UDC 004.738.5:343
DOI: https://doi.org/10.17721/1728-2195/2024/2.128-5

Oleh ZAIARNYI, DSc (Law), Prof.
ORCID-ID: 0000-0003-4549-7201
e-mail: oleganalitik.knu@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

LEGISLATIVE SUPPORT FOR THE IMPLEMENTATION OF THE "SMART CITY" CONCEPT IN THE EUROPEAN UNION AND PROPOSALS FOR UKRAINE DURING WARTIME AND POST-WAR RECOVERY

Background. *The article explores the features of legislative regulation of implementing the smart city concept within the law of the European Union. It characterizes the essence of the legal nature of its main components, which require comprehensive legislative regulation.*

Methods. *In preparing the research, dialectical, comparative-legal, formal-logical, and historical methods of scientific knowledge were used.*

The article aims to study the legislative foundations for implementing the "smart city" concept in the European Union and formulate proposals for legislative support for the post-war reconstruction of Ukrainian cities based on this concept.

Results. *The article characterizes the sectoral approach to regulating various aspects of the "smart city" concept in European Union legislation, identifying the specifics of applying certain information technologies, including artificial intelligence and open data, in this legal field. The necessity of specific regulation for the application of artificial intelligence in the development of smart infrastructure for urban settlements is justified, and an approach to improving the legal requirements for using this technology, considering European human rights standards, is proposed. The legal significance of certain public administration tools for smart cities, including the standardization and certification of smart infrastructure components and the stimulation of projects in this field under the "Digital Europe 2030" program, is substantiated. The need for further implementation of the European approach to ensuring the cybersecurity of digital urban infrastructure, based on secure-by-design principles and default protection of infrastructure elements, is emphasized.*

Conclusions. *Based on the research findings, the conclusions highlight the main directions for implementing the European Union's experience in legislative support for implementing the "smart city" concept into Ukraine's national legislation. On this basis, specific recommendations for local governments are formulated, providing practical guidance for developing and implementing a roadmap for developing smart cities during wartime and post-war reconstruction in Ukraine.*

Keywords: *European Union smart city legislation; personal data protection; information rights of smart city residents; smart city cybersecurity; post-war reconstruction of Ukrainian cities; smart city.*

Background

According to UN projections, by 2050, up to 68 % of the global population will reside in urban areas (World Cities Report, 2022). This trend urges governments to seek innovative solutions, primarily by applying the latest information and communication technologies, to address challenges such as effective resource use, infrastructure optimization (transport, energy, communications, etc.), waste disposal, and climate change monitoring to ensure comfortable living conditions. This goal directly aligns with the Sustainable Development Goals for 2030, adopted by the UN General Assembly at its Seventieth Session on September 25, 2015, where, under point 11.4, UN member states committed to expanding the scope of inclusive and sustainable urbanization and enhancing comprehensive and sustainable planning and management of urban areas based on broad participation in all countries by 2030.

One of the priority areas in this regard is implementing the smart city concept, aimed at generating new solutions to improve residents' quality of life amidst global challenges and environmental pollution, enhancing cities' competitiveness, and promoting sustainable development. The "Smart City" concept is not merely about using new technologies to deliver urban services; it is rather a comprehensive strategy unique to each city, defining its development goals and ways to achieve them. However, purely local legal initiatives for developing the smart city concept are insufficient; it requires entirely new approaches at the national level.

Relevance of the Study. Under the martial law regime in Ukraine and during the period of post-war economic recovery, most cities will face a range of systemic socio-economic, technological, and legal issues. One of the key tools to address these issues is the digital transformation of local communities, focusing on managing municipal assets, delivering public services at the local level, conducting business activities, and ensuring public order and security. Some services envisaged by the Smart City concept are already operational in Ukraine; however, the overall trend lacks a strategic character at the level of developing and implementing nationwide concepts (Smart City Ukraine). In particular, there are no unified regulatory requirements or state technical standards for the development of smart cities and compatibility of technological solutions; there is a lack of comprehensive, standardized approaches for implementing smart management and infrastructure in communities and regions; and the issues of IT staff shortages and necessary competencies among local government employees responsible for developing information infrastructure remain unresolved. Funding for digitalization is also insufficient at both the state and local levels, and there are no conditions necessary to attract private investors (Recommendations of Parliamentary Hearings, October 26, 2021).

At the same time, significant progress in bridging the digital divide in urban municipal infrastructure development, developing a system of legal and economic incentives for the "smart city" concept, ensuring cybersecurity for community residents, and addressing other issues has been achieved by the European Union (hereafter – the EU).

