Slipchuk Yuriy Andriiovych, Postgraduate Student, National University of Civil Defence of Ukraine, Ukraine

PEOPLE-CENTRED INTEROPERABILITY OF E-GOVERNANCE AS AN INSTRUMENT FOR IMPLEMENTING GOOD GOVERNANCE IN UKRAINE

Abstract

The article substantiates a people-centred interoperability model of e-governance as an instrument for implementing good governance in Ukraine. The relevance of the study is determined by the transformation of electronic governance from a tool of administrative convenience into a condition for the continuity of public authority, service accessibility and protection of citizens' rights under martial law, European integration and post-war recovery.

The study proceeds from the premise that digital tools create public value only when they are linked with the principles of transparency, accountability, rule of law, effectiveness, inclusiveness and people-centredness. The proposed model includes six dimensions of interoperability: legal, institutional, data, service, communication and participatory. Particular attention is paid to the relationship between national digital infrastructure, regional coordination and local service delivery. The model explains how electronic identification, register exchange, open data, digital services, cybersecurity and e-democracy tools can be integrated into a coherent public-administration system.

The practical value of the article lies in the formulation of recommendations for Ukraine: simplification of procedures before digitization; harmonization with EU standards on data protection, digital identity and trust services; strengthening of regional and municipal capacity; development of assisted digital access for vulnerable groups; introduction of user-experience indicators; and connection of

digital participation tools with real decision-making procedures. The results may be used in public-administration research, digital-transformation planning and the preparation of recommendations for improving e-governance in Ukraine.

Keywords: e-governance, good governance, digital state, public administration, interoperability, electronic services, e-democracy, Ukraine.

Problem statement. Ukraine's movement toward a digital state is no longer a narrow technological reform. Under martial law, accelerated European integration and the need for post-war recovery, e-governance has become a condition for the continuity of public authority, the protection of citizens' rights and the delivery of services in situations where physical infrastructure may be damaged or inaccessible. The dissertation material shows that electronic governance in Ukraine has moved from the logic of administrative convenience to the logic of state resilience: public registers, electronic documents, remote services and secure data exchange make it possible to preserve interaction between the state, citizens and businesses even under crisis pressure.

At the same time, the mere digitisation of procedures does not automatically create good governance. A service may be formally available online but remain complicated, fragmented, legally uncertain, inaccessible to vulnerable users or poorly connected with other administrative systems. This is why the development of e-governance should be interpreted not only as a process of introducing portals, applications and registers, but also as a transformation of the institutional architecture of public administration. Digital instruments must be assessed by whether they strengthen transparency, accountability, rule of law, efficiency, inclusiveness and people-centredness.

The practical problem is the gap between national-level digital platforms and local-level public needs. National systems establish common standards, interoperability rules, identification tools, cybersecurity requirements and

electronic-service infrastructure. However, citizens experience public administration primarily through concrete life situations: registration of residence, access to social assistance, recovery of documents, interaction with a community, participation in decision-making, receipt of compensation, access to education or health care. Therefore, the effectiveness of e-governance depends on how coherently the national digital infrastructure is connected with regional and municipal administrative processes.

This issue is particularly important for Ukraine because the principles of good governance are a core part of the European integration agenda. The dissertation emphasizes that the European model is based on subsidiarity, openness, accountability, predictability, effectiveness and people-centredness. These principles require not simply the transfer of existing bureaucracy to an electronic form, but a rethinking of how public authorities collect data, make decisions, provide services, involve citizens and report on results. In this context, a scientifically grounded model of people-centred e-governance is needed as an instrument for implementing good governance in Ukraine.

Analysis of recent research and publications. The scientific and policy literature on e-governance is developing in several directions. The first direction concerns the global transformation of public administration under the influence of digital technologies. The United Nations e-government framework treats digital government as a combination of online services, telecommunication infrastructure and human capital, while also paying attention to inclusion and the capacity of institutions to provide public value [1]. This position is important because it shifts the emphasis from the technical existence of online services to the real accessibility and usefulness of public interaction.

