TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 2
JUNE 2025

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.2.
E-ISSN: 2181-1024

Founder: Tashkent State University of Law

TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 2
JUNE 2025

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.2.

«TSUL Legal Report» international electronic scientific journal was registered by the Press and Information Agency of Uzbekistan on April 21, 2020, with certificate number 1342.The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

Publication Officer:
Orifjon Choriev

Editor:
Elyor Mustafaev

Graphic designer:
Umid Sapaev

Editorial office address:
Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact

Tel.: (+998 71) 233-66-36

Fax: (+99871) 233-37-48

Website: legalreport.tsul.uz

E-mail: info@legalreport.tsul.uz

Publishing license
№ 174625, 29.11.2023.

E-ISSN: 2181-1024

CONTENTS

12.00.03 – CIVIL LAW. BUSINESS LAW. FAMILY LAW. INTERNATIONAL PRIVATE LAW

TSUL LEGAL REPORT

Journal home page: www.legalreport.tsul.uz

TSUL LEGAL REPORT
TLR

Received: 10.04.2025 Accepted: 03.06.2025 Published: 23.06.2025

DOI: 10.51788/tsul.lr.6.2./BMAD6201

MODERN CYBERCORRUPTION: CONCEPT, PROBLEMS AND WAYS OF COUNTERACTION IN THE CENTRAL ASIAN REGION

Gulyamov Said Saidakhrarovich,
Head of the Department of Cyber Law,
Chairman of the Council of Young Scientists
of the Academy of Sciences of the Republic of Uzbekistan,
Tashkent State University of Law
Doctor of Science in Law, Professor,
ORCID: 0000-0002-2299-2122
e-mail: said.gulyamov 1976@gmail.com

Rustambekov Islambek Rustambekovich,
Acting Rector of Tashkent State University of Law,
Doctor of Science in Law, Professor
ORCID: 0000-0002-8869-8399
e-mail: i.rustambekov@tsul.uz

Abstract. This study examines the phenomenon of cybercorruption–the use of digital technologies to carry out corrupt practices–in the context of the Central Asian region. The purpose of the study is to analyze the essence of cybercorruption, identify key manifestations of this phenomenon, and develop recommendations to counter this threat. The research methodology is based on a comprehensive analysis of the legal framework for cybersecurity and anti-corruption, a comparative study of international experience, and the systematization of recommendations from international organizations. The results indicate the growing vulnerability of the region to cybercorruption due to the insufficient adaptation of legal systems to digital transformation, the limited capacity of law enforcement agencies, and inadequate regional coordination. The proposed recommendations include improving the legal framework, developing institutional mechanisms, and expanding regional cooperation to effectively prevent and suppress cybercorruption. The presented analysis is important for the formation of a comprehensive policy to ensure digital security and transparency in Central Asia.

Keywords: cybercorruption, digital finance, cybersecurity, legal regulation, cryptocurrencies, digital assets, cross-border cooperation, Central Asia

Introduction

Corruption is a multifaceted global problem that imposes significant social, economic, and political costs on societies worldwide [1]. The World Economic Forum estimates that global losses from corruption amount to approximately US$2.6 trillion, or 5% of global GDP [2]. However, in recent years, there has been a qualitative transformation of corrupt practices associated with the digitalization of the economy and society. The emergence and spread of new digital technologies, such as cryptocurrencies, online banking, blockchain, and encrypted communications, have created conditions for the evolution of corruption into a new form–cybercorruption [3].

Cybercorruption can be defined as the use of digital technologies and infrastructure to carry out and conceal corrupt acts, as well as the exploitation of digital spaces and assets as objects of corruption. Unlike traditional forms of corruption, cybercorruption is characterized by its cross-border nature, technological complexity, and increased anonymity, which pose significant challenges to existing legal systems and law enforcement structures [4].

The Central Asian states (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan) are particularly vulnerable to this growing threat. On the one hand, these countries are actively promoting the digital transformation of their economies by introducing e-government, digital financial services, and developing ICT infrastructure. On the other hand, the legal and institutional frameworks for cybersecurity and anti-corruption in the region often lag behind the pace of technological change [5]. This creates favorable conditions for the spread of various forms of cybercorruption.

