Politique et relations internationales

UDC 004.8:316.42:351.86

ARTIFICIAL INTELLIGENCE REGULATION IN WARTIME GOVERNANCE: ADAPTING EU AI ACT APPROACHES TO UKRAINE

Kateryna Hannouf, PhD, Ukrainian-French Institute of Science, Innovation and Economic Development, Paris, France; E-mail: katerinahann@gmail.com; ORCID: 0000-0001-7689-9938

Abstract. The article examines the challenges of regulating artificial intelligence in public governance under martial law and substantiates the need to adapt risk-based approaches embedded in the EU Artificial Intelligence Act (EU AI Act), adopted by the European Union, to the specificities of Ukraine's wartime context. The study aims to assess the limitations of directly implementing the EU AI Act under emergency governance and to develop an adaptive regulatory approach focused on digital resilience, security, and human rights protection. The methodology relies on an interdisciplinary framework and includes legal and regulatory analysis of the EU AI Act provisions, comparative analysis of international approaches to AI regulation, institutional and structural-functional analysis of wartime governance, and conceptual modelling. The findings indicate that the static risk-based logic of the EU AI Act is insufficient for wartime public governance marked by emergency powers, accelerated decision-making, and a growing role of algorithmic systems. Key regulatory constraints are identified, supporting a shift toward a flexible, context-sensitive regulatory approach. A model of flexible AI regulation for wartime public governance is proposed, grounded in proportionality, temporality, and reinforced human oversight. Scientific novelty lies in a conceptual approach to AI regulation under martial law that extends the EU AI Act framework by integrating wartime conditions, an adaptive regulatory loop, and a system of mandatory risk-limiting safeguards. The findings can inform the design of national AI policy and legal instruments for Ukraine during martial law and throughout post-war recovery. and legal instruments for Ukraine during martial law and throughout post-war recovery.

Keywords: artificial intelligence; EU AI Act; martial law; public governance; regulation; digital resilience.

LA RÉGULATION DE L'INTELLIGENCE ARTIFICIELLE EN CONTEXTE DE GUERRE: ADAPTATION DES APPROCHES DE L'AI ACT DE L'UNION EUROPÉENNE À L'UKRAINE

Kateryna Hannouf, PhD , Institut franco-ukrainien de science, d'innovation et de développement économique, Paris, France ; e-mail : katerinahann@gmail.com ; ORCID : 0000-0001-7689-9938.

Résumé. Cet article analyse les défis liés à la régulation de l'intelligence artificielle dans la gouvernance publique sous le régime de la loi martiale et étaye la nécessité d'adapter les approches fondées sur les risques, consacrées par le Règlement de l'Union européenne sur l'intelligence artificielle (EU Artificial Intelligence Act, « EU AI Act »), aux spécificités du contexte de guerre en Ukraine. L'étude vise à évaluer les limites d'une mise en œuvre directe de l'EU AI Act dans des conditions de gouvernance publique d'urgence et à élaborer une approche réglementaire adaptative centrée sur la résilience numérique, la sécurité et la protection des droits humains. La méthodologie s'appuie sur un cadre interdisciplinaire et comprend une analyse juridique et réglementaire des dispositions de l'EU AI Act, une analyse comparative des approches internationales de régulation de l'IA, une analyse institutionnelle et structurelle-fonctionnelle de la gouvernance publique en temps de guerre, ainsi qu'un modèle conceptuel. Les résultats montrent que la logique statique fondée sur les risques de l'EU AI Act est insuffisante pour la gouvernance publique en temps de guerre, caractérisée par des pouvoirs d'exception, l'accélération des cycles décisionnels et le rôle croissant des systèmes algorithmiques. Des contraintes réglementaires majeures sont identifiées, ce qui plaide pour un basculement vers une approche flexible et sensible au contexte. Un modèle de régulation flexible de l'IA pour la gouvernance publique en temps de guerre est proposé, fondé sur les principes de proportionnalité, de temporalité et de renforcement du contrôle humain. La nouveauté scientifique réside dans une approche conceptuelle de la régulation de l'IA sous loi martiale, qui élargit le cadre de l'EU AI Act par l'intégration des conditions de guerre, d'un circuit réglementaire adaptatif et d'un système de garanties obligatoires de limitation des risques. La valeur pratique réside dans la possibilité d'utiliser ces résultats pour concevoir une politique nationale de l'IA et des instruments juridiques en Ukraine durant la loi martiale et dans le cadre de la reconstruction post-conflit.

