e-ISSN **3041-248X**

Philosophy and Governance

https://www.eu-scientists.com/index.php/fag

Post-War Reconstruction Through Digitalization: Recommendations for the Social Protection Sphere in Ukraine

Maksym Yamkovyi [1] • Viktoriia Zalizniuk [2] *

[1] *State University of Trade and Economics (Ukraine). PhD Student at the Department of Public Management and Administration.*

[2] *State University of Trade and Economics (Ukraine). Head of the Department of Public Administration and Administration, Doctor of Science in Public Administration, Professor.*

* ***Corresponding Author,*** e-mail: zalvikii@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3041-248X/2026.2.02

Received:
29 December 2025
Accepted:
31 January 2026
Published online:
6 February 2026

ABSTRACT

The article analyzes the conceptual, regulatory, institutional and technological foundations of the digital transformation of the social protection system of Ukraine in the context of post-war reconstruction and European integration transformations. Digitalization is considered a systemic tool for ensuring the continuity of social services, increasing their targeting, accessibility and institutional stability in the context of large-scale socio-economic shocks caused by armed aggression. Based on the analysis of international approaches to the development of digital public infrastructure, in particular the concept of Digital Public Infrastructure, it was found that the effectiveness of the modern model of social protection is determined by the level of integration of digital identity, social registers, interoperable data exchange platforms, analytical tools and multi-channel service mechanisms for interaction with users. It is substantiated that the formation of a single digital architecture of social protection contributes to reducing the administrative burden, increasing the accuracy of verification of the right to assistance, optimizing management decisions and ensuring the adaptability of the system to crisis conditions. The institutional prerequisites for the digital modernization of the social sphere of Ukraine are determined, including the development of the Unified Information System of the Social Sphere, the functioning of the electronic services platform and the implementation of mechanisms for the interoperability of state registers. It is proven that the digitalization of social protection is not only a technological process, but a complex institutional transformation that combines legal regulation, data management, cybersecurity, organizational changes and the development of digital competencies of personnel. On this basis, a conceptual model and a roadmap for the phased implementation of digital transformation have been developed, which involves the formation of integrated digital services, the development of analytical and algorithmic tools, ensuring compliance with European standards of data protection and cyber resilience, as well as the implementation of the principles of human-centricity and inclusiveness. The study concluded that digitalization is a key factor in increasing the efficiency, transparency and sustainability of the social protection system, ensuring its adaptability to post-war challenges, contributing to improving the quality of social process management and creating the prerequisites for Ukraine's integration into the European digital space of social policy.

KEYWORDS

digitalization, social protection, post-war recovery, digital public infrastructure, Unified Information System of the Social Sphere, social registers, interoperability, digital identity, electronic public services, artificial intelligence, cybersecurity, inclusiveness, public administration, European integration.

e-ISSN **3041-248X**

Філософія та управління

https://www.eu-scientists.com/index.php/fag

Поствоєнне відновлення через цифровізацію: рекомендації для сфери соціального захисту в Україні

Максим О. Ямковий [1] ● Вікторія П. Залізнюк [2] *

[1] *Державний торговельно-економічний університет (Україна). Аспірант кафедри публічного управління і адміністрування.*

[2] *Державний торговельно-економічний університет (Україна). Завідувачка кафедри публічного управління та адміністрування, д-р держ. упр., професор.*

* ***Автор-кореспондент,*** e-mail: zalvikii@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3041-248X/2026.2.02

Отримана: 29.12.2025 р.
Прийнята: 31.01.2025 р.
Опублікована: 06.02.2026 р.

