

LEGAL PRINCIPLES OF DIGITALIZATION OF PUBLIC ADMINISTRATION IN UKRAINE: CHALLENGES AND PERSPECTIVES

Kateryna Manyilova

Department of Public Administration and
Regionalism

Odesa Polytechnic National University

65044, 1 Shevchenko Ave., Odesa, Ukraine

e-mail: katerinamanyilova@gmail.com

<https://orcid.org/0000-0002-0721-7232>

Yuriy Norchuk

Department of Units Daily Activities
Management,

Odesa Military Academy

65009, 10 Fontanska Road, Odesa, Ukraine

e-mail: lopster@ua.fm

<https://orcid.org/0000-0003-0850-2278>

Abstract

The Ukrainian government's adoption of digital technologies marks a critical transition aimed at enhancing operational efficiency, strengthening accountability, and encouraging more active citizen engagement in governance. This study looks at the current legal framework in Ukraine that underpins this digital transformation and identifies key challenges that slow its progress. It is imperative that the following factors are given due consideration: the existence of gaps within the regulatory environment, the presence of cybersecurity vulnerabilities, and the limited institutional capacity to fully implement digital innovations. The study employed a variety of research methods, including the analysis of legislation, policy documents, and consultations with experts in the field. It is evident that Ukraine has already made a certain amount of progress in the development of legal instruments for e-government in the country. At the same time, it reveals persistent obstacles in the effective implementation and harmonization of these legal norms within the broader administrative context. In order to further implement digitalization, the Ukrainian government must adopt a multidimensional strategy. Significant legislative changes are required to ensure that national legislation is in line with the evolving requirements of digital governance. These reforms must address existing legislative gaps, reinforce data protection and privacy safeguards, and establish clear regulatory pathways for the integration of emerging technologies into the public domain. It is equally important to emphasize the enhancement of institutional capacity at all levels of public administration. International collaboration plays a pivotal role in advancing Ukraine's digital transformation in public governance. Such cooperation facilitates the exchange of knowledge and best practices. Further research should be directed towards the extensive comparative analysis of digital governance systems across various nations, with a particular emphasis on the legal intricacies inherent in the integration of artificial intelligence, block chain technologies and big data within public administration. It is imperative to give due consideration to the aforementioned challenges, as this will facilitate the establishment of robust legal strategies and the creation of adaptive regulatory mechanisms that can effectively respond to the evolving dynamics of technological development.

Keywords: digital transformation; public administration; legal framework; e-governance.

1. Introduction

Digital transformation has emerged drivers of contemporary societal evolution, delineating a novel paradigm of interaction among the pivotal actors within the public sphere: citizens, businesses, and the state. In the 21st century, the implementation of digital technologies has had a profound impact on the functional nature of public administration, leading to its transition to a new paradigm that is characterized by efficiency, openness, and technological adaptability. Information and communication technologies are emerging as catalysts for transformational processes. The digitalization of public administration is regarded as a pivotal mechanism for modernizing the state apparatus. The primary objectives of this process are to enhance transparency, accountability, institutional capacity, and the adaptability of government structures to the evolving socio-political environment. It opens up new opportunities for the realization of democratic principles in management practice, ensuring citizens' access to information, expanding feedback channels, and fostering the preconditions for inclusive participation in managerial decision-making processes (Hedikov, 2024).

Digital technologies are increasingly being integrated into public policy, changing the very logic of its implementation. Their actions contribute to the establishment of an intelligent governance framework. The model is founded upon the strategic utilization of data, supplemented by advanced analytical capabilities for predictive modeling. Moreover, it harnesses automation to streamline administrative tasks and adopts innovative technologies for the efficient delivery of public services. This process necessitates not only technical modernization but also profound institutional changes, including a revision of approaches to legal regulation, the development of digital infrastructure, and the advancement of digital competencies in the public sector. It is imperative to acknowledge that digitalization should not be regarded as an independent objective. The primary objective of digitalization should be aligned with the fundamental principles of democratic governance, including the protection of human rights, the safeguarding of personal data, the assurance of information security, and the facilitation of access to information. In order to achieve a successful digital transformation within the sphere of public administration, it is imperative to integrate technological progress with a robust legal framework, institutional capacity, and active citizen participation.

