

PUBLIC CONTROL OVER PUBLIC AUTHORITIES THROUGH DIGITAL TECHNOLOGIES AS A TOOL FOR REDUCING ECONOMIC LOSSES FROM CORRUPTION: EUROPEAN EXPERIENCE AND PROPOSALS FOR UKRAINE

Victoria Savitska¹

Abstract. The article examines public control over public authorities exercised by means of digital technologies as an economic and legal mechanism for reducing corruption losses of the national economy. The *relevance* of the study is twofold. Firstly, the scale of such losses is considerable; for the European Union, it is estimated at between 179–990 billion EUR of GDP annually. Secondly, it is vital to consider the needs of Ukraine's post-war reconstruction, in which the credibility of accountability mechanisms directly determines the volume and cost of available international financing. The *purpose of the article* is threefold: firstly, to reveal the dual administrative-legal and economic nature of digital public control; secondly, to assess, on the basis of European experience and verified empirical data, its impact on reducing corruption-related losses; and thirdly, to formulate proposals for improving Ukraine's legislation. The *research methods* employed encompass the dialectical method, analytical and synthetic approaches, statistical analysis, economic and legal modelling based on agency and transaction cost categories, and a comparative legal approach to EU law, Member States' legislation and Ukrainian legislation. The main *results* show that digital public control has the characteristics of a public good and economies of scale. One-off public investments in open data reduce the marginal cost of each subsequent act of civic monitoring to almost zero. Meanwhile, e-procurement transparency in Ukraine measurably lowered final contract prices. An effective European model is based on four principles: the openness of data by default; the protection of whistleblowers; the institutionalisation of control outcomes; and the secure design of control platforms. The *conclusions* substantiate a system of legislative measures for Ukraine, including a framework law on public control, harmonisation with Directives (EU) 2019/1024 and 2019/1937, classification of participation platforms as critical information infrastructure, and legal regulation of algorithmic risk indicators, framed as public investments with high expected returns during post-war recovery.

Keywords: open data, e-procurement, transparency, whistleblower protection, e-participation, agency costs, good governance, post-war reconstruction, critical information infrastructure.

JEL Classification: D73, D82, H57, H83, K23, K42, O33, O52

1. Introduction

Corruption remains one of the most costly institutional defects of modern economies. According to econometric estimates produced by RAND Europe for the European Parliament, the European Union loses between 179 billion EUR and 990 billion EUR of GDP every year due to the direct and indirect consequences of corrupt practices, ranging from inflated public procurement prices to investment decisions being deterred by institutional risk

(Hafner et al., 2016). At the same time, a new class of instruments has emerged over the past decade that can be used to counter these losses. Digital platforms, open data and electronic registers have transformed public control over public authorities, turning it from a declarative democratic institution into an economically measurable mechanism for reducing corruption rents. International comparative studies have found a consistent correlation between the extent to which citizens interact digitally with the state and

Received on: June 23, 2026 **Accepted on:** August 21, 2026 **Published on:** September 28, 2026

¹ Taras Shevchenko National University of Kyiv, Ukraine
E-mail: v.v.savitska@knu.ua
ORCID: <https://orcid.org/0000-0002-1403-125X>



This is an Open Access article, distributed under the terms of the Creative Commons Attribution CC BY 4.0

corruption indicators, while OECD analytical work has identified the transparency of public data as a key indicator of public integrity (OECD, 2024).

The relevance of the problem in Ukraine is determined by the convergence of three circumstances. Firstly, Ukraine has developed one of the most open public data ecosystems in Europe. Its anti-corruption and economic effects, particularly those of the Prozorro electronic procurement system, have attracted international empirical research. Secondly, Ukraine's candidate status for EU membership means it must align its national open data, whistleblower protection and digital administrative services regimes with the Union's *acquis*. Thirdly, the cost of post-war reconstruction is measured in hundreds of billions of dollars. This makes the trust that international donors have in Ukrainian accountability mechanisms a direct determinant of the volume and cost of capital available to the state. Every percentage point of reduced corruption risk translates into a lower risk premium and a larger flow of recovery financing.

The **purpose of this article** is to analyse the economic and administrative-legal nature of public oversight of state authorities, carried out with the aid of digital technologies, and to assess, on the basis of European experience and empirical data, its impact on reducing corruption-related losses to the economy, and to formulate proposals for improving Ukrainian legislation aimed at maximising the economic return from the national digital transparency infrastructure, taking into account the challenges of post-war reconstruction.

To achieve this purpose, several interrelated tasks must be completed: providing a doctrinal substantiation of the concept of digital public control and its dual legal and economic nature; establishing the causal link between the openness of public data and the reduction of corruption losses on the basis of verified empirical studies; systematising the legal models of digital control in the EU and its Member States; identifying the gaps in Ukrainian legislation that reduce the economic efficiency of existing platforms; developing a system of legislative changes with an expected economic effect.

Research methods. The study relies on general scientific and special cognitive methods. The dialectical method, as well as the methods of analysis and synthesis, are employed to reveal the interconnections between the transparency of public data, the behaviour of corrupt agents, and the structure of losses to the national economy. Statistical methods are employed to evaluate the extent of corruption-related losses in the EU and Ukraine, as well as the economic impact of electronic procurement, based on international analytical reports. The method of economic and legal modelling facilitates the description of digital public control through the categories of agency and transaction costs, thereby substantiating the investment

nature of expenditure on transparency infrastructure. The comparative legal method is employed to juxtapose the approaches of the EU *acquis*, the legislation of the Member States and Ukrainian legislation in the fields of open data, whistleblower protection and digital citizen participation. This enables the formulation of specific proposals for improving Ukrainian legislation.