This study aims to address the following research questions:

1) What is the essence of cybercorruption, and what are its key manifestations in the Central Asian region?

2) What are the main shortcomings of the existing legal and institutional frameworks that create conditions for the spread of cybercorruption?

3) What regulations and measures should be adopted in Central Asian countries to effectively combat cybercorruption?

The relevance of the study stems from the rapid penetration of digital technologies into all spheres of public life in the region and the need for timely adaptation of legal and institutional mechanisms to prevent new forms of corruption. The novelty of the study lies in its comprehensive analysis of cybercorruption as an interdisciplinary problem situated at the intersection of legal, technological, and socioeconomic aspects.

Theoretical Foundations of Cybercorruption Research

Conceptualization of Cybercorruption

To formulate a theoretical framework for analysis, it is necessary to clearly distinguish among the concepts of "cybercorruption," "cybercrime," and "cyberfraud." Although these terms are often used interchangeably, they reflect distinct, albeit overlapping, phenomena.

Cybercrime is a broad category of illegal activities committed using computer systems and networks [6]. It encompasses a variety of offenses, from hacking into computer systems to data theft and the distribution of malware.

Cyberfraud, a subcategory of cybercrime, refers to acts aimed at deception for the purpose of obtaining financial or material gain in the digital environment [7].

Cybercorruption, in contrast, has specific characteristics that distinguish it from other forms of cybercrime. Based on the classic definition of corruption as "the abuse of entrusted power for private gain" [8], cybercorruption can be defined as the use of digital technologies and systems to abuse power or trust to obtain undue benefits. The key difference between cybercorruption and other forms of cybercrime is the presence of an element of abuse of power or trust, typically associated with state or corporate institutions.

Cybercorruption can manifest in various forms:

1. Traditional corruption facilitated by digital technologies–for example, the use of cryptocurrencies to pay bribes or encrypted messengers to organize corruption schemes.

2. Corruption in the management of digital assets and systems–for example, manipulation of electronic public procurement systems or the illegal allocation of digital resources, such as radio spectrum.

3. Systemic capture of the digital regulatory environment–for example, shaping cybersecurity or data protection legislation to benefit certain groups [9].

The Relationship between Digitalization and Corruption Risks

Digitalization processes have dual effects in the context of corruption. On the one hand, the introduction of digital technologies has the potential to promote transparency and accountability, reducing opportunities for corruption [10]. Electronic public service systems, digital public procurement platforms, and automated decision-making processes can minimize human intervention and reduce the discretionary powers that traditionally create opportunities for corruption.

On the other hand, digitalization also creates new opportunities for corruption through:

- **Technological complexity**–many digital systems and processes are difficult for nonprofessionals to understand, creating information asymmetries and hindering public oversight.
- **Digital monopolies and oligopolies**–the concentration of control over digital infrastructure and key technologies creates new forms of power that can become targets of corruption.
- **Anonymity and cross-border nature**–digital technologies facilitate anonymous and cross-border fund transfers, making it more difficult to trace corrupt transactions [11].

Empirical research shows that the relationship between digitalization and reduced corruption is not automatic and depends on the quality of institutions, the legal environment, and political will [12]. In countries with strong institutions, digitalization does indeed reduce corruption, while in countries with weak institutions, the effect may be the opposite–digitalization may facilitate the emergence of more complex and difficult-to-detect forms of corruption.

Materials and methods

This study employs four complementary methodological approaches to examine cybercorruption trends in Central Asian states and identify policy responses to this problem. First, it provides a detailed review of existing legal frameworks and governance policies related to cybercrime, cybersecurity, and anti-corruption at the national level in Central Asia. Second, it analyzes the current discourse and data on measured and estimated cybercorruption activities in the region, produced by government agencies, international organizations, and investigative journalists. Third, it compares policy frameworks and reported forms of cybercorruption in Central Asia with those in other developing countries. Finally, it summarizes proposed legal, institutional, and technological measures to counter cybercorruption risks, drawing from global standard-setting bodies, regional organizations, and national governments.