The European Union is implementing a coherent and focused digital development strategy. In the EU Member States, governments are implementing a comprehensive Digital Europe initiative, also known as the Digital Europe Programmer. This ambitious plan provides funding for digital innovation in several key areas, including artificial intelligence, cybersecurity, the development of digital skills, and the modernization of public institutions through digitalization (EUR-Lex, 2025). The EU is actively pursuing digital sovereignty while strengthening its competitive edge, set against a backdrop of global volatility and increasing cyber risks. This focus has gained further significance since the COVID-19 crisis and the Russian Federation's full-scale invasion of Ukraine. In alignment with the European Commission's Communication, «Shaping Europe's Digital Future,» the digital transformation is intended to be guided by democratic values, ensuring transparency and promoting inclusivity. (EU4Digital, 2025). In its quest to become a digitally integrated nation within Europe, Ukraine is actively pursuing the digital transformation of its government operations. However, this effort faces a number of challenges. These include inconsistencies within existing legal documents, the fragmented nature of its regulatory system, and the need to adopt European digital governance models and standards. The aim of this research is to examine the basic legal framework supporting the digitization of the Ukrainian public administration, identify the main legal barriers to this process, and forecast future progress.

This essay aims to explore the current framework supporting Ukraine's shift toward digital public administration. It will analyze the significant challenges within

the existing legal and regulatory mechanisms. Additionally, it seeks to outline potential future directions, drawing on best practices observed across Europe. The focus will be on aligning Ukrainian laws with those of the European Union and examining how digital tools can contribute to the strengthening of democratic principles in governance. In the context of the digital transformation of public administration, it is of particular importance to study legislation that ensures the efficiency, security and transparency of digital processes. Contemporary scientific discourse highlights the critical importance of developing a flexible and well-integrated legal and regulatory framework. Such a framework is considered essential for supporting the sustainable, digitally-driven advancement of a nation. In particular, at the European level, research on the harmonization of digital contract law is relevant, having intensified after the adoption of the so-called «Twin Directives» of the EU in 2019 concerning digital content and services (De Franceschi & Schulze, 2023). This sets a benchmark for Ukraine in the context of implementing relevant norms into national legislation.

A number of studies have focused on digitization in the context of crisis, war and reconstruction. In this context, the work of M. Negrei, I. Kostenko, and Yu. Kravchenko (CSD EIS 2022) is of particular importance, presenting the dynamics of the transformation of digital processes in Ukraine in the pre-war and wartime periods. The focus here shifts to the emerging need for adjusting legal frameworks to address crises, specifically encompassing both the immediate aftermath and subsequent recovery. This necessitates not only a fundamental physical reconstruction, but also a thorough reassessment of the legal framework governing their activities (Nehrey et al., 2023). The study by K. Schedler (Schedler et al., 2019), A.A. Gündüz, and R. Frischknecht provides a significant theoretical contribution by explaining the institutional and organizational barriers that hinder the progress of digitalization. The researchers identified the absence of a robust legal framework as a significant impediment to digitalization (Schedler, et al., 2019). This conclusion is of particular pertinence in the context of Ukraine, where the fragmentation of regulatory frameworks constitutes a significant impediment to the advancement of digital transformation within the public sector.

The European approach to digital transformation in crisis conditions is also analyzed in the research by C.M. Profiroiu, C.I. Negoită, and A. Costea (Profiroiu et al., 2023). Although it does not have a purely legal focus, the authors demonstrate that the effectiveness of digitalization directly depends on the availability of stable legal and financial mechanisms (Profiroiu et al., 2023). Summarizing the scientific approaches, it can be argued that the key challenges for the legal support of digitalization in Ukraine are:

- fragmentation and lack of systematicity in the legal and regulatory framework;
 - lack of institutional continuity in the implementation of digital policies;
 - the necessity of harmonizing with European digital legislation
- the need for legal regulation of crisis and emergency digital solutions.

At the same time, the prospects lie in the formation of a unified legal space for digital governance, based on the principles of openness, interoperability, and civic participation. Also, in the development of regulatory support for public digital platforms.

