Journal of Theoretical and Applied Information Technology
15th March 2026. Vol.104. No.5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

USE OF DIGITAL PUBLIC GOVERNANCE TOOLS IN A STATE OF EMERGENCY TAKING INTO ACCOUNT ADMINISTRATIVE AND LEGAL RESTRICTIONS

IRYNA MURAVIOVA[1*], OLEKSANDR YERMAK[2], VIKTORIIA KORETSKA[3], VALERIIA RIADINSKA[4], NADIIA VASYLENKO[5]

[1]Interregional Academy of Personnel Management, Kyiv, Ukraine.
[2]Department of Public Administration and Law, Educational and Research Institute of Finance, Economy, Management and Law, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine.
[3]Department of Law, Lutsk National Technical University, Lutsk, Ukraine.
[4]Department of Public and Private Law, Private Joint Stock Company "Higher Educational Institution "National Academy of Management", Kyiv, Ukraine.
[5]Department of Management and Administration, PHEE "Vinnytsia Academy of Continuing Education", Vinnytsia, Ukraine.

E-mail: [1]maup.com.ua, [2]ermakoleksandr89@gmail.com, [3]Koreckaviktoria@gmail.com, [4]corbazol@ukr.net, [5]nadezhdavasilenko2016@gmail.com

ABSTRACT

The article presents the results of a comparative study of the use of digital public governance tools in a state of emergency using the example of Ukraine, Germany, and Estonia. The aim is to assess the administrative and legal balance of digital governance using the integrated Administrative and Legal Balance Index (ALBI), which covers efficiency (Eff), transparency (Transp), legal compliance (LegComp), and human rights protection (HRProt). The methodology combines comparative law, statistical and modelling approaches using k-means clustering, PCA visualization, bootstrap estimation (n = 1000), and scenario modelling of three management situations (interdepartmental coordination, electronic identification, citizens' appeals). The ALBI weights were determined based on the results of a three-round Delphi survey and AHP-consensus of 27 experts from three countries. The research is based on the analysis of regulatory acts (Onlinezugangsgesetz, Public Information Act, Government Regulation No. 105; the laws of Ukraine "On the Legal Regime of Martial Law", "On Electronic Trust Services") and the aggregated indicators DESI, EGDI, and Rule of Law Index. It was found that Germany has the highest level of balance (ALBI = 0.86) due to the combination of technological maturity with effective judicial control. Estonia demonstrates maximum efficiency (Eff = 0.88) and regulatory stability due to X-Road and the data once only principle. Ukraine is characterized by high rates of digitalization (Eff = 0.78) with lower values of transparency (Transp = 0.61) and human rights protection (HRProt = 0.59). It was established that the balance of digital governance critically depends on harmonization with Regulation (EU) 2024/1183 (eIDAS 2.0), Recommendation CM/Rec(2018)7 of the Council of Europe, and the OECD Digital Government Framework. The academic novelty is the developed lawful-by-design model that integrates digital solutions with administrative and legal procedures at the design stage. Further research prospects for are related to the creation of adaptive crisis management systems capable of automatically maintaining a balance between speed, legality, and protection of citizens' rights in emergency legal regimes.

Keywords: *Digital Public Governance, E-Governance, Administrative Law, Rule Of Law, Human Rights, Sustainable Institutions*

1. INTRODUCTION

Active digitalization of public administration is fundamentally changing the decision-making processes, interagency interaction, and the exercise of administrative powers in times of crisis. In a state of emergency, the government must act quickly, but in accordance with the law, so the administrative and legal balance becomes key: efficiency without legality generates abuse, and excessive regulation

paralyses management decisions [1, 2]. In European practice, the effectiveness of legal support for digital governance in crises varies. In Ukraine, large-scale digital modernization has been taking place since 2022 – from the Diia system to analytical security platforms, but the regulatory framework remains fragmented and does not always guarantee proper control over personal data and administrative liability [3, 4]. In Germany, the Digital Governance Act (Onlinezugangsgesetz, OZG) combines a centralized infrastructure with clear legal guarantees and judicial control over the use of emergency powers [5, 6]. Estonia has implemented the once-only principle enshrined in the Public Information Act and Government Regulation No. 105, which ensures unified data exchange via X-Road and minimizes duplication of functions or risks of abuse [7, 8]. A comparison of these models demonstrates that the administrative and legal regulation of the data collection, processing, and storage that is a safeguard against abuse in a state of emergency [9, 10]. Determining the limits of discretion, grounds for restricting access to information and procedures for judicial control form the basis of the legitimacy of digital governance even in times of crisis. International practice confirms that successful digital governance in crisis regimes is possible only with a system of preventive legal safeguards. In Germany, they are provided by the Constitutional Court, which determines the proportionality of digital restrictions, in Estonia – by the principle of transparency of state registers. In Ukraine, a culture of legal accountability in the digital environment is only being formed [2, 4]. Therefore, a comparative study of how different administrative and legal systems support the effectiveness of digital governance in a state of emergency without violating the fundamental rights and freedoms of citizens remains relevant.

The aim of the study is to assess the features of the administrative and legal regulation of digital public governance tools in a state of emergency and assess the effectiveness of their application using the example of Ukraine, Germany, and Estonia.

The aim was achieved through the fulfilment of the following research objectives:

1. Analyse the effectiveness of digital public administration tools and their impact on ensuring administrative and legal balance and sustainability of public administration in a state of emergency.
2. Investigate the administrative and legal framework and limitations of the use of digital services in the management systems of Ukraine, Germany, and Estonia, identifying key factors that affect transparency, legality and protection of citizens' rights.
3. Assess models of legal control and accountability mechanisms of government bodies during digital governance in crisis regimes using ALBI, correlation analysis methods, clustering, and bootstrap estimation.
4. Provide recommendations for harmonizing Ukraine's national digital governance system with European standards of legality (*lawful-by-design*), transparency, and protection of human rights in a state of emergency.

The academic hypothesis of the study is that the integration of digital tools of public administration into the legal field of administrative law based on the principles of the rule of law, transparency, and algorithmic accountability enables increasing the efficiency of emergency management, while maintaining the legitimacy of decisions and citizens' trust in the state. Faster and broader digital services in emergencies don't guarantee equitable legislation. Fair laws are not ensured simply because they are digital. Efficiency and speed may be present in government operations yet transparency fairness and adequate rights protection can still be lacking. Testing and alteration of this idea will happen as additional understanding is gained. There is a desire to observe how digital innovations enable a government that honors fairness and rights.

So, the study is aimed at forming a holistic comparative assessment of the use of digital technologies in public administration in a state of emergency, taking into account the principles of the rule of law, legal certainty, and proportionality of administrative restrictions. This paper interprets digital public governance in a state of emergency as a stress-tested socio-technical system in which technological efficiency must be continuously reconciled with administrative legality and the protection of fundamental rights. Effectiveness during challenging situations is assessed. Technology should not only function efficiently but also adhere to regulations and safeguard rights. Different scenarios are used to examine Ukraine Germany and Estonia. Issues in digital systems can be identified after the reading. Comparing methods of operation is not something that is overlooked. Improvement of digital tools that comply with legal standards can occur especially during urgent situations. Better designs are often created by skilled developers. Digital tools should not disregard regulations even under pressure.

2. LITERATURE REVIEW

Over the past decade, digital technologies have radically transformed public administration, changing the principles of transparency, efficiency, and accountability of state power. The study by Ranchordás [11] reveals the phenomenon of the "invisible citizen" in the digital state and formulates the concept of *digital constitutionalism*, which requires a balance between innovation and the human rights protection. Almada [12] complements this paradigm with the concept of "automated uncertainty", which challenges the rule of law. Doran et al. [13], Eom and Lee [14] emphasize the managerial and institutional aspect. The former argue that the effectiveness of e-government depends on the integration of digital tools and a clear regulatory framework, the latter – that successful crisis models are based on the resilience of IT systems and the political responsibility of leaders. Kim et al. [15] developed the idea of "platform government", considering the state as a digital platform that integrates services, data, and algorithms. Newman et al. [16] examine the impact of AI on bureaucracy, emphasizing the need for re-institutionalization of administrative law. Peng [17] focuses on digital leadership as a factor that combines innovation with legal certainty. Androniceanu et al. [18] show that the anti-corruption effect of digitalization is possible only under conditions of legal oversight. This is confirmed by Sadik-Zada et al. [19], who find a decrease in petty corruption but the persistence of risks at the algorithmic level.