Mots-clés **:** intelligence artificielle ; EU AI Act ; loi martiale ; gouvernance publique ; régulation ; résilience numérique.

Problem Statement

Digital transformation of public governance in Ukraine during the full-scale war has reached an unprecedented scale and pace. According to assessments by international organizations, during 2022–2024 more than 70% of basic administrative procedures in social protection, registration, identification, and public service delivery in countries operating under crisis or emergency governance regimes function in digital or hybrid formats, aligning with global trends in digital public infrastructure development (United Nations Development Programme, 2024).

Rapid deployment of digital solutions is accompanied by a growing role of algorithmic and AI-oriented systems in data governance, automated verification, risk forecasting, and decision support. World Economic Forum (2025) assessments suggest that, under crisis and turbulent conditions, the share of automated or semi-automated managerial decisions may reach 40–60%, significantly exceeding peacetime levels dominated by human-centred decision-making (20–30%).

The use of artificial intelligence in public governance offers significant potential to enhance efficiency, responsiveness, and institutional adaptability. PwC (2024) reports that AI technologies may increase productivity of managerial and analytical processes by 15–25%, particularly under wartime constraints related to human and financial resource shortages.

At the same time, concentration of governance functions in digital and algorithmic systems intensifies socio-economic and legal risks. OECD (2024) research indicates that up to 30% of AI-based decisions in public governance may involve latent risks of discrimination, opacity, or erroneous predictions in the absence of clear regulatory frameworks, especially when human oversight is limited.

Martial law creates a specific institutional regime where national security priorities prevail over standard democratic procedures, and decisions are taken under high uncertainty and asymmetric threats. Under such conditions, as emphasized by Hannouf (2025), artificial intelligence becomes not only a technological tool but also a factor in redistributing public authority, potentially strengthening centralized control over data and governance processes without adequate global and national safeguards.

Research relevance is further reinforced by adoption of the EU Artificial Intelligence Act, which shapes a new normative paradigm for governing AI in the European Union by combining innovation development with protection of human rights, public interests, and digital sovereignty (European Parliament and Council of the European Union, 2024).

Implementation of the EU AI Act in the European Union establishes the world's first comprehensive risk-based model of AI regulation, classifying AI systems by threat level and imposing strict requirements for high-risk applications within public governance (European Parliament and

Council of the European Union, 2024). The model was designed for stable institutional environments and peacetime conditions, which complicates direct transposition into Ukraine's wartime public governance.

Escalating cyber threats add further risk. International analytical assessments show that during armed conflicts, the number of cyberattacks targeting government digital systems increases multiple times, and up to 30–40% of incidents involve automated or AI-enhanced tools (OECD, 2024; World Economic Forum, 2025). In the absence of a specialised legal regime for AI regulation during war, such dynamics create risks extending beyond technical failures to violations of human rights and the rule of law.

Consequently, a complex scholarly problem emerges: adapting the EU AI Act's risk-based model to Ukraine's wartime public governance while balancing security, digital resilience, and human rights protection. Addressing the problem requires flexible, context-sensitive regulatory approaches that preserve European legal standards while accounting for realities of emergency and wartime governance.

Review of Recent Research and Publications

Issues related to artificial intelligence regulation have been actively examined in works produced by international organizations and research centres. Major contributions to the global understanding of AI governance have been made by the European Commission through the development of the EU AI Act, the United Nations through the Digital Public Infrastructure initiative and the Global Digital Compact, as well as analytical and expert institutions such as the World Economic Forum (WEF), OECD, and PwC. (European Parliament and Council of the European Union, 2024; United Nations Development Programme, 2024; World Economic Forum, 2025; OECD, 2024; PwC, 2024)

Contemporary academic discourse on AI regulation in public governance is formed at the intersection of legal and regulatory, institutional, socio-economic, and ethical–political approaches. Most studies focus on peacetime conditions, stable institutional environments, and the functioning of full-fledged mechanisms of democratic accountability.

