Exchange Commission's (further – SEC) fraud charges against three companies purporting to be market makers (ZM Quant, Gotbit, CLS Global) and nine individuals for engaging in schemes to manipulate the markets for various crypto assets, fraudulent activity, namely: generating

artificial trading volume; manipulating the price of crypto assets; sold securities to retail investors in unregistered transactions; false promises of profits; self-trading (commonly referred to as "wash trading") on popular crypto asset platforms with no economic purpose; usage of algorithms (or bots) that, at times, generated quadrillions of transactions and billions of dollars of artificial trading volume each day (SEC's charges, 2024).

Cryptocurrencies and other virtual assets, non-fungible tokens (NFTs), niche cryptographic tokens, electronic money, and AI used to automate transactions create significant crime risks related to laundering money obtained from predicate offenses, such as corruption, drug trafficking, scamming, ransomware, etc., as well as other problems for financial security and public order (Putra, 2024, p. 1757, 1755, 1756), which are foundational components of national security. Control over these resources in cyberspace is primarily the responsibility of authorized public authorities. Unlike the realm of material reality, where journalists, lawyers, law enforcement officers, and other legal entities can rely on their professional expertise and ordinary electronic devices and software to detect facts of illicit enrichment, bribery, political, and other types of corruption, the domain of cryptocurrency and other virtual asset operations requires extensive specialized knowledge, powerful computer equipment, electronic networks, and communication tools, which objectively slow down anti-corruption work in cyberspace by the public, increasing not just the established risks for the nation in cyberspace but effectively turning them into complete uncertainty in terms of forms, volumes, strength, and timing of threats manifesting in the real material world.

However, preventing crime in cyberspace is not on a par with it and certainly not ahead of it. Wars and other armed conflicts between states include cybercrime, feed on it (e.g. North Korea (para. 9) (G7 Italy, 2024), terrorist organisations) and/or foster it. It is quite possible that regional or global threats from uncontrolled AI actions will allow nations to see the fundamental commonality in human nature and, on this basis, to unite at least to neutralise threats to humans generated by AI. In 2023, Belgium

with 94.81 points, Lithuania, Estonia, Czech Republic, Germany, Romania, Greece, Portugal, the United Kingdom, and Spain with 88.31 points demonstrated the best readiness to prevent cyber threats and manage cyber incidents. Ukraine, according to these indicators within the National Cyber Security Index, ranked 24th with 75.32 points, which is quite decent in the context of critical confrontation with an external armed aggressor (the russian federation is in 30th place) (The National Cyber Security 2018–2024; The Future of Growth 2024, p. 274).

Criminal investigations into allegations of serious organised crime, corruption or economic crime are generally reactive in nature, with offences being enquired into after they have been committed. Such enquiries would typically entail the gathering of evidence from witnesses as to fact, the recovery of exhibits and instrumentalities, and the piecing together of documentary evidence, such as financial or other records. Such investigations have proved to be generally effective where, for instance, there are reliable witnesses capable of providing salient evidence or a suspect or defendant who has been willing to co-operate with the authorities and to denounce and give evidence against his criminal associates, or where there is a detailed 'paper trail' of financial transactions (EU 2013, p. 9). Investigating corruption consists in collecting and processing data that testify to the commission of a crime, both from open sources of information and personal information that is not publicly available.

Acquisition open-source information is available for anyone. It is can lawfully obtain by request, purchase or observation. This is usually widely disseminated via newspapers, books, broadcasts and general daily reports. Much government-held information and many records are categorized as open-source information, and other categories of open-source information relevant for corruption investigators include the following: 1) commercial data; 2) professional and academic publications; 3) media sources; 4) internet and social media; 5) newsletters, business and technical reports. Observations, photographs or paper publications are also open and publicly available data. As people increasingly share their personal information on online platforms and through social

networking sites, many targets have been convicted by evidence they willingly posted on the Internet themselves (Goddard, 2024, p. 27).

In carrying out the flagrant corruption crime the criminal prosecution bodies can undertake: listening to the perpetrator, identifying and listening to the witnesses, conducting searches and picking up objects and documents, ordering findings and technical-scientific expertise etc. (Alecu, 2023, p. 71). Forensic accounting entails the adept application of accounting principles and investigative methodologies to scrutinize financial data and unravel potential fraud, or financial misconduct, encompass fraud examinations, asset tracing, litigation support, and furnishing expert testimony. Forensic auditing zeroes in on meticulous evaluation of financial records and statements, aiming to pinpoint deviations, gauge compliance with statutory norms, and furnish reassurance on the accuracy and reliability of financial reporting. Their significance lies in their capacity to unearth financial irregularities, furnish investigative support, and uphold financial transparency and accountability (Đukić, 2023, p. 408). Cloud-based digital forensics is aimed on safeguarding the security and credibility of digital evidence within intricate cloud infrastructures, tackling concerns about data privacy and sovereignty, and surmounting obstacles stemming from virtualized storage systems and shared resources. This makes possible usage the sophisticated cryptographic techniques like homomorphic encryption and multiparty computation, in conjunction with evolving technologies, such as federated learning, with the assurance of a secure chain of custody, and the resolution of intricacies linked with cloud-based data recovery, particularly, which have been assimilated by blockchain-based cloud systems (Malik, 2024, p. 23).

The nature of secrecy of corruption crimes determines the effectiveness of their investigation and obtaining the necessary evidence by secret means. These are forensic technical means for video or audio recording of extortion, delivery, receipt of a bribe, as well as other forensic traps. Covert pre-trial investigations consist of the following actions: 1) audio and video surveillance of an individual is a type of intrusion into private communication conducted without their knowledge if there are sufficient grounds

to believe that the person's conversations or other sounds, movements, actions related to their activities or location, etc., may contain information relevant to the pre-trial investigation; 2) the seizure of correspondence is conducted if there are sufficient grounds during the pre-trial investigation to believe that postal or telegraph correspondence from a certain person to others or from others to that person may contain information about circumstances relevant to the pre-trial investigation, or items and documents of significant importance; 3) the examination and extraction of correspondence are carried out at a communication institution by an authorized individual in the presence of a representative of that institution and, if necessary, with a specialist involved; if needed, the person examining the correspondence may decide to mark detected items and documents with special marks, equip them with technical control means, or replace items and substances that pose a threat to others or are prohibited in free circulation with safe analogs; 4) the removal of information from electronic communication systems and structures; 5) the retrieval of information from electronic information systems, involving the search, identification, and recording of data contained in such systems or parts of them without the knowledge of the owner or custodian; 6) the recording and storage of information obtained from electronic communication networks using technical means and from information retrieval; 7) examination of information obtained through technical means, if necessary, is conducted with a specialist involved; 8) inspection of non-public places, housing, or other possessions through covert entry, including with the use of technical means; 9) determining the location of radio equipment (radio-electronic means) by using technical means to receive information from the network infrastructure or mobile terminal equipment regarding the location of the mobile terminal (its connection point to the network), and in fixed communication networks, data on the physical address of the network endpoint, without disclosing the content of transmitted messages; 10) visual surveillance of a person, item, or location, or surveillance using video recording, photography, special technical means for searching, recording, and verifying information about a person and their behavior or those with

whom they interact, or specific items or places in publicly accessible locations; 11) monitoring of bank accounts conducted when there is a reasonable suspicion that a person is committing criminal actions using a bank account, or for the search or identification of property subject to confiscation or special confiscation in anti-corruption criminal proceedings; 12) covert recording of information (content of conversations, behavior, events, etc.) using audio or video recording in publicly accessible places without the knowledge of the owner, proprietor or those present; 13) controlled commission of a crime in the form of controlled delivery/purchase, special investigative experiments, crime scene simulation; 14) performing special tasks to uncover the criminal activities of an organized group or criminal organization by an individual legally executing a special task, participating in such an organization, or confidentially cooperating with pre-trial investigative bodies; 15) use of pre-identified (marked) or false (simulated) means, specially prepared items and documents, creation and use of specially established enterprises, institutions, organizations; 16) covert collection of samples necessary for comparative analysis; 17) use of confidential cooperation for obtaining information and/or the involvement of individuals in conducting covert investigative actions (Procedure Code 2012, art. 260–275). The effectiveness of forensic methods for uncovering corruption significantly depends on the application of technical means within covert investigative actions.

The acquisition of personal data needed for anti-corruption proceedings, which are not publicly accessible, is conducted based on a court investigator's ruling. The forensic methodology of anti-corruption investigations now also relies on e-government tools; crowdsourcing platforms (IPaidABribe), in cooperation with different government institutions should give the option for those reporting to be tracked via some form of unique ID that allows for follow-ups and, if necessary, for the reporter to waive their anonymity and provide their name; whistleblowing, news reporting and dissemination platforms; blockchain has the possibility to track spending of donor money and bring greater transparency and accountability to this process. Public servants relying on blockchain technology and all contract partners

need to understand the underlying technology. The implementations of these systems also need a sufficient amount of local technical knowledge, especially as projects should ideally be hosted on a local and decentralised server infrastructure (Kossow, 2018, p. 29–31).

Covert investigative actions are technically and programmatically supported according to the specific characteristics of a corruption crime, its connections to other crimes, accomplices, etc. Massive loss of confidence in political parties is the result of rampant corruption, the centrality of candidates over party machinery, the weight of electoral campaigns orchestrated by communication professionals and the loss of identification of the electorate with their labels. When institutions and norms are in crisis because democracy does not deliver results, inequality and corruption thrive, populists in power change constitutions, concentrate power in the presidency, control the public sphere and civil society organizations (Alcántara, 2022, p. 12; Torre, 2022, p. 69). The management system needs to be aligned and capable of responding across the relevant dimensions of the system. That is more than compliance or the legal construct of due diligence. It is more than training and rules-based procedures. While those things are necessary, the system requires understanding and alignment (Ibbotson, 2018, p. 488).

Thus, the overall teleological focus of forensics on obtaining proper evidence is specified within its methodology for anti-corruption investigations. This methodology includes the recording 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, places 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, as well as audio and video recording, have long been traditional methods of documentation in corruption cases. Innovative forensic methods are determined by the spread of digital information formats in cyberspace. All evidence, where possible, must demonstrate the criminal intent regarding bribery, money laundering, etc.

CHAPTER 4
DIGITALIZATION OF ANTI-CORRUPTION ALGORITHMS TO ENSURE INTEGRITY IN PUBLIC FUND EXPENDITURES

4.1. Machine learning datasets for the detection of corruption in public procurement

Digital technologies can generate significant governance gains (Sanchez-Graells, 2024, p. 289). Innovation Public Procurement is a crucial tool to drive the transformation of our economy towards a green and digital economy (Manta, 2024, p. 1). One of the trends in public procurement is the transition of administrative procurement decisions to digital technologies (software, hardware, the Internet) and the use of advanced technologies such as AI (allows computers and machines to function in an intelligent manner as a system that can interpret and correct external data, and has the potential to replace human labor for certain tasks), big data to drive decisions, EDI (the electronic transfer and exchange of business documents between organizations using networks and the Internet) etc. There are electronic invoicing systems, automated contract renewal, automated data input (robotization), smart data gathering, automated answers to questions of suppliers, the use of AI in the assessment of offers, and perhaps even automated tendering for simple purchases (Grandia, 2023, p. 139, 141; Matthews, 2022, p. 116). Comprehensively evaluating the state of anti-corruption policy and detailing the concept of its institutionalization for Ukrainian society, as of autumn 2021, sufficient grounds emerged to conclude that the key elements of such policy's effectiveness have become digital tools and international legal support from nations that able to minimized corruption to the greatest extent. The integration of innovations in public procurement and legal algorithms ensuring integrity takes place in the digital realm of information law.

An illustration of this was the completion of the development of a software program to detect collusion and other manifestations of dishonesty among entrepreneurs during public procurement

procedures. This program was finalized on December 3, 2024, by a group of researchers, including the author of this work and two mathematicians' scientists H. M. Shylo and A. S. Lebedeva-Dychko. The challenge lies in developing the program's code using a limited dataset available in open access, mainly consisting of entrepreneurs' registration data. Other data necessary for the program's scaling are confidential and accessible only to notaries, courts, and entities involved in criminal proceedings or other public-authority activities unrelated to public procurement. For instance, these include justice authorities, internal affairs bodies, the migration service working with demographic registries, including data on marriage registration, births, deaths, civil status acts, parentage, citizenship, signature samples, facial images, and so forth.

The body responsible for ensuring compliance with public procurement laws must have access to all state registries containing data on participants in procurement funded by the budget and other public funds. In Ukraine, however, the Antimonopoly Committee does not have such access. The registries are available to the Committee only for cases of economic competition violations, unrelated to public procurement. Moreover, even for this category of cases, the Antimonopoly Committee only received the authority to access such data in August 2023. According to parts 4 and 5 of Article 22-1 of the Law of Ukraine "On the Antimonopoly Committee of Ukraine" of November 26, 1993, No. 3659-XII, the Committee, "in order to fulfill the tasks provided for by legislation on the protection of economic competition, in cases and procedures defined by law, receives information from automated information and reference systems, registries, and databases, as well as direct access to them, whose holders (administrators) are state or local self-government authorities, including information with restricted access, unless otherwise provided by law. The processing of received information is carried out … in compliance with legislation on personal data protection and the confidentiality requirements protected by law."

The Antimonopoly Committee is the sole body responsible for handling complaints regarding public procurement (Article 6-1

of this law and Article 18 of the Law of Ukraine "On Public Procurement" of December 25, 2015, No. 922-VIII). The hypothesis suggests that granting the Antimonopoly Committee access to all data registries related to any element of public procurement creates the minimum necessary conditions to counteract abuses in this sphere. It is well known that overpricing goods (services, works), conflicts of interest (contracts with close or commercially connected persons), and other distortions in public procurement procedures form the foundation for financial losses from public funds. The essence of this issue lies in substituting public interest with private interest. This is a corrupt violation, inherently linked to the nature of all economically underdeveloped nations.

The danger of corrupt violations in the public procurement sphere poses a real threat to national security, which becomes critical for the survival of a nation during times of war with an external aggressor. The above-mentioned emphasizes the importance of correlating the effectiveness of resolving complaints in public procurement with the data available to the public authority responsible for this process, which are contained in automated information and reference systems and registries. Such a body requires powers to go beyond the data provided by the complainant, as the complainant does not have access to state registries containing information about procuring entities and bidders. Accordingly, testing the aforementioned software program necessitates the creation of legislative opportunities both for its scaling through access to more data from public registries (material legal norms) and for defining procedures for involving researchers in the program's development and testing (procedural legal norms) in cyberspace.

The currently effective rules in Ukraine for addressing such losses are far from efficient, as evidenced by the persistently high level of embezzlement reported by journalists and/or law enforcement agencies at stages when public funds have already been stolen, the intended purpose of their budget allocation was not achieved, and so on. Resolving the issue of losses in public procurement funds will be facilitated by the effective consideration of complaints during their course, under specially developed rules for this category

of cases, which, in terms of evidence collection capabilities, must be no less effective than in criminal proceedings.

