ISSN 1648-2603 (print)
ISSN 2029-2872 (online)

VIEŠOJI POLITIKA IR ADMINISTRAVIMAS
PUBLIC POLICY AND ADMINISTRATION
2026, T. 25, Nr. 1/2026, Vol. 25, No 1

LEGAL CHALLENGES OF DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION BODIES IN UKRAINE

Liudmyla Shapenko

Department of Administrative and Information Law
Faculty of Law and International Relations
Kyiv Aviation Institute
1 Lubomyr Huzar Ave., 03058, Ukraine

Iryna Hrytsai

Department of Theory of State and Law
Educational and Scientific Institute of Law and Innovative Education
Dnipro State University of Internal Affairs
26 Nauka Ave., 49005, Ukraine

Andrii Paraka

Interregional Academy of Personnel Management
2 Frometivska Str., 03039, Ukraine

Mykhailo Kostytskyi

Department of History, Philosophy and Law
Institute of Lawmaking and Scientific-Legal Expertise
National Academy of Sciences of Ukraine
3 Pylyp Orlyk Str., 01001, Ukraine

Andrii Fomenko

Department of Public Law
Institute of Humanities and Social Sciences
National Technical University "Dnipro Polytechnic"
49005, 19 Dmytro Yavornytskyi Ave., Dnipro, Ukraine

https://doi.org/10.5755/j01.ppaa.25.1.42012

Abstract. *As the public sector undergoes a digital transformation, digital technologies are systematically incorporated into government operations, service delivery, and citizen interactions with the goal of improving responsiveness, efficiency, and transparency. The aim of this article is to analyse the main legal challenges of digital transformation in public administration, with a particular focus on data protection, cybersecurity and inclusiveness, and develop practical recommendations for harmonising Ukraine's legal framework with EU standards. The study applied a theoretical and legal approach based on the principles of the rule of law, legal certainty, proportionality, and the protection of fundamental human rights. Important components of digital transformation are inclusiveness and accessibility. Compatibility is another important factor that guarantees the seamless flow of data between government systems and boosts service effectiveness. Data-driven deci-*

sion-making uses analytics to shape policy, optimise resource allocation and forecast population needs. A reliable model of digital governance exists at the EU level, backed by important treaties that uphold individual liberties, foster competition and innovation, and advance a single digital market. However, certain legal relationships are unregulated in Ukraine, while the regulatory framework is antiquated. This issue impedes the adoption of modern digital tools and global e-governance trends. Although there has been some noticeable progress, the war has significantly disrupted legal and technical infrastructure reforms. A dynamic legal framework that ensures inclusivity and accessibility while adjusting to technology advancements is required to handle these legal concerns.

Keywords: *digital transformation; public administration; legal issues; cybersecurity; principle of transparency; public authorities.*

Reikšminiai žodžiai: *skaitmeninė transformacija; viešasis administravimas; teisiniai klausimai; kibernetinis saugumas; skaidrumo principas; viešosios institucijos.*

Introduction

The digital transformation of Ukraine's public authorities involves the state exercising an influence over social institutions, society, the state apparatus, businesses and the economy. Its aim is to introduce digital information and communication technologies into social relations through state and legal activities, as well as public-private partnerships (Sobko et al., 2024). Contemporary Ukraine is facing new realities shaped by military aggression, affecting all areas of society. This has slowed the pace of digital transformation and shifted focus towards national security (National Institute for Strategic Studies, 2024). Nevertheless, digital transformation in public administration remains urgent and integral to the Ukraine's broader development, even in wartime. At the same time, the global shift towards remote interaction underscores the importance of addressing the needs of individuals from various social backgrounds. Consequently, new management approaches are emerging, making it essential to thoroughly examine the legal issues surrounding the adoption and use of new technologies in public administration (Sakharuk, 2024).

The introduction of digitisation tools opens up new options to increase citizen engagement in public processes, hence enhancing the efficiency and transparency of services. Digital platforms create the groundwork for unhindered access to public services, reducing bureaucratic delays and increasing accountability through open data efforts (Lutsenko & Pikulya, 2024). This revolutionary influence is most visible in the fast expansion of e-government platforms. These systems are intended to be user-friendly, saving time and resources. For example, citizens can easily arrange online consultations, apply for social benefits or renew licences without having to visit in person. However, the increasing dependence on digital public administration highlights the necessity of addressing data privacy and cybersecurity issues, as these systems are susceptible to cyberattacks (Kohut, 2022).

This study stresses the need of inclusion and accessibility in bridging the digital gap, especially for marginalised communities with insufficient resources or digital literacy abilities (Nynyuk & Nynyuk, 2024). To do this, the legislative framework must encourage digital literacy and fair access while balancing concerns such as innovation, privacy, security, and equity in the digital transformation of public administration.

The increasing reliance on digital tools creates complex legal issues that need for strong systems for inclusive, safe, and sustainable governance. Finding a balance between innovation and legislative protections that preserve the system's integrity and individuals' rights is frequently a challenge for policymakers (National Institute for Strategic Studies, 2024). Maintaining the right balance is a necessary step towards sustainable digital governance that serves different segments of the population fairly. To achieve this goal, policymakers need practical solutions that will help them integrate the latest technologies with existing legal requirements. Particular attention should be paid to security and the protection of personal data. Only in this way can digital transformation benefit society without undermining trust and fairness.

The legal elements of digital transformation in public administration have received little attention, particularly in terms of integration across different dimensions (Kopotun et al., 2019). The bulk of studies focus on specific topics like data protection or cybersecurity, with few addressing inclusion and accessibility. Furthermore, there is currently a paucity of practical advice on how to overcome typical problems in digital transformation (Nalyvaiko et al., 2022).