Given the priority of Ukraine's European integration policy and the deepening of multilateral cooperation between Ukrainian cities and EU member states, studying the EU's experience in legislative solutions for the aforementioned problems is of great importance.

Purpose of the article. The article aims to study the legislative foundations for implementing the "smart city" concept in the European Union and formulate proposals for

ISSN 1728-3817

legislative support for the post-war reconstruction of Ukrainian cities based on this concept.

Methods

In preparing the research, dialectical, comparative-legal, formal-logical, and historical methods of scientific knowledge were used.

Results

In modern legal literature, as in the legislation of most countries worldwide, there is no universal definition of the concept of a "smart city" (Pleskach, M., Zaiarnyi, O., & Pleskach, V., 2020, p. 760). Similarly, there are no unified approaches in practice to the primary mechanisms for implementing its modern concepts.

The official website of the European Commission provides the following definition: "A smart city is an urban area (administrative-territorial unit) where traditional networks and services become more efficient with the help of digital solutions for the benefit of its residents and businesses" (Smart cities. European Commission).

A smart city is not only about using digital technologies to utilize resources better and reduce emissions but also includes "smart" urban transportation networks, upgraded water supply and waste management systems, more efficient ways of lighting and heating buildings, interactive and responsive city administration, organizing safer public spaces, and meeting the needs of an aging population.

Today, developing the Smart City ecosystem involves including various physical and intangible objects intended for collecting, accumulating, and processing different types of information. The main goal of this interaction between the components of the Smart City infrastructure is to create various services designed to meet the legitimate needs and interests of city residents, businesses, and the local government authorities themselves.

An analysis of current approaches to achieving this goal in the practice of urban development in different countries allows us to identify three main smart city concepts: decentralized (horizontal), centralized (vertical), and mixed (comprehensive).

The essence of the decentralized concept is revealed in organizing information interaction between local government bodies, residents of territorial communities, and businesses, based primarily on an isolated municipal information ecosystem supported by a local coordination center for the "smart" city. Implementing this concept requires the formation of one or more information resources that serve as the core of the city's information ecosystem. These may include a register of residents of the territorial community, a register of local taxpayers, an official interactive map of the settlement, etc. The legitimate needs and interests of residents of "smart" cities can be met through the use of both municipal information ecosystem objects and national registers and digital services, including those designed to provide public services.

A centralized (Vertical) Smart City Concept can be implemented only through information interaction between local governments and state authorities, citizens, and businesses, primarily using national information infrastructure.

In a Mixed Smart City Concept, different information types can be exchanged between components of the city's information ecosystem and national information resources. This approach allows local authorities responsible for implementing the "smart city" concept to engage in information relations with residents of territorial communities, municipal enterprises, and government authorities at various levels (Zayarny, 2022, p. 9–16).

Each of these Smart City Concepts has its advantages and disadvantages. At the same time, the integration of any of these concepts in each individual country is determined by the conditions of information exchange between authorities, the level of development of local self-government, and the financial, digital, and political autonomy of each territorial community.

The Smart Cities Market was created in the EU by merging two platforms: the European Innovation Partnership on Smart Cities and Communities (EIP-SCC Marketplace) and the Smart Cities Information System (SCIS).

According to the European Commission, the implementation of the Smart City concept in EU member states encompasses the following main areas: sustainable urban mobility; sustainable neighborhoods and built environment; integrated infrastructures and processes in energy, ICT, and transport; citizen orientation; policy and regulation; integrated planning and management; knowledge sharing; key indicators of vitality, performance metrics, and development of urban innovation infrastructure; open data management; standards and specifications; business models, procurement, and financing of digital solutions for sustainable urban and community development.

In the absence of a specific EU law on implementing the Smart City concept, the legal regulation of social relations in this field is predominantly developed through a sectoral approach, combining supranational regulation of the most critical aspects of Smart City development with acts of the European Parliament, considering specific features at the level of national legislation in EU member states.

The sectoral approach to regulating social relations in this area implies that individual EU regulations or directives regulate aspects like cybersecurity, personal data protection, open data management, municipal infrastructure, climate neutrality, and public initiatives. In contrast, requirements for a national smart city development model, national informatization programs, conditions for reallocating grants and economic incentives to local budgets, and procedures for implementing e-democracy tools at the local level are the prerogatives of each EU member state's national legislation.