A core regulatory reference point in the field is the EU Artificial Intelligence Act (EU AI Act), which is widely discussed in scholarly literature as the first comprehensive risk-based model for AI regulation. Within this approach, AI systems are classified by risk level, while applications in public governance, security, social control, and justice are placed in the high-risk category. Researchers emphasize the preventive nature of the model, its focus on human rights protection, algorithmic

transparency, and accountability of public institutions. At the same time, the literature stresses that the EU AI Act has been designed for stable institutional systems and does not incorporate the specificities of emergency and wartime governance regimes. (European Parliament and Council of the European Union, 2024)

In parallel, international research has actively developed an institutional approach to AI within the concept of digital public infrastructure. UNDP reports consider digital and AI-oriented systems as instruments for ensuring continuity of government functions, social inclusion, and resilience under crisis conditions. (United Nations Development Programme, 2024) At the same time, UNDP highlights the need for safeguards to prevent abuse, excessive data concentration, and exclusion of vulnerable population groups, particularly under conditions of limited public oversight. (United Nations Development Programme, 2024)

Socio-economic and managerial dimensions of AI deployment are analysed in publications by the World Economic Forum, OECD, and PwC. These studies frame AI as a factor that can increase productivity of governance processes, optimize public resources, and compensate for workforce shortages. (OECD, 2024; PwC, 2024; World Economic Forum, 2025) However, they also emphasize that the expanding role of algorithmic decisions in public governance is associated with risks of diminished human oversight, decision opacity, and reduced trust in public institutions in the absence of clear regulatory frameworks.

A significant strand of scholarship addresses ethics and responsible AI use. (Dignum, 2019; Floridi, 2019; Floridi, 2023) In works by Luciano Floridi (2019) and Virginia Dignum (2019), AI is conceptualized as a new type of institutional agent that influences the nature of public authority and administrative decision-making. The authors stress the necessity of human-centredness, algorithmic explainability, and preservation of state responsibility. (Dignum, 2019; Floridi, 2019) Yet these concepts generally assume a stable legal environment and fully operational control procedures, which substantially limits their applicability in wartime conditions.

A separate research direction focuses on security aspects of AI use and emergency governance regimes. Studies by Paul Scharre (2018, 2023) and Matthias C. Kettemann (2024) examine the expanded role of automated systems in critical situations and the risks of weakened legal constraints under emergency state powers. These works underscore the importance of maintaining meaningful human control, but they concentrate primarily on military or international-law dimensions, leaving civil wartime public governance largely outside their analytical focus. (Kettemann, 2024; Scharre, 2018; Scharre, 2023)

A critical perspective is developed in works by Shoshana Zuboff (2019) and Evgeny Morozov (2019), which analyse digital technologies as instruments of power concentration and political control. (Morozov, 2019; Zuboff, 2019) Although these studies are not specifically oriented toward wartime contexts, their conclusions remain relevant for assessing risks of excessive algorithmic centralization of authority under war.

Special attention should be given to Hannouf (2025), where AI is examined as a factor reshaping global and national power structures. The author emphasizes that, in the absence of specialised regulatory mechanisms, AI may reinforce power asymmetries, which is particularly dangerous under martial law.

Overall, the reviewed sources demonstrate the dominance of normative and theoretical approaches tailored to peacetime and stable institutional conditions. At the same time, the contemporary literature lacks systematic studies addressing adaptation of risk-based AI regulatory models—particularly the EU AI Act—to conditions of wartime public governance. This constitutes a research gap and underlines the need to develop flexible, context-sensitive regulatory approaches capable of reconciling security requirements, digital resilience, and human rights protection.