The second direction is related to the concept of good governance. The Council of Europe and the OECD/SIGMA approach interpret good governance through principles that include openness, participation, rule of law, effectiveness,

efficiency, accountability and sound financial management [2; 3]. For Ukraine, these principles are not abstract recommendations but practical benchmarks for public-administration reform and preparation for EU membership. They are also criteria for evaluating whether digital services actually improve governance rather than only modernize its external form.

The third direction concerns European digital regulation. EU policy increasingly connects digitalization with trust, data protection, interoperability and cross-border identification. The eIDAS framework, the General Data Protection Regulation, the Data Governance Act and interoperability-oriented European initiatives show that digital government must be legally secure, technically compatible and rights-based [4-6]. These requirements are relevant for Ukraine because the development of digital services and registers must be compatible with the European digital environment.

The fourth direction is Ukrainian practice of digital state-building. The dissertation highlights the role of the Diia ecosystem, electronic documents, digital public services, the Trembita system of electronic interaction, open data and the transfer of administrative procedures into electronic form. These tools are interpreted as instruments for reducing corruption, lowering transaction costs, simplifying access to services and increasing the transparency of public authorities. At the same time, the dissertation material also identifies unresolved problems: uneven digital access, insufficient digital literacy, cybersecurity risks, fragmentation of registers, legal uncertainty and the need for better coordination among public bodies.

The fifth direction relates to electronic democracy and public participation. The development of e-petitions, public consultations, participatory budgeting, open data portals and digital feedback channels expands the possibilities for citizens to influence decisions. However, digital participation may remain symbolic if it is not connected with decision-making procedures, feedback

obligations and accountability mechanisms. Therefore, e-democracy should be considered not as a separate supplement to e-governance, but as one of the core components of people-centred good governance.

Despite the significant number of publications, the applied question remains insufficiently developed: how should Ukraine design an integrated model in which national digital infrastructure, regional implementation capacity and local participation jointly produce good governance outcomes? The existing titles of Slipchuk's published works and conference materials already cover administrative-legal principles, general mechanisms of e-governance, normative support, foreign experience, cyberspace in military operations, higher education digitalization and digital resilience. The present article therefore deliberately focuses on another angle - people-centred interoperability as a practical model for linking digital infrastructure with public value, service accessibility and multi-level governance.

Purpose of the article. The purpose of the article is to substantiate a people-centred interoperability model of e-governance as an instrument for implementing good governance in Ukraine. The achievement of this purpose requires: clarifying the relationship between e-governance and good governance; identifying the levels and components of people-centred interoperability; determining the role of national, regional and local actors; and formulating practical recommendations for improving digital public administration in the conditions of martial law, European integration and post-war recovery.

Presentation of the main material of the study. E-governance should be understood as a system of institutional, legal, technological, organizational and communication relations that enable public authorities to provide services, exchange data, involve citizens and make decisions through information and communication technologies. In this interpretation, digital tools are not self-sufficient. They acquire public value only when they change the quality of

interaction between the state and the citizen: make it faster, clearer, safer, more transparent, more inclusive and less dependent on personal discretion of officials.

Good governance provides a normative framework for evaluating this transformation. If the principle of openness is applied, e-governance must ensure access to public information, open data and understandable explanations of administrative decisions. If accountability is applied, digital systems must leave verifiable traces of actions and allow citizens to appeal or correct decisions. If efficiency is applied, electronic services must reduce unnecessary administrative steps and paper circulation. If people-centredness is applied, services must be designed according to life situations rather than according to the internal structure of institutions.

The proposed model is based on the concept of people-centred interoperability. In the usual technical sense, interoperability means the ability of information systems and registers to exchange data. In the public-administration sense, it should be broader. People-centred interoperability means the coordinated ability of legal norms, public institutions, digital platforms, administrative procedures and communication channels to support a citizen's interaction with the state without duplication, excessive paperwork, unjustified delays or exclusion. Thus, interoperability should connect not only databases but also responsibilities, standards, services and feedback.