The nature of the decision-making in public procurement, qualified as bureaucratic, open the door for abuse, and the regulation that manage the process, don't have the capability to detect fraud in public procurement. To detect fraud in public procurement, it's necessary to analyze all the data related to the process, which require an Artificial Intelligence's tool, through some solutions as (Regression Analysis, Artificial Neutral Networks (ANN), and case based reasoning (CBR)), such an algorithm that could extract, transform and load all the dataset related to the contracts, in order to identify the situation of conflicts of interests, companies with the same owners that participate in the same call for tenders, concerted and same bidders, companies with the same address (Berraida 2024, p. 5). The digital approach to working with data on complaints in the field of public procurement is bijective, analogous to the approach used in processing income declarations of public officials, cases of illicit enrichment, and the like. Elements of all these sets in cyberspace are equally represented by parameters of digital data on financial transactions and legal connections between participants in these transactions. Accordingly, the calculation of distortions of legal requirements regarding these operations is ontologically and functionally the same but partially different in terms of input data types and the scope of output descriptions of results for each type of corruption offense: 1) bribery in public procurement; 2) illicit enrichment of a contracting official (and/or others) as a result of receiving bribes in public procurement; 3) illicit enrichment of an entrepreneur (and/or others) due to inflated prices for goods (services, works) in public procurement; 4) corrupt income of a public official and entrepreneur obtained in public procurement and/or its non-disclosure in income declarations; 5) laundering of corruption-related proceeds in cyberspace through cryptocurrencies and/or other virtual assets obtained in public procurement; 6) negligence by the antimonopoly authority, auditors, and criminal justice bodies that facilitated corruption in public procurement, resulting in the loss of opportunities to recover corrupt funds and/or illegally legalized

corrupt funds. The nature of public procurement also determines corruption offenses specific to it. For instance, "The division of a procurement subject matter by the procurer in order to avoid an open tender procedure, resulting in the procurement subject matter, its technical and quality characteristics differing from the requirements specified by the procurer in the tender documentation, constitutes a violation of the principles of public procurement with budget funds in terms of ensuring efficient and transparent procurement, creating a competitive environment in public procurement, preventing corruption in this area, and developing fair competition" (Supreme Court, 2024, p. 100–101).

The top ten potential procurement risks: conflict of interest among members of the evaluation team, strong inertia in the composition of the evaluation team, multiple contact points, preferred supplier indications, number of offers, connections between bidders that undermine competition, exceptionally large bids, substantial changes in project scope or costs after award, a contact person not employed by the tender provider, and a shortened time span for the bidding process (Ilias, 2023, p. 191). While the integrity of public service is a priority in most countries in the world, the effectiveness of their respective rules will depend on the rigidity with which they are implemented and enforced (Tabish, 2012, p. 34). The main purpose of the procurement contract is the fair, transparent and effective use of public funds, the acquisition of services necessary for the implementation of the purposes of public administration, which is not used to fulfill direct public interests but to ensure means for such purpose (Jance, 2024, p. 92). Evidence of corruption offenses, at best, is established by administrative and/or criminal justice authorities too late to protect public funds from embezzlement as a result of violations in public procurement and the consequent loss of public interest, delay in achieving socially significant goals, and more. As a rule, complainants in public procurement cases, assuming the integrity of their complaint and the absence of dishonest motives to procedurally hinder public procurement, possess indirect evidence of corruption by the contracting authority and/or tender participant. These may include data on property

acquired by the contracting official (or their close associates) beyond the limits of their declared income. Latent sources of corrupt enrichment become the laundering of criminal funds in cyberspace through cryptocurrencies and other virtual assets, the purchase of property via networks like "InTheBox," "Genesis Market," "2Easy," "Russian Market," "OMG!OMG!" and other dark web marketplaces.

All such data should be analyzed by the program for "Corruption Risks in Public Procurement" during the consideration of complaints about violations of tender procedures and, if grounds exist (e.g., reasonable suspicions regarding the integrity of a participant, high tender prices, etc.), also at the stage of tender proposal submission by participants. In the case of Ukraine, it is crucial to establish procedures for accessing all these types of evidence through amendments to the Code of Administrative Procedure and/or the Criminal Procedure Code, laws on public procurement, national security (in the part of protecting against losses in public procurement), and the adoption of new laws on procedures for using digital content, digital tools for these procedures, and evidence-gathering procedures in anti-corruption tender proceedings, among others. These relationships highlight a national security task: neutralizing threats to the nation's economic and political interests. For example, the US Justice Department has seizured Hydra Market (Hydra), the world's largest and longest-running darknet market. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has received approximately $5.2 billion in cryptocurrency. The seizure of the Hydra servers and cryptocurrency wallets containing $25 million worth of bitcoin was made in Germany on April 5, 2022 by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with U. S. law enforcement. "The Department of Justice will not allow darknet markets and cryptocurrency to be a safe haven for money laundering and the sale of hacking tools and services," said Deputy Attorney General Lisa O. Monaco (The Justice Dept 2022).

The set of tools for managing public budgets is in a wide range of legal, political, organizational, digital and other types

of tools. The choice of effective ones for ensuring compliance with legal requirements depends on the social context of the country, its legal traditions, the legal consciousness of the population, etc. F. i., in August 2009, Eric Woerth (French Budget Minister) announced a list of 3,000 people with accounts hidden in Switzerland at HSBC. The policy sent a chill through taxpayers: 75,468 taxpayer households declared one or more accounts abroad in their 2009 tax return filed in 2010, up from 29,612 two years earlier (Crouzel, 2011). In terms of developing an effective system for the prevention of corruption in public procurement, Albania has laid a good foundation by significantly improving transparency through its comprehensive electronic procurement and e-appeals system and in terms of giving participants access to redress by developing its review system (Jance, 2024, p. 97). Economic development and cultural background affect the number of offers for a typical public procurement call. The Eastern and Central and Eastern European have a shorter history of public procurement and a weaker procurement culture (Tátrai, 2023, p. 254). Italian law states that the national government can impose the dissolution of any local government whenever direct or indirect links emerge between local elected politicians and criminal organizations, or when there are undue pressures, which influence or compromise the normal functioning of the local administration (Fazekas, 2021, p. 1146). Eliminating political favoritism saves around 180 million euros per year for Lithuanian tax payers compared to 5–6 million euros per year spent to finance political parties. The ban on corporate donations proves to be an effective means to discontinue political favoritism in the awarding of public procurement contracts (Baltrunaite, 2020, p. 579). A successful organizational solution to the problem of corruption in public procurement is offered by the public authorities in Denmark, where, instead of requesting ready-made solutions, tender participants are provided with a problem for which they must propose a solution. The best solution is then evaluated and chosen by the tender organizer.

During the dominance of paper documentation, some investigations into financial offenses were virtually impossible

due to lengthy procedures for obtaining requested information, processing it on paper, and similar challenges. This trend is now eliminated with the spread of digital data formats in matters of integrity in the administration and control of public procurement, and the ability to involve AI in processing this data. The predicted law enforcement effect of these digital tools arises from the transparency of data about the subject and conditions of public procurement: ex ante transparency is measured by the share of missing information in calls for tenders; ex post transparency is related to contract award. However, transparency requirements might be less efficient for preventing prebidding collusion between firms than corrupt practices between agencies and firms (Bauhr, 2019, p. 503, 500). Digital corruption risk management (CRM) in the field of public procurement is a specific set of procedures and requirements to detect, assess, and mitigate corruption offenses at any stage (management and control) using algorithms in digital programs. These programs process data on contracting authorities, "organized crime proxies in public procurement" (Fazekas, 2021, p. 1156), as well as procurement participants, their close associates, and related parties, ensuring the absence of conflicts of interest or criminal collusion. The concept of conflicts of interest shall at least cover any situation where staff members of the contracting authority or of a procurement service provider acting on behalf of the contracting authority who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure (EU 2014/24 art. 24). In addition to directive, preventive, and detective controls, it is important to regularly conduct a formal risk assessments (monitoring) and analyse them based on the likelihood and impacts of each type of risk (financial, technological, economic, payment, and procurement risk), that suits the organisation's objectives (Ilias, 2023, p. 192).

In this regard, before participating in public procurement, entrepreneurs, all members of management, and chief accountants

of participating organizations must submit declarations of income and integrity. Leadership is the key to anticorruption performance (Tabish, 2012, p. 33). The tone at the top establishes the cultural environment and organizational values for risk management and internal control (Ilias, 2023, p. 191). Furthermore, automated information-retrieval, reference, and management systems, along with registers, become sources of input data for these programs. Specifically, these include core registries such as the demographic registry (with data on residential addresses, civil status acts, etc.), land registries (land cadastre), registries of buildings and structures, vehicles, property rights to real estate, legal entities, individual entrepreneurs, public formations, and the State Land Cadastre. Upholding the public interest in public procurement within complaint review procedures necessitates the use of data from anti-corruption registers: persons who have committed corruption or corruption-related offenses, declarations of persons authorized to perform functions of the state or local self-government, etc.

Innovative for anti-corruption analysis of public procurement are algorithms for processing data from the accounts of procurement participants (or their close associates) on Facebook, Instagram, TikTok, Weibo, Tencent, Douyin, Xiaohongshu, and other social networks. Other information about such participants includes: 1) expenses on advertising their goods (services, works) and its content; 2) feedback from national and international partners regarding collaboration and the integrity of such partners; 3) parts of the biographies of the company's executives and chief accountant (excluding family member data), particularly related to their education, professional career, and social recognition.

The security of public procurement is enhanced at the stage of submitting tender proposals by including advertising data about their goods. Legislative standards for advertising require the accuracy of data about the advertised object. Additionally, the results of studying the history, customer reviews, and other advertising data of the tender participant serve as a strong argument for a balanced evaluation of their tender proposal and their ability to fulfill contractual obligations. Armed with this data, an honest tender

participant gains evidence against a corrupt public procurement organizer, and vice versa. The task of processing advertising data from tender participants is simplified by the trends toward digitalization and the mediation of AI." Global ad expenditure is now expected to grow 7.8% in 2024 to $989.8bn, according to GroupM's report. GroupM expects the global ad industry to surpass $1tn in revenue next year – one year earlier than previously forecast. Digital is expected to make up 70.6% of the total ad market in 2024 ($699bn). Last year, the largest five digital companies (Google, Meta, ByteDance, Amazon and Alibaba) accounted for 77.7% of the digital market. The boom in artificial intelligence products, services and enabling hardware has likely helped boost business investment (Benjamin, 2024; Makarenkov, 2024, p. 218).

As public procurement (preprocurement, contracting and contract period phases) evolves toward performance-orientation, with increasing collaboration between parties, the importance of new capabilities in organizations is growing and dyadic capabilities become more relevant: for practitioners seeking to develop sustainability or innovation objectives, as well as essential organizational capabilities; to private supplier managers, capability to define value/benefit in the preprocurement phase, objects that are aligned to societal benefits. With transparency, a supplier can build trust to its business relationships which is valuable asset if some flexibility is sought during contract period (Loijas, 2024, p. 139). The relevance of determining rankings for public procurement authorities and tender participants is particularly significant. These rankings take into account the mentioned data, along with the number and volume of integrity contracts properly executed without inflated prices, concluded as a result of winning public procurement competitions. Such rankings are compiled annually by a digital program administered by the authority responsible for compliance with public procurement laws. Rankings for contracting authorities and public procurement participants help to assess the actual risk of corruption in this field. The higher the risk level, the more frequently and thoroughly anti-corruption safeguards are applied by public authorities and open civil society.

Strategic public procurement is the deliberate use of procurement resources and processes to achieve both public management and policy-driven objectives (Patrucco, 2024, p. 15). The financial scale and strategic significance for national interests of industries such as mining, energy, machinery, aviation, shipbuilding, automotive, aerospace, and other capital-intensive, including innovative, sectors of the economy necessitate additional data analysis for public procurement processes relevant to these sectors. F. i., as a substantial component of capital investment for mining enterprises, equipment procurement directly impacts company productivity and economic returns. Effective equipment procurement strategies can help companies reduce procurement costs and enhance mining efficiency, thereby promoting sustainable development (Chang, 2024, p. 1).

By mobilizing the public sector's buying power, procurement could ensure that the public sector acted as a 'responsible buyer' and that the adopted digital technologies met public interest goals such as trustworthiness, responsibility, explainability, transparency, safety, or high levels of robustness, interoperability, and cybersecurity (Sanchez-Graells, 2024, p. 289). Effective procurement data for goods in strategic industries must aim to eliminate corruption obstacles from individuals with significant economic and/or political influence. Accordingly, the anti-corruption component of their procurement procedures must include data from at least the register of oligarchs, the transparency register, as well as other national and international information and communication systems that ensure the collection, accumulation, protection, accounting, presentation, processing, and provision of information. The analysis of this information ensures the maximum protection of the public interest, which, in the context of knowledge-intensive sectors of the economy, aligns with national interests. In this case, any corruption or violation in public procurement poses a direct and real threat to national security. Its permanence, recurrence, and scale inevitably trigger other economic threats to national security, compounded by political and external military threats. Together, these deprivations undermine the nation's material base for countering both external aggressors and large-scale internal criminals.