In the field of crisis management, Graf et al. [20] demonstrate how digital tools ensure the continuity of municipal services, while Eckhard et al. [21] introduce the concept of "latent hybridity" – the combination of formal and informal practices during crises in Germany. Lee et al. [22] use the example of China to analyse digital response mechanisms in healthcare, but emphasize mainly the technological aspect, while Ranchordás [11] and Almada [12] focus on the legal boundaries of innovation. Latupeirissa et al. [23] in a systematic review argue that the success of digitalization of public services is determined by the institutional context and the level of legal culture: digital initiatives remain declarative without a proper administrative and legal framework. Summarizing the review, three conceptual directions of research can be distinguished. The first is legal, which is presented in the studies of Ranchordás [11] and Almada [12]. it focuses on digital constitutionalism, procedural justice, and the rule of law in digital governance. The second is institutional and managerial, which is demonstrated by Doran et al. [13], Eom and Lee [14], and Graf et al. [20]. They focus on the efficiency, flexibility, and resilience of the public sector in times of crisis. The third is innovative and analytical, combining technical aspects (AI, big data, platforms) with administrative modernization [16, 24]. A modern paradigm of digital governance is being formed at the intersection of these directions. This paradigm seeks to harmonize technological dynamics with the principles of legal certainty, transparency, and accountability.

3. PROBLEM STATEMENT

Active digitalization of public governance increases the speed of state response to crises, while exacerbating the issue of the legal balance between efficiency and respect for citizens' rights. In a digital governance, digital services, electronic identification, and analytical modules based on AI ensure the efficiency of decisions [11, 22]. However, risks of automatism, opacity, and weakening of judicial control are revealed in a state of emergency [12, 14]. The lack of a holistic model that would combine the effectiveness of the response with administrative and legal standards is a key problem. Germany combines transparency with judicial supervision through the Onlinezugangsgesetz (OZG), while Ukrainian platforms, in particular Diia, are only partially integrated with the legal system [2, 5]. The Estonian data once-only model based on X-Road ensures legality and avoids duplication of functions [8]. In the academic field, the contradiction between technological pragmatism and regulatory constraints is described as "automated uncertainty" [12] or the risk of an "invisible citizen" [11]. At the same time, Graf et al. [20] argue that clearly regulated digital tools ensure the resilience of governance during crises. Therefore, the problem is the lack of a single legal and methodological model for the use of digital tools in public administration in emergency situations, which would combine the speed of response with the principles of the rule of law, proportionality, accountability, and human rights protection. Existing practices demonstrate fragmentation: there is a lack of regulatory coherence in Ukraine, stability and digital maturity in Estonia, and strict legal regulation and effective judicial control in Germany.

4. METHODOLOGY

4.1 Research design

The methodological structure of the study is based on a combination of comparative legal, analytical, empirical, and index approaches using digital

modelling of management processes in times of crisis. The study was conducted in three interconnected stages.

The first stage of the study was a regulatory and legal inventory of digital public governance mechanisms used in a state of emergency in Ukraine, Germany, and Estonia. The choice of these countries is determined by the principle of contrasting representativeness, which enables comparing different levels of digital maturity, as well as administrative and legal institutionalization within the European legal space. Ukraine represents a model of a state that is at the stage of active digital transformation under martial law. Germany is an example of a stable legal system with developed mechanisms of judicial control. In turn, Estonia is a benchmark for digital integration of state processes and legal harmonization. The selection criteria were legally established digital administrative mechanisms, the validity of the state of emergency in 2020–2025, the availability of official regulations and data from the DESI, EGDI, and Rule of Law Index, as well as compliance with European acts – Regulation (EU) 2024/1183 (eIDAS 2.0), Recommendation CM/Rec(2018)7 of the Council of Europe and the OECD Digital Government Framework.

So, the sample of the study is three national models of digital governance, within which key legal acts that determine the mechanisms for the functioning of electronic administrative processes in a state of emergency were analysed. For the regulatory and legal analysis, the basic acts that directly define the legal framework of digital governance in a state of emergency were selected: the Law of Ukraine "On the Legal Regime of Martial Law" (ed. 2024) [25], the Law of Ukraine "On Electronic Trust Services" (as amended in 2023) [26], the Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG, ed. 2022) [27], as well as the Public Information Act (Avaliku teabe seadus, updated in 2023), and Government Regulation No. 105 "Data Exchange Layer for Information Systems" (ed. 2022) of the Republic of Estonia [28, 29]. The criteria for selecting these acts were: 1) their legal validity in 2020–2024; 2) regulation of digital procedures for management or data exchange in crisis and emergency conditions; 3) provisions on legality, transparency, and protection of citizens' rights when using information systems; 4) consistency with European documents – Regulation (EU) 2024/1183 (eIDAS 2.0), Recommendation CM/Rec (2018)7 of the Council of Europe [30], OECD Digital Government Framework [31]. These acts ensure the representativeness of three models: the Ukrainian transitional system of crisis governance, the German legal model of "lawful digitalization", and the Estonian integrated architecture X-Road, which remain benchmarks of European practice in the field of administrative and legal support of digital services.

The second stage of the study was aimed at assessing existing models of digital interaction between government agencies under crisis management. Based on a comparative analysis of regulatory acts, administrative procedures and statistical indicators, three typical management situations were analytically recreated that most fully reflect the logic of the functioning of digital systems during a state of emergency: a) interdepartmental coordination of response to emergency events; b) electronic identification of citizens during the period of restriction of physical access to services; c) processing of citizens' appeals and complaints through online platforms. For each of these models, the effectiveness (Eff), transparency (Transp), legal compliance (LegComp), and citizens' rights protection (HRProt) were assessed, and key risks were identified – potential restrictions on rights, algorithmic opacity, and delays in making management decisions.

At the third stage, the effectiveness of digital tools were assessed using the integral ALBI developed by the author. The index makes it possible to quantitatively assess the balance between digital management efficiency and compliance with administrative and legal principles (legality, proportionality, accountability, personal data protection).

4.2 Evaluation metrics

The digital tools were evaluated according to four indicators that form the basis of the ALBI (Table 1).

Table 1: Metrics for evaluating the effectiveness of digital public governance tools in a state of emergency

Parameter	Designation	Calculation method	Range	Interpretation
Effectiveness of digital response	Eff	Share of administrative processes that are transferred online without loss of functionality	0–1	Effectiveness of management
Transparency of algorithmic decisions	Transp	Number of procedures that have open documentation or citizen control	0–1	Openness and accountability
Legal compliance	LegComp	Share of digital processes that comply with national and European regulations (GDPR, eIDAS, OZG, Data Exchange Act)	0–1	Legality and legitimacy
Guarantees of citizens' rights	HRProt	Number of available appeal and judicial review mechanisms	0–1	Protection of rights and justice

Source: developed by the authors based on the principles of CM/Rec(2018)7 of the Council of Europe [30], Regulation (EU) 2024/1183 (eIDAS 2.0) [32], and the OECD Digital Government Framework [31]

Table 1 presents a system of indicators for a comprehensive assessment of the effectiveness of digital public governance tools in a state of emergency. The ALBI integrates both technical and legal parameters of the functioning of digital systems. The Eff indicator reflects the level of actual digitalization of administrative processes and the speed of transition of administrative functions to the online environment without losing their functionality. Transp indicates the degree of openness of algorithmic solutions, which is critical for ensuring the accountability of authorities and preventing opaque practices of automated decision-making. The LegComp parameter assesses the compliance of digital processes with national and supranational legal norms, in particular, the requirements of GDPR, eIDAS, OZG, and the Estonian Data Exchange Layer Act, which define the standards of legality, identification, and trust. Finally, the HRProt indicator reflects the real level of legal protection of citizens through the effective appeal mechanisms, independent supervision, and judicial control over automated administrative decisions. The combined use of these four metrics provides a balanced assessment of the effectiveness, legitimacy, and social justice of digital governance in crisis settings.