As Ukraine pursues its path toward integration with Europe, it must also pay close attention to these developments. The imperative of aligning its legal framework with the *acquis communautaire* is a crucial aspect of this endeavour. According to Ukrainian researchers Vavrynychuk (2023), Shulzhenko (Shulzhenko et al., 2021), Michalak and Śniadach (2023), the digitization of governmental processes requires a shift that goes beyond technological advancements. A comprehensive legal overhaul of existing laws is necessary to fully embrace this transformation. This involves formulating specific legal frameworks for artificial intelligence, refining existing regulations on the protection of personal information, and strengthening laws concerning cybersecurity and digital

infrastructure. According to Ukrainian researchers Vavrynychuk (2023), Shulzhenko (Shulzhenko et al., 2021) and Michalak and Śniadach (2023), the digitization of governmental processes requires a shift that goes beyond technological advancements. A comprehensive legal overhaul of existing laws is necessary to fully embrace this transformation. This involves formulating specific legal frameworks for artificial intelligence, refining existing regulations on the protection of personal information, and strengthening laws concerning cybersecurity and digital infrastructure. (Vavrynychuk, 2023; Shulzhenko et al., 2021; Michalak and Śniadach, 2023).

The primary issue identified by scholars pertains to the incongruity between the rapid advancements in information technology (IT) and the gradual evolution of the legal framework. This discrepancy ultimately impedes the efficacy of digital transformation initiatives. Furthermore, a lack of adequate alignment between national laws and European Union regulations obstructs international cooperation and undermines confidence in digital services within the public sector.

Academic research emphasizes the need for a multifaceted strategy regarding the legal frameworks surrounding digitalization, which must include both technological and legal harmonization. The EU's experience in digital law can serve as a methodological and practical basis for updating the Ukrainian regulatory framework to ensure sustainable digital development and effective public administration. While these studies significantly enhance our understanding of the legal aspects of digital transformation, most of them are general in nature. There is a tendency to overlook the institutional challenges posed by the digitalization of public administration under martial law, underscoring the necessity for research to be conducted into the legal framework governing digital transformation. It is imperative to emphasize the necessity of aligning national legislation with international and European standards. The objective of this study is to analyze Ukrainian legislation on digital governance, with a focus on the effective and sustainable implementation of reforms in the public sector.

2. Materials and Methods

The present study employs qualitative methodologies, a particularly apt approach when analyzing the legal and institutional dimensions of the digitalization of public administration in Ukraine. The primary methodology employed is that of documentary analysis, a technique which facilitates a comprehensive examination of the prevailing legal framework that governs digital transformation within Ukraine's public sector. This encompasses the analysis of legislative acts, governmental resolutions and other regulatory documents that delineate the legal framework for digital governance. This specifically encompasses laws and directives related to e-governance initiatives, safeguards against cyber threats, the establishment of electronic trust services, administrative processes, and the protection of personal information. A thorough examination was conducted of key legislative instruments such as Ukraine's Law "On Electronic Governance" (as outlined in Order No. 649-r) and the Law "On Personal Data Protection" (Verkhovna Rada of Ukraine, 2025c), alongside relevant Presidential decrees and governmental strategies focused on digital development. This analysis considered not only the substantive content of these legal resources but also their internal coherence, alignment with the overarching national strategic objectives, and conformity with established international standards—with particular attention to those promoted by the European Union.

A comparative analysis constitutes the second key method, which facilitates the comparison of Ukrainian legislation with international standards and European practices in the field of digital governance. This enables the identification of the primary issues and lacunae in national legislation, in addition to the identification of areas for enhancement.

In addition to document analysis, this study employed semi-structured interviews.

A diverse group of stakeholders—including legal professionals, lawmakers, governmental officials, and IT specialists—formed the interviewee pool. These individuals played active roles in shaping and implementing digital transformation initiatives in Ukraine. The primary objective of the interviews was to gain a practical understanding of how legal regulations are applied, how various institutions collaborate, and how digital initiatives are actually implemented in practice. Special attention was devoted to identifying implementation barriers. Owing to the flexible nature of semi-structured interviews, they enabled discussions to be guided by predefined themes while also allowing for the emergence of novel, context-specific insights. Furthermore, the study's methodological framework strongly incorporated comparative legal analysis. This provided a systematic means of contrasting Ukraine's legal landscape with globally recognized standards, particularly those set by the European Union. Key reference points in this comparative examination included the General Data Protection Regulation (GDPR), the Tallinn Declaration on e-Governance, and the OECD's guidelines on digital government. Furthermore, expert interviews with specialists in public administration, law, and information technology are also an important research tool. These interviews are instrumental in acquiring practical knowledge and experience from individuals directly involved in the implementation of digital innovations in the public sector.

