УДК: 35.077.2

E-GOVERNANCE: A PATHWAY TO DEMOCRACY OR TOTALITARIANISM?

ЕЛЕКТРОННЕ УРЯДУВАННЯ: ШЛЯХ ДО ДЕМОКРАТІЇ ЧИ ТОТАЛІТАРИЗМУ?

Olha Andrieieva
Doctor Of Political Sciences, Professor, Professor of International Information Department, Educational and Scientific Institute of International Relations, Taras Shevchenko National University of Kyiv,
e-mail: andreevaolga@knu.ua,
ORCID ID: https//orcid.org/0000-0003-4587-1267

Ольга Андрєєва
Доктор політичних наук, професор, професор кафедри міжнародної інформації Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка,
e-mail: andreevaolga@knu.ua,
ORCID ID: https//orcid.org/0000-0003-4587-1267

Abstract. *The article explores e-governance as a tool for transforming modern governance idea, which can both promote the deepening of democracy and create prerequisites for strengthening totalitarian control. It analyzes the advantages of implementing digital technologies in public administration, particularly in terms of transparency, accessibility, and efficiency. At the same time, it outlines the risks of excessive data centralization, digital surveillance, and abuse of power. Special attention is given to the concept of "digital dictatorship" and examples of e-governance practices across different political regimes. Particular focus is placed on the issues of digital authoritarianism and the mechanisms of digital dictatorship, manifested through the centralization of data control, mass surveillance, algorithmic discrimination, and information manipulation. Based on international experience, the article formulates recommendations for ensuring the democratic nature of digital transformation: respect for human rights, transparency of digital solutions, and the creation of institutional safeguards for the protection of digital rights. The study emphasizes the importance of legal, ethical, and technological support for e-governance processes to prevent the risks of digital dictatorship. Conclusions are drawn regarding the conditions under which e-governance promotes democratization and warnings are provided about potential challenges in the field of human rights.*

Keywords: *e-governance, democracy, totalitarianism, digital technologies, state, human rights, digital sovereignty, cybersecurity, digital dictatorship, data privacy.*

Анотація. *У статті розглядається електронне урядування як інструмент трансформації сучасного управління, що може як сприяти поглибленню демократії, так і створювати передумови для посилення тоталітарного контролю. Проаналізовано переваги впровадження цифрових технологій у державне управління, зокрема щодо прозорості, доступності та ефективності. Водночас окреслено ризики надмірної централізації даних, цифрового нагляду та зловживання владою. Особливу увагу приділено поняттю «цифрової диктатури» та прикладам використання електронного урядування в різних політичних режимах. Окрема увага приділяється проблематиці цифрового авторитаризму та механізмам цифрової диктатури, які проявляються у централізації контролю над даними, масовому нагляді, алгоритмічній дискримінації та маніпуляції інформацією. На основі міжнародного досвіду сформульовано рекомендації щодо забезпечення демократичності*

цифрової трансформації: дотримання прав людини, прозорості цифрових рішень, створення інституційних гарантій захисту цифрових прав. Робота підкреслює важливість правового, етичного та технологічного супроводу процесів електронного урядування для запобігання ризикам цифрової диктатури. Зроблено висновки щодо умов, за яких електронне урядування сприяє демократизації, та застереження щодо потенційних викликів у сфері прав людини.

Ключові слова: *електронне урядування, демократія, тоталітаризм, цифрові технології, держава, права людини, цифровий суверенітет, кібербезпека, цифрова диктатура, приватність даних.*

Introduction. In the context of globalization and the rapid development of information and communication technologies (ICT), public governance is undergoing significant transformations. These changes are driven, on the one hand, by the need to enhance the efficiency, transparency, and openness of government institutions, and on the other hand, by citizens' expectations for improved service delivery in public institutions. One of the key factors behind these transformations is e-governance, which is becoming an integral part of the modern public administration system. E-governance serves as a tool for transitioning from a traditional bureaucratic model to a more flexible, service-oriented, and interactive model of interaction between the state and its citizens (UN E-Government Survey, 2022).

The digitalization of public administration has become a global trend in the 21st century. Through the implementation of innovative technologies, governments can improve the efficiency of public service delivery, ensure transparency, and engage citizens in governance processes. However, alongside these advantages, new risks are emerging — the intensification of digital control, data manipulation, and cyber surveillance. This raises a dilemma: is e-governance truly a step towards democracy, or is it becoming a tool for strengthening authoritarian power?