The final ALBI is calculated using the formula (1):

$$ALBI = (0.3 \times Eff) + (0.25 \times Transp) + (0.25 \times LegComp) + (0.2 \times HRProt) \quad (1)$$

where the weighting coefficients were determined by experts based on a three-stage survey of 27 specialists from three countries – Ukraine, Germany, and Estonia – representing the fields of public administration, administrative law, cybersecurity and digital transformation. The survey consisted of 12 questions, of which 8 were closed (using a Likert scale from 1 to 5) and 4 were open for substantiation of the assessments. The questions concerned the assessment of the weighting of the four components of the index (Eff, Transp, LegComp, HRProt), the determination of the acceptable level of compromise between efficiency and legality, as well as the assessment of the real risks of digital restrictions of citizens' rights in a state of emergency. The responses were aggregated using the weighted average expert agreement method in order to establish the final coefficients of Formula (1). The questionnaire was developed based on the provisions of Recommendation CM/Rec(2018)7 of the Council of Europe, Regulation (EU) 2024/1183 (eIDAS 2.0), and the OECD Digital Government Framework, which define criteria for efficiency, transparency, legality, and protection of rights in digital governance.

The number of 27 experts was determined taking into account the principle of representativeness for expert assessment, which provides for a minimum of 8–10 participants per country; the selection was carried out according to the criteria of professional competence (at least 10 years of experience), publication activity in the field of digital governance, and participation in the development or implementation of regulatory and legal acts. Such a sample is considered sufficient to achieve statistical consistency of assessments and reduce expert error. The first stage of the assessment was carried out in the format of an online questionnaire survey using the Delphi method with three rounds of coordination to determine the priority of the Eff, Transp, LegComp, and HRProt criteria. The survey was conducted on the Google Forms platform, which ensured the anonymity of responses and the possibility of statistical processing of the results for further calculation of the ALBI weights. At the second stage, the results were collected and

discussed during a focus group seminar (3 experts from each country), and the final coordination of weights was carried out using an expert matrix of pairwise comparisons (Analytic Hierarchy Process – AHP). As a result, a stable system of weighting coefficients was formed, reflecting the consensus between technical efficiency, legal legitimacy and social guarantees: Eff – 0.30, Transp – 0.25, LegComp – 0.25, and HRProt – 0.20.

Unlike traditional digital governance indicators (such as DESI or EGDI), ALBI assesses not only technical efficiency, but also legal legitimacy and human rights protection. This enables creating our own metric scale for assessing the balance between "efficiency and legitimacy" in digital public governance.

4.3 Methods of analysis

Quantitative and qualitative methods were used to compare digital governance models.

At the quantitative level, a correlation analysis was conducted using Pearson coefficients (to identify linear relationships) and Spearman (to test the stability of results under non-normal data distribution) between the digital readiness level (DESI), the ALBI, and the Rule of Law indicator. K-means clustering was used to group countries by similar digital governance characteristics. At the qualitative level, legal modelling of administrative processes was carried out using the "condition-authority-restriction" logic schemes to identify critical points of risk of offences in a state of emergency.

The bootstrap simulation method (n=500) was also used to verify the reliability of the calculations, which provided the formation of confidence intervals and an assessment of the stability of ALBI for each country.

4.4 Technical environment

Calculations were performed in Python 3.12 using Pandas, NumPy, SciPy, Matplotlib, and scikit-learn libraries. The statistical data on digital readiness and public administration were processed using the EU DESI (2024), UN E-Government Development Index (EGDI), and World Justice Project (Rule of Law Index) databases. The indexes were visualized in Power BI. Legal acts of Germany, Estonia, and Ukraine were analysed through the EUR-Lex, Riigi Teataja, and Verkhovna Rada of Ukraine databases. Such methodological architecture provided a comprehensive comparison of digital administrative practices from the perspective of legality, technological efficiency, and human rights protection to identify the level of administrative and legal balance of each management model.

5. RESULTS

5.1 Comparative assessment of the effectiveness of digital public governance tools

A comparative analysis of three countries – Ukraine, Germany and Estonia – showed significant differences in the balance of digital efficiency and compliance with administrative and legal standards. According to the calculations of the ALBI, the highest values are observed in Estonia, where the combination of the once-only principle and X-Road regulatory integration ensures high legal compliance and transparency of processes. In Germany, the Onlinezugangsgesetz (OZG) model demonstrates the maximum indicators of legality and citizens' rights protection, which is due to strict administrative control, a developed system of judicial supervision and transparent channels of access to services. Ukraine, on the other hand, demonstrates the highest rates of digitalization of administration, but under conditions of partial legal unregulation and a limited mechanism for citizens' appeal, which is reflected in the lower indicators of LegComp and HRProt. The values of the metrics Eff, Transp, LegComp and HRProt are given in Table 2.

Table 2: Values of the metrics Eff, Transp, LegComp, and HRProt in three countries (Ukraine, Germany, and Estonia)

Country	Eff	Transp	LegComp	HRProt	ALBI
Ukraine	0.78	0.61	0.66	0.59	0.67
Germany	0.84	0.83	0.89	0.86	0.86
Estonia	0.88	0.80	0.85	0.78	0.83

Source: created by the authors based on their own calculations using Formula (1) and expert data from the ALBI survey (Ukraine, Germany, Estonia)

The results of Table 2 show that Estonia demonstrates the highest efficiency of digital response (Eff = 0.88), which is explained by the high level of integration of state platforms and the absence of duplication of procedures. Germany has the highest indicators of legal compliance (LegComp = 0.89) and protection of citizens' rights (HRProt = 0.86), which reflects a strong administrative and legal framework and a tradition of judicial control. Ukraine still maintains an asymmetry between digitalization and legality: the Eff indicator is high (0.78), but Transp (0.61) and HRProt (0.59) indicate

a lack of transparency of algorithmic processes and weakness of appeal mechanisms in digital governance. Figure 1 visualizes the integral distribution of ALBI.

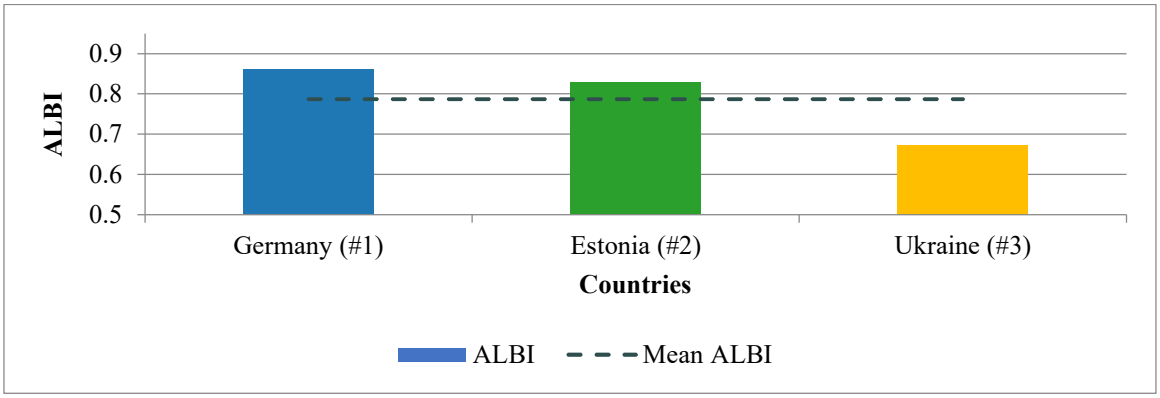

Figure 1: ALBI integral values for three digital governance models

Source: created by the authors based on their own calculations using Formula (1) and expert data from the ALBI survey (Ukraine, Germany, Estonia)

Figure 1 shows that the integral distribution of ALBI confirms that Germany maintains the highest balance between technological efficiency and legal guarantees (ALBI = 0.86), while Estonia demonstrates the optimal balance between efficiency and transparency (ALBI = 0.83). Ukraine has potential for growth, but needs regulatory strengthening of transparency and procedural control over digital administrative decisions. So, the basic comparative analysis shows: high digital efficiency does not guarantee legal balance without proper regulatory institutionalization, and the integration of elements such as judicial control, open registries and independent verification of algorithms are crucial for achieving a true balance between technological modernization and the legitimacy of governance.