Within the current European regulatory discourse, a key role is played by the EU Artificial Intelligence Act, which institutionalizes a risk-based, human-centred, and preventive approach to AI regulation. The Act classifies AI systems by risk levels, introduces mandatory requirements for high-risk uses, strengthens principles of transparency, human oversight, and accountability, and contributes to reinforcing the European Union’s digital sovereignty. Within this logic, AI is treated not only as an innovation technology but also as an object of public governance and ethical responsibility.

Formulation of the Article’s Objectives (Task Setting)

In line with the stated purpose, the article seeks to systematize current scholarly and regulatory approaches to the governance of artificial intelligence in public governance, with a focus on the risk-based model of the EU AI Act and related international approaches. The study aims to identify distinctive features of AI deployment in Ukraine’s wartime public governance, shaped by an emergency legal regime, asymmetric security threats, accelerated digitalization of state functions, and constraints on institutional oversight. The article also demonstrates that, under such conditions, the baseline risk-based regulatory logic requires contextual refinement, as requirements for decision speed increase and the risk profile changes. In addition, the study determines regulatory constraints that limit direct implementation of the EU AI Act under martial law, given institutional instability

and heightened demands for rapid administrative decision-making. On this basis, the article substantiates the feasibility of introducing flexible, context-sensitive regulatory mechanisms for AI use in wartime public governance, aimed at ensuring digital resilience, security, human rights protection, and adherence to democratic standards. The final outcome is a conceptual model for adapting EU AI Act approaches to Ukraine's wartime public governance, combining risk-based regulation with the principles of proportionality, temporality, and reinforced human oversight.

Presentation of the Main Research Material

The main body is structured as a sequential development of the argument: from the European Union's baseline regulatory framework to analysis of conditions for AI use within Ukraine's public governance under the legal regime of martial law, and further to the design of practically feasible adaptation mechanisms. This logic aligns a risk-based regulatory model with real governance constraints arising under emergency conditions, while preserving priorities of security, digital resilience, accountability, and human rights protection. The focus is placed not on formal transposition of EU AI Act provisions, but on their functional suitability for governance practices where the role of algorithmic systems expands, decision cycles accelerate, and risks of error, abuse, and opacity intensify.

To ensure analytical coherence and a transition from the regulatory framework to applied conclusions, the paper distinguishes interrelated analytical blocks that reflect stages of adapting risk-based regulation to Ukraine's public governance under martial law. These blocks include: the EU AI Act risk-based regulatory model; specificities of AI use in Ukraine's wartime public governance; constraints on direct implementation of the EU AI Act in such conditions; justification for flexible regulatory mechanisms; a conceptual vision for adapting the EU AI Act to wartime public governance; development of a conceptual model of flexible AI regulation and adaptation in wartime public governance; and directions for practical application of the model in national policy and secondary regulation. The essence of these blocks is outlined below.

1. Risk-based model of AI regulation under the EU AI Act

In scholarly and regulatory literature, AI governance in public governance increasingly relies on a risk-based approach, with the EU Artificial Intelligence Act (EU AI Act) (European Parliament and Council of the European Union, 2024) serving as its key embodiment. The Act introduces a classification of AI systems by risk level—from unacceptable to minimal—while imposing particularly stringent requirements for applications in public governance, security, and social control.

Scholarly assessments indicate that, within public governance, up to 60% of AI applications may fall into the high-risk category, as they affect access to public services, social benefits, personal identification, and administrative decision-making. (OECD, 2024) For such systems, the EU AI Act requires mandatory risk assessment procedures, human oversight, algorithmic transparency, and data documentation.

At the same time, the EU AI Act model is built on assumptions of institutional stability, full judicial oversight, and predictable administrative processes, which substantially limits its applicability under wartime conditions.

2. Specificities of AI use in Ukraine's wartime public governance

Martial law creates a fundamentally different public governance regime characterized by emergency powers of public authorities, accelerated decision-making, and an expanded role of digital tools. According to United Nations Development Programme (2024), under crisis and wartime conditions more than 70% of core state functions shift to digital or hybrid formats, while the share of automated decisions rises to 40–60%. (World Economic Forum, 2025)

Reports by the World Economic Forum (2025) and PwC (2024) suggest that AI use in the public sector during crises enables the following: (World Economic Forum, 2025; PwC, 2024)

- reducing administrative decision-making time by 20–30%;
- compensating for shortages of human resources;
- increasing productivity of analytical functions by 15–25%.