The purpose (the aim) of the scientific article is to provide a comprehensive analysis of e-governance as a factor in the modernization of public administration and to address the issue of the dual nature of digitalization — as both a means of democratization and a potential instrument of digital authoritarianism.

Main results of the research. E-governance is an interdisciplinary phenomenon that encompasses the fields of public administration, information technology, law and social communication. The theoretical foundation of the concept of e-governance lies in the idea of modernizing public administration through the implementation of information and communication technologies (ICT) to enhance the efficiency, transparency and accountability of government. E-governance is defined as the use of information and communication technologies by government agencies to improve the quality of public services, ensure effective interaction with citizens, businesses and other stakeholders and enhance the decision-making process (Heeks, 2006).

Several key principles underlie e-governance, including: (a) citizen-centricity, which involves simplifying access to administrative services and reducing barriers to interaction with the state; (b) interoperability, or the ability of different government information systems to interact with one another; (c) open data, which creates conditions for public oversight; and (d) digital inclusiveness, which ensures the accessibility of services for all segments of the population (Bannister & Connolly, 2012).

Conceptually, e-governance is seen as part of the broader process of digital transformation of public administration, which includes e-democracy, e-participation and the development of electronic services (UN E-Government Survey, 2022).

In this context, e-governance is not merely a technical innovation but also a tool of institutional modernization that impacts all levels of government — from local to national. The application of the e-governance concept contributes to the simplification of administrative procedures, the automatization of document management, the development of digital services, and the provision of real-time access to public information. In particular, the introduction of government service portals helps to reduce corruption risks, improve service quality and lower administrative

costs (Gil-García & Helbig, 2006). At the same time, digital platforms open new opportunities for citizen participation in decision-making processes, including through electronic petitions, online consultations, and e-voting (Bannister & Connolly, 2012).

The development of service-oriented platforms, which integrate service delivery based on the "one-stop shop" principle, is becoming especially relevant. This approach ensures a seamless citizen experience and minimizes physical interactions with government representatives, which is particularly important in the context of pandemics, emergencies, military conflicts or temporary occupations.

However, there are also challenges. Among them are unequal access to digital technologies, insufficient levels of digital literacy, cybersecurity threats, and the risks of excessive data centralization and citizen control (Brown, Fishenden, & Thompson, 2014).

In countries with established democratic traditions, e-governance functions as a tool for enhancing government transparency, accountability, and citizen engagement. In countries with transitional democracies or authoritarian tendencies, its application may be more formalistic or controlling, preserving centralized governance models (Welch, Hinnant, & Moon, 2005). Thus, the effectiveness of e-governance largely depends on the political and institutional context, the level of digital literacy among the population, and the existence of legal and technical mechanisms for ensuring digital rights.

At the same time, in countries with authoritarian regimes, e-governance can be used as a tool for mass surveillance, behavioral control of citizens and restriction of rights and freedoms. Examples include China's "social credit system," as well as the use of facial recognition and artificial intelligence technologies for population monitoring.

In the process of deploying e-governance systems, vast amounts of citizens' personal data are accumulated, which, in the absence of appropriate control mechanisms, may lead to their use for mass surveillance, discrimination, or political persecution (Bosch Stiftung, 2022). Big data analytics tools, artificial intelligence, and automated decision-making systems can be employed not only to optimize services but also to build systems of social scoring for citizens, as observed, for example in China (Creemers, 2018). Similar trends are also recorded in other countries with non-democratic regimes, where electronic services are transformed into tools of digital censorship and political control (Feldstein, 2019).

The main totalitarian risks traditionally associated with e-governance include: (-) the centralization of control over information flows; (-) the expansion of digital surveillance capabilities; (-) the restriction of privacy and digital rights; (-) the strengthening of manipulative influence on public opinion through digital algorithms; (-) the increase in inequality regarding access to digital resources and legal protection (Bosch Stiftung, 2022).

Although e-governance holds significant potential for promoting open and democratic governance, without proper regulatory, ethical and technological safeguards, it may evolve into an instrument of digital authoritarianism. Awareness of these risks is crucial for building a safe and inclusive digital society. Table 1 visually presents the most common totalitarian risks in the digitalization era along with countermeasures.