The aim of this article is to analyse the main legal challenges of digital transformation in public administration, with a particular focus on data protection, cybersecurity and inclusiveness, and develop practical recommendations for harmonising Ukraine's legal framework with EU standards. The research question is as follows: "What are the main legal benefits and problems of digital transformation in public administration, and how can we improve the legal framework to make sure digital governance is effective, transparent, and secure?".

The research novelty stems from the incorporation of the legal elements of digital transformation, such as privacy, cybersecurity, and inclusion. Thus, the research fills a vacuum in the legal literature and provides practical advice for tackling the obstacles of digital transition. It offers a fresh perspective on the legal foundation for public administration's digital transformation, highlighting practical procedures that are becoming increasingly important as governments grapple with rapid technological change. The academic and practical value of this essay stems from its thorough examination of the legal concerns and framework of digital transformation in public administration. It investigates how the legal framework might enhance benefits while reducing hazards. The recommendations can assist the government in creating secure, accessible, and efficient public administration, ensuring that all citizens benefit from the digital transformation.

Methodological Framework

The study applied a theoretical and legal approach based on the principles of the rule of law, legal certainty, proportionality, and the protection of fundamental human rights. This approach allowed to consider the digital transformation of public administration not only as a technological or managerial process, but primarily as a legal phenomenon that requires proper regulatory regulation. The use of a theoretical and legal framework made it possible to formulate recommendations in the field of law, in particular regarding the protection of personal data, cybersecurity and guarantees of inclusiveness, reflecting the specific nature of the study in the legal sphere.

The legal dogmatic method is used to substantiate the analysis of the categories of legal certainty, the rule of law, the protection of human rights, and proportionality, and to explain why the challenges of digital transformation in public administration need to be assessed through the prism of legal principles. The descriptive method was used to study the legal framework of Ukraine, the EU, and selected international practices (Estonia, Singapore). The systematic analysis method allowed us to identify the interrelationships and contradictions between digital governance tools, data protection rules, and cybersecurity requirements. The comparative method made it possible to assess Ukraine's legal progress in line with EU standards and best practices. Finally, a dialectical approach was used to identify contradictions between rapid technological development and slower legal adaptation. The combination of these methods provided the basis for formulating specific and practically meaningful recommendations.

The statutory interpretation method was used to understand the conceptual foundations and regulatory context of digital transformation in public administration. A detailed review of the regulatory frameworks of Ukraine, the EU, Estonia, and Singapore was conducted using the comparative legal method and case law analysis. Ukraine is the main object of analysis, as it is its legal system that defines the framework for the digital transformation of public administration and identifies key gaps and challenges. The European Union was chosen as a regulatory benchmark, as Ukraine is in the process of harmonising its legislation with European standards in the field of personal data protection, cybersecurity and digital services.

Estonia's experience is a valuable example within the EU, as it has implemented an effective 'gov-

ernment as a service' model and created a robust legal infrastructure for interoperability, transparency and citizen trust. At the same time, Singapore has been included as a global example outside the EU, demonstrating a successful combination of innovative technologies and legal mechanisms to ensure inclusiveness, accessibility and security, offering a globally recognised 'Smart Nation' model that emphasises inclusiveness, accessibility and real-time data management. Thus, the combination of these four jurisdictions forms a balanced comparative basis for research, allowing for the assessment of regional and global approaches to the legal framework for the digital transformation of public administration.

The use of the philosophical legal method made it possible to consider digital transformation as a process that is constantly accompanied by contradictions between the dynamics of technological change and the relatively slow adaptation of legislation. Through the prism of these contradictions, it was possible to identify the main gaps in legal regulation, particularly in the areas of algorithmic decision-making systems, personal data protection, and the coordination of state registries. This method helped to trace how existing legal norms are gradually losing their relevance in the new conditions, and at the same time showed the need for adaptive legislation capable of responding flexibly to the challenges of digital transformation. The identification of the necessary procedures and systems to guarantee that the digital transformation of public administration goes smoothly and with few obstacles was made easier by the analytical legal method.

Results and Discussion

3.1. *Conceptual framework and regulatory context of digital transformation in public administration*

As the public sector undergoes a digital transformation, digital technologies are systematically incorporated into government operations, service delivery, and citizen interactions with the goal of improving responsiveness, efficiency, and transparency. It demonstrates a new approach to public administration through the use of cutting-edge technology such as blockchain, artificial intelligence, cloud computing, and data analytics (Sydorenko et al., 2023). The key components of this shift include data-driven decision-making, user-centred services, interactive procedures, and accessibility (Yevdokimov & Kolomiyets, 2024).

Digital transformation in public administration also involves organisational and cultural changes. It promotes easily adaptable management methods, public participation in the development of universally accessible digital solutions, and improved digital literacy among the general public and government employees (Nalyvaiko & Lebedieva, 2022). These measures aim to make services more efficient by reducing bureaucracy, making services more accessible, and ensuring transparency through open data. The ultimate objective of the programme is the building of trust in public administration among citizens. However, a robust legal framework that addresses technological challenges and protects public interests is necessary for this transformation to be successful (Semenets-Orlova et al., 2022).

Important components of digital transformation are inclusiveness and accessibility. When public services are digitised, it is critical that no one falls behind. This necessitates assessing the requirements of all demographic groups and making decisions appropriately. Inclusiveness also refers to society's engagement in digital changes through consultations, public discussions, and polls, allowing for the development of policies that benefit everyone. Accessibility is concerned with individuals' practical capacity to use digital services, which includes both access to digital infrastructure and platform usability (Hryshchenko, 2024) Inclusiveness and accessibility improve justice in interactions between citizens and the state, boosting trust in institutions. Practical, straightforward, and easily available online services help to reduce corruption, administrative responsibilities, and improve quality of life (Sydorenko et al., 2023).