The study's logic is subordinate to its purpose. Firstly, the article defines the concept and economic-legal nature of digital public control. Secondly, it substantiates its link with reducing corruption losses to the economy using empirical material. Thirdly, it analyses the European experience of providing legal support for the relevant instruments. Fourthly, it assesses the state of, and gaps in, Ukrainian legislation. Finally, on this basis, it formulates a system of proposals for Ukraine.

Theoretical basis of the study. The problem under consideration lies at the intersection of several research traditions. Cross-national econometric studies have examined the economic dimension of the relationship between e-government and corruption, identifying a statistically significant anti-corruption effect of public sector digitalisation, dependent on internet penetration and institutional quality (Elbahnasawy, 2014; Nam, 2018; Sadik-Zada et al., 2024). Adam and Fazekas (2021) carried out a systematic review of the evidence on the impact of technologies on anti-corruption efforts, demonstrating that solutions which expand the possibilities of external monitoring have the strongest effects. Meanwhile, the methodology for objectively measuring corruption risks based on open procurement data was developed by Fazekas and Kocsis (2020), and the potential of machine learning in predicting corruption was explored by Lima and Delen (2020). The legal aspects of the problem are represented by analyses of the EU Whistleblower Directive (Abazi, 2020) and studies of the institutionalisation of e-participation in European states (Randma-Liiv & Lember, 2022). Other relevant works include those on the role of open government in creating a culture of transparency (Attard et al., 2015; Bertot et al., 2010). The author's previous works (Zaiarnyi & Katerynych, 2025; Zaiarnyi, 2025; Pleskach et al., 2020) have addressed the Ukrainian context of the digital transformation of public administration, particularly with regard to the risks of fragmented legal regulation, cybersecurity of digital platforms, and respect for the information rights of individuals. Concurrently, a comprehensive study of digital public control as an economic-legal mechanism for reducing corruption losses, with an assessment of its investment return and the development of proposals for Ukrainian legislation under the conditions of post-war reconstruction, is still absent from the scholarly literature. This determines the novelty of the present work.

2. Public Control under Digital Transformation: Concept and Economic-Legal Nature

In the doctrine of administrative law, public control has traditionally been understood as the activity of civil society institutions in observing, verifying and evaluating the decisions and actions of public authorities for their conformity with the law and the public interest. While this approach was legally sound, it omitted the economic dimension of the institution, namely the capacity of civic scrutiny to influence the cost structure of the public sector, the price of administrative procedures and the volume of corruption rents extracted from the national economy.

The digital transformation of public administration has altered the technology used to exercise public control. While public access to information about the activities of the authorities used to be mediated by requests, hearings or participation in advisory bodies, machine-readable open data, electronic registers and real-time transactional traces of public finances now serve as the primary source of control activity. In scholarly literature, this shift is described as a transition from 'transparency upon request' to 'transparency by default', whereby the disclosure of data becomes an inherent property of public administration information systems (Attard et al., 2015; Bertot et al., 2010).

For the purposes of this study, digital public control is defined as the activity of citizens and civil society institutions based on administrative law norms. This activity involves monitoring, analysing and publicly evaluating the decisions, actions or omissions of public authorities using open data, electronic registers, digital platforms and analytical tools. The aim is to prevent, detect and terminate violations of the public interest, particularly corrupt practices.

The proposed definition enables the dual administrative and legal, as well as economic, nature of the institution under study to be distinguished. From an administrative law perspective, digital public control constitutes a means of citizen participation in public administration, realised through a set of public rights, such as the right of access to public information, the right to submit appeals and petitions, and the right to participate in consultations with public authorities. From an economic perspective, the institution functions as a mechanism for reducing the information asymmetry between the principal (society) and the agent (the public administration). It is precisely information asymmetry that is identified by modern institutional economics as the key precondition of corrupt behaviour. An official who is in a position of authority will monetise the advantage of access to information on the distribution of public resources, while society will bear the costs in the form of inflated procurement prices, inefficient

investments and foregone tax revenues (Elbahnasawy, 2014).

A systematisation of the digital instruments of public control applied in the EU Member States and Ukraine allows five main groups to be distinguished: (1) monitoring of open data sets on public finances, property and decisions of public authorities; (2) civic analysis of electronic public procurement systems; (3) electronic petitions, consultations and other channels of digital expression of will; (4) digital services for verifying the declarations of public officials and other anti-corruption registers; and (5) protected electronic channels for reporting violations (whistleblowing). Although each of these instruments has its own legal regime, they are all united by a common economic function: raising the expected costs of corrupt behaviour by increasing the probability of detection.

From an economic standpoint, the described mechanism is most accurately explained by the category of agency costs. In the relationship between society and public administration, the costs of monitoring the agent were traditionally borne by the principal. It was precisely the magnitude of these costs under paper-based governance technologies that made systematic control economically inaccessible to ordinary citizens, leaving it the prerogative of specialised state bodies with the necessary budgetary resources. Digitalisation radically alters the structure of these costs: one-off public investments in opening data and creating control platforms minimise the marginal cost of each subsequent instance of civic monitoring. In other words, digital public control has the characteristics of a public good with economies of scale: the more people who use open data, the greater the likelihood of identifying violations, with no additional state expenditure on maintaining the transparency infrastructure.