The basis for the modern development of EU Smart City legislation is the EU Single Digital Market Strategy ("Digital Europe 2030") (Europe's Digital Decade). This program document establishes an annual cycle of cooperation to achieve common EU and member state goals in digital transformation, including smart cities as a separate component. The proposed governance structure is based on an annual cooperation mechanism involving the European Commission and EU member states. This cooperation mechanism includes elements such as a structured, transparent, and collaborative monitoring system based on the Digital Economy and Society Index (DESI) to measure progress toward each goal by 2030, an annual report in which the European Commission assesses progress and makes recommendations within the framework of "Digital Europe 2030" (the first Report on the State of the Digital Decade was published in September 2023); and a support mechanism for the implementation of multinational projects, the European Digital Infrastructure Consortium, whose strategic tasks include developing joint digital platforms for smart cities and enhancing the digital competencies of residents in municipalities implementing the smart city concept.

On December 15, 2022, the European Declaration on Digital Rights and Principles was adopted in the EU (Declaration …, 2022). This soft law demonstrates the EU's commitment to secure and sustainable digital transformation based on human-centered principles and

respect for human rights and freedoms. The Declaration builds on the "Digital Europe 2030" provisions, particularly in the context of smart cities.

A key institutional element in implementing the smart city concept in the EU is the Regulation 2024/1689, adopted by the European Parliament on March 13, 2024, "On Certain Legal Frameworks for Harmonizing Artificial Intelligence Legislation and Amending Certain Legislative Acts of the European Parliament" (EU Regulation 2024/1689). This Regulation is an act of EU primary law, directly applicable and mandatory for implementation by all EU member states. Concerning smart cities, Regulation 2024/1689 defines principles and conditions for developing and applying artificial intelligence, establishes criteria for assessing AI's impact on residents' rights and freedoms, and sets requirements for developers of digital solutions based on this technology. Additionally, it establishes cybersecurity requirements for digital objects created using AI and types of sanctions for AI legislation violations.

The Regulation sets certain restrictions on applying artificial intelligence or its individual functions that could potentially be used in smart cities. It prohibits and imposes significant restrictions on digital solutions such as biometric identification systems that use sensitive characteristics, such as political, religious, or philosophical beliefs, sexual orientation, or racial identity. Such systems may only be used based on grounds specified in Regulation 2024/1689 or a court decision in criminal proceedings.

The Regulation also identifies types of artificial intelligence that pose risks to human rights and freedoms, including AI used for social scoring based on social behavior or personal characteristics; manipulation of people's behavior to deprive them of free choice; and exploitation of vulnerable people (due to age, disability, social, or economic status). Regulation 2024/1689 also introduces a classification of AI based on the risk level for human rights and freedoms, imposing additional obligations on developers and contractors of AI-based digital solutions to ensure user safety.

Individual testing centers for AI-based smart city projects are being established in EU member states. These projects are funded jointly by EU member states and the European Commission. Large-scale reference sites across Europe are open to all technology providers for extensive testing and experimentation with advanced AI solutions in real-world environments. These testing centers offer a combination of physical and virtual tools, allowing technology providers to receive support for testing their latest AI-based technologies in real-world environments.

An integral component of smart city infrastructure is open data–sets of official information generated through the city's activities, as well as enterprises, institutions, and organizations operating within its territory. The normative basis for legal regulation of social relations in this area within the EU and member states consists of the Directive 2019/1024 of the European Parliament and Council from June 20, 2019, on open data and the reuse of public sector information (EU Directive 2019/1024, 2019), as well as Regulations (EU) 2018/1807 and 2022/868.

The Directive (EU) 2019/1024 is aimed at promoting the use and reuse of public sector information. At the same time, Regulation (EU) 2022/868 seeks to establish a comprehensive and coherent legal framework for data management within the EU (Kabanov, & Oleksiyuk, 2023). According to Regulation (EU) 2018/1807, the free flow of data (excluding personal data) within the Union is ensured by setting rules concerning data localization requirements, data access for competent authorities, and data transfer for professional users.

A separate aspect of the legal support for implementing the smart city concept in the EU is cybersecurity. In this context, the Regulation 2019/881 of the European Parliament and the Council, dated April 17, 2019, on the EU Agency for Cybersecurity (ENISA) and cybersecurity certification of information and communication technology (ICT) and repealing Regulation (EU) 526/2013 (Cybersecurity Act) (referred to as EU Regulation 2019/881) plays an important role.

