CHALLENGES AND LEGAL SUPPORT OF THE ECONOMY IN THE CONDITIONS OF DIGITALIZATION

COLLECTION OF SCIENTIFIC WORKS

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”
FACULTY OF SOCIOLOGY AND LAW
DEPARTMENT OF INFORMATION,
ECONOMIC AND ADMINISTRATIVE LAW
WARSAW UNIVERSITY OF TECHNOLOGY
FACULTY OF ADMINISTRATION AND SOCIAL SCIENCES

DOI https://doi.org/10.59647/978-617-520-883-0/1

CHALLENGES AND LEGAL SUPPORT OF THE ECONOMY IN THE CONDITIONS OF DIGITALIZATION

COLLECTION OF SCIENTIFIC WORKS

Kyiv
2024

UDC 34:33]:004](06)=111
C43

Published by decision of Academic Counsil of Faculty of sociology and law of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (protocol № 10, June, 3, 2024)

Editors (compilers):

BEVZ Svitlana – Doctor of Legal Sciences, Professor, Head of the Department of Information, Economic and Administrative law of Igor Sikorsky Kyiv Polytechnic Institute

PODOLYAK Svitlana – Candidate of Legal Science, Associate Professor, Associate Professor of the Department of Information, Economic and Administrative Law of Igor Sikorsky Kyiv Polytechnic Institute

SYDORENKO Viktoriia – Candidate of Legal Science, Associate Professor of the Department of Information, Economic and Administrative Law of Igor Sikorsky Kyiv Polytechnic Institute

Reviewers:

DOROSHENKO Lina – Doctor of Legal Sciences, Associate Professor, Associate Professor of Department of Economic Law And Economic Jurisprudence of Educational and Scientific Institute of Law of Taras Shevchenko Kyiv National University

DUTOV Mykhaylo, Candidate of Juridical Sciences (Ph.D), Senior Research Officer of State Organization "V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine"

C43 **Challenges** and Legal Support of the Economy in the Conditions of Digitalization : collection of scientific works. Kyiv : Publishing Lira-K. 2024. 128 p.

Gaps and conflicts in legal regulation of economic relations in the conditions of digitalization are highlighted. Attention is focused on challenges to legal regulation caused by the digitalization of the economy. Topical issues of various branches of law in the conditions of digitalization are presented.

The Collection is addressed to scientists, lecturers, practitioners, applicants for academic degrees and students.

Виклики та правове забезпечення економіки в умовах цифровізації : збірник наукових праць. – Київ : Видавництво Ліра-К, 2024. – 128 с. – анг. мовою

Висвітлено прогалини та колізії правового регулювання економічних відносин в умовах діджиталізації. Акцентовано увагу на викликах правовому регулюванню, що зумовлені цифровізацією економіки. Представлено актуальні питання різних галузей права в умовах цифровізації.

Для науковців, лекторів, практиків, здобувачів наукових ступенів та студентів.

Published in the author's edition.

UDC 34:33]:004](06)=111

ISBN 978-617-520-883-0
DOI https://doi.org/10.59647/978-617-520-883-0/1

CONTENTS

Olena AKIMOVA

Candidate of Philosophical Sciences, Associate Professor, Dean of the Faculty of Sociology and Law, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Ladies and Gentlemen,

Let me take the opportunity to welcome you to the International Scientific and Practical Conference "Challenges and Legal Support of Digitalization in the Economy." It is my honor to open this significant event, which gathers esteemed scholars, practitioners, and policymakers from around the globe to discuss one of the most pressing issues of our time.

First and foremost, I would like to extend my deepest gratitude to all the organizers who have worked tirelessly to bring this conference to life. Your dedication and hard work have made this gathering possible. Special thanks are also due to the people of Poland for their unwavering support of Ukraine and Ukrainians during these challenging times. Your solidarity and generosity have been a beacon of hope and a source of strength for us, and we are profoundly grateful.

Today, we come together to delve into the complexities of digitalization in the economy, a topic of immense importance, especially in times of transformation. The rapid advancement of digital technologies is reshaping economies worldwide, creating new opportunities, and posing significant challenges. Understanding these processes is crucial as we navigate the intricate landscape of the digital age.

For Ukraine, the study and implementation of digitalization hold particular significance. As we look towards the future and the prospect of post-war recovery, digitalization offers a pathway to rebuild and rejuvenate our economy. By embracing digital tools and innovations, we can foster economic resilience, enhance efficiency, and create a more inclusive and sustainable economic environment.

This conference is not just a platform for intellectual exchange but also a testament to the growing collaboration between Ukrainian and Polish institutions of higher education. Our partnership with Poland is exemplified by initiatives such as the Incubating Freedom project, which is spearheaded by the Kyiv Polytechnic Institute (KPI). This project is dedicated to developing digital skills among migrant women in Poland, empowering them to contribute meaningfully to the digital economy. Additionally, our collaboration with the Narodowa Agencja Wymiany Akademickiej (NAWA) and other agencies is a testament to the strong and enduring bonds between our nations.

As we embark on this conference, I encourage each of you to engage actively, share your insights, and explore new ideas. Let this gathering be a catalyst for innovation, collaboration, and progress. Together, we can address the challenges of digitalization and harness its potential for the betterment of our economies and societies.

In closing, I wish you all a fruitful and inspiring conference. May your discussions be filled with creativity, your debates with insight, and your time here with new connections and ideas that will drive us forward.

Thank you, and let us begin this journey together.

Anna ZALTSEWICH

PhD, DSc, Professor of the University, Dean of the Faculty of Administration and Social Sciences Warsaw University of Technology, Poland

Ladies and Gentlemen, dear Guests,

It is my great pleasure to welcome you to the International Conference "CHALLENGES AND LEGAL SUPPORT OF DIGITALIZATION IN THE ECONOMY".

Today's conference is a special scientific event. It first of all highlights the cooperation between the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" and the Warsaw University of Technology, between two Faculties which find the issues of research on the social aspects of technological development crucial. Secondly, it focuses on a topic that is particularly important nowadays: legal conditions for the functioning of the digital economy. Thirdly, acceptance of an invitation to this conference by such an esteemed group of speakers and guests from research centers of various countries offers an opportunity for an international debate on the challenges the society of each country faces and on finding supra-national solutions for their development.

There is no doubt that the project of digitization of the economy implemented in the European Union and other countries around the world, requiring a multi-faceted approach to ensuring civilizational and social progress, has an impact on the functioning of public administration, the lives of citizens and challenges related to the protection of freedom and human and civil rights. With the development of new technologies and digital services and in various spheres of life, people's expectations and needs related to high availability, cybersecurity, data and privacy protection are changing. All this makes it necessary to constantly improve existing legal solutions, which must be adequate to both technological possibilities and val-

ues considered important and subject to protection in most modern legal systems.

I am convinced that today, a joint, international debate will allow us to look at the legal, IT and technical challenges facing humanity in a useful way for society.

I wish us fruitful deliberation and exciting joint scientific exploration.

Before I leave the floor to you let me express my gratitude for Prof. Svitlana BEVZ, Head of the Department of Information, Economic and Administrative Law and Prof. Olena AKIMOVA Dean of the Faculty of Sociology and Law, who invited the Faculty of Administration and Social Sciences to jointly organize this conference. I would also like to thank all faculty and staff members who are making this conference possible. Special thanks go to Dr. Svitlana Podolyak for our excellent cooperation in all activities related to the organization of today's conference.

Thank you very much.

ECONOMIC SECURITY OF UKRAINE IN THE DIGITAL ECONOMY: CHALLENGES FOR LEGAL REGULATION

Bevz S.

Head of the at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Doctor of Law, Professor

In modern conditions, a characteristic feature of the development of any sphere of social relations is its digital transformation. As the foundation of the state's functioning, the economy has not been spared such changes.

The course towards digitalization of the economy and specific steps aimed at its implementation were enshrined in the Concept for the Development of the Digital Economy and Society for 2018-2020 [1], which states that the main goal of digitalization is to achieve digital transformation of existing and creation of new sectors of the economy, as well as transformation of spheres of life into new more efficient and modern ones. In this case, the term 'digital economy' means an activity in which the main means (factors) of production are digital (electronic, virtual) data, both numerical and textual.

One of the results of the implementation of this Concept in the legal sphere was the Law of Ukraine 'On Stimulating the Development of the Digital Economy in Ukraine' dated 15 July 2021 No. 1667-IX [2], which, according to Article 2 of the said Law, introduced the functioning of the legal regime of Diia City to stimulate the development of the digital economy in Ukraine by creating favorable conditions for conducting innovative business, building digital infrastructure, attracting investment, and talented specialists.

At the same time, in the context of the full-scale invasion of Russia, the issue of national security, including economic security, has become extremely relevant.

According to part 4 of Article 3 of the Law of Ukraine 'On National Security of Ukraine' [3], the state policy in the spheres of national security and defense is aimed at ensuring, among other things, the economic security of Ukraine. According to clause 66 of the National Security Strategy of Ukraine [4], one of the national security and defense planning documents that defines the ways and tools for its implementation is the Economic Security Strategy [5], which also states that "an important place in the security sector is occupied by challenges related to the armed aggression of the Russian Federation and the temporary occupation of part of the territory of Ukraine".

However, the scientific literature rightly emphasizes the priority of economic security as a component of national security. In particular, Y.G. Neustroev points out that 'since the economy is a vital aspect of the activities of society, the state and the individual, economic security will remain the basis of national security... That is, economic security, which manifests itself in the spheres of influence of other types of national security, penetrating them and interacting with them, in turn, accumulates their effect, while remaining the basis (basis) of national security [6, p.4]. The expert-analytical report of the National Institute for Strategic Studies 'Current Challenges and Threats to the Economic Security of Ukraine in the Context of Martial Law' states that economic security as the ability of the national economy to maintain stability and invulnerability to internal and external threats, to ensure high competitiveness in the global economic environment, sustainable and balanced growth are important criteria for assessing the quality parameters of the national economy, strategic efficiency of economic policy and the

However, the challenges and threats that are identified and analyzed, and certain action plans are developed to prevent them, minimize attention to the digitalization of the economy and the challenges and threats caused by this transformation of the economic sphere. Mean-

while, based on official statistics and other ratings in 2021 and early 2022, Ukraine's IT infrastructure ranks 7th among 23 countries in Central, Eastern, Southeastern and North Eastern Europe in terms of its impact on the national economy (Estonia is first). It is ahead of most countries in the ranking in terms of exports and contribution to GDP [8]. At the same time, among the risks and challenges to the economic security of the state, such a vector as digital transformation is only partially mentioned. Thus, among the main challenges and threats related to the digital transformation of the economy and specified in the Economic Security Strategy of Ukraine until 2025, we can distinguish

– in the field of production security (defined as one of the components of economic security in the relevant Strategy): the inconsistency of the structure of the national economy with modern technological development; low level of introduction of the latest production technologies; the potential threat of unauthorized physical and cyber interference with critical infrastructure and:

– in the area of investment and innovation security (which is also defined as one of the components of economic security in the relevant Strategy) – lack of favorable conditions for the creation and development of technology companies, innovative enterprises, and start-ups; unlawful access to domestic technological developments and innovations by foreign entities and the risk of their unauthorized leakage abroad.

At the same time, the tasks set in these areas to implement the direction of development in the field of economic security, although they do not provide for the development/improvement of legislation on these issues, but without such steps, the implementation of the tasks seems rather doubtful.

For example, one of the tasks in the field of investment and innovation security is to develop a mechanism and implement state support for the implementation of the latest technologies developed in Ukraine in the sectors of strategic importance for the national security of the state and its critical infrastructure. In the context of martial law, such an industry is primarily the defence industry.

In accordance with part two of Article 19 of the Constitution of Ukraine, public authorities are obliged to act only on the basis, within the limits of their powers and in the manner provided for by the Constitution and laws of Ukraine. Therefore, state support for the implementation of the latest technologies developed in Ukraine should be included in the powers of the relevant state authorities.

At the same time, the Regulation on the Ministry of Strategic Industries of Ukraine, approved by Resolution No. 819 of the Cabinet of Ministers of Ukraine of 7 September 2020, does not mention support for the introduction of new technologies at all. In addition, the Economic Security Strategy is not listed among the acts to which the Ministry prepares proposals (clause 2, part 4 of the Regulation).

At the same time, according to the Regulation on the Ministry of Digital Transformation of Ukraine, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 856 of 18 September 2019, this Ministry, in accordance with its tasks, maintains the software of the Diia City registry. There is no question of supporting other technologies. The tasks and powers of the Ministry of Economy of Ukraine, the Ministry of Defense of Ukraine, and the State Agency for the Restoration and Development of Infrastructure of Ukraine in accordance with the Regulations on these state bodies do not include support for the introduction of new technologies.

Therefore, the implementation of state support for the introduction of the latest technologies developed in Ukraine in the areas of strategic importance for the national security of the state and its critical infrastructure is not possible at this stage, based on the absence of a state body authorized and responsible for the implementation of such a measure, which requires appropriate amendments to the legislation.

At the same time, we would like to draw your attention to the fact that following a joint initiative of the Ministry of Defense, the General Staff of the Armed Forces of Ukraine, the National Security and Defense Council, the Ministry of Digital Transformation, the Ministry of Strategic Industries and the Ministry of Economy, the Brave1 cross-sectoral project was launched to stimulate and support

the development of companies working in the field of defense technology [9]. Representatives of state institutions signed a memorandum of cooperation and support within the project, which aims to supply and transfer advanced Ukrainian technological solutions to the frontline to gain an advantage over the enemy and win, provide comprehensive support to Ukrainian developers in the field of innovative defense technologies, and develop the sector to turn Ukraine into a world leader in defense tech. [10]. The main goal of Brave1 is to create a fast-track for the development of defense technologies. Brave1 solves the problem of endless bureaucratic procedures by providing developers with project support at all stages of their implementation and financing the most promising ones [11]. However, no information on the legal regime of such a platform can be found. Given that under the simplified regime, the focus of public law regulation is 'aimed at ensuring information security on platforms, including the protection of intellectual property and personal data of users of various platforms, as well as transparency of investments in the development of information infrastructure and other related issues' [12], we can conclude that these issues require legislative regulation in relation to the Brave1 platform.

Thus, based on the foregoing, we can conclude that Ukraine's course towards building a digital economy, as laid down in conceptual and strategic legal acts, continues to be actively implemented, especially in priority industries. At the same time, it is not always accompanied by proper legislative support and without assessing the impact of such processes on the state's economic security.

Therefore, to legislatively regulate certain issues of ensuring economic security in the digital economy, we consider it expedient, first of all, to systematize the challenges and threats to Ukraine's economic security related to the digital transformation of the economy; clearly define the powers of state bodies aimed at implementing measures to ensure the economic security of the state in the context of the digital transformation of the economy; establish at the regula-

tory level the legal regime of platforms implemented by state bodies to support the digitalisation of the economy.

References:

1. The Concept for the Development of the Digital Economy and Society for 2018-2020, approved by the Resolution of the Cabinet of Ministers of Ukraine dated January 17, 2018 № 67. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (accessed: 05/14/2024).
2. On Stimulating the Development of the Digital Economy in Ukraine: Law of Ukraine dated July 15, 2021 №1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (accessed: 05/14/2024).
3. On National Security of Ukraine: Law of Ukraine dated June 212, 2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed: 05/14/2024).
4. Human Security – Country Security: National Security Strategy of Ukraine , approved by the Decree of the President of Ukraine dated September 14, 2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n5 (accessed: 05/14/2024).
5. Economic Security Strategy of Ukraine for the period up to 2025, approved by the Decree of the President of Ukraine dated of August 11, 2021 № 347/2021 https://zakon.rada.gov.ua/laws/show/347/2021#Text (accessed: 05/14/2024).
6. Neustroiev, Y. (2021), 'Modern approaches to the concept of "economic security of the country"', Efektyvna ekonomika, [Online], vol. 1, available at: http://www.economy.nayka.com.ua/?op=1&z=8538 (accessed 10 May 2024). DOI: 10.32702/2307-2105-2021.1.98
7. Expert and analytical report of the National Institute for Strategic Studies 'Current Challenges and Threats to the Economic Security of Ukraine under Martial Law'. URL: https://niss.gov.ua/sites/default/files/2023-05/executive-1.pdf
8. IT image of Ukraine in the world: a study. URL: https://brandukraine.org.ua/documents/101/Ukraines_IT_perceptions_report_web_29_09_2023.pdf
9. Fedorov M. In a few years, defence technology companies worth more than a billion dollars will appear in Ukraine. URL: https://www.ukrinform.ua/rubric-technology/3700941-mihajlo-fedorov-vicepremer-

ministr-z-innovacij-rozvitku-osviti-nauki-ta-tehnologij-ministr-cifrovoi-transformacii.html

10. Defence Technology Development Cluster BRAVE1 was launched in Ukraine. URL: https://www.mil.gov.ua/news/2023/04/26/v-ukraini-zapustili-klaster-z-rozvitku-oboronnih-tehnologij-brave1/

11. The Brave1 Defence-tech cluster is one year old. Main achievements of the project. URL: https://www.kmu.gov.ua/news/defense-tech-klasteru-brave1-rik-holovni-dosiahnennia-proektu (accessed: 05/14/2024).

CITIZEN-GENERATED DATA IN AS OPEN DATA: LEGAL REGULATION FOR ARTIFICIAL INTELLIGENCE DEVELOPMENT

Dubniak M.

Head of the Scientific Laboratory of Legal Support for Digital Transformation, State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine", PhD in Law
ORCID: 0000-0001-7281-6568

A set of training data is needed at the stage of development of artificial intelligence technologies. In the process of forming such training datasets, developers often face problems due to different regulatory regimes of data protection. For example, the processing of personal data requires the informed consent of the data subject. By combining training datasets, it is possible to fulfill the "specifically identified person" criterion. This means that by using different datasets and combining them in a training dataset for artificial intelligence, developers get a dataset that specifically identifies a person, and such datasets are subject to legal protection of personal data. To create images, texts, music, and videos in training data, developers need to obtain permissions and licenses from the owners of intellec-

tual property rights. Since training datasets use hundreds, perhaps tens of thousands, of individual objects protected by intellectual property laws, entering into tens of hundreds of license agreements for each such object would significantly complicate the development of the technology. In such a highly competitive environment as the development of artificial intelligence technologies, the rapid and legal collection of data to form training datasets is of paramount importance. Therefore, it is relevant to study the legal regulation of open data as data that can be legally obtained and used quickly and without excessive bureaucratic procedures as training data sets for the development of artificial intelligence technologies.