Compatibility is another important factor that guarantees the seamless flow of data between government systems and boosts service effectiveness. An excellent illustration of this approach is Estonia, which

pioneered digital government and was the first to embrace the idea of a country as a service. According to this paradigm, 99% of services are offered online, and only some services, such as marriage, divorce, and real estate, require a physical presence. Every year, the country saves about 2% of its GDP owing to these changes (Hryshchenko, 2024). The X-Road technology facilitates Estonia's compatibility by connecting all state registries through standardised data exchange protocols, guaranteeing single data entry and current data (Melnyk et al., 2022). However, Estonia's experience is frequently idealised. Scalability presents challenges for larger governments, while Estonia's small population makes universal standards easier to execute. Another concern is depending too much on certain digital system suppliers, which might limit the government's flexibility and ability to adjust.

Data-driven decision-making uses analytics to shape policy, optimise resource allocation and forecast population needs. Real-time data is used in Singapore's Smart Nation effort to improve urban planning (Kovbas & Redko, 2025). Making digital services accessible entails catering to the requirements of all demographics, including those with low levels of computer literacy and impairments. Similarly to Estonia, Singapore is pursuing the state in a smartphone paradigm, offering more than 1,500 services through a single site that connects more than 140 institutions (Naumyk et al., 2024).

A reliable model of digital governance exists at the EU level, backed by important treaties that uphold individual liberties, foster competition and innovation, and advance a single digital market. Thus, the General Data Protection Regulation (GDPR) is a set of rules intended to protect personal information by placing strict restrictions on how it may be processed and stored. It states that individuals should be able to know how data is used, that it should be utilised for a specific purpose, and that data should be limited to a minimum. The extraterritorial effect of the GDPR indicates that it is not limited to the EU. It affects Ukraine that is working closely with the EU and amending its legislation to conform to EU norms (European Parliament and Council, 2016).

Secondly, the Electronic Commerce Directive (European Parliament and Council, 2000), which sets regulations for e-services, intermediary responsibility, consumer protection, and electronic contracts, is another important piece of EU legislation. The Digital Markets Act (Shchybun, 2022) regulates large digital platforms, preventing monopolies and guaranteeing fair competition. Moreover, the European Parliament and Council (2014) established guidelines for the use of electronic signatures, seals, and trust services throughout the continent. Apart from that, the regulatory framework controlling telecommunications services is established by the European Electronic Communications Code (Directive 2018/1972) (European Parliament and Council, 2018).

Through the establishment of training programs to enhance digital skills and the setting of goals for universal digital access, the EU's Digital Decade Strategy promotes inclusivity and accessibility. It also ensures ubiquitous access to services like electronic voting and social benefit applications (European Commission, 2022). In this regard, the Artificial Intelligence Act (2024) created a legislative framework for the application of AI in electronic public services in response to the fast technological advancements (Samman & De Vanssay, 2024). These international standards provide Ukraine with rules for aligning their legal systems, ensuring that they are dependable and compatible with digital administration.

These policies underpin digital transformation in public administration by addressing data privacy, e-government, cybersecurity, innovation, and inclusiveness. Although they are uniform and generally applicable (Kussainov et al., 2023), compliance is uneven. Thus, economically disadvantaged EU nations frequently confront budgetary difficulties when it comes to reaching the required standards. As a result, while harmonisation is necessary, obtaining complete cross-border compatibility requires time.

Before Russia's full-scale invasion, digital transformation was a key driver of Ukraine's state policy, with the aim of improving services, boosting economic growth, attracting investment and enhancing global competitiveness. However, the war has disrupted this process across all sectors of society (Treshchov & Naumyk, 2023). Despite the challenges that Ukraine is currently facing, there is growing momentum behind digital transformation, which is set to become a springboard for more efficient administrative

services. Electronic document management, modern technologies, and convenient identity verification systems are being adopted by state bodies, while access to information is being expanded through open registers and data. The optimisation of interdepartmental cooperation, automation of service delivery, and improvement in the productivity of civil servants at both the individual and collective levels is enabled by these advances (Treshchov & Naumyk, 2023).

Ukraine's policies and legal framework demonstrate the notable advancements in digital transformation. In 2010, the Verkhovna Rada of Ukraine adopted the Law of Ukraine "On Personal Data Protection", which is in line with the GDPR and places an emphasis on consent and data minimisation for data processing in the public sector. In 2023, the Verkhovna Rada of Ukraine approved the Law of Ukraine "On Electronic Documents and Electronic Document Management", which creates the legal framework for electronic records, digital signatures, and e-government services, are important pieces of legislation.

Moreover, the Law of Ukraine "On Information" (Verkhovna Rada of Ukraine, 1992) guarantees the safety and clarity of the information. The Law of Ukraine "On Electronic Means of Communication" (Verkhovna Rada of Ukraine, 2020) regulates state policy in the field of electronic means of communication and radio frequency spectrum. Ukraine has also made progress in bringing its laws into compliance with EU norms, facilitating its entry into the EU digital market. This alignment directs the adaptation of national legislation to contemporary digital developments and improves conformity with EU standards, such as the European Digital Identity Regulation (European Parliament and Council, 2014).

There was also a lot of discussion about accessibility and the even more active digitalisation of administrative services, including the Single Digital Gateway enhancements and the harmonisation of important points with EU requirements in line with the European Interoperability Framework (National Institute for Strategic Institute, 2024). In this regard, Ukraine became a member of the Potential consortium, which is primarily responsible for creating a digital identity wallet for Europeans. Furthermore, the EU and Ukraine have made great strides in introducing an e-trust list of services (National Institute for Strategic Institute, 2024). In November 2024, the Verkhovna Rada of Ukraine confirmed Ukraine's progress towards creating a strong economic space using digital innovative technologies by passing the Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding the Functioning of the National System of Confidential Communications and the National Electronic Communications Network" (Verkhovna Rada of Ukraine, 2024).