3. Corruption Losses of the Economy and Their Link with the Effectiveness of Digital Control

The scale of economic losses caused by corruption means that the problem in question has not only legal significance, but also macroeconomic significance. According to an econometric study carried out by RAND Europe for the European Parliament, the European Union's total annual losses from corruption are estimated to be between 179 billion EUR and 990 billion EUR in GDP terms, depending on the measure of corruption applied. This estimate covers not only direct losses to public finances, but also the indirect effects of corruption, such as deterred investment, distorted competition, and foregone tax revenues (Hafner et al., 2016). Notably, the same study also quantified the anti-corruption potential of digitalisation. The introduction of a comprehensive pan-European electronic procurement system could reduce corruption costs in public procurement by

around 920 million EUR per year – almost one-fifth of the current level.

Public perception has been shown to confirm the systemic character of the problem. According to a special Eurobarometer survey, approximately seven out of ten EU citizens consider corruption to be a widespread phenomenon in their country (European Commission, 2023). The problem is even more acute for Ukraine: although the country has made noticeable progress in the Transparency International Corruption Perceptions Index over the past decade, its score remains substantially below the EU average. The need for hundreds of billions of dollars of international assistance and public investment for post-war reconstruction means that controlling public finances has become a matter of national economic security (Transparency International, 2026).

Table 1 summarises the updated consolidated empirical estimates characterising the economic scale of corruption and the measurable effects of digital control instruments in the EU and Ukraine, based on data from 2025–2026.

The current literature substantiates the causal link between digital instruments of public control and the reduction of corruption losses through the rational choice model of the corrupt agent. The decision of an official to commit a corruption offence is determined by the ratio of the expected benefits to the expected costs; the latter is the product of the probability of detection and the severity of the

sanction. Digital transparency has a direct impact on the first multiplier. When data on procurement, expenditure, assets and officials' decisions is open, machine-readable and available for automated analysis by anyone, the probability of detecting anomalies increases significantly without a proportional increase in the budget for the state control apparatus. In this sense, anti-corruption oversight based on open data is the most cost-effective form of public control: the state effectively utilises the free analytical resources of society, such as investigative journalists, non-governmental organisations and competitors in the public procurement market (Kossow & Kukutschka, 2017).

Empirical studies generally confirm this theoretical mechanism, though with important reservations. A review of the evidence on the impact of emerging technologies on anti-corruption efforts shows that digital solutions that expand the possibilities of external monitoring, including civic monitoring, have the most robust effects, whereas purely internal administrative automation yields much weaker results (Adam & Fazekas, 2021). Cross-national econometric studies have found a statistically significant negative correlation between e-government development and corruption levels. This effect is stronger in countries with higher internet penetration, where digital channels of control are used by a large proportion of the population (Elbahnasawy, 2014; Nam, 2018; Sadik-Zada et al., 2024). At the same time, however, researchers emphasise

Table 1

Empirical Estimates of the Economic Dimension of Corruption and the Effects of Digital Control Instruments: the EU and Ukraine (2025–2026)

Indicator	Value	Source
Annual GDP losses of the EU from corruption (baseline econometric estimate)	179–990 billion EUR	Hafner et al., 2016
Damage to the EU and national budgets under EPPO investigation (end of 2025)	67.27 billion EUR in 3,602 active cases (against 24.8 billion EUR in 2024); freezing orders of 1.13 billion EUR; conviction rate close to 95%	EPPO, 2026
Share of EU citizens who consider corruption widespread in their country	71% in 2026 (69% in 2025)	European Commission, 2026
Corruption Perceptions Index 2025: Ukraine / global average / Western Europe and EU average	36 points (104th of 182) / 42 points / 64 points	Transparency International, 2026
Open data maturity (ODM 2025): Ukraine / EU-27 average	4th place among 36 countries, 97% / about 85%	data.europa.eu, 2025
EU open data market	184.45 billion EUR in 2019, with a forecast of 199.5–334.2 billion EUR in 2025	Huyer & van Knippenberg, 2020
Economic effects of the Prozorro system	Reduction of final contract prices by 3.5–5.8%; 2.38 bidders per tender in 2024, above the EU average; Prozorro Market: volume of about 100 billion UAH and savings of about 9 billion UAH in 2025	Kovalchuk et al., 2019; EBRD, 2025; Cabinet of Ministers of Ukraine, 2025
Harmonised EU criminal law response	Fines for legal persons of up to 4% of global turnover, mandatory national anti-corruption strategies, annual publication of corruption data	Directive (EU) 2026/1021

Source: compiled by the author on the basis of the sources indicated in the table

that technology alone cannot eliminate corruption in systems with flawed institutions. While digital platforms can reduce petty administrative corruption, large-scale corruption schemes tend to migrate to areas not covered by transparency (Lewis-Faupel et al., 2016).

The Ukrainian experience is one of the most frequently cited examples in this discussion. The public procurement reform, which was based on the Prozorro system and which made electronic auctions and full disclosure of data under the Open Contracting standard mandatory for all public procurement as of August 2016, was accompanied by measurable economic effects. According to the estimates of the Center for Global Development, final contract prices in the post-reform period turned out to be 3.5–5.8% lower relative to the expected value compared with the pre-reform period, while the duration of procurement procedures shortened by five to six days on average (Kovalchuk et al., 2019). From the outset, the architecture of Prozorro was designed with public control in mind: the open analytics module and civic monitoring tools, such as the Dozorro portal, transformed every internet user into a potential controller. It is this feature, rather than the mere electronic processing of procedures, that sets the Ukrainian model apart from similar systems. The estimated savings accumulated over the years of the system's operation, totalling over 100 billion UAH according to domestic and foreign literature, provide a basis for considering expenditure on creating and maintaining digital control platforms as a form of public investment with one of the highest rates of return among all areas of administrative reform.