5.2 Scenario analysis of digital emergency response

The scenario analysis assessed the adaptability of digital management systems to three typical emergency situations: interagency coordination, electronic identification of citizens, and processing of applications. A comparison of the ALBI values in three countries – Ukraine, Germany, and Estonia – showed that the digital maturity of the system directly affects the degree of legal balance in times of crisis. Table 3 shows the results of ALBI calculations in each of the three scenarios. Estonia obtained the highest indicators, where the interagency coordination scenario (ALBI = 0.85) provided the best combination of technological efficiency and legality thanks to the use of X-Road as a universal platform for data exchange. In Germany, the electronic identification scenario (ALBI = 0.88) revealed the highest level of legal guarantees and judicial control. Ukraine, on the other hand, demonstrates a relatively high indicator in the coordination scenario (ALBI = 0.69), but significantly lags behind in the aspects of transparency and protection of rights in the citizen appeals scenario (ALBI = 0.61).

Table 3: ALBI values in three governance scenarios (coordination, e-identification, citizen appeals)

Country	Interdepartmental coordination	Electronic identification	Citizen appeals
Ukraine	0.69	0.64	0.61
Germany	0.84	0.88	0.83
Estonia	0.85	0.82	0.80

Source: created by the authors based on their own calculations using Formula (1) and expert data from the ALBI survey

The results show that the opacity of algorithmic procedures and the lack of rapid mechanisms for appealing decisions in digital format remain the most vulnerable points for Ukraine. In Estonia, the key risk is the algorithmic opacity of artificial intelligence (AI) systems integrated into X-Road, while in Germany, the overload of legal control procedures, which can slow down the response. ALBI variations are shown in Figure 2.

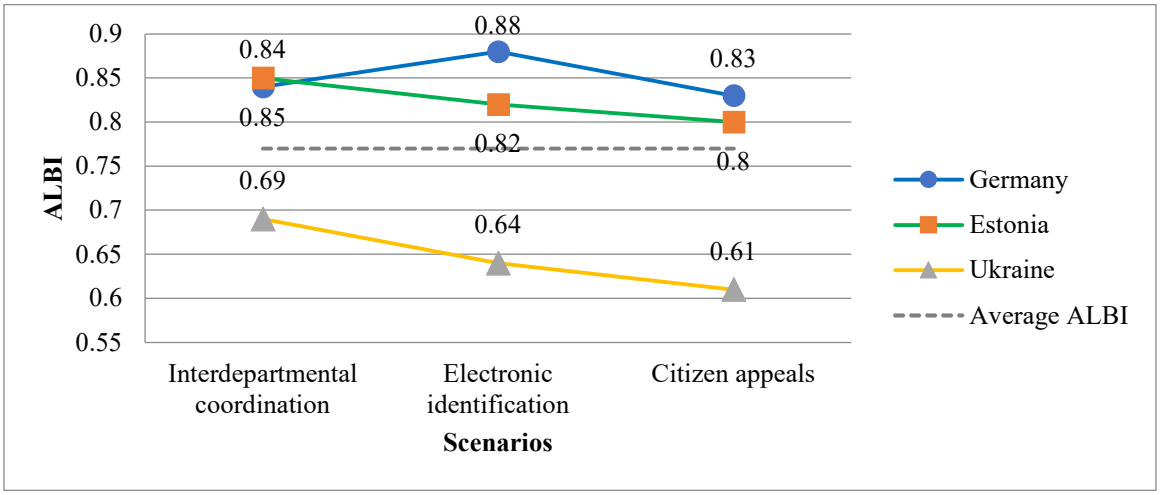

Figure 2: ALBI variations across scenarios for each country

Source: created by the authors based on their own calculations relying on the ALBI survey data (Ukraine, Germany, Estonia)

Figure 2 shows that for Germany, the ALBI curve maintains consistently high values in all scenarios, indicating a balanced administrative system even during crisis situations. Estonia is characterized by fluctuations within 0.80–0.85, with a tendency to decrease in the e-identification scenario due to the increased role of automated systems. Ukraine demonstrates the most pronounced fluctuations in the index – from 0.61 to 0.69, which confirms the lack of procedural stability and the weakness of legal control in the context of digital transformation. Scenario analysis confirms that the balance between responsiveness and legal guarantees is possible only provided comprehensive institutionalization of the principles of legality in digital governance mechanisms. The most effective is the German model, which combines high technical standards with procedural accountability, while the Estonian experience demonstrates the advantage of technological integration. Ukraine needs to strengthen the legal infrastructure of digital governance, in particular the development of administrative oversight and judicial control mechanisms in the online environment.

5.3 Correlation analysis of ALBI with digital maturity indicators

The consistency of the ALBI with international indicators was checked through a correlation analysis conducted with three external indicators – DESI, EGDI, and Rule of Law Index. Calculations based on panel data "country × scenario" (n = 9) showed a stable positive relationship between ALBI and the level of digital maturity and legal capacity of states. The highest correlation was recorded between ALBI and Rule of Law Index ($r = 0.82$; $p < 0.01$), which confirmed the sensitivity of the developed index to legal factors. Correlations with EGDI ($r = 0.76$) and DESI ($r = 0.71$) showed that technological maturity is consistent with an increase in administrative-legal balance, although it is not a determining factor. The results are presented in Table 4.

Table 4: Correlation coefficients between ALBI, DESI, EGDI and Rule of Law Index

Pair of variables	r (Pearson)	95% CI (bootstrap)	p-value	rp (partial)*
ALBI – DESI	0.71	[0.32; 0.90]	0.032	–
ALBI – EGDI	0.76	[0.41; 0.92]	0.019	–
ALBI – Rule of Law	0.82	[0.54; 0.94]	0.008	0,68 (contr. DESI)

Note: rp is the partial correlation of ALBI with Rule of Law for a fixed DESI

Source: calculated by the authors using Formula (1) based on ALBI estimates and aggregated DESI, EGDI, and Rule of Law indicators; methodological framework [30–32]

The obtained values indicate a stable positive relationship between ALBI and all three external indicators. The closest association is with the Rule of Law Index ($r=0.82$; $p<0.01$), which confirms the construct validity of ALBI as an index sensitive to the legal capacity of the state. Correlations with EGDI ($r=0.76$) and DESI ($r=0.71$) demonstrate that technological and organizational digital maturity is consistent with more balanced (legal and accountable) digital processes, but does not fully

determine them. The partial correlation of ALBI–Rule of Law, controlled for by DESI (rp=0.68), indicates that the legal component retains an independent contribution to explaining ALBI variations beyond "pure" technological maturity. Figure 3 shows a cluster comparison of the ALBI and DESI indices of the three countries.

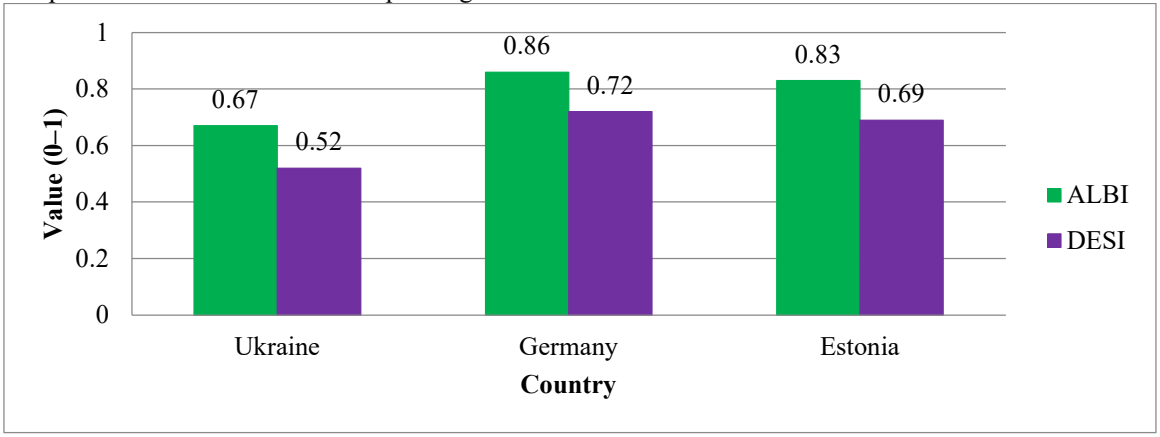

Figure 3: Comparison of ALBI and DESI for Ukraine, Germany, and Estonia

Source: created by the authors based on panel values of ALBI (3 countries × 3 scenarios) and DESI; 95% CI – bootstrap (1,000 repetitions)

Figure 3 shows that Germany maintains the highest scores on both indices, indicating a deep integration of digital services into the regulatory framework and an effective system of judicial control. Estonia demonstrates similar results with an emphasis on technological efficiency and transparency thanks to X-Road and the once-only model. Ukraine has a lower digital maturity, but is rapidly approaching European standards, especially in the area of electronic trust services.