These four sources of evidence are integrated to define the contours of cybercorruption as a concept, map its current manifestations in Central Asia, examine the vulnerabilities that allow it to grow, and develop responses rooted in legal precedents, best institutional practices, and technological solutions already emerging worldwide.

Research results

Manifestations of Cybercorruption in a Global Context

Before analyzing the specifics of the Central Asian region, it is appropriate to examine the most common manifestations of cybercorruption in global practice, with particular attention to examples from developed countries, which can serve as a warning for developing economies.

Manipulation of Electronic Procurement Systems

Electronic public procurement systems have been implemented in many countries to enhance transparency and efficiency. However, these systems have also become targets for cybercorruption. In recent years, a scheme was uncovered in South Korea to manipulate the e-procurement system, allowing bidders to submit the most advantageous offers [13]. In Italy, a scheme was revealed in which technical specifications in e-tenders were formulated to favor specific suppliers [14].

Such manipulations are enabled by technical vulnerabilities in e-procurement systems, insufficient safeguards against insider threats, and limited understanding of digital processes by regulatory authorities.

Use of Cryptocurrencies in Corruption Schemes

Cryptocurrencies, which offer a high level of anonymity for transactions, are increasingly used as a tool for corrupt payments. In 2022, a case was uncovered in the United States in which a federal employee received bribes in Bitcoin for providing confidential information [14].

Of particular concern is the use of so-called “privacy” cryptocurrencies, such as Monero and Zcash, which provide greater anonymity than Bitcoin, making it even more challenging to track corrupt transactions [15].

Corruption in Digital Asset Management

The distribution and management of digital assets, such as radio spectrum, top-level domains, and digital identifiers, are increasingly vulnerable to corruption. In 2017, an investigation was launched into irregularities in the distribution of 4G frequencies, where certain telecommunications companies received preferential treatment [16]. In Spain, a 2019 case exposed corruption in the allocation of public contracts for digital infrastructure development [17].

Manipulation of Digital Data

Digital data is becoming a valuable resource, and its distortion or misuse can be an element of corruption schemes. In 2016, the United Kingdom uncovered cases of air pollution data manipulation conducted to benefit certain industrial enterprises [18]. In Japan, a 2018 case revealed manipulation of bank stress test data, allowing financial institutions to evade stricter regulation [19].

Corruption in Cybersecurity

Corruption in cybersecurity is particularly concerning, as it undermines the digital protection of states and societies. In the United States, numerous cases of cybercorruption and cybercrime have been uncovered in recent years [20]. In Sweden, a 2019 case revealed that a government official responsible for cybersecurity concealed information about serious vulnerabilities in exchange for a reward [21].

These examples from developed countries demonstrate the diversity and complexity of cybercorruption schemes and underscore the need for a comprehensive approach to countering them. Central Asian states, in the early stages of digital transformation, have an opportunity to apply these lessons when developing strategies to ensure digital transparency and security.

Analysis of research results

Analysis of Legal and Institutional Frameworks in Central Asia

Current State of the Regulatory Framework

An analysis of the legislation of Central Asian countries reveals several key issues that limit the effectiveness of efforts to combat cybercorruption.

Inadequate Definitions of Corruption Crimes

In many countries in the region, legislative definitions of corruption crimes, such as bribery and abuse of office, focus on tangible assets. For example, the Criminal Code of the Republic of Uzbekistan (Article 211) defines a bribe as “material assets or property benefits,” which does not always allow for effective application to digital assets, such as cryptocurrencies or virtual goods [22]. Similar issues are observed in the legislation of Tajikistan and Kyrgyzstan.

Fragmented Regulation

There is a disconnect between anti-corruption legislation and laws governing cybersecurity and cybercrime. For example, in Kazakhstan, the Anti-Corruption Law and the Electronic Document and Electronic Digital Signature Law operate in parallel without sufficient integration mechanisms [23]. This creates legal gaps that can be exploited for cybercorruption activities.

Differences in Regional Approaches

Central Asian countries exhibit varying levels of development in cybersecurity and anti-corruption legislation. Uzbekistan and Kyrgyzstan have adopted dedicated cybersecurity laws, whereas Tajikistan and Turkmenistan regulate these issues primarily within the framework of general information security legislation or through separate provisions in various regulations [24]. This heterogeneity complicates regional coordination in combating cybercorruption.