Figure 1 presents the causal mechanism linking the scale of corruption losses, the digital infrastructure of public control, and the measurable economic effects of this infrastructure.

Thus, the link between digital public control and the reduction of corruption-related economic losses is not merely declarative, but can be measured empirically. This enables the initial thesis to be formulated for further analysis: the quality of administrative and legal support for digital control instruments, such as the completeness of the open data regime, access to information guarantees, whistleblower protection and legal certainty regarding the consequences of civic evaluation, is an economic as well as a legal variable on which the volume of corruption in the national economy directly depends.

4. European Experience of Legal Support for Public Control by Digital Means

Legal support for digital public control in the European Union is provided at three interconnected levels: the EU acquis, national legislation in the Member States and institutional guarantees for the operation of relevant platforms.

At EU level, the framework of the mechanism under study comprises three acts. Directive (EU) 2019/1024 on open data and the re-use of public sector information established the principles of openness by design and by default. It also introduced the concept of high-value datasets, which are to be published free of charge in a machine-readable format

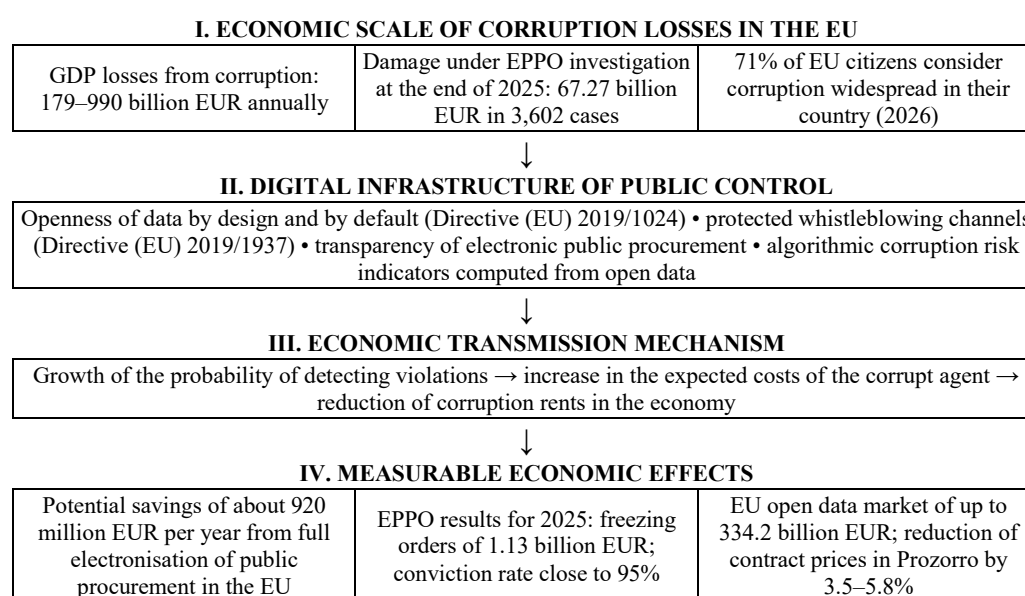


Figure 1. The economic mechanism of digital public control in the EU: from corruption losses to measurable effects

Source: compiled by the author based on (Hafner et al., 2016; EPPO, 2026; European Commission, 2026; Huyer & van Knippenberg, 2020; Kovalchuk et al., 2019)

via application programming interfaces. These datasets include information on companies, their owners, and public expenditure specifically, which constitutes the raw material for anti-corruption civic monitoring (Directive (EU) 2019/1024). The economic rationale underpinning this act is articulated in its preamble, which asserts that open data is regarded as both a resource for the digital economy and an instrument of accountability for public administration.

The economic scale of the EU's open data policy is confirmed by official estimates. According to calculations performed for the European Commission within the European Data Portal, the EU's open data market was worth 184.45 billion EUR in 2019. It is forecast to grow to between 199.5 and 334.2 billion EUR by 2025. The measurable effects cover not only business revenues from data reuse, but also public sector cost savings and efficiency gains for society (Huyer & van Knippenberg, 2020). This dual return – the commercial value of data for the digital economy and its control value for holding authorities accountable – explains why open data has become central to the European model. Member states finance transparency infrastructure not as an expense of democratic procedure, but as an investment that pays off simultaneously through the tax base of new, data-driven businesses, and through reduced corruption and losses to public finances.

The second element is Directive (EU) 2019/1937, which provides protection for individuals reporting breaches of EU law. This directive obliged Member States to establish secure channels for internal and external reporting of breaches, prohibited retaliation against whistleblowers, and shifted the burden of proof for establishing the absence of a link between the report and any adverse measures against the employee onto the employer. In the doctrine, this directive is rightly assessed as a paradigm shift. Whistleblowing is transformed from a risky individual initiative into an institutionalised element of the public control system, and protected electronic reporting channels become the most cost-effective way of detecting concealed corrupt practices that are inaccessible to open data analysis (Abazi, 2020). The third element is Regulation (EU) 2018/1724, which establishes a single digital gateway. This guarantees cross-border online access to administrative procedures and information, unifying the digital environment of citizen-administration interaction across the entire internal market (Regulation (EU) 2018/1724).