Public information in the form of open data can be freely used and disseminated. Any person may reproduce, publish, distribute, use, including for commercial purposes, in combination with other information or by incorporating it into their own product, with a mandatory reference to the source of such information [1].

Of all the discussed legal regimes of data protection, the use of public information in the form of open data in training datasets seems to be the safest and most legal for the purposes of artificial intelligence technology development.

The peculiarity of open data is that it is created and published by public information administrators. However, in today's globalized world, a huge amount of data is generated by users when they use various smart things and mobile applications in the course of their daily life. Some of this data is collected by companies that own technical devices (smart things) or mobile applications and is used by companies to change and improve their business models [2, p. 65]. The data collected in this way is protected as confidential or business information by private companies, and it is usually impossible to obtain such structured data sets in the public domain. Even if such private companies acquire the status of a Manager (e.g., they have a dominant position in the market, special or exclusive rights, or are natural monopolies), they are obliged to publish data on the terms of supply of goods, services and prices for them [1]. Of all

the discussed legal regimes of data protection, the use of public information in the form of open data in training datasets seems to be the safest and most legal for the purposes of artificial intelligence technology development.

The peculiarity of open data is that it is created and published by public information administrators. However, in today's globalized world, a huge amount of data is generated by users when they use various smart things and mobile applications in the course of their daily life. Some of this data is collected by companies that own technical devices (smart things) or mobile applications and is used by companies to change and improve their business models [2, p. 65]. The data collected in this way is protected as confidential or business information by private companies, and it is usually impossible to obtain such structured data sets in the public domain. Even if such private companies acquire the status of a Manager (e.g., they have a dominant position in the market, special or exclusive rights, or are natural monopolies), they are obliged to publish data on the terms of supply of goods, services and prices for them [1].

Such data is often readily available on companies' websites as part of their marketing strategy.Data about goods, services, and their prices are much less interesting for use in training datasets compared to data that companies receive from citizens who use their mobile apps or that they receive from smart things while using them.

There is a large institutional structure for publishing open data sets that can be freely used, including for commercial purposes, and for using this data in training datasets for the development of artificial intelligence, so it is important to investigate whether there are opportunities on Open Data Portals for publishing data not only by Data Managers but also by citizens themselves. Such a social model will allow removing private companies from the process of collecting citizen-generated data and making this data open and public for all interested parties.

The issues associated with the research of citizen-generated data are addressed in the works of the following scientists: O. Corcho,

J. Blanco, C. Morote, Simperl E. [3], A. Meijer, S. Potjer [4], A. Suman [5], M. Ponti, M. Craglia [6]. In their scientific works, they proposed categories of data, their characteristics of classification, and the scope of their collection (from volunteer initiatives to government policies on the use of citizen-generated data) [3 p. 10].

Among researchers, there is no single definition for the concept of "citizen-generated data (hereinafter CGD)". In particular, there are the following views on this category:

- Data consciously created by people is open and available in the *public domain* [4].
- Citizen-generated resources that allow us to question the expert knowledge produced. By evaluating this data using critical thinking techniques, real alternative views on the same problem can be formed by citizens themselves. As a result, these data can be seen as a form of social protest and grounds for policy change [5].
- pen data are essential for public administration, as their use will help to coordinate joint actions of stakeholders t*o solve social problems* [6].
- Data that individuals or a community of citizens create to directly monitor or stimulate change in issues that concern them [7]. That is, as one of the tools for participating in public affairs management.
- Data that provides direct representation of their interests and is an alternative set of data compared to the data collected by governments and international organizations [3, p.8].

Thus, the concept of CGD is highly dependent on the context of the study and is described both through the information categories of "data", "collection", "processing" and the intellectual property category of "public domain", as well as tools for direct citizen participation in public affairs, "solving issues that concern them", "alternative views". The concept of CGD is mixed with forms of participation in public affairs management and citizen science (crowdsourced science, volunteer data). To distinguish these related

categories from CGD, we will provide some essential features and examples.

For the legal regulation of CGD, the essential characteristics are as follows:

data are generated by individual citizens, not by Data Controllers;

data is generated by citizens in the course of their daily life through the use of various mobile applications and smart things;

citizens have the opportunity to upload the necessary data sets to specially created modules on Open Data Portals;

data sets are uploaded in machine-readable formats.

Crowdsourced science is characterized by the wide involvement of stakeholders to provide specifically defined data to be used in scientific research [8]. That is, the qualifying features of these data are as follows:

he purpose of their collection is for scientific activities;

a specific data topic (e.g., health).

Such cooperation can take various forms, such as the placement of specific data by any person on specially designated information resources. This is how the largest database of coronavirus symptoms, Covid 19 – called ZOE was created; or by involving individuals in collaboration with teams of scientists to generate new scientific knowledge.

The legal regulation of open data provides for the use of this data legally in training datasets for the AI technology development. It is necessary to supplement the national legislation with the category of "open data in the form of citizen-generated data", allowing interested parties to post additional categories of data on the Open Data Portal. It will also remove private companies from the chain of data processing and use by providing the possibility to publish citizen-generated data independently, at their own discretion. Some categories of citizen-generated data can be used as feedback and alternative communication tools in the process of engaging citizens in the direct management of state or local affairs. Use this data for

scientific purposes, statistics and monitoring, and to supplement the data of SDG indicators..

References:

1. On access to public information: Law of Ukraine № 2939-VI, as amended on 08.10.2023, URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text. (accessed: 04/28/2024)
2. Dubniak M.V. (2023) Data economy: legal and ethical aspect. Information and Law, No. 3(46), pp. 64-74 DOI: https://doi.org/10.37750/2616-6798.2023.3(46).287147
3. Corcho O., Blanco J.J., Morote C., Simperl E. (2022) Data.europa.eu and citizen-generated data. Luxembourg: Publications Office of the European Union, 32 p. Doi: 10.2830/137589.
4. Meijer A., Potjer S. (2018). Citizen-generated open data: an explorative analysis of 25 cases. *Government Information Quarterly,* Vol. 35, № 4, Elsevier, pp. 613–621.https://doi.org/10.1016/j.giq.2018.10.004Suman A., Schade S. Abe, Y. (2020). Exploring legitimization strategies for contested uses of citizen-generated data for policy. Journal of Human Rights and the Environment. Vol. 11, № 3, Edward Elgar Publishing, pp. 74–102. https://www.elgaronline.com/view/journals/jhre/11-3/jhre.2020.03.04.xml
5. Ponti M., Craglia M. (2020). Citizen-generated data for public policy, Joint Research Centre. https://ec.europa.eu/jrc/communities/en/community/ citizensdata/document/citizen-generated-data-public-policy/ (accessed: 28.04.2024)
6. Sieber R., Johnson P. (2015). Civic open data at a crossroads: dominant models and current challenges. Government Information Quarterly, Vol. 32, № 3, Elsevier, pp. 308–315. https://doi.org/10.1016/j.giq.2015.05.003
7. Kullenberg C. Kasperowski D. (2016) What is citizen science? – a scientometric meta-analysis. PLoS ONE, Vol. 11, № 1, PLOS, San Francisco, California, United States. https://doi.org/10.1371/journal.pone.0147152

PROBLEM ISSUES OF JURISDICTION AND PROCESSING OF PERSONAL DATA IN THE CONDITIONS OF THE DEVELOPMENT OF DIGITALIZATION

Dyakovsky O.

Senior Lecturer at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", PhD in Law.

https//orcid.org/0000-0003-3412-9278

In modern conditions of the development and functioning of electronic document circulation, the use of trust services, the operation of registers, their increase, expansion of functionality affects the accumulation of information. The collection of information and personal data also takes place during judicial proceedings, including with the help of the "Electronic Court" software. The introduction of the digitalization vector requires the exchange of information between various state authorities, but in this area there is a need to resolve the issue of the interaction of bodies and institutions with the work and functioning of the "Electronic Court", which indicates the relevance of this study.

Data protection has always been and remains the object of increased attention of lawyers. Modern researchers pay considerable attention to problematic issues of personal protection, among them the following should be noted: O.V. Bryntsev, I.M. Horodyskyi. Sukhorilskyi P. and others. The question of the functioning of the "Electronic Court" was investigated by V. S. Politanskyi. as well as other scientists. Each of them made a significant contribution to the study of this issue, but the problem of the interaction of state

authorities and institutions with the work of the court needs further elaboration.

The regulation on the functioning of individual subsystems (modules) of the Unified Judicial Information and Telecommunication System determines the functioning of certain subsystems (modules) of the Unified Judicial Information and Telecommunication System, in particular the "Electronic Cabinet" and "Electronic Court" subsystems in courts and justice system bodies [3] .

As of today, the participants in the case have the opportunity to use the "Electronic Court" by sending lawsuits, appeals, petitions, statements, participating in video conferences and performing other procedural actions. With the help of this software, the participants in the case are also notified.

We should support the position of V. S. Politanskyi. that the electronic court is not only a certain form of use of information and communication technologies by all interested parties of the judicial process in order to increase its efficiency and quality, but also a direct and full-fledged procedure for the implementation and/or delivery of justice in electronic form, starting from the preparation of the case, its consideration of the merits, court debates and ending with the adoption of the verdict and the announcement of the decision in electronic form [4, p. 37].

It is worth noting that the Decree of the President of Ukraine dated February 24, 2022 No. 64/2022 "On the introduction of martial law in Ukraine" introduced martial law from 05:30 on February 24, 2022 for a period of 30 days [2]. Martial law has been repeatedly extended and continues to this day.

Along with this, the functioning of the state register of real property rights, the unified state register of court decisions, the unified state register of legal entities, individual entrepreneurs and public organizations, and the unified register of debtors is observed. In fact, more than thirty types of registers with various types of information and personal data are functioning. natural persons.

Legal and organizational principles for the creation and functioning of the Unified State Register of conscripts, conscripts and reservists, regulation of relations in the field of state registration of citizens of Ukraine who are in reserve for the recruitment of the Armed Forces of Ukraine and other military formations formed in accordance with the laws of Ukraine for a special period, and also for the performance of work to ensure the defense of the state and persons assigned to conscription stations is carried out on the basis of the Law of Ukraine "On the Unified State Register of Conscripts, Conscripts and Reservists" [1].

This regulatory and legal act contains 16 articles that regulate: the unified state register of conscripts, conscripts and reservists, main tasks, language of conduct, subjects and obtaining information from the Register, personal data, official data, rights and obligations, guarantees protection and security of data of conscripts, conscripts and reservists, creation, formation and form of keeping the Register, electronic cabinet of conscript, conscript, reservist, electronic cabinet of the center for providing administrative services, responsibility, final provisions.

From the above articles of regulation, it is possible to single out the main areas of regulation related to maintaining the register and filling it with personal and official data and additional ones related to guarantees and responsibilities in this area.

In accordance with Part 1 of Art. 6 of the Law of Ukraine "On the Unified State Register of Conscripts, Conscripts and Reservists" in the version of the law dated 04.04.2024 states that personal and official data of conscripts, conscripts and reservists are entered, processed and stored in the Register [1].

Analyzing judicial proceedings under martial law, a problem was revealed, which consists in the fact that the judicial authorities do not contain information on whether a person has been mobilized at the time of the case. In fact, a person is notified at his place of registration, which as of today is not sufficient, taking into account the

mobilization of a participant in the process who is not at the place of registration and is involved in hostilities.

Therefore, there is a need to solve this issue by making changes to national legislation by providing access to judicial authorities to information about the "Oberig" database and other information systems in order to obtain information about the possible mobilization of a person. After receiving this information, the court in each specific case took this information into account when making a court decision and decided on the issue of a possible suspension of the proceedings.

Thus, as a conclusion, it should be noted that the national legislation enshrined in the procedural codes of general, civil and administrative jurisdiction does not provide for the proper notification of the person who is mobilized due to the lack of connection to the necessary information systems, which indicates the need to amend the national legislation and expand the access of judicial authorities to the repulsive registers.

References:

1. Pro Yedynyi derzhavnyi reiestr pryzovnykiv,viiskovozoboviazanykh ta rezervistiv: Zakon Ukrainy vid 16.03.2017 [On the Unified State Register of Conscripts, Conscripts and Reservists: Law of Ukraine dated March 16, 2017]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/1951-19#Text [in Ukrainian]. (accessed: 04/30/2024).

2. Pro vvedennia voiennoho stanu v Ukraini : Ukaz Prezydenta Ukrainy vid 24.02.2022 [On the introduction of martial law in Ukraine: Decree of the President of Ukraine dated February 24, 2022]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/1951-19#Text [in Ukrainian]. (accessed: 04/30/2024).

3. Polozhennia pro poriadok funktsionuvannia okremykh pidsystem (moduliv) Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy, zatverdzhene rishenniam Vyshchoi rady pravosuddia vid 17 serpnia 2021[Regulations on the procedure for the functioning of individual subsystems (modules) of the Unified Judicial Information and Telecommunication System, approved by the decision of the High Council of Justice

dated August 17, 2021]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/rada/show/v1845910-21#Text [in Ukrainian]. (accessed: 04/30/2024).

4. Polozhennia, S. (2020). Osoblyvosti vprovadzhennia ta funktsionuvannia elektronnoho sudu v Ukraini [Politansky S. Peculiarities of implementation and functioning of the electronic court in Ukraine]. Law and Society, 5, 35-40. Retrieved from http://pravoisuspilstvo.org.ua/archive/2020/5_2020/8.pdf [in Ukrainian]. (accessed: 04/30/2024).

LEGAL REGULATION OF LABOR RELATIONS IN MODERN CONDITIONS OF DIGITALIZATION

Golosnichenko D.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Doctor of Law, Associate Professor

It is quite clear that legal regulation is derived from the changes taking place in the field of digitization and the labor market. Ukraine is at the beginning of the journey regarding changes in the legal regulation of labor relations in conditions of digitalization, and these changes are taking place in a fragmented manner.

To date, the new Labor Code has not been adopted. This codified legislative act would be able to systematically regulate labor relations in the conditions of digitalization.

The current Labor Code was developed in an industrial society, when the employee was inextricably linked to the workplace during the working day. Now, technical progress makes it possible to be mobile, often go on business trips, and conduct dozens of projects in parallel. The employee is now available 24/7, some office workers do not have a specific workplace assigned to them, but there

is a general open space and WiFi. And work becomes available online, even when you are on sick leave or on vacation [1, p. 140].

Ukrainian labor legislation consists of many legislative acts of the USSR, which do not correspond to modern realities and lead to certain difficulties in law enforcement [2, p. 103]. For example, until recently, regulatory and legal regulation was provided only in relation to home work and flexible working hours. But the norms regulating these types of work were also quite outdated.

In 2020 and 2021, appropriate changes were made to the current Labor Code with the aim of regulating flexible working hours, remote or home work [3].

In our opinion, the mentioned changes to the labor legislation are effective and necessary not only in relation to their application in the conditions of the threat of the spread of an epidemic, a pandemic, an emergency situation of man-made, natural or other nature, martial law, but also in relation to the organization of work in conditions of digitalization.

The impact of digitization on labor relations in modern conditions is manifested in the following. First, digitalization is an integral part of labor market reform. Secondly, digitalization allows reducing the burden on business, carrying out effective deregulation of labor relations, influencing the bureaucratization of labor relations. Thirdly, it allows inspections using a risk-based approach – only in companies that have signs of the greatest risks of violating labor legislation.

In today's world, the role of interactive platforms through which online employment is implemented is growing. The most popular digital online employment tools include Uber, Lyft, TaskRabbit, UpWork, and Amazon Mechanical Turk. The data generated by these platforms is becoming important for understanding the specifics of employment in the digital economy. In general, foreign experience shows the rapid spread of digital tools, interactive platforms and information technologies in the labor market [4].

Digitalization is most evident in the regulation of labor relations in the field of information technologies. It is necessary to support the opinion of O. G. Sereda that the labor relations between employers and specialists in the IT sphere can be characterized as one of the most dynamic and those that have atypical forms and conditions, reacting as quickly as possible to changes in the social existence of mankind [5, p. 258].

Quite often, specialists in the field of IT prefer to perform work and provide services in the status of natural persons – entrepreneurs on the basis of concluded civil-legal contracts for the provision of services or subcontracting. But at the same time, there is a certain risk of reclassification of such relations from civil law to labor law with corresponding legal consequences.

One of the main features of labor relations is the systematic performance of a labor function. In other words, it is manifested in the daily performance of the relevant tasks and duties defined by the employee's employment contract or job description. At the same time, the performance of a labor function does not aim to achieve a certain result.

Unlike an employment contract, a civil law contract establishes the obligation of the executor or contractor to provide the customer with a finished product or perform a certain specified service. For example, the development of a website, software, or any other product can be formalized through the conclusion of a civil law contract. If an IT specialist at an enterprise, institution, or organization, regardless of the form of ownership, performs the duties of ensuring information security, maintenance of equipment, equipment, and networks on a permanent basis, this is a sign of labor relations [6].

Until recently, one of the main features that made it possible to distinguish labor relations from civil-law ones was the employee's submission to the rules of the internal procedure, while under the civil-law contract, the process of organizing activities involves independent organization of one's work and performance at one's own risk.

But in 2020, relevant changes were made to Article 21 of the Labor Code, according to the provisions of this article, an employment contract is defined as "an agreement between an employee and the owner of an enterprise, institution, organization or a body or natural person authorized by him, under which the employee undertakes to perform work, determined by this agreement, and the owner of the enterprise, institution, organization or a body or individual authorized by him undertakes to pay the employee a salary and ensure the working conditions necessary for the performance of work, provided for by the labor legislation, the collective agreement and the agreement of the parties" [3].

As we can see, in contrast to the previous version of the article, such a mandatory feature of the employment contract as the subjection of the employee to the internal labor regulations was excluded from the definition.

The specifics of work in the IT field, compared to other fields, quite often involve flexible working hours, remote or home work. This is also due to the fact that IT specialists, not infrequently, given the specifics of their activity, do not have a permanent workplace.

Digitalization of employment is becoming a problem of the modern labor market. It causes not only the appearance of new professions in recent decades, but also the disappearance of some of them.

EU initiatives are aimed at creating a single digital market. According to EU experts, automation in many industries will lead to the creation of 2 million new jobs for unique software workers and engineers, which in turn will lead to the reduction of 7 million jobs for specialists with average qualifications – they will be replaced by robots [1, p. 140].

In the conditions of globalization and digitalization, new forms of labor organization are emerging. In addition to the usual for us, home work, traveling nature of work, remote work, flexible employment, electronic self-employment have emerged. The emergence of new forms of labor organization requires not only their legal reg-

ulation, but also changes in the legal regulation of concluding an employment contract, work regime, rest, vacations, etc.

An important component for reforming the labor market is the transition to keeping records of labor activity in electronic form.