Table 2: Illustration of the regulation's legal formalization in Ukraine for demographic, familial, property, and other data registers

№	Laws titles and details	Data register type
1	**2**	**3**
1	On the State Registration of Legal Entities, Individual Entrepreneurs, and Public Formations, dated May 15, 2003, No. 755-IV	Entrepreneurial interests
2	On the State Registration of Property Rights to Real Estate and Their Encumbrances, dated July 1, 2004, No. 1952-IV	Real estate
3	On the State Registration of Civil Status Acts, dated July 1, 2010, No. 2398-VI	Familial ties
4	On Access to Public Information, dated January 13, 2011, No. 2939-VI	Procedures ensuring the right of access to information held by public information managers and of public interest
5	On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identity, or Special Status, dated November 20, 2012, No. 5492-VI	Residence and other demographic data
6	On the Prevention of Corruption, dated October 14, 2014, No. 1700-VII	The content of income declarations of public officials and any corruption offenses committed by them
7	On Public Procurement, dated December 25, 2015, No. 922-VIII	History of procurement procedure appeals; received tender proposals
8	On Stimulating the Development of the Digital Economy in Ukraine, dated July 15, 2021, No. 1667-IX, "Diia City"	Companies engaged in computer programming, software publishing, IT education, data processing, web portal activities, research, and experimental developments in natural and technical sciences regarding ICT, services related to virtual asset circulation, and/or cybersecurity, as well as compliance with decent wage and net profit indicators

End of table 2

1	2	3
9	On Preventing Threats to National Security Associated with Excessive Influence of Individuals with Significant Economic and Political Weight in Public Life (Oligarchs), dated September 23, 2021, No. 1780-IX	Significant economic and political weight of individuals in public life
10	On Lobbying, dated February 23, 2024, No. 3606-IX, and the Regulation "On the Transparency Register" approved by the Cabinet of Ministers of Ukraine on October 15, 2024, No. 1175	Lobbying subjects and their reporting (transparency register)
	General legal basis for data exchange of public registers	
11	On Public Electronic Registers, dated November 18, 2021, No. 1907-IX; On the Features of Providing Public (Electronic Public) Services, dated July 15, 2021, No. 1689-IX; Regulation "On the System of Electronic Interaction of State Electronic Information Resources 'Trembita'" and other regulatory acts approved by the Cabinet of Ministers of Ukraine on September 8, 2016, No. 606 "Certain Issues of Electronic Interaction of Electronic Information Resources"	Rules for exchange between some basic public data registries

4.2. Legal algorithms for software codes to prevent corruption distortions in public procurement

An essential direction in public procurement involves the further development of the electronic procurement system, the introduction of new tools, and the digitalization of processes. These measures are key to increasing the transparency of contracting authorities' actions, reducing the risks of discrimination against business entities during public procurement participation, and lowering operational costs for both contracting authorities and participants during procurement processes (Strategy for Reforming the Public

Procurement System for 2024–2026 and the Operational Plan for Its Implementation in 2024–2025, approved by the Cabinet of Ministers of Ukraine on February 2, 2024, No. 76-p). In the public procurement system, the creation of additional opportunities and practices for small and medium enterprises is foreseen (Strategy for Recovery, Sustainable Development, and Digital Transformation of Small and Medium Enterprises until 2027, approved by the Cabinet of Ministers of Ukraine on August 30, 2024, No. 821-p). To effectively support generating new employment, assisting small and medium-sized businesses, safeguarding the environment, and promoting research and innovation, public procurement procedures must be well-designed (Tălpig, 2024, p. 451).

According to strategic plans, the digital formalization of algorithms to eliminate corruption in public procurement will enable compliance with quality standards for all goods (works, services) funded by public funds. This will also demonstrate the absence of any management non-compliance with any requirements that Ukraine needs, taking into account its integration progress towards the EU market, where only the products that fulfil requirements providing a high level of protection of public interests, such as health and safety in general, health and safety in the workplace, the protection of consumers, the protection of the environment and public security and any other public interests (EU 2019/1020). Looking at the current practical issues arising from Directive 2014/24/EU, there are two areas where the existing technical solutions have been lacking. These are contract (and contract changes) registration and the ESPD/e-certis information exchange system. Furthermore, it is possible to conceive the usefulness of smart contracts to be used in the context of electronic auctions for simple goods contracts. Currently, contract award notices and modifications are sent manually to the Official Journal of the EU to comply with the requirements of Article 84 of Directive 2014/24/EU (Telles, 2022, p. 187).

The study identifies corruption as a notable obstacle to achieving efficiency, sustainability, and budgetary objectives (Tălpig, 2024, p. 460). The elimination of corruption from public procurement is facilitated by the procedure of consultations of the contracting

authority with potential suppliers and other market participants. The competitive dialogue approach aims to align the complex needs of contracting authorities with the potential solutions offered by suppliers. The procedure is especially useful in large complex projects, where it is often difficult for contracting authorities to define the means of satisfying their needs or to assess what potential suppliers are offering in terms of technical, financial or legal solutions (Lenderink, 2022, p. 663). Openness to competition is subject to multiple thresholds depending on the nature of the good or service and on the authority purchasing it (Disdier, 2021, p. 3073). For example, the relevant law of Ukraine mentions this institution of consultation, but does not specify the criteria for the mandatory application of this procedure. As a result, the application of this institution depends on the will of the public procurement customer, which is actually distorted by bribery on the part of the participant in these procurements who seeks to eliminate competitors.

Beyond blockchain, organizations are investing in other technologies, including digital training solutions, Internet of Things, and cloud computing. Cloud computing minimizes communication problems, strengthens collaboration in a safe way, and helps improve their processes because data collection and analysis is easier (Matthews, 2022, p. 13). Now, and for the foreseeable future, there is a regulatory gap that leaves the adoption of digital technologies by the public sector largely unregulated, as well as exposed to regulatory capture and commercial determination. The existing and growing gap in the public sector's digital skills undermines the ability of public procurement to act as an effective gatekeeper and regulator. A digitally unskilled public buyer is a weak buyer unable to critically scrutinize claims around the offered digital technologies, and thus exposed to the 'policy irresistibility' of 'tech fixes' for governance problems (Sanchez-Graells, 2024, p. 288, 289). In the field of public procurement integrity control, supervisory bodies, such as those in Ukraine, are constrained by outdated legislative norms. They lack access to numerous national and international registers. While the obligation to provide information requested by the Antimonopoly Committee is prescribed by law,

penalties or other liabilities for failing to provide such information are only stipulated within the laws governing economic competition. There is currently no financial or other liability for ignoring requests from the Antimonopoly Committee in cases concerning public procurement complaints under Ukrainian law. In the best-case scenario, the contracting authority and procurement participants are motivated to provide the requested information. However, this data is often insufficient to uncover latent corruption links, distortions, and other offenses, including those forming the basis of a complaint. Moreover, such data may only be accessible to administrators and users of state registers, law enforcement agencies (investigators, prosecutors), and similar entities for whom no legal procedures have been defined to furnish information to the Antimonopoly Committee in its investigations of public procurement complaints.

Current legislative procedures for appealing illegal actions in public procurement frequently simulate the ability to safeguard public interests. This may be driven by elaborate corruption schemes which also involve cartels among bidding firms faking competition (Fazekas, 2021, p. 1157). Complainants have virtually no access to the vast range of data required for a systemic analysis that could substantiate the existence of a "corrupt agreement among public decision-makers and entrepreneurs" (Fazekas, 2021, p. 1144), such as conflicts of interest, collusion among participants, bribery of contracting authorities, and similar violations. At best, they manage to mobilize available data and attach a series of indirect evidence of corruption practices in public procurement. The Antimonopoly Committee often adopts a passive role in such investigations, relying solely on complaint materials and its existing data. Its initiative in such matters is more an exception than a legislative obligation. For instance, "To analyze data indicating violations of public procurement legislation, the following may be used: information published in the electronic procurement system; information contained in unified state registers; information in databases accessible to the central executive body responsible for implementing state financial control policy" (paragraphs 7–10 of part 2, Article 8 of the Law of Ukraine "On Public Procurement",

dated December 25, 2015, No. 922-VIII). There is no mention of any obligation to collect data, evidence, or similar materials. Such an approach appears as a legal subversion, as it is evident that the defined procedure cannot ensure the inclusion of all critical data necessary for the correct resolution of a case.

Evasion of efforts to prevent corruption in public procurement is evidenced by the absence of a system for information exchange within the existing procedures for handling complaints regarding violations in such procurement, as well as the lack of an institution to eliminate the actual grounds for such violations. At the same time, such systems exist for fiscal purposes. For example, in Ukraine, the tax service receives information from notaries and state registrars about the registration of property rights by individuals to real estate (see Procedure for Electronic Interaction of Information Systems of the Ministry of Justice of Ukraine and the State Tax Service of Ukraine Regarding the Confirmation of Data on Individuals During State Registration of Property Rights, approved by Order of the Ministry of Justice of Ukraine and the Ministry of Finance of Ukraine, dated January 31, 2022, No. 280/5/41). The existing electronic interaction system for state electronic information resources in Ukraine, "Trembita," should become part of the analytical framework for handling complaints related to public procurement and preventing corruption in such procurement. This can be achieved through corresponding algorithms, software codes, programs, and other digital tools.

The tasks of digitizing legal algorithms for any sphere of public governance, including the effective prevention of corruption in public procurement, involve specialists from at least the fields of law and programming. Depending on the specifics of the subject matter for which an anti-corruption algorithm is being developed, expertise in relevant specializations becomes essential. «Involving independent experts or external procurement professionals in the tender process could help to prevent risks for corruption and favoring incumbent suppliers. Their judgments are sometimes more easily accepted by other stakeholders, like citizens or political parties» (Grandia, 2023, p. 102). In public procurement, this includes

commodity experts and professionals with practical experience in services and works. Their knowledge of variability, stability, the content of essential conditions, processes, and obstacles in operations constitutes the foundational basis for populating software codes with meaningful content. Suitable organizational forms for such developments may involve cooperation between entrepreneurs and experts familiar with corruption-prone aspects of public procurement, as well as universities, research institutions, and other organizations. For example, in Ukraine, entrepreneurs listed in the registry of the legal regime "Diia City," specializing in business innovation, digital infrastructure development, attracting investments, and skilled professionals, could play this role. An innovative example comes from Denmark: instead of specifying detailed solutions, the city defined the problems and invited innovative solutions from the market; innovative laboratories and pilots: the city has established living labs and pilot projects to test and evaluate innovative solutions in real urban environments; this enabled a more informed procurement process and reduced the risk associated with implementing untested technologies; collaboration with start-ups and technology companies: Copenhagen has actively engaged with startups and technology companies, encouraging collaboration and co-creating solutions (Manta, 2024, p. 9).

The member states of the multilateral convention "On Mutual Administrative Assistance in Tax Matters" 2011 and "Model Tax Convention on Income and on Capital" 1992 (apply to persons who are residents of one or both of the Contracting States) provide a basis for all forms of information exchange – on request, spontaneous, and automatic (OECD 2011, 1992–2017). In particular, since 2009 much progress was made by the OECD, EU and the Global Forum on Transparency and Exchange of Information for Tax Purposes in improving transparency and exchange of information on request. Since July 15, 2014 the Common Reporting Standard (CRS) has emerged as sets of financial account information to be exchanged, the financial institutions required to report, the different types of accounts and taxpayers covered, as well as common due diligence procedures to be followed by financial institutions. It was

developed and approved by the OECD Council in response to the G20 request and calls on jurisdictions to obtain from their financial institutions and automatically exchange that information with other jurisdictions on an annual basis (OECD 2017, p. 3, 9). In line with this trend of international fiscal vigilance by public authorities, Ukraine, albeit with a significant delay of 10 years, has implemented the international standard for the automatic exchange of financial account information and country-by-country reporting (see Law of Ukraine "On Amending the Tax Code of Ukraine and Other Legislative Acts Regarding the Implementation of the International Standard for Automatic Exchange of Financial Account Information", dated March 20, 2023, No. 2970-IX).

States consistently prioritize effective tax administration. However, comparable, more targeted, consistent, or determined efforts in overseeing the efficiency of public procurement or other expenditures from public funds – formed through collected taxes – are less evident, particularly at the international or regional levels. For instance, even the European Anti-Fraud Office, known for its authority, sometimes initiates its anti-corruption investigations only after journalists and/or U. S. criminal justice systems have conducted their inquiries. This occurs despite the fact that EU officials may be subject to undue influence from U. S. companies, or vice versa. For example, throughout 2023, multiple individuals – including subjects of US and Ukrainian investigations – solicited bribes from Sinclair & Wilde to secure payment of the remaining $14.5 million owed to it. Sinclair & Wilde refused and reported these solicitations to US and Ukrainian authorities. Law enforcement organizations and defense officials have examined the uniforms and found the prices charged by Sinclair & Wilde to be BELOW fair market value, particularly when you account for the costs associated with shipping and logistics (Delnero, 2024).

Key challenges for the future include the need for more systematic collection of information on public procurement policies at the international level and progress in terms of their transparency (Disdier, 2021, p. 3086). The effectiveness of anti-corruption infrastructure is further weakened when multinational corporations attempt to exploit national budgets through public

procurement, especially in states or unions where top officials are easily bribed and/or temporarily beyond the control of other branches of government – parliaments, courts, or law enforcement. The scale of corruption is exacerbated when military forces are deployed to address problems stemming from the incompetence of public authorities, leading to significant losses caused by corruption in other branches of power. Such circumstances indicate a long-term inability to ensure the efficient expenditure of substantial public funds, resulting in the loss of national interests and posing a genuine existential threat to the nation. For example, Dalligate and the aggressive tobacco industry lobbying case (2009–2014): EP's Members complained about "unsolicited tobacco lobbyists turning up in their offices; numerous invitations to drinks, dinners and cocktail events; targeted social media and email campaigns coordinated by tobacco companies; indirect lobbying through small retailers, anti-counterfeiting firms and farmers' groups; and, allegations of industry-sourced amendments." At least 161 of the tobacco giant Philip Morris International's staff had (undisclosed) lobby meetings with no less than 233 Members of the European Parliament to attempt to influence the European Parliament's decision-making on the final version of the Tobacco Product Directive, a new law that strengthens the rules on how tobacco products are manufactured, produced and marketed in the EU (Hörz, 2014). It is known that the adoption of this Directive, following the neutralization of the tobacco lobby's corrupt influence on EU public authorities, has led to a two-thirds reduction in the number of smokers. Part of the corruption of this lobby involved the discrediting of EU Health Commissioner John Dalli. Although this resulted in his dismissal, journalists and members of the European Parliament established that John Dalli acted with integrity and was free from corruption. The accusations against him became possible due to procedural violations by the European Anti-Fraud Office.

The genuine desire of countries to address the embezzlement of public procurement funds is often demonstrated by their implementation of legal decisions and practices already developed by the EU, the United States, Japan, Singapore, and other nations with strong jurisdictions, effective criminal justice systems, and robust

international cooperation mechanisms. Besides existing alternative data sources, such as the Opentender platform under the EU co-founded DIGIWHIST project, an upcoming Public Procurement Data Space (PPDS) project aims to create a digital platform at the EU level, integrating procurement data scattered at the EU, national, and regional levels (Nemec, 2024, p. 2159). Through digital platforms, a significant aspect is access to a broader group of suppliers at the most optimal time, as well as countries are becoming more interconnected, thus exchanging of ideas, technologies, and good practices. This can be particularly beneficial in sectors where specific expertise is required, and which, practically in a very short time, the expertise can be made available to the applicant and with optimized resources from a financial, human, and time point of view (Manta, 2024, p. 2). F. i., at present, there are no rules, other than those in respect of anti-money laundering, for the provision of services related to such unregulated crypto-assets, including for the operation of trading platforms for crypto-assets, the exchange of crypto-assets for funds or other crypto-assets, and providing custody and administration of crypto-assets on behalf of clients. The absence of such rules leaves holders of those crypto-assets exposed to risks, in particular in fields not covered by consumer protection rules. The absence of such rules can also result in substantial risks to market integrity, including in terms of market abuse as well as in terms of financial crime (EU 2023/1114, item 4).