АНОТАЦІЯ

У статті проаналізовано концептуальні, нормативно-інституційні та технологічні засади цифрової трансформації системи соціального захисту України в умовах поствоєнного відновлення та євроінтеграційних перетворень. Розглянуто цифровізацію як системний інструмент забезпечення безперервності надання соціальних послуг, підвищення їх адресності, доступності та інституційної стійкості в умовах масштабних соціально-економічних потрясінь, спричинених збройною агресією. На основі аналізу міжнародних підходів до розвитку цифрової публічної інфраструктури, зокрема концепції Digital Public Infrastructure, з'ясовано, що ефективність сучасної моделі соціального захисту визначається рівнем інтегрованості цифрової ідентичності, соціальних реєстрів, інтероперабельних платформ обміну даними, аналітичних інструментів та багатоканальних сервісних механізмів взаємодії з користувачами. Обґрунтовано, що формування єдиної цифрової архітектури соціального захисту сприяє зниженню адміністративного навантаження, підвищенню точності верифікації права на допомогу, оптимізації управлінських рішень і забезпеченню адаптивності системи до кризових умов. Визначено інституційні передумови цифрової модернізації соціальної сфери України, включаючи розвиток Єдиної інформаційної системи соціальної сфери, функціонування платформи електронних послуг та впровадження механізмів інтероперабельності державних реєстрів. Доведено, що цифровізація соціального захисту є не лише технологічним процесом, а комплексною інституційною трансформацією, яка поєднує правове регулювання, управління даними, кібербезпеку, організаційні зміни та розвиток цифрових компетенцій персоналу. На цій основі розроблено концептуальну модель і дорожню карту поетапної реалізації цифрової трансформації, що передбачає формування інтегрованих цифрових сервісів, розвиток аналітичних і алгоритмічних інструментів, забезпечення відповідності європейським стандартам захисту даних і кіберстійкості, а також впровадження принципів людиноцентричності та інклюзивності. У результаті дослідження сформовані висновки, що цифровізація виступає ключовим чинником підвищення ефективності, прозорості та стійкості системи соціального захисту, забезпечує її адаптивність до поствоєнних викликів, сприяє підвищенню якості управління соціальними процесами та створює передумови для інтеграції України до європейського цифрового простору соціальної політики.

КЛЮЧОВІ СЛОВА

цифровізація, соціальний захист, поствоєнне відновлення, цифрова публічна інфраструктура, єдина інформаційна система соціальної сфери, соціальні реєстри, інтероперабельність, цифрова ідентичність, електронні публічні послуги, штучний інтелект, кібербезпека, інклюзивність, публічне управління, євроінтеграція.

1. Introduction

The post-war reconstruction of Ukraine actualizes the need for structural modernization of the social protection system as one of the basic institutions for ensuring social stability, poverty reduction and restoration of human capital. In the context of large-scale demographic changes, internal displacement of the population, loss of income, destruction of infrastructure and growth of budget constraints, the social protection system faces the need to simultaneously expand support coverage, increase targeting the allocation of resources and ensure institutional resilience to repeated shocks. According to the RDNA4 estimates, employment, means-tested programs, support for internally displaced persons, and restoration of social services are identified as priority areas for recovery, which indicates the systemic nature of transformational tasks in this area [8].

At the same time, state policy defines digitalization as a key tool for the modernization of the social sphere, which is enshrined in the Strategy for Digital Transformation of the Social Sphere, which provides for the regulatory and technological renewal of the components of the social protection system [2].

However, the presence of a regulatory framework does not guarantee the systematic integration of digital tools into the mechanisms of targeting, verification of eligibility for assistance, case management, payment and protection of personal data. Thus, there is a scientific and practical problem of determining the conceptual foundations and applied recommendations for the use of digitalization as a tool for post-war recovery in the field of social protection, taking into account the requirements of efficiency, transparency, security and social justice.

2. Literature Review

In modern academic discourse, the digital transformation of the public sector is conceptualized primarily through the category of Digital Public Infrastructure (DPI), which is considered as a set of interoperable and secure digital components (digital identity, data exchange, payment mechanisms) that ensure the scalability, efficiency and sustainability of public services. At the same time, the OECD documents focus on the structural risks of digital transformation, in particular, digital exclusion, threats of inappropriate use of data, and technological dependence on suppliers, which actualizes the need for institutional capacity and proper data management [16].

The development of this approach can be traced in the works on the phenomenon of digital resilience, where digital infrastructure is interpreted as a key factor in maintaining the functional capacity of the state in the face of military and crisis challenges. Brookings' analytical materials link the scaling of Ukrainian digital services with the processes of cloudization, cyber defense, and adaptation of management procedures to the military context, while emphasizing the need to bridge the digital divide and modernize the registry architecture [1].

Within the framework of research on the digitalization of social protection, the focus is shifting to the transformation of the delivery chain. Empirical results show that the introduction of digital self-service mechanisms can redistribute the administrative burden on users ("accidental caseworker"), which is especially noticeable for socially vulnerable groups. This justifies the need to evaluate digital reforms not only according to performance criteria, but also through the prism of accessibility and fairness [12].