At the national level, the most illustrative example is the Estonian model, in which transparency is embedded in the very architecture of state information systems. The X-Road data exchange platform is predicated on the principle of logging every access to personal data, thereby enabling the citizen to monitor independently which authority accessed information about them, when and for what purpose. Researchers studying the

Estonian digital transformation emphasise that the controllability of those in control became the key factor in gaining public trust. Without this, the widespread use of digital services, and therefore digital channels for participation and control, would have been impossible (Kattel & Mergel, 2019). The Estonian experience demonstrates an economically significant regularity: investments in the transparency of infrastructure are converted into a reduction of the transaction costs of the entire system of public administration, since trust reduces the need for duplicative checks and paper-based document flows.

The broader Baltic and Eastern European regional context merits discrete consideration. Over the past decade, Lithuania and Latvia have deliberately developed open data portals and electronic registers of public procurement participants, combining them with analytical risk detection tools. Comparative studies of e-participation in Europe show that the success of such initiatives is more dependent on institutionalisation – the existence of a legal obligation for authorities to respond to the results of civic monitoring – than on the technological component, and on the integration of digital participation channels into real administrative procedures (Randma-Liiv & Lember, 2022). The typical reason why e-participation platforms in some states remain showcase solutions without a measurable impact on the quality of governance is precisely the deficit of institutionalisation, rather than of technology.

Table 2 provides a comparative overview of the legal models of digital public control and the related integral indicators in the selected EU Member States and Ukraine.

Another aspect of the European experience is the use of big data analytics to objectively measure corruption risks. Risk indicators developed from European electronic procurement systems, such as single-bidder tenders, abnormally short submission periods and recurrent links between buyers and winners, make it possible to quantitatively assess the probability of collusion and favouritism at the level of individual contracts and administrative units (Fazekas & Kocsis, 2020). Such indicators are fundamentally computed from open data, making them available not only to state auditors, but also to civic analytical centres. In combination with machine learning tools, this provides the technological basis for predictive public control, which can identify risks before a corrupt transaction is completed (Lima & Delen, 2020). At the same time, the automation of control analytics gives rise to its own legal questions, ranging from data quality to the basis for the legal implications of algorithmically generated suspicions. These questions require regulatory safeguards to prevent excessive discretion on the part of both developers and users of such systems (Kuziemski & Misuraca, 2020).

Table 2

**Comparative Characteristics of Legal Models of Digital Public Control and Integral Indicators:
Selected EU Member States and Ukraine**

Country	Key digital instruments of public control	Harmonisation with the EU acquis (Directives (EU) 2019/1024, 2019/1937)	Institutionalisation of control outcomes	CPI 2025, score (rank of 182)	EGDI 2024, rank of 193
Denmark	Open state registers; digital reporting channels	Full	High	89 (1st)	1
Estonia	X-Road platform with logging of every access to data; national open data portal	Full	High (embedded in system architecture)	76 (12th)	2
Lithuania	National open data portal; risk analytics of public procurement	Full	Medium to high	65 (28th)	21
Latvia	National open data portal; electronic registers of procurement participants	Full	Medium	60 (37th)	29
Ukraine	Prozorro/Dozorro; spending.gov.ua; register of asset declarations; DREAM ecosystem	Partial (candidate status)	Fragmentary (no framework law on public control)	36 (104th)	30

Source: compiled by the author based on (Transparency International, 2026; United Nations, 2024; Kattel & Mergel, 2019; Randma-Liiv & Lember, 2022)

Note: in the Online Service Index component of the EGDI 2024, Ukraine ranks 5th among 193 states (United Nations, 2024), which sharpens the contrast between the technological maturity of its control platforms and its integral integrity indicators.

Generalising the European experience leads to the conclusion that an effective model of legal support for digital public control rests on four elements: normatively enshrined openness of data by default; legal guarantees protecting individuals who report violations; institutionalised consequences of public control, such as the obligation of authorities to respond; and the security of the digital control infrastructure itself. The absence of any one of these elements reduces the economic return of the others, since corrupt practices will naturally migrate to the least transparent part of the system.

5. Administrative-Legal Support of Digital Public Control in Ukraine: Achievements and Gaps

The Ukrainian model of digital public control emerged in specific circumstances: the 2014–2016 reforms were implemented under the direct influence of civil society, resulting in a level of transparency regarding fundamental state data that is unique in the region. The normative foundation of this model is formed by the Law of Ukraine “On Access to Public Information”, which introduced the category of public information in the form of open data; the Law of Ukraine “On Transparency in the Use of Public Funds”, in pursuance of which the spending.gov.ua portal operates; the Law of Ukraine “On Public Procurement” which institutionalised the Prozorro system; and the Law of Ukraine “On Prevention of Corruption” in the part concerning the Unified State Register of Declarations, open for free round-the-clock access. Resolution of the Cabinet of Ministers of Ukraine No. 835 defined more than a thousand data

sets subject to mandatory publication in machine-readable format, which by formal criteria brought the Ukrainian open data regime close to the requirements of Directive (EU) 2019/1024 even before Ukraine obtained the status of a candidate for EU membership.

The economic results of this model, examined in the third section, suggest that it is generally successful. Another argument in its favour is the launch of the DREAM (Digital Restoration Ecosystem for Accountable Management) ecosystem in 2023, a digital environment for managing reconstruction projects which accumulates data on all stages of recovery project life cycles. The aim is to ensure transparency in the use of international assistance. The emergence of DREAM demonstrates the state’s recognition of the direct link between transparency and the cost of reconstruction capital. For international donors, digital verification of accountability is a financing condition, so reducing corruption risk by even a small amount increases the recovery resources available to Ukraine.

At the same time, a systematic analysis of the current legislation reveals several gaps that reduce the infrastructure’s economic return.