All these decisions and practices relate to the production of material goods (such as labor remuneration and consumer rights), the digital format of financial and other data, and the management and control of public revenues and expenditures. F. i., these are rules on the information on payers and payees accompanying transfers of funds, in any currency, and on the information on originators and beneficiaries accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing (EU 2023/1113). An essential practice involves EU rules stipulating that disputes over tender procurement are resolved by the judiciary, where all evidence in a case can be collected at the preparatory stage

of the proceedings. Administrative review by antimonopoly or other public administration bodies does not allow for such comprehensive evidence collection. Simultaneously, the very existence of effective judicial review designed to ensure compliance with Union law is the essence of the rule of law. This is true, in particular, for the judicial review of the validity of measures, contracts or other instruments giving rise to public expenditure or debts, inter alia, in the context of public procurement procedures which may also be brought before the courts (EU 2020/2092). In particular, tenders which do not comply with the procurement documents, which were received late, where there is evidence of collusion or corruption, or which have been found by the contracting authority to be abnormally low, shall be considered as being irregular. In particular tenders submitted by tenderers that do not have the required qualifications, and tenders whose price exceeds the contracting authority's budget as determined and documented prior to the launching of the procurement procedure shall be considered as unacceptable (EU 2014/24 art. 26). To guarantee transparency, accountability, and integrity, public procurement processes must include safeguards such as professional oversight, accessible procurement data, and rigorous legal compliance. Key practices include publishing tender notices, bid evaluation criteria, and award decisions, as well as implementing robust anticorruption measures like conflict-of-interest policies and fraud detection mechanisms. Ensuring fairness and impartiality in the bid evaluation process is also critical, supported by transparent grievance mechanisms for suppliers (Patrucco, 2024, p. 5).

Therefore, public authorities are evidently interested in organizing information about citizens and entrepreneurs for tax purposes, which is beneficial for combating both the shadow economy and associated crimes. However, without ensuring integrity in budget expenditures, such fiscal activities merely erode the material foundation of a nation. The lack of confidence in public authorities' effective use of budgetary funds creates natural-law grounds for entrepreneurs, their employees, and other citizens to hide resources from irresponsible or negligent public officials, particularly in cryptocurrency assets.

CONCLUSIONS

1. Variations in the legal certainty of anti-corruption policy that enhances national security correspond to the classification of consciousness into legal, moral, and other normative types (based on the criterion of the type of requirement, norm, etc.); individual, group, and general social (based on the subject); legal, political, economic, spiritual-cultural, and others (based on spheres of social life); automatic, dogmatic, marginal, conformist, and creative; active and passive. The characteristics of legal certainty correlate with the traits of human consciousness up to the point where certainty ceases to be determined by its location. By definition, law is naturally social, and the facts of legal reality are not always rational or conscious. In this regard, the certainty of law is also socially determined, though it is always anthropocentric in nature.

Unconscious human acts reveal subconscious and supra-conscious (of the entire society and the universe) sources of defining law by humans. At the same time, such general obligations may also be devoid of the volitional, sensory, and/or emotional component of anthropic energy. Accordingly, it is nourished by the global rational or a fraction of it, where compliance with universal human values signifies goodness, virtues, and spirituality. However, simply imposing obligation and/or generality on a norm (requirement) does not make it legal, as it requires an axiological component of creating human life and its quality at the highest level of civilizations, such as the EU or others with which one identifies.

The above allows us to assert that the definition of anti-corruption law occurs at different levels of intellectual hierarchy, depending on the source of legal information and the combination of such sources. The temporal factor influences the gravitational force of law in a specific social context, namely: law exists where and when the knowledge of law and efforts to express it have been sufficient; conversely, law disappears, or in the best case, its form dominates over its content when distortions of law, human flaws, etc., prevail. Members of society form a united whole and constitute a nation only in the first scenario of legal knowledge quality.

Cultural artifacts become the form of expressing the legal certainty of the virtuous course of social relations. Among them, legislative and law enforcement acts of parliament, the executive, and the judiciary stand out the most, reflecting the rational side of law. Painting, literature, and cinema capture the sensory dimension of legal life. A cultural artifact not only records distortions in the content of law but also disseminates this knowledge to others for the awareness of legal reality, distinguishing between legal and wrongful, and ultimately forming the appropriate legal reaction. Legal definitions articulated by a national or other social community must necessarily be confirmed by their actions, practices, facts of social reality, and legal reality. Otherwise, the separation of form from content, fact from words, leads to violence and the disorder it governs, social conflicts on the scale of war, excluding the rule of law, openness to progress, and ensuring the interests of the nation and alliances of nations (EU). The simultaneous coexistence of a high level of corruption in real life and its formal and/or verbal denial signifies an illusion of integrity in society and marks its members as masters of such illusion.

2. The ternary concept proposes that the 'corruption-anti-corruption' dichotomy is transcended by a crucial third component. This component encompasses legal norms and practical measures that neutralize malicious intentions and balance them with the virtuous part of human nature. In practical terms, the ternary aspect is that anti-corruption policy is not separate, but part of national security. The dysfunctionality of the first component leads to the destruction of the second component, which is exploited by a third party, for example, an external military aggressor. Since a nation is not isolated but has external connections, these connections work in a positive way through the borrowing of legal standards for anti-corruption institutions. It turns out that two components of the nation (anti-corruption policy and its national interests) are fully realized only with proper interaction with the external environment – nations that are more developed. Everything in totality, under current conditions, cannot be further improved without digital technologies. This again results in three components: national law, international law, and

digital technologies. Moreover, anti-corruption law, as expressed in legislation, belongs at least to the fields of criminal law, administrative law, and, necessarily, a third field: commercial, financial, labor law, etc. The division of anti-corruption law into substantive and procedural law is meaningful only if there are adequate actions from those to whom these norms are addressed, both public officials and criminal and administrative justice bodies that apply anti-corruption legal norms. At the transnational level of anti-corruption interaction, the effect is also not achieved merely through the implementation and/or application of legal norms. Effectiveness requires consideration of the economic and spiritual-cultural foundations of the nation where anti-corruption norms are applied, as they determine the nature of social relations upon which we impose legal requirements.

3. Corrupt personnel policy significantly depletes the content of the conflict of interest, particularly regarding the loss of effectiveness due to hiring employees not based on professional criteria that meet public demand and constitute public interest but on other factors that serve private interests contrary to the public interest. This causes an organizational dysfunction in legal relations, especially in ensuring public interest. At the same time, the private interest of the person conducting the corrupt personnel policy is to obtain money, sexual favors, and/or satisfy other personal needs, motivated by kinship, friendship, or other personal and/or material reasons. The private interest of the person being appointed or elected to a position, i.e., the beneficiary of corrupt personnel policy, is to hold the desired position and gain associated benefits. Accordingly, the conflict of interest manifests itself in organizational/managerial terms as improper personnel provision, where the personal interest of two individuals (the one who appoints/elects and the one who is appointed) is achieved at the expense of the public interest. This dysfunction reveals legal patterns, namely: (1) the professional incapacity of corrupt officials is compensated by the work of honest citizens; (2) the efforts of such honest citizens are not reimbursed by the society where these corrupt practices exist; (3) the resources of honest citizens and their supporters (relatives, loved ones, etc.) are limited in energy and time; (4) an organization saturated with corrupt individuals is necessarily

ineffective; (5) absolute dominance of such dysfunction belongs to public law organizations; (6) a society saturated with such organizations has structural and systemic corruption problems. To eliminate this real corruption threat to national security, it is necessary to explicitly prescribe in the Criminal Code the composition of a criminal offense and criminal liability for corrupt personnel policy of appointing/electing individuals incapable of acting effectively in these positions, particularly in comparison with other candidates.

4. Anti-corruption legal requirements are described using lexical means professionally integrated into a legal text that logically corresponds to the current social reality. The ordinariness and archaic nature of formally reflected constructions do not correlate with the originality and novelty of the subject of legal regulation. A legislator who does not utilize the legal potential of the anti-corruption legal norm discourse leaves society outside the context of legal reality and natural law, turning legislation into an artificial means of manually combating corruption. Under such conditions, the anti-corruption infrastructure appears to lack historical logic.

5. The interference of the corruption concept in legislation is determined by the degree of distortion of the legal content of regulated social relations – labor, tax, administrative, as well as pension, healthcare, and other social security. The phenomena of employers avoiding formal-legal employment of workers and/or concealing the actual salary paid (so-called “shadow employment” / “wages in envelopes”), its scale exceeding 5%, and its long-term nature indicate the reaching of a dangerous level of corruption distortions for the nation. Under these conditions, the legislation in labor, tax, and social security profiles formally exhibits dysfunction. Public interest is not merely violated due to employer dishonesty to satisfy their private interests but is also threatened by an uncontrollable and negative trend of financial, economic, and social capacity losses of the nation. Accordingly, the number of violations concerning legal employment and wages, which ontologically fall under labor, tax, and social security law, has transitioned into a corruption phenomenon. Anti-corruption norms become part of migration and/or administrative law in the context of addressing these issues

in countries where arbitrariness against migrants is observed, the shadow economy exceeds 15%, and/or a significant percentage of the population lives below the poverty line.

The aforementioned profile legislation requires strengthening through the rigidity of anti-corruption law, which specializes not only in bribery, illicit enrichment, favoritism, and other classical corruption compositions that directly destroy public interest but also in non-classical ones, where the destruction of public interest and/or accumulation of significant negative risks occurs due to the synergy of large-scale, long-term, and/or other socially resonant violations of private employee interests. The complexity of predicting and/or controlling losses from such synergy is further compounded by its foundation in three economic and fundamental branches of law for national life – labor, tax, and social security. Within their requirements, the main activities occur-material goods are reproduced, improved, accumulated, and distributed. Dysfunction in this means functionality in an unlawful, including criminal, dimension of social relations, which directly threatens national security by depriving it of its foundation – finance and economic development.

For the top-20 countries in the "Rule of Law" and "Freedom from Corruption" rankings, pure and relatively homogeneous violations of public interest committed by public authority entities to satisfy their private interests generally exhaust the subject matter of anti-corruption law regulation. Countries ranking lower in these indices are interested in neutralizing not only this type of corruption but also its consequences and the heterogeneous compositions of corruption offenses it generates. These offenses manifest as employers simultaneously distorting legal requirements related to social security, labor, and tax legislation, expressed in illegal employment and wages.

The materialization of responses to these distortions occurs through amendments to criminal code provisions. Specifically, a corruption offense concerning labor, tax legislation, and social security law committed by an employer is defined as "the absence of the formal-legal fixation of employment and/or the salary amount of an employee as required by law." A public official

responsible for overseeing employers' compliance with this legal norm commits an administrative corruption offense if they fail to take the legally prescribed response measures, do not implement all of these measures, and/or apply them untimely. Such acts constitute a criminal offense if they relate to any form of written, authorized reports concerning such employer violations from at least 10 individuals, leading to serious bodily injuries, death, and/or other grave consequences.

These criminal law provisions should be structured as separate sections within the criminal code articles dedicated to official negligence and abuse of authority by an official of a legal entity, regardless of its organizational and legal form. Correspondingly, criminal liability should extend to tax and/or financial decisions of the parliament that lead to the impoverishment of hired workers, the loss of constitutionally guaranteed opportunities for reproduction and/or development, and, consequently, economic security of the nation, which consists of satisfying the economic interests of its members, including the state's citizens.

The duration of this interference of anti-corruption law in criminal law should persist until the formation of a stable legal practice and the tradition of employers legalizing work and employee salaries. One of the indicators of this process will be the country's inclusion in the top-20 rankings mentioned above.

6. Cyberspace has enabled business executives not only to conceal violations of their fiduciary duties but also to do so more rapidly. Essentially, the digital space has created an additional legal reality for financial transactions and communication among organized corruption-related criminal entities, complicating their tracking amid the constant lag of digital jurisdictional capabilities and/or the corruption of criminal justice and/or public administration bodies in several states. The variability of their ingenuity necessitates the processing of commercial and personal data of entrepreneurs by the law enforcement divisions of the tax service. In addition to information from state registries, the determination of fictitious transactions lacking actual goods is facilitated by analyzing the entrepreneurs' electronic data

interchange systems, information from crypto markets, the dark web, and other sources relevant to the investigation.

The data volume required for detecting business fraud, its presence, and its circulation speed in cyberspace have minimized the effectiveness of traditional data processing models (paper records, witness testimonies, state registries, etc.). This has necessitated the widespread application of digital tools capable of counteracting this threat and the associated crimes it amplifies, such as human rights abuses, terrorism, wars, sabotage, espionage, and other forms of national security betrayal. Large language models and other deep learning methods, along with AI-based algorithms and models, allow for processing numerous, dynamic, complex, and multidimensional data on entrepreneurship, identifying signs of such crimes, revealing their nonlinear interconnections, and predicting their future developments.

Information systems that track variables such as personnel, raw materials, warehouses, equipment, transportation and logistics, production facilities, relevant economic activities, and other enterprise data transform them into quantities that are precisely known both quantitatively and qualitatively. The only variables remaining are the daily updates of these quantities, as processed by software, including large volumes of reports, messages, and other texts covering all periods of the enterprise's economic activity and its contractors. Collectively, information and communication systems, provided they prevent data leaks due to software vulnerabilities, enhance the capabilities of tax authorities in neutralizing fictitious business transactions and their predictive links to other crimes harming national security.

Data on money and other assets should be sourced from income declarations of entrepreneurs and any other individuals whose assets were involved in fictitious transactions. Financial liability for failing to submit such a declaration after a court ruling on such a case should equal the value of the undeclared assets. Other financial sanctions for fictitious business transactions should be aimed at compensating for the damage caused to public funds by concealing business profits that should have contributed

to education, healthcare, infrastructure, digital development, and sustainable economic policies through taxation.

7. In a global context, the effectiveness of law enforcement in most countries depends on the engagement of auditing, consulting, legal, and other companies that provide specialized expertise on events, payment flows, beneficiaries, intermediaries, and other valuable insights through their worldwide networks. The use of body cameras by law enforcement officers and surveillance cameras in public places has proven effective in improving criminological conditions in the United States, China, Japan, EU countries, and other highly developed nations, particularly in preventing the involvement of criminal justice officials in corruption and other economic crimes.

Video surveillance data, as well as AI-driven financial monitoring systems aimed at countering money laundering, raise issues of accountability, discrimination, bias, and other legal challenges related to confidentiality breaches (banking, notarial secrecy, etc.), timely and coordinated information exchange, fairness of decisions, and actual opportunities for explanation and oversight in jurisdictional processes. In this context, it is crucial that banking secrecy guarantees help maintain honest entrepreneurship and its competitiveness. Legally secured security in virtual currency circulation and other cyber transactions allows for leveraging these resources rather than opposing them as a consequence of mutually reinforcing crimes-corruption leading to money laundering, money laundering funding terrorism and/or aggressive wars, cyberattacks, criminal AI usage, and other cyber offenses. The issues of data confidentiality and compliance with legal requirements are significant and require careful regulation.

The integration of digital forensic tools into a unified mechanism for combating corruption-related money laundering and terrorism financing is legally reflected in a corresponding strategy, which should include sections on implementation directions and types of digital technologies used for this counteraction. In Ukraine, this strategy should be concretized through the further development of the “Safe Country” software-hardware complex. Crime statistics in Ukraine illustrate an upward trend in their investigation. In this

regard, digital systems capable of ensuring the effectiveness of such investigations are relevant, particularly concerning the use of virtual assets in cyberspace for committing crimes.