The first level of the model is legal interoperability. It determines whether different public bodies may lawfully collect, process, exchange and use data. For Ukraine, this level includes legislation on electronic documents, electronic identification, trust services, personal data protection, public electronic registers, cybersecurity, open data and administrative procedures. Legal interoperability is essential because a technically possible data exchange may be unacceptable if the purpose, legal basis, consent, access rights and responsibility are not defined.

Therefore, the further development of e-governance requires harmonization with EU data-protection and digital-identity standards.

The second level is institutional interoperability. It concerns the distribution of functions among central executive bodies, regional administrations, local self-government bodies, service centres and digital-system administrators. The dissertation material emphasizes that the national level should provide unified rules, platforms and standards, whereas the local level fills digital tools with concrete content and adapts them to the needs of communities. Institutional interoperability is achieved when these levels do not duplicate one another but form a coherent chain: the state defines the architecture, regions coordinate implementation, and communities provide direct service interaction with citizens.

The third level is data interoperability. Its practical foundation in Ukraine is the electronic interaction of registers, particularly through the Trembita system. Data interoperability implements the once-only principle: citizens should not repeatedly provide information that is already available to the state. In practice, this reduces the number of certificates, paper documents and visits to public offices. However, data interoperability must be combined with data quality, cybersecurity, auditability and minimization of access. Otherwise, the expansion of data exchange can create new risks instead of solving old problems.

The fourth level is service interoperability. It means that electronic services should be organized around user needs and life events. For example, displacement, birth of a child, loss of documents, damage to housing, registration of business activity or obtaining veteran-related support are not isolated bureaucratic actions. They involve several institutions and several types of data. A people-centred electronic service should guide the user through the whole administrative path rather than force the user to understand the internal division of competence among agencies.

The fifth level is communication interoperability. Digital governance cannot rely only on portals and applications. Citizens need clear information about their rights, service algorithms, required documents, deadlines, appeal procedures and data-protection guarantees. Communication interoperability means that information is consistent across websites, mobile applications, administrative service centres, hotlines, community offices and social networks. This is particularly important under martial law, when citizens may be displaced, lose documents, have limited access to internet or need urgent assistance.

The sixth level is participatory interoperability. It connects e-governance with e-democracy. Citizens should not only receive digital services but also influence public decisions through consultations, petitions, participatory budgeting, digital surveys, open-data analysis and public monitoring. Participatory interoperability means that feedback is not lost in the system: it is registered, analyzed, transmitted to the responsible authority and reflected in decisions or public explanations. Without this level, digital government may become administratively efficient but democratically weak.

The national dimension of the model includes the development of a unified digital infrastructure. Its core components are national registers, electronic identification, trust services, interoperable data exchange, cybersecurity standards, open data, state portals, digital documents and integrated public-service platforms. This level is responsible for ensuring equality of standards across the country. A citizen should not lose access to basic public services because of the region of residence, displacement or the administrative capacity of a particular community.

The regional dimension includes coordination of implementation. Regional authorities have to adapt national digital tools to territorial conditions, support communities, analyze service gaps, coordinate recovery needs, ensure continuity of public administration and collect feedback from service users. In frontline and de-occupied territories, the regional dimension is connected with emergency

communication, remote access to services, preservation of registers, support for internally displaced persons and protection of critical information infrastructure. In relatively safe regions, the emphasis may be on service load, integration of displaced persons, expansion of administrative service centres and digital inclusion.

The local dimension is the most visible for citizens. Communities organize access points, municipal services, local registers, electronic queues, school and health-care-related digital services, local consultations, public-budget platforms and open data on community assets. Local e-governance should not be reduced to the purchase of software. It requires trained staff, service standards, accessible premises, reliable communication with residents and capacity to use national platforms correctly. A community that lacks institutional capacity may formally have access to digital tools but fail to transform them into better governance.