A certain step towards the introduction of electronic record-keeping was the adoption of the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding the Accounting of Labor Activities of Employees in Electronic Form" dated February 5, 2021. According to the norms of this legislative act, employees and employers are given time until June 10, 2026.

The electronic work book, as a digital analogue of the paper work book, was introduced to improve the accounting of labor activities, reduce paper document circulation and the associated risks of document loss or damage. Accounting of labor activity in electronic form allows you to accumulate, store and use information about the employee's work experience, education, qualifications to confirm the existing work experience.

In our opinion, an important step in the digitization of labor activity should be the introduction of an electronic labor contract. In accordance with the provisions of Article 24 of the Labor Code of Ukraine, an employment contract is usually concluded in writing, but in accordance with the provisions of Articles 9, 205, 207 of the Civil Code of Ukraine, an electronic form is equated to a written form.

In order for the employee to conclude the contract in electronic form, he needs an electronic signature. This issue is also already regulated by the norms of the current Ukrainian legislation. In Ukraine, the two most common types of electronic signature are a qualified electronic signature and an improved electronic signature with qualified certificates, which are equivalent to a handwritten signature.

Ukrainian legislation needs to be amended in order to regulate the conclusion of an employment contract in electronic form, in addition, this provision must be taken into account when adopting the new Labor Code.

Summing up, it should be noted that the improvement of the legal regulation of the labor market in Ukraine in the conditions of digitalization should take into account the interests and be positive for all subjects of labor relations – employees, employers and state bodies.

References:

1. Butynska R. J. Vpliv tsyfrovykh tekhnolohij na trudove pravo: vikliki ta zavdannja / Problemi tsivilnoho, gospodarskoho, trudovoho prava ta prava socialnoho zabezpechenia: Chasopis Kievskogo universiteta prava. № 3/2019. – P.139-144

2. Skripnik J. O. Osoblivosti trudovih pravovidnosin iz distantsyinimi pratsyvnikami: zarubizhnij dosvid ta perspektivy dlja Ukrainy / Juridychnij zhurnal/. . № 6/2020. – P. 101-105

3. Kodeks zakoniv pro pratsiu Ukrainy: Zakon Ukrainy vid 10 grudnja 1971 p. № 322–VIII. URL: https://zakon.rada.gov.ua/laws/ show/322-08#Text (accessed: 05/10/2024).

4. Vyshnovetska, S.V. Problemy trudovoho zakonodavstva v umovakh prekaryzatsii ta tsyfrovizatsii zainiatosti. Aktualni problemy trudovoho zakonodavstva, zakonodavstva pro derzhavnu sluzhbu ta sluzhbu v pravookhoronnykh orhanakh: mater. VII Vseukr. nauk.-prakt. konf. (m. Kharkiv, 16 lystop. 2018 r.) / za zah. red. K.Yu. Melnyka. Kharkiv: Kharkiv. nats. un-t vnutr. sprav , -- 2018. C. 57–60.

5. Sereda O. G. Do pytannja vyznachennja okremych osoblivostej trudovyh vidnosyn pratsivnykiv IT-sfery / Naprjami rozvytku nauky trudovoho prava ta prava socialnoho zabezpechenia: materialy VI Vseukrainskoi nauk.-prakt. konf., prisvjachenoi 25-richchju kafedry trudovoho ta gospodarskoho prava (m. Kharkiv, 3 listopada 2017 r.) nats. un-t vnutr. sprav Kharkiv:; / za zah. red. K.Yu. Melnyka. Kharkiv: Kharkiv. nats. un-t vnutr. sprav, -- 2017. – P. 257-259.

6. Kurilko Veronika. Robota v IT: kljuchovi osoblyvosti / Jurydychna gazeta online №27 (681). 02 липня 2019. URL: https://yur-gazeta.com/dumka-eksperta/robota-v-it-klyuchovi-osoblivosti.html. (accessed: 05/10/2024).

THE GENESIS OF CRIMINAL LIABILITY FOR MISAPPROPRIATION AND EMBEZZLEMENT OF PROPERTY

Hvasaliia A.

postgraduate student of the first year of study at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute"

Misappropriation of property causes significant damage to the state, legal entities and even individual citizens, although it is only the third most common property crime after theft and fraud. Despite the efforts made by the state to combat this negative phenomenon, the number of cases of criminal misappropriation does not decrease. Many criminals avoid criminal liability, which is evidenced by, in particular, numerous publications in the mass media. It is necessary to find out the reasons for the insufficient efficiency of the state policy of combating the misappropriation of property and similar acquisitive crimes. Criminogenic factors in this case can be determined not only by the social, political or economic circumstances of our life, but also by the flaws of the relevant criminal legislation, the practice of its application, insufficient qualifications and abuses among representatives of law enforcement agencies and judges. This prompts a deep study of the issues of criminal liability for misappropriation, embezzlement of property or taking possession of it through abuse of official position, which requires a detailed analysis of the historical experience of the application of legislation in the relevant field. Our research is dedicated to the study of the genesis of criminal liability for misappropriation of property in Ukraine from the oldest legal monuments to the current criminal law.

For the first time, the misappropriation of property, which was in someone's possession, was mentioned in "Ruska Pravda" [1], which envisaged it as a violation of the rights of individuals (offenses). Such offenses were punished by compensation for damages or by selling the offender into slavery. For the recovery of property from a person to whom it was previously entrusted, "Ruska Pravda" provided for a simplified procedure, which laid the prerequisites for specific legal responsibility for misuse of entrusted property.

Lithuanian statutes defined misappropriation as a crime punishable by the state in the person of the sovereign. The first criminally punishable misappropriations were essentially corrupt, i.e., were committed by persons endowed with state-authority functions or related to state property. For example, illegal collection of tax by the headman according to the Statute of 1529 [2] or misappropriation by the minter of gold provided for minting coins according to the Statutes of 1566 [3] and 1588 [4]. Misappropriation of state property was punishable by death, and therefore was recognized by Lithuanian statutes as more socially dangerous than taking possession of other people's property even by abuse of official position.

The Council Regulation of 1649 [5], sequentially, punished misappropriation of property regardless of the status of the perpetrator, which laid the foundations for the formation of the principle of equality before the criminal law. Along with this, private individuals' misappropriation of property that did not belong to the state was still considered a civil tort.

The Military article of 1715 [6], borrowing provisions of German law, covers misappropriations to retention (non-return), concealment and consumption for self-benefit. For the first time, the Article defines the signs of a person's connection with the property he encroaches on. Thus, the sign of "having state funds in self hands" supposed certain powers regarding state property, which is given to a person for ensuring state interests and official purposes, i.e. to give in possession. To give property into "safe hands" implied trust relationship between the owner of the property and the culprit, therefore

the retention (non-return and concealment) of such property was a violation not of the interests of the service, but of the trust shown to the culprit. This understanding of the indicated connection between a person and property should be considered as prototypes of the misappropriation signs "to be in the possession" or "to entrust" in the current version of Art. 191 of the Criminal Code of Ukraine [7].

Compared to the Article, the Laws by which the "Malorussian" people are tried of 1743 [8] were more lenient to the guilty in terms of property, not establishing the confiscation of property in case of misappropriation. The rights distinguished the illegal acquisition of property by the method of its committing, laying the prerequisites for the modern distinction between misappropriation of property and taking possession of it through abuse of official position.

The Code of Laws of the Russian Empire of 1832 [9] highlighted in misappropriation a sign of using (turning) someone else's property to self-benefit without the consent of its owner and for the first time established criminal liability for misappropriation of private property. The rules of the Code abolished the death penalty for misappropriation and embezzlement of property, which was not established until the Soviet legislation of 1917-1921.

In the Provisions on Punishments of 1845 [10], an attempt was made to criminalize specific cases of misappropriation in all their certain features, which only led to excessive casuistry and complexity in law enforcement. The general composition of misappropriation of someone else's movable property entrusted to a person is established only by the Criminal Code of 1903 [10]. The peculiarity of the mentioned laws was the differentiation of punishment for illegal appropriation depending on status, which contradicted the idea of equality before the criminal law, which was quite widespread at that time.

In the Austrian Criminal Code of 1803 [11] (acted in Galicia), only two types of misappropriation ("veruntreuung") of entrusted property were provided for: official and committed by the debtor in relation to the creditor's property. In Austria these crimes were punished much more stringently than in other European countries

of that time. Thus, the maximum term of imprisonment for qualified misappropriation was supposed to be five times longer than the maximum term of imprisonment for the same crime according to the Provisions on Punishments of 1845.

The Criminal Code of the Ukrainian SSR of 1922 [12, p. 570-591] for the first time singled out and established two main types of encroachment on property committed by a person who has certain powers over someone else's property: misappropriation and embezzlement. At the same time, the sign of "entrusting property" did not refer to the authority of the official person in relation to the property (which was typical for "property in possession"), but assumed a certain trust of the owner of the property in the culprit. According to this trust the owner entrusted his own property to the culprit.

The Criminal Code of the Ukrainian SSR in 1960 [13] decriminalized the misappropriation of non-state property, which was criminalized again only in 2001 with the adoption of the current Criminal Code of Ukraine. Along with this, in Art. 84 of the Criminal Code of 1960 introduced a new method of taking possession of state or collective property – by abuse of official position. The corresponding norm provided for cases when an official person (officer), not having authority over property, can turn it to his advantage by using his official position. Thus, the signs of illegal collection of taxes, laid down in Lithuanian statutes, found their consolidation in the composition of taking possession of property by abuse of official position. Today, the acquisition by an official, for example, of a charitable organization, of funds that come to it from citizens, will be qualified as taking possession of property by abuse of official position.

The approaches of the Soviet laws to the criminalization of certain cases of acquisitive and corruption crimes changed, taking into account the specifics of the criminogenic situation. In particular, the death penalty was imposed for misappropriation with aggravating circumstances in 1917 until it was replaced by imprisonment for up to ten years with confiscation of property by the Criminal Code of the Ukrainian SSR in 1927 [14]. According to the decree of the Presidium

of the Supreme Council of the USSR dated June 4, 1947 [14], the punishment for misappropriation and embezzlement was increased in connection with post-war measures to combat economic crime – the maximum term of imprisonment was increased to twenty-five years. The severity of the punishment for misappropriation was again reduced according to the Criminal Code of 1960 to imprisonment for up to fifteen years. In 1961, the death penalty was again introduced for acquisition of state property in particularly large amounts, which was applied until its abolition in 1992. The Soviet codes were also characterized by an alternative confiscation of property for simple misappropriation and embezzlement and mandatory – for qualified.

In the current edition of Art. 191 of the Criminal Code of Ukraine, confiscation of property is mandatory only for the commission of misappropriation in particularly large amounts or by an organized group. Just like the provisions of the Laws by which the "Malorussian" people are tried of 1743, the Criminal Code of Ukraine of 2001 also proved to be lenient towards those guilty of misappropriation. On the other hand, the lenience of property penalties for misappropriation is inconsistent with the large amount of damage caused by such crimes. Therefore, the issue of the adequacy of the punishment for the level of public danger of misappropriation and embezzlement in Ukraine requires in-depth study and will be the subject of further research.

References:

1. Karamzinsky list. Pravda russka: Texts based on 7 lists and 5 editions / comp. S. Yushkov. Kyiv: VUAN, 1935. URL: http://litopys.org.ua/yushkov/yu.htm (accessed: 05/01/2024).

2. Statute of the Grand Duchy of Lithuania in 1529 [Text in Old Russian]. Statutes of the Grand Duchy of Lithuania: in 3 volumes / edited by S. Kivalova, P. Muzychenka, A. Pankova. Odesa: Legal literature, 2002. Vol. 1. P. 37-191.

3. Statute of the Grand Duchy of Lithuania in 1566 [Text in Old Russian]. Statutes of the Grand Duchy of Lithuania: in 3 volumes / edited by S. Kivalova, P. Muzychenka, A. Pankova. Odesa: Legal literature, 2003. Vol. 2, pp. 33-201.

4. Statute of the Grand Duchy of Lithuania in 1588 [Text in Old Russian]. Statutes of the Grand Duchy of Lithuania: in 3 volumes / edited by S. Kivalova, P. Muzychenka, A. Pankova. Odesa: Legal Literature, 2004. Vol. 3. P. 19-327.

5. The Council Regulation of 1649 / sub. ed. M.N. Tikhomirova, P.P. Epifanova. M.: Izd-vo Moscow. University, 1961. 431 p.

6. Military article [Text]. Russian legislation of the 10th – 20th centuries: in 9 volumes. M.: Yuryd. lit., 1986. T. 4. C. 327–389.

7. Criminal Code of Ukraine: Law of Ukraine dated 04/05/2001 No. 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (accessed: 05/01/2024).

8. Laws by which the Malorussian people are tried. 1743. / edit. K.A. Vyslobokov; resp. ed. and author prev. : Yu. S. Shemshuchenko; National Academy of Sciences of Ukraine, Institute of State and Law named after V. M. Koretskyi, Institute of Ukrainian archeography and source studies. named after M. S. Hrushevskyi. Kyiv, 1997. 547 p.

9. Code of laws of the Russian Empire [Text]. St. Petersburg, 1832. T. 15. 560 p.

10. Code of laws of the Russian Empire: in 16 volumes / under the editorship. and with note I. D. Mordukhai-Boltovsky. St. Petersburg, 1912. T. 15. 272 p.

11. Strafgesetz¸ber Verbrechen,Vergehen und bertretungen mit Kundmachungs-Patent. vom 27. Mai 1852. Osterreichisches. URL: https://e-archiv.li/files/1852_05_27 _Strafgesetzbuch.pdf. (accessed: 05/01/2024).

12. Collection of Resolutions and Orders of the Workers' and Peasants' Government of Ukraine for 1922-1923 / Council of People's Commissars of the Ukrainian SSR. Kharkiv: "Knygospilki" summer printing house, 1922. 1147 p.

13. Mykhaylenko P.P. Criminal Code of the Ukrainian SSR [Text]: Official text with changes and additions on March 1, 1968 and articles / Legal Commission under the Council of Ministers of the Ukrainian SSR. – Kyiv: Politvydav of Ukraine, 1968. – 238 p.

14. Mykhaylenko P.P. Laws Criminal Code of the Ukrainian SSR [Text]: Approved. June 8, 1927: Official text with changes and additions on November 1, 1949, from the post materials and add. / Ministry of Justice of the Ukrainian SSR. Kyiv: Derzhpolitvydav of the Ukrainian SSR, 1949. 167 p.

DIGITALISATIOND AS A PREREQUISITE FOR ENSURING ACCESS TO JUSTICE IN MODERN REALITIES

Kozakevych O.

Senior Lecturer at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", PhD in Law

The introduction of e-courts is an important step in reforming the judicial system, which is aimed at global information and communication development. Under current conditions, Ukraine is gradually creating the necessary favourable technical conditions and the e-court is now being practically implemented in the Ukrainian judiciary. The full implementation of e-justice in Ukraine was inextricably linked to the outbreak of the pandemic and the introduction of quarantine restrictions. The transition of justice to a remote mode of operation is an example of a response to a global challenge in a democracy. It can be stated that the prerequisites for the functioning of e-justice are the development of technological progress and the desire to make the process of interaction between citizens and courts more convenient and comfortable.

The introduction of the E-Court is one of the most modern forms of access to justice. In support of this, it is worth noting that the UJITS ensures the exchange of documents in electronic form between all parties to the process and the court. Participants in the court proceedings can exchange electronic documents, which saves time and costs for producing paper documents, as well as sending and receiving them in court. Users of the UJITS subsystems can use the online help function, callbacks, and correspondence via various

messengers to receive advice or provide feedback on the operation of electronic services [1].

The use of the eCourt subsystem means the transition of justice to a modern, convenient and affordable way of not only accepting documents in electronic form, but also holding court hearings via videoconference without the personal presence of the participants and their representatives in courtrooms. Conducting court hearings via videoconference saves time and resources for the parties, as it minimises time spent on travelling to court and saves costs associated with, for example, travelling to a court in another region.

In addition, the consideration of corporate disputes via videoconferencing is quite relevant for the parties to such disputes. With significant savings in time and resources, the company can ensure that all participants are present at such a meeting without interrupting its core business. Obviously, this factor will also contribute to the administration of justice.

Pursuant to a number of legislative acts, including the Code of Administrative Procedure, the Code of Civil Procedure, the Code of Criminal Procedure and the Code of Criminal Procedure, the SLC team has provided the possibility of convenient and fast submission of documents to the Grand Chamber of the Supreme Court through the Electronic Cabinet"[1].

In addition, in the context of ensuring access to justice, it is possible to apply to the High Council of Justice through the Electronic Court to express your reasonable comments or file a complaint against a judge[1].

This indicates progressive steps towards speeding up the consideration of cases, which in the long run will relieve the courts. At the same time, the current legislation provides for the right to submit documents to the court in the classic paper form, after the introduction of the UJITS, which also provides certain categories of citizens with access to justice.

The functioning of the E-Court is not only a legislative novelty, but also a manifestation of the modern information society aimed

at accessibility, using "Open Principle" to all spheres of public life, including justice. Thus, it can be stated that in the current conditions, the use of the functionality of the UJITS "Electronic Court" subsystem is a new, accessible and effective form of ensuring access to justice for citizens.

The introduction of the legal regime of martial law on the territory of Ukraine has undoubtedly affected the administration of justice. It can be argued that ensuring its accessibility has become one of the state's top priorities. Obviously, Ukrainian courts are currently facing unfavourable and unequal conditions. All of this changes the timeframe for consideration of cases and affects the attendance of participants at court hearings. That is why the active use and implementation of information technology in the work of courts, the functionality of the UJITS subsystem "Electronic Court" solves the above barriers and is indeed a means of ensuring access to justice during martial law. However, the most important factor is that the use of UJITS provides citizens with access to the video conferencing subsystem, which makes it technically possible to participate in a court hearing regardless of location.

At the same time, the question of how Ukraine will be rebuilt and restored and return to a peaceful way of life is becoming more relevant. Certain steps have already been taken in this direction. In particular, the Recovery Plan for Ukraine has been created, which aims to accelerate sustainable economic growth and is based on the following principles: immediate start and gradual development; building equitable prosperity; EU integration; rebuilding better than before on a national and regional scale; and stimulating private investment. The Plan identifies a list of national programmes to achieve key results[2].

When analysing the category of access to justice in the context of the National Programmes for Future Reconstruction, it should be noted that the projects of the National Programme Fundamentals of Recovery: Digital State and Strengthening Institutional Capacity.

