

TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026



JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.7.2.
E-ISSN: 2181-1024



Founder: Tashkent State University of Law



TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.7.2.

«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.

Copyright belongs to Tashkent State University of Law. All rights reserved. Use, distribution and reproduction of materials of the journal are carried out with the permission of the founder.

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

© 2026. TSUL – Tashkent State University of Law.

EDITOR-IN-CHIEF

B. Khodjaev – Rector of Tashkent State University of Law, Doctor of Law, Professor

DEPUTY EDITOR

Z. Esanova – Deputy Rector for Scientific Affairs and Innovations of Tashkent State University of Law, Doctor of Law, Professor

EXECUTIVE EDITOR

E. Mustafaev – Head of the Periodicals Department of the Editorial and Publishing Center of Tashkent State University of Law

MEMBERS OF THE EDITORIAL BOARD

N. Koutras – Kurtin Law School, PhD (Australia)

H. Yeung – Associate Professor of Leicester Law School, University of Leicester, (UK)

C. Kelley – Associate Professor of Law School of Arkansas University (USA)

A. Younas – Researcher of the Chinese Academy of Sciences, General Director of Ai Mo Innovation Consultants (China)

Sh. Al-Fatih – Lecturer of the University of Muhammadiyah Malang (Indonesia)

A. Jaelani – Lecturer of Sebelas Maret University (Indonesia)

N. Upadhyay – Associate Professor of the Department of Law and Programs of the Symbiosis Law School (India)

Y. Ogurlu – Rector of Balikesir University (Turkey)

K. Molodyko – Chief Expert of the Institute of National and Comparative Law Research at the "School of Higher Economics" of the National Research University of Russia, Associate Professor of the Department of International Law (Russia)

N. AllahRakha – Lecturer of the Department of Law and Technology of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Pakistan)

N. Rakhmonkulova – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

A. Tadjibaeva – Associate Professor of the Department of Criminal Procedure Law of Tashkent State University of Law, Candidate of Legal Sciences (Uzbekistan)

R. Urinboev – Professor of the Department of Sociology of Law of Lund University, Doctor of Law (Austria)

M. Kudratov – Doctor of the University of Regensburg (Germany)

Kh. Radjapov – Associate Professor of the Department of Entrepreneurship and Corporate Law of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Uzbekistan)

O. Narziev – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

Sh. Rakhmanov – Head of the Department of International Law and Human Rights of Tashkent State University of Law, Doctor of Law, Professor (Uzbekistan)

CONTENTS

12.00.01 – THEORY AND HISTORY OF STATE AND LAW. HISTORY OF LEGAL DOCTRINES

MAKSUDBOY SADIKOV ABDULAJONOVICH, YOUNAS AMMAR

Artificial intelligence in legal drafting: a comparative analysis of Uzbekistan and China5

12.00.02 – CONSTITUTIONAL LAW. ADMINISTRATIVE LAW. FINANCIAL AND CUSTOMS LAW

NODIRBEKOVA DILDONA ABDUMALIK KIZI

The right to access environmental information: problems of implementing
the Aarhus Convention in Uzbekistan 12

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

**IMOMOV NURILLO FAYZULLAEVICH, JUCHNIEWICZ EDWARD,
MAKHMUDKHODJAYEVA UMIDA MUMINOVNA,
KORYOGDIEV BOBUR UMIDJON UGLI**

Civil law status of a bona fide possessor in CIS countries: a comparative
legal analysis 22

12.00.04 – CIVIL PROCEDURAL LAW. ECONOMIC PROCEDURAL LAW. ARBITRATION PROCESS AND MEDIATION

MASADIKOV SHERZODBEK MAKHMUDOVICH

International commercial arbitration law in the turkic states of Azerbaijan,
Türkiye and Uzbekistan 40

12.00.07 – JUDICIAL BRANCH. PROSECUTOR'S CONTROL. ORGANIZATION OF LAW ENFORCEMENT. ADVOCACY

MATMUROTOV ALIBEK RAVILOVICH

The importance of citizenship and educational qualifications requirements
for applicants to obtain advocate status 58

12.00.08 – CRIMINAL LAW. CRIMINAL-EXECUTIVE LAW

FAZILOV FARKHOD MARATOVICH, AMANJOLOVA BOTAGOZ ATYMTAEVNA

Criminal liability for digital corruption: Uzbekistan in comparative perspective 72

12.00.09 – CRIMINAL PROCEEDINGS. FORENSICS, INVESTIGATIVE LAW AND FORENSIC EXPERTISE

TULANBOEVA ADIBA ALIJON KIZI

Scientific-theoretical issues of electronic evidence in investigating cyberbullying
crimes 85

12.00.10 – INTERNATIONAL LAW

EGAMBERDIEV DILSHODJON ALISHEROVICH, DUBEY DEEPA

Crypto-actives as a new means of corruption crime: international and national criminal responsibility mechanisms 98

RASBERGENOVA SARBINAZ ALISHEROVNA

The system of international legal instruments for ensuring the human right to a healthy environment 110

NURULLAEV FARRUKH UMIDJONOVICH

Prospects of international cooperation of the Republic of Uzbekistan in combating cybercrime against children 116