3.2. Legal challenges of implementing digital technologies in public administration

Ukraine's digital transformation is a resounding success, as evidenced by the Diia portal and mobile application. These platforms have a user-friendly interface, a large range of services, and room for improvement (National Institute for Strategic Studies, 2024). However, the ongoing invasion and resource shortages are posing problems for its judicial system. Moreover, when rules are amended too frequently and without consulting other authorities, the efficacy of digital transformation is diminished. This draws attention to the more consistent implementation. Furthermore, Ukraine's digital transformation of public administration is still unequal. Alignment with EU standards, the creation of electronic services, enhancements to Diia, the digitisation of public registers, and the Prozorro system are all significant developments. Large-scale, stable execution of the full transition is still pending. Legal challenges that must be addressed to ensure fair, secure, and effective governance are created by the integration of new technologies into public service delivery. The identification and analysis of the key challenges and the guiding of strategies for their addressing was done by means of risk criteria.

In this study, the term legal is used in a broad sense, referring not only to existing laws and regulations, but also to those legal aspects that directly or indirectly affect the functioning of public administration in the context of digital transformation. This means that legal challenges cover both regulatory issues (e.g., outdated legislation or lack of regulation for new technologies) and the legal consequences of institutional or organisational shortcomings, if they are directly reflected in legal norms or create legal loopholes. That is why the issue of coordinating state registries is considered a legal issue: the lack of unified legal regula-

tion of their interaction creates legal barriers to information exchange, reduces legal certainty, and complicates the proper functioning of electronic documents and services in different jurisdictions. Thus, in this study legal covers the entire spectrum of legal regulation and its impact on digital public administration.

Consequently, the classification of legal challenges by risk level (high, medium, low) is based on a combination of two main criteria: the probability of the relevant challenge arising in the context of the digital transformation of public administration, and the scale of its possible consequences for the functioning of public institutions and the protection of citizens' rights. This approach is consistent with generally accepted approaches to risk management in the public sector and cybersecurity (Verkhovna Rada of Ukraine, 2017; European Commission, 2022). For example, threats to cybersecurity and personal data leaks are classified as high risk because they are both highly probable and capable of causing significant damage to the security of state information systems and citizens' rights. On the other hand, issues of digital literacy or citizen trust are classified as low risk because they have less of a critical impact on the sustainability of systems, although they remain important for achieving the inclusiveness of digital services. Thus, the risk scale in our study reflects a combination of the probability and impact of each challenge, providing a more systematic view of their priority.

Empirical data confirm the scale and ambivalence of digital transformation. As of 2024, more than 19 million Ukrainians use the Diia platform, which is more than half of the country's adult population, and the number of available administrative and business services has exceeded 120 (National Institute for Strategic Institute, 2024). This indicates that Diia has become a key tool for the state in its interaction with citizens. At the same time, according to data from the State Service for Special Communications and Information Protection of Ukraine, in 2023 alone, more than 2,500 incidents targeting state digital systems, including the Diia platform, were recorded (Zaporozhets, 2024). It remains a serious concern that such incidents directly disrupt the operation of many information systems and platforms, including Diia, threatening services such as digital IDs and social benefits.

According to a survey conducted by the Kyiv International Institute of Sociology (2023), approximately 40% of respondents consider personal data protection in Ukraine to be insufficient. Accordingly, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" (Verkhovna Rada of Ukraine, 2017) regulates the protection of critical infrastructure, including state digital systems, and requires risk assessments and incident reports. Online attacks continue to target state registries, government entities, and platforms in spite of these regulations. This is particularly true in light of the extensive intrusion, which jeopardises government operations and user data. Timely and coordinated actions are further hampered by authorities' inconsistent cybersecurity requirements (Lytvyn et al., 2022).

A crucial component of public administration digital transformation is making sure that personal data is protected while processing massive amounts of data. Hence, finding a balance between the necessity to access data in order to deliver public services and privacy is the challenge (Rybkina, 2024). For instance, Diia requires extensive data exchange, which raised concerns about overcollection and abuse. An issue with a regional government website in 2023 demonstrated that there were issues with the quality of the checks and made it evident that new and improved methods were required.

Apart from that, certain legal relationships are unregulated in Ukraine, while the regulatory framework is antiquated. This issue impedes the adoption of modern digital tools and global e-governance trends. Although there has been some noticeable progress, the war has significantly disrupted legal and technical infrastructure reforms (Kovbas & Redko, 2025). Information systems are at risk of becoming fragmented and non-interoperable due to a lack of coordination among state registers (Rachinsky & Tytarenko, 2024).

Due to their legal position and regulation, digital documents and electronic signatures represent a medium-level danger to digital transition in Ukraine. Digital papers and electronic signatures are essential to safe computerised administrative procedures. Zaporozhets (2024) asserts that, as long as digital documents satisfy the required technological requirements, Ukrainian legislation acknowledges their le-

gal equivalent to paper documents. Moreover, this law regulates the use of electronic signatures, which provides a structure that makes platforms like Diia more efficient. However, interoperability issues arise due to differences between regional frameworks and national standards. The law also varies in how it recognises advanced electronic signatures that require biometric or cryptographic verification, which also creates uncertainty. The main problem is that there are no clear rules about how digital documents should be used in court (Halushchak et al., 2023).