The combination of these methodologies facilitates a comprehensive comprehension of the legal, institutional and procedural dimensions of digital public administration. Moreover, it offers a framework for the effective formulation of recommendations to enhance digital transformation in Ukraine.

3. Result and Discussion

Throughout recent history, Ukraine has progressively implemented a range of significant regulatory and legal instruments aimed at advancing digital governance. This process has involved the adoption of several pivotal legislative acts. These include provisions on electronic identification systems (Order No. 649-r), the functioning of state information systems (Order No. 1556-p), legislation on digital communication networks (Verkhovna Rada of Ukraine, 2025c), the delivery of administrative services through digital platforms (Verkhovna Rada of Ukraine, 2024), and regulations governing interactions via electronic platforms (Verkhovna Rada of Ukraine, 2023). Collectively, these legal measures have significantly reconfigured the national regulatory framework, laying a foundational path for the digital transformation of public sector administration.

These adopted regulations firmly establish foundational principles that prioritize clarity, accessibility, and the interoperability of governmental data systems. Furthermore, they underscore the importance of meeting the needs of both the public and the commercial sectors. The core provisions align closely with contemporary European models aimed at constructing efficient, accountable, and forward-looking governance structures. This legal framework is fully consistent with the concept of a “digital state” and embodies the fundamental ideals of sound public administration (Verkhovna Rada of Ukraine, 2022).

An analytical review of current Ukrainian regulations concerning the digital transformation of public administration reveals a set of recurring systemic challenges that significantly impede successful implementation (Verkhovna Rada of Ukraine, 2025a). A notable issue lies in the drafting of numerous legislative acts without adequate coordination among governmental bodies, which has led to fragmentation and insufficient integration. This lack of cohesion obstructs the creation of a unified regulatory environment, essential for facilitating effective interaction between digital infrastructures across various levels of public authority. Furthermore, the absence of clearly defined legal frameworks for interoperability contributes to overlapping mandates, inefficient information flows, and operational disjunction among institutions engaged in digital governance.

The main problems of interagency coordination and interoperability in the current laws of Ukraine regarding the digital transformation of public administration are summarized below, as shown in Table 1.

Table 1. key issues of interagency coordination in ukrainian digital governance laws

Law of Ukraine	Problem	Example
"On Electronic Communications" (Law No. 1089-IX)	The absence of mechanisms for regulatory interoperability of ICT systems.	There are no legal provisions regarding the integration of digital platforms of government bodies.
"On Information" (Law of Ukraine No. 2807-IX)	Unclear regulatory framework for the integration of information resources between government agencies.	The information is presented fragmentarily, without proper coordination of exchange.
«On Administrative Services» (Law No. 1907-IX)	Insufficient regulatory support for digital interaction between public administration entities.	The Diia platform functions in isolation from other state systems.
"On Personal Data Protection" (Law No. 2297-VI)	Lack of standardized approaches for the exchange of personal data between public authorities.	The lack of unified approaches to data processing complicates the integration of public administration information systems.

Compiled by the authors

In this context, the viewpoint of V. Hedykov is particularly relevant, as he suggests that the consolidation of legislation through the development of a Digital Code of Ukraine represents both a feasible and pragmatic solution (V. Hedykov). According to the author, such a codified act would effectively systematize the key regulations governing the digitalization sphere and establish a unified legal foundation for the balanced development of a digital state. The adoption of this code would serve as a logical response to the challenges posed by regulatory fragmentation, enhance the coherence between sectoral policies, and create an integrated framework for digital governance, aligning it with European standards of good governance.

A significant obstacle hindering the modernization of Ukraine's public administration is the inadequacy of its legal and regulatory frameworks to accommodate cutting-edge digital technologies. Specifically, current legislation fails to provide clear guidelines for integrating innovative tools, such as automated decision-making processes, machine learning applications, and artificial intelligence systems, into administrative operations. This legal gap significantly undermines both the predictability and transparency of government agencies' operations as they transition to digital practices.