Unlike previous EU cybersecurity legislation adopted before 2018, EU Regulation 2019/881 introduced a mechanism to ensure cybersecurity by preventing threats during the design of information systems rather than merely protecting against or counteracting them. For this purpose, European cybersecurity certification frameworks have been established, extending to most smart city infrastructure digital components.

Building on the approach to ensure cybersecurity for smart city components set out by EU Regulation 2019/881, the Council of the EU approved Directive (EU) 2022/2555 on December 14, 2022, introducing measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Directive 2022/2555 aims to achieve a high common level of cybersecurity within the Union to improve the functioning of the internal market.

Notably, Directive 2022/2555 legalizes the transition from protecting information infrastructure objects to ensuring cyber resilience. It includes provisions on the standardization of IT products, IT services, and processes relevant to the smart city concept in terms of meeting modern cybersecurity requirements. European frameworks for certifying products, goods, and services for cybersecurity compliance have been improved to achieve this. Additionally, EU member states are required to implement international ISO standards related to cybersecurity, particularly in the smart city sector.

Thus, Directive 2022/2555 specified several provisions from EU Regulation 2019/881, covering IT product and service certification, particularly for smart cities, to ensure cyber resilience, address jurisdictional aspects of countering cyber threats, and establish requirements for national cybersecurity strategies in EU member states.

Additionally, it is worth mentioning EU Regulation 2016/679 of the European Parliament and the Council, dated April 27, 2016, on the protection of natural persons regarding the processing of personal data and the free movement of such data (General Data Protection Regulation, GDPR) (EU Regulation 2016/679, 2016). This regulation applies to the proper handling and protection of the personal data of smart city residents. This legislative act defines general requirements for the principles, purposes, and grounds for processing the personal data of smart city residents and introduces a rule for data security through digital solutions designed to protect the personal information of individuals.

As of today, EU legislation is developing by combining general and sector-specific (special) approaches to regulating different aspects of the smart city concept's implementation.

At the same time, the development of legislation in this area is guided by the priority of digital rights and freedoms of individuals, as proclaimed by international legal acts.

Another feature of EU smart city legislation is the significant enhancement of the legal significance of

international standards and technical specifications in defining requirements for data exchange, the development of digital operational infrastructure, and the cybersecurity of smart city components.

Discussion. In recent years, the European Union has taken significant steps to lay the foundation for developing the smart city concept.

1. As rightly noted in scientific literature, there has been a strong shift in the legal regulation of smart cities toward the cybersecurity of their infrastructure and issues of compatibility between digital devices and information exchanges (Peisert et al., 2021, p. 15). This trend is largely achieved through the introduction of international certification frameworks for information exchanges within smart city infrastructure. Additionally, there is a steady trend toward increasing the legal significance of international standards and creating sectoral standards in smart city development.

2. At the same time, in the European Union, areas related to strengthening special cybersecurity for smart cities' use of the Internet of Things (IoT) remain underexplored and open for further development (Dimitrov et al., 2021, p. 648). This position remains relevant for both general-purpose IoT and individual digital solutions that can be integrated into the smart city concept. This is also relevant for the security of personal data, which can be processed through IoT.

Although advancements in managing the data security of smart city residents are recognized in the legal literature (Kamleitner and Mitchell, 2019, p. 442), modern technologies also introduce new privacy risks. One such technology is artificial intelligence. EU Regulation 2024/1689, in connection with EU Regulation 2016/679, has created a quality legislative basis for protecting the data of smart city residents. However, the diversity of AI models and their deep integration into smart city infrastructure throughout the EU further indicate the need to improve privacy policies within urban spaces. There is a need for further legislative restrictions on using high-risk AI applications for public electronic services and managing data on citizens' behavior.

Similarly to EU legislation, Ukraine does not have a specific law on smart cities. The regulation of certain categories of social relations arising in this field is primarily carried out through general norms on electronic governance at the local level. At the same time, the universal technical conditions for forming the smart city concept in Ukraine are defined in the State Technical Standard DSTU ISO 37106:2019 “Sustainable Cities and Communities. Guidance on Establishing Smart City Operating Models for Sustainable Communities” (referred to as DSTU-37.106), which, with national legislative and terminological adjustments, aligns with ISO 37106 Sustainable Cities and Communities – Guidance on Establishing Smart City Operating Models for Sustainable Communities.

This document provides recommendations for leaders in smart cities and communities (from public, private, and voluntary sectors) on how to develop an open, collaborative, citizen-oriented, and digital functional model for their city that puts their vision of a sustainable future into action.