At the same time, a scientific discourse on "digital welfare state" is being formed, within which the consequences of intensifying the use of data and algorithmic decisions in social policy are analyzed. The researchers draw attention to the risks of opacity, potential discrimination, and a decrease in the level of public participation in the adoption of data processing rules, which raises the question of the legitimacy of digital reforms [19].

In addition, the OECD analyzes the use of artificial intelligence in social security as a tool for optimizing eligibility checks and payment administration, emphasizing the need to implement risk management, human oversight and accountability systems. These approaches correlate with the regulatory requirements of the European Union for high-risk artificial intelligence systems [17].

The Ukrainian context of digitalization of the social sphere is characterized by the institutionalization of the UISSS as an integrated platform for social data management and the development of inter-register interaction through the Trembita system, which forms the technological basis of electronic services and extraterritorial access to them [5; 13].

Generalization of scientific and analytical sources allows us to state that, despite a significant array of studies, institutional mechanisms for assessing the impact of digital solutions on the accessibility of social protection, the issue of integrated cyber resilience and overcoming the fragmentation of the registry architecture, which necessitates further comprehensive analysis, remain insufficiently developed.

3. Problem Statement

The purpose of the article is to scientifically substantiate the conceptual foundations and develop practical recommendations for the use of digitalization as a systemic tool for the post-war recovery of the sphere of social protection of Ukraine.

4. Methods and Materials

The study employs a combination of theoretical and analytical methods, including systemic approach to conceptualize digital transformation of social protection as an integrated sociotechnical system, comparative analysis of international DPI models (OECD, World Bank, EU standards) and Ukrainian practices, content analysis of regulatory acts (Laws of Ukraine on electronic services, public registers, personal data protection, Cybersecurity Strategy), strategic documents (Digital Transformation Strategy of the Social Sphere, RDNA4, Recovery Plan), and international reports (OECD, Brookings, EU4DigitalUA). The research draws on monographs, scientific articles, official Ukrainian legislation (as of 2025–2026), analytical materials from international organizations (OECD, World Bank, NIST, W3C), and statistical data on Diia usage, UISSS development, and Trembita interoperability to substantiate the conceptual model and phased roadmap for digitalization of social protection in post-war Ukraine.

5. Results and Discussion

The conceptual framework of the post-war reconstruction of social protection requires a transition from the fragmentary logic of the introduction of individual electronic forms to the formation of an integral architecture of social protection as a sustainable digital service system. In the OECD approaches, Digital Public Infrastructure (DPI) is defined as a set of common interoperable "building blocks" that ensure the functioning of many sectors of public policy. Social protection. This means the formation of an integrated stack that encompasses digital identity and trust services, interoperable data exchange, payment mechanisms, industry registers and social register, business process orchestration (case management), as well as multi-channel models of user interaction (online, offline, assisted digital) [16].

The Ukrainian institutional trajectory creates preconditions for the implementation of such a model. The strategic vector of the digital transformation of the social sphere was fixed in 2020 at the level of a government decision, which determined the regulatory and organizational basis for the modernization of the industry [2]. At the operational level, the Unified Information System of the Social Sphere (UISSS) is being formed, which is positioned as a tool for integrating disparate information systems and ensuring extraterritorial access to support regardless of the place of registration or stay [13].

At the same time, the national digital interface of public services – Diia – is functioning, which, according to the results of the 2021 assessment, united more than 11 million unique users and a set of digital documents, including a certificate of an internally displaced person [4]. In 2023, the number of users increased to 20 million, which indicates the high potential of this platform as a channel for delivering social services in crisis conditions [10].

The functional evolution of digital services involves a shift to a "life-event services" model that integrates several administrative procedures within a single life scenario and reduces the transaction costs of households that have experienced displacement, loss of documents or changes in family status. The practice of comprehensive services demonstrates the possibility of integrating registration and social components within a single process. The war context has additionally actualized the need for scalable assistance platforms: a significant volume of applications submitted on the eDopomoga

platform confirms the need for a sustainable infrastructure for processing, validating, and coordinating social payments.

Digital identity is a key prerequisite for the functioning of social protection in electronic format, since identification errors have direct budgetary and legal consequences. The Ukrainian model of electronic passports has enshrined the legal equivalence of digital and physical documents [23]. Further development of this direction involves the introduction of a digital identity wallet in the Diia application, which is determined by a government decision of 2025 [3]. Given the European integration course, such decisions should be consistent with the reform of eIDAS and Regulation (EU) 2024/1183 on the European Digital Identity [6].