The current lack of explicit regulations concerning the deployment and use of AI technologies, automated decision-making systems, and machine learning algorithms presents various potential risks. Firstly, it generates legal uncertainty regarding responsibility for the consequences caused by decisions made in an automated mode. In particular, it remains unclear who will be held responsible in case of violation of citizens' rights or errors made by the system – the state body, the software developer, or the operator of the technical solution. Secondly, insufficient legal regulation complicates the proper control over algorithms that may be prone to bias, discrimination, or violation of the principles of transparency and integrity. Thirdly, without standards for the use of such

technologies, the state lacks the necessary levers to ensure the protection of personal data, prevent abuse, and ensure procedural fairness in the use of innovative tools in public administration. Finally, this situation not only hinders the innovative development of the administrative sphere, but also significantly limits the potential for modernization of the state's electronic services. This makes it impossible to fully implement the principles of digital governance, such as client-orientation, efficiency, transparency, and public trust. As Ukraine seeks to integrate into the European digital space, one of the most significant obstacles to this process is the absence of clearly defined legal guidelines for the use of advanced technologies in government operations. This gap not only impedes alignment with the regulatory systems already established in the EU but also hampers the adoption of principles related to digital self-determination.

In addition, it is important to note that the absence of specific legal provisions has the potential to impact Ukraine's international competitiveness. Other countries have already taken steps to implement relevant regulations and utilize cutting-edge technologies to enhance the efficiency of government processes and foster trust in digital institutions. Ensuring the sustainable development of digital governance is a crucial aspect to consider. In this regard, the establishment of a contemporary regulatory framework for artificial intelligence technologies is a strategic priority to ensure the continued advancement and growth of our digital landscape. Furthermore, a serious problem remains the lack of clear regulations regarding the cross-border transfer of personal and administrative data. In a globalized world, where interaction between countries requires the rapid and secure transfer of data, the existing legal environment does not provide adequate legal protection for the exchange of information between state bodies of different countries. This leads to legal uncertainty, which can become a barrier to international cooperation in the field of digital technologies, particularly for the expansion of digital services and data exchange within international initiatives.

The absence of clearly defined regulations governing the cross-border exchange of personal and administrative data remains a critical concern. In an increasingly interconnected global environment—where the secure and rapid sharing of data between nations is essential—existing legal frameworks provide insufficient safeguards for intergovernmental data exchange. This legal ambiguity generates uncertainty and may impede international cooperation in the field of digital technologies, particularly in the context of expanding digital services and cross-border data initiatives. Ukraine's cybersecurity vulnerabilities have become increasingly critical amidst the ongoing, large-scale military conflict with Russia. While the country has foundational legal frameworks in place—most notably the Law of Ukraine “On the Basic Principles of Cybersecurity” (Verkhovna Rada of Ukraine, 2025b)—the existing legal structure remains insufficient. It is fragmented, lacks technical specificity, and fails to account for the complexities of modern cyber warfare.

As A. Pravdiuk emphasizes, the rapid evolution of information technology and the intensifying threats to Ukraine's national security—particularly within the context of hybrid warfare and Russian cyberattacks—demand a continuous refinement of cybersecurity legislation (A. Pravdiuk). Although current laws establish some essential principles of cyber defence, they fall short in terms of coherence and practical applicability. In particular, the absence of detailed technical standards, clearly articulated response protocols, and coordinated mechanisms for interagency collaboration severely undermines the protection of critical information infrastructure. The timely mitigation of cyber incidents, and the broader resilience of the country's digital landscape. In such circumstances, legal uncertainty not only limits the internal capacity of the public administration system to counter threats but also reduces Ukraine's potential for full integration into the European and global cybersecurity ecosystem.

The issue of the lack of an effective mechanism for interagency coordination in the context of multi-level information attacks and destructive information and

psychological operations by the aggressor state is becoming particularly relevant. Against the backdrop of systemic cyberattacks aimed at destroying information resources, disrupting governance, demoralizing the population and the military, legal instruments remain insufficiently flexible and do not cover the full spectrum of hybrid threats. The imperfection of legal regulation limits Ukraine's potential for interaction with international partners in the field of cyber defense and hinders the formation of a unified cybersecurity space with the EU and NATO. Therefore, revising the legal architecture governing cybersecurity to account for military threats, emerging technologies, and evolving global norms constitutes an urgent priority. Such reform is essential for strengthening the nation's digital resilience and ensuring the continuity and protection of governmental functions, particularly during times of armed conflict.