Limited Regulation of Digital Finance

The regulation of new financial technologies, such as cryptocurrencies and blockchain, which can be used in corruption schemes, remains underdeveloped across the region. For example, Uzbekistan legalized cryptocurrencies in 2018, but the regulatory framework for monitoring and controlling related transactions is still inadequate [25].

Institutional Mechanisms and Their Effectiveness

Central Asian countries have established various institutional mechanisms to combat corruption and ensure cybersecurity, but their effectiveness in addressing cybercorruption remains limited.

Multiplicity and Overlap of Powers

In many countries in the region, overlapping functions among government bodies hinder effective coordination. For example, in Kazakhstan, cybersecurity issues are managed by the National Security Committee, the Ministry of Digital Development, and the State Technical Service, with no clear delineation of responsibilities [26]. A similar situation exists in anti-corruption efforts, where functions are distributed among anti-corruption agencies, law enforcement bodies, and specialized units within various ministries.

Limited Technical Capacity

Most anti-corruption agencies in the region lack the technical capacity to detect and investigate complex cybercorruption schemes. The shortage of digital forensics specialists, modern equipment, and specialized software for analyzing digital evidence reduces the effectiveness of efforts to combat cybercorruption [27].

Insufficient Interagency Cooperation

There is limited cooperation between cybersecurity and anti-corruption agencies. For example, in Uzbekistan, the Anti-Corruption Agency and the Cybersecurity Centre operate relatively autonomously, hindering a comprehensive approach to cybercorruption [28].

Limited Private Sector and Civil Society Involvement

The involvement of the private sector and civil society in countering cybercorruption remains insufficient in the region. In developed countries, private companies, particularly in the financial and telecommunications sectors, often play a key role in identifying suspicious transactions and cyberattacks linked to corruption [29].

International and Regional Cooperation

Central Asian countries participate in various international initiatives in the areas of anti-corruption and cybersecurity, but their level of engagement varies.

Participation in International Conventions

All countries in the region have ratified the United Nations Convention against Corruption, providing a common legal basis for international cooperation. However, engagement with cybersecurity frameworks is less consistent. None of the Central Asian countries are party to the Budapest Convention on Cybercrime, which provides an international legal framework for combating cybercrime [30].

Regional Initiatives

The Shanghai Cooperation Organization (SCO), which includes Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, is developing mechanisms for cooperation in information security. In 2019, the SCO adopted an action plan to implement its Development Strategy until 2025, incorporating measures to strengthen information security [31]. However, these initiatives often lack specificity in addressing cybercorruption.

Technical Assistance and Exchange of Experience

Countries in the region participate in technical assistance programs offered by international organizations, such as the United Nations, OSCE, and the World Bank. These programs include training specialists, developing methodologies, and providing technical equipment to combat corruption and cybercrime [32].

Recommendations for Improving the Regulatory Framework and Institutional Mechanisms

Improving Legislation

To effectively combat cybercorruption, Central Asian countries are advised to:

Expand Definitions of Corruption Offenses: Definitions of corruption offenses should include digital assets and intangible benefits. For example, the definition of a bribe should encompass not only tangible assets but also cryptocurrencies, virtual assets, and access to digital data, aligning with OECD recommendations for modernizing anti-corruption legislation in the digital age [33].

Adopt Specialized Cybercorruption Legislation: Countries should consider enacting laws specifically targeting cybercorruption, defining offenses such as manipulation of e-procurement systems, misuse of digital public resources, and corruption in the distribution of digital assets. Singapore's Digital Trust Act, which includes provisions to combat digital fraud and corruption, serves as a model [34].

Harmonize Cybersecurity and Anti-Corruption Legislation: Legislation should be harmonized to eliminate gaps and contradictions, incorporating uniform terminology, standardized investigation procedures, and consistent sanctions for related offenses.