A fundamental condition for the effectiveness of social protection is the interoperability of registers and platforms, since verification of eligibility for assistance involves the processing of significant amounts of data on household composition, income, employment, disability and displacement status. In this context, the Trembita system ensures secure data exchange between state registers and creates an infrastructural basis for the development of electronic services [5]. At the same time, the UISSS in the state architecture functions as a sectoral superstructure aimed at integrating social registers and business processes and reducing the territorial linkage of the provision of services. However, in order to assess its strategic potential, it is advisable to consider such an architecture as a technical solution for data integration and as an element of a broader transformation of the social protection paradigm. It is in this dimension that the international analytical and scientific literature has formed an approach to considering social registers as an institutional basis for shock-responsive social protection. In this context, the register is interpreted not as a static database of aid recipients, but as a dynamic information and analytical tool capable of ensuring the prompt deployment of interventions in response to crisis events.

According to the World Bank, the effectiveness of such systems depends on their ability to regularly update data, include valid vulnerability indicators, and ensure interoperability with other government information resources, which creates prerequisites for more accurate targeting and rapid scaling of support [9]. Thus, the functional capacity of social protection is increasingly correlated with the quality of data architecture.

The Ukrainian context of recovery after full-scale aggression confirms this pattern. The RDNA4 materials emphasize that along with the physical reconstruction of social infrastructure facilities, the continuity of social benefits and services is of decisive importance in the context of a sharp change in the structure of household incomes, internal displacement of the population and high macroeconomic uncertainty [8]. This objectifies the need for analytical tools that provide scenario modeling and forecasting of needs, as well as support data-driven decision-making.

Further digitalization of social protection is associated with the introduction of automated decision-making (AI/ADM) systems. The OECD records examples of the use of algorithmic solutions for verification of the right to payments, document processing and optimization of administrative processes, while emphasizing the need to comply with the principles of data quality, transparency of algorithms, risk management and prevention of discriminatory consequences [14]. In this regard, the integration of AI requires a combination of technological efficiency with regulatory safeguards for the protection of human rights and procedural fairness.

Empirical studies of digital "self-service" in public administration demonstrate the ambivalent nature of digitalization. In particular, Madsen et al. [12] prove that the transfer of administrative procedures to the digital environment without proper support and a clear interface can increase the administrative burden of citizens, especially in difficult life situations, transforming them into "random case managers". This justifies the need for a human-centered automation model that combines digital tools with the possibility of face-to-face or consultative support.

In the European integration dimension, the design of digital social protection systems should be carried out taking into account the EU regulatory environment, in particular the AI Act regime, which establishes special requirements for high-risk systems, including transparency, accountability, and assessment of the impact on fundamental rights. Therefore, algorithmic decisions in the social sphere must comply with the principles of legal certainty, proportionality and non-discrimination.

Cybersecurity is an integral structural component of the digital transformation of social protection. Since these systems operate with significant amounts of personal and sensitive data, cyber risk management should be carried out at the strategic and operational levels. In Ukraine, the strategic guidelines are determined by the Cybersecurity Strategy approved by the Decree of the President of

Ukraine No. 447/2021 [18]. At the international level, the methodological basis is NIST CSF 2.0 (2024), which systematizes the results of management cyber risks and singles out the "Govern" function as a separate dimension of strategic management [15]. At the same time, ISO/IEC 27001:2022 defines requirements for information security management systems (ISMS) [17], and Directive (EU) 2022/2555 (NIS2) strengthens risk management and incident reporting requirements for essential and important entities within the EU [7]. Harmonization with these standards is a prerequisite for the institutional sustainability of digital social services.

At the same time, the principle of inclusiveness of digital transformation provides for the implementation of a "digital-first, but not digital-only" approach. The materials of the Recovery Plan of Ukraine indicate that the limitations of digital systems are associated with the insufficient level of digital literacy of some beneficiaries and uneven access to the Internet [14], which is consistent with international approaches to the development of digital public infrastructure (DPI), which identify the risk of exclusion of persons with a low level of digital skills. In this regard, it is necessary to develop "assisted digital" mechanisms (ASCs, social workers, hotlines, mobile teams) and ensure that digital services comply with accessibility standards, in particular WCAG 2.2 as a W3C recommendation [24].