DSTU 37106 does not describe a model that meets all future smart city requirements. Instead, the focus is on the enabling processes through which the innovative use of technology and data, combined with organizational changes, can help each city achieve its vision of a sustainable future in a more efficient and flexible way (DSTU ISO 37106).

Analysis of the provisions of this DSTU suggests that a mixed model of implementing the smart city concept is gradually taking shape in Ukraine. This approach not only develops the goals and objectives of the State Regional Development Strategy for 2021-2027, approved by the Cabinet of Ministers of Ukraine on August 5, 2020, No. 695, but also better meets the interests of municipal communities by allowing more effective use of informational, human, industrial, and management resources. This result can be achieved through a consistent combination of state regulation and local initiative when addressing issues related to forming a smart city's information ecosystem and effectively managing and scaling its components.

Despite the consistent steps taken by the Verkhovna Rada of Ukraine to align national legislation with EU standards, including in the field of smart city development and the introduction of specific national standards in this area of legal regulation, a wide range of issues remain that require solutions based on the experience of the EU and its member states. Many of these issues can be addressed by adapting Ukraine's digital transformation legislation to primary sources of EU law in this field. Another necessary step to overcome existing problems in implementing the smart city concept is further updating national standards on relevant issues through the implementation of ISO standards.

Discussion and conclusions

The research conducted on the legislative foundations for implementing the smart city concept in the European Union and its member states allows us to formulate the following key conclusions and recommendations for Ukraine that may promote the sustainable development of cities and communities with a view to the innovative post-war recovery of their digital infrastructure.

In the EU, the legislative foundations for smart city development are shaped by defining a general mechanism for protecting personal data, managing open data, ensuring cybersecurity, organizing public procurement of innovative products, and setting requirements for climate-neutral cities in acts of the European Parliament.

The approach to forming the smart city concept is based on recognizing the individual, their rights, and freedoms as core values that the urban infrastructure supports. Smart city infrastructure is developed based on interoperability, technical neutrality, and resilience to cyber threats.

Regarding smart cities' cybersecurity, EU legislation develops based on combining protection during infrastructure design and default security. This balance is achieved by increasing the legal significance of public administration tools, such as the standardization and specification of components and processes within the urban digital infrastructure.

With Ukraine pursuing a European integration policy, the primary tool for adapting national smart city legislation to EU legal standards is the adoption of specific laws, including: "On Digital Operating Platforms for Smart Cities," "On Open Data Processing and Management," "On the Basic Principles of Artificial Intelligence Use in Ukraine," and an updated version of the Law of Ukraine "On Personal Data Protection."

In addition, to ensure the practical implementation of the European approach to legislatively defining the smart city concept, it is proposed that the Cabinet of Ministers of Ukraine approve a "Strategy for Implementing the Smart City Concept in Ukraine". Apart from defining this concept's main legal and technological components, the Strategy should enshrine principles, conditions, and means of promoting the development of smart cities in Ukraine. It should include a set of measures aimed at ensuring compliance with the informational rights of smart city residents, cybersecurity of municipal smart infrastructure, and more. An essential part of this Strategy should be a

roadmap for implementing the smart city concept within the activities of territorial communities. This normative legal act may include specific current (tactical) measures for the digitalization of local self-government, particularly based on best practices of EU member states, optimal models of information exchange, provision of electronic public services at the local level, and the involvement of international grant support for individual projects in this regulatory field.

In general, as the practice of legislative support for implementing the smart city concept in the EU demonstrates, the main focus for policy in this field remains on the rights of city residents. Their rights shape the prioritization of clusters for the digital transformation of cities and define the obligations of the state and local authorities regarding the nature of systemic changes in local self-government.

The article was prepared by the author in fulfillment of the tasks of the Personal Scholarship of the Verkhovna Rada of Ukraine for Young Scientists – Doctors of Science.

References

Dimitrov, V., Zhekov, B., & Hristov, P. (2021). Analysis of Cybersecurity Deficiencies in the DLT Ecosystem. *Springer International Publishing*, 645–655. https://doi.org/10.1007/978-3-030-77442-4_54

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). EUR-Lex. https://eur-lex.europa.eu/eli/dir/2019/1024/oj

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) 2016/1148 (NIS 2 Directive). EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

DSTU ISO 37106:2019. *Sustainable Cities and Communities. Guide for Establishing Intelligent Operational Models for Sustainable Communities* (ISO 37106:2018, IDT) [in Ukranian].