Medium-risk difficulties also include problems with algorithmic decision-making, which employs AI to allocate resources, evaluate risks, and share social benefits (Bazaluk et al., 2023). These technologies increase efficiency, streamline procedures, and save time, but they also raise legal questions about accountability and transparency. Transparency means that citizens can understand the rules that guide decisions made by algorithms. Many AI systems operate as black boxes, which creates legal issues when it comes to appealing algorithmic decisions. In Ukraine, concerns have arisen over unclear criteria in the use of AI to assess social benefits. Without transparent algorithms, citizens may lose trust in administrative processes, and responsibility for biased or erroneous decisions remains unclear (Halushchak et al., 2023). The war has further worsened the situation by limiting the development of AI and postponing attempts at transparency, a problem also evident in slow implementation of AI governance by the EU (Kovbas & Redko, 2025).

A low-risk issue that restricts citizens' and government officials' ability to embrace new procedures and systems is their comparatively low level of digital literacy. According to Halushchak et al. (2023), more than 60% of public personnel lack fundamental digital abilities. The Ukrainian society is also impacted by the digital divide: elderly people frequently struggle to utilise digital administrative tools, and more than 25% of Ukrainian villages lack internet connection (Rachinsky & Tytarenko, 2024). Furthermore, concerns about the protection of personal data hinder public confidence in digital services and registries.

Therefore, a flexible legal framework that can keep up with technology advancements while maintaining accessibility and inclusivity is needed to handle these issues. Governments may create a safe, equitable, and efficient public administration in this way. Thus, state policies must be adjusted to the warfare and risk considerations must be taken into account in order to provide steady results.

3.3. Practical recommendations on the way to a modern legal framework for the digital transformation of public administration bodies

Public administration digital transformation in Ukraine is regulated by the Law of Ukraine "On Electronic Documents and Electronic Document Management" (Verkhovna Rada of Ukraine, 2023) and the Law of Ukraine "On Information" (Verkhovna Rada of Ukraine, 1992), the Law of Ukraine "On Electronic Communications" (Verkhovna Rada of Ukraine, 2020) and the Law of Ukraine "On Personal Data Protection" (Verkhovna Rada of Ukraine, 2010). It is also important to note that in November 2024, the Law of Ukraine "On Amendments to Certain Laws of Ukraine on the Functioning of the National Confidential Communications System and the National Electronic Communications Network" was adopted to harmonise Ukrainian legislation with EU principles.

Despite its challenges, Ukraine has a real chance to transition to a digital economy. In this regard, strengthening the Ministry of Digital Transformation is necessary. This ministry has demonstrated its ability to adjust to digital developments and create successful plans while ensuring that all branches of government remain coordinated. If this strategy is used as a basis, the full potential of digital technology in the public sector may be fulfilled. By using Estonia as an example, these actions may strengthen cybersecurity, data protection, and digital governance, laying the groundwork for long-term digital management.

First of all, priority should be given to creating the Strategy for the Digital Transformation of Public Administration that outlines precise actions, goals, and anticipated results for the digital transformation of public administration. This approach should be all-encompassing rather than industry-specific, and it should be flexible and responsive to innovation. It ought to be the cornerstone of a digital state that

is focused on its citizens. This Strategy should be based on the principles of digital by default, involving single data entry, interoperability, inclusivity, and accessibility (Hryshchenko, 2024). In addition, it should guarantee stability during times of peace and war while fostering long-term efficacy through concerted efforts in cybersecurity, data protection, and inclusiveness.

Revising the regulatory framework is another crucial step. Even if the reforms have recently accelerated, changes must be finished faster and with uniform guidelines for all participants. In this regard, the adoption of the digital by default approach would make digital formats the main way that internal government operations and public services are conducted. Innovative technology testing should also be permitted within a provisional regulatory framework. These may include public services powered by AI. It is best to test them in supervised sandboxes. These sandboxes would strike a balance between supervision and creativity (Sakharuk, 2024).

Furthermore, frequent audits of state digital platforms should be carried out to make sure that accessibility regulations are being followed and to find any possible data leaks in order to improve cybersecurity and data privacy. Blockchain or AI technology may be used in these audits (Nynyuk & Nynyuk, 2024). The procedure should be supervised by a specialised organisation inside the Ministry of Digital Transformation of Ukraine. In order to improve future security and foster confidence in e-governance, audits should be conducted on a quarterly basis and include reports on key risks, given the vulnerabilities in Diia in 2023 (Kovbas & Redko, 2025).

With its uniform, simplified interface, the Diia platform is set to become the cornerstone of Ukraine's digital state, seamlessly integrating all governmental services for enterprises and residents. With only a few clicks, users should be able to access services, and relevant services should be instantly connected. Re-engineering and optimisation should be the main goals of platform improvements (Yevdokimov & Kolomiyets, 2024). Tsypko et al. (2019) assert that modernising cryptographic protocols and upgrading electronic identity systems like BankID or SmartID would improve security and interoperability.

Another recommendation is to disclose public information in computer-readable formats to increase objectivity and transparency. Open data, which powers the digital economy, necessitates prudent governmental control. Effective collaboration between the public, corporations, and government is essential to creating a common digital vision and advancing digital culture and education to raise digital literacy.

Enhancing government officials' digital literacy is essential to the public sector effective digital transformation. Hence, a national training program or a platform that is updated often should provide employees with access to learning materials and skill development opportunities. Human resources would also be strengthened by hiring data analysts, product managers, service designers, and IT professionals. Improving people's digital literacy is also crucial, particularly in rural regions where connection is restricted and Diia use is slowed down. Long-term training initiatives can enhance accessibility and aid in closing this gap.

In addition, implementing institutional and procedural protections can support digital legality, the preservation of citizens' rights, and inclusiveness in public administration. Through specialised digital governance organisations and websites for challenging governmental decisions, these actions address algorithmic unfairness, data privacy breaches, and accessibility barriers (Hryshchenko, 2024). In this regard, Ukraine can follow Estonia's example, where GDPR compliance is monitored by the Data Protection Inspectorate.