Firstly, Ukraine lacks a framework law on public control. The norms that define its forms and consequences are scattered across dozens of legal instruments of varying strength. Its typical instruments, such as civic expert reviews, public councils and electronic consultations, are predominantly regulated by subordinate legislation that does not oblige the authorities to respond substantively to the results of control measures. Consequently, the most expensive element of the control cycle – the public’s analytical work – often does not result in administrative decisions. From an economic standpoint, this means that the social

investments already made in monitoring are depreciated. This defect is a manifestation of the broader problem of fragmented legal support for digital transformation in Ukraine. As demonstrated in the context of smart city governance, the absence of a coherent legislative framework can lead to uncoordinated digital deployments, dependence on individual technology suppliers ('vendor lock-in'), and blurred responsibility between levels of public administration (Zaiarnyi & Katerynych, 2025). These risks also apply to public control platforms, which are currently being developed without a unified legal strategy.

Secondly, Ukrainian legislation only partially implements the standards set out in Directive (EU) 2019/1937 regarding whistleblowing. Although the institution of the whistleblower has been introduced into the Law of Ukraine "On Prevention of Corruption", and the Unified Whistleblower Reporting Portal has been created, the scope of protection is predominantly limited to corruption offences. In contrast, the European model covers a broad spectrum of violations of the public interest, which restricts the flow of socially significant information and weakens the preventive effect of the institution.

Thirdly, there is a separate group of problems concerning the cybersecurity of the digital control infrastructure itself. In the event of full-scale war, platforms such as those for open data, electronic petitions and procurement are subject to systematic cyberattacks. Compromising such a platform incurs a dual cost: not only is there direct damage, but public trust in digital participation channels is also destroyed, and it takes years to restore it. The author has previously substantiated the measurement of the economic consequences of digital threats through the prism of respect for the digital rights of the person. Furthermore, the principles of security by design and data protection by default should be normatively enshrined as mandatory for critical information systems (Zaiarnyi, 2025). Applying this approach to public control platforms means their legal regime should include mandatory requirements for architectural security, auditing, and cyber incident response plans. This is because trust in the integrity of data is a prerequisite for the results of civic monitoring to have evidentiary value. Another aspect of this problem concerns respect for individuals' information rights: control platforms process large amounts of personal data relating to officials and procurement participants. Therefore, their operations must strike a balance between transparency and privacy guarantees. This concept has been developed in the context of smart city digital services, where respect for individuals' information rights is recognised as a condition of residents' cybersecurity (Pleskach et al., 2020).

Fourthly, martial law has led to restrictions on access to certain public registers and datasets for security

reasons. While recognising the legitimacy of such restrictions, it must be noted that the legislation lacks clear criteria for their proportionality and duration. Decisions to restrict access to data are made at the discretion of those in power, with no obligation to periodically review them. This creates the risk of normalising opacity during the post-war period, precisely when the scale of public expenditure on reconstruction will require maximum accountability.

6. Proposals for Ukraine

The analysis carried out enables a system of measures to be formulated for improving the administrative and legal support for digital public control. Each measure is expected to have an economic effect.

The first measure should be the adoption of the Law of Ukraine "On Public Control", which should contain a separate chapter on digital forms of control. This law should provide an exhaustive list of control subjects and instruments, and the legal consequences of their outcomes. This should include the obligation of public authorities to respond to the conclusions of civic expert reviews within a fixed timeframe, and the grounds for initiating a state audit based on civic monitoring. It should also include guarantees of access to open data for those subject to control. The institutionalisation of the consequences of control will eliminate the main cause of the depreciation of civic analytical efforts. Judging by the European experience, this is the most effective way of converting transparency into a measurable reduction in corruption-related losses.

The second area of focus is the completion of the harmonisation of the open data regime with Directive (EU) 2019/1024. This involves the legislative enshrinement of the principle of openness by design and by default for all newly created state information systems (including DREAM), the definition of a list of high-value datasets, and the introduction of judicial and administrative mechanisms for challenging unjustified refusals to publish. At the same time, clear criteria should be established for wartime restrictions on access to data. These criteria should include exceptionality, proportionality to the threat, mandatory periodic review and automatic restoration of access after martial law is terminated or cancelled.

The third measure is to extend the scope of whistleblower protection in line with Directive (EU) 2019/1937. This will provide coverage for reports of violations of public interest relating to public finance, the environment, product safety, and public procurement, as well as corruption offences. At the same time, the security requirements for digital reporting channels will be strengthened.

The fourth area of focus is the normative enshrinement of secure design requirements for digital participation and control platforms. This involves

introducing a norm into the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" that makes the principles of security by design and privacy by default mandatory for information systems through which citizens exercise their right to participate in governance. This also involves classifying such systems as critical information infrastructure objects and introducing a mandatory independent security audit.

The author's fifth proposal is for the legislative regulation of the use of analytical algorithms and artificial intelligence technologies in civic and state anti-corruption monitoring. This would entail defining the legal status of automatically generated risk indicators as grounds for verification, but not for legal liability; setting requirements for the quality and transparency of training data; and ensuring individuals have the right to an explanation of an algorithmic assessment. This approach would enable predictive control to be scaled up without violating due process guarantees.

The implementation of the proposed measures should be regarded as an investment with a high expected return, rather than a costly regulatory initiative. Even under a conservative estimate, whereby improvements to digital control reduce corruption losses by only a few percentage points from their current level, the economic effect will far exceed the expenditure on building the corresponding legal and technological infrastructure. In the post-war period, it will also directly affect the volume and cost of Ukraine's reconstruction financing from abroad.

7. Conclusions

The study of the economic and administrative-legal nature of public control over public authorities exercised by means of digital technologies allows the following main conclusions and proposals to be formulated.