The project Fundamentals of Recovery: Digital State, to ensure accessibility of justice, includes: development of the Strategy for

the transfer of public services into electronic form during the reconstruction period, development of electronic interaction of electronic information resources, development of the Diia.Centres network, development of the system of public electronic registers, digital accessibility (barrier-free), artificial intelligence in the provision of public services[2].

It should be added that the project "Ukraine after the Victory: Preparation and Communication of Reforms for the Implementation of the Vision of Ukraine – 2030" envisages the digitalisation of justice, which includes the digitalisation of court document management processes; ensuring centralised, secure storage of court case files and other court documents in cloud services; and the widespread introduction of modern digital technologies, in particular artificial intelligence, to facilitate dispute resolution by the parties, search for relevant case law, and prepare draft laws and regulations[3].

These programmes are relevant in the area of access to justice. Some programmes are already operating in the national justice system and are characterised as effective means of ensuring access to justice (Unified Judicial Information and Telecommunication System, development of electronic interaction of electronic information resources, development of the system of public electronic registers). At the same time, the inclusion of these areas in the priority restoration programmes indicates further development of their technical functionality in line with the latest information trends.

On 1 March 2024, Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technologies in judicial proceedings" was presented to the Council of Europe Project "Support to the Judiciary of Ukraine in the Context of War and Post-War Period" jointly with the Supreme Court. According to the Head of the Council of Europe Office in Ukraine, the development of assistive technologies and their use by the judiciary is an inevitable process, especially for Ukraine, given the impact of a full-scale war and the excessive workload of judges [4]. This Opinion contains relevant theses, including the official

introduction of court hearings in a remote format and the introduction of relevant amendments to the procedural legislation.

According to the Mission of the Supreme Court Development Strategy for 2023 – 2027, the Supreme Court is to ensure fair, efficient and prompt resolution of conflicts (disputes) between members of society, including through innovation (digital transformation of justice); to constantly move forward, to be an agent of change in the judicial system and an example for other courts and justice organisations in terms of efficiency, transparency and first-class service; to promote European integration (to bring our judicial system closer to EU standards in the field of justice, to implement the best European practices of court management). To ensure these goals, the SC. The priority goal is to promote digital transformation of processes (digitalisation) to ensure better access to justice, better service and cost reduction [5].

Analysing the above, it is possible to assert certain steps of Ukrainian justice towards digitalisation. The outbreak of the pandemic, followed by the introduction of martial law throughout Ukraine, has led to the judicial system stumbling over problems that can be immediately solved by using the latest information technology. This demonstrates that justice is indeed becoming more accessible to everyone, especially in such a difficult time.

Undoubtedly, these are the latest ideas for ensuring access to justice, which are in line with the trends of the information society, aimed at saving time and costs, transparency and dynamism of case consideration, and processing large amounts of information.

It is noteworthy that the terms “remote justice”, “predictive justice”, and “accessible justice” are increasingly used in the literature and media. This indicates that the use of the latest information technologies has a real impact on modern justice and is one of the mechanisms for overcoming barriers to the implementation and protection of the right to access to justice.

In general, e-justice activities are aimed at the interaction of people, technology, and the court, which provides access to the court without personal presence in the courtroom, publicity, openness,

impossibility of outside influence on the independence and impartiality of judges, which ultimately contributes to the implementation of access to justice and strengthening confidence in justice as the realisation of justice.

References:

1. The State Enterprise "Centre of Court Services" has introduced communication with users regarding the improvement of the E-Court account. URL: https://court.gov.ua/press/news/1413560/. (accessed: 05/07/2024).

2. Plan for the Reconstruction of Ukraine. URL: https://recovery.gov.ua. (accessed: 05/07/2024).

3. Concept of Justice System Reform "Ukraine after Victory" Vision of Ukraine 2030. URL: https://pravo.org.ua/sformovano-kontseptsiyu-reformy-systemy-pravosuddya. (accessed: 05/07/2024).

4. The new Opinion of the Consultative Council of European Judges No. 26 on the use of assistive technologies in court proceedings is presented .URL: http://surl.li/tgrws. (accessed: 05/07/2024).

5. The Supreme Court Development Strategy for 2023-2027. URL: https://surl.li/tgruo. (accessed: 05/07/2024).

DIGITAL ECONOMY: CURRENT CHALLENGES AND OPPORTUNITIES FOR UKRAINE

Lupak Z.
Master of Laws

During globalization, there is a world tendency to transition from a traditional economy to a digital one and its dynamic development, which has caused the Fourth Industrial Revolution. Knowledge, information and innovative technologies are a priority in the 21st century. Production, sale, supply of traditional goods and services are now accomplished with the help of information and communication technologies on the Internet. Today it is very important to

be flexible and quickly adapt to new conditions. That is why countries throughout the world are actively introducing the digitalization of all spheres of life, including the economy.

At the same time, in Ukraine, IT services provide a significant part of foreign currency income to the economy and are an integral part of it, especially in time of economic crisis. In 2023, IT services are the largest export industry. This is approximately 40% among Ukraine's services exports, which is 9.3% less than in 2022 [1]. Today, the share of the IT sector in the GDP of the country is 4.9% (the contribution to the Gross Value Added is $5.5 billion) [1].

Furthermore, two scenarios of digitalization of Ukraine's economy are known: target (forced) and inertial (evolutionary). The first involves the rapid development of the digital economy in 5 years, the establishment of Ukraine as a European leader in the field of information technologies, the attraction of investments and the creation of a productive labor market with the most favorable working conditions for specialists. All this is possible only with the cooperation of the state, business and civil society. The second scenario involves the construction of an inefficient, uncompetitive, investment-unattractive economy that does not meet external and internal challenges and labor migration of specialists abroad.

Nowadays, there are certain challenges in Ukraine that hinder the rapid transformation processes of the digital economy, including the following:

– Unfavorable economic situation due to the Russian-Ukrainian war, which slows down the introduction of new technologies and makes the country unattractive for investments.

– Low involvement of state bodies in the implementation of digitalization processes and the use of outdated technology in state structures. Along with that, to speed up the digitalization process, the Ministry of Digital Transformation of Ukraine (hereinafter – MDT) introduced the position of chief digital transformation officer (CDTO). Today, about 55 CDTOs are working at the level of ministries, regional administrations and city councils. In addition,

in 2023, the CDTO Campus digital transformation leaders training project for the modernization of the civil service with the help of innovations and technologies was launched.

– Low level of state support for the digitization process in the business sector. Currently, most large enterprises use advanced technologies to optimize the business process. At the same time, small and medium-sized businesses need additional support from the state and international organizations.

– The inadequacies in the legal framework of Ukraine and the inconsistency of legislation with modern transformational challenges.

– Digital infrastructures cover the country to a limited extent. According to MDT, licenses were reissued to cover 95% of the population of Ukraine with the Internet [2]. However, the armed aggression of the Russian Federation creates additional obstacles to access to the Internet and further damage to the infrastructure of Ukraine, interruptions in electricity supply and communication. In 2024, the Ministry of Digital Transformation is planning to launch a test 5G cellular connection. Covering 100% of the country with high-quality Internet should also be a priority of state policy.

– The digital gaps refer to the unequal access of individuals to Internet technologies. Thus, according to the digital literacy survey conducted by MDT in 2023, about 60% of Ukrainian adults have basic and advanced digital skills, which is 12.6% more than in 2019 [3]. In spite of that, the percentage of users with undeveloped digital skills remains high.

– Undeveloped advanced digital infrastructures. For example, the Internet of Things (IoT) – an advanced concept for collecting and exchanging data on the Internet, which is not effectively developed due to the complexity of integration, lack of unified standardization, high cost, weak cyber security and lack of qualified specialists for effective implementation.

– Shortage of highly qualified specialists who could facilitate and speed up the development of the state's digital economy. This is due to the complexity of the work of IT specialists in the interna-

tional market and the lack of opportunity for them to go abroad, the mobilization and priority participation of IT specialists in military projects during a full-scale war in Ukraine. The lower level of wages and working conditions compared to European countries causes the migration of workers abroad.

Despite all the challenges, Ukraine is the first state to equate a digital passport with a paper one and is already sharing its experience of providing electronic administrative services to citizens through the "Diia" application with other countries. Besides, approximately three million Ukrainians gained access to 4G technology for the first time in the past few years [2]. From now on, Ukrainians can develop digital skills on "Diia.Education" platform.

In addition, the Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine" No. 1667-IX dated July 15, 2021 regarding the operation of a special legal regime "Diia.City" to establish enabling environment for conducting business in IT sphere was adopted. Moreover, the Law of Ukraine "On Amendments to the Tax Code of Ukraine and some other laws of Ukraine regarding the specifics of taxation of business activities of electronic residents" No. 2654-IX dated October 6, 2022 provides an opportunity for electronic residents to accomplish business activities in Ukraine, etc.

In order for the digital economy to develop rapidly, the state should take a number of measures, such as:

– Removal of legislative barriers preventing the development of the digital economy. Especially, this concerns data security and privacy, protection against cybercrime. The reduction of the tax burden and the availability of credit for entrepreneurs developing innovative initiatives are also relevant. The implementation of the tax reform "10-10-10" and the finalization of the state program "Affordable loans 5-7-9%" can have a major impact. In addition, the functionality of the State Tax Service of Ukraine, started a few years ago, needs further digitization.

– State stimulation and assistance to businesses in the use of innovative technologies, especially in the target industries: military-industrial complex, energy, mechanical engineering, etc. The automation and digitization of business processes, the implementation of e-document management, and the restructuring of corporate culture are also important. All this will increase the competitiveness of companies, reduce costs and increase labor productivity.

– Creation of training programs that will help employees quickly adapt to the new requirements of the digital economy and ensure their access to the labor market. Today, almost every profession requires digital thinking, integration of information technologies in professional activity, new professions are appearing more and more often. Ukrainian IT specialists are highly valued abroad, so the IT industry works more for export due to its high adaptability. That is why, Ukraine needs to improve working conditions for specialists (including foreign ones), create effective and affordable additional trainings not only in schools and universities, but also at the state level.

The research of current challenges and opportunities of the digital economy of Ukraine leads to the following conclusions:

1. Today, it is critically important for Ukraine to prioritize digitization in the economic policy of the state, which is a component of Ukraine's national security.

2. Electronic innovations present a chance to effectively optimize Internet processes, increase productivity, reduce costs and create new prospects for development. The process of digitalization of the state allows to ensure fast, open and transparent access to information, which will help to reduce the level of bureaucracy, minimize malfeasance and corruption of government representatives, facilitate and improve the quality of obtaining public services for citizens, speed up the resolution of tasks, reduce costs for the state, optimize the state budget.

3. The potential and stability of Ukraine allows us to use the forced scenario of digital economy advancement in the nearest fu-

ture and to gain the leading position among European countries in the export of digital products and services. All this is possible under the condition of solving the current problems facing the economy of Ukraine.

References:

1. The volume of IT services exports from Ukraine in 2023 decreased by 8.4% and amounted to $6.7 billion. Ain, 2024. URL: https://ain.ua/2024/01/31/ukrayinskyj-it-eksport-u-2023-roczi-skorotyvsya-na-84/ (accessed: 05/11/2024).

2. Ministry of Digital Transformation: two years in effect. URL: https://2years.thedigital.gov.ua/ (accessed: 05/11/2024).

3. Study of digital skills of Ukrainians. The third wave. Ministry of Digital Transformation, 2023. URL: https://osvita.diia.gov.ua/research (accessed: 05/11/2024).

IMPACT OF DIGITALIZATION OF ENVIRONMENTAL RELATIONS ON BUSINESS

Lypnytska Y.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Candidate of Science of Law, Associate Professor.

Digitization is the driving force behind the transformation of the modern economy, and its impact on environmental relations and entrepreneurship is significant. In today's world, environmental issues are becoming more and more relevant, since the sustainability of the environment is critically important for sustainable development and

the future of humanity. Digitization opens up new opportunities for improving the management and regulation of environmental relations, increasing the efficiency of resource use and contributing to the preservation of the environment.

We can agree with the conclusion of scientists O. Vinnyk and N. Malysheva, that digitalization, as one of the most significant features of today, significantly affects not only the economic sphere, but also all aspects of social development, including ecological and social, contributing to the implementation of the concept of sustainable development [1, p. 250]. At the same time, the concept of digitalization of environmental relations should be understood as the introduction of digital technologies and innovations to optimize management in the field of ecology by increasing the effectiveness of measures to protect the natural environment, use nature and ensure environmental safety [2, p. 329].

Digitization, including in the field of environmental relations, is increasingly becoming the subject of scientific discussions. Studies of various aspects of the digitalization of environmental relations are presented in the scientific works of O. Vinnyk, N. Malysheva, P. Kulynycha, N. Ilkov and other scientists in the field of environmental law. At the same time, it is advisable to investigate in more detail the impact of digitalization of environmental relations on business entities, as well as the legal basis for such digitalization.

The main legislative acts in the field of environmental protection almost do not provide provisions for the digitization of individual processes, despite the fact that the corresponding measures take place in practice.

Thus, the Law of Ukraine "On Environmental Protection" [3], which is the basic legislative act in the field of environmental relations, does not regulate the digitalization of the environmental industry, nor does it even establish the directions for the use of digital technologies. Digitization has not been singled out as a separate area of state environmental policy in the Law of Ukraine "On the Basic Principles (Strategy) of the State Environmental Policy of Ukraine

for the Period Until 2030", which defines the main tasks and measures of state authorities for the coming years. At the same time, among the goals of the Strategy is the introduction of electronic governance, informatization of the sphere of environmental protection and nature management at all levels [4].

Individual digitization measures are mentioned in the National strategy for waste management in Ukraine until 2030, approved by the order of the Cabinet of Ministers of Ukraine dated November 8, 2017, in particular, measures to ensure the functioning of the information system for providing electronic reporting by business entities that conduct activities in the field of waste management with waste [5].

Digitization measures are regulated in more detail in the State Forest Management Strategy of Ukraine until 2035, approved by the decree of the Cabinet of Ministers of Ukraine dated December 29, 2021. Among such measures are defined: ensuring transparency of forestry activities in the part of open electronic sale of wood; organization and support of the electronic information system in the field of forestry, which will focus on information about all forest users, in particular, on the monitoring of internal wood consumption, summarized data of electronic wood accounting, the register of logging tickets, the register of permanent forest users, the register of certificates of origin of wood, electronic auctions from the sale of wood, etc.; monitoring the activities of forest users of all forms of ownership by analyzing data on an electronic portal in the field of forestry [6].

The Water Strategy of Ukraine for the period until 2050, approved by the decree of the Cabinet of Ministers of Ukraine dated December 9, 2022 [7], does not provide for any measures to digitize the water use industry, although in practice the relevant electronic registers function and the possibility of obtaining permits for water use using an online service is provided (it was before martial law). At the same time, the Water Code of Ukraine provides for the possibility of submitting an application by a legal entity, an individual, or an individual entrepreneur to obtain (reissue, obtain a dupli-

cate, cancel) a permit for special water use and relevant documents in both paper and electronic form (Article 49) [8].

Digitization measures in the field of subsoil use are defined by the Subsoil Code of Ukraine. Thus, the operation of a single state electronic geo-information system for the use of subsoil and its components is envisaged, which includes: the State Fund of Subsoil of Ukraine, the state register of special permits for the use of subsoil, the state register of oil and gas wells, the state register of artesian wells, the state water cadastre (section "Underground waters"), the state geological web portal, the electronic cabinet of the unified state electronic geoinformation system of subsoil use and the electronic cabinet of the subsoil user, etc. (Article 5-1) [9]. The submission of documents for obtaining a permit for special subsoil use is provided through the electronic cabinet of the subsoil user in accordance with the Regulation on the electronic cabinet of the subsoil user, approved by the Order of the Ministry of Environment Protection and Natural Resources of Ukraine on March 28, 2023 [10].

The importance and timeliness of these measures is also mentioned in the project of the Recovery Plan of Ukraine in the section "Reconstruction of a clean and protected environment", where one of the main tasks that must be carried out to overcome the inefficiency of state management in the field of environmental protection and nature management is defined as the digitization of the nature protection industry [11].

To study the impact of digitalization on business entities that are nature users, it is appropriate to note the important role of the electronic platform "EkoSystem" – a state-wide ecological automated information and analytical system administered by the Ministry of Environmental Protection and Natural Resources of Ukraine and aimed at ensuring access to environmental information. The main tasks and functioning of EcoSystem are defined in the Regulation on the Unified Ecological Platform "EkoSystem", approved by the resolution of the Cabinet of Ministers of Ukraine dated October 11, 2021 [12].

This is a convenient service with digital services for business, as well as official information from open environmental registers. Currently, 21 online services out of 29 existing in the environmental sector are available for business. Over 120,000 permit documents were issued by business entities during the service's operation. The most popular electronic services were: 1) waste declaration (over 58,000 submitted); 2) issuing a logging ticket (over 27,000); 3) certificate of origin of timber and lumber made from it (almost 14.5 thousand) [13]. Work on digitalization of services in this area continues.

The user receives access to EcoSystem services through an electronic account. Login to the system is done using the authorization service, id.gov.ua. In the electronic cabinet, enterprises can conveniently receive services, submit reports, and receive answers to sent requests [14]. This allows entrepreneurs to minimize the time to receive the service, as well as corruption risks.

Among the most popular digital services for business entities provided through EcoSystem, the following can be distinguished [15]. Services in the field of waste management that business entities receive include: obtaining / reissuance / suspension of validity / restoration of validity / narrowing of validity / cancellation of a license for conducting economic activities for the management of hazardous waste; submission of an application for verification of the compliance of the material and technical base of the license applicant; submission of a waste declaration (for entities of economic activity – generators or owners of waste); obtaining an opinion on cross-border transportation of waste included in the Green list of waste (according to the Basel Convention); permission to carry out waste processing operations; waste transfer service; electronic reporting form of waste accounting.

In the forestry sector, business entities can receive the following online services: issuance of a special permit for the special use of forest resources – logging ticket; certificate of origin of timber and lumber made from it (is a mandatory document for export).

In the field of atmospheric air protection, it is possible to obtain the following online services: state registration of the installation in the Unified register for monitoring, reporting and verification of greenhouse gas emissions; state registration of the facility in the National Register of Emissions and Transfer of Pollutants; state registration of objects that have or may have a harmful effect on human health and the state of atmospheric air, types and volumes of pollutants emitted into the atmosphere (removal from state registration, adjustment of types and volumes of emissions).

Through the electronic cabinet of the subsoil user, services are provided for the registration of a special permit for the use of subsoil.

Given that it is prohibited by law to start the implementation of a planned activity without obtaining a conclusion on the assessment of the impact on the environment and obtaining a decision on the implementation of the planned activity, it is important for business entities to be able to obtain such a conclusion using the Ecosystem electronic platform.