One of the main objectives of digital transformation is transparency in public administration. Digital technologies, such as open data, e-government, and online platforms, provide citizens with fast, thorough information, which reduces corruption and fosters trust. Publication of laws, financial information, ad statistics in machine-readable forms, and interactive avenues for public comment serve to advance transparency.

It is vital to follow important legislative requirements in order to address these issues. These measures must be properly implemented and adequately funded if they are to provide safe and flexible digital public

administration. Simultaneously, the consequences of the war and the inherent challenges must be considered.

Conclusions

- Public administration digital transformation marks a new era of change in service delivery and how the government interacts with its citizens. It makes clever use of digital technology to improve, streamline, and expedite government operations. This process, which is characterised by interactivity, data-driven decision-making, user-centricity, inclusivity, and accessibility, also calls for organisational and cultural changes. Ensuring compatibility is equally crucial for improving the efficiency of integrated services and facilitating smooth information transmission between government systems.
- The legal documents such as the GDPR, E-Commerce Directive, Digital Markets Act, Regulation on Electronic Identification and Trust Services, European Electronic Communications Code, Digital Decade Strategy, and AI Regulation, offer a trustworthy model of digital governance. The Law "On Amendments to Certain Laws of Ukraine on the Functioning of the National Confidential Communications System and the National Electronic Communications Network" was adopted in November 2024, further advancing Ukraine's compliance with EU norms.
- The war has a significant influence on the digital revolution of public administration. Other difficulties include out-of-date laws, disorganised state registries, and low levels of digital literacy among residents and government personnel. These issues are linked to more significant concerns, such as the legal standing of digital signatures and documents, the use of computer algorithms for decision-making, data security, cybersecurity, digital infrastructure, and inclusivity. All of them require a robust legal framework to enable sustainable digital governance.
- A dynamic legal framework that ensures inclusivity and accessibility while adjusting to technology advancements is required to handle these legal concerns. The development of a unified state-level Strategy for the Digital Transformation of Public Administration with specific objectives and quantifiable results, the updating of the regulatory framework, the implementation of regular cybersecurity audits and accessibility compliance, the creation of temporary regulatory sandboxes for testing new technologies, the development of the Diia platform, the updating of electronic identification systems, the improvement of digital literacy among citizens and civil servants, the strengthening of transparency and objectivity, and the introduction of institutional and procedural safeguards are all important courses of action.

Data Availability Statement

The data used to support the findings of this research are available from the corresponding authors upon request.

The authors declare they have no financial and competing interests. The authors did not receive support from any organization for the submitted work.

No funding was received to assist with the preparation of this manuscript.

No funding was received for conducting this study.

No funds, grants, or other support was received.

References

1. Bazaluk, O., O. Anisimov, P. Saik, V. Lozynskyi, O. Akimov, and L. Hrytsenko. 2023. "Determining the Safe Distance for Mining Equipment Operation When Forming an Internal Dump in a Deep Open Pit." Sustainability 15, no. 7: 5912. *https://doi.org/10.3390/su15075912*
2. European Commission. 2022. Advancing Europe's Digital Decade. The EU: A Pioneer towards a Safe and Secure

Digital World. *https://state-of-the-union.ec.europa.eu/state-union-2022/state-union-achievements/advancing-europes-digital-decade_uk*

3. European Parliament and Council. 2000. Directive (EU) No. 2000/31/EC "On Certain Legal Aspects of Information Services, in Particular Electronic Commerce, in the Internal Market". *https://zakon.rada.gov.ua/laws/card/994_224*
4. European Parliament and Council. 2014. Regulation (EU) No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". *https://eur-lex.europa.eu/eli/reg/2014/910/oj*
5. European Parliament and Council. 2016. Regulation (EU) 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC". *https://eur-lex.europa.eu/eli/reg/2016/679/oj*
6. European Parliament and Council. 2018. Directive (EU) No. 2018/1972 "Establishing the European Electronic Communications Code". *https://eur-lex.europa.eu/eli/dir/2018/1972/oj*
7. Halushchak, O., M. Halushchak, and N. Mashliy. 2023. "Digitalization in Ukraine: Evolutionary Transformations." Galician Economic Journal 2, no. 81: 155-163. *https://doi.org/10.33108/galicianvisnyk_tntu*
8. Hryshchenko, O. O. 2024. "Some Aspects of Current Trends of Digital Transformation of Public Administration in Ukraine." In Digitalization of Science as a Challenge of Today, edited by I. O. Korenuik, 84-86. Vinnytsia: UKRLOGOSGroup.
9. Kohut, Y. I. 2022. Cyberwars, Cybercrime (Concepts, Strategies, Technologies). Kyiv: Sidkon.
10. Kopotun, I. M., B. M. Holovkin, L. R. Nalyvaiko, I. O. Hrytsai, and O. V. Tkachova. 2019. "Health-Improvement Competences Formation Technique in Future Police Officers by Means of Personality-Oriented Approach to Physical Education." International Journal of Learning, Teaching and Educational Research 18, no. 11: 205-217. *https://doi.org/10.26803/ijlter.18.11.12*
11. Kovbas, I. V., and O. M. Redko. 2025. "Electronic Governance in the Countries of the European Union and in Ukraine." Academic Visions 41: 1-6. *https://doi.org/10.5281/zenodo.15276074*
12. Kussainov, K., N. Goncharuk, L. Prokopenko, L. Pershko, B. Vyshnivska, and O. Akimov. 2023. "Anti-Corruption Management Mechanisms and the Construction of a Security Landscape in the Financial Sector of the EU Economic System against the Background of Challenges to European Integration." Economic Affairs 68, no. 1: 509-521. *https://doi.org/10.46852/0424-2513.1.2023.20*
13. Lutsenko, V. R., and T. O. Pikulya. 2024. "Legal Support of Digital Transformation in Ukraine." Scientific Bulletin of Uzhgorod National University 81, no. 1: 61-67. *https://doi.org/10.24144/2307-3322.2024.81.1.9*
14. Lytvyn, N., H. Andrushchenko, Y. V. Zozulya, O. V. Nikanorova, and L. M. Rusal. 2022. "Enforcement of Court Decisions as a Social Guarantee of Protection of Citizens' Rights and Freedoms." Prawo i Więź 39: 80-102. *https://doi.org/10.36128/priw.vi39.351*
15. Melnyk, D. S., O. A. Parfylo, O. V. Butenko, O. V. Tykhonova, and V. O. Zarosylo. 2022. "Practice of the Member States of the European Union in the Field of Anti-Corruption Regulation." Journal of Financial Crime 29, no. 3: 853-863. *https://doi.org/10.1108/JFC-03-2021-0050*
16. Nalyvaiko, L. R., and Yu. V. Lebedieva. 2022. "Reproductive Human Rights: International Standards, Experience of Ukraine and Lithuania." Evropsky Politicky a Pravni Diskurs 9, no. 4: 60-73. *https://doi.org/10.46340/eppd.2022.9.4.6*
17. National Institute for Strategic Studies. 2024. Digital Transformation of the Economy of Ukraine in Wartime Conditions. *https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-zhovten-2024*
18. Naumyk, A. S., Ya. M. Kondratova, and N. S. Sydorenko. 2024. "The Rule of Law and Civil Society: The History of State and Legal Thought in the Context of Public Management and Administration." Universum 7: 19-23.
19. Nynyuk, I., and M. Nynyuk. 2024. "Digital Transformation of Public Administration in Ukraine: Challenges and Prospects." Successes and Achievements in Science 4, no. 4: 509-521. *https://doi.org/10.52058/3041-1254-2024-4(4)-509-521*
20. Rachinsky, A. P., and O. M. Tytarenko. 2024. "Digital Transformation of Public Administration in the Direction of Servitization." State Construction 2, no. 36: 553-567. *https://doi.org/10.26565/1992-2337-2024-2-38*
21. Rybkina, S. 2024. "Development of Electronic Governance as a Driver of Competitiveness of the Countries of