KHOLMIRZAEVA SHOKHISTA ARZIQUL KIZI

The European Union's regional approach to combating illegal migration 125

12.00.13 – HUMAN RIGHTS

ODILOV JAMSHID BOBIRMIRZO UGLI

Guaranteeing public environmental rights through the regulatory framework of sanitary tree treatment 133

12.00.14 – CRIME PREVENTION. ENSURING PUBLIC SAFETY. PROBATION ACTIVITY

KHOSILOVA MADINA ERKINOVNA

Legal consequences of enforcing a foreign arbitral award annulled in the court of origin: analysing COMMISA v. PEMEX and Chromalloy Aeroservices v. Arab Republic of Egypt 141



TSUL LEGAL REPORT

Journal home page: www.legalreport.tsul.uz



Received: 12.05.2026

Accepted: 10.06.2026

Published: 30.06.2026

DOI: <https://dx.doi.org/10.51788/tsul.lr.7.2./CREX3919>

CRIMINAL LIABILITY FOR DIGITAL CORRUPTION: UZBEKISTAN IN COMPARATIVE PERSPECTIVE

Fazilov Farkhod Maratovich,

Acting Professor of the Department of the Criminal Law,
Criminology and Anti-Corruption,
Tashkent State University of Law,
Doctor of Science in Law

ORCID: <https://orcid.org/0000-0001-8603-1948>

e-mail: f.fazilov@tsul.uz

Amanjolova Botagoz Atymtaevna,

Professor of the Department of Criminal Law,
Criminal Procedure and Criminalistics,
Karaganda National Research University
named after Academician E.A. Buketov,
Candidate of Legal Sciences

ORCID: <https://orcid.org/0000-0002-9508-2234>

e-mail: Botanik76@mail.ru

Abstract. Digital transformation has significantly altered state operations while simultaneously reshaping the landscape of corruption. New schemes, inherently tied to emerging technologies, are increasingly categorized as “digital corruption.” This paper examines how criminal liability for such acts is regulated across several jurisdictions, focusing on the United States, Germany, and Singapore. These international approaches are subsequently compared with the legislative framework of the Republic of Uzbekistan using a comparative legal methodology to identify both commonalities and regulatory gaps. The analysis encompasses legal definitions, enforcement mechanisms, and practical experiences regarding corruption linked to digital assets, e-government platforms, and cyber-related misconduct. A key finding is the efficacy of flexible legal language in leading jurisdictions; terms such as “anything of value,” “benefit,” or “gratification” provide the necessary breadth to encompass modern forms of bribery, including cryptocurrency transfers and intangible advantages. While Uzbekistan’s Criminal Code remains robust, its reliance on the traditional formulation of “tangible valuables or pecuniary benefit” may be insufficiently broad to capture non-material digital advantages. Consequently, the paper concludes that Uzbekistan would benefit from updating its legal terminology to

reflect international standards. Furthermore, the development of specialized expertise in digital evidence and the deepening of international cooperation are presented as essential requirements for the legal system to effectively mitigate contemporary corruption risks in the digital age.

Keywords: *digital corruption, criminal liability, cryptocurrency bribery, cyber-enabled corruption, anti-corruption enforcement, digital assets in criminal law*

Introduction

Digital transformation has noticeably changed how corruption actually works in practice. It is no longer just about envelopes of cash or simple bank transfers. Today, corrupt deals can be arranged through encrypted messaging, hidden behind digital platforms, or carried out using new financial instruments. In my view, this shift makes corruption both more subtle and, at times, harder to detect (Nurmukhammedova, 2025).

At the same time, international anti-corruption law still relies on fairly broad legal concepts. For example, the United Nations Convention against Corruption uses the term “undue advantage.” This wording is important because it is not limited only to money or property. It may also cover other benefits, including non-material advantages. A similar approach can be seen in the position of the Financial Action Task Force, which treats virtual assets as a digital form of value and draws attention to their possible use in illegal financial transactions.

The purpose of this article is to analyze how criminal liability for digital corruption is regulated in selected foreign jurisdictions and to compare these approaches with the criminal legislation of the Republic of Uzbekistan. The article also seeks to determine whether the current legal framework of Uzbekistan is sufficient to respond to corruption risks that arise in the digital environment.

To achieve this purpose, the article sets several tasks. First, it is necessary to clarify the legal nature of digital corruption and identify its main forms. Second, the article examines the experience of the United States, Germany and Singapore in regulating criminal liability for corruption involving digital assets and cyber-related mechanisms. Third, it analyzes the strengths and weaknesses of Uzbekistan’s current criminal law in this area. Finally, the article develops proposals aimed at improving national legislation and law enforcement practice.

The main idea of the study is that criminal liability for digital corruption is more effective when the law uses flexible and technologically neutral concepts. Terms such as “anything of value,” “benefit,” “gratification” or “undue advantage” make it possible to cover not only traditional material benefits, but also digital assets and certain non-material advantages. From this point of view, the criminal legislation of Uzbekistan may need further conceptual and terminological improvement in order to respond more effectively to corruption risks in the digital age.

Special attention is paid to several issues: bribery involving digital assets, misuse of e-government systems and other forms of cyber-enabled corruption. By comparing foreign approaches, the article identifies both useful legal solutions and existing gaps. Some of these approaches may be adapted to the Uzbek legal system, while others depend on the institutional and procedural features of each country.