Therefore, the conducted analysis gives reasons to claim that digitalization is an effective tool for interaction between the state and business, including in the field of environmental relations. It ensures transparency, availability of services and data, which are generated and summarized with the help of electronic resources, the possibility of quick response to changes and the adoption of reasoned decisions by relevant authorities, minimization of the corruption component. This contributes to the creation of a more balanced and sustainable economy, where businesses can cooperate with government agencies to achieve common goals in the field of environmental protection.

The analysis of the legislation gives reason to conclude that there is no single terminology "digitalization" when defining the relevant information and communication activities that are carried out through Internet resources. At the same time, the relevant digitization measures are not systematically regulated. Digitization of environmental relations should be determined as a priority direction

of the state environmental policy. It is at the level of the law (strategy) that priority areas in the field of environmental protection, nature management, and environmental safety that will be subject to digitalization should be determined. In addition, digitalization should be included in the principles of environmental protection (according to Article 3 of the Law of Ukraine "On Environmental Protection").

References:

1. Malysheva N.R., Vinnyk O.M. Ecology, economy, digitalization: legal problems of interaction. Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy. 2022. Tom 29. № 2. S. 238-360.
2. Ilkiv N.V. State and prospects of legal regulation of digitalization of public participation in environmental protection. Analitychno-porivnialne pravoznavstvo. 2024. № 1. S. 328-333.
3. On environmental protection: Zakon Ukrainy vid 25.06.1991r. № 1264-XII. Veb-sait Verkhovnoi Rady Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/1264-12#Text (accessed: 05/05/2024).
4. About the main principles (strategy) of the state environmental policy of Ukraine until 2030: Zakon Ukrainy vid 28.02.2019 r. № 2697-VIII. URL: https://zakon.rada.gov.ua/laws/show/2697-19#Text (accessed: 05/05/2024).
5. National waste management strategy in Ukraine until 2030: rozporiadzhennia Kabinetu Ministriv Ukrainy vid 08.11.2017 r. № 820-r. URL:https://zakon.rada.gov.ua/laws/show/820-2017-%D1%80?find=1&text=%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD#w1_16 (accessed: 05/05/2024).
6. State strategy of forest management of Ukraine until 2035: rozporiadzhennia Kabinetu Ministriv Ukrainy vid 29.12.2021 r. № 1777-r. URL: https://zakon.rada.gov.ua/laws/show/1777-2021-%D1%80#Text. (accessed: 05/05/2024).
7. Water strategy of Ukraine for the period until 2050: rozporiadzhennia Kabinetu Ministriv Ukrainy vid 9.12.2022 r. № 1134-r. URL: https://zakon.rada.gov.ua/laws/show/1134-2022-%D1%80#Text. (accessed: 05/05/2024).

8. Water Code of Ukraine: Zakon Ukrainy vid 06.06.1995 r. URL: https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80#Text. (accessed: 05/05/2024).

9. Subsoil Code of Ukraine: Zakon Ukrainy vid 27.07.1994 r. URL: https://zakon.rada.gov.ua/laws/show/132/94-%D0%B2%D1%80#Text. (accessed: 05/05/2024).

10. Regulations on the electronic cabinet of the subsurface user: nakaz Ministerstva zakhystu dovkillia ta pryrodnykh resursiv Ukrainy 28.03.2023 r. № 177. URL: https://zakon.rada.gov.ua/laws/show/z0709-23#Text. (accessed: 05/05/2024).

11. Project of the Recovery Plan of Ukraine: Materials of the Working Group "Environmental Safety". The National Council for the Recovery of Ukraine from the Consequences of the War. URL:https://uploads-ssl.webflow.com/625d81ec8313622a52e2f031/62dea19b8b3d4e2f5b65c8ce_%D0%95%D0%BA%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%B7%D0%B1%D1%96%D1%80%D0%BA%D0%B0_%D1%83%D0%BA%D1%80.pdf. (accessed: 05/05/2024).

12. Regulations on the Unified Environmental Platform "Eco System": postanova Kabinetu Ministriv Ukrainy vid 11.10.2021 r. № 1065. URL: https://zakon.rada.gov.ua/laws/show/1065-2021-%D0%BF#Text. (accessed: 05/05/2024).

13. Business services and up-to-date information on the state of the environment. Government portal. URL: https://www.kmu.gov.ua/news/posluhy-dlia-biznesu-ta-aktualna-informatsiia-pro-stan-dovkillia-onlain-servisamy-mindovkillia-vzhe-skorystalosia-ponad-13-mln-korystuvachiv. (accessed: 05/05/2024).

14. Ecosystem: The only online platform in the field of environmental protection. URL: https://kitsoft.ua/ua/projects/ekosistema. (accessed: 05/05/2024).

15. National online platform "Ecosystem". URL: https://eco.gov.ua/. (accessed: 05/05/2024).

WHAT DOES CRIMINAL LAW PROTECT: THE ECONOMY OR BUSINESS ACTIVITIES?

Myslyvyy V.

Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Doctor of Law, Professor.

The development of social relations in Ukraine, associated with radical transformations in the conditions of building a market economy, the establishment of economic and entrepreneurial activities, the strengthening of financial, banking, and other spheres of the state's functioning, necessitates the important role of legal means in this process. These means serve not only as regulators of the mentioned social relations but also as tools for preventing criminal offenses. In this context, the sharpest weapon against subjects of criminal offenses in the economic sphere is criminal liability and other measures of criminal-legal influence.

One of the main groups of criminal-legal norms that provide for responsibility for encroachments in the economic relations sphere is concentrated in Chapter VII "Criminal Offenses in the Sphere of Economic Activity" of the Special Part of the Criminal Code of Ukraine (hereinafter – the CC of Ukraine). The norms of this chapter were created in the context of the draft CC of Ukraine from 1993 to 2001, with the developers considering elements of continuity, as these actions traditionally bore the name "Economic Crimes" in all criminal codes of Ukraine (1922, 1927, 1960).

However, changes occurring in social relations could not but affect the content of the current CC of Ukraine for several reasons. Thus, the legislator adjusted several articles taking into account the acquired experience or the requirements of the time, while others

became the product of subjective influence and fluctuations in the processes of criminalization and decriminalization of actions in the business sphere. In particular, 20 articles were excluded from the mentioned chapter, which related to: the procedure for engaging in economic activity, currency regulation, actions in the sphere of trade services and measuring instruments, and others. At the same time, actions related to counterfeit products, gambling business, raiding, bankruptcy, insider information, etc., were criminalized. These changes were prompted not only by transformations in business relations but also by the shortcomings of the criminal-legal doctrine, and at times – unmotivated actions and legal ignorance.

It is no coincidence that criminals who commit economic crimes are openly "surprised" by the high risks of severe punishment faced by their "colleagues" who commit common criminal offenses such as robbery, extortion, and assault, claiming that criminal business activities are not only "safer" but also significantly more "profitable." There might be some criminal logic to this, as property crimes in Ukraine annually account for about 60% of total crime, while criminal offenses in the economic sphere barely reach 2%.

The development of economic social relations in certain areas has shown not only the necessity of reinstating some criminal-law prohibitions but also expanding their scope to prevent criminal encroachments on the country's economy. For instance, Ukraine's choice of a European development vector has led to a certain openness of state borders for freer movement of goods, which in turn led to the decriminalization of so-called "commodity smuggling." The subjects of Article 201 of the Criminal Code of Ukraine were limited by the legislator to the illegal movement of cultural values and certain other dangerous and prohibited items and substances. However, these changes in the composition of criminal offenses led to a sharp increase in illegal smuggling of excisable and other goods, as only administrative liability was provided for such offenses, which could not be an effective means of influencing offenders. Consequently, under martial law conditions, the legislator not only reinstated the

prohibition on smuggling goods in the newly created Article 201-3 of the Criminal Code of Ukraine but also had to criminalize the smuggling of excisable goods in Article 201-4 of the Criminal Code of Ukraine. This example clearly demonstrates that the norms of this chapter should be directly aimed at protecting economic relations.

In this context, it should be noted that one of the key provisions of the science of criminal law regarding the system of criminal legislation and its structure, particularly the Special Part, is the doctrine of the object of a criminal offense. Based on the title of the section "Criminal Offenses in the Sphere of Economic Activity" in the current Criminal Code of Ukraine, which is the subject of our consideration, the generic object of these actions is social relations in the sphere of economic activity, which, in our opinion, does not always accurately reflect its content. The reason for this phenomenon may be the insufficient legal definition of the essence of social relations protected by criminal law.

In our opinion, a key point to consider is the essence of the relationship between such social phenomena as "economy" and "economic activity." Given that all the most important social relations are declared in the Constitution of Ukraine, it should be noted that Part 4 of Article 13 proclaims: "The state ensures the protection of the rights of all subjects of ownership and economic activity, the social orientation of the economy" (our emphasis – V.M.). In subsequent constitutional norms, terminology related to the terms "economy" and "economic" is used quite frequently (statistically – 25 instances). As for the term "economic activity," apart from the above-mentioned Article 13, the legislator uses it only twice in Article 137 in such formulations as "agriculture" and "housing economy."

Thus, the above shows that constitutional provisions in the system of social relations give priority to the concept of "economy" rather than "economic activity" and realistically orient society towards the understanding that economic relations are fundamental to its existence. In our conviction, this conclusion is because the economy has always been and remains the basis of any mode of material

production. The thesis that the economy is a set of production relations that constitute the economic structure of society, its real basis, has not yet been refuted by anyone. It should also be agreed that the obvious advantage of this approach is that economic activity in its structure includes both the production and non-production spheres, and thus is a broader concept than economic activity.

Of course, such a conclusion in no way diminishes the importance of economic, entrepreneurial, financial, banking, privatization activities, taxation, customs, and other spheres. However, all of these can be protected within the framework of the generic object, which is social relations in the economy.

In this regard, the new approach to resolving this issue in the draft of the new Criminal Code of Ukraine should be supported. The proposed Book Six "Criminal Offenses Against the Economy" encompasses such components as: Chapter 6.1 "Criminal Offenses Against Property," Chapter 6.2 "Criminal Offenses Against Intellectual Property," Chapter 6.3 "Criminal Offenses Against Finances," Chapter 6.4 "Criminal Offenses Against the Order of Economic Activity," Chapter 6.5 "Criminal Offenses Against the Order of Use of Natural Resources" . Thus, social relations in the sphere of the economy take their rightful place among the objects protected by the law on criminal liability. Of course, the presented structure of criminal offenses against the economy is not the final version of the future component of the Special Part of the criminal code, as its provisions can be debated, changed, and supplemented. Nevertheless, its model serves as an important guide for continuing legislative work in this direction.

It appears that the proposed legislative innovation finally resolves both the issue of legislative implementation of the scientific concept of the classification of objects of criminal offenses "vertically" (general, generic, specific, direct), and acknowledges that the criminal-legal protection of the economic sphere should be carried out on the principles of a modern, scientifically justified, criminal-legal doctrine, which will serve more effective protection of economic relations in Ukraine.

At the same time, considering that the process of creating a new Criminal Code of Ukraine is taking place in the context of the development of modern digital technologies directly related to the economy, it is deemed necessary to draw attention to the provisions of the Law of Ukraine "On Public Electronic Registers" dated November 18, 2021 , which establishes the legal, organizational, and financial principles for the creation and functioning of public electronic registers to protect the rights and interests of individuals and legal entities during the creation, storage, processing, and use of information in public electronic registers. The practice of functioning of these and other registers shows that their resources contribute to determining the objective situation in certain sectors and the economy, ensuring transparency, control, and efficiency of economic and business relations in Ukraine, and thus should timely influence their condition and development.

At the same time, as demonstrated by jurisprudence, relevant registries play a crucial role in detecting, disclosing, and preventing criminal offenses in the economic sphere. An illustrative example in this regard is the application of Article 205-1 of the Criminal Code of Ukraine, which provides for criminal liability for forgery of documents submitted for state registration of legal entities and individual entrepreneurs, as this provision serves as a tool for preventing such a dangerous phenomenon as raiding. Considering the rapid development of modern digital technologies in society, as well as the proliferation of challenges associated with criminal encroachments on them, it would be appropriate in future criminal legislation to provide for criminal liability for unlawful encroachments on information and cyber security, including illegal interference with the functioning of the public registers.

References:

1. On Amendments to the Criminal and Criminal Procedure Codes of Ukraine Regarding the Criminalization of Smuggling of Goods: Law

of Ukraine dated December 9, 2023, No. 3513-IX. Verkhovna Rada of Ukraine Information. 2024. No. 1. Article 4.

2. Text of the Draft of New Criminal Code of Ukraine. URL: https://newcriminalcode.org.ua/upload/ media/2024/02/26/kontrolnyj-tekst-proyektu-kk-25-02-2024.pdf (accessed: 05/02/2024).

3. "On Public Electronic Registers": Law of Ukraine dated November 18, 2021, No. 1907-IX. Verkhovna Rada of Ukraine Information. 2023. No. 11. Article 27. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text (accessed: 05/02/2024).

LEGAL BASIS FOR THE FUNCTIONING OF THE STATE AGRARIAN REGISTER

Pavliuchenko Y.

Acting head of the department of economic and administrative law Vasyl' Stus Donetsk National University, Doctor of Law, Professor

Digitalisation has covered almost all spheres of public life, the economy, and relations between government agencies and business entities. Public electronic registers can be considered a significant product of digitalisation, one of which is the State Agrarian Register (SAR). Practice shows that although this Register contains information about more than 95,000 agricultural producers, not everyone knows about the purpose and capabilities of this register, and therefore is in no hurry to join it.

The formation of the legal framework for the functioning of the State Agency for Agricultural Research began in 2020 with amendments to the Law of Ukraine 'On State Support of Agriculture in Ukraine' (the Law). Later, the Laws of Ukraine 'On the National Informatisation Programme', 'On Public Electronic Registers' and others were adopted, which create a general legal framework for the functioning of public electronic registers. At present, the issues of correlation between general and special legislation, which should ensure

the efficiency of the functioning of the SAR, need to be analysed.

In legal science, the issue of digitalisation in the economic sphere has been actively developed by O. Vinnyk, L. Mashkovska, O. Shapovalova and some others, but the legal basis for the functioning of the SAR requires additional analysis. Accordingly, the chosen topic is relevant and is devoted to specifying the legal framework for the functioning of the SVA.

The legal definition of digitalisation as the process of introducing digital technologies into all spheres of public life (Article 2 of the Law of Ukraine 'On Public Electronic Registers') allows us to state that the introduction of such technologies enables a business entity to operate remotely, store and process significant amounts of data, receive certain administrative services, have unlimited access to information for all or a certain number of users, and makes interaction between business entities and public authorities or local self-government bodies Today, public electronic registers have become a way to accumulate and exchange certain information about business entities.

Some researchers highly appreciate the importance of these registers, noting that they play the role of universal legal mechanisms designed to ensure order in a particular area by accumulating and using the information necessary for its functioning. The use of digital technologies to ensure the functioning of public electronic registers confirms that these registers are an important component of digitalisation [1, p. 138].

According to Art. 6 of the Law of Ukraine 'On Public Electronic Registers', the system of registers of the State Aid does not belong to the basic registers, which are all named, but to other registers. By the way, digital registers of support for farmers have been introduced in such countries as: Ireland, Estonia, Spain, Italy, the Netherlands and other EU countries [2].

The State Agrarian Register is defined as a state automated information system for collecting, recording, storing, processing and providing information on agricultural producers and their agricultural activities (Article 2 of the Law).

In addition to the provisions of the Law of Ukraine 'On State Support of Agriculture of Ukraine', the functioning of the State Agrarian Register is ensured by the Procedure for Maintaining and Administering the State Agrarian Register, the List of Information of the State Agrarian Register, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 573 of 2 June 2021.

The legislator has defined the purpose of the SAR as a comprehensive integration of information on agricultural producers, their property, land, environmental, labour, financial and credit and other rights and characteristics (part 1 of Article 2-2 of the Law). At the same time, the provisions of Articles 2-2 and other of the Law allow us to state that the main purpose of the SAR is to collect information on agricultural producers applying for various types of state support. In particular, this follows from the list of rights of agricultural producers (Art. 2-2 of the Law), as well as from the information officially published about the SAR. In particular, it is stated that the SAR was created by the Ministry of Agrarian Policy and Food of Ukraine with the aim of efficient and transparent attraction and distribution of all types of support for Ukrainian farmers, both at the expense of the state budget and in the form of soft loans, international grants or technical assistance [2].

The second important purpose of the SAR is to obtain permits for agricultural producers.

The SAR is maintained at the expense of the state budget, is state property and, as part of the National Archival Fund, is subject to lifelong storage. The implementation of the SAR is supported by the European Union and the World Bank.

Based on the analysis of the provisions of Articles 2-2 of the Law, the legal basis for the functioning of the SAR can be summarised. They include, in particular: 1) voluntary principles of keeping (agricultural producers voluntarily enter reliable information about themselves); 2) electronic information interaction with other state registers and cadastres containing information about agricultural producers; 3) ensuring electronic interaction between individuals and legal entities, state bodies, local self-government bodies, admin-

istrative service centres for the purpose of implementing the state agricultural policy, including providing state support to agricultural producers, 4) providing agricultural producers with access to a personal electronic account and management of their profile; 5) granting agricultural producers who have registered with the SAR certain rights to receive state support, free access to information about themselves and its use for obtaining permits, etc.

Attention should be paid to the compliance of provisions of general and special legislation on public electronic registers. For example, in terms of free and accessible registration data as one of the principles of activity in the field of public electronic registers (Article 3 of the Law of Ukraine 'On Public Electronic Registers').

According to the SAR application, it is already connected to the Unified State Register of Legal Entities and Individual Entrepreneurs, the State Land Cadastre, the State Register of Property Rights, and the Unified State Register of Animals [2]. It is important to note here the principles of operation of the SAR, in particular the principle of openness and accessibility of SAR data, the legality of their receipt, dissemination and storage, and the principle of no duplication of data from other registers, cadastres and information systems.

Along with the positive factors of the SAR functioning, it should be agreed that one of the main threats to the functioning of all public electronic registers is the growth of cybercrime, the lack of secure exchange of identification data of individuals and legal entities processed in the information systems of public authorities and the private sector [3, p. 117]. However, it is declared that the data of the electronic cabinet of the agricultural producer in the SAR will be available only to the Ministry of Agrarian Policy and Food of Ukraine, as well as to third parties to whom the producer has personally granted access to the data [2]. However, overcoming cybercrime is not possible only by means of legal action, but requires the use of a wide range of other remedies.