1. Digital public control is proposed to be understood as the activity of citizens and civil society institutions, based on the norms of administrative law, in monitoring, analysing and publicly evaluating the decisions, actions or omissions of subjects of public authority. This is carried out with the use of open data, electronic registers and digital platforms and is aimed at preventing and detecting violations of the public interest, above all corrupt practices. The dual nature of this institution has been demonstrated. Legally, it is a form of citizen participation in public administration. Economically, it is a mechanism for reducing information asymmetry between society and public administration. It possesses the properties of a public good with economies of scale: one-off public investments in open data reduce the marginal cost of every subsequent act of civic monitoring to almost nothing.

2. Based on verified empirical data, it has been confirmed that there is a measurable link between

digital transparency and reduced corruption losses to the economy. The EU's annual losses from corruption are estimated to be between 179 and 990 billion EUR of GDP, while the full electronic management of public procurement could reduce these costs by up to 20%. The Ukrainian experience of the Prozorro system, which achieved a 3.5–5.8% reduction in final contract prices and shorter procedures, confirms that investment in digital control infrastructure is one of the most cost-effective forms of administrative reform. This suggests that the quality of administrative and legal support for digital control should be regarded as an economic variable that directly affects the volume of corruption in the national economy, as well as the cost and availability of international reconstruction capital in the post-war period.

3. The broadening of the European experience has enabled the identification of four elements of an effective model of legal support for digital public control. Firstly, the normatively enshrined openness of data by design and by default (Directive (EU) 2019/1024). Secondly, legal guarantees of whistleblower safety (Directive (EU) 2019/1937). Thirdly, the institutionalisation of the consequences of control through the obligation of the authorities to respond to its results. And finally, the security of the digital control infrastructure based on the principles of secure design. It has been established that the absence of any of these elements reduces the economic return of the others. This is because corrupt practices naturally migrate to the least transparent part of the administrative system.

4. The key gaps in Ukrainian legislation that limit the economic efficiency of the created transparency infrastructure have been identified. These include the absence of a framework law on public control and legal certainty regarding the consequences of its results, incomplete implementation of European whistleblower protection standards, the absence of mandatory secure design requirements for digital participation platforms, and discretionary and open-ended wartime restrictions on access to public data. To address these issues, the following is proposed: the adoption of the Law of Ukraine "On Public Control", which includes a separate chapter on digital forms. This would enshrine the obligation of the authorities to respond in a reasoned manner to the conclusions of civic expert reviews; to complete the harmonisation of the open data regime with Directive (EU) 2019/1024, including the extension of the openness-by-default principle to the DREAM ecosystem and the establishment of criteria of proportionality and duration for wartime restrictions; to extend whistleblower protection following the model of Directive (EU) 2019/1937 to all violations of the public interest; and to classify digital participation platforms as objects of critical information infrastructure with the mandatory application of the principles of security by design and privacy by default.

5. The development of a predictive public control mechanism based on analytical algorithms and artificial intelligence technologies that compute corruption risk indicators from open data has been identified as a promising approach. It is proposed that the legal status of automatically generated risk indicators be defined by law as grounds for verification, but not for legal liability. This would be subject to data quality requirements and the right of the individual to an explanation of the algorithmic assessment. Further research should focus on quantitatively measuring the economic return of individual digital control instruments in the context of Ukraine's post-war reconstruction, as well as developing

a methodology for evaluating the impact of public data transparency on the cost of securing international financing.

AI-Assisted Language Editing Statement

The author used ChatGPT and Grammarly exclusively to edit the English version of the manuscript and refine its style. These tools were used to enhance grammar, vocabulary, clarity and readability. They were not used to generate the research idea, design the study, conduct the analysis, interpret the findings or draw scientific conclusions. The author takes full responsibility for the content, originality, accuracy and integrity of the manuscript.

References:

- Abazi, V. (2020). The European Union Whistleblower Directive: A 'game changer' for whistleblowing protection? *Industrial Law Journal*, 49(4), 640–656.
- Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, 57, 100950. <https://doi.org/10.1016/j.infoecopol.2021.100950>
- Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32(4), 399–418.
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), 264–271.
- Cabinet of Ministers of Ukraine (2025). Prozorro Market Becomes a Driver for Efficient Procurement and Ukraine's Integration into EU Standards. <https://www.kmu.gov.ua/en/news/prozorro-market-staie-draiverom-efektyvnykh-zakupivel-ta-intehratsii-ukrainy-do-standartiv-ies>
- data.europa.eu (2025). Open Data Maturity Report 2025. Luxembourg: Publications Office of the European Union. <https://data.europa.eu/en/open-data-maturity/2025>
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. <https://eur-lex.europa.eu/eli/dir/2019/1024/oj>
- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. <https://eur-lex.europa.eu/eli/dir/2019/1937/oj>
- Directive (EU) 2026/1021 of the European Parliament and of the Council of 29 April 2026 on combatting corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371. <https://eur-lex.europa.eu/eli/dir/2026/1021/oj>
- EBRD (2025). The Impact of the Prozorro Procurement System on the Ukrainian Economy. Law in Transition Journal 2025. London: European Bank for Reconstruction and Development. https://www.ebrd.com/content/dam/ebd_dxp/assets/pdfs/legal-transition/Law%20in%20Transition%20journal/LiTJ%202025/ebd-lit25-the-impact-of-the-prozorro-procurement-system-on-the-ukrainian-economy.pdf
- Elbahnasawy, N. G. (2014). E-government, internet adoption, and corruption: An empirical investigation. *World Development*, 57, 114–126.
- European Commission (2023). Special Eurobarometer 534: Citizens' attitudes towards corruption in the EU in 2023. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/anti-corruption/corruption-public-opinion_en
- European Commission (2026). Special Eurobarometer: Citizens' Attitudes towards Corruption in the EU in 2026. <https://europa.eu/eurobarometer/surveys/detail/3693>
- European Public Prosecutor's Office (2026). Annual Report 2025. Luxembourg: EPPO. <https://www.eppo.europa.eu/assets/annual-report-2025/index.html>
- Fazekas, M., & Kocsis, G. (2020). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. *British Journal of Political Science*, 50(1), 155–164.
- Hafner, M., Taylor, J., Disley, E., Thebes, S., Barberi, M., Stepanek, M., & Levi, M. (2016). The Cost of Non-Europe in the area of Organised Crime and Corruption: Annex II – Corruption. RAND Europe; European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/579319/EPRS_STU\(2016\)579319_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/579319/EPRS_STU(2016)579319_EN.pdf)