5.4 Clustering of digital governance models according to the ALBI

Structural differences between national digital governance models were identified through k-means clustering (k = 3) based on four ALBI metrics – Eff, Transp, LegComp, and HRProt. The analysis included 12 observations (three scenarios for each of the three countries), which allowed to form stable profiles of management balances. Preliminary dimensionality reduction using the principal component analysis (PCA) method showed that the first two components explain 87.4% of the total variance of the data, which is sufficient to build a visual classification model (Table 5).

Table 5: K-means cluster profiles (mean values of metrics in each cluster)

Cluster	Characteristics	Eff	Transp	LegComp	HRProt	ALBI (average)	Model type
1	High legal balance, developed control and protection of rights	0.84	0.81	0.88	0.86	0.85	Germany
2	Technologically efficient, moderate transparency, flexible integration	0.87	0.78	0.83	0.79	0.82	Estonia
3	High speed of digitalization, but partial legal unregulation	0.78	0.62	0.67	0.60	0.67	Ukraine

Source: created by the authors based on their own calculations using Formula (1) and the results of k-means clustering in Python (scikit-learn and Pandas libraries)

The results obtained in Table 5 indicate a clear distinction between the three types of digital governance. Cluster 1 (Germany) is characterized by maximum legal balance, a high level of accountability and developed mechanisms of judicial control, which ensures the systemic legitimacy of digital decisions. Cluster 2 (Estonia) demonstrates a technological advantage thanks to the X-Road platform and the interoperability by design model, however, lower HRProt values indicate the need to expand appeal mechanisms in cases of automated decision-making. Cluster 3 (Ukraine) is

distinguished by a high speed of digital reforms, but limited institutional maturity of control procedures, which is reflected in the lowest values of transparency and legal compliance. Figure 4 presents a spatial visualization of the three clusters of digital governance.

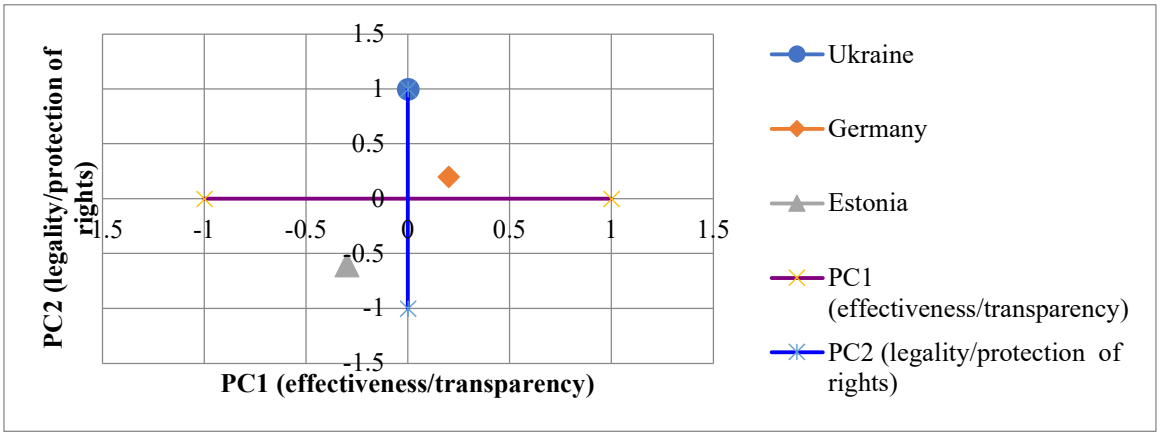

Figure 4: Visualization of clusters on the PCA plane

Source: created by the authors based on k-means clustering and PCA (Python, scikit-learn and)

Figure 4 shows that the PC1 axis (explaining 62% of the variation) reflects the growth of digital efficiency (Eff) and transparency (Transp), while the PC2 axis (25.4% of the variation) characterizes legal compliance (LegComp) and protection of citizens' rights (HRProt). Visually, a clear grouping is observed: Germany has formed a separate cluster with the dominance of legal parameters. Estonia is a technological cluster with a balance of efficiency and legality. In turn, Ukraine is a transitional model that tends to technological modernization, but with insufficient legal institutionalization. So, the clustering results confirm that digital governance develops along three trajectories: legal maturity (Germany), technological integration (Estonia), and reform dynamics (Ukraine). This creates an empirical basis for comparative modelling of the evolution of administrative and legal systems in the context of a digital state.

5.6 Assessment of the stability and sensitivity of the ALBI

The reliability of the obtained results was verified through a statistical bootstrap evaluation of the ALBI with 1,000 repetitions (n = 1000, α = 0.05). This approach allowed us to form 95% confidence intervals and assess the stability of the country ranking even with variations in the weight coefficients of Formula (1). An analysis of the sensitivity of the model to changes in the weights of the Eff, Transp, LegComp, and HRProt metrics within ±10% was also performed to check how much the relative position of each country is preserved under uncertain conditions. The results of the bootstrap evaluation are given in Table 6.

Table 6: Results of the bootstrap evaluation (95% confidence intervals for ALBI)

Country	Average ALBI	95 % CI (lower – upper threshold)	Variance (ALBI)	Rank change by ±10% of weights
Ukraine	0.672	0.653 – 0.689	0.00018	0 (stable rank)
Germany	0.861	0.849 – 0.873	0.00009	0 (stable rank)
Estonia	0.829	0.812 – 0.844	0.00013	0 (stable rank)

Source: created by the authors based on the results of bootstrap simulations (Python 3.12, NumPy, SciPy)

The results of Table 6 demonstrate the high stability of the ALBI: even with random variations in the sample and correction of weight parameters, the relative order of countries remains unchanged. The smallest variance is observed in Germany (0.00009), which confirms the stability of its legal model of digital governance. Estonia is characterized by moderate variability (0.00013), associated with the dynamic implementation of innovative solutions in the X-Road system. Ukraine preserved the stability of the ranking despite a slightly larger variance (0.00018), which indicates the consistency of the results even under conditions of changing weight coefficients and scenarios. So, the bootstrap analysis confirmed the statistical reliability of the ALBI calculations and demonstrated that the

obtained ranking of the three countries is stable, and the index model is sensitive to significant, but not random changes in parameters.

5.7 Legal and organizational interpretations of the results

The results showed that the effectiveness of digital public administration directly depends on the level of legal integration and institutional control. The highest values of the ALBI are observed in countries where digitalization is supported by legislative guarantees of legality, transparency, and appeal protection. In Germany, the Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) [27] ensures not only the technical accessibility of electronic services, but also the legal accountability of their delivery. The law establishes the responsibility of the administration for compliance with the principles of proportionality and openness, which ensures high LegComp (0.89) and HRProt (0.86) indicators. In Estonia, the *once-only principle* enshrined in the Public Information Act (Avaliku teabe seadus) [28] and Government Regulation No. 105 "Data Exchange Layer for Information Systems" [29], creates a unified X-Road platform that guarantees data exchange between government agencies even in crisis situations. This provides a combination of high efficiency (Eff = 0.88) with legal stability (LegComp = 0.85), confirming that innovation does not contradict legality. Ukraine, in turn, demonstrates high digitalization rates thanks to the laws "On the Legal Regime of Martial Law" [25] and "On Electronic Trust Services" [26], but legal integration remains incomplete. Despite high efficiency (Eff = 0.78), the Transp (0.61) and HRProt (0.59) indicators indicate the need for increased transparency, independent audit and judicial control. Harmonization with Regulation (EU) 2024/1183 (eIDAS 2.0) [32], Recommendation CM/Rec(2018)7 of the Council of Europe [30], and the OECD Digital Government Framework [31] is a necessary condition for increasing LegComp and HRProt without losing efficiency. The implementation of the *lawful-by-design* model, when digital solutions are designed immediately within the framework of administrative and legal procedures, will allow Ukraine to create a balanced crisis management system that combines technological speed, legality, and real protection of citizens' rights.