Digital Risks of E-Governance

Totalitarian Risks	Risk Description	Countermeasures
Centralization of data control	Concentration of large volumes of personal information in the hands of the state	Establishment of independent data protection bodies; legislative limits on data collection
Digital surveillance and mass monitoring	Use of ICT for continuous monitoring of citizens	Implementation of "privacy by design" principles; public oversight
Violation of privacy	Uncontrolled circulation and use of personal data	Strict regulation of data collection and use; sanctions for violations
Algorithmic	Automated decision-making	Ensuring algorithmic transparency;

discrimination	systems lacking transparency and fairness	mechanisms for appealing digital decisions
Information manipulation	Use of algorithms to manipulate public opinion	Openness of recommendation algorithms; promotion of citizens' digital literacy
Social stratification through digitalization	Deepening inequality in access to digital services and protection of citizens' rights	Digital inclusion programs; investment in digital education

E-governance was originally conceived as a tool for democratizing government and enhancing its transparency. However, in the practice of some states, an inversion of this process can be observed: instead of expanding civil liberties, digital technologies are increasingly used as mechanisms of restriction. This phenomenon has been termed the "digital dictatorship" (Feldstein, 2019).

Digital dictatorship is a form of authoritarian governance in which digital technologies are employed for mass data collection, citizen surveillance, information manipulation and the restriction of human rights and freedoms. Unlike traditional authoritarianism, which relied on physical coercion, digital dictatorship operates through control over information flows, personal data and the digital behavior of citizens.

Under conditions of digital dictatorship, rights to privacy, freedom of speech and freedom of assembly are severely restricted. Technologies that could serve as instruments of democratization and emancipation instead become mechanisms of repression. The lack of transparency in data governance further deepens distrust toward institutions and undermines the potential for civic participation (see Table 2).

Mechanisms of Digital Dictatorship

Mechanism	Description
Surveillance	Continuous monitoring of the population through biometrics, big data analysis, and AI algorithms.
Censorship	Filtering and blocking of undesirable content.
Information operations	Use of trolls, bots, and manipulation of information flows.
Internet isolation	Creation of internal networks that reduce or block access to global information.
Repression through data	Use of digital footprints to selectively persecute opposition members.

Digital technologies are not inherently good or evil. Their impact depends on the political context, legal culture and the level of institutional democracy. For example, the use of biometric identification systems in India (Aadhaar) has sparked both praise from international experts and criticism over privacy violations.

The key question is: who controls the data and how are the rules for their use established?

In authoritarian regimes, e-government is often used to strengthen control over the population.

China is the most striking example of a digital dictatorship. The social credit system evaluates citizens' loyalty based on their behavior: payments, posts on social media and even associations with "untrustworthy" individuals. A low score can restrict access to travel, credit and education. Mass digital surveillance is carried out through widespread use of facial recognition cameras (Skynet project), analysis of online activity and banking operations and restrictions on the use of cryptocurrencies — for example, China has banned Bitcoin and other decentralized payment systems, while promoting its state-controlled digital yuan (e-CNY) (Creemers, 2018).

russia has implemented a facial recognition surveillance system, which was actively used to identify protest participants. Additionally, systems for operational investigative measures (SOIM) provide the government with full access to citizens' electronic communications. The state also has the capability to isolate the russian segment of the Internet from the global network, block access to independent media, restrict VPN services and ban foreign social media platforms (Human Rights Watch, 2017).

Internet isolation in Iran became evident during the mass protests of 2019, when the Iranian government completely disconnected the country from the global Internet, creating a localized alternative — the "national Internet." This allowed for strict control of information flows and suppression of protest coordination. Additionally, cyberattacks against opposition members and journalists have been reported (Freedom House, 2022).

Thus, the digitalization of public governance is not automatically democratic or secure. In order for electronic technologies to serve the goals of strengthening human rights, promoting democratic governance, and ensuring national security, a set of principles and institutional safeguards must be observed. Based on current research in the field of e-government (UNESCO, 2021; World Bank, 2022), the following key conditions can be identified:

Primacy of human rights. All digital processes must be carried out with full respect for fundamental human rights and freedoms, including the right to privacy, freedom of expression, and the protection of personal data. The development and implementation of digital services should be accompanied by a human rights impact assessment.