A people-centred model also requires inclusion. Digitalization may reduce administrative barriers for many users, but it can increase exclusion for those who lack devices, internet access, digital literacy, language accessibility or trust in online systems. Therefore, the digital state should preserve alternative channels: administrative service centres, mobile service teams, assisted digital access points, telephone support, community mediators and paper-based solutions for exceptional cases. The goal is not to force everyone into one digital channel but to ensure that every person can receive a service safely and conveniently.

Another component is cybersecurity and digital trust. Under wartime conditions, public digital infrastructure is a target of attacks. Trust in electronic governance depends not only on user-friendly interfaces but also on the confidence that data will be protected, services will remain available, and errors or unauthorized actions can be detected. For this reason, cybersecurity, backup systems, cloud resilience, access control, regular audits and incident-response

procedures must be considered part of good governance, not only part of information technology management.

The model can be operationalized through a public-administration cycle. The first stage is diagnosis: authorities identify which services are fragmented, duplicated, inaccessible or vulnerable. The second stage is legal and institutional alignment: responsibilities, data-exchange rules and service standards are clarified. The third stage is digital redesign: procedures are simplified before being converted into electronic form. The fourth stage is implementation: platforms, registers, access points and staff training are deployed. The fifth stage is monitoring: user satisfaction, processing time, error rates, accessibility and security incidents are measured. The sixth stage is correction: services are improved on the basis of evidence and feedback.

This cycle is especially relevant for administrative services related to wartime needs. Internally displaced persons, veterans, families of fallen defenders, citizens whose housing has been damaged and businesses relocating to safer regions often interact with several institutions simultaneously. The quality of governance is determined by whether these interactions are integrated. For example, an internally displaced person may need confirmation of status, social payments, registration of children in school, access to medical care, employment support and housing assistance. A people-centred interoperable system should not treat these as unrelated actions but as elements of one life situation.

The proposed model differs from a purely technological approach. It does not start with the question of what platform should be introduced, but with the question of what public value should be created. Public value in this context includes time saved by citizens, reduced corruption risks, fewer administrative visits, improved transparency, greater accessibility, better data quality, stronger participation and more reliable protection of rights. The measurement of e-

governance should therefore include not only the number of digital services but also their impact on trust, convenience, fairness and administrative outcomes.

A practical example may be the development of local digital services on the basis of national infrastructure. The state provides secure identification, register exchange and legal standards. The region coordinates implementation and identifies territorial priorities. The community uses these tools for local services such as electronic queues, permits, school enrollment, consultations, public-budget voting or information about recovery projects. Citizens receive services and provide feedback. This chain shows that e-governance becomes effective when all levels are connected through common standards and shared responsibility.

Another example concerns open data and accountability. Publishing datasets is important, but people-centred interoperability requires that open data be connected with understandable dashboards, public explanations, monitoring of projects and feedback channels. For recovery policy, open data should allow citizens to see which projects are planned, how they are funded, what stage they are at, who is responsible and how to report problems. This converts digital transparency into a real accountability mechanism.

The article proposes several practical recommendations. First, the development of e-governance should be guided by an explicit people-centred interoperability principle. This principle should be reflected in strategic documents, service standards and digital-transformation plans. Second, the simplification of administrative procedures must precede their digitization. Otherwise, digital tools will reproduce bureaucratic complexity. Third, interoperability projects should include legal, institutional, data, service, communication and participatory components, not only technical integration.

Fourth, regional and municipal capacity-building should become a permanent element of digital-state policy. Officials need skills in data governance, cybersecurity awareness, user-centred service design, public communication,

digital participation and evaluation. Fifth, digital inclusion should be treated as a criterion of service quality. Every major digital service should be assessed according to its accessibility for elderly people, people with disabilities, displaced persons, rural residents and persons with limited digital skills. Sixth, electronic services should be monitored through indicators of user experience, processing time, error correction, appeal rates and citizen satisfaction.

Seventh, Ukraine should continue alignment with EU digital standards. This includes personal data protection, electronic identification, trust services, interoperability, open data and responsible data governance. Such alignment is necessary not only for formal European integration but also for creating a trusted digital environment in which Ukrainian citizens and businesses can interact with public authorities and European partners. Eighth, participatory tools should be linked with decision-making obligations. Public consultations and digital feedback should result in published responses, explanations or revisions of policy decisions.