the European Union." Public Administration and Regional Development 26: 1365-1381. *https://doi.org/10.34132/pard2024.26.13*

22. Sakharuk, A. 2024. "Legal Regulation of Digital Transformation in the Public Sector." *https://consultant.net.ua/consultant-article/5146*
23. Samman, T., and B. De Vanssay. 2024. "Main Points of the European Artificial Intelligence Act." *https://www.robert-schuman.eu/ua/visnyk/1076*
24. Semenets-Orlova, I., R. Shevchuk, B. Plish, A. Moshnin, Y. Chmyr, and R. Poliuliakh. 2022. "Human-Centered Approach in New Development Tendencies of Value-Oriented Public Administration: Potential of Education." Economic Affairs 67, no. 5: 899-906. *https://doi.org/10.46852/0424-2513.5.2022.25*
25. Shchybun, O. 2022. "EU Digital Markets Act in Compliance Activities." *https://biz.ligazakon.net/analitycs/226112_zakon-s-pro-tsifrov-rinki-v-komplans-dyalnost*
26. Sobko, G., A. Fomenko, L. Nalyvaiko, D. Pryputen, and I. Verba. 2024. "The Impact of the Istanbul Convention on Legislative and Legal Practices Regarding the Appointment of Responsibility for Domestic Violence." Observatorio 18, no. 2: 219-244. *https://doi.org/10.15847/obsOBS18220242360*
27. Sydorenko, N., T. Pakulova, and A. Naumyk. 2023. "Theoretical and Applied Approach to Reforming the System of Administrative Services as a Key Factor in the Transition of Ukraine to the Concept of a 'Service State.'" Grail of Science 31: 64-67. *https://doi.org/10.36074/grail-of-science.15.09.2023.09*
28. Treshchov, M. M., and A. S. Naumyk. 2023. "Digitalization of a Warring State: Necessity and Advantages." Problems of Modern Transformations. Series: Law, Public Administration and Administration 9. *https://doi.org/10.54929/2786-5746-2023-9-02-10*
29. Tsypko, V. V., K. I. Alieksieieva, I. A. Venger, N. I. Galunets, and A. V. Klyuchnik. 2019. "Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction." Journal of Advanced Research in Law and Economics 10, no. 6: 1664-1672.
30. Verkhovna Rada of Ukraine. 1992. Law of Ukraine No. 2657-XII "On Information". *https://zakon.rada.gov.ua/laws/show/2657-12#Text*
31. Verkhovna Rada of Ukraine. 2010. Law of Ukraine No. 2297-VI "On Personal Data Protection". *https://zakon.rada.gov.ua/laws/show/2297-17#Text*
32. Verkhovna Rada of Ukraine. 2017. Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity in Ukraine". https://zakon.rada.gov.ua/laws/show/2163-19#Text Verkhovna Rada of Ukraine. 2020. Law of Ukraine No. 1089-IX "On Electronic Communications". *https://zakon.rada.gov.ua/laws/show/1089-20#Text*
33. Verkhovna Rada of Ukraine. 2023. Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". *https://zakon.rada.gov.ua/laws/show/851-15#Text*
34. Verkhovna Rada of Ukraine. 2024. Law of Ukraine No. 4070-IX "On Amendments to Certain Laws of Ukraine Regarding the Functioning of the National System of Confidential Communications and the National Electronic Communications Network". *https://zakon.rada.gov.ua/laws/show/4070-20#Text*
35. Yevdokimov, V. O., and S. A. Kolomiyets. 2024. "Digital Transformation of Public Administration: Challenges and Prospects." Current Issues in Modern Science 9, no. 27: 403-415.
36. Zaporozhets, T. 2024. "Mechanisms of Public Management of the Development of Intellectual Potential in the Conditions of Digitalization." Scientific Perspectives 11, no. 53: 193-203. *https://doi.org/10.52058/2708-7530-2024-11(53)*