Thus, the modern architecture of social protection in the context of recovery should be considered as a comprehensive sociotechnical system integrating dynamic registers, algorithmic tools with legal guarantees, standardized cyber risk management and inclusive access mechanisms. Only the systemic interaction of these components ensures the adaptability, legal legitimacy and sustainability of the digital transformation of social policy.

The digital transformation of the social protection system provides for the introduction of information and communication technologies and the formation of a holistic and coordinated legal architecture that determines the principles of the functioning of electronic services, data circulation and guarantees of protection of the rights of subjects. The regulatory basis for the legal regime of electronic public services is the Law of Ukraine "On the Peculiarities of the Provision of Public (Electronic Public) Services" dated 06.10.2020 No. 1689-IX, which defines the concept of electronic public service, establishes the possibility of its provision in automatic mode and fixes the principles of digital interaction between the subjects of provision and recipients of services [21].

The institutional prerequisite for the implementation of automated procedures is the legal regime of public electronic registers, enshrined in the Law of Ukraine "On Public Electronic Registers" dated 22.10.2020 No. 1907-IX (as amended), which establishes the legal and organizational foundations for the creation, maintenance, interaction and operation of public electronic registers, defines the requirements for their interoperability, reliability and information protection [22]. Thus, digital social protection is based on a normatively defined system of data exchange and integration.

The basic requirements are established by the Law of Ukraine "On Personal Data Protection" dated 01.06.2010 No. 2297-VI, which defines the grounds, principles and guarantees for the processing of personal information, including sensitive data, which are widely used in the field of social security [20]. At the same time, in the context of European integration, the modernization of national legislation is underway in order to harmonize it with the provisions of the GDPR, which reflects the tendency to tighten standards for the protection of the rights of data subjects.

An integral part of the legal architecture of digital social protection is the regulation of cybersecurity and cryptographic protection of information. The strategic principles are determined by the Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" dated 14.06.2021 No. 447/2021, which outlines long-term priorities for the formation of a national cybersecurity system, including the protection of state information resources [18]. The implementation of these provisions is specified in bylaws and standards in the field of cryptographic protection of information.

Financial support for digital transformation also has a regulatory basis. In particular, the Resolution of the Cabinet of Ministers of Ukraine "Some Issues of the Implementation of the Pilot Project on the Formation and Use of Electronic Identity Certificates and Electronic Attributes Certificates Using a Wallet with Digital Identification as a Functionality of the Mobile Application of the Unified State Web Portal of Electronic Services (Diia)" dated 24.10.2025 No. 1400 provides for the financing of the relevant project at the expense of the state budget, international technical assistance and other sources not prohibited by law [3]. In addition, international support for digital transformation is confirmed by the European Union's 2026 decision to allocate funding for the development of Trembita 2.0 and bring data management closer to European standards.

Along with regulatory and financial support, personnel and organizational changes are crucial. Scientific studies of the digital transformation of social security show that its effectiveness depends on the level of digital competencies of staff, the ability of institutions to manage change, the optimal distribution of functions between a person and automated systems, as well as ensuring institutional accountability [12]. For Ukraine, this means the need for systematic training of social professionals in the areas of digital skills, data analytics, cyber hygiene and service design of public services.

Therefore, digital social protection should be considered as a comprehensive institutional transformation that combines the regulation of electronic services, the functioning of registers, personal data protection, cybersecurity, financial support and personnel modernization. The effectiveness of this transformation should be assessed by a system of measurable performance indicators, in particular in terms of accessibility, quality, reach, inclusion, safety and the level of public trust. After analyzing the regulatory, institutional, financial and personnel prerequisites for the digital transformation of social protection, it is advisable to move to the instrumental level of research. In particular, in order to systematize technological components and assess their functional role in the architecture of digital social protection, it is necessary to apply a comparative approach that allows correlating individual technologies with their functions, implementation risks and minimum safeguards that ensure the legal, organizational and technical stability of the system.

Based on the above, we will present a generalized comparative matrix of digital social protection technologies and tools, which is basic in nature and is subject to adaptation depending on a specific program, territorial community or departmental system, taking into account local parameters (data owners, source registers, interaction channels, cost of ownership, risk profile). Its application is aimed at supporting management decisions within the digital change portfolio.