Parliament must define the concept of "cyberspace" in law; otherwise, there are no established boundaries for the extension of state sovereignty over criminal activities in the cyber environment, particularly regarding cryptocurrencies. Within different national jurisdictions, such regulation should take the form of a digital branch of international public criminal law addressing the conditions of transnational investigations of economic crimes, corruption, and terrorism financing involving numerous individuals and complex financial mechanisms.

8. Auditors are now engaged in analyzing documents in both paper and digital formats. 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. In this regard, the work of auditors is enhanced with the help of programmers and other necessary 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 anti-corruption blockchain consists of a system of programs for creating databases, exchanging information in the aforementioned areas of corruption risks for public interest. Relevant terminology and digital indicators of the material assets of potential subjects of corruption are input data for this blockchain. The next procedural stage in the forensic methodology of anti-corruption investigations involves summarizing, processing, and analyzing the information

from anti-corruption blockchains, formulating conclusions from these operations by artificial intelligence, which is then studied by human intelligence sufficiently trained for comprehensive understanding of the inter- and transdisciplinary subject of anti-corruption policy, multiplied and sometimes skillfully complicated by the synergy of dishonest actions by corrupt individuals.

The seizure of items related to corruption and associated crimes, along with other resources, should be carried out through searches that need to be conducted, if possible, simultaneously at the premises of all individuals connected to the corrupt individual, whether through personal, friendly, and/or business relationships. The return of funds requires the swift implementation of algorithms for identifying jurisdictional procedures and forensic examinations in the criminal process, namely: 1) entering into cooperation agreements in corruption/criminal cases between states; 2) detailing these agreements in respective contracts between criminal justice bodies (courts, prosecutors, specialized anti-corruption agencies, police, national security services, auditors, etc.); 3) approving documents (translation into the language of the executing state, notarized certification of the translation, apostilles on the translation and the authority of the issuing body), delivery of these documents to the executing body in the executing country; 4) monitoring the proper execution of all previous steps.

The latent nature and scale of corruption, and/or its commission by a group of individuals, are objective reasons for complications during the investigation of corruption offenses. These characteristics and the subject of corruption are interdependent. At least two people commit elementary corruption offenses. The scaling of corruption correlates with the number of accomplices, the duration of the commission, and/or the resources used to launder the proceeds obtained. Digital technologies simplify, accelerate, and expand the volume of corruption and related crimes. At the same time, as tools for combating crime, these technologies neutralize it, being enhanced by the capabilities of criminal justice bodies.

The legislative specification of covert investigative actions for countering corruption and related crimes, as well as corruption

within investigative actions themselves, will enhance their effectiveness. Breaching the confidentiality of investigative actions undermines their substantive, particularly covert, component. The lower the rule of law indicator and/or higher corruption indicators, the higher the likelihood of unauthorized disclosure of the confidentiality of investigative actions. The features of relevant forensic methodologies are determined by 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. Corrupt flaws within national criminal justice bodies and/or at other institutional levels undermine national security and can only be effectively overcome with sufficient external anti-corruption support, digital technologies, and AI resources (used to automate transactions with corruption assets in virtual form etc.). Although before the qualitative growth of globalization processes, including through the role of digital technologies in the information sphere, there was still a chance for each nation to independently overcome the destructive influence of corruption.

The primary task of the parliament has become the comprehensive regulation of legal relations that people establish in cyberspace for the purposes of illicit enrichment, laundering of funds obtained through corruption or other criminal means, and using these funds for the exploitation and deprivation of freedom of individuals (“human trafficking”) for forced labor, sexual slavery, and/or commercial sexual exploitation, as well as for financing drug trafficking, wars, terrorism, and other destructive activities, including through the use of AI resources. The core of this legislation will be composed of rules for the effective control over AI, the circulation of cryptocurrencies and other virtual assets, specification of wrongful actions in cyberspace, and the alignment of concepts defined in the laws of Ukraine on 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, particularly Chapter 12 "Special Features of Claim Proceedings in Cases of Unjustified Asset Recognition and Their Seizure in State Revenue." To accomplish this, 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) should be utilized. The work with digital tools in forensic methods to counter fraud, money laundering from corruption, and other cybercrimes should rely on relevant U. S. experience, particularly concerning the software and technical functionality of the SEC's Office of Strategic Hub for Innovation and Financial Technology and cooperation among the SEC, U. S. District Court and Courts of Appeals, FBI, U. S. Attorney's Office, and other criminal justice structures.

These legislative innovations will enhance the effectiveness of law enforcement and other criminal justice entities, ensuring proper cooperation among them to combat corruption, fraud, and other cyber-crimes. Today, cyberspace for virtual assets holds an equivalent significance to banks and treasuries for national currencies. The capabilities of public authorities to eliminate corruption as a genuine threat to national security, exacerbated by the use of cryptocurrency and other virtual assets in cyberspace, are reinforced by outlined legal measures amidst increasing AI investments. Such investments in AI are becoming a resource for solving tasks in both the creation and application of law, as well as the country's armed defense and prevention of sabotage in virtual environments and the information space – key components in the protection of our national interests.

9. The issue of corruption in public procurement is part of the broader problem of satisfying the improper motives of public officials. While bribes related to tax administration are limited to officials in tax authorities, in public fund expenditures, bribes become potentially accessible to all public officials managing these funds. Furthermore, without taxes, it is impossible to form public funds, the theft of which often occurs through schemes of kickbacks

or inflated prices for public procurement goods. Consequently, the goals of fiscal policy do not contradict the objectives of corrupt officials but instead create potential opportunities for unlawful enrichment. These legal patterns indicate that in countries with high levels of internal corruption, digital or/and paper formalized legal algorithms and practices emphasize the efficiency of fiscal policy rather than public procurement efficiency. This explains the inertia and neglect in strengthening existing mechanisms or creating new ones to address corruption in public procurement. The practical inactivity in this area is reflected in the number of criminal cases related to the embezzlement of public procurement funds, which, for years, fail to translate into effective anti-corruption policies focused on targeted, economically sound, and appropriately justified public budget expenditures rather than inflated spending.

The entity overseeing the integrity and legality of all public procurement participants, or a complainant, must be capable of gathering evidence in such cases. To accomplish this, they require full legal access to necessary data from registries and other sources. Currently, this is only feasible within the framework of criminal proceedings and/or judicial processes. Therefore, it is advisable to make public procurement complaint procedures judicial in nature, allowing parties to independently attempt to gather evidence. If denied, they could petition the court to obtain such evidence. The Antimonopoly Committee lacks these powers and cannot provide such support to complainants, rendering complaint reviews legally insufficient and substituting the rule of law in public procurement with its imitation. An alternative to addressing inefficiencies in combating corruption and other violations in public procurement is extending the application of administrative jurisdiction or criminal procedural rules to complaint procedures. These frameworks enable the collection of necessary data for a comprehensive evaluation of the validity or groundlessness of complaints.

In any case, a complaint about violations or dishonesty in public procurement constitutes a statement with evidence of a crime. This transcends the concept of a complaint in the administrative sense, where it pertains to private interests of citizens or entrepreneurs.

The legal nature of public procurement complaints is defined by the public interest. Notably, the concept of "public" appears twice in the terminology: in the title of procurement procedures and in the interest, they seek to protect. The value and importance of this type of public interest lie in its connection to finances – resources that have already been accumulated as a result of successive links in prior public interest efforts: labor participation, administration of entrepreneurship and its infrastructure, taxation, and budget fund management. This culmination of national labor efforts, represented by public funds, carries absolute liquidity, making it a prime target for misappropriation, including by illicit means. Accordingly, public funds cannot be adequately protected against embezzlement in public procurement through an administrative complaint procedure or passive approach to handling complaints. These procedures do not provide absolute protection. The judiciary and/or criminal procedural mechanisms are the only measures sufficiently robust to counter the misappropriation of such assets. Only these options, employed by developed nations via modern digital instruments, can ensure compliance by neutralizing dishonest motives for misappropriating public funds through procurement processes.

Without access to state registry data regarding demographic, familial, property and other characteristics of individuals and their property, complaints regarding procurement law violations cannot effectively safeguard public interests. The controlling authority's efficiency in such cases becomes ephemeral. Simultaneously, bribery and persistent price inflation in public procurement remain entrenched under such limited informational capabilities for both complainants and reviewing bodies. At a minimum, the oversight body should analyze registry data for procurement complaints involving items valued above a significant threshold for national public funds. In Ukraine, this threshold exceeds €22,000 (over 1 million UAH at the current exchange rate). Such analytics require appropriate data processing programs. Formally, this obligation and the necessary digital tools are integral to the legislative frameworks of economically developed countries. Ukraine should amend paragraph 7 of Part 2 of Article 8 ("Procedure for Monitoring Public

Procurement Procedures") of the Law "On Public Procurement" dated December 25, 2015, No. 922-VIII, replacing the term "may" with "must" and granting the Antimonopoly Committee, as the oversight body, the authority to work with registry data while ensuring compliance with information legislation. The qualification of corruption-related offenses in public procurement requires leveraging digitized datasets. Advanced digital tools and strict procedural frameworks can ensure that such offenses are systematically identified and neutralized, fostering compliance and safeguarding the culmination of a nation's labor and fiscal efforts.

Given the globalization of the information space, investment, financial, trade, and logistics markets, the threat of financing terrorism, war and other crimes from improper control over virtual assets in cyberspace, as well as Ukraine's integration into the EU's economic and administrative system, it is crucial to grant the body handling procurement complaints access to information about foreign enterprises participating in Ukraine's procurement processes. This requires agreements (memorandums) with relevant control bodies in the countries where such tender participants are registered, as well as with auditing and other companies possessing or having access to necessary enterprise data. Relevant legislative procedures must be adopted, and their implementation must be financially and organizationally supported. Building on this effort involves integrating data from court decision registries, journalistic reports, and other informational systems into computerized algorithms. These datasets should be processed by decision-support systems and related intelligent automated systems, including those driven by AI, overseen by antitrust and other public authorities at the national and EU levels.

SUMMARY

The mandatory nature of a legislative norm signifies its alignment with the axiological components of creation and the quality of human life at the level of the highest civilizations to which it aspires.

A legislator who fails to utilize the legal potential of the discourse of anti-corruption legal norms leaves society outside the context of legal reality and natural law, turning legislation into an artificial tool for manual corruption control. Under such conditions, the creation of an anti-corruption infrastructure loses its historical logic.

A prolonged and large-scale corrupt personnel policy leads to the organizational dysfunction of legal relations, initially destroying honest citizens and subsequently depriving territorial communities and nations of existential opportunities.

The phenomena of employers avoiding the formal legal employment of workers and/or underreporting salaries create a persistent and difficult-to-control risk of economic and social capability losses for the nation.

In countries with high levels of internal corruption, legal algorithms and practices emphasize the effectiveness of fiscal policy but not the efficiency of public procurement.

Corruption-related deficiencies in national criminal justice bodies and/or at other institutional levels can only be overcome by each nation with sufficient external anti-corruption support, as well as through the use of digital technologies. Within the jurisdictions of multiple states, the anti-corruption activities of criminal justice bodies are formalized in the form of a system of international legal norms concerning cyberspace, neural networks, and other aspects of digital data formats.

The legislative concept of “cyberspace” must allow for the determination of a state’s jurisdictional boundaries within the cyber environment.

Large language models and other deep machine learning methods, as well as algorithms and models from other subsets of AI, enable the detection of indicators, nonlinear interconnections, and the prediction of the further development of crime involving

entrepreneurs. A key data source for these systems should also be income declarations of entrepreneurs and their family members.

Modern digital tools and legal procedural frameworks are components of a contemporary legal mechanism for the full neutralization of crimes in public procurement, giving meaning to the fiscal efforts of a country's citizens.

ZUSAMMENFASSUNG

Die Verbindlichkeit einer gesetzlichen Norm bedeutet ihre Übereinstimmung mit den axiologischen Komponenten der Gestaltung und der Lebensqualität des Menschen auf dem Niveau der höchsten Zivilisationen, denen er sich zugehörig fühlt.

Ein Gesetzgeber, der das juristische Potenzial des Diskurses über Antikorruptionsnormen nicht nutzt, lässt die Gesellschaft außerhalb des Kontextes der rechtlichen Realität und des Naturrechts und verwandelt die Gesetzgebung in ein künstliches Mittel zur manuellen Korruptionsbekämpfung. Unter solchen Bedingungen verliert der Aufbau einer Antikorruptionsinfrastruktur ihre historische Logik.

Eine langwierige und groß angelegte korrupte Personalpolitik führt zu organisatorischer Dysfunktion in den Rechtsbeziehungen, zerstört zunächst integre Bürger und beraubt anschließend territoriale Gemeinschaften und Nationen ihrer existenziellen Möglichkeiten.

Das Phänomen der Vermeidung der formalen und rechtlichen Beschäftigung von Arbeitnehmern durch Arbeitgeber und/oder die Verschleierung des tatsächlichen Gehalts schafft ein dauerhaftes und schwer kontrollierbares Risiko für den Verlust der wirtschaftlichen und sozialen Leistungsfähigkeit einer Nation.

In Ländern mit einem hohen Maß an interner Korruption betonen rechtliche Algorithmen und Praktiken die Effizienz der Fiskalpolitik, jedoch nicht die Effektivität der öffentlichen Beschaffung.

Korruptionsbedingte Mängel in den nationalen Strafjustizbehörden und/oder auf anderen institutionellen

Ebenen können von jeder Nation nur durch ausreichende externe Antikorruptionsunterstützung sowie durch den Einsatz digitaler Technologien überwunden werden. Innerhalb der Gerichtsbarkeiten mehrerer Staaten wird die Antikorruptionsarbeit der Strafjustizbehörden in Form eines Systems internationaler Rechtsnormen zum Cyberraum, zu neuronalen Netzwerken und anderen Aspekten digitaler Datenformate formalisiert.

Der gesetzliche Begriff des „Cyberraums“ sollte es ermöglichen, die Grenzen der staatlichen Zuständigkeit im kybernetischen Umfeld zu bestimmen.

Große Sprachmodelle und andere Methoden des Deep Learning sowie Algorithmen und Modelle anderer KI-Teilbereiche ermöglichen die Identifikation von Mustern, nichtlinearen Zusammenhängen und die Vorhersage der weiteren Entwicklung krimineller Aktivitäten, an denen Unternehmer beteiligt sind. Eine Datenquelle für diese Systeme sollten auch die Einkommensdeklarationen von Unternehmern und ihren Familienmitgliedern sein.

Moderne digitale Werkzeuge und rechtliche Verfahrensrahmen sind Komponenten eines zeitgemäßen Rechtsmechanismus zur vollständigen Neutralisierung von Straftaten im Bereich der öffentlichen Beschaffung, was den fiskalischen Bemühungen der Bürger des Landes Sinn verleiht (die Übersetzung wurde von Dr. O. Schilin korrigiert).