Europe's Digital Decade: digital targets for 2030. European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#t/he-path-to-the-digital-decade

European Digital Infrastructure Consortium (EDIC). European Commission. https://digital-strategy.ec.europa.eu/en/policies/edic

Kabanov, O., & Oleksiuk, T. (2023). *Compliance of Ukrainian Legislation with Certain Provisions of the Legal Regulation of Open Data in the European Union: Analytical Report* [in Ukranian]. https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-/pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing*, 38(4), 433–450. https://doi.org/10.1177/0743915619858924

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the SolarWinds incident. *IEEE Security & Privacy*, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

Pleskach, M., Zaiarnyi, O., Pleskach, V. (2020). *Respect for Information Rights of a Person as a Condition for Cybersecurity of Smart Cities Residents*. 10th International Conference on Advanced Computer Information Technologies (ACIT), 759–764. https://ieeexplore.ieee.org/document/9208977

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.). EUR-Lex. https://www.legislation.gov.uk/eur/2018/1807/body/2020-01-31

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32022R0868

Smart cities. European Commission. https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

Smart City Ukraine: What It Is and How It Works in Ukrainian Realities. https://visitukraine.today/uk/blog/2183/smart-city-ukraine-what-it-is-and-how/-it-works-in-ukrainian-realities

World Cities Report. Envisaging the Future of Cities. (2022). https://unhabitat.org/sites/default/files/2022/06/wcr_2022.pdf

Zaiarnyi, O. A. (2022). Information-Legal Aspects of Implementing Global Smart City Concepts at the Current Stage of Ukraine's Digital Transformation. *Law of Ukraine*, 8, 13–27 [in Ukranian]. https://pravoua.com.ua/ua/store/pravoukr/pravo_2022_8/

Отримано редакцією журналу / Received: 31.10.24
Прорецензовано / Revised: 15.11.24
Схвалено до друку / Accepted: 20.11.24

Олег ЗАЯРНИЙ, д-р юрид. наук, проф.
ORCID-ID: 0000-0003-4549-7201
e-mail: oleganalitik.knu@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ "РОЗУМНОГО МІСТА" В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА ПРОПОЗИЦІЇ ДЛЯ УКРАЇНИ В УМОВАХ ВІЙНИ Й ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ

В с т у п . *У статті досліджено особливості законодавчого регулювання реалізації концепції "розумного міста" в праві Європейського Союзу, охарактеризовано сутність правової природи її основних компонентів, які потребують комплексного законодавчого регулювання.*

М е т о д и . *При підготовці дослідження були використані діалектичний, порівняльно-правовий, формально-логічний, , історичний методи наукового пізнання.*

Метою статті було дослідження законодавчих засад реалізації концепції "розумного міста" в Європейському Союзі, формулювання пропозицій щодо законодавчого забезпечення післявоєнного відновлення міст України на основі згаданої концепції.

Р е з у л ь т а т и . *У статті охарактеризовано галузевий підхід до врегулювання різних аспектів концепції "розумного міста" в законодавстві Європейського Союзу, визначено особливості застосування окремих інформаційних технологій, зокрема штучного інтелекту, відкритих даних у цій сфері правового регулювання. Доведено необхідність спеціального регулювання застосування штучного інтелекту для потреб розвитку смартінфраструктури населених пунктів, запропоновано підхід до вдосконалення правових вимог застосування вказаної технології з урахуванням європейських стандартів прав людини. Додатково обґрунтовано юридичне значення окремих інструментів публічного адміністрування "розумних міст", зокрема стандартизації, сертифікації компонентів смартінфраструктури населених пунктів, стимулювання проєктів у цій сфері за програмою "Цифрова Європа 2030" тощо. Обґрунтовано необхідність подальшої імплементації європейського підходу до забезпечення кібербезпеки цифрової інфраструктури міст, який ґрунтується на основі поєднання безпечного проєктування та захисту елементів інфраструктури за замовчуванням*

В и с н о в к и . *За результатами проведеного дослідження у висновках виокремлено основні напрями імплементації досвіду Європейського Союзу у сфері законодавчого забезпечення реалізації концепції "розумного міста" у національне законодавство України. На цій основі сформульовано окремі рекомендації для органів місцевого самоврядування щодо формування і виконання дорожньої карти розвитку "розумних міст" у період війни та післявоєнного відновлення України.*

К л ю ч о в і с л о в а : *законодавство Європейського Союзу про "розумні міста", захист персональних даних, інформаційні права жителів "розумних міст", кібербезпека "розумного міста", післявоєнне відновлення міст України, "розумне місто".*

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest.The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.