Thus, the SAR contributes to more efficient management and use of agricultural resources, ensures transparency, legal security and support for agricultural development.

To summarise, the SAR is one of the public electronic registers, and its functioning helps agricultural producers to solve two tasks: obtaining state support and obtaining permits, and the Ministry of Agrarian Policy and Food of Ukraine to accumulate and use information on property, land, environmental, labour, financial and credit and other rights and characteristics of agricultural producers.

References:

1. Vinnyk O.M., Shapovalova O.V. (2023). Pravove zabezpechennya sfery publichnykh elektronnykh reyestriv. Aktual′ni problemy prava: teoriyai praktyka. 1 (45). 137-149. DOI: https://doi.org/10.33216/2218-5461/2023-45-1-137-149. (accessed: 05/02/2024).
2. About the state agrarian register: website: URL: https://www.dar.gov.ua/. (accessed: 05/02/2024).
3. Petrenko N.O., Mashkovs′ka L.V. (2020). Tsyfrovizatsiya derzhavnykh administratyvnykh posluh v Ukrayini: normatyvno-pravovi aspekty. Pravo i suspil′stvo. 2. 112-119. DOI: https://doi.org/10.32842/2078-3736/2020.2-1.18 .

CONCERNING THE FEATURES OF PERSONAL INCOME TAXATION OF ENGAGED SPECIALISTS BY THE DIIA.CITY RESIDENTS

Petrenko G.

Associate Professor of the Department of Commercial and Administrative Law of Vasyl' Stus Donetsk National University, PhD in Economics, Associate Professor

Pomazanov M.

attorney-at-law, lawyer at Axon Partners Attorneys Association

At the beginning of the development of digital technologies, the level of service provision in the modern state inevitably has to undergo a stage of digital transformation, which involves the gradual reformation of all state services into convenient online services. In particular, the IT sector requires special conditions for future development, including improved approaches to the administration of taxes and fees in this industry. Therefore, studying the peculiarities of the Diia.City legal framework establishment and its taxation features is highly relevant today.

The issue of taxation of IT companies' activities has been studied by domestic scientists such as A.O. Tymoshenko, Y.V. Tyshchenko, O.M. Vinnyk, S.M. Veretyuk, and others. For instance, Y.V. Tyshchenko examined the legal regime of 'Diia City' as a factor in attracting investments [1, p. 31], while A.O. Tymoshenko's publications are dedicated to the study of fiscal policy peculiarities in the taxation of IT services [2, p. 47].

Today, the establishment of one of the best environments in the region for the development of IT products and the launching of startups is defined by the Government in the National Economic Strategy for the period up to 2030 (hereinafter referred to as 'the Strategy')

as one of the strategic objectives for the country's development. Furthermore, the Strategy identifies several challenges and impediments to achieving these goals, such as the low share of production of complete IT products in the industry, the absence of a simplified taxation regime for the IT sector (IP box), malpractice and unlawful interference by law enforcement and regulatory officials in the business of IT companies, as well as an uncertain tax policy and regulatory environment. To achieve these committed goals, amendments to the Tax Code of Ukraine were initiated to establish a virtual legal framework for the optimization of taxation and the reduction of shadow activity in the IT industry. In connection with these commitments, the Law of Ukraine 'On Stimulating the Development of the Digital Economy in Ukraine' (hereinafter referred to as 'the Law') was enacted [3]. The Law aims to guarantee the stability and consistency of tax rates and to prevent any deterioration of taxation conditions [4, p.73, 77]. The Law determines the organizational, legal, and financial grounds for the functioning of the legal framework Diia.City, which aims to stimulate the development of the digital economy in Ukraine by creating supportive conditions for innovative business activity, building digital infrastructure, attracting investments, and bringing in talented specialists. Additionally, the Law guarantees the preservation of the Diia.City legal regime and its stability, as stipulated by the Law and other laws of Ukraine. It specifies corporate income taxation, personal income taxation peculiarities and payment peculiarities of single contribution for Diia.City residents within a defined period, including the prohibition of limiting or narrowing the scope of rights and guarantees provided by the Diia.City legal regime, as well as the inadmissibility of increasing the regulatory burden on Diia.City residents during for an unlimited period, but not less than 25 years from the date of entry of the first Diia.City resident in the Diia.City register.

Moving forward with the development of the Strategy, numerous amendments were introduced by the enacted Law of Ukraine 'On Amendments to the Tax Code of Ukraine and Other Laws

of Ukraine on Stimulating the Development of the Digital Economy in Ukraine', resulting in the implementation of some of the Strategy's objectives, including the introduction of the Diia.City virtual tax environment [5].

Thus, a resident of Diia.City can be an IT company registered in Ukraine that offers its engaged employees and gig-specialists, whose average number must be at least 9, an average monthly remuneration of at least the equivalent of EUR 1,200. The amount of qualified income of the IT company must be at least 90% of the amount of its total income from the following business activities: computer programming (development, modification, testing, and technical support of software), development of online platforms and cloud services, activities in the field of IT education, organization of eSports competitions, ensuring cybersecurity of information and communication systems, digital marketing, creation and maintenance of large databases, conducting transactions related to the circulation of virtual assets, development of artificial intelligence, development in the field of international payment systems, hosting, cloud data centers, and other activities stipulated in part 4 of Article 5 of the Law. Currently, 985 companies registered in Ukraine have become residents of Diia.City, including EPAM, SoftServe, GlobalLogic, Luxoft, Ciklum, and others [6].

Worth mentioning, that the reduction of shadow activity in the IT industry is deemed one of the reasons for the establishment of the virtual tax environment Diia.City, aimed to offer an alternative model of cooperation with highly qualified specialists taking into account that IT business within its client's delivery structure is actively engages and utilize individual entrepreneurs (hereinafter referred to as the 'IE'). Such IEs are widely use simplified taxation system which lead tax evasion and disguising labour relationships. For instance, an IE single tax payer of Group III pays 5% of any income and a minimum unified social contribution of 22%, while an employee under an employment contract has a tax burden of 41.5%. This discrepancy leads to misuse of the simplified taxation system,

a formal increase in unemployment, and ultimately, the shadowing of the economy as a whole.

The provisions of Article 43 of the Constitution of Ukraine stipulate that everyone has the right to labour, including the possibility to earn a living by labour that he or she freely chooses or to which he or she freely agrees. The State creates conditions for citizens to fully realize their right to labour, guarantees equal opportunities in the choice of profession and types of labour activity, and implements programs of vocational education, training, and retraining of personnel according to societal needs. Analyzing this constitutional guarantee in the context of the Law, it is possible to conclude that the provisions of the Law expand abilities and create conditions for citizens to fully realize their right to labour in the digital environment. This is one of the primary aims for the establishment of the virtual taxation legal regime Diia.City, within which the state offers multiple ways to realize the right to labour [7, c.88].

Therefore, the Law stipulates that a Diia.City resident has the right to engage any specialists on the basis of employment agreements (contracts), specialists such as gig-specialists on the basis of gig-contracts, and individual entrepreneurs on the basis of other civil law or commercial law contracts.

According to the Law, a resident of Diia.City is deemed to be the tax agent of a taxpayer, specifically a gig-specialist of a resident of Diia.City, when accruing (paying) income in his favor. This income may be in the form of salary, other incentive and compensation payments, or other payments and remuneration accrued (paid, provided) to the taxpayer in connection with employment relations or in connection with the execution of a gig-contract. Besides, a resident of Diia.City is obliged to accrue and pay a single contribution to the compulsory state social insurance for a gig-specialist in the amount of the minimum insurance contribution, which is 22% of the minimum wage [8]. At the same time, the income of gig-specialists in the form of remuneration under a gig-contract is taxed at a special personal income tax rate of 5%, provided that the amount of such

income for the year does not exceed the equivalent of EUR 240,000 (applied to the total income under all gig-contracts, i.e., the total annual taxable income), as well as 1.5% of the military fee. The taxpayer (gig-specialist) pays additional tax at the rate of 18% on the excess amount and submits an annual tax return [9].

In summary, it can be concluded that the establishment of the Diia.City tax regime has achieved another goal aimed at unshadowing the IT industry, namely the legislative consolidation of gig-contracts, which combine labour and civil law relations with a flexible approach to personal income taxation of gig-specialists. Such changes will help create positive incentives for the development of the digital economy in the country, facilitate the transition of IT companies to the virtual tax environment of Diia.City, and become a key driver of further growth of the Ukrainian economy in the future.

References:

1. Tyshchenko Y.V. Legal Regime Of "Action City" As A Factor for Attracting Investments. Foreign trade: economics, finance, law. 2022. № 1. C. 29-37. URL: http://journals.knute.edu.ua/foreigntrade/article/download/15/874.
2. Tymoshenko A.O. It Services Taxation: Challenges And Prospects. Economy and State. 2018. № 4. P.46-52 URL: http://www.economy.in.ua/?op=1&z=4029&i=9 (accessed 04/15/2024).
3. On Stimulating the Development of The Digital Economy in Ukraine: Law of Ukraine of 15 July 2021 No. 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (accessed 04/15/2024).
4. On Approval of The National Economic Strategy for the Period Up To 2030: Resolution of the Cabinet of Ministers of Ukraine; Strategy of 03 March 2021, No. 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text (accessed 04/15/2024).
5. On Amendments to the Tax Code of Ukraine and Other Laws of Ukraine to Stimulate the Development of the Digital Economy in Ukraine: Law of Ukraine of 14 December 2021 No. 1946-IX. URL: https://zakon.rada.gov.ua/laws/show/1946-20#Text (accessed 04/15/2024).

6. Diia.City register. URL: https://city.diia.gov.ua/registry/resident (accessed 04/15/2024).

7. Sayenko Y.O. Ways to Exercise the Right to Work in The Legal Regime of Diia City. Collection of scientific works of H. S. Skovoroda Kharkiv National Pedagogical University "PRAVO". Issue 37, 2023. C.86-93. https://doi.org/10.34142/23121661.2023.37.11.

8. On the Collection and Accounting of the Single Contribution for Compulsory State Social Insurance: Law of Ukraine of 08 July 2010 No. 2464-VI. URL: https://zakon.rada.gov.ua/laws/show/2464-17#n169 (accessed 04/15/2024).

9. Tax Code of Ukraine: Law of Ukraine of 2 December 2010, No. 2755-VI. Bulletin of the Verkhovna Rada of Ukraine. 2011. № 13-14. Art. 556 URL: https://zakon.rada.gov.ua/laws/show/2755-17 (accessed 04/15/2024).

FREE MOVEMENT OF CAPITAL IN EU: LEGAL ASPECTS

Podolyak S.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Candidate of Legal Science, Associate Professor

After February 24, 2022, Ukrainian people and business were forced to live and work in new reality. Lots must find how to integrate quickly in the EU society and its internal market. And one of the forms of such integration is movement of capital in the digital age. But nevertheless, it is stated that in the EU there is a free movement of capital, it has rules. So the freedom is not absolute.

The freedom of capital movement is one of the four fundamental freedoms alongside free movement of goods, persons, and services. It assists in operation of the EU internal market.

The development of this freedom was not fast. It is directly connected with long-lasting release of capital markets and reluctance of states to deeper liberalization in this area. Free movement of capital relates to cross-border transfers of financial assets, investing in shares and in immovable property, in the financial participation of foreigners in domestic enterprises etc. The actual opening of the markets for the investors has a significant connection with the area of state economic policy and taxation.

I'd like to indicate that free movement of capital is one freedom with two subcategories. First one is connected with capital movement, the second one – with payment movement. Both freedoms have parallel legal regime within the European Union. But each Member State of the European Union may have its own legal rules for the free movement of capital and payments between them and third countries. This characteristic this freedom was upheld also by the European Court of Justice in decision 203/80 Casati when Court pointed out that the free movement of capital, in addition to the free movement of goods, persons and services, forms the fundamental freedom within the Community [1].

The European Court of Justice in the Case 286/82 and Case 26/83 [2] indicated that movement of capital is financial transactions that are significantly related to the investment of the relevant funds. In the Case 7/78 [3] the European Court of Justice stated that movement of capital takes place when financial resources located in a country are used to finance another country, and the investment is not transferred back to the country of original location of financial resources within a reasonable time. Also the notion of movement of capital was considered by European Court of Justice in many other cases. e.g. Case 171/08 [4]; Case 483/99 [5] etc.

The "Capital and Payments" chapter of the Title IV: Free Movement of Persons, Service and Capital of the Treaty on the Function-

ing of the European Union (TFEU) sets out the provisions regarding capital and payments [6]. It covers three main sub-areas [6]:

Capital movements and payments

Payment systems

Fight against money laundering.

In the field of capital movements and payments, capital is defined as financial operations aiming investment and gaining profit which are the following:

- direct investments,
- investments in real estate,
- operations in securities dealt in on the capital markets,
- operations in securities and other instruments dealt in on the money market,
- operations in current and deposit accounts with financial institutions,
- credits related to commercial transactions or to the provision of services in which resident is participating,
- financial loans and credits,
- sureties, other guarantees and rights of pledge,
- transfers in performance of insurance contracts,
- personal capital movements,
- physical import and export of financial assets,
- other capital movements.

In the Article 63 of the TFEU it is pointed out that all restrictions on the movement of capital between Member States and between Member States and third countries shall be prohibited. This prohibition works only when the restrictions are based on nationality [6].

Pursuant to Article 65 of the TFEU, the provisions of Article 63 shall be without prejudice to the right of Member States:

- to apply the relevant provisions of their tax law which distinguish between taxpayers who are not in the same situation with regard to their place of residence or with regard to the place where their capital is invested;

- to take all requisite measures to prevent infringements of national law and regulations, in particular in the field of taxation and the prudential supervision of financial institutions,
- to lay down procedures for the declaration of capital movements for purposes of administrative or statistical information
- to take measures which are justified on grounds of public policy or public security [6].

The exceptions on free movement of capital are generally implemented in the field of taxation, prudential control, prevention of money laundering, public policy priorities and sanctions that are defined in accordance with common foreign and security policy.

The origin of capital is the criterion in cases of discrimination.

Article 63 TFEU prohibits [6]: unequal treatment between domestic and foreign capital, other forms of restrictions on the free movement of capital, such as the authorization scheme; in the form of obstacles that may discourage from the exercise of free movement of capital; or in the form of measures that degrade movement of capital to just theoretical, illusory possibility.

The European Court of Justice, e.g. in Case 101/05 [7] and others, stated out that the prohibition of restrictions on free movement of capital has direct effect: Article 63 TFEU contains a clear and unconditional prohibition, which does not require further implementation and is therefore applicable in proceedings before national courts and in case of conflict with the national legislation it should take precedence.

As to the legal regulation of payment systems, the European Union adopted in 2015 a new directive on payment services (PSD 2 – Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC) to improve the existing rules and take new digital payment services into account [8] and Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July

2021 on cross-border payments in the Union (codification)) on charges for cross-border payments in euro [9].

As to the legal regulation of fight against money laundering, the European Union adopted Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC on anti-money laundering and combating terrorist financing [10].

But the European Commission did not stop on that and proceeded to further strengthen the EU's fight against money laundering and terrorist financing.

On 7 December 2022, EU Council (ECOFIN) agreed its position on an anti-money laundering (AML) regulation and a new directive (AMLD6) and the proposal for a recast of the transfer of funds regulation which will together form the new EU AML rulebook once adopted.

The creation of a new EU authority that will transform AML/CFT supervision in the EU and enhance cooperation among financial intelligence units (FIUs) is at the heart of the new legislative package. The package also includes arrangements for:

– accelerating access to bank account information,

– limiting the amount of cash withdrawals from banks with 10,000 euros (Member states will have the flexibility to impose a lower maximum limit if they wish),

– introducing a monitoring mechanism for transfers of crypto assets: entire crypto sector, obliging all crypto-asset service providers (CASPs) to conduct due diligence on their customers. This means that they will have to verify facts and information about their customers. In its position, the Council demands CASPs to apply customer due diligence measures when carrying out transactions amounting to €1000 or more, and adds measures to mitigate risks

in relation to transactions with self-hosted wallets. The Council also introduced specific enhanced due diligence measures for cross-border correspondent relationships for crypto-asset service providers,

– third-party financing intermediaries, persons trading in precious metals, precious stones and cultural goods, will also be subject to the obligations of the regulation, as will jewellers, horologists and goldsmiths,

– third countries that are listed by the Financial Action Task Force (FATF) will also be listed by the EU "black list" and a "grey list", reflecting the FATF listings,

– the Council clarifies that beneficial ownership is based on two components – ownership and control – which need to be analysed in order to assess how control is exercised over a legal entity, and to identify all natural persons who are the beneficial owners of that legal entity. Related rules applicable to multi-layered ownership and control structures are also clarified. The Council also spells out further how to identify and verify the identity of beneficial owners across types of entities, including non-EU entities. Data protection and record retention provisions are also clarified. This is expected to make the work of the competent authorities easier and faster [11].

So, as we can see in the EU the legal regulation of movement of capital is developing due to the digital era. And Ukraine must be ready also to implement such regulation in its legislation.

References:

1. European Court of Justice. Judgment of the Court of 11 November 1981. Criminal proceedings against Guerrino Casati. URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-203/80 (accessed 05/02/2024).

2. European Court of Justice. Joined Cases 286/82 and 26/83. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:61982CJ0286&from=SV (accessed 05/02/2024).

3. European Court of Justice. Case 7/78. URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-7/78 (accessed 05/02/2024).

4. European Court of Justice. Case C-171/08 URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2010%3A412 (accessed 05/02/2024).

5. European Court of Justice. Case 483/99 URL: https://curia.europa.eu/juris/liste.jsf?num=C-483/99 (accessed: 02.05.2024).

6. Consolidated version of the Treaty on the Functioning of the European Union URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT (accessed 05/02/2024).

7. European Court of Justice. Case 101/05 URL: https://curia.europa.eu/juris/liste.jsf?num=C-101/05 (accessed 05/02/2024).

8. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC) URL:https://eur-lex.europa.eu/eli/dir/2015/2366/oj (accessed 05/02/2024).

9. Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union URL: https://eur-lex.europa.eu/eli/reg/2021/1230/oj (accessed 05/02/2024).

10. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC/ URL: https://eur-lex.europa.eu/eli/dir/2015/849/oj (accessed 05/02/2024).

11. Anti-money laundering: Council and Parliament strike deal on stricter rules URL: https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti- money-laundering-council-and-parliament-strike-deal-on-stricter-rules/ (accessed 05/02/2024).

DIGITALIZATION OF ENFORCEMENT PROCEEDINGS: LAW VS TECHNOLOGY

Popov K.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Candidate of Laws, Associate Professor

The digitization of human life in all its dimensions cannot be stopped. New versions of software, generative text models, which can easily solve problems previously accessible only to the human mind, appear almost every year. Against this background, the issue of competition between legal rules and software algorithms in the field of enforcement proceedings attracts special attention.