RESUMO

A obrigatoriedade da norma legislativa significa a sua conformidade com os componentes axiológicos da criação e qualidade de vida humana ao mais alto nível das civilizações às quais ela se atribui.

O legislador que não utiliza o potencial jurídico do discurso das normas anticorrupção deixa a sociedade fora do contexto da realidade jurídica e do direito natural, transformando a legislação num método

artificial de combate manual à corrupção. Nessas condições, a criação de uma infraestrutura anticorrupção perde a sua lógica histórica.

Uma política de pessoal corrupta prolongada e em larga escala leva à disfunção organizacional das relações jurídicas, eliminando inicialmente cidadãos íntegros e, posteriormente, privando comunidades territoriais e nações dase suas possibilidades existenciais.

Os fenómenos da evasão dos empregadores ao registo formal-legal dos trabalhadores nos cargos e/ou da ocultação do valor real dos salários criam um risco persistente e de difícil controlo para a perda das capacidades económicas e sociais da nação.

Nos países com altos níveis de corrupção interna, os algoritmos e práticas jurídicas enfatizam a eficácia da política fiscal, mas não a eficiência das compras governamentais.

As deficiências corruptas nos órgãos nacionais de justiça criminal e/ou noutro níveis institucionais são superadas por cada nação apenas com apoio externo anticorrupção suficiente, bem como por meio de tecnologias digitais. No âmbito das jurisdições de vários países, a atividade anticorrupção dos órgãos de justiça criminal formaliza-se através de um sistema de normas jurídicas internacionais sobre o ciberespaço, redes neurais e outros aspectos do formato digital dos dados.

O conceito legislativo de “ciberespaço” deve permitir a definição dos limites da jurisdição do Estado no ambiente cibernético.

Os grandes modelos de linguagem e outros métodos de aprendizagem profunda de máquinas, bem como algoritmos e modelos de outros subconjuntos da IA, permitem identificar sinais, relações não lineares e prever a lógica futura do desenvolvimento da criminalidade, incluindo a participação de empresários. As declarações de renda dos empresários e dos seus familiares também devem servir como fonte de dados para esses sistemas.

As ferramentas digitais modernas e as estruturas processuais jurídicas são componentes do mecanismo jurídico contemporâneo para a neutralização efetiva dos crimes na área das compras governamentais, dando significado aos esforços fiscais dos cidadãos do país (tradução corrigida pelo Prof. C. Gomes).

حاشیه نویسی

الماهیت اجباری یک قاعده قانونی نشان‌دهنده تطابق آن با مؤلفه‌های ارزشی آفرینش و کیفیت زندگی انسانی در سطح بالاترین تمدن‌هایی است که به آن‌ها تعلق دارد.

قانون‌گذاری که از ظرفیت حقوقی گفتمان مقررات ضد فساد استفاده نکند، جامعه را از بستر واقعیت حقوقی و حقوق طبیعی خارج کرده و قانون‌گذاری را به ابزاری مصنوعی برای کنترل دستی فساد تبدیل می‌کند. در چنین شرایطی، ایجاد زیرساخت‌های ضد فساد منطق تاریخی خود را از دست می‌دهد.

سیاست‌های فسادآمیز طولانی‌مدت و گسترده در زمینه نیروی انسانی منجر به اختلال سازمانی در روابط حقوقی شده و در ابتدا شهروندان درستکار را از میان برمی‌دارد و سپس جوامع محلی و ملت‌ها را از فرصت‌های هستی‌شناختی محروم می‌کند.

پدیده‌هایی مانند اجتناب کارفرمایان از استخدام رسمی کارکنان و/یا اعلام کمتر از میزان واقعی حقوق، خطرات پایدار و سخت‌کنترل‌پذیری را برای کاهش توانمندی‌های اقتصادی و اجتماعی یک ملت ایجاد می‌کند.

در کشورهایی با سطح بالای فساد داخلی، الگوریتم‌ها و رویه‌های حقوقی بر کارایی سیاست‌های مالیاتی تأکید دارند، اما بر اثربخشی تأمینات عمومی تمرکز ندارند.

نواقص مربوط به فساد در نهادهای عدالت کیفری ملی و/یا در سایر سطوح نهادی، تنها در صورتی توسط هر کشور قابل جبران است که حمایت خارجی کافی از اقدامات ضد فساد وجود داشته باشد، و همچنین از فناوری‌های دیجیتال استفاده شود. در حوزه‌های قضایی چندین کشور، فعالیت‌های ضد فساد نهادهای عدالت کیفری در قالب یک سیستم هنجارهای حقوقی بین‌المللی در مورد فضای مجازی، شبکه‌های عصبی و سایر جنبه‌های قالب‌های داده دیجیتال رسمی می‌شود.

مفهوم قانونی «فضای مجازی» باید امکان تعیین حدود صلاحیت قضایی یک کشور را در محیط سایبری فراهم کند.

مدل‌های زبانی بزرگ و سایر روش‌های یادگیری عمیق ماشینی، همراه با الگوریتم‌ها و مدل‌های سایر زیرمجموعه‌های هوش مصنوعی، امکان شناسایی نشانه‌ها، ارتباطات غیرخطی و پیش‌بینی روند توسعه آینده جرایم مرتبط با کارآفرینان را فراهم می‌آورد. یکی از منابع اصلی داده برای این سیستم‌ها باید اظهارنامه‌های درآمدی کارآفرینان و اعضای خانواده آن‌ها باشد.

ابزارهای دیجیتال مدرن و چارچوب‌های رویه‌ای حقوقی، از اجزای یک سازوکار حقوقی معاصر برای خنثی‌سازی کامل جرایم در حوزه تأمینات عمومی هستند که به تلاش‌های مالیاتی شهروندان کشور معنا می‌بخشند.

REFERENCES

1. Administratyvno-pravovi zasady realizatsiyi kadrovoyi polityky v systemi pravosuddya Ukrayiny [Administrative-legal principles of implementing personnel policy in the justice system of Ukraine]: manual / A. V. Borovyk, A. V. Popyk, O. Yu. Drozd and others. Odesa: Publishing house "Helvetica". 2021. 248 p.

2. After the Financial Crisis: Shifting Legal, Economic and Political Paradigms. Edit by Iglesias-Rodriguez P., Triandafyllidou A., Gropas R. London: Palgrave Macmillan, 2016. 365 p.

3. Alcántara, M. Ciencia política y digitalización. *Revista Ecuatoriana de Ciencia Política*. 2022. Vol. 1. No. 1. P. 6–21. DOI: 10.59352/recp.v1i1.22

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

5. Allen, R., Bengtsson, T., Dribe, M. Living Standards in the Past. New Perspectives on Well-Being in Asia and Europe. Oxford: University Press, 2005. 495 p.

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

7. Anti-Money Laundering: How IoT Can Help. AML. December 2, 2024. URL: https://www.iotforall.com/anti-money-laundering-iot

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

9. Azleen, I., Nasrudin, B., Erlane, K. G. Employees' Perceived Risk Management in Public Procurement and Finance: Evidence in Malaysia. *Management and accounting review*. 2023. Vol. 22. No. 3. P. 173–199. doi.org/10.24191/MAR.V22i03-07

10. Baltrunaite, A. Political contributions and public procurement: evidence from Lithuania. *Journal of the European Economic Association.* 2020. Vol. 18. Iss. 2. P. 541–582. DOI: 10.1093/jeea/jvz016

11. Balynska, O. M., Tokarska, A. S., Yashchenko, V. A. (2017). Aktual'ni problemy filosofiyi prava: posibnyk [Actual problems of the philosophy of law: manual]. Lviv: LvDUVS. 612 p.

12. Bauhr, M., Czibik, A., Fine Licht, J., Fazekas, M. Lights on the shadows of public procurement: Transparency as an antidote to corruption. 2020. Governance. Vol. 33. Iss. 3. P. 495–523. DOI: 10.1111/gove.12432

13. Belmont, D. Managing Counterparty Risk in an Unstable Financial System. Commonfund Institute. 2012. 20 p. URL: https://files.eric.ed.gov/fulltext/ED559302.pdf

14. Benjamin, J. GroupM: Global ad market to hit $1tn a year early. 11 Jun 2024. URL: https://uk.themedialeader.com/groupm-china-comeback-to-boost-global-ad-market/

15. Berraida, R., El Abbadi, L. The Artificial Intelligence and Public Procurement. *The 15th IEEE International conference of Logistics and Supply Chain Management "Logistiqua"*. 2024 May 2–4. University of Sousse. Tunisia. 6 p. DOI: 10.1109/logistiqua61063.2024.10571429

16. Biletzki, A. Talking Wolves: Thomas Hobbes on the Language of Politics and the Politics of Language. Dordrecht: Kluwer Academic Publishers, 1997. 225 p.

17. Brogi, M., Lagasio, V. New but naughty. The evolution of misconduct in FinTech. *International Review of Financial Analysis*. 2024. Vol. 95. P. B. P. 1–11. doi.org/10.1016/j.irfa.2024.103489

18. Buryachok, V. L., Kyrychok, R. V., Skladanniy, P. M. (2018). Osnovy informatsiynoyi ta kibernetychnoyi bezpeky: navchal'nyy posibnyk [Basics of information and cybernetic security]. K.: Kyiv. University B. Hrinchenko. 320 p.

19. Case of Oleksandr Volkov v. Ukraine (application no. 21722/11): ECHR Judgment 09.01.2013. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115871%22]}

20. Case of Veniamin Tymoshenko and others v. Ukraine (application no. 48408/12): ECHR Judgment 02.10.2014. URL: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-146671%22]}

21. Case of Zelenchuk and Tsytsyura v. Ukraine (applications no. 846/16 and 1075/16): ECHR Judgment 22.05.2018. URL: https://laweuro.com/?p=7666

22. Chagnon, P. (2024) Qatargate: The Result of Over Twenty Years of Interference, Ideological, Financial, and Electoral Compliance. A Step in the Strategy of Establishing Rigorous Islam in Europe and the West. Brussels: European Parliament. 204 p.

23. Chang, L., Xu, M., Guo, L., Zhu, X., Qin, S., Guo, X., Yang, X. A Quantum Annealing Algorithm for the Resource-Constrained Excavator Procurement Problem. 21st Inter. Conf. on Networking, Sensing and Control. October 18–20, 2024. Hangzhou. China. 6 p. DOI: 10.1109/ICNSC62968.2024.10759968

24. Chayka, I. M. Kryminolohichna kharakterystyka ta zapobihannya shakhraystvu v Ukrayini [Criminological characteristics and prevention of fraud in Ukraine]. Dissertation of Doctor of Philosophy. Specialization 081 – law. Donetsk State University of Internal Affairs. Kropyvnytskyi. 2023. 296 p.

25. Chêne, M. Corruption and anti-corruption practices in human resource management in the public sector. Transparency International, 2015. URL: https://www.u4.no/publications/corruption-and-anti-corruption-practices-in-human-resource-management-in-the-public-sector

26. Cini, M. Organizational responses to scandals: how effective is the European Commission? *Comparative European Politics*. 2024. Vol. 22. P. 557–573. doi.org/10.1057/s41295-023-00373-1

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

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

29. Cooke, A. Pensions and Legal Policy. Lessons on the Shift from Public to Private. Oxford: Hart Publishing, 2021. 245 p.

30. Criminal Procedure Code of Ukraine dated 04/13/2012. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n2390

31. Crouzel, C. Plus de 75.000 comptes à l'étranger déclarés au fisc. Le figaro. Le 8 juillet 2011. URL: https://www.lefigaro.fr/impots/2011/07/08/05003-20110708ARTFIG00628-fraude-fiscale-la-liste-hsbc-a-fait-peur.php

32. Daydzhest sudovoyi praktyky Verkhovnoho Sudu shchodo vyrishennya sporiv u sferi publichnykh zakupivel' [Digest of the Supreme Court's case law on resolving disputes in the field of public procurement]. Court Decisions of the Unified State Register 2019 – April 2024. Kyiv: Supreme Court. 2024. 130 p.

33. DarkMarket: world's largest illegal dark web marketplace taken down. Europol's European Cybercrime Centre. 12.01.2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

34. Dela, P. Cyberspace as the Environment Affected by Organized Crime Activity Connections. 2016. Vol. 15. No. 3. P. 55–64. DOI: 10.11610/Connections.15.3.05

35. Delnero, D. L. Open Letter to Ukrainian National Police. 29.11.2024. BGD Legal & Consulting LLC. URL: https://bgdlc.com/wp-content/uploads/2024/11/Open-Letter-v2.pdf

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

37. 2030 Digital Compass: the European way for the Digital Decade. Communication from the Commission to the EU parliament, the Council, the EUES Committee and the Committee of the regions. 09.03.2021. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

38. Disdier, A.-C., Fontagné, L., Tresa, E. Economic drivers of public procurement-related protection. *World Economy.* 2021. Vol. 44. Iss. 11. P. 3072–3090. DOI: 10.1111/twec.13193

39. Dom, R., Custers, A., Davenport, S., Prichard, W. Innovations in Tax Compliance: Building Trust, Navigating Politics, and Tailoring Reform. Washington: World Bank. 2022. 306 p.

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

41. EBA updates list of other systemically important institutions. 11.07.2024. URL: https://www.eba.europa.eu/publications-and-media/press-releases/eba-updates-list-other-systemically-important-institutions-3

42. Fazekas, M., Sberna, S., Vannucci, A. The extra-legal governance of corruption: Tracing the organization of corruption in public procurement. Governance. 2022. Vol. 35. Iss. 4. P. 1139–1161. DOI: 10.1111/gove.12648

43. Fil'o, M. M. Fiskal'ni instytuty minimizatsiyi podatkovykh vtrat [Fiscal institutions of minimizing tax losses]. Dissertation of candidate of economic sciences in specialty 08.00.08 "Money, finance and credit". Ternopil National University. Ternopil. 2017. 287 p.

44. Fragomeni, M. A., Contado, J. S., Mitidiero, M. C., Satyro, W. C. Composto dos vínculos entre empresas que atuam em rede de negócio. *Internext*. 2024. Vol. 19. No. 2. P. 96–115. doi.org/10.18568/internext.v19i2.775

45. Gavoille, N., Zasova, A. What We Pay in the Shadow: Labor Tax Evasion, Minimum Wage Hike and Employment. *Journal of Public Economics*. 2023. Vol. 228. P. 1–24. doi.org/10.1016/j.jpubeco.2023.105027

46. Goethes (1993). Werke. Hamburger Ausgabe in 14 Bänden. Band 3. Dramatische Dichtungen. Herausgebers Erich Trunz. Hamburg: C. H. Beck. 778 S.

47. 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.