Table 1. Generalized comparative matrix key components of digital social protection

Component	Functional purpose	Main risks	Key Fuses and Metrics
E-services and digital identity	Submission of applications, identification, signature, access to personal data	Digital Divide; exclusion of vulnerable groups; Compromise of credentials	The principle of "digital-first, not digital-only"; MFA; Success rate average processing time; NPS/CSAT
Interoperability and social registers	Automatic checks; the principle of "data once"; Targeting of assistance	Data errors; leaks; fragmentation; decreased trust	Data quality standards; access logging; audit; coverage of the register; Share of appeals
Analytics and AI	Decision support; detection of anomalies; Load forecasting	Discrimination; opacity of algorithms; false positives	AI impact assessment; human-in-the-loop; Bias/False Positives Metrics
Cybersecurity and resilience	Data protection; Continuity of services	Cyber attacks; service suspension; Compromise of information	Implementation of NIST CSF 2.0 / ISO 27001; DR/BCP; RTO/RPO
Accessibility and inclusion	Equal access for people with disabilities, the elderly, people with limited mobility	Exclusion of groups; Violation of rights	WCAG 2.2 AA; Part of the Assisted Digital; Inclusive Coverage Indicators

Source: [21].

The presented matrix demonstrates that digital social protection is a multi-component sociotechnical system in which technological solutions must correlate with risks, safeguards and measurable performance indicators. At the same time, a systematic understanding of the architecture of components requires their ordering in the time and management sequence of implementation. In this regard, it is advisable to supplement the analytical generalization of the tools with a phased implementation model, which reflects priorities, institutional capacities and resource constraints in the context of recovery.

Table 2 presents the roadmap in three phases. It is consistent with the logic of the stages traced in the materials of the Recovery Plan of Ukraine, as well as with the approach to short-, medium- and long-term horizons in digital recovery and institutional modernization policies.

The proposed model outlines a consistent transition from stabilizing basic digital processes to scaling an integrated data platform and further institutionalization of analytical tools with cyber resilience and European interoperability. At the same time, its implementation requires clearly defined management priorities and a systematic approach to minimizing risks.

First, the manageability and accountability of digital change. Digital transformation should be carried out within a continuous "policy-to-product" cycle, which provides for an interconnected sequence: regulation – service design – implementation – evaluation of results – correction of decisions.

It is advisable to supplement the quantitative indicators existing in the recovery planning documents (in particular, coverage of aid recipients) with metrics of the full-service provision process (execution time, the share of successful transactions, the level of errors and appeals, and indicators inclusion).

Table 2. Implementation Roadmap

Phase	Strategic focus	Key activities	Performance Indicators (KPIs)
0–12 months	Formation of a minimum viable digital chain of social support	Inventory of programs and registers; standardization of data and access; orchestration of priority services (IDPs, low-income, disability/care, subsidies); deployment of assisted digital; basic cyber resilience measures (logging, redundancy, DR plans)	Share of paperless applications; average term of appointment; share of automatic validation; Assisted digital coverage; reducing the number of critical incidents
1–3 years	Scaling of the UISSS, interoperability and data management	Expansion of registry integrations; introduction of a dynamic social register/household profile; standardization of data exchange with MFIs; data quality management systems; strengthening the personal data protection regime (approximation to the GDPR)	Targeting accuracy; share of data reuse ("data once"); reduction of errors and appeals; coverage of the social register; Access audit results
3–6 years	Industrialization of analytics and AI, European DPI interoperability	Integration of digital identity (digital wallet); implementation of AI tools with audits; development of Trembita 2.0 and data management standards; increasing cyber management maturity (NIS2 compatible practices)	Reduction of administrative burden (time/number of visits); indicators of trust and satisfaction; coverage of digital identity; compliance with standards; Results of AI fairness audits

Source: [21].

Secondly, the protection of personal data on the principle of "privacy by design". Social protection as a field of sensitive information processing requires legal certainty and harmonization with European standards. The current Law of Ukraine "On Personal Data Protection" dated 01.06.2010 No. 2297-VI establishes basic guarantees, while initiatives to modernize legislation indicate a focus on approximation to GDPR approaches. and implementing transparency policies on data collection, storage, and access.

Thirdly, inclusion as an architectural requirement. Recognition of the risks of digital illiteracy and uneven Internet coverage in materials restores necessitates a multi-channel access model, i.e. a combination of online services with assisted digital mechanisms, compliance with accessibility standards (WCAG 2.2), testing solutions with vulnerable groups, and ensuring offline loops of functioning in case of infrastructure failures.