Observations from various nations and contexts indicate a debatable yet testable point. Laws and regulations are regarded as fundamental rather than mere additions following the adoption of new technology. Technology should not be mismanaged due to a lack of structure. Proper frameworks are vital in effectively addressing challenges with technology.

Government regulations benefit significantly from incorporating robust protections that individuals can access such as appealing decisions undergoing court reviews and adhering to explicit legal guidelines (protections). Strong protections are prioritized over mere implementation of technology. A quick technological approach does not guarantee the preservation of rights as seen in Ukraine's rapid advancements that lack transparency and adequate safeguards. Stability in Germany demonstrates that regulations can facilitate effective functioning during various crises. Emergency situations often benefit from established guidelines. Without proper rules efficiency in handling urgent matters may diminish.

Understanding the notion that it is not intended as a conclusive solution is crucial. The concept will be examined and debated further as additional information and improved data emerge. It cannot be assumed that this idea will remain unchanged as insights increase; deeper analysis of various contexts is necessary. By investigating sequential processes such as reviewing data and analyzing appeal outcomes enhancements to this idea can occur. Exploring alternative regulations might also yield an equally effective outcome promoting fairness and safeguarding rights. Presenting our results in this manner suggests a concept that can be invalidated facilitating a link between observations and concrete reasoning. Others find it simpler to scrutinize our findings and express counterarguments effectively.

6. DISCUSSION

The obtained results confirm that the effectiveness of digital public administration tools in a state of emergency is determined by the level of institutional capacity, legal maturity, and the quality of interdepartmental coordination. As Graf et al. [20] point out, the transition of authorities to a crisis regime is possible only if there are stable digital procedures that ensure the continuity of public services. Eckhard et al. [21] describe this process as "latent hybridity" – a combination of formal and informal management practices that increases the adaptability of the system in crises. Similar trends are recorded by Latupeirissa et al. [23], who prove that the successful digitalization of public services depends on the institutional context, regulatory certainty and the level of legal culture. Ahn and Chen [33] emphasize that the effective implementation of AI in public administration is possible only if the staff is ready for technological changes and adheres

to ethical standards. In the context of crisis governance, the Agbodzakey concept [34] identifies *collaborative governance* as the key to overcoming systemic challenges, which requires a combination of digital solutions and inter-organizational trust. At the same time, Wang et al. [35] show that the synergy of digital technologies and public health in the fight against the COVID-19 pandemic is possible only provided clear coordination between government agencies, legal control, and protection of citizens' data. So, the obtained results confirm that the sustainability of digital governance is ensured by a combination of institutional interaction, legal legitimacy and technological adaptability in times of crisis. This is consistent with the *lawful-by-design* principle, which involves the creation of digital solutions in compliance with the rules of law, transparency, proportionality, and human rights protection.

The differences in the ALBI between Ukraine, Germany, and Estonia are determined by the different depth of legal integration of digital governance. In Germany, the high values are explained by the Onlinezugangsgesetz (OZG), which ensures legal accountability and judicial control, consistent with the principles of the Council of Europe CM/Rec(2018)7. Estonia achieves a balance thanks to the once-only model and the X-Road platform, which implement the OECD recommendations on open data and inter-agency coordination. Ukraine, despite rapid digitalization, has lower indicators because of limited legal harmonization and the lack of independent audit systems provided for by eIDAS 2.0. So, the difference in ALBI values reflects the maturity of national policies – from legal control (Germany) and technological integration (Estonia) to the stage of regulatory reform (Ukraine).

Planning and enhancing government use of digital systems for emergencies is achievable through this study. Problems in online services are identified by officials. Changes that ensure clarity fairness and the protection of individual rights are not always guaranteed. Implementing these improvements can occur swiftly even in a crisis.

Open research issues and computing contribution

Recent research concerning digital governance in emergencies emphasizes two key domains. Legal studies examine principles of fairness regulations and safeguarding fundamental rights. Yet these concepts are frequently left unconverted into tangible assessable characteristics of the system. Management and technology research centers around the complexity of digital systems the durability of services and the interaction of platforms. In such investigations notions like transparency and accountability are perceived more as goals rather than confirmed realities. As a result tools designed to measure and analyze the equilibrium between speed legality and rights protection within digital public systems across different situations are insufficient.

Research on computing and governance benefits from this study (evaluation). A clear method has been established to assess the compliance of digital public systems with legal standards. Legal rules are transformed into quantifiable indicators (Eff Transp LegComp HRProt) that contribute to the formation of a new metric named the Administrative and Legal Balance Index (ALBI). Clear formulas are utilized with understandable weights while reliability is verified through techniques such as bootstrap confidence intervals. Patterns are identified using clustering and PCA which are techniques for grouping data alongside the exploration of various scenarios. An advanced method provides more than basic comparisons; it presents a structured means to assess the functioning of digital governance in emergency situations. A lack of assurance exists that advanced digital tools alone can ensure equitable governance. Both legal capabilities and established safeguards continue to play a crucial and quantifiable role. A robust connection exists regarding ALBI and a recognized Rule of Law metric (indicator). A strong association has been established. There are not any weak ties noted.

Research questions remain evident (inquiry). Several future computing studies should utilize audit features which can be automatically verified by computers along with standard process markers to enhance measurement objectivity. It is not necessary for the model to be limited to just current data; incorporating temporal data would reveal how reforms influence outcomes. Employing approaches that uncover cause and effect can assist in determining which legal safeguards most effectively enhance equity in various situations. Incorporating detailed process information including administrative records appeal outcomes decision durations and records of modifications must be prioritized with simulations utilized to evaluate systems under pressure rather than merely depending on analytical scenarios. Addressing these issues plays a crucial role in transitioning from sporadic evaluations to continuous embedded lawful oversight of digital public administration frameworks.

Interpretation criteria and relation to prior literature. Results are analyzed through the established criteria of the ALBI framework. Efficiency transparency legal compliance and human rights protection are not adequately evaluated in terms of digital governance effectiveness. Evaluation of digital governance requires consideration of multiple factors rather than a single aspect. Assessment cannot rely solely on one factor to determine effectiveness. A broad range of elements should be included in the evaluation.

Digital governance is often assessed by analyzing legal compliance or measuring technological readiness which frequently overlooks a combined approach. Previous research has not typically evaluated effectiveness by looking at both user engagement with digital tools and the system's robustness. Examining the interplay of various elements in distinct scenarios is essential. A clear distinction can be observed between high efficiency without adequate legal protection and compliance with the law lacking in efficiency. Understanding the outcomes requires adherence to stricter rules compared to alternative approaches. Improved evaluation of digital governance occurs during the implementation of emergency laws. Enhanced insights are gained regarding its effectiveness. It does not provide clarity on how effective governance can adjust in crises.

Comparison of results with prior work and added value of the proposed approach.

Certain aspects of our findings were overlooked by others utilizing the ALBI concept. Many studies suggest that increased technology deployment in government during emergencies is beneficial since it accelerates processes ensures service continuity and aids recovery efforts. A common belief is that an increased use of technology by a government leads to improved management. Improved management is often assumed with advanced technological integration. It isn't true that technology alone guarantees better outcomes in governance.

Despite effective technology use by a government it does not necessarily indicate openness or adherence to legal standards. Generally other studies assess the legality of actions or a government's preparedness in employing technology. Findings from our ALBI indicate that proficiency in technology does not consistently align with legal compliance across various nations.