One of the main problems is the lack of proper mechanisms for the implementation of established norms. The legislation provides general guidelines and principles but does not define specific ways and procedures for ensuring cybersecurity in practice. This includes the absence of clear procedures for monitoring cyber threats, managing security incidents, as well as for continuously updating and adapting security policies in the face of new cyber threats and technological changes. Furthermore, existing rules and guidelines often diverge from internationally recognized standards, hindering the alignment of a nation's cybersecurity posture with global collaborative frameworks and weakening its capacity to contribute to collective defense mechanisms in cyberspace.

Of particular concern is the lack of established technical standards, which poses significant risks to information security across both governmental and commercial sectors. The absence of clear technical benchmarks for cyber protection obstructs accurate assessments of current infrastructure vulnerabilities and impedes the effective integration of advanced information security technologies. These include cryptographic systems, multifactor authentication, intrusion detection and prevention systems (IDS/IPS), and other state-of-the-art protective mechanisms. For the effective solution of these problems, it is necessary to develop clear technical standards and methodologies that meet the requirements of both national legislation and international standards. Furthermore, it is crucial to establish dynamic mechanisms that ensure the continuous review and adaptation of the regulatory framework. Such mechanisms are essential for keeping pace with the rapid evolution of emerging cyber threats and the advancement of cutting-edge technologies. This allows for an adequate level of cybersecurity to be ensured in the context of digital transformation and the globalization of cyber threats.

A major systemic obstacle impeding the digital transition of Ukraine's public administration lies in its institutional deficiencies within the realm of digital governance. These weaknesses manifest in limited coordination capacities, insufficiently defined responsibilities, and a lack of strategic coherence across governmental bodies responsible for implementing digital reforms. A significant part of state bodies demonstrates a limited capacity for proper legal support of digital processes, which is due, in particular, to an acute shortage of legal professionals with competencies in the field of digital, information, and cyber law. The absence of specialized lawyers complicates the development and implementation of legal and regulatory acts capable of effectively regulating digital management tools, personal data protection, the use of artificial intelligence, as well as electronic identification and authentication. Consequently, a fragmented approach to the legal support of digital initiatives emerges, accompanied by a sluggish response to the complex challenges posed by rapidly evolving technologies. This disjointed framework undermines the coherence and adaptability of public administration in the face of digital transformation.

The core issue is further exacerbated by persistent financial constraints, which significantly hinder the capacity of government institutions to adequately train personnel, implement digital reforms, and ensure the long-term sustainability of innovation. Low salaries, limited opportunities for career advancement, and insufficient investment

in digital skills development collectively diminish motivation to adopt and integrate new technological solutions. In essence, the state's institutional deficiencies in digital governance impede the effective deployment of technology and threaten to stall the broader modernization of public administration. This modernization is vital for Ukraine's alignment with European and international digital policy standards. Addressing these systemic challenges requires a comprehensive reform of human resource management, the creation of resilient professional development frameworks, and the allocation of adequate financial resources to the institutions spearheading digital transformation.

The disparity between Ukrainian legislation and European Union standards on personal data protection constitutes a significant barrier to Ukraine's integration into the EU's unified digital space. While Ukraine has expressed strong support for transparency in the digital domain and for aligning with European regulatory norms, its current legal framework does not fully conform to the fundamental provisions enshrined in the General Data Protection Regulation (GDPR). In particular, the Ukrainian legal system reveals notable shortcomings in implementing the rights of data subjects. Key aspects such as the "right to erasure" and the right to data portability remain either insufficiently regulated or ambiguously defined. These rights are essential elements of the modern European legal architecture on digital rights, underpinning the principle of individual control over personal data. Their effective implementation is crucial not only for protecting user autonomy, but also for ensuring legal interoperability in the context of cross-border digital services and broader international cooperation.