Methods

This research is built on a comparative legal approach. In simple terms, different legal systems are placed side by side and carefully examined. At the same time, the analysis is not purely formal. It also looks at how the law actually works in practice, which, in my view,

is just as important.

At the first stage, the study turns to jurisdictions with strong anti-corruption enforcement — the United States, Germany, and Singapore. Their legislation and legal doctrine are reviewed in a systematic way. The focus is mainly on criminal law provisions dealing with bribery, abuse of office, and related offenses. One key question runs through this part: are these norms flexible enough to cover corruption involving digital assets and cyber-mediated schemes?

The analysis does not stop at the text of the law. Statutes are examined together with doctrinal interpretations, court decisions, and enforcement guidelines. This gives a more complete picture. In particular, attention is paid to real cases — for example, situations involving cryptocurrency bribery or the misuse of digital infrastructure. These examples help to see how legal norms operate in practice, not just on paper.

By combining comparative analysis with a focused national case study, the research manages to highlight both strengths and weaknesses. Some gaps in regulation become quite visible. At the same time, certain institutional efforts look promising. Overall, this methodological approach provides a solid basis for further recommendations, especially those that are realistic and evidence-based rather than purely theoretical.

The United States, Germany and Singapore were selected for comparison on the basis of several criteria. First, these jurisdictions have developed anti-corruption enforcement practice and relatively strong institutional mechanisms. Second, their criminal law uses broad legal concepts, such as “anything of value,” “benefit” and “gratification,” which are important for assessing whether digital and non-material advantages may fall within the scope of bribery offences. Third, these countries represent different legal and institutional traditions: the United States reflects a common law and enforcement-oriented model, Germany represents a continental European legal approach, while Singapore demonstrates a strict preventive and institutional model of anti-corruption control.

Results

United States

The United States has a fairly strong and well-structured anti-corruption system. It is not just detailed on paper — it is also actively enforced, which, in practice, makes a real difference.

At the core of this framework are federal criminal laws that clearly prohibit bribery of public officials. One of the key provisions is 18 U.S.C. § 201. Its wording is quite broad, and that seems intentional. The law does not limit itself to money or traditional benefits.

Under this provision, liability arises when a person offers, gives, or even promises “anything of value” to a public official. What matters is the intent — there must be a corrupt purpose, namely to influence an official act. Even indirect actions fall within this rule, which closes many potential loopholes.

At the same time, the law applies equally to public officials themselves. If an official solicits, demands, or agrees to receive such a benefit under similar circumstances, criminal liability also follows. In other words, both sides of the corrupt transaction are covered.

What is particularly noteworthy, in my view, is the flexibility of the phrase “anything of value.” It allows the law to adapt to new realities, including digital forms of bribery, without constant amendments (Kohn, Kohn & Colapinto, n.d.).

The breadth of the phrase “anything of value” plays a key role in the U.S. approach. It is intentionally broad and, importantly, technologically neutral. Courts and enforcement authorities in the United States have consistently interpreted it in an expansive way. This means it covers not only physical assets, but also intangible and digital benefits.

In practice, the category includes money, cryptocurrencies, gifts, services, travel, entertainment, and even advantages that have subjective value.

This flexibility is not just theoretical. It actually allows the legal system to keep up with new forms of corruption. For instance, a bribe paid in Bitcoin is treated no differently from cash. Both are seen as “things of value” capable of influencing an official’s actions.

A similar logic can be seen in the Foreign Corrupt Practices Act (FCPA). It also uses the same broad concept and prohibits giving “anything of value” to foreign public officials in order to gain business advantages. Enforcement practice confirms that this includes digital assets. A notable example occurred in 2023, when U.S. authorities charged the founder of a cryptocurrency exchange for arranging a large-scale bribery scheme involving about \$40 million in digital assets to influence foreign officials. This case clearly shows that existing law already covers cryptocurrency bribery without the need for new special norms.

Beyond classic bribery provisions, the U.S. legal system relies on additional tools. The Computer Fraud and Abuse Act criminalizes unauthorized access to protected computer systems. While not designed specifically for corruption, it becomes relevant when officials misuse digital systems for personal gain.

At the same time, general fraud statutes — especially wire fraud and honest-services fraud — extend liability to schemes carried out through electronic means. This includes email, encrypted messaging apps, and online payment systems. In practice, these provisions significantly strengthen the ability of law enforcement to address cyber-enabled corruption.

Institutionally, the system also adapts quite quickly. A good example is the creation of the National Cryptocurrency Enforcement Team within the U.S. Department of Justice in 2021. This step reflects a clear focus on crimes involving digital assets.

Enforcement practice in the U.S. is often described as aggressive — and not without reason. Authorities actively pursue cases involving cryptocurrency-based bribery, as well as related offenses such as money laundering and fraud. What is particularly important is that they have learned to trace and confiscate digital assets. Courts have already ordered the seizure of cryptocurrencies linked to corruption cases.

Interestingly, all of this has happened without major legislative reforms. The law itself did not need to change drastically. Instead, the evolution took place at the level of interpretation and enforcement (Cohen & Stempel, 2023).

Germany

Germany’s legal framework for combating corruption looks quite structured and well thought out. The Strafrechtsgesetzbuch (StGB) plays a central role here, covering both public and private sector corruption in a systematic way.