Liudmyla Shapenko, Iryna Hrytsai, Andrii Paraka, Mykhailo Kostytskyi, Andrii Fomenko

UKRAINOS VIEŠOJO ADMINISTRAVIMO INSTITUCIJŲ SKAITMENINĖS TRANSFORMACIJOS TEISINIAI IŠŠŪKIAI

Anotacija. *Viešasis sektorius patiria skaitmeninę transformaciją, todėl skaitmeninės technologijos sistemingai įtraukiamos į valdžios institucijų veiklą, paslaugų teikimą ir bendravimą su piliečiais, sie-*

kiant pagerinti reagavimo greitį, veiksmingumą ir skaidrumą. Šio straipsnio tikslas – išanalizuoti pagrindinius skaitmeninės transformacijos viešajame administravime teisinius iššūkius, ypatingą dėmesį skiriant duomenų apsaugai, kibernetiniam saugumui ir įtraukčiai, bei parengti praktines rekomendacijas, kaip suderinti Ukrainos teisinę sistemą su ES standartais. Tyrime taikytas teorinis ir teisinis požiūris, grindžiamas teisinės valstybės, teisinio tikrumo, proporcingumo ir pagrindinių žmogaus teisių apsaugos principais. Svarbūs skaitmeninės transformacijos komponentai yra įtrauktis ir prieinamumas. Suderinamumas yra dar vienas svarbus veiksnys, užtikrinantis sklandų duomenų srautą tarp vyriausybės sistemų ir didinantis paslaugų veiksmingumą. Sprendimų priėmimas remiantis duomenimis – tai politikos formavimas, išteklių paskirstymo optimizavimas ir gyventojų poreikių prognozavimas naudojant analitinius duomenis. ES lygmeniu egzistuoja patikimas skaitmeninio valdymo modelis, pagrįstas svarbiais susitarimais, kurie gina asmens laisves, skatina konkurenciją ir inovacijas bei remia bendrą skaitmeninę rinką. Tačiau Ukrainoje tam tikri teisiniai santykiai nėra reglamentuoti, o reguliavimo sistema yra pasenusi. Ši problema trukdo diegti šiuolaikines skaitmenines priemones ir pasaulines e. valdymo tendencijas. Nors buvo pasiekta tam tikra pažanga, karas smarkiai sutrikdė teisines ir technines infrastruktūros reformas. Norint išspręsti šias teisines problemas, reikalinga dinamiška teisinė sistema, užtikrinanti įtrauktį ir prieinamumą bei prisitaikanti prie technologijų pažangos.

Liudmyla Shapenko, PhD in Law, Department of Administrative and Information Law, Kyiv Aviation Institute; Department of Administrative Services of the Department (Center) for Administrative Services of the Solomyansk District State Administration in the city of Kyiv, Kyiv, Ukraine.
E-mail: *liudmyla_shapenko@edu-iosa.org*

Iryna Hrytsai, Department of Theory of State and Law Educational and Scientific Institute of Law and Innovative Education of Dnipro State University of Internal Affairs, Dnipro, Ukraine.
E-mail: *irinagritsay86@gmail.com*

Andrii Paraka, PhD Student Interregional Academy of Personnel Management, Kyiv, Ukraine.
E-mail: *paraka@tutamail.com*

Mykhailo Kostytskyi, Full Doctor in Law, Department of History, Philosophy and Law, Institute of Lawmaking and Scientific-Legal Expertise of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
E-mail: *nkkiev1966@gmail.com*

Andrii Fomenko, Full Doctor in Law, Department of Public Law Institute of Humanities and Social Sciences National Technical University "Dnipro Polytechnic", Dnipro, Ukraine.
E-mail: *fomenkoa@nmu.one*

Liudmyla Shapenko, Teisės mokslų daktaras, Administracinės ir informacinės teisės katedra, Kijevo aviacijos institutas; Administracinių paslaugų skyrius, Administracinių paslaugų departamentas (centras), Solomyansk rajono valstybinė administracija, Kijevas, Ukraina.
El. paštas: *liudmyla_shapenko@edu-iosa.org*

Iryna Hrytsai, Valstybės ir teisės teorijos katedra, Dnipro vidaus reikalų universiteto, Teisės ir novatoriško švietimo mokslo ir švietimo institutas, Dnipro, Ukraina.
El. paštas: *irinagritsay86@gmail.com*

Andrii Paraka, Doktorantas Tarpregioninė personalo vadybos akademija, Kijevas, Ukraina.
El. paštas: *paraka@tutamail.com*

Mykhailo Kostytskyi, Teisės mokslų daktaras, Istorijos, filosofijos ir teisės katedra, Ukrainos nacionalinės mokslų akademijos Teisės aktų leidybos ir mokslinės-teisinės ekspertizės institutas, Kijevas, Ukraina.
El. paštas: *nkkiev1966@gmail.com*

Andrii Fomenko, Teisės mokslų daktaras, Viešosios teisės katedra, Humanitarinių ir socialinių mokslų institutas, Nacionalinis technikos universitetas „Dnipro Polytechnic“, Dnipro, Ukraina.
El. paštas: *fomenkoa@nmu.one*

This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 (CC BY 4.0) License (*http://creativecommons.org/licenses/by/4.0/*).