- Huyer, E., & van Knippenberg, L. (2020). The Economic Impact of Open Data: Opportunities for value creation in Europe. European Data Portal; Publications Office of the European Union. <https://data.europa.eu/sites/default/files/the-economic-impact-of-open-data.pdf>
- Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In M. E. Compton & P. 't Hart (Eds.), *Great Policy Successes* (pp. 143–160). Oxford: Oxford University Press. <https://doi.org/10.1093/oso/9780198843719.003.0008>
- Kossow, N., & Kukutschka, R. M. B. (2017). Civil society and online connectivity: Controlling corruption on the net? *Crime, Law and Social Change*, 68(4), 459–476. <https://doi.org/10.1007/s10611-017-9696-0>
- Kovalchuk, A., Kenny, C., & Snyder, M. (2019). Examining the Impact of E-Procurement in Ukraine (CGD Working Paper 511). Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/examining-impact-e-procurement-ukraine>
- Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, 44(6), 101976.
- Lewis-Faupel, S., Neggers, Y., Olken, B. A., & Pande, R. (2016). Can electronic procurement improve infrastructure provision? Evidence from public works in India and Indonesia. *American Economic Journal: Economic Policy*, 8(3), 258–283. <https://doi.org/10.1257/pol.20140258>
- Lima, M. S. M., & Delen, D. (2020). Predicting and explaining corruption across countries: A machine learning approach. *Government Information Quarterly*, 37(1), 101407.
- Nam, T. (2018). Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study. *Government Information Quarterly*, 35(2), 273–282.
- OECD (2024). Anti-Corruption and Integrity Outlook 2024. Paris: OECD Publishing.
- Pleskach, M., Zaiarnyi, O., & Pleskach, V. (2020). Respect for information rights of a person as a condition for cybersecurity of smart cities residents. *10th International Conference on Advanced Computer Information Technologies (ACIT)*, 759–764. <https://ieeexplore.ieee.org/document/9208977>
- Randma-Liiv, T., & Lember, V. (Eds.) (2022). Engaging Citizens in Policy Making: e-Participation Practices in Europe. Cheltenham: Edward Elgar Publishing.
- Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services. <https://eur-lex.europa.eu/eli/reg/2018/1724/oj>
- The Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Regulations on Data Sets Subject to Publication as Open Data” of October 21, 2015, No. 835. <https://zakon.rada.gov.ua/laws/show/835-2015-п>
- Sadik-Zada, E. R., Gatto, A., & Niftiyev, I. (2024). E-government and petty corruption in public sector service delivery. *Technology Analysis & Strategic Management*, 36(12), 3987–4003. <https://doi.org/10.1080/09537325.2022.2067037>
- The Law of Ukraine “On Access to Public Information” of August 8, 2025, No. 2939-VI. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2011, No. 32, Article 314. <https://zakon.rada.gov.ua/laws/show/2939-17>
- The Law of Ukraine “On Transparency in the Use of Public Funds” of 14.06.2025, No. 183-VIII. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2015, No. 16, Article 109. <https://zakon.rada.gov.ua/laws/show/183-19>
- The Law of Ukraine “On Prevention of Corruption” of May 30, 2026, No. 1700-VII. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2014, No. 49, Article 2056. <https://zakon.rada.gov.ua/laws/show/1700-18>
- The Law of Ukraine “On Public Procurement” of August 24, 2026, No. 922-VIII. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2016, No. 9, Art. 89. <https://zakon.rada.gov.ua/laws/show/922-19>
- The Law of Ukraine “On the Basic Principles of Cybersecurity in Ukraine” of October 19, 2025, No. 2163-VIII. The Official Bulletin of the Verkhovna Rada (BVR), 2017, No. 45, Article 403. <https://zakon.rada.gov.ua/laws/show/2163-19>
- Transparency International (2026). Corruption Perceptions Index 2025. <https://www.transparency.org/en/cpi/2025>
- United Nations (2024). United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: UN Department of Economic and Social Affairs. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024>
- Zaiarnyi, O. (2025). Cyber risk management in the business strategies of healthcare institutions and compliance with digital patients' rights: EU experience and proposals for Ukraine in wartime. *Baltic Journal of Economic Studies*, 11(1), 95–103. <https://doi.org/10.30525/2256-0742/2025-11-1-95-103>
- Zaiarnyi, O., & Katerynych, P. (2025). Governing smart city development in post-war Ukraine. *Transylvanian Review of Administrative Sciences*, Special Issue 2025, 186–205. <https://doi.org/10.24193/tras.SI2025.10>