At the heart of this system is the concept of *Vorteil* — “benefit.” It may sound simple, but in reality it is interpreted very broadly. In German doctrine, a benefit means almost any advantage a person is not legally entitled to receive. This includes not only money or gifts, but also services, discounts, hospitality, and even non-material advantages. In my view, this flexibility is one of the strongest aspects of the German approach.

Importantly, this concept is technologically neutral. Even though the law does not explicitly mention cryptocurrencies or digital assets, they clearly fall within the notion of a “benefit.” For example, if a public official receives Bitcoin in exchange for a decision, it is treated the same way as a cash bribe. This reflects a practical understanding: the form of value does not matter — its effect does.

The key anti-corruption provisions are found in § 331–335 StGB, which deal with bribery in the public sector, and § 299 StGB, which covers commercial bribery. These rules apply to both sides of corruption — the one who gives and the one who receives.

In practice, such cases are often combined with related offenses like fraud or money laundering.

Another interesting point is how German law connects corruption with cybercrime. Certain provisions, such as § 202a StGB (unauthorized access to data) and § 303a StGB (data manipulation), can be used alongside bribery charges. This creates a kind of cumulative liability. For instance, if an official manipulates an electronic procurement system, they may be liable not only for bribery but also for interference with data. This combined approach seems quite effective.

At the same time, not everything works perfectly. The rapid growth of digital technologies has exposed some gaps. A notable example comes from a recent court decision in 2025. The court found that cryptocurrency does not qualify as “property” (Sache) under traditional theft provisions because it lacks a physical form. As a result, the unlawful taking of digital assets did not meet the legal definition of theft, and the defendant was acquitted.

This case is quite revealing. It shows that while anti-corruption rules are flexible enough, other parts of criminal law may lag behind. There is a certain tension between traditional legal concepts and modern digital realities. This is not a failure of the system, but rather a sign that the law needs to evolve further.

Despite these challenges, Germany remains a country with a high level of integrity in public administration. According to Transparency International, it consistently ranks well in global corruption perception indices. Enforcement is carried out mainly by public prosecutors (Staatsanwaltschaften), who handle both domestic and international cases.

In the digital sphere, German authorities increasingly rely on international cooperation, especially within the European Union. Access to electronic evidence often depends on cross-border mechanisms, which are becoming more important every year. At the same time, there is a growing focus on digital forensics and specialized training.

Overall, the German model feels balanced. It combines broad legal concepts with practical enforcement tools. The idea of *Vorteil* allows the system to adapt to new forms of bribery, including digital ones. At the same time, ongoing debates about cryptocurrency and property law show that adaptation is still in progress (Atkins, 2025).

Singapore

Singapore’s anti-corruption system is often described as one of the strictest in the world. In addition, this reputation is well deserved. The legal framework is clear, and enforcement is consistently tough. The core statute here is the Prevention of Corruption Act (PCA), which works together with provisions of the Penal Code.

What is interesting is the terminology. Unlike many other jurisdictions, Singapore does not focus on the word “bribery.” Instead, it uses the concept of *gratification*. At first glance, it may seem like just a different label, but in reality, it carries a broader meaning.

The notion of gratification is intentionally wide. It covers not only money or obvious financial benefits, but also gifts, loans, rewards, and valuable securities. Beyond that, it includes services, favors, promises — basically any advantage given to a person. This open-ended wording is not accidental. It is designed to prevent loopholes.

From a doctrinal point of view, this approach feels quite modern. The concept is flexible and, importantly, technologically neutral. Even though the law does not explicitly mention digital assets, they clearly fall within its scope. For example, a transfer of cryptocurrency or access to a digital service can qualify as gratification if it is linked to corrupt intent.

In my view, this is one of the strengths of the Singaporean model. The law does not try to list every possible form of benefit. Instead, it relies on a broad concept that can adapt to new realities. As a result, digital forms of corruption — which are becoming more common

— do not escape criminal liability simply because they look different from traditional bribes.

Overall, Singapore’s framework shows how a well-designed legal concept can remain effective even as technology evolves (DLA Piper, 2022).

The concept of *gratification* in Singaporean law is intentionally broad — and this is not just a formal feature. In practice, it means that almost any advantage can fall within the scope of anti-corruption rules. It is not limited to direct payments. Indirect or non-monetary benefits are equally relevant. For instance, a paid vacation, exclusive event tickets, or preferential services may all qualify as unlawful if they are linked to corrupt intent. This approach, in my view, is quite practical: it minimizes grey areas that often exist in other legal systems.

Naturally, this logic extends to digital forms of value. A transfer of cryptocurrency or even a high-value NFT is treated in the same way as a cash payment. The specific form is not decisive — what matters is the benefit itself. The same applies to granting access to premium digital services, restricted databases, or paid platforms. If such access is provided to influence an official’s conduct, it can constitute gratification. This position is reinforced by the Singapore Penal Code, particularly Section 165, which prohibits public officials from receiving “anything of value” in connection with their duties without lawful justification.

At the same time, Singapore does not treat corruption in isolation. The legal framework operates in an integrated manner. There is no separate offense formally labeled “digital corruption,” but related conduct — such as manipulation of electronic records or unauthorized access to systems — is prosecuted under the Computer Misuse Act and relevant provisions of the Penal Code. These offenses can be combined with charges under the Prevention of Corruption Act, which results in a fairly comprehensive response.