Clarity is being enhanced by illustrating that a balance occurs when technology is utilized by governments alongside mechanisms for citizens to voice concerns judicial oversight and well-defined legal procedures. Comparisons have been provided through tables and visuals highlighting our unique approach versus that of others. Patterns across various nations and circumstances are also illustrated in these comparisons.

Novelty and contribution. The novelty of this work lies in operationalizing "administrative and legal balance" of digital public governance under emergency legal regimes as a computable, scenario-based construct and demonstrating its empirical relevance in a comparative setting. Further research may expand the sample of countries, involve time series for analysing ALBI dynamics, integrate multifactor indicators (citizen trust, level of cyber protection, financial efficiency), and test the model based on data from real crisis scenarios. This will increase the validity of the index and form a more comprehensive assessment of the legal sustainability of digital governance.

8. DIFFERENCES FROM PRIOR WORK AND CONTRIBUTION

Research conducted previously indicates the significance of digital governance in sustaining operations enhancing administrative efficiency and updating governmental procedures. (system effectiveness) Some risks have been identified in legal analysis such as ambiguous processes unpredictability due to automation and diminished personal safeguards in data-driven decision-making. A clear understanding of why governance risks intensify during emergencies is not provided by these studies. A common approach is to concentrate on significant concepts such as constitutional regulations and justice or to assess the effectiveness of technology and systems. Comparisons are rarely made regarding how various legal and administrative frameworks maintain legality transparency and rights respect during urgent situations.

Turning the legal and administrative trade-off into measurable data is assisted by this study. (measurable) The relationship between digital effectiveness and legal balance is demonstrated. It is not the case that the study establishes an Administrative and Legal Balance Index (ALBI). Four components are integrated into this index: system efficiency transparency adherence to legal standards and the protection of human rights. Responses are assessed by ALBI while legality and fairness are ensured. Legal strengths of a state are not concentrated on by general digital-

readiness measures unlike ALBI. A robust link exists between ALBI and the Rule of Law Index (relationship). Detailed analysis has shown that the legal component is significant. It cannot be claimed that the legal element lacks importance.

Scenario models have been utilized in the study to illustrate how balance varies by context (situation). Variations in ALBI are influenced by factors such as inter-departmental collaboration the implementation of electronic IDs and the avenues available for citizens to contest decisions. Legal weaknesses do not occur uniformly across all administrative sectors simply due to a nation being digital.

Research and decision-makers obtain valuable insights through country comparisons (countries). Useful information is provided when digital tools are integrated with effective decision-making processes judicial reviews and adherence to clear legal standardsnot solely by establishing well-connected technology platforms. Germany does not fall short on ALBI attributed to its robust legal compliance and strong rights protection. Efficiency and transparency benefit from designing systems that collaborate as demonstrated by Estonia. More attention must be directed toward safeguarding rights in automated decisions. A gap arises leading to faster efficiency while transparency and rights protection experience delays. Ukraine illustrates how rapid digital reforms can outpace the speed of legal frameworks.

Findings affirm the concept of a lawful-by-design model (law-focused). A legal integration is demonstrated to be essential for transforming rapid digital responses into credible and reliable governance during crises. The crucial point isn't only the ALBI index but also that robust legal safeguards are an independent and significant element for effective digital governance in emergency situations. Greater transparency along with the opportunity to verify decisions can enhance governance's equilibrium. Decisions can be checked more thoroughly. Opportunities to appeal do not hinder the effectiveness of governance. With these improvements governance may operate more smoothly while remaining fair and open.

9. CONCLUSIONS

The study confirmed that the effectiveness of digital public governance tools in a state of emergency is determined by the level of legal integration, institutional control, and regulatory coherence. A comparison of Ukraine, Germany, and Estonia showed significant differences in the balance between technological efficiency, transparency, and legal guarantees. The highest indicators of administrative and legal balance (ALBI = 0.86) are in Germany, where the Onlinezugangsgesetz (OZG) ensures a combination of digital maturity, judicial control, and an effective appeals mechanism. Estonia (ALBI = 0.83) confirmed the effectiveness of the once-only principle and the X-Road system, which supports transparent data exchange even in times of crisis. Ukraine demonstrates high digitalization rates (Eff = 0.78), but retains legal asymmetry (Transp = 0.61; HRProt = 0.59) because of the fragmentation of the regulatory framework and limited control procedures. The scenario analysis showed that Germany has the most robust digital response model, while Ukraine faces risks of algorithmic opacity and lack of appeal procedures. The correlation between ALBI and the Rule of Law Index (r = 0.82) proves that the legal capacity of the state is key to ensuring balanced digital governance. Clustering revealed three development trajectories: legal maturity (Germany), technological integration (Estonia), and reform dynamics (Ukraine). Legal harmonization with Regulation (EU) 2024/1183 (eIDAS 2.0), Recommendation CM/Rec(2018)7 of the Council of Europe and the OECD Digital Government Framework is a necessary condition for increasing LegComp and HRProt without losing efficiency. For Ukraine, the strategic direction is the implementation of the lawful-by-design model, the development of algorithmic audit, the expansion of digital appeal mechanisms, and the strengthening of judicial control. This will create a legal and transparent crisis management system compatible with European standards of digital statehood.

In conclusion the inquiries raised at the outset are addressed by this study. It has been revealed that effective digital public governance in emergencies requires more than just adequate technology. Digital tools are not solely reliant on their integration within regulations and safeguards. Fast digitalization in Ukraine Germany and Estonia presents various legal challenges. Legal problems are encountered in the process of achieving quick digital transformation. Not every scenario showcases an ideal relationship among efficiency transparency law and rights. Questions arise regarding the influence of regulations on digital governance during emergencies. Emergencies challenge digital public administration. Governance is assessed by whether digital tools actually improve decision-making or merely hasten the process while lacking adequate safeguards. A focus on law in the design has not been recognized as essential for effective digital

governance in emergencies contrary to merely having sophisticated technology. Utilizing the ALBI to evaluate balance in various contexts demonstrates this importance convincingly.

Taken together, the results support the hypothesis that emergency legal regimes reveal a structural gap between rapid digital service delivery and legally balanced governance unless digital tools are designed and operated within enforceable administrative-law safeguards. The findings show that effectiveness must be interpreted jointly with transparency, legal compliance, and rights protection (as captured by ALBI), that national legal frameworks condition this balance across Ukraine, Germany, and Estonia, and that scenario-specific stress points concentrate in concrete administrative pathways – especially contestability and appeal mechanisms in citizen-facing processes. Overall, the evidence confirms the core argument of the paper: technological maturity alone is insufficient, while institutionalized transparency, auditability, and reviewability determine whether digital governance remains both fast and lawful during emergencies.

REFERENCES:

[1] R. V. Mihal, Y. M. Fityak and D. O. Kuzik, "Administrative-Legal Regulation of the Digitalization of Administrative Procedures in Ukraine", *Academic Visions,* Vol. 33, 2024. https://doi.org/10.5281/zenodo.14771983

[2] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov and A. Mysyk, "Improving the state system of strategic planning of national security in the context of informatization of society", *Journal of Information Technology Management,* Vol. 14, 2022, pp. 1–24. https://doi.org/10.22059/jitm.2022.88861

[3] I. Semenets-Orlova, V. Kushnir, L. Rodchenko, I. Chernenko, O. Druz and M. Rudenko, "Organizational development and educational changes management in public sector (case of public administration during war time). *International Journal of Professional Business Review,* Vol. 8, No. 4, 2023. https://doi.org/10.26668/businessreview/2023.v8i4.1699

[4] V. Tkachenko, Y. Kotviakovskyi and S. Zinchenko, "Contemporary European Concepts of Public Administration in the Context of Digital Transformation and their Legal Framework", *Public Administration and Law Review,* Vol. 1, No. 21, 2025, pp. 99-109. https://doi.org/10.36690/2674-5216-2025-1-99-109

[5] F. Wollenschlager, "Judicial Review of Government Pandemic Responses: Emerging Basic Lines in the Federal Administrative Court's First Judgments", *Georgia Law Review,* Vol. 58, No. 3, 2023, p. 9. https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1545&context=glr