At the same time, risks grow related to concentration of sensitive data, algorithmic opacity, and reduced accountability, which becomes particularly dangerous under limited public and judicial oversight.

3. Constraints on direct implementation of the EU AI Act under wartime conditions

Analysis of scholarly sources and public governance practice makes it possible to identify key constraints on applying EU AI Act provisions in a wartime context. They stem from tension between regulatory rigidity and the need for operational governance, as well as from the practical inability to fully ensure all procedural requirements under conditions of war.

4. Rationale for Flexible Regulatory Mechanisms

In light of the constraints identified above, a shift from a rigid, universal regulatory model toward flexible regulatory mechanisms tailored to wartime public governance is scientifically justified. This approach aligns with the positions of Luciano Floridi (2019), Virginia Dignum (2019), and Matthias C. Kettemann (2024), who emphasize the need to preserve human-centred governance even under crisis conditions. (Dignum, 2019; Floridi, 2019; Floridi, 2023; Kettemann, 2024)

Table 1. Comparison of the EU AI Act approach and the conditions of wartime public governance in Ukraine

Criterion	EU AI Act approach	Wartime public governance in Ukraine
Institutional environment	Stable, predictable	Emergency, highly dynamic
Decision-making regime	Procedural, multi-level	Accelerated, crisis-driven
Share of AI-enabled decisions	20–30%	40–60%
Human oversight	Full, formally structured	Partially constrained
Judicial and public oversight	Continuous	Temporarily limited
Primary regulatory priority	Human rights protection	Security and resilience
Risk of algorithmic centralization	Moderate	Elevated

Source: synthesised from (European Parliament and Council of the European Union, 2024; OECD, 2024; United Nations Development Programme, 2024; World Economic Forum, 2025); percentage ranges are approximate.

Key principles of flexible regulation should include:

- proportionality of regulatory requirements to the level of threat;
- temporality of emergency regulatory derogations and accelerated procedures;
- reinforced human oversight over critical AI-enabled decisions;
- post-crisis auditing of algorithmic systems.

5. Conceptual Vision for Adapting the EU AI Act to Wartime Public Governance

Based on the analysis, a conceptual vision for adapting the EU Artificial Intelligence Act (EU AI Act) is developed, combining the risk-based approach with the principles of digital resilience and security. In the proposed framework, AI is not treated as an autonomous subject of governance; it is conceptualized as a decision-support and operational tool whose use is subordinated to the state's strategic objectives and to the preservation of human rights under martial law.

The core idea of the model is the introduction of an adaptive regulatory loop that supplements the baseline logic of the EU AI Act with contextual parameters of emergency governance. (European Parliament and Council of the European Union, 2024; Dignum, 2019; Floridi, 2023; Kettemann, 2024) This loop enables flexibility without diluting human-rights standards by institutionalizing three principles.

Proportionality means that the permissible scope of AI use and the required level of oversight are determined by the balance between expected public benefit and potential harm.

Temporality introduces a regime-based, time-limited nature of special authorizations, accelerated procedures, and derogations from standard compliance processes, with mandatory review

triggered by defined events (change in threat level, change in function, incident, complaint, model update).

Reinforced human oversight establishes non-delegable responsibility of the public official and prohibits full automation of decisions with high impact on rights, freedoms, and access to public goods.

Structurally, the model differentiates AI applications in wartime public governance by impact and risk, focusing on domains with the highest probability of negative externalities: identity verification, access to social benefits and services, administrative ranking/prioritization, resource allocation, decision-making in security, and critical infrastructure. For such cases, a system of mandatory risk-mitigation safeguards is proposed as a minimal set that does not depend on institutional capacity. These safeguards include: documenting the purpose of use; defining the boundaries of use and admissibility criteria; ensuring data quality and result traceability; designating a responsible process owner and escalation procedures; auditability and retention of event logs; bias and error testing on critical groups; and a rapid mechanism to suspend or restrict use in case of incidents.