Another important strength is the legal recognition of digital assets. Courts in Singapore have confirmed that cryptocurrencies can be frozen, seized, and confiscated. This is critical — without such recognition, enforcement would be significantly weaker. In addition, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act provides robust mechanisms for recovering illicit gains, regardless of whether they take the form of traditional money or digital assets. Again, the focus is on the benefit, not its form.

In terms of enforcement, Singapore is often seen as a benchmark. The Corrupt Practices Investigation Bureau (CPIB) plays a central role and operates with a high degree of independence. Cases are handled efficiently, and conviction rates remain consistently high. This contributes to Singapore’s reputation as one of the least corrupt jurisdictions globally.

What is also noteworthy is the preventive dimension. Digital governance tools — such as e-procurement systems and online public services — reduce direct interaction between officials and citizens. This, quite simply, lowers opportunities for corruption. At the same time, authorities actively rely on digital forensics to trace communications and financial flows, including those involving cryptocurrencies.

A particularly strong feature is the evidentiary presumption under the PCA. Where a public official receives gratification, it is presumed to have been received corruptly unless proven otherwise. This significantly simplifies the burden of proof and increases prosecutorial effectiveness, especially in complex cases involving indirect or technologically mediated transfers.

Overall, Singapore’s model appears coherent and well-balanced. Broad legal definitions, strong institutions, and the effective use of technology work together. In my view, this combination largely explains why the system remains resilient, even as corruption becomes more sophisticated and increasingly digital (Thuraisingam, 2023).

This, combined with the broad definition of *gratification*, creates a strong deterrent effect. It sends a clear signal that almost any improper benefit can trigger liability, regardless of how it is delivered.

At the same time, Singapore's recognition that even non-traditional forms of value may be corrupt has made the system particularly adaptable. Whether it is cryptocurrency, digital services, or other modern forms of exchange, such benefits are treated no differently from traditional payments. This allows authorities to deal with new schemes without constantly changing the law.

In summary, the experience of Singapore shows that clear and flexible legal definitions, combined with a specialized and effective enforcement body, are essential for addressing corruption in the digital era.

Uzbekistan

Legal Framework in Uzbekistan

Uzbekistan's criminal law addresses corruption through a set of specific provisions in the Criminal Code, supported by framework legislation. The Criminal Code of the Republic of Uzbekistan (1994, as amended) contains the core norms on bribery and related offenses.

Article 210 establishes liability for taking a bribe. It defines this offence as the knowing and unlawful acceptance by an official of material valuables, either directly or through an intermediary, or the obtaining of a pecuniary benefit in exchange for performing or refraining from performing actions within the scope of official duties.

The corresponding provision is Article 211, which criminalizes giving a bribe. Article 212, in turn, covers bribe intermediation, that is, the conduct of persons who facilitate, arrange, or transfer bribes between the parties.

Corruption in the private sector is also covered. Article 213 addresses so-called commercial bribery, namely the unlawful remuneration of employees of organizations for the misuse of their position. Article 214 deals with the extortion of such remuneration.

Taken together, these provisions form the core framework of criminal liability for corruption-related offences in Uzbekistan.

A key issue here is how the law defines the object of a bribe. Uzbek legislation refers to "tangible valuables" and "pecuniary benefit." This clearly covers traditional forms — cash, property, expensive gifts. It may also extend to digital assets like cryptocurrency, since they can be converted into money and thus represent economic value. In that sense, the wording is not entirely narrow.

However, compared to some foreign jurisdictions, the approach is still more conservative. The law does not explicitly mention intangible, non-monetary advantages. International standards, such as those reflected in the United Nations Convention against Corruption, use a broader concept of "undue advantage," which can include non-material benefits. Uzbek law is gradually moving in this direction, but the shift is not yet complete.

In practice, if corruption involves digital elements — for example, misuse of a government information system — liability may arise under other provisions, such as abuse of authority (Articles 205–209).

At the same time, Uzbekistan has developed a broader regulatory framework. The Law of the Republic of Uzbekistan On Combating Corruption establishes general principles and preventive measures. It does not introduce new crimes, but it plays an important coordinating role in anti-corruption policy.

There are also developments in the regulation of digital assets. Cryptocurrency-related activities are subject to strict control, and unauthorized operations can lead to liability. This indirectly supports the idea that crypto-assets may be treated as objects of bribery, even though the Criminal Code does not explicitly mention them.

Finally, cybercrime provisions also come into play. Offenses such as illegal access to computer information or interference with digital systems can be prosecuted alongside corruption charges. For example, if an official manipulates an electronic procurement system or deletes digital evidence, both corruption and cybercrime norms may apply.

Overall, the Uzbek framework is functional but still evolving. It covers classical corruption quite well, but the digital dimension is only partially integrated. Further development — especially clearer recognition of intangible and digital benefits — would make the system more consistent with modern realities.

Recent international developments support this broader understanding. Updated guidance from global bodies such as the United Nations Office on Drugs and Crime highlights the growing interconnection between cybercrime and corruption. In this view, technical methods—such as hacking or bypassing digital systems—are increasingly used as mechanisms for illicit enrichment, blurring the line between traditionally separate categories of crime (OECD, 2020).