Failure to comply with GDPR requirements complicates interaction with European partners, creates barriers to cross-border data exchange, and limits the opportunities for Ukrainian authorities and the private sector to integrate into joint digital platforms and information ecosystems of the EU. This situation also negatively affects trust in Ukrainian institutions in the context of ensuring information security and protecting digital rights. Considering the current circumstances, aligning Ukraine's domestic legislation with the General Data Protection Regulation (GDPR) is an objective necessity. In particular, this entails enacting a revised version of the Law of Ukraine "On Personal Data Protection" (Verkhovna Rada of Ukraine, 2025c) to ensure full compliance with European standards. Such a legislative revision is not only essential for harmonizing regulatory frameworks, but also for establishing a robust legal basis for the free and secure exchange of data between Ukraine and EU member states. This alignment would significantly strengthen Ukraine's position within the European digital ecosystem and facilitate its broader integration into the EU's digital single market.

Ukraine's transition toward digital governance in the public sector is constrained by a fragmented and complex legal environment. A key challenge lies in the absence of comprehensive legislative frameworks capable of accommodating innovative technologies such as artificial intelligence and automated decision-making systems. The digitalization process is further impeded by insufficient interagency cooperation, internal inconsistencies within the legal system, and a lack of full compliance with the European Union's directives on personal data protection. To overcome these systemic obstacles, a series of strategic legal reforms is required. These should include the formalization of laws tailored to digital technologies, the modernization of cybersecurity legislation, and the harmonization of national regulations with European legal standards. Such measures are essential not only for Ukraine's integration into the EU digital market, but also for strengthening its digital administrative infrastructure to effectively confront global technological and security challenges.

5. Conclusions

This study has conducted a comprehensive legal analysis of digital public administration in Ukraine, which has revealed both significant achievements and pressing problems in the existing regulatory environment. Ukraine's legal framework

has made commendable progress with the adoption of pivotal legislative acts, notably the Law on Electronic Governance and the Law on Personal Data Protection. These serve as foundational pillars for establishing operational mechanisms for digital platforms, enabling electronic authentication systems, and ensuring the protection of personal data within the digital environment. However, significant legislative gaps remain, particularly in areas concerning emerging technologies such as artificial intelligence and the cross-border transfer of data. The absence of comprehensive regulation in these domains impedes technological innovation and poses serious risks to the transparency, accessibility, and resilience of public administration. Addressing these shortcomings is essential to reinforce Ukraine's digital transformation and align it with international standards. It has become evident that, despite the existence of cybersecurity laws, their implementation remains inconsistent and lacks the necessary technical detail. The operational capacity of governmental institutions is further constrained by limited financial resources and a shortage of qualified personnel, which significantly impedes the successful execution of digital initiatives. Additionally, persistent discrepancies between Ukrainian and EU legal frameworks create substantial barriers to regulatory alignment and hinder Ukraine's advancement toward full integration into the European digital ecosystem.

Drawing from the conclusions reached in this research, several key recommendations are proposed to strengthen the legal and institutional foundations of digital public administration in Ukraine:

1. Develop comprehensive legislation on emerging technologies. It is imperative to prioritize the adoption of legal frameworks regulating the use of advanced digital technologies, particularly artificial intelligence, within public sector operations. These frameworks should clearly articulate ethical principles, establish mechanisms for accountability, and safeguard individual rights in cases where algorithmic decision-making systems are employed.

2. Strengthen cybersecurity legislation and its enforcement mechanisms.

Existing regulatory acts in the field of cybersecurity should be updated by introducing precise technical standards and clearly defined control procedures. Emphasis should be placed on creating mechanisms for compliance, incident response, and regular security audits in state institutions.

3. Develop institutional capacity through legal and digital literacy.

Continuous investment in the professional development of civil servants is required. Specialized training programs should be implemented, covering the legal, ethical, and technical aspects of digital governance.

4. Harmonize national legislation with the standards of the European Union.

To advance Ukraine's ambitions for European integration, it is essential to align national legislation with European Union standards—particularly in the areas of digital governance, data protection, and cybersecurity. Such legal harmonization will facilitate more effective cross-border cooperation and support the adoption of advanced methodologies for modernizing the public sector.