Transparency and accountability of digital decisions. A key safeguard against digital dictatorship is ensuring transparency of algorithms and procedures used in e-governance: open-source code for state digital platforms, audits of artificial intelligence algorithms and independent public oversight of data processing practices. Information about data use must be made available to citizens in a simple and understandable form (European Union Agency for Fundamental Rights, 2021).

Institutional safeguards for controlling digital power. It is necessary to establish and strengthen independent institutional mechanisms, such as digital rights ombudsmen, data protection regulatory bodies, and specialized parliamentary committees on digital security. These bodies must have real powers to prevent abuses by governments or private companies.

Cybersecurity and protection of critical infrastructure. Democratic digital governance cannot exist without guaranteed cybersecurity. Data security breaches threaten privacy, democracy and even national sovereignty. Essential measures include mandatory encryption of communications, multilayered data protection, and international cooperation in the field of cybersecurity.

Ensuring pluralism in the information space. Digital democracy is only possible with an open information environment. It is necessary to prevent the monopolization of digital platforms, ensure citizens' access to a variety of information sources, and support the development of independent media. Control over the spread of disinformation must be exercised without suppression on freedom of speech, involving independent expert institutions.

Conclusions. E-government is not only a tool for optimizing public administration but also a factor in shaping a new model of interaction between the state, civil society and business. Its effective implementation requires a comprehensive approach that combines regulatory, institutional and technological frameworks, while also taking into account the social context of digital transformations.

Digital governance has the potential both to strengthen democracy and to reinforce authoritarianism. Its impact depends on the political context, the level of transparency and accountability of the authorities and the existence of mechanisms for protecting citizens' rights. To ensure democratic development, e-government must be implemented based on the principles of openness, participation and the protection of human rights. However, without adequate safeguards for citizens' rights, it can devolve into a form of digital dictatorship. Therefore, the future of e-government will depend on maintaining a balance between innovation and democratic guarantees.

Secure and democratic digitalization requires a systemic approach founded on the values of human rights, the rule of law and political accountability. Only by adhering to these principles can e-government become a tool for strengthening democracy rather than a catalyst for digital authoritarianism.

References

1. Bannister, F., & Connolly, R. (2012). Defining e-government: A stakeholder approach. European Journal of Information Systems, 21(5), 527–539. https://doi.org/10.1057/ejis.2012.14
2. Bosch Stiftung. (2022). Exploring Worldwide Democratic Innovations: A Series of Case Studies. Retrieved from https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-11/Exploring_Worldwide_Democratic_Innovations_Long_Report.pdf Robert Bosch Stiftung
3. Brown, A., Fishenden, J., & Thompson, M. (2014). Digitizing government: Understanding and implementing new digital business models. Palgrave Macmillan. Retrieved from https://www.researchgate.net/publication/277076845_Digitizing_Government
4. Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. SSRN. https://doi.org/10.2139/ssrn.3175792
5. European Union Agency for Fundamental Rights. (2021). Artificial Intelligence and Fundamental Rights. https://fra.europa.eu/en/publication/2021/artificial-intelligence-and-fundamental-rights
6. Feldstein, S. (2019). The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
7. Freedom House. (2022). Freedom on the Net 2022 - Countering an Authoritarian Overhaul of the Internet. Retrieved from https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internetWikipedia
8. Gil-García, J. R., & Helbig, N. (2006). Exploring e-government benefits and challenges. Public Administration Review, 66(6), 913–926. https://doi.org/10.1111/j.1540-6210.2006.00656.x
9. Heeks, R. (2006). Implementing and Managing eGovernment: An International Text. SAGE Publications. DOI: https://doi.org/10.4135/9781446220191
10. Human Rights Watch. (2017). Online and On All Fronts: Russia's Assault on Freedom of Expression. Retrieved from https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault
11. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000381137
12. United Nations. (2022). UN E-Government Survey 2022: The Future of Digital Government. Department of Economic and Social Affairs. Retrieved from https://publicadministration.un.org/egovkb
13. Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. Journal of Public Administration Research and Theory, 15(3), 371–391. https://doi.org/10.1093/jopart/mui021
14. World Bank. (2022). GovTech: Putting People First. Retrieved from https://www.worldbank.org/en/topic/governance/brief/govtech-putting-people-first