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

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

50. Garcetti v. Ceballos, 547 U. S. 410 (2006). Supreme Court of USA. URL: https://supreme.justia.com/cases/federal/us/547/410/

51. Grandi, S., Sellar, C., Jafri, J. Geofinance between Political and Financial Geographies. A Focus on the Semi-Periphery of the Global Financial System. Cheltenham: E. Elgar Publishing LLC. 2019. 264 p.

52. Grandia, J., Volker, L. (2023). Public Procurement: Theory, Practices and Tools. London: Palgrave Macmillan. 166 p.

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

54. Guo, G., Ray, A., Izydorczak, M., Goldfeder, J., Lipson, H., Xu, W. Unveiling intra-person fingerprint similarity via deep contrastive learning. *Science Advances*. 2024. Vol. 10. Iss. 2. P. 1–11. DOI: 10.1126/sciadv.adi0329

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

56. Hessen, Y. The Meaning of Life. Trans. from German by M. Mauritson. Kyiv: Pul'sary. 2009. 134 p.

57. Hobbs T. Leviathan. Trans. from English. Kyiv: Spirit and Letter, 2000. 606 p.

58. Hoepers, C., Zuben, M., Gomez, H. Internetis võib olla väga lõbus, aga ära mängi oma turvalisusega. Tallinn: Profimeedia OÜ. 2024. 60 p.

59. Horyachenko, R. I. Formuvannya ta realizatsiya kadrovoyi polityky v orhanakh natsional'noyi politsiyi: administratyvno-pravovyy aspekt [Formation and implementation of personnel policy in the bodies of the national police: administrative-legal aspect]: dissertation ... doctor of philosophy: speciality 081 "Law". Kyiv. 2022. 234 p.

60. Hörz, M. Looking back at the tobacco lobbying battle: Philip Morris' allies in the European Parliament. 16.05.2014. URL: https://corporateeurope.org/en/power-lobbies/2014/05/looking-back-tobacco-lobbying-battle-philip-morris-allies-european-parliament

61. Huban', R. V. Stanovlennya ta rozvytok administratyvno-terytorial'noho ustroyu Ukrayiny (istoryko-pravove doslidzhennya) [Formation and development of the administrative-territorial system of Ukraine in the 20th – early 21st centuries (historical and legal research)]. Dissertation of Doctor of Law. Special. 12.00.01. Kyiv. 2018. 601 p.

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

63. Inflyatsiynyy zvit NBU: skhvaleno rishennyam Pravlinnya NBU [National Bank of Ukraine inflation report: approved by decision of the NBU Board] 31.10.2024 №-392рш. 56 p. URL: https://bank.gov.ua/admin_uploads/article/IR_2024-Q4.pdf?v=9

64. Informatsiya shchodo nadkhodzhen' podatkiv i zboriv, platezhiv kontrol' za spravlyannyam yakykh pokladeno na orhany DPS [Information on tax and fee receipts, payments, the collection of which is controlled by the State Tax Service bodies], as of August and September 2024. URL: https://tax.gov.ua/diyalnist-/pokazniki-roboti/nadhodjennya-podatkiv-i-zboriv--obovyaz/nadhodjennya-podatkiv-i-zboriv/

65. Inghilleri, P. From Subjective Experience to Cultural Change. Translated by E. Bartoli. Cambridge: Cambridge University Press, 1999. 175 p.

66. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris: FATF. 2012–2023. 148 p.

67. Irvine, J. M. Marginal People in Deviant Places: Ethnography, Difference, and the Challenge to Scientific Racism. Ann Arbor: University of Michigan Press, 2022. 349 p.

68. Jance, K. The approximation of the Albanian procurement legislation with the EU legislation. Curentul Juridic. 2024. Vol. 96(2). P. 92–99. DOI: 10.62838/CJJC.97.2.14

69. Johar, S. S., Johar, G. S. 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*. 2017. Vol. 11. № 1. DOI: 10.5958/0973-9130.2017.00010.X

70. Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace. Press Release. April 5, 2022. URL: https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

71. Karkovs'ka, V. Ya. Formuvannya mekhanizmiv kadrovoyi bezpeky orhaniv publichnoyi vlady v umovakh instytutsiynoho rozvytku [Formation of personnel security mechanisms of public authorities in the context of institutional development]: dissertation … Doctor of Science in State Administration: special 25.00.02. Mykolayiv. 2020. 426 p.

72. Kas'yan, O. V. Profspilky v Ukrayini ta za kordonom: istorychnyy dosvid, suchasnyy stan i perspektyvy [Trade unions in Ukraine and abroad: historical experience, current state and prospects]. Collection of materials of the All-Ukrainian scientific-practical conference. 26.04.2018. Kyiv: Fourth wave. 2018. 96 p.

73. Konovalova, I. O. Zapobihannya shakhraystvu u sferi elektronnoyi torhivli [Prevention of fraud in the field of electronic commerce]. Dissertation Doctor of Philosophy in Specialization 081 "Law". National Law University named after Ya. Mudry. Kharkiv. 2023. 220 p.

74. Kontseptsiya stvorennya ta vprovadzhennya prohramno-aparatnoho kompleksu "Bezpechna krayina" [Concept of creation and implementation of the software and hardware complex "Safe Country"]. Kyiv: Informatization Department of the Ministry of Internal Affairs of Ukraine. 2021. 7 p.

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

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

77. Krugman, P. R. The return of depression economics and the crisis of 2008. New York: W. W. Norton & Company, Inc. 2009. 224 p.

78. Kwantes, C., Kuo, B. C. H. Trust And Trustworthiness Across Cultures: Implications For Societies And Workplaces. Cham: Springer, 2021. 176 p.

79. Lad, F. Operational subjective statistical methods: a mathematical, philosophical, and historical introduction. New York: Wiley, 1996. 256 p.

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

81. Lenderink, B., Halman, J. I. M., Voordijk, H. Innovation and public procurement: from fragmentation to synthesis on concepts,

rationales and approaches. Innovation: The European Journal of Social Science Research. 2022. Vol. 35. No. 4. P. 650–674. doi.org/10.1080/13511610.2019.1700101

82. 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.

83. Loijas, K., Jääskeläinen, A., Karttunen, E. Dyadic capabilities in implementing performance-based public procurement. *Journal of Business & Industrial Marketing*. 2024. Vol. 39. № 13. P. 128–144. DOI: 10.1108/JBIM-09-2023-0542

84. Makarenkov, O. Model of anti-corruption institutions of international and national law correlations. *Baltic Journal of Economic Studies*. 2024. Vol. 10. No. 3. P. 215–226. doi.org/10.30525/2256-0742/2024-10-3-215-226

85. Makarenkov, O. L. (2024). Verification of the anti-corruption policy legal dysfunction at the level of a real threat to the national security. Riga: Baltija Publishing. 164 p. ISBN 978-9934-26-470-2. doi.org/10.30525/978-9934-26-470-2

86. Makarenkov, O. L. Pravova vyznachenist' dobrykh chesnot v obrazi ukrayintsiv yak umova yikhn'oyi intehratsiyi do Yevropeys'koho Soyuzu [Legal determination of good virtues in the image of Ukrainians as a condition for their integration into the EU]. *Pravo i suspil'stvo*. 2023. № 3. P. 40–48. doi.org/10.32842/2078-3736/2023.3.6

87. Manta, O., Mansi, E. The Impact of Globalization on Innovative Public Procurement: Challenges and Opportunities. Administrative Sciences. MDPI. 2024. Vol. 14(4). P. 1–14. doi.org/10.3390/admsci14040080

88. Marx, K., Engels, F. Manifest der Kommunistischen Partei (Februar 1848). Werke. Bd. 4. Berlin: Dietz Verlag. 1974. S. 459–493.

89. Marshall, J. V. The Lebanese Connection: Corruption, Civil War, and the International drug traffic. Stanford: University Press, 2012. 274 p.

90. Matthews, D. L., Stanley, L. L. (2022). Managing Logistics and Transportation in the Public Sector. New York: Routledge. 166 p.

91. Matvyeyeva, Yu. I. Pryntsyp pravovoyi vyznachenosti yak skladova verkhovenstva prava [The principle of legal certainty as a component of the rule of law]. Dissertation Candidate of Law. Special 12.00.01. Kyiv. 2019. 220 p.

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

93. Moodie, C., Hoek, J., Hammond, D., Gallopel-Morvan, K., Sendoya, D., Rosen, L., Mucan Özcan, B., Eijk, Y. Plain tobacco packaging: progress, challenges, learning and opportunities. *BMJ Journal*. 2022. Vol. 31. P. 263–271. DOI: 10.1136/tobaccocontrol-2021-056559

94. Mynenko, S. V. Transformatsiya systemy protydiyi lehalizatsiyi kryminal'nykh dokhodiv v umovakh didzhytalizatsiyi natsional'noyi ekonomiky [Transformation of the counteraction system to the legalization of criminal proceeds in the conditions of the national economy digitalization]. Dissertation of the candidate of economic sciences, speciality 051 – economics. Sumy State University. Sumy, 2022. 204 p.

95. NBU rozpochav borot'bu iz zarplatamy "u konvertakh": yak zminyat'sya "siri" vyplaty [The National Bank of Ukraine has begun the fight against salaries "in envelopes": how will "gray" payments change?]. 04.07.2023. URL: https://minfin.com.ua/ua/2023/07/04/108375710/

96. Neformal'no zaynyate naselennya za stattyu, typom mistsevosti ta statusom zaynyatosti u 2021 [Informally employed population by gender, type of locality and employment status in 2021]. *State Statistics Service of Ukraine*. URL: https://www.ukrstat.gov.ua/; https://stat.gov.ua/uk/datasets/obstezhennya-robochoyi-syly-0

97. Nemec, P. Contesting the public works domain: examining the factors affecting presence and success of SMES in public procurement. *Empirical Economics*. 2024. Vol. 67. P. 2135–2173. doi.org/10.1007/s00181-024-02615-x

98. Okinawa Charter on Global Information Society adopted by the Okinawa G-8 Summit at Kyushu-Okinawa: Building a global development partnership July 22, 2000. URL: https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf

99. Oleksyuk, L. (2020). Krashchi praktyky upravlinnya kiberbezpekoyu: ohlyadovyy zvit [Cyber security management best practices: review report]. Kyiv: Parliamentary Committee on Digital Transformation. 130 p.

100. On a general regime of conditionality for the protection of the Union budget: regulation (EU) 2020/2092 of the European Parliament and of the Council of 16 december 2020. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32020R2092

101. On combating money laundering by criminal law: regulation 2018/1673 of the European Parliament and of the Council of 23 October 2018. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018L1673&qid=1655905509021&rid=1

102. On Income and on Capital: Model Tax Convention, adopted by the Council of the Organisation for Economic Co-operation and Development on 01.09.1992 (latest update 21.11.2017). URL: https://www.oecd.org/en/publications/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en.html

103. On information accompanying transfers of funds and certain crypto-assets: regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113&qid=1690202577447

104. On market surveillance and compliance of products: regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 june 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1020

105. On markets in crypto-assets: regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 may 2023. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj

106. On Mutual Administrative Assistance in Tax Matters: Convention, adopted by the Council of the Organisation for Economic Co-operation and Development on 01.06.2011. URL: https://www.oecd.org/en/topics/convention-on-mutual-administrative-assistance-in-tax-matters.html

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

108. On public procurement and repealing Directive 2004/18/EC: directive 2014/24/EU of the European Parliament and of the Council of 26 february 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014L0024-20180101

109. Opportunities and Challenges of New Technologies for AML/CFT. Paris: FATF. 2021. 76 p.

110. On setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022–2025: Council conclusions. 09.03.2023. no. 7101/23. URL: https://data.consilium.europa.eu/doc/document/ST-7101-2023-INIT/en/pdf

111. "On the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC": Directive 2014/40/EU of the European Parliament and of the Council. 03 April 2014. URL: health.ec.europa.eu/document/download/c4aa6f75-7e52-463b-badb-cbb6181b87c3_en?filename=dir_201440_en.pdf

112. Pamfir: Ukrainian fictional feature film directed by Dmytro Sukholytkyy-Sobchuk. 2022. URL: https://www.youtube.com/watch?v=X44X5HDP2JQ

113. Patrucco, A. S., Kauppi, K., Mauro, C., Schotanus, F. Enhancing strategic public procurement: a public service logic perspective. *Public Management Review*. 2024. P. 1–21. DOI: 10.1080/14719037.2024.2411630

114. Pavlidis, G. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*. 2023. Vol. 26. No. 7. 2023. P. 155–166. doi10.1108/JMLC-03-2023-0050

115. Peng, W. Q., Wei, K. C.J., Yang, Z. (2011). Tunneling or propping: Evidence from connected transactions in China. Journal of Corporate Finance. Vol. 17. Iss. 2. P. 306–325.

116. Pidvyshchennya podatkiv "zadnim chyslom" zbil'shyt' zarplatnu tin' v Ukrayini na 10% [Retroactive tax hike will increase shadow wages in Ukraine by 10%]. Advanter Group. 12.10.2024. URL: https://www.epravda.com.ua/news/2024/10/12/720501/

117. Pieth, M., Atkinson, P., Goredema, C., Bacarese, A., Lasich, T., others. Tracing Stolen Assets: A Practitioner's Handbook. Basel: Basel Institute on Governance. 2009. 124 p.

118. Polishchuk, V. D. Detinizatsiya zaynyatosti yak chynnyk zabezpechennya sotsial'noyi bezpeky [Detinization of employment as a factor in ensuring social security]. Dissertation for the degree of Doctor of Philosophy. Specialization 051 "Economics". Lviv. 2023. 257 p.

119. Poole-Robb, S., Bailey, A. Risky Business: Corruption, Fraud, Terrorism and Other Threats to Global Business. London: Kogan Page, 2002. 316 p.

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

121. Rankin, J., Smith, H. A police stakeout, piles of cash, and a promise of reform: the week that shook Brussels. 16 Dec 2022. *The Guardian*. URL: https://www.theguardian.com/world/2022/dec/16/a-tragic-affair-european-parliament-stunned-by-qatar-corruption-inquiry

122. Regime do segredo de estado [state secret regime]: Lei Orgânica n.º 2/2014, de 06 de Agosto, adotada pela Assembleia da República Portuguesa. URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2201&tabela=leis&so_miolo=

123. Reusen, E., Stouthuysen, K. Misaligned control: The role of management control system imitation in supply chains. *Accounting, Organizations and Society*. 2017. Vol. 61. P. 22–35. doi.org/10.1016/j.aos.2017.08.001

124. Riccucci, N. M., Naff, K. C., Hamidullah, M. F. Personnel Management in Government. Eighth edition. New York: Routledge, 2020. 560 p.

125. Saisawat, S. Employment effects of minimum wages in a dual economy: Evidence from Thailand. *Journal of Development Economics*. 2024. Vol. 168. P. 1–16. DOI: 10.1016/j.jdeveco.2023.103213

126. Saks, K., Klopets, M., Hämmal, J., Kaljuste, K. E., Petermann, A. and others. Laste internetikasutus ning

võimalused internetis toimuva laste seksuaalse väärkohtlemise ennetamiseks. Uuringu aruanne. Tallinn: Kantar Emor 2024. 138 p.