In Uzbekistan, digital corruption typically appears in five main forms.

The first is traditional bribery carried out through digital channels, including crypto-assets and encrypted transactions within decentralized financial systems.

The second involves the manipulation of government decision-making platforms, such as e-procurement systems or subsidy registries, where outcomes can be quietly adjusted in favor of specific actors.

The third form is the abuse of privileged access. In these cases, officials or technical staff use their control over databases—whether cadastral, tax, or educational—to alter information for personal benefit.

The fourth pattern includes the use of malicious software to enable the embezzlement of public funds, often in ways that are difficult to trace.

The fifth, and perhaps most concerning, is the targeting of accountability mechanisms themselves. This includes deleting audit logs, altering metadata, or otherwise interfering with digital records in order to conceal wrongdoing (Yugai, 2025).

Enforcement Practices in Uzbekistan

In recent years, Uzbekistan has clearly stepped up its anti-corruption efforts, including the digital dimension. One of the key institutional changes was the creation of the Anti-Corruption Agency of the Republic of Uzbekistan in 2020. This body coordinates national policy and, in practice, plays a central role in shaping enforcement priorities.

At the same time, the state has started to actively use digital tools. A good example is the online platform *e-anticor.uz*, which allows citizens to report corruption cases directly. This kind of digital whistleblowing mechanism is quite important. It lowers barriers for reporting and, in my view, gradually builds a culture of accountability.

Enforcement statistics also suggest that the system is not passive. Each year, hundreds of officials are prosecuted for corruption-related offenses. This indicates that the legal framework is being applied in practice, not just formally.

Another noticeable trend is the focus on capacity building. In 2023–2024, initiatives were announced at the highest level to address cyber-related corruption, which was openly described as more complex and harder to detect. Starting from 2025, specialized training programs have been introduced in law enforcement academies. These include areas such as combating crime in digital technologies and legal support for cybersecurity. This is a logical step — without trained specialists, even the best laws remain ineffective.

There is also growing attention to international cooperation. Digital corruption, especially when it involves cryptocurrencies, often crosses borders. Uzbek authorities increasingly recognize the need to work with foreign partners, including crypto exchanges,

and to use tools like blockchain analytics to trace transactions. This reflects a gradual shift toward more modern investigative methods.

At the same time, certain challenges remain. One of them is the legal definition of a bribe. Current legislation focuses on tangible valuables and pecuniary benefits, which may not always clearly cover intangible advantages — for example, access to data or non-material favors. This creates some uncertainty in legal qualification.

In practice, the concept of “digital corruption” is still developing. Most cases so far involve traditional corruption schemes, even if they are facilitated by digital tools such as messaging apps or online platforms. Fully digital schemes — for example, those based entirely on cryptocurrencies or digital assets — are still relatively rare in enforcement practice.

Overall, Uzbekistan is moving in the right direction. There is visible progress in institutions, tools, and training. However, further refinement of legal definitions and continued investment in technical expertise will be essential to effectively address corruption in an increasingly digital environment (World Governments Summit, 2026).

Discussion

Comparison of Best Practices Across Jurisdictions

A clear pattern emerges from the comparison. The most effective systems rely on flexible legal definitions. In the United States, Germany, and Singapore, anti-corruption laws use broad terms such as “anything of value,” “benefit,” or “gratification.” These concepts are not tied to cash or physical property. Because of that, they easily cover modern forms of bribery — including cryptocurrency transfers, digital assets, or even non-material advantages.

This is, in many ways, a key lesson. Laws that are too narrow quickly become outdated. By contrast, broader wording allows the legal system to adapt without constant amendments. In the case of Uzbekistan, current legislation already covers digital assets as pecuniary benefits. However, it would be more effective to explicitly include both material and non-material advantages. This would remove any doubt in practice — for example, whether access to valuable data or a crypto-token can qualify as a bribe.

Another important practice is institutional design. Strong enforcement bodies make a real difference. Singapore’s Corrupt Practices Investigation Bureau is a good example of a specialized and independent institution. In the United States, there is no single agency, but entities like the Department of Justice and the Securities and Exchange Commission operate dedicated units for corruption and financial crimes. Germany relies on general prosecution bodies but strengthens them through training and coordination. Uzbekistan has followed this path by establishing the Anti-Corruption Agency of the Republic of Uzbekistan. The next step, in my view, is to deepen technical expertise — especially in digital forensics and financial analysis.

Digital Government and Prevention

Digitalization plays a dual role. It can create new corruption risks, but it also provides tools to reduce them. Singapore shows how e-government systems can limit opportunities for bribery. When procedures are automated and transparent, there is simply less room for informal arrangements. Uzbekistan is moving in the same direction by expanding digital public services and centralized service platforms.

At the same time, digital systems must be protected. As more processes move online, risks such as data manipulation or interference with electronic procurement increase. This means that strong IT controls, audit mechanisms, and clear liability rules are essential. Some countries, including Germany, already combine corruption offenses with cybercrime provisions. Uzbekistan can further develop this approach by ensuring that digital manipulation linked to corruption is consistently prosecuted.