A separate component of the model is a fast-track compliance assessment regime, applied under time and resource constraints, replacing “full” compliance with a minimally sufficient package of safeguards. It includes rapid risk screening, specification of admissible use scenarios, determination of the level of human oversight, transparency obligations toward affected persons (notification of AI use and limits of automation), and ex post review procedures with mandatory reconsideration of contested or high-impact decisions. This approach narrows the regulatory gap between operational urgency and accountability requirements while preserving the core rights-protective guarantees.

Overall, adaptation of the EU AI Act to Ukraine’s wartime public governance is conceptualized as a system that integrates risk-based regulation with resilience and security governance, ensures control over high-impact applications, and minimizes risks of opacity, error, discrimination, and abuse of emergency powers.

6. Conceptual Model of Flexible AI Regulation in Wartime Public Governance

The analysis of academic sources, regulatory approaches, and the specificities of wartime public governance makes it possible to develop a conceptual model of flexible AI regulation that integrates the risk-based logic of the EU AI Act with the needs of emergency governance, digital resilience, and security.

Unlike the classical EU AI Act model, designed for stable institutional environments, the proposed approach introduces an adaptive regulatory loop in which requirements vary depending on:

- the level of wartime threat;
- the criticality of the governance function;
- the degree of impact of the AI system on human rights.

The model's central idea is to preserve human-centred governance even under expanded state powers, in line with Floridi (2019) and Dignum (2019), while incorporating wartime realities.

Model architecture

The proposed model is built on the interaction of five interrelated blocks that reflect the transition from wartime context to regulatory outcomes.

Block 1 - Wartime governance context. This block reflects governance under martial law, emergency powers, asymmetric threats, constrained decision time, and heightened uncertainty.

Block 2 - AI systems in public governance. This block covers automated data processing, risk forecasting, decision support, digital public services, and cybersecurity components. International assessments indicate that in crisis conditions the share of AI-supported managerial decisions may reach 40–60%. (OECD, 2024; World Economic Forum, 2025)

Block 3 - Adapted risk-based regulatory loop. This block is the core of the model. It relies on the EU AI Act logic but is modified to account for wartime conditions. It provides for:

- simplified procedures for low-risk AI systems;
- a reinforced oversight regime for high-risk applications;
- time-limited regulatory derogations for critical wartime AI applications, with clearly defined validity periods and review triggers.

Block 4 - Safeguards and human oversight mechanisms. This block performs a preventive function and includes maintaining human-in-the-loop, logging algorithmic decisions, post-war auditing of AI systems, and restoration of full oversight after the end of the emergency regime, consistent with UNDP recommendations.

Block 5 - Expected regulatory outcomes. This block captures the expected effects of the flexible model: strengthening state digital resilience; maintaining controllability of AI systems; reducing the likelihood of human-rights violations; lowering algorithmic opacity; and sustaining trust in public authority under wartime conditions.

Methodological limitations of applying the EU AI Act under wartime conditions

The study is conceptual and analytical in nature, which entails methodological limitations to be considered when interpreting results.

First, the EU AI Act risk-based model presupposes institutional stability, continuous judicial and public oversight, and predictable administrative processes. Under martial law, democratic accountability mechanisms may be temporarily constrained or transformed, which complicates direct application of certain provisions without adaptation.

Second, the research does not rely on empirical data regarding the practical implementation of AI regulation in Ukraine during the war due to restricted access to sensitive information in security and public governance domains. Therefore, the results represent theoretical generalization and conceptual modelling rather than an evaluation of effectiveness in specific administrative cases.

Third, the wartime context is highly dynamic and unpredictable, limiting the feasibility of universal regulatory solutions. The proposed model does not claim normative universality and is presented as a framework that may vary with the intensity of hostilities, institutional digital maturity, and the nature of security threats.

Fourth, the article focuses on civil wartime public governance. The use of AI in military systems, autonomous weapons, and operational–tactical command and control is intentionally excluded, as it requires separate legal and ethical analysis.