The expected result of implementing the model is a transition from electronic administration to digital good governance. Electronic administration is mainly about converting procedures into electronic form. Digital good governance is broader: it makes public administration more transparent, accountable, inclusive, effective and oriented toward public value. For Ukraine, this transition is especially significant because the digital state has already demonstrated its resilience under extraordinary conditions. The next step is to deepen the connection between resilience, European standards and everyday service quality.

Conclusion. The development of e-governance in Ukraine should be viewed as a strategic instrument for implementing good governance rather than as a separate technological reform. The dissertation material confirms that electronic services, digital documents, register interoperability, cybersecurity, open data and e-democracy tools have become essential for the modernization of public administration, especially under martial law and European integration.

The article substantiates a people-centred interoperability model that connects legal, institutional, data, service, communication and participatory dimensions of e-governance. The model emphasizes that interoperability should link not only information systems but also administrative responsibilities, service standards, citizen feedback and public accountability. National authorities provide common infrastructure and standards; regional authorities coordinate implementation and adaptation; local self-government bodies ensure direct interaction with citizens and community participation.

The proposed approach allows e-governance to be evaluated through good-governance outcomes: transparency, accountability, efficiency, inclusiveness, trust and protection of rights. Practical implementation requires simplification of procedures before digitization, harmonization with EU standards, strengthening of regional and municipal capacity, preservation of assisted access for digitally vulnerable groups, cybersecurity measures and integration of participation tools into decision-making. Further research should focus on empirical testing of this model in selected Ukrainian regions and on the development of indicators for evaluating the public value of digital services.

References

1. United Nations. (2024). E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: United Nations. DOI: absent. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024.

2. Council of Europe. (n.d.). 12 Principles of Good Democratic Governance. DOI: absent. URL: https://www.coe.int/en/web/good-governance/12-principles.

3. OECD/SIGMA. (2023). The Principles of Public Administration. Paris: OECD. DOI: absent. URL: https://www.sigmaweb.org/publications/principles-public-administration.htm.

4. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. DOI: absent. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj.

5. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). DOI: absent. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

6. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/868 on European data governance (Data Governance Act). DOI: absent. URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj.

7. Cabinet of Ministers of Ukraine. (2017). Concept for the Development of Electronic Democracy in Ukraine and the Action Plan for its Implementation. Order No. 797-r. DOI: absent. URL: https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text.

8. Verkhovna Rada of Ukraine. (2017). Law of Ukraine On Electronic Trust Services. DOI: absent. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Verkhovna Rada of Ukraine. (2021). Law of Ukraine On Public Electronic Registers. DOI: absent. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text.

10. Ministry of Digital Transformation of Ukraine. (n.d.). Diia: State services online. DOI: absent. URL: https://diia.gov.ua/.

11. Ministry of Digital Transformation of Ukraine. (n.d.). Trembita: electronic interaction system. DOI: absent. URL: https://trembita.gov.ua/.

12. Open Government Partnership. (n.d.). Ukraine. DOI: absent. URL: https://www.opengovpartnership.org/members/ukraine/.

13. OECD. (2022). Rebuilding Ukraine by Reinforcing Regional and Municipal Governance. OECD Multi-level Governance Studies. DOI: https://doi.org/10.1787/63a6b479-en. URL:

https://www.oecd.org/en/publications/rebuilding-ukraine-by-reinforcing-regional-and-municipal-governance_63a6b479-en.html.

14. OECD. (2022). Public Governance in Ukraine: Implications of Russia's War. OECD Policy Responses. DOI: absent. URL: https://www.oecd.org/en/publications/public-governance-in-ukraine_c8cbf0f4-en.html.

15. European Commission. (n.d.). eGovernment and digital public services. DOI: absent. URL: https://digital-strategy.ec.europa.eu/en/policies/egovernment.