Repeated and frequent changes in the procedural legislation of Ukraine (Code of Commercial Procedure of Ukraine, 1991, pt. 4 art. 327; Civil Procedure Code of Ukraine, 2004, pt. 4 art. 431; Code of Administrative Proceedings of Ukraine, 2005, pt. 4 art. 373) lead to the conclusion that during 2020-2022, the legislator persistently experiments with the form of presentation of enforcement documents by courts (electronic or paper). Despite the noticeable desire of the legislator to "play" with the form of the enforcement document, hinting that the electronic form of the enforcement document is not its only form, nevertheless the law, which regulates procedural issues related to the execution of court decisions in commercial, civil and administrative cases, did not provide and does not provide (except for transitional provisions) other form of enforcement document than electronic. Other legislative provisions also provide only for the electronic form of the enforcement document.

Instead, in accordance with the current version of clause 19.1 of the Transitional Provisions of the Code of Commercial Proce-

dure of Ukraine (similar provisions are provided in the Civil Procedure Code of Ukraine and the Code of Administrative Proceedings of Ukraine), before the day the Unified State Register of Enforcement Documents (hereinafter – USRED) starts functioning, execution and issuance of enforcement documents shall be carried out by the court that adopted the relevant judgment, *in paper or electronic form* by using The Unified Judicial Information and Telecommunication System (hereinafter – UJITS) or its separate subsystem (module) that provides document exchange.

At the same time, the specified transitional provisions do not establish the rules (procedure) for issuing enforcement documents by courts before the day the USRED starts functioning, referring only to "*using* the UJITS or its separate subsystem (module) that provides document exchange".

At the end of June 2022, the State Judicial Administration of Ukraine (hereinafter – SJA of Ukraine) reported that, due to the lack of budget allocations, the software of the USRED had not been developed, and as a result, the impossibility of ensuring compliance with the requirements of the procedural codes of Ukraine ("Joint Order Issued by the State Judicial Administration of Ukraine and the Ministry of Justice of Ukraine," 2022).

Instead, already in September 2023, the SJA of Ukraine presented *the service of sending electronic enforcement documents* to the parties, as well as *the possibility of submission them for enforcement in electronic form* ("New service in the Electronic Court", 2023). As a result of the partial digitalization of enforcement proceedings, the legislation established the possibility of electronic information interaction of the subjects of enforcement proceedings using the Automated System of Enforcement Proceedings (hereinafter – ASEP).

Simultaneously, the requirements for a signature of an authorized person and a seal on enforcement document were excluded from the legislation, although such a decision of the legislator caused admonition and even discomposure of the Ministry of Justice of Ukraine (Horovets Y., 2024). However, this concern (as well as the corre-

sponding legislative changes) did not affect the practical activities of the bodies and persons who carry out enforcement of judgments.

The repeal of the provisions of the Law of Ukraine "On Enforcement Proceedings" about execution and issuance of enforcement documents (in particular, in paper form) is one of the consequences of the inconsistent state policy in the field of digitization of enforcement proceedings. Enforcement documents are not only documents issued by courts, but also enforcement inscriptions of notaries, certificates of commissions on labor disputes, resolutions of bodies (officials) authorized to consider cases of administrative offenses, decisions of other state bodies, which today are issued mainly in paper form. Therefore, the abolition of requirements for the details of enforcement documents in paper form creates uncertainty of the rules for issuance and submission such documents for enforcement.

Insufficient legal provision of real digitalization of enforcement proceedings complicates the formation of legal mechanisms to prevent abuse during submission documents for enforcement. Gaps in the rules for issuance of enforcement document actually make it impossible for the collector to submit an electronic document for enforcement in accordance with law, since the current legislation does not provide the issuance of the original enforcement document to the collector.

What is the practice of issuance and submission documents for enforcement today? In the conditions of the legislative uncertainty described above, the SJA of Ukraine issued a Clarification No. 15-12512/23 (2023, October 19) on the procedure for issuance and submission documents for enforcement in electronic form and information on the functioning of the service (hereinafter – Clarification).

Despite the fact that neither the law nor the Regulations on the SJA of Ukraine provide for the authority of the SJA of Ukraine to give instructions to the courts of Ukraine, and even more so, the participants of enforcement proceedings, instructions about the issuance (submission) of enforcement documents by them or on other issues, the Clarification was not recognized as illegal and was not canceled, but it also

became *the only document* that currently regulates the procedure for issuance and submission documents for enforcement.

The Clarification sets out the "*Procedure for functioning* of the service of issuance and submission documents for enforcement in electronic form", which provides that in order to send an electronic enforcement document to the electronic office of the collector and the debtor, the courts must follow the algorithm defined in the Clarification.

Particular attention is paid to the efforts of the SJA of Ukraine to establish in the Clarification the rules for correcting errors in enforcement documents, which oblige courts to recognize the enforcement document as unenforceable on grounds not provided for by procedural legislation, and to issue a new enforcement document in a manner not prescribed by law.

In Clarification the SJA of Ukraine establishes not only the procedure for issuing enforcement documents by courts in electronic form, which is not prescribed by law, but also the extralegal procedure, deadlines and even the duty of the collector to apply to the court for obtaining the enforcement document in paper form.

The results of the research lead to the following conclusions:

the current legislation of Ukraine does not contain provisions regarding the rules (procedure) for issuance enforcement documents by courts and submission them to enforcement during the transition period before the day the USRED starts functioning. At the same time, providing for the possibility of the courts to issue enforcement documents in paper form during the transitional period, the current procedural legislation does not establish the procedure or rules for their issuance. On the other hand, the procedure for issuance of enforcement documents by courts in electronic form is established only under the conditions of the USRED functioning;

fairly frequent and contradictory changes to the procedural legislation, which establishes the rules for the enforcement of court judgements, allow us to assert the inconsistency of the legislator regarding the requirements for the form and details of enforcement document;

the practice of applying the procedural legislation, which regulates the enforcement of court judgements, shows that courts, bodies and persons who carry out the enforcement of court judgements have ambiguous understanding of the meaning of the concepts enshrined in the law " enforcement document in electronic form" and "copy of enforcement document in electronic form ", coinciding them with each other;

in the conditions of legislative uncertainty with the rules for issuance and submission documents to enforcement before the start of the USRED functioning, such rules are formed on instructions from state bodies that are not authorized to legally regulate the processes of issuance and submission documents to enforcement, and even to issue such instructions. The legislative role in the relevant field of the process is also taken over by the algorithms of applied program interfaces and technical regulations of the UJITS and other information and telecommunication systems, which are not intended to regulate the relations between participants in the enforcement proceedings.

References:

1. Code of Commercial Procedure of Ukraine. (1991). The Official Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/1798-12#Text. (accessed 05/02/2024).
2. Civil Procedure Code of Ukraine. (2004). The Official Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/1618-15#Text. (accessed 05/02/2024).
3. Code of Administrative Proceedings of Ukraine. (2005). The Official Bulletin of the Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2747-15#Text. (accessed 05/02/2024).
4. Joint Order Issued by the State Judicial Administration of Ukraine and the Ministry of Justice of Ukraine. (2022, June 23). Press service of the SJA of Ukraine. Retrieved from https://dsa.court.gov.ua/dsa/pres-centr/news/1287616/. (accessed 05/02/2024).
5. New service in the Electronic Court! (2023, September 12). SJA of Ukraine. Retrieved from https://dsa.court.gov.ua/dsa/pres-centr/news/1475342/. (accessed 05/02/2024).

6. Horovets Y. (2024, January 13). It has become impossible to enforce judgements issued in electronic form, and there are risks of massive forgery of enforcement letters. Retrieved from https://sud.ua/uk/news/publication/290171-stalo-nevozmozhnym-prinuditelnoe-ispolnenie-resheniy-vydannykh-v-elektronnoy-forme-i-est-riski-massovoy-poddelki-ispolnitelnykh-pisem-minyust-zayavil-o-bezotlagatelnom-zakonoproekte. (accessed 05/02/2024).

7. Clarification No. 15-12512/23 on the procedure for issuance and submission documents for enforcement in electronic form and information on the functioning of the service. (2023, October 19). Retrieved from https://atari.ua/posts/65379e1d9ff6444118799ec9. (accessed 05/02/2024).

LEGITIMACY OF THE RESTRICTION OF THE RIGHT ON ACCESS TO INFORMATION UNDER THE MARTIAL LAW

Rudnyk L.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Candidate of Laws.

On the 24th February, 2022, the Russian Federation has launched a full-scale invasion of the territory of Ukraine, since then martial law has been introduced in our country. On the 8th May, 2024, the Verkhovna Rada of Ukraine extended its validity and general mobilization in Ukraine until August 11, 2024. The Constitution of Ukraine, the Law of Ukraine "On the Legal Regime of Martial Law" and the decree of the President of Ukraine on the introduction of martial law in Ukraine or in some of its localities, approved by the Verkhovna Rada of Ukraine are the legal basis for the introduction of martial law.

First of all, it's very important to emphasize on the legal definition, namely in accordance with the Law "On the Legal Regime of Martial Law": martial law is a special legal regime introduced in Ukraine or in some of its localities in the event of armed aggression or threat of attack, danger to the state independence of Ukraine, its territorial integrity and provides for the provision of the relevant state authorities, military command, military administrations and local self-government bodies with the powers which are necessary to avert the threat, repulse armed aggression and ensure national security, eliminate the threat of danger to the state independence of Ukraine, its territorial integrity, and as well as a temporary restriction of the constitutional rights and freedoms of a person and a citizen, as well as the rights and legal interests of legal entities, with an indication of the period of validity of these restrictions, caused by a threat [1].

On the 28th April, 2024, the Ministry of Justice of Ukraine updated the list of rights and freedoms regarding which, during the period of martial law, temporary restrictions on the constitutional rights of people in Ukraine may be imposed. The corresponding message was sent to the European Council.

Human information rights are enshrined in the Constitution of Ukraine, the Laws "On Information", "On Appeals of Citizens", "On Access to Public Information", "On Protection of Personal Data", etc. In the generalized interpretation, information rights of a person are state-guaranteed opportunities of a person to satisfy their needs in obtaining (access to information), using, distributing, security and protecting the volume of information necessary for life.

The right on information, which includes the right to freely collect, store, use and distribute information orally, in writing or in another way – at one's choice is the basis of human information rights. The right of a person to receive information is the basis of the right on information. It is necessary to emphasize that the right on information is not absolute and unlimited. In particular, the realization of one's right on information by citizens, legal entities and the state

should not violate public, political, economic, social, spiritual, environmental and other rights, freedoms and legitimate interests of other citizens, rights and interests of legal entities. The attention should also be paid to the principle that it is not allowed to collect information that is a state secret or confidential information of a legal entity. From these provisions, it can be determined that a person's right to information ends where another person's right begins.

The basic grounds for the restriction of human rights in Ukraine are the provisions of the Constitution of Ukraine and the corresponding interpretations of the Constitutional Court of Ukraine, which, based on the theory of human rights and the requirements of International Human Rights Law in its decisions regarding the restriction of various human rights, formed a number of basic legal positions that became a formalized component of the legal system of Ukraine.

Analyzing the articles of the Constitution in respect of which restrictions are established, it is worth noting that they guarantee a number of not only informational, but also other human and citizen rights, but it is needed to focus only on those that perform the scientific interest to the author:

• non-interference in personal and family life (Article 32), in particular, it is not allowed to collect, store, use and distribute confidential information about a person without their consent, except in cases specified by law, and only in the interests of national security, economic well-being and human rights [2]. Confidential information is information about a natural person, as well as information to which access is limited to a natural or legal person, except for subjects of authority. The legislation of Ukraine also enshrines the provision that confidential information can be disseminated at the request (consent) of the relevant person in the manner determined by it in accordance with the conditions stipulated by it, as well as in other cases determined by law (Parts 1, 2 of Article 21 of the Law on Information). Analyzing the problems of restriction of human rights, the Constitutional Court of Ukraine in its numerous interpretations proceeds from the requirements of the rule of law, as one

of the principles for the existence of a legal state, which is Ukraine, and the basic understanding of restrictions as "narrowing the content and scope of constitutional rights and freedoms." In accordance with the decision of the Constitutional Court of Ukraine, the list of personal data recognized as confidential information is not exhaustive. But such intervention is permitted exclusively in cases specified by law, and only in the interests of national security and economic well-being and human rights [3].

• another right that is subject to restriction in the current conditions is the right on freedom of thought and speech, free expression of views and beliefs, as well as the right to freely collect, store, use and disseminate information (Article 34) [2]. The issue of the realization of informational rights in the conditions of martial law is particularly urgent, since the occupiers, having not obtained a military advantage on the battlefield, are increasingly resorting to so-called cyberwar (digital war) by carrying out cyberattacks on the websites of state authorities and local self-government, calls "on behalf of the authorities in Ukraine" to civilians, spreading misinformation in the Ukrainian mass media, spreading false information, viral attacks on civilians, hacking pages in social networks, etc. Another type of violation of human information rights, which appeared against the background of the war in Ukraine, is the violation of the right to publish digital media. After the full-scale invasion of the Russian Federation of the territory of Ukraine, such social networks as Instagram and Facebook began to classify content about the Ukrainian war as "sensitive content". This became a violation not only of such a digital right as the right to publish digital media, but also a violation of Article 19 of the Universal Declaration of Human Rights, which states the right of every person to freedom of beliefs and to their free expression; this right includes the freedom to hold one's beliefs without hindrance and the freedom to seek, receive and impart information and ideas by any means and regardless of national boundaries [4, p.94].

Applying acts of international human rights law as key principles in the field of human rights restrictions, it is worth emphasizing that the relevant provisions of the documents adopted by the UN, in particular the International Covenant on Civil and Political Rights, the Council of Europe Convention on the Protection of Human Rights and Fundamental Freedoms, as well as the American conventions on human rights do not differ significantly. The withdrawal of states from their obligations, defined by these acts, is possible only in extraordinary conditions that create national threats, changing the balance of private and public interests. Similar guarantees of inviolability of human rights are defined by the Constitution of Ukraine.

For example, according to Article 15 of the Convention on the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) [5], it is provided that during the period of martial law, temporary restrictions on people's constitutional rights may be introduced.

In accordance with the provisions of Article 64 of the Constitution of Ukraine, in conditions of martial law or a state of emergency, separate restrictions of rights and freedoms may be established with an indication of the period of validity of these restrictions (it is assumed that these restrictions will be valid during the period of martial law and should be removed in 30 days after its cessation – author). The rights and freedoms stipulated by Articles 24, 25, 27, 28, 29, 40, 47, 51, 52, 55, 56, 57, 58, 59, 60, 61, 62, 63 of this Constitution cannot be limited in any situations [2].

That is, any restrictions on rights (on access to information, in particular) can be implemented to ensure national security, which, in turn, is defined at the legislative level as the protection of state sovereignty, territorial integrity, the democratic constitutional order and other national interests of Ukraine from real and potential threats (Article 1) [6]. And threats to the national security of Ukraine are phenomena, trends and factors that make it impossible or difficult or may make impossible or difficult the realization of national

interests and the preservation of national values of Ukraine (armed aggression of the Russian Federation against Ukraine) [6].

The analysis of the legislation of Ukraine shows that the principles and system of possible limitations of the constitutionalized informational rights of a person (the right on respect of personal and family life, to the secrecy of correspondence, telephone conversations, telegraphic and other correspondence, freedom of thought and speech, free expression of one's views and beliefs), meets the requirements and principles of international human rights law. Under normal conditions, the establishment of the limits of these traditional, but informational in nature, human rights takes place on a democratic basis and in accordance with the requirements of the rule of law [7, p. 38].

I agree with the position that one of the starting points for evaluating restrictions on human rights is the requirement of legal certainty – restrictions are established by law, the law must be accessible, and the application of restrictions in practice is permissible only if they are predictable [8, 9].

Therefore, after analyzing a number of normative legal acts, it can be stated that the restriction of information rights is currently legitimate and does not violate the provisions of national and international legislation and Ukraine's obligations under it. Such a deviation is called a derogation. When a country introduces or ends such restrictions, it must notify the Secretary General of the Council of Europe of what has been done. Ukrainians still have the right to appeal to the ECHR with complaints about rights violations, and the court will check whether the restriction is justified in each specific case.

Refereces:

1. On the Legal Regime of Martial Law: the Law of Ukraine dated May 12, 2015. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (access date 05/09/2024)

2. The Constitution of Ukraine dated June 28, 1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (accessed 05/09/2024).

3. Decision of the Constitutional Court of Ukraine No. 2-rp/2012 dated January 20, 2012 in the case of the constitutional submission of the Zhashkiv District Council of the Cherkasy Region regarding the official interpretation of the provisions of the first and second parts of Article 32 and the second and third parts of Article 34 of the Constitution of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#n51 (accessed 05/09/2024).

4. Denysenko K. V., Borko I. S., Kosov O. M. Implementation of digital and informational human rights under martial law. Scientific Bulletin of the Uzhhorod National University, 2023, No. 93, pp. 90-94. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/16-1.pdf (accessed 05/09/2024).

5. Convention on the Protection of Human Rights and Fundamental Freedoms (with Protocols) (European Convention on Human Rights) dated November 4, 1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (accessed 05/09/2024).

6. On the National Security of Ukraine: the Law of Ukraine dated June 21, 2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 05/09/2024).

7. Tikhomirov O.O. Limits and limitations of human informational rights. Law and society. 2023, No. 1. P. 31-39 URL: http://pravoisuspilstvo.org.ua/archive/2023/1_2023/5.pdf (accessed 05/09/2024).

8. European Court of Human Rights. Case of Oleksandr Volkov v. Ukraine (Application no. 21722/11). 9 January 2013. URL: https://hudoc.echr.coe.int/%20eng#{%22itemid%22:[%22001-115871%22]} (accessed 05/09/2024).

9. Decision of the Constitutional Court of Ukraine dated June 29, 2010 No. 17-рп/2010 in the case on the constitutional submission of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine regarding compliance with the Constitution of Ukraine (constitutionality) of the eighth paragraph of paragraph 5 of part one of Article 11 of the Law of Ukraine "On Militia" URL: http://www.ccu.gov.ua/sites/default/files/ndf/17-rp/2010.doc (accessed 05/09/2024).

PERSONAL DATA PROTECTION AS A COMPONENT OF THE ECONOMIC SECURITY OF THE COMPANY

Samchynska O.

Postgraduate student, lecturer at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute".