Regulate Digital Finance: Comprehensive regulation of digital financial technologies, such as cryptocurrencies and blockchain, should balance innovation with preventing their use in corruption schemes. The European Union's Fifth Anti-Money Laundering Directive, which mandates customer identification and transaction monitoring for cryptocurrency exchanges, provides a model [35].

Adopt Data Protection Legislation: Given the misuse of data in cybercorruption, countries should adopt modern data protection laws aligned with international standards, such as the European Union's General Data Protection Regulation (GDPR). These should include provisions for transparency, purpose limitation, and liability for violations [36].

Strengthening Institutional Mechanisms

Establish Specialized Units: Countries should create specialized units within anti-corruption agencies to address cybercorruption, staffed with experts in information technology, digital forensics, and financial analysis. Estonia's department for combating digital financial crimes within its Anti-Corruption Bureau is a successful example [37].

Develop Technical Capacity: Investments in modern digital forensics equipment, specialized data analysis software, and staff training in cybercorruption investigation methods are essential. The United Kingdom's Digital Investigation Enhancement Program serves as a model [38].

Establish Interagency Coordination Mechanisms: Formal coordination mechanisms, such as interagency working groups or joint operational centers, should be established between anti-corruption and cybersecurity agencies. The Netherlands' National Cyber Security Centre exemplifies this approach [39].

Engage the Private Sector and Civil Society: Mechanisms for involving the private sector and civil society should be developed, including platforms for sharing cyber threat information, safe reporting channels for cybercorruption cases, and public awareness programs. The United Kingdom's Cyber Defense Alliance, which collaborates with financial institutions and law enforcement, is a successful example [40].

Develop Digital Monitoring Systems: Digital monitoring systems using machine learning to detect suspicious activities in government information systems, particularly those related to public resource allocation, should be implemented. The European Commission's ARACHNE system, used to identify fraud and corruption risks in EU-funded projects, is a relevant example [41].

Expanding International and Regional Cooperation

To address cross-border cybercorruption, Central Asian countries should:

Join International Conventions: Countries should consider acceding to the Budapest Convention on Cybercrime, which provides an international legal framework for cooperation in cybercrime investigations and facilitates harmonization with international standards [42].

Develop Regional Cooperation Mechanisms: Within regional groupings like the SCO or the Commonwealth of Independent States, specialized mechanisms for combating cybercorruption should be established, including regional cyber threat information exchange centers, joint investigation teams, and experience-sharing programs [43].

Establish a Regional Information-Sharing Platform: A regional platform for exchanging information on cyber threats and suspicious transactions, involving law enforcement, financial institutions, and telecommunications companies, should be created, modeled on the European Union's Financial Intelligence Units [44].

Participate in Technical Assistance Programs: Countries should actively engage in technical assistance programs from organizations like the United Nations, OSCE, and World Bank to access best practices, technologies, and knowledge for combating cybercorruption [45].

Collaborate with Global Technology Companies: Partnerships with companies like Microsoft, Google, and IBM can provide expert support in cybersecurity and countering digital fraud. The partnership between Microsoft and the Government of Singapore under the Digital Crime Unit program is a notable example [46].

Implementing Technological Solutions

To enhance efforts against cybercorruption, Central Asian countries should implement the following technological solutions:

Blockchain for Transparency: Blockchain technology can ensure transparency and immutability in critical government processes, such as public procurement, property registration, and subsidy distribution. Estonia's e-Estonia system demonstrates successful blockchain application in public administration [47].

Big Data Analytics Tools: Big data analytics tools should be implemented to identify suspicious patterns and relationships indicative of corrupt activity, analyzing data from government registries, financial transactions, and social media. The World Bank's Corruption Hunter Network is an example [48].

Data Integrity Monitoring Systems: Systems to detect unauthorized changes to critical information systems should be implemented to prevent data manipulation. Such systems are used in the U.S. banking sector to prevent financial data fraud [49].

Automated Compliance Systems: Automated systems to monitor compliance with rules and regulations by public officials and public resource use should be adopted to detect deviations and signal corruption risks. Mexico's SIIGAT system for monitoring public contracts is a relevant example.

Digital Platforms for Public Oversight: Digital platforms enabling citizens to monitor public resource use and report potential corruption should be created to enhance transparency and foster a culture of intolerance toward corruption. India's I Paid A Bribe platform is a successful example [50].