Implications and Recommendations for Uzbekistan

From a legal perspective, targeted reforms would be useful. One step would be to expand the definition of a bribe to clearly include intangible and digital benefits. This would align national law with international standards and eliminate interpretative uncertainty. It may also be worth considering more specific provisions addressing the misuse of digital systems or data for personal gain.

Enforcement capacity is equally important. Continued investment in training for investigators, prosecutors, and judges is essential, particularly in areas such as digital evidence and blockchain analysis. Establishing specialized units or laboratories focused on digital investigations could significantly improve effectiveness. At the same time, international cooperation should be strengthened. Digital corruption often involves cross-border elements, so collaboration with global networks and foreign partners is crucial.

On the preventive side, further development of e-governance should continue, but with built-in safeguards. Transparency tools, secure authentication systems, and data analytics can all help detect suspicious patterns. Public awareness also matters — citizens should be able to recognize and report new forms of corruption, including those involving digital payments.

A broader issue is balancing innovation with control. Digital finance and new technologies bring economic benefits, but they also create risks. Uzbekistan is already taking a cautious approach by regulating cryptocurrency activities. Going forward, it would be important to integrate these rules with anti-corruption and anti-money laundering frameworks. Measures such as asset disclosure requirements for officials, including digital assets, could also strengthen transparency.

In the context of Uzbekistan, this comparative experience should be directly linked to Articles 210–214 of the Criminal Code, which regulate taking a bribe, giving a bribe, mediation in bribery, commercial bribery and unlawful receipt of remuneration. These provisions form the core of national criminal liability for corruption, but their wording is still mainly based on “material valuables” and “pecuniary benefit”. Such an approach works well for traditional forms of bribery, yet it may create difficulties when the unlawful advantage has a digital or non-material form. For this reason, the most suitable direction for Uzbekistan would be to preserve the existing structure of Articles 210–214, but to modernize their terminology in line with the broader concept of “undue advantage” used in the United Nations Convention against Corruption. This would allow the law to cover not only money and property, but also digital assets, access to valuable data, digital services, privileges and other non-material benefits capable of influencing the conduct of an official or another relevant person.

Conclusion

Digital corruption is a complex and evolving phenomenon. It crosses borders and relies on rapidly changing technologies. At the same time, the comparative analysis shows that existing legal systems can respond effectively — provided they are flexible and supported by strong enforcement.

The experience of leading jurisdictions demonstrates that broad legal definitions, combined with modern investigative tools and institutional capacity, remain effective even in the digital era. Uzbekistan has already made meaningful progress by strengthening its legal and institutional framework and recognizing cyber-related corruption as a growing challenge.

To build on these achievements, further steps are needed. These include refining legal definitions, investing in digital expertise, and expanding preventive mechanisms. Adopting best practices — such as technologically neutral legal concepts, specialized enforcement

capacity, and digital transparency tools — would significantly enhance the country's ability to combat corruption.

Ultimately, these efforts are not only about enforcement. They are also about trust. A system that can effectively respond to modern corruption risks strengthens confidence in public institutions and reinforces the principles of transparency, integrity, and the rule of law in a rapidly digitalizing world.

In April 2026, the Legislative Chamber of the Oliy Majlis passed a bill that formally classified 19 types of acts as corruption-related crimes. This decision has resolved a long-standing legal ambiguity where technical manipulations within databases could be interpreted as either disciplinary misconduct or ordinary regulatory violations. Now, this clear classification provides a legal foundation for the courts and investigative bodies (Government of Uzbekistan, 2024).

Digital evidence presents unique challenges: it is highly volatile, can be easily altered, and is often stored across multiple cloud environments.

Current analysis shows that Uzbekistan's legal and judicial systems are still adapting to international standards such as ISO/IEC 27037, which govern the identification, collection, and preservation of digital evidence. This transition is ongoing, and several practical challenges remain (The Tashkent Times, 2025):

Data Integrity: How can it be proven that log files extracted from the public procurement system were not altered by an administrator after the investigation began? (Gazeta.uz, 2026).

Metadata as the Key: It is often metadata (access time, IP address, device type) that establishes a link between an official and a corrupt transaction within a system that they were not formally authorized to access.

Proportionality of Collection: Maintaining a balance between the necessity of full data seizure for forensics and the right to privacy, especially in light of the implementation of the Law on Personal Data Protection (Kun.uz, 2026).

In 2026, Uzbekistan plans to establish a joint unit to combat digital corruption, comprising forensic specialists, financial analysts, and prosecutors, which should improve the quality of evidence collection in high-tech cases.

The 2025–2026 reforms in anti-corruption legislation have a direct economic dimension. The creation of a transparent digital environment and the strengthening of liability for manipulations within it are considered an “economic necessity.”

Uzbekistan has significantly improved its position in open data rankings (reaching 11th in the world and 1st in Central Asia by 2025), which sends a powerful signal to foreign investors. The implementation of the “Business Charter of Uzbekistan against Corruption” and the issuance of “compliance marks” to companies that have implemented internal anti-corruption control systems are contributing to the formation of a clean business environment (UNODC, 2026).