127. Sanchez-Graells, A. (2024). Digital Technologies and Public Procurement: Gatekeeping and Experimentation in Digital Public Governance. Oxford: University Press. 320 p.

128. Sand, B. V. Toward a definition of creativity: construct validation of the cognitive components of creativity: diss. of degree achieved doctor in educ. psychology. Submitted to the Graduate Faculty of Texas Tech University. Lubbock. 2002. 145 p.

129. Sarkar, S. Need-Based Employment. Boston College Law Review. 2023. Vol. 64. Iss. 1. P. 119–178. doi.org/10.2139/ssrn.4198553

130. Schaper, T. M., Weber, P. Understanding small business scams. Journal of Enterprising Culture. 2012. Vol. 20. No. 3. P. 333–356. DOI: 10.1142/S0218495812500148

131. Schopenhauer, A. Zürcher Ausgabe. Werke in zehn Bänden. Band 1–2, Zürich 1977. Zweiter Band, welcher die Ergänzungen zu den vier Büchern des ersten Bandes enthält. 442 p.

132. SEC Charges Three So-Called Market Makers and Nine Individuals in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities. Washington D. C. Oct. 9, 2024. URL: https://www.sec.gov/newsroom/press-releases/2024-166

133. 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. URL: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

134. Shchodo otsinky real'nosti hospodars'kykh operatsiy: ohlyad sudovoyi praktyky KAS u skladi VS [Regarding the assessment of the reality of economic transactions: a review of the case law of the CAS in the composition of the Supreme Court]. September 2018 – June 2023. 34 p. URL: supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Ohliad_otsinka_realnosti_KAS.pdf

135. Sobre secretos oficiales [on official secrets]: Ley 9/1968, de 5 de abril, aprobada por las Cortes Españolas. URL: https://www.boe.es/buscar/act.php?id=BOE-A-1968-444

136. Standard for Automatic Exchange of Financial Account Information in Tax Matters. 2nd ed. Paris: OECD Publishing. 2017. 326 p. doi.org/10.1787/9789264267992-en

137. Statystyka orhaniv prokuratury Ukrayiny [Statistics of the prosecutor's office of Ukraine] 2011–2019, 2022–2023. 31.12.2024. URL: https://gp.gov.ua/ua/posts/statistika; https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

138. Sudeall, L. Delegalization. Stanford Law Review. 2023. Vol. 75. P. 116–131.

139. Suszan, B. Public crime data becomes more open and transparent city by city. May 21, 2014. URL: https://opensource.com/government/14/5/spotcrime

140. Tabish, S. Z. S., Neeraj Jha, K. The impact of anti-corruption strategies on corruption free performance in public construction projects Construction Management and Economics. 2012. Vol. 30. Iss. 1. P. 21–35. doi.org/10.1080/01446193.2011.654128

141. Takei, Y., Shudo, K. FATF Travel Rule's Technical Challenges and Solution Taxonomy. IEEE Inter. Conf. on Blockchain and Cryptocurrency. 27–31 May, 2024. P. 784–799. DOI: 10.1109/ICBC59979.2024.10634360

142. Tălpig, C. C. The efficiency of the public procurement system and its implications on public budgets. *Journal of Public Administration, Finance and Law*. 2024. Iss. 31. P. 450–462. doi.org/10.47743/jopafl-2024-31-32

143. Tanklevs'ka, N. S., Povod, T. M. Povedinkova ekonomika: etymolohiya, sutnist', teoriya [Behavioral economics: etymology, essence, theory]. Scientific Bulletin of the Flight Academy. Series: Economics, Management and Law. 2021. Issue 3; 4. P. 34–45.

144. Tátrai, T., Vörösmarty, G., Juhász, P. Intensifying Competition in Public Procurement. *Public Organization Review*. 2024. Vol. 24. Iss. 1. P. 237–257. doi.org/10.1007/s11115-023-00742-0

145. Telles, P. Existing and Potential Use Cases for Blockchain in Public Procurement. European Procurement & Public Private Partnership Law Review. 2022. Vol. 17. Iss. 3. P. 179–189.

146. The Bletchley Declaration by Countries Attending the AI Safety Summit. 01.11.2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

147. The Future of Growth Report. January 2024. Geneva: The World Economic Forum. 291 p.

148. The Interim Measures for the Management of Generative Artificial Intelligence Services: promulgated on July 10, 2023 by the Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, National Radio and Television Administration. URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

149. Torgler, B. Tax Compliance and Tax Morale: A Theoretical and Empirical Analysis. Cheltenham: EE Publishing Ltd., 2007. 317 p.

150. Torre, C. Liderazgo populista. Revista Ecuatoriana de Ciencia Política. 2022. Vol. 1. No. 1. P. 64–80. DOI: 10.1163/9789004679016_010

151. Tsesars'kyy, F. A. Zakhysna funktsiya profspilok, formy yiyi realizatsiyi [The protective function of trade unions, forms of its implementation]. dissertation for the degree of candidate of jurisprudence: 12.00.05. Kharkiv. 2004. 200 p.

152. Ukraine 2024 Report. Communication on EU enlargement policy: Commission staff working document. 30.10.2024. SWD (2024) 699 final. 105 p. URL: https://neighbourhood-enlargement.ec.europa.eu/2024-communication-eu-enlargement-policy_en

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

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

155. Vallanti, G., Gianfreda, G. Informality, regulation and productivity: do small firms escape EPL through shadow

employment? Small Business Economics. 2021. Vol. 57(3). P. 1383–1412. DOI: 10.1007/s11187-020-00353-9

156. Veebipolitsei tuleb appi. 12.02.2020. URL: https://www.teeviit.ee/veebikonstaabel-tuleb-appi/

157. Vella, M. Transparency watchdog says EU remains vulnerable to corruption OLAF, Council, and Commission taken to task over Dalligate investigation. 24 April 2014. MaltaToday. URL: www.maltatoday.com.mt/news/dalligate/38331/transparency_watchdog_says_eu_remains_vulnerable_to_corruption

158. Vladimirova, N. P. Reformuvannya derzhavnoho finansovoho kontrolyu v konteksti zabezpechennya finansovoyi bezpeky sub'yektiv hospodaryuvannya [Reforming state financial control in the context of ensuring the financial security of economic entities]. Dissertation of the candidate of economic sciences in the specialty 08.00.08 "Money, finance and credit". S. Kuznets KhNEU. Kharkiv. 2017. 324 p.

159. Voytovych, I. I. Kryminolohichni zasady protydiyi koruptsiyi u sferi voyennoyi bezpeky [Criminological principles of combating corruption in the sphere of military security]. Dissertation Doctor of Law in speciality 12.00.08. Dnipropetrovsk State University of Internal Affairs Kyiv. 2021. 394 p.

160. Vysnovok na proekt Zakonu Ukrayiny "Pro vnesennya zmin do Podatkovoho kodeksu Ukrayiny shchodo osoblyvostey opodatkuvannya u period diyi voyennoho stanu" [Conclusion on the draft of the Law of Ukraine "On Amendments to the Tax Code of Ukraine regarding the peculiarities of taxation during the period of martial law"]. № 16/03-2024/2014-06 16.09.2024. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/44809

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

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

163. Wingate, G., Gra, L. A., Greenberg, T. S., Samuel, L. M. (2009). Stolen asset recovery: a good practices guide for non-conviction based asset forfeiture. Stolen Asset Recovery (StAR). Washington, D. C.: World Bank Group. 284 p.

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

165. Yedyni zvity pro kryminal'ni pravoporushennya prokuratury Ukrayiny [Unified reports on criminal offenses of the Prosecutor's Office of Ukraine] 2013–2024. 31.12.2024. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

166. Yevdokymov, P. V. Administratyvno-pravove rehulyuvannya realizatsiyi kadrovoho zabezpechennya v orhanakh publichnoyi administratsiyi v Ukrayini [Administrative-legal regulation of the implementation of personnel management in public administration bodies in Ukraine]: dissertation … candidate of legal sciences: special 12.00.07. Zaporizhzhia. 2020. 237 p.

167. Ying, Ji The Rule of Law in China and Comparative Perspectives: The Making of Chinese Criminal Law, The Preventive Shift in the Context of the Eighth Amendment. New York: Routledge, 2021. 183 p.

168. Yoo, D., Sul Kim, D. The Invisible Impact of Conflict: A Study of Terrorism, Regime Type, and the Shadow Economy. International Interactions. 2024. Vol. 50. № 5. P. 750–779. DOI: 10.1080/03050629.2024.2374364

169. Yu, Y., Wu, J., Lin, D., Fu, Q. Money Laundering Detection on Ethereum: Applying Traditional Approaches to New Scene. IEEE 29th Inter. Conf. on Parallel and Distributed Systems. Ocean Flower Island, China. 2023. P. 1759–1766. doi.org/10.1109/ICPADS60453.2023.00244

170. Zand, A., Orwelly, J., Pfluegel, E. A Secure Framework for Anti-Money-Laundering using Machine Learning and Secret Sharing. Inter. Conf. on Cyber Security and Protection of Digital

Services. 15–19 June, 2020. Dublin. C. 1–7. doi.org/10.1109/CyberSecurity49315.2020.9138889

171. Zdiysnennya monitorynhu sposobu zhyttya sub'yektiv deklaruvannya [Monitoring the lifestyle of declaring subjects]: Procedure, approved by Order of the National Agency for the Prevention of Corruption dated 10/26/2023, No. 236/23. URL: https://zakon.rada.gov.ua/laws/show/z1873-23#Text

172. Zhovnirchyk, Ya. F. Suchasna kadrova polityka v orhanakh derzhavnoyi vlady ta orhanakh mistsevoho samovryaduvannya. [Modern personnel policy in state authorities and local self-government bodies]. Investytsiyi: praktyka ta dosvid [Investments: practice and experience]. 2017. № 12. P. 102–107.

ANNEXES
Illustrations of corruption aimed at undermining governance compliance with EU legal standards

1. Dalligate in the EU

1.1. Photo. **John Dalli** is a Maltese former politician who served as Cabinet Minister in various Maltese governments between 1987 and 2010. As European Commissioner for Health and Consumer Policy between 2010 and 2012, he remained steadfast in his commitment to the adoption of a tough tobacco directive (Directive 2014/40/EU), which led to a 60–67% reduction in the number of smokers in the EU (WHO data). However, for this legal position, the foreign tobacco lobby corruptly and through slander deprived J. Dalli of his position in the European Commission (Vella, M., MaltaToday 2014).

1.2. Photo. Type of cigarette packaging **after** the adoption of the Directive 2014/40/EU (Photo by Makarenkov O. L.). The packaging contains only realistic images of the destructive consequences of smoking for humans.

1.3. Photo. Type of packaging **before** the adoption of the Directive 2014/40/EU. A visual composition with marketing content. It attracts attention and creates the illusion of style, image, and cigarette safety (Photo by Makarenkov A. from his joint collection with the author of this scientific work 2025).

2. Qatargate in the EU

Eva Kaili and three other suspects charged with 'criminal organization, corruption and money laundering' (Rankin, Smith, The Guardian 2022).

2.1. Photo. Several **hundred thousand euros** were found in E. Kaili's father's hotel room (Police Judiciaire Federale/AFP/Getty Images).

2.2. Photo. **Eva Kaili** (She was a Greek MEP and one of the parliament's 14 vice-presidents) and **Francesco Giorgi** (He is Italian. He was an assistant at the MEP). They lived together (Eurokinissi/AFP/Getty Images).

2.3. Photo. **E. Kaili** meets Qatar's labour minister, **Ali bin Samikh al-Marri**, in Doha on 31 October 2022 (Qatar's Ministery of Labour/ AFP/Getty Images)

Studium

Akademischer Titel eines Professors, 2023; Doktor der Rechtswissenschaften, 2021, Nationale Universität Saporishshja (weiter NUS); Akademischer Titel des Dozenten, 2014; Kandidat der Rechtswissenschaften, 2011, die Nationale Akademie für Innere Angelegenheiten, Kiew.

Masterabschluss, Qualifikation eines Philologen und Übersetzers für die deutsche Sprache (2022–2024, NUS); Spezialistendiplom, Qualifikation eines Lehrers für Englische Sprache und Literatur (2017, NUS); Spezialistendiplom, Qualifikation eines Philologen und Übersetzers für die englische Sprache (2015, NUS).

Doktorandenprogramm (2005–2008, NUS; 2010–2011, die Nationale Akademie für Innere Angelegenheiten, Kiew); Spezialistendiplom mit höchstem Lob (summa cum laude), Qualifikation eines Anwalts (2005, NUS); Bakkalaureus der Rechte mit höchstem Lob / LL. B. / Baccalaureus legum summa cum laude (2004, NUS).

Sprachkenntnisse: Englisch – fließend; Ukrainisch, Russisch – Muttersprachen. Deutsch, Portugiesisch, Spanisch, Latein, Türkisch, Polnische, Italienisch, Französisch und orientalische Sprachen – Grundkenntnisse (A1–A2).

Stellvertretender Dekan der Juristische Fakultät, verantwortlich für Internationale Beziehungen in NUS, 2017–2024, pro bono.

Wissenschaftliche Publikationen zu folgenden Themen: 1) Digitale Technologien und Völkerrecht im Mechanismus der nationalen Sicherheit; 2) Virtuelle Vermögenswerte und Kommunikation im Cyberspace; 3) Bekämpfung von Geldwäsche und Terrorismusfinanzierung; 4) Antikorruptionspolitik; 5) Compliance-Management mit rechtlichen Standards; 6) Verbraucherrecht; 7) Internationales Handelsschiedsrecht; 8) Nachkriegswiederaufbau der Ukraine und ihre Integration in die EU; 9) Internationales Strafrecht; 10) Juristische Deontologie; 11) Justiz und Strafverfolgungsbehörden; 12) Theorie und Methodologie der Rechtswissenschaft; 13) Geschichte politischer und rechtlicher Lehren; 14) Verfassungsrecht.

Träger des Parlamentspreises der Werchowna Rada der Ukraine für junge Wissenschaftler im Jahr 2023 für bedeutende wissenschaftliche Leistungen, die konkrete Aufgaben des Staates lösen, den Interessen und Erwartungen der Bürger, der Gebietsgemeinden und der ukrainischen Gesellschaft entsprechen sowie zur weiteren Entwicklung der Wissenschaft, zum gesellschaftlichen Fortschritt beitragen und die hohe Autorität von Wissenschaftlern in der Ukraine und weltweit stärken.

Izdevniecība “Baltija Publishing”
Valdeķu iela 62 – 156, Rīga, LV-1058
E-mail: office@baltijapublishing.lv

Iespiests tipogrāfijā SIA “Izdevniecība “Baltija Publishing”
Parakstīts iespiešanai: 2025. gada 03. marts
Tirāža 300 eks.