Conclusion

Cybercorruption is a complex problem situated at the intersection of legal, technological, and socioeconomic aspects. In the context of the accelerated digital transformation of Central Asian countries, this issue is particularly pressing and requires targeted solutions.

An analysis of global efforts to combat cybercorruption reveals the diversity of its manifestations, from the manipulation of e-procurement systems to the use of cryptocurrencies in corruption schemes and corruption in the management of digital assets. Examples from developed countries serve as valuable warnings for developing economies in Central Asia, enabling them to anticipate potential risks and develop preventive measures proactively.

An assessment of the legal and institutional frameworks in Central Asian countries highlights several key challenges: definitions of corruption crimes not adapted to digital realities, fragmented regulation, divergent regional approaches, and limited oversight of digital finance. At the institutional level, issues include overlapping responsibilities among agencies, limited technical capacity, insufficient interagency cooperation, and minimal involvement of the private sector and civil society in combating cybercorruption.

To address these challenges effectively, Central Asian countries should adopt a comprehensive approach, encompassing legislative improvements, strengthened institutional mechanisms, expanded international and regional cooperation, and the adoption of modern technological solutions. Particular emphasis should be placed on harmonizing and modernizing the regulatory framework, establishing specialized units to combat cybercorruption, developing interagency coordination mechanisms, and actively engaging the private sector and civil society.

Implementing these recommendations will enable Central Asian countries not only to counter current forms of cybercorruption but also to establish a robust foundation for preventing emerging forms of corruption driven by further technological advancements. This, in turn, will foster an environment conducive to the digital transformation of economies and societies, enhancing trust in government institutions and strengthening the region's position in the global digital economy.

Ultimately, success in combating cybercorruption will depend not only on technical and legal solutions but also on political will, institutional capacity, and societal digital literacy. Central Asian countries have a unique opportunity to learn from the experiences of developed nations, avoid many of the challenges encountered during their digital transformations, and develop tailored approaches to ensure digital transparency and security that reflect local conditions.

REFERENCES

1. Mauro P. Corruption and growth. *The Quarterly Journal of Economics*, 1995, vol. 110(3), pp. 681–712.

2. W.E.F. Global Competitiveness Report: The Cost of Corruption. World Economic Forum. 2020.

3. Abbott J., Genschel P., Snidal D., Zangl B. Orchestration: Global governance through intermediaries. Oxford University Publ., 2022.

4. Burkert H. Legal aspects of cybersecurity. In Cybersecurity in Digital Governance. 2022, pp. 65–86.

5. ITU. Global Cybersecurity Index 2020. International Telecommunication Union. 2020.

6. UNODC. Cybercrime and Anti-Corruption: Challenges and Responses in Central Asia. United Nations Office on Drugs and Crime. 2020.

7. Jaeger M.D. Globalization and cyber-corruption. *International Journal of Management, Accounting and Economics*, 2018, vol. 5 (9), pp. 656–663.

8. Jain, A. K. Corruption: A review. *Journal of Economic Surveys*, 2001, vol. 15(1), pp. 71–121.

9. Ramappa, T., Aithal, P.S. Digital Corruption: Forms, Causes and Consequences. *International Journal of Management, Technology, and Social Sciences*, 2022, vol. 7(1), pp. 120–135.

10. Chetwynd E., Chetwynd F., Spector B. Corruption and poverty: A review of recent literature. Management Systems International. 2003.

11. World Bank. Enhancing Government Effectiveness and Transparency: The Fight against Corruption. World Bank Group. 2020.