These methodological limitations also point to directions for further research, particularly empirical validation of AI regulatory models and comparative analysis of wartime and post-war public governance regimes.

Directions for Further Research

Further research should focus on: (i) empirical assessment of the effects of AI systems on the effectiveness of wartime public governance; (ii) development of indicators for digital resilience; and (iii) analysis of legal mechanisms that support Ukraine’s integration into the European digital space during post-war recovery.

Conclusions

The article provides a comprehensive analysis of challenges related to regulating artificial intelligence in public governance under martial law and substantiates the need to adapt the EU AI Act’s risk-based approaches to the specificities of Ukraine’s wartime context.

It is established that direct implementation of the EU AI Act in wartime conditions is constrained, as the Act is grounded in assumptions of institutional stability, fully operational procedural oversight, and peacetime governance. By contrast, wartime public governance is

characterised by emergency powers, accelerated decision-making, and increased reliance on digital and AI-enabled tools.

The study demonstrates that, during war, AI functions not only as a technological instrument but also as a factor of redistributing governance power. This intensifies risks of algorithmic opacity, data concentration, and potential human rights violations in the absence of specialised regulatory mechanisms.

Drawing on the analysis of academic sources and international approaches, the paper proposes a model of flexible AI regulation in wartime public governance that combines the EU AI Act logic with the principles of adaptability, proportionality, and temporality of regulatory decisions. A key feature of the model is a shift from static rule-setting to a context-sensitive regulatory loop while mandating the preservation of human oversight mechanisms and ex post accountability.

It is argued that implementing a flexible approach to AI regulation can ensure state digital resilience without abandoning fundamental legal and democratic standards, even under martial law. The proposed framework may serve as a conceptual basis for shaping national AI regulatory policy in Ukraine during the war and throughout post-war recovery.

Further studies should prioritise empirical validation of the proposed model and analysis of sector-specific implementation practices across public governance. Promising lines of inquiry also include designing mechanisms to integrate AI regulatory regimes operating under martial law with peacetime regimes into a unified system of digital governance. A separate research direction concerns the development of digital resilience indicators and the analysis of legal mechanisms for Ukraine's integration into the European digital space during post-war recovery.

References

Dignum, V. (2019). *Responsible artificial intelligence*: *How to develop and use AI in a responsible way*. Springer. https://doi.org/10.1007/978-3-030-30371-6

European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Floridi, L. (2019). Translating principles into practices of digital ethics: Five risks of being unethical. *Philosophy & Technology, 32*(2), 185–193. https://doi.org/10.1007/s13347-019-00354-x

Floridi, L. (2023). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press.

Hannouf, K. (2025). *How artificial intelligence is reshaping power structures—and why the world needs a global digital constitution* [Working paper / policy essay]. https://www.ukrinform.ua/rubric-diaspora/4056434-ukrainska-diaspora-proponue-francuzam-spivpracu-z-pricilom-na-vidbudovu.html

Kettemann, M. C. (2024). Digital sovereignty, emergency powers and AI governance. *European Journal of International Law, 35*(2), 367–390. https://doi.org/10.1093/ejil/chad045

Morozov, E. (2019). Digital socialism? The calculation debate in the age of big data. *New Left Review, 116*, 33–67. https://newleftreview.org/issues/ii116/articles/evgeny-morozov-digital-socialism

OECD. (2024). *Governing with artificial intelligence*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf

PwC. (2024). *PwC's 2024 global AI jobs barometer*. https://rgb-prod-public-pdfs.s3.us-east-2.amazonaws.com/iK88ETzspoNNn2_z65pzs3renyQ.pdf

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. W. W. Norton & Company.

United Nations Development Programme. (2024). *Universal DPI safeguards framework: A guide to building safe and inclusive digital public infrastructure (DPI) for societies*. https://www.dpi-safeguards.org/framework

World Economic Forum. (2025). *The future of jobs report 2025*. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

Reçu le : 27/01/2026
Accepté le : 27/01/2026
Publié le : 26/03/2026