[6] L. Vyhnánek, A. Blechová, M. Bátrla, J. Míšek, T. Novotná, A. Reichman and J. Harašta, "The Dynamics of Proportionality: Constitutional Courts and the Review of COVID-19 Regulations", *German Law Journal,* Vol. 25, No. 3, 2024, pp. 386-406. https://doi.org/10.1017/glj.2023.96

[7] K. Härmand, "Digitalisation before and after the Covid-19 crisis", In *ERA Forum* (Vol. 22, No. 1, pp. 39-50). Berlin/Heidelberg: Springer Berlin Heidelberg, 2021. https://doi.org/10.1007/s12027-021-00656-8

[8] E. Blake Jackson, R. Dreyling and I. Pappel, "A historical analysis on interoperability in Estonian data exchange architecture: perspectives from the past and for the future", In *Proceedings of the 14th international conference on theory and practice of electronic governance* (pp. 111-116), 2021. https://doi.org/10.1145/3494193.3494209

[9] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk and S. Podolyaka, "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine", *Journal of Information Technology Management,* Vol. 13, 2021, pp. 75–90. https://doi.org/10.22059/jitm.2021.80738

[10] J. M. Barrutia and C. Echebarria, "Effect of the COVID-19 pandemic on public managers' attitudes toward digital transformation", *Technology in Society*, Vol. 67, 2021, 101776. https://doi.org/10.1016/j.techsoc.2021.101776

[11] S. Ranchordás, "The invisible citizen in the digital state: administrative law meets digital constitutionalism", In *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era* (pp. 15-40). The Hague: TMC Asser Press, 2024. https://doi.org/10.1007/978-94-6265-647-5_2

[12] M. Almada, "Automated Uncertainty: A Research Agenda for Artificial Intelligence in Administrative Decisions", *Review of European Administrative Law,* Vol. 16, No. 3, 2023,pp. 137-158. https://doi.org/10.7590/187479823X16970258030172

[13] N. M. Doran, S. Puiu, R. M. Bădîrcea, M. G. Pirtea, M. D. Doran, G. Ciobanu and L. D. Mihit, "E-government development–A key factor in government administration effectiveness in the European Union", *Electronics,* Vol. 12, No. 3, 2023, p. 641. https://doi.org/10.3390/electronics12030641

[14] S. J. Eom and J. Lee, "Digital government transformation in turbulent times: Responses, challenges, and future direction", *Government Information Quarterly,* Vol. 39, No. 2, 2022, 101690. https://doi.org/10.1016/j.giq.2022.101690

[15] S. Kim, K. N. Andersen and J. Lee, "Platform government in the era of smart technology. *Public Administration Review,* Vol. 82, No. 2, 2022, pp. 362-368. https://doi.org/10.1111/puar.13422

[16] J. Newman, M. Mintrom and D. O'Neill, "Digital technologies, artificial intelligence, and bureaucratic transformation", *Futures,* Vol. 1*36*, 2022, 102886. https://doi.org/10.1016/j.futures.2021.102886

[17] B. Peng, "Digital leadership: State governance in the era of digital technology", *Cultures of Science*, Vol. 5, No. 4, 2022, pp. 210-225. https://doi.org/10.1177/2096608321989835

[18] A. Androniceanu, I. Georgescu and J. Kinnunen, "Public administration digitalization and corruption in the EU member states. A comparative and correlative research analysis", *Transylvanian Review of Administrative Sciences,* Vol. 18, No. 65, 2022, pp. 5-22. https://doi.org/10.24193/tras.65E.1

[19] E. R. Sadik-Zada, A. Gatto and I. Niftiyev, "E-government and petty corruption in public sector service delivery", *Technology Analysis & Strategic Management,* Vol. 36, No. 12, 2024, pp. 3987-4003. https://doi.org/10.1080/09537325.2022.2067037

[20] F. Graf, A. Lenz and S. Eckhard, "Ready, set, crisis–transitioning to crisis mode in local public administration", *Public Management Review,* Vol. 26, No. 7, 2024, pp. 2039-2063. https://doi.org/10.1080/14719037.2023.2242851

[21] S. Eckhard, A. Lenz, W. Seibel, F. Roth and M. Fatke, "Latent hybridity in administrative crisis management: The German refugee crisis of 2015/16", *Journal of Public Administration Research and Theory,* Vol. 31, No. 2, 2021, pp. 416-433. https://doi.org/10.1093/jopart/muaa039

[22] C. H. Lee, D. Wang, S. Lyu, R. D. Evans and L. Li, "A digital transformation-enabled framework and strategies for public health risk response and governance: China's experience", *Industrial Management & Data Systems,* Vol. 123, No. 1, 2023, pp. 133-154. https://doi.org/10.1108/IMDS-01-2022-0008

[23] J. J. P. Latupeirissa, N. L. Y. Dewi, I. K. R. Prayana, M. B. Srikandi, S. A. Ramadiansyah and I. B. G. A. Y. Pramana, "Transforming public service delivery: A comprehensive review of digitization initiatives", *Sustainability,* Vol. 16, No. 7, 2024, 2818. https://doi.org/10.3390/su16072818

[24] P. Dunleavy and H. Margetts, "Data science, artificial intelligence and the third wave of digital era governance", *Public Policy and Administration,* Vol. 40, No. 2, 2025, pp. 185-214. https://doi.org/10.1177/09520767231198737

[25] Verkhovna Rada of Ukraine, "Law of Ukraine on the Legal Regime of Martial Law (No. 389-VIII)", *Official Bulletin of the Verkhovna Rada of Ukraine,* Vol. 28, 2015 May 12, Art. 250. https://zakon.rada.gov.ua/laws/show/389-19

[26] Verkhovna Rada of Ukraine, "Law of Ukraine on Electronic Trust Services (No. 2155-VIII)", *Official Bulletin of the Verkhovna Rada of Ukraine,* Vol. 45, 2017 October 5, Art. 400. https://zakon.rada.gov.ua/laws/show/2155-19

[27] Federal Ministry of the Interior and Community (Germany), "Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG)", *Federal Law Gazette* (BGBl. I, p. 3122), 2017 August 14. https://www.gesetze-im-internet.de/ozg/

[28] Riigikogu, *Public Information Act* (Consolidated version, ELI: 529032019012) [Act], 2019. https://www.riigiteataja.ee/en/eli/529032019012/consolide . Riigi Teataja

[29] Government of the Republic of Estonia, *Infosüsteemide andmevahetuskiht – Government Regulation No. 105 (Data Exchange Layer for Information Systems*). RT I, 27.09.2016, 4; with amendments RT I, 06.08.2019, 6, 2016 September 23; https://www.riigiteataja.ee/akt/106082019017

[30] Council of Europe, *Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on guidelines to respect, protect and fulfil the rights of the child in the digital environment.* Strasbourg, France:

Council of Europe, 2018. https://rm.coe.int/09000016808b79f7

[31] Organisation for Economic Co-operation and Development (OECD), *The OECD Digital Government Policy Framework: Six dimensions of a digital government.* Paris: OECD Publishing, 2020. https://doi.org/10.1787/f64fed2a-en

[32] European Parliament & Council of the European Union, "Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0)", *Official Journal of the European Union, L 123*, 2024 April 30, pp. 1–65. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[33] M. J. Ahn and Y. C. Chen, "Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government", *Government Information Quarterly,* Vol. 39, No. 2, 2022, 101664. https://doi.org/10.1016/j.giq.2021.101664

[34] J. Agbodzakey, "Collaborative Governance and Crisis Management: A Focus on COVID-19", In *Collaborative Governance Primer: An Antidote to Solving Complex Public Problems* (pp. 147-157). Cham: Springer International Publishing, 2024. https://doi.org/10.1007/978-3-031-57373-6_14

[35] Q. Wang, M. Su, M. Zhang and R. Li, "Integrating digital technologies and public health to fight Covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare", *International Journal of Environmental Research and Public Health,* Vol. 18, No. 11, 2021, 6053. https://doi.org/10.3390/ijerph18116053