12. UNCTAD. 2018.

13. Algorithm Watch. Entirely automated public tenders in Italy. 2024. Available at: https://algorithmwatch.org/en/entirely-automated-public-tenders-in-italy/

14. TRM Labs. The illicit crypto ecosystem report 2022. Available at: https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022

15. Elliptic. Cryptocurrency Financial Crime Report. Elliptic Research. 2021.

16. VOI.ID. 2022. Available at: https://voi.id/en/technology/280711

17. El País. Corruption in digital infrastructure contracts exposed. El País International. 2020. Available at: https://english.elpais.com/

18. Environmental Audit Committee. Report on Air Quality Data Manipulation. UK Parliament. 2017.

19. Regulation Asia. FSA Japan issues order over use of falsified data in stress tests. 2024. Available at: https://www.regulationasia.com/fsa-japan-issues-order-over-use-of-falsified-data-in-stress-tests/

20. FBI. Annual Report on Cryptocurrency-Related Crimes. Federal Bureau of Investigation. 2020.

21. Swedish National Council for Crime Prevention. Report on Corruption in Public Sector Cybersecurity. Government Offices of Sweden. 2020.

22. OSCE. Analysis of Anti-Corruption Legislation in Central Asia. Organization for Security and Co-operation in Europe. 2019.

23. OSCE. Cybersecurity in Central Asia: Policy Developments and Regional Cooperation. Organization for Security and Co-operation in Europe. 2020.

24. ITU. Cybersecurity Regulatory Frameworks in Central Asia. International Telecommunication Union. 2021.

25. IMF. Financial Sector Assessment Program: Regulatory Frameworks for Fintech. International Monetary Fund. 2019.

26. OECD. OECD Public Integrity Handbook. OECD Publ., 2020.

27. Council of Europe. Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Office. 2021.

28. SCO. Shanghai Cooperation Organization Strategy until 2025: Implementation Plan. SCO Secretariat. 2019.

29. OECD. Anti-Corruption Reforms in Eastern Europe and Central Asia. OECD Publ., 2021.

30. Government of Singapore. Digital Trust Act: Implementation Guidelines. Infocomm Media Development Authority. 2019.

31. European Commission. Fifth Anti-Money Laundering Directive. Official Journal of the European Union. 2018.

32. European Data Protection Board. Guidelines on GDPR Implementation. EDPB Secretariat. 2020.

33. Government of Estonia. Digital Crime Unit: Structure and Functions. Ministry of Justice of Estonia. 2020.

34. UK National Crime Agency. Digital Investigation Enhancement Program: Evaluation Report. National Crime Agency. 2021.

35. Government of the Netherlands. National Cyber Security Center: Strategic Framework. Ministry of Justice and Security. 2021.

36. Cyber Defense Alliance. Annual Report 2021: Collaborative Defense against Cyber Threats. CDA Publ., 2022.

37. European Commission. ARACHNE Risk Scoring Tool: Technical Guidelines. Publications Office of the European Union. 2021.

38. SCO. Cooperation in Information Security within the SCO Framework. SCO Secretariat. 2020.

39. Egmont Group. Annual Report: Strengthening Financial Intelligence Cooperation. Egmont Group Secretariat. 2020.

40. UNODC. Technical Assistance Program for Countering Cybercrime in Central Asia. United Nations Office on Drugs and Crime. 2022.

41. Microsoft. Digital Crime Unit: Public-Private Partnerships in Cybersecurity. Microsoft Corporate Report. 2022.

42. e-Estonia. Digital Government Blueprint: Blockchain Applications in the Public Sector. e-Estonia Briefing Centre. 2022.

43. World Bank. Corruption Hunter Network: Leveraging Data Analytics. World Bank Group. 2021.

44. Financial Crimes Enforcement Network. Advisory on Cyber-Enabled Financial Crime. US Department of the Treasury. 2020.

45. I Paid A Bribe. Citizen-Powered Anti-Corruption Platform: Impact Assessment. Janaagraha Center for Citizenship and Democracy. 2021.

46. Department of Justice. Report on Law Enforcement Cyber Incidents. US Department of Justice. 2018.

47. European Anti-Fraud Office. The OLAF Report 2019. Publications Office of the European Union. 2020.

48. Financial Services Agency. Report on Banking Data Manipulation Incidents. Government of Japan. 2019.

49. OECD. Preventing Corruption in Public Procurement. OECD Publ., 2016.

50. Transparency International. Corruption in Public Procurement: Evidence and Solutions. Transparency International Secretariat. 2019.

SINCE 2020

TSUL LEGAL REPORT

T L R

TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 2
JUNE 2025