In 2006, British mathematician Clive Humby stated that "data is the new oil," which essentially laid the foundation for the modern understanding of the digital economy. The development of information and communication technologies and artificial intelligence continues to open up new opportunities for collecting, analysing, and using information about natural persons in various fields and for different purposes. As a result, in the context of the ongoing development of the digital economy, it is evident that the processing of personal data has become an integral part of business entities' activities that, work with clients (consumers) who are natural persons.

Companies can optimize their processes and utilize available resources more efficiently by carrying out various operations with personal data. For instance, they can conduct preliminary market analysis, including the assessment of demand and the needs of the target audience, and subsequently, based on the collected information, model the behaviour of potential clients and create a more relevant and effective business development plan. Another essential element of any entrepreneurial activity is advertising, the majority of which is currently disseminated online. The processing of a considerable volume of personal data by modern technologies offers numerous opportunities to enhance the effectiveness of marketing communications, such as personalized advertising, retargeting, and micro-targeting.

Therefore, the processing of personal data facilitates more informed and effective managerial decisions, which in turn has a positive effect on the economic condition and overall development of the company. Conversely, failure to address this aspect may result in the company's growth and development being jeopardised.

At the same time, it is worth noting that entrepreneurial activity not only provides the entities engaged in it with certain opportunities, i.e. rights but also imposes obligations that they must fulfil and provides for the existence of rules that must be followed. One of these responsibilities is to respect and promote the realisation of human and civil rights and fundamental freedoms.

Digitalisation, particularly the opportunities, and perspectives of personal data use, also entails many risks in addition to its benefits. So, the Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020 identifies the growth of cybercrime, exacerbated by the increasing number of information systems utilizing personal data, as one of the primary concerns. In addition, one of the fundamental principles of digitalisation is defined as trust and security, which encompasses information and cybersecurity, the protection of personal data and privacy, the protection of the other rights of digital technology users, and the strengthening and protection of trust in cyberspace. These elements are prerequisites for digital development and, at the same time, for the effective prevention, elimination, and management of related risks [1].

In light of the above, it can be argued that, in today's environment, personal data protection is not only a legal obligation of business entities but also an important component of their economic security. Because the leakage, breach of integrity, or unauthorised access to such data may result in a series of negative consequences that have different impacts on the company's economic condition.

It is worthy of note that the scientific literature lacks a unified understanding of the concept of economic security of an enterprise. However, the approach according to which it is defined as the state of protection of vital economic interests of an enterprise from in-

ternal and external threats is quite common. In particular, N.M. Hapak determines the economic security of an enterprise as a state of corporate resources (capital, personnel, information, technology, machinery and equipment, rights) and entrepreneurial opportunities, which guarantees, firstly, the most efficient use of them for stable functioning and dynamic scientific, technical and social development, and, secondly, prevention of internal and external negative influences (threats). The primary goal of economic security, according to Hapak, is to guarantee the stable and most efficient functioning of the enterprise in the present and high development potential in the future [2, c. 63, 64].

Given the above, we can conclude that in the context of the active development of the digital economy, information that constitutes personal data is one of the company's corporate resources. Therefore, we will examine the main aspects indicating the significant role and importance of personal data protection for the economic security and development of the enterprise.

First and foremost, it is essential to note that in modern conditions, personal data protection is not merely a component of the right to respect for private and family life, but is recognized as a separate fundamental human right. This is explicitly enshrined in Article 8 of the Charter of Fundamental Rights of the European Union [3]. Furthermore, the preamble to the General Data Protection Regulation (GDPR), the primary legal act of the European Union (EU) in this area, states that the protection of individuals during the processing of personal data is a fundamental right of a natural person [4]. Although these documents do not currently have a legal force on the territory of Ukraine, given the European vector of our country's development, as enshrined in the Constitution of Ukraine, and the attainment of EU candidate status and the commencement of accession negotiations, their relevance is a matter of time. After all, the harmonisation of national legislation with EU law is one of the components of European integration.

In addition, it should be noted that one of the peculiarities of the GDPR is its extraterritorial scope. Therefore, even though Ukraine is not currently a member of the Union, some national business entities are already required to comply with its provisions. Thus, under Article 3 of the GDPR, even if a company is not established in the EU, the GDPR requirements apply in two cases:

– if business entities process personal data for the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;

– if data processing is carried out to the monitoring of natural person`s behaviour as far as their behaviour takes place within the Union [4].

In other words, even if a Ukrainian company does not currently provide services (supply goods) to citizens of EU member states, but is going to do so and conducts market analysis for this purpose that includes personal data processing, it is required to comply with the Union's data privacy legislation. In case of non-compliance with the principles and rules of personal data processing established by the GDPR, it will be legally liable under Article 83, which, for certain violations, establishes fines of up to 20000000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher [4]. This will undoubtedly have a negative impact on the company's economic situation.

In addition, foreign investment and collaboration with international partners, including the EU, represent a significant aspect of the growth and development of numerous national companies. Ensuring proper protection of personal data in this case is an important element of the company's investment attractiveness, as it serves as a certain guarantee of the security of the invested capital. Concurrently, the appropriate protection of personal data is also a prerequisite for collaboration with European partners, which frequently entails the processing of personal data.

An equally crucial aspect of business activity and a pivotal factor in the advancement of the digital economy is the trust of consumers

and customers. Although the level of privacy culture in our country is still relatively low, more and more people are paying attention to a company's personal data protection measures when choosing goods and services. Furthermore, as previously stated, the enhancement of trust and security is one of the fundamental principles of the digitalisation of the economy. Consequently, it can be posited that this is the foundation of business operations.

It is our contention that particular attention should be paid to the issue of leakage and unauthorised access to personal data, which may have a number of negative consequences of various kinds.

Firstly, this may indicate a failure to ensure the fundamental principle of data integrity and confidentiality, which is a prerequisite for imposing fines on the company. In accordance with Article 32 of the GDPR, the controller and processor are obliged to implement appropriate technical and organisational measures to ensure an adequate level of security for the processed data. This article specifies that these measures should consider the current state of technology, the nature, scope, context, and purposes of processing, and, importantly, the potential risks and harms to the rights and freedoms of individuals who are personal data subjects in the event of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data [4].

The rectification of the consequences of such incidents typically necessitates a significant investment of time and additional resources, which may result in the disruption or even cessation of the company's operations for a specified period. As a result, such incidents may lead to loss of profits.

Furthermore, in the event of a data breach or unauthorised access to personal data, competitors may gain access to the company's client base and information about its employees, which would undoubtedly have negative consequences for the company. Such information could be used in the future for the purpose of "poaching" employees, blackmail, extortion, or other forms of information-psychological influence.

It is also of equal importance to note that instances of cyberattacks resulting in data breaches can have a detrimental impact on the reputation of the business entity in question, as well as its attractiveness to existing and potential clients and partners.

Therefore, in light of the ongoing development of the digital economy and the rising incidence of cyberattacks, personal data protection represents a vital aspect of economic security and a cornerstone of enterprise growth.

At the same time, it should be noted that the value of information about an individual and the potential for its utilisation in the achievement of pre-defined objectives has attracted not only the attention of businesses but also other stakeholders, particularly in the political, ideological, and military spheres. Consequently, the gathering and examination of individual data, and especially profiling, has become a crucial element in the planning and execution of information and psychological influence operations. The exploitation of cybersecurity vulnerabilities in individual companies allows interested parties to gain access to personal data and use it to create and disseminate disinformation, which can have negative consequences not only within a single company but also at the state level. It can therefore be posited that the protection of personal data is an essential element of the company's economic security, while at the same time playing a significant role in safeguarding the national interests of the state in the information sphere.

References:

1. On approval of the Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020 and approval of the action plan for its implementation: Order of the Cabinet of Ministers of Ukraine. January 17, 2018 № 67-p. Retrieved from: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text [in Ukrainian]. (accessed 05/04/2024).

2. Hapak N. M. Economic Security of an Enterprise: Essence, Content and Basis of Assessment. Naukovyi visnyk Uzhhorodskoho univer-

sytetu. 2013. 3(40). P. 62-65. Retrieved from: https://dspace.uzhnu.edu.ua/jspui/handle/lib/1145 [in Ukrainian]. (accessed 05/04/2024).

3. Charter of Fundamental Rights of the European Union 2012/C 326/02 Retrieved from: http://data.europa.eu/eli/treaty/char_2012/oj [in English]. (accessed 05/04/2024).

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [in English]. (accessed 05/04/2024).

LEGAL REGULATION OF DIGITAL TRANSFORMATION AS A FACTOR OF INFLUENCE ON THE ECONOMY OF UKRAINE

Sydorenko V.

Associate Professor at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute", Candidate of Science of Law

Legal regulation of digital transformation in Ukraine has a significant impact on the country's economy. Moreover, this influence has a multi-vector nature, exerting, in the end, a synergistic influence on a number of parameters of the economy of Ukraine.

First, such legal regulation of digitalization stimulates innovation and technological development, creating a favorable environment for the development of venture capital, startups and research projects. Second, effective legal regulation attracts foreign investment, especially in sectors related to digital technologies and e-commerce.

Thirdly, digitalization of public services helps to reduce bureaucracy, increase transparency and improve the quality of service to citizens, which is important for increasing the efficiency of government structures. Fourth, the strengthening of legislation in the field of intellectual property protects the rights of authors and innovators , which is critically important for the development of the digital economy.

Fifth, legal regulation that simplifies and standardizes electronic commerce can significantly increase its volumes, ensuring the development of this sector of the economy. Finally, the development and implementation of laws to ensure data protection and cybersecurity are critical to consumer and business confidence in digital technologies.

Each of these aspects has the potential to stimulate economic growth, increase the efficiency of production and services, and provide Ukraine with competitive advantages at the international level.

One of the main legal acts that regulates legal relations in the digital sphere is the Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine" dated July 15, 2021 No. 1667-IX [1]. It plays a key role in shaping the future digital landscape of our country. First, it is aimed at stimulating the development of the digital economy by creating favorable conditions for conducting innovative business, developing digital infrastructure, attracting investments and talented specialists. Second, the law guarantees freedom of economic activity and limits non-interference of the state, creating a favorable environment for development and innovation. It also establishes a presumption of legality for the activities of Diya City residents, which provides a certain level of protection against unforeseen legal risks.

Third, the stability of the legal regime, guaranteed for a period of at least 25 years, ensures long-term planning and investment in the digital sector. In addition, the procedure for acquiring the status of a Diya City resident is formal in nature and does not require obtaining special permits or licensing, which simplifies the process of business integration into this legal regime. Also important is the

principle of voluntary residency , which emphasizes the need for free choice for business.

These aspects of the law have the potential to contribute significantly to the growth of the Ukrainian economy, especially in the field of digital technologies. They create favorable conditions for innovation, attract investments and qualified personnel, which can have a positive impact on the overall economic development of the country.

The Law of Ukraine "On Virtual Assets" dated February 17, 2022 No. 2074-IX [2] establishes the legal framework for regulating the turnover of virtual assets in Ukraine. It defines the rights and obligations of participants in the virtual assets market, as well as the foundations of state policy in this area.

First, the law introduces the definition of virtual assets as intangible goods that have value and are expressed in the form of data. It distinguishes between secured and unsecured virtual assets, and defines the concepts of a virtual asset wallet, a virtual asset key, and other important terms related to virtual assets. Secondly, the law establishes the scope of its application, indicating that it regulates all legal relations related to virtual assets that have a registered location or permanent representation in Ukraine, as well as those that occur between residents of Ukraine. Thirdly, the general principles of state regulation of the circulation of virtual assets include expediency, adequacy, efficiency, balance, predictability, transparency and consideration of public opinion. These principles are aimed at ensuring rational, effective and transparent regulation of this rapidly developing area.

The impact of this law on the economy of Ukraine can be significant. It helps create a stable and predictable legal environment for virtual assets that can attract investment and stimulate the development of new digital technologies. In addition, the law brings clarity and security to transactions with virtual assets, which is important to protect the interests of investors and consumers, as well as to maintain the integrity and transparency of the country's financial system.

Despite the difficult military and political situation, the decline

in the rate of economic growth and the outflow of investments that inevitably accompany the state of war, thanks to the legal regulation of digital transformation, Ukraine is gradually transforming into an attractive hub for technological startups, especially in areas such as information technology, blockchain, artificial intelligence and other advanced technologies. This trend can be explained by several key factors.

First of all, Ukraine has a strong and dynamic IT industry with a large number of highly qualified specialists. The country is known for its IT specialists, programmers and engineers who can offer innovative solutions and high-quality services. Such resource potential is an important asset for the development of startups. Another important aspect is the support of innovations and start-ups at the state level. The Ukrainian government is developing initiatives and programs aimed at supporting innovative entrepreneurship, which includes financing, tax incentives and assistance in the commercialization of ideas and technologies. Finally, innovations in IT, blockchain, artificial intelligence and other advanced technologies have the potential to become catalysts for economic growth. They open up new opportunities for creating products and services that can be used in various industries.

Thus, digital transformation is not only changing today's labor market, but also shaping the future of professional skills, requiring educational institutions to adapt to new technological demands.

Digital transformation in Ukraine plays an important role in the development of small and medium-sized enterprises, contributing to their entry into international markets and increasing competitiveness. Optimization of business processes with the help of digital technologies, access to new markets through digital platforms and opportunities for innovation significantly expand development prospects for Ukrainian enterprises.

Legal regulation of digital transformation has a significant impact on the economy in Ukraine. Moreover, this influence has a multi-vector nature, exerting, in the end, a synergistic influence on a number of parameters of the economy of Ukraine. First, such legal

regulation of digitalization stimulates innovation and technological development, creating a favorable environment for the development of venture capital, startups and research projects. Second, effective legal regulation attracts foreign investment, especially in sectors related to digital technologies and e-commerce. Third, digitalization of public services helps to reduce bureaucracy, increase transparency and improve the quality of service to citizens, which is important for the development of freedom of entrepreneurship, on the one hand, and increasing the efficiency of government structures, on the other. Fourth, the strengthening of legislation in the field of intellectual property protects the rights of authors and innovators, which is critical for the development of the digital economy, and also helps to ensure that the intellectual capital produced in Ukraine remains in it and works for its benefit. Fifth, legal regulation that simplifies and standardizes electronic trade increases its volume, ensuring an increase in the capitalization of this sector of the economy. Finally, the development and implementation of laws to ensure data protection and cybersecurity strengthens consumer and business confidence in digital technologies.

In conclusion, digital transformation in Ukraine opens up new opportunities for economic development, innovative growth and efficiency improvement in various sectors. However, it also presents challenges for the country to adapt to changing market conditions and develop appropriate skills among the workforce.

References

1. On Stimulating the Development of the Digital Economy in Ukraine: Law of Ukraine dated July 15, 2021. No. 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (accessed 05/05/2024).

2. On Virtual Assets: Law of Ukraine dated February 17, 2022. No. 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (accessd 05/05/2024).

THE TREATY OF SPITZBERGEN: PROBLEMS AND SOLUTIONS FOR AN ARCTIC FUTURE

Tsybulenko E.
Ph.D., Senior Mentor, TalTech Law School

Diaz E.
LL.B. cand., TalTech Law School

Svalbard has recently been making headlines in world news, with Russia substantiating her veiled threats about the sovereignty of the archipelago [2, p.2]. Russia's growing economic and military power, the oppression of Russian people abroad, and the economic future of its settlement further clarify Russia's resolve to maintain a position. Geographically, Svalbard is currently a territory of Norway, a key NATO member in the Arctic. An attack on the archipelago would, therefore, trigger NATO's retaliation, putting NATO in direct conflict with Russia [5, p.2].

Investigations reveal that Russia seems to have great aspirations for the Arctic and has put the hubris of its intentions on full display since 2007 when it first planted a Russian flag below the North Pole on the seabed, signifying its ambition to have its Exclusive Economic Zone (EEZ) extended to the continental shelf and thus control the resources up to this point [17, p.2]. However, their applications to have the EEZ extended have not been accepted yet, and the placement of the flag drew criticism from the rest of the Arctic Nations. Expedition leader, Artur Chilingarov, stated that the mission's purpose was to prove "The Arctic is Russian." Russia is constructing military bases throughout the Arctic and its recent war with Ukraine has led to global concerns regarding when Russia will cease its actions [18, p.3]. Fears of hybrid warfare and irregular incursions into NATO territory are at the forefront of European leaders' minds in relation to Russia such as were executed in Ukraine specifically Crimea [25, p.143]. Svalbard presents a peculiar case of sovereign-

ty, with all parties to the agreement supposed to enjoy uninhibited economic use of the land, making it a focal point of unnatural levels of Russian attention.

The Arctic has always been difficult to navigate, requiring icebreakers to traverse its icy waters safely and securely. However, as the planet warms, sea ice is dramatically receding, making shipping lanes in the Arctic navigable in the winter and possibly without icebreakers in the future. The ability to export and import resources is crucial for a country's economic success [28, p.1]. With Finland and Sweden joining NATO, Russian territories situated on the Baltic Sea, such as Kaliningrad and St. Petersburg, now find themselves surrounded by NATO member countries before they can reach the open ocean. This underscores the vital nature of Russian aspirations in the Arctic for freedom of movement and shipping.

This research investigates and asks the following questions with a Thematic analysis approach [6, p. 63] :

- How have the involved parties of the Treaty of Svalbard potentially violated this treaty amidst the rising geopolitical tensions in the Arctic area of Svalbard?
- What mechanisms exist that could be invoked to settle the dispute?

The initial discovery of Svalbard, previously named Spitzbergen, is shrouded in mystery. Vikings have claimed to have found an island during northern expeditions in sagas from the twelfth century. According to [12, p.1], the name "Svalbard" means "Cold Coast" in Old Norse. However, this claim is disputed among historians as to whether the Vikings indeed originally found the Archipelago we now know as Svalbard or if the island they found was another island much further south [1, p.6]. The first confirmed discovery of Svalbard occurred during an expedition seeking a new route to China through the waters of the Arctic from Europe, dubbed the "Northeast Passage" The Dutch navigator Willem Barentsz created the first chart of the Svalbard Archipelago in 1596, commissioned by the Dutch. The Northeast Passage [7, p.4], which at that time in the Age

of Exploration represented the possibility of massive economic gain from finding the northerly route to China [8, p. 2] The name "Spitsbergen," perhaps borrowed from the sharp peaks of the archipelago and meaning "pointed mountains," could have been one of the most logical word choices [19, p.3]. This first official founding of the island of Svalbard is subsequently followed by a third theory: a Russian claim of an initial founding of Svalbard by a group of people known as the "Pomars" who are thought to have come from the White Sea region. [21, p.2].

Major countries, particularly Russia and NATO members, are interested in