These conclusions underscore both the practical and conceptual contributions of the study, emphasizing the urgent need for a progressive legal framework. This framework should be adaptable and resilient, capable of supporting a sustained transition to digital practices in the management and delivery of public administration.

Our deepest appreciation is extended to the legal scholars, practitioners, and public officials whose invaluable insights and expertise have significantly enriched this study. We are particularly grateful to the academic and governmental institutions whose practical and intellectual support made the completion of this scholarly work possible. Their contributions were instrumental to the study's success, and we sincerely thank them for their enduring commitment to advancing digital public administration.

References

- Cabinet of Ministers of Ukraine. (2017). Order No. 649-r On the approval of the Concept for the Development of e-Government in Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/649-2017-p#Text>
- Cabinet of Ministers of Ukraine. (2021). Order No. 1556-p On the approval of the Concept for the Development of Artificial Intelligence in Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text>
- De Franceschi, A., & Schulze, R. (2023). Harmonizing digital contract law: The impact of EU Directives 2019/770 and 2019/771 and the regulation of online platforms (1st ed.). Nomos.
- EU4Digital. (2025). New EU4Digital Academy 'Cybersecurity' course available in English. EU4Digital. Retrieved from <https://eufordigital.eu/new-eu4digital-academy-cybersecurity-course-available-in-english/>
- EUR-Lex. (2025). EUR-Lex - 52020DC0067 EUR-Lex — Access to European Union law. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0067>
- Hedikov, V. (2024). General analysis of legal acts in the field of digitalization in Ukraine. *Legal Bulletin*, 3, 54–61. <https://doi.org/10.32782/yuv.v3.2024.7>
- Michalak, M., & Śniadach, O. (2023). The obligation to accept *acquis communautaire*: Some thoughts on Ukraine's accession to the EU and value of the rule of law. *Al'manah Prava* 14, 67–74. <https://doi.org/10.33663/2524-017x-2023-14-67-74>
- Nehrey, M., Kostenko, I., & Kravchenko, Y. (2023). Digital transformation in Ukraine during wartime: Challenges and prospects. In Z. Hu, Y. Wang, & M. He (Eds.), *Advances in intelligent systems, computer science and digital economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies* (Vol. 158, pp. 404–416). Springer. https://doi.org/10.1007/978-3-031-24475-9_33
- Profiroi, C. M., Negoită, C. I., & Costea, A. V. (2023). Digitalization of public administration in EU member states in times of crisis: The contributions of the national recovery and resilience plans. *International Review of Administrative Sciences*. <https://doi.org/10.1177/00208523231177554>
- Schedler, K., Guenduez, A. A., & Frischknecht, R. (2019). How smart can government be? Exploring barriers to the adoption of smart government. *Information Polity*, 24(1), 3–20. <https://doi.org/10.3233/IP-190169>
- Shulzhenko, F. P., Ryndiuk, V. I., Kuzmenko, O. V., Kozhura, L. O., & Gryshko, O. M. (2021). Transformation of the national legislation of Ukraine in the context of globalization. *Revista Amazonia Investiga*, 10(46), 191–200. <https://doi.org/10.34069/ai/2021.46.10.19>
- Vavrynychuk, A. S. (2023). Significance of *acquis communautaire* for the formation of modern legislation of Ukraine. *Juridical Scientific and Electronic Journal*, 12, 471–474. <https://doi.org/10.32782/2524-0374/2023-12/117>
- Verkhovna Rada of Ukraine. (2022). Law of Ukraine No. 2807-IX On the National Informatization Program. Retrieved from <https://zakon.rada.gov.ua/laws/show/2807-20#Text>
- Verkhovna Rada of Ukraine. (2023). Law No. 1907-IX On Public Electronic Registers Retrieved from <https://zakon.rada.gov.ua/laws/show/1907-20#Text>
- Verkhovna Rada of Ukraine. (2024). Law No. 2155-VIII On electronic trust services. Retrieved from <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
- Verkhovna Rada of Ukraine. (2025a). Law No. 1089-IX On electronic communications. Retrieved from <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text>
- Verkhovna Rada of Ukraine. (2025b). Law No. 2163-VIII On the Basic Principles of Ensuring Cybersecurity of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- Verkhovna Rada of Ukraine. (2025c). Law No. 2297-VI On the Protection of Personal Data. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>