However, the 2025 Corruption Perceptions Index (CPI) showed a one-point decrease (to 31 points), which dropped the country to 124th place. This indicates that while digital monitoring tools are identifying more violations, the judicial system and civil society institutions are not yet fully coping with the pressure from “old elites” who resist transparency. The professor's legal opinion emphasizes that without ensuring judicial independence and protecting investigative journalists who expose corruption, digital reforms may remain mere “technical facades” (LCG Discovery, 2026).

Digital corruption is a complex and rapidly evolving phenomenon that combines elements of bribery, cybercrime, money laundering and abuse of official authority. The comparative analysis shows that the most effective legal systems use broad and

technologically neutral concepts, such as “anything of value,” “benefit,” “gratification” and “undue advantage.” In this regard, Uzbekistan should preserve the existing structure of Articles 210–214 of the Criminal Code, but modernize their terminology by clearly extending the object of a bribe to digital assets, access to information systems, digital services, privileges and other non-material advantages capable of influencing the conduct of an official or another relevant person.

At the same time, legal reform should be supported by practical enforcement mechanisms. It is advisable to include digital assets in the system of asset declarations for public officials, introduce clear procedures for collecting and preserving digital evidence, and develop specialized forensic expertise for cases involving cryptocurrency, e-government platforms and electronic databases. Strengthening cooperation with foreign law enforcement bodies, financial intelligence units, crypto exchanges and international organizations is also necessary, since digital corruption often has a cross-border nature. These measures would help Uzbekistan adapt its anti-corruption framework to modern digital risks while maintaining legal continuity and institutional stability. Corruption casts a long shadow over Uzbekistan’s socio-political landscape, hindering economic growth and social harmony. To confront this formidable challenge, Uzbekistan seeks to draw upon extensive experience harnessing New Emerging Technologies (NET) and the Unified Payments Interface (UPI), for effective anti-corruption measures. (Thommandru & Maratovich, 2024).

REFERENCES

- Atkins, J. (2025, August 1). *Legal loophole leaves Germany unable to prosecute ‘crypto’ theft*. CoinGeek. <https://coineek.com/legal-loophole-leaves-germany-unable-to-prosecute-crypto-theft/>
- Cohen, L., & Stempel, J. (2023, March 29). *U.S. charges FTX’s Bankman-Fried with paying \$40 mln Chinese bribe*. Reuters. <https://www.reuters.com/legal/ftxs-bankman-fried-charged-with-bribery-conspiracy-new-indictment-2023-03-28>
- DLA Piper. (2022, January 11). *Singapore – Global bribery offenses guide*. <https://www.dlapiper.com/en/insights/publications/2019/09/global-bribery-offenses-guide/singapore>
- Forensics and futures: Navigating digital evidence, AI, and risk in 2026 – Part 4. (2026). *LCG Discovery*. <https://lcgdiscovery.com/forensics-and-futures-navigating-digital-evidence-ai-and-risk-in-2026-part-4/>
- Gazeta.uz. (2026, February 13). *Uzbekistan falls in Corruption Perceptions Index for second year in a row*. <https://www.gazeta.uz/en/2026/02/13/corruption-perceptions-index/>
- Government of Uzbekistan. (2024). *The fight against corruption intensifies: 19 types of offences brought under new legislation*. <https://gov.uz/en/kontexnazorat/news/view/154163>
- Kohn, Kohn & Colapinto. (n.d.). *Understanding bribery in politics: Types and examples*. <https://kkc.com/frequently-asked-questions/understanding-bribery-in-politics-types-and-examples/>
- Kun.uz. (2026, February 18). *Uzbekistan to introduce new employment restrictions for former officials to combat corruption*. <https://m.kun.uz/en/news/2026/02/18/uzbekistan-to-introduce-new-employment-restrictions-for-former-officials-to-combat-corruption/>
- Nurmukhammedova, G. B. (2025). Topical issues of improving the legal definition of corruption in legislation. *American Journal of Public Diplomacy and International Studies*, 3(6).

Organisation for Economic Co-operation and Development. (2020). *The path to becoming a data-driven public sector*. <https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm>

The Tashkent Times. (2025). *Uzbekistan slips 3 places to 124th on Global Corruption Index*. <https://tashkenttimes.uz/national/16945-uzbekistan-slips-3-places-to-124th-on-global-corruption-index-2025>

Thommandru, A., & Maratovich, F. F. (2024). Harnessing novel technologies to fortify anti-corruption efforts: Assimilating India's experiences into Uzbekistan's fight against criminality. *Revista Brasileira de Politicas Publicas*, 14(1), 320–339. <https://doi.org/10.5102/rbpp.v14i1.9273>

Thuraisingam, K. (2023, March 23). *When will gifts and hospitality be considered corruption?* <https://thuraisingam.com/resources/when-will-gifts-and-hospitality-be-considered-corruption>

United Nations Office on Drugs and Crime. (2026). *Standards and best practices for digital forensics*. <https://www.unodc.org/cld/pt/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html>

World Governments Summit. (2026). *Algorithmic state: AI impact on modern governance decision-making*. <https://www.worldgovernmentssummit.org/media-hub/news/detail/trends-releases-report-on-'algorithmic-state'-analysing-ai-impact-on-modern-governance-decision-making>

Yugai, L. (2025, March 14). *Cyber corruption without borders: How criminals use digital assets*. UZA. https://uza.uz/en/posts/cyber-corruption-without-borders-how-criminals-use-digital-assets_697975



TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026