Fourth, cyber resilience and continuity of operation. Given the threats of wartime, social services must remain operational in the face of cyberattacks and partial failures, which involves coordination with the national cybersecurity strategy, the application of risk management frameworks (NIST CSF 2.0), the implementation of information security management systems (ISO 27001) and the establishment of critical component recovery indicators (RTO/RPO).

Fifth, result-oriented financing. In the context of limited resources and significant sector needs (RDNA4), digital investments should be selected as efficiency tools that reduce administrative costs, minimize errors, and expand coverage. Mixed funding models (state budget + international technical assistance), which are already enshrined in regulations on digital components, in particular pilot digital identity projects, are appropriate.

Therefore, the implementation of the roadmap requires a combination of institutional manageability, legal guarantees of data protection, architectural inclusiveness, cyber resilience and results-oriented financing, which together ensures the resilience and legitimacy of the digital modernization of social protection.

6. Conclusions

Thus, based on the analysis of the regulatory, institutional, technological and organizational foundations of the digital transformation of social protection, it has been established that its effectiveness during the recovery period is determined not so much by the implementation of individual IT solutions as by the formation of an integral sociotechnical system. Such a system should ensure territorial independence of access to support, increased targeting based on integrated data, reduction

of administrative burden on recipients and personnel, a guaranteed level of cyber resilience and legal protection of personal data, as well as institutionally enshrined inclusivity.

It has been proven that Ukraine has the basic institutional prerequisites for the formation of a full-fledged digital public infrastructure of social protection, in particular due to the development of the UISSS as an integration platform, the functioning of interoperability mechanisms through the Trembita system, and the availability of a scalable digital channel for interaction with citizens – the Diia portal and application. At the same time, the key challenge remains the transformation of these elements into a consistent DPI stack, within which data governance, cybersecurity, privacy-by-design principles, and inclusion standards are built-in components of the architecture.

It is substantiated that the optimal model of implementation is a step-by-step approach, which includes: at the first stage – the creation of minimally viable end-to-end digital chains for the provision of priority services; at the second stage, scaling integrations and forming a dynamic social register with proper data quality management; the third is the institutionalization of analytical and AI tools with audit procedures and ensuring European compatibility. Such a sequence allows you to ensure the manageability of changes, minimization of risks and long-term sustainability of the digital model of social protection.

References

1. Brookings Institution. (2024). *Ukraine's digital government is central to resilience*. https://www.brookings.edu/articles/ukraine-digital-government-is-central-to-resilience/
2. Cabinet of Ministers of Ukraine. (2020). *Pro skhvalennia Stratehii tsyfrovoi transformatsii sotsialnoi sfery* [On approval of the Strategy for Digital Transformation of the Social Sphere] (Order No. 1353-r of October 28, 2020). https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text (in Ukrainian)
3. Cabinet of Ministers of Ukraine. (2025). *Deiaki pytannia realizatsii eksperymentalnoho proektu shchodo formuvannia i vykorystannia elektronnykh posvidchen identyfikatsiinykh danykh ta elektronnykh posvidchen atrybutiv za dopomohoiu hamantsia z tsyfrovoiu identyfikatsiieiu yak funktsionalnoi mozhlyvosti mobilnoho dodatka Yedynoho derzhavnoho vebportalu elektronnykh posluh (Diia)* [Certain issues regarding the implementation of the experimental project on the formation and use of electronic certificates of identification data and electronic certificates of attributes using a digital identity wallet as a functional feature of the mobile application of the Unified State Web Portal of Electronic Services (Diia)] (Resolution No. 1400 of October 24, 2025). https://zakon.rada.gov.ua/laws/show/1400-2025-%D0%BF#Text (in Ukrainian)
4. EU4DigitalUA. (2021). *Diia mobile application*. https://eu4digitalua.eu/wp-content/uploads/2021/12/diia-evaluation-report.pdf
5. EU4DigitalUA. (n.d.). *EU-supported Trembita system benefits the development of digital government in Ukraine*. https://eu4digitalua.eu/en/news/eu-supported-trembita-system-benefits-the-development-of-digital-government-in-ukraine/
6. European Commission. (n.d.). *The European Digital Identity Regulation*. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The%2BEuropean%2BDigital%2BIdentity%2BRegulation
7. European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2013/1148 (NIS 2 Directive)*. Official Journal of the European Union, L 333, 27.12.2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
8. Government of Ukraine, World Bank Group, European Commission, & United Nations. (2024). *Fourth Rapid Damage and Needs Assessment (RDNA4): Ukraine*. Ministry for Communities, Territories and Infrastructure Development of Ukraine. https://mva.gov.ua/media/1/Fourth_Rapid_Damage_and_Needs_Assessment__RDNA4_.pdf
9. Guven, M., Yeachuri, A., & Almenfi, M. (2025). *Global insights on social registries: Coverage and beyond* (Report No. P177331). The World Bank. https://documents1.worldbank.org/curated/en/099071525165029379/pdf/P177331-a772f9c1-e340-4f76-aeb0-90fd4e7a3496.pdf
10. Ingram, G., & Vora, P. (2024). *Ukraine: Digital resilience in a time of war. Brookings Institution, Center for Sustainable Development* (Working Paper No. 185). https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf

11. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001
12. Madsen, C. Ø., Lindgren, I., & Melin, U. (2022). The accidental caseworker – How digital self-service influences citizens' administrative burden. *Government Information Quarterly, 39*(1), 101653. https://doi.org/10.1016/j.giq.2021.101653
13. Ministry of Social Policy, Family and Unity of Ukraine. (n.d.). *Yedyna informatsiina systema sotsialnoi sfery (YeISSS)* [Unified Information System of the Social Sphere (UISSS)]. https://www.msp.gov.ua/e-servisy/yeisss (in Ukrainian)
14. National Council for the Recovery of Ukraine from the Consequences of the War. (2022, July). *Draft Ukraine Recovery Plan – Social protection section*. https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/eng/social-protection-eng.pdf
15. National Institute of Standards and Technology. (2024, February 26). *NIST releases version 2.0 of landmark Cybersecurity Framework*. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
16. Organisation for Economic Co-operation and Development. (2024). *Digital public infrastructure for digital governments*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf
17. Organisation for Economic Co-operation and Development. (2025). *Harnessing artificial intelligence in social security: Use cases, governance and workforce readiness* (OECD Digital Government Studies). OECD Publishing. https://doi.org/10.1787/b52405c1-en
18. President of Ukraine. (2021). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy"* [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"] (Decree No. 447/2021 of June 14, 2021). https://www.president.gov.ua/documents/4472021-40013 (in Ukrainian)
19. van Zoonen, L. (2020). Data governance and citizen participation in the digital welfare state. *Data & Policy*, (2), Article e10. https://doi.org/10.1017/dap.2020.10
20. Verkhovna Rada of Ukraine. (2010). *Pro zakhyst personalnykh danykh* [On the protection of personal data] (Law of Ukraine No. 2297-VI of June 1, 2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text (in Ukrainian)
21. Verkhovna Rada of Ukraine. (2020). *Pro osoblyvosti nadannia publichnykh* (elektronnykh publichnykh) posluh [On the peculiarities of the provision of public (electronic public) services] (Law of Ukraine No. 1689-IX of October 6, 2020). https://zakon.rada.gov.ua/laws/show/1689-20#Text (in Ukrainian)
22. Verkhovna Rada of Ukraine. (2020). *Pro publichni elektronni reiestry* [On public electronic registers] (Law of Ukraine No. 1907-IX of October 22, 2020). https://zakon.rada.gov.ua/laws/show/1907-20#Text (in Ukrainian)
23. Verkhovna Rada of Ukraine. (2021). *Pro vnesennia zmin do Zakonu Ukrainy "Pro Yedynyi derzhavnyi demohrafichnyi reiestr ta dokumenty, shcho pidtverdzhuiut hromadianstvo Ukrainy, posvidchuiut osobu chy yii spetsialnyi status"* [On amendments to the Law of Ukraine "On the Unified State Demographic Register and documents confirming citizenship of Ukraine, certifying a person or its special status"] (Law of Ukraine No. 1368-IX of March 30, 2021). https://zakon.rada.gov.ua/laws/show/1368-20#Text (in Ukrainian)
24. World Wide Web Consortium. (2023, October 5). *Web Content Accessibility Guidelines (WCAG) 2.2 becomes W3C Recommendation*. W3C Web Accessibility Initiative (WAI). https://www.w3.org/WAI/news/2023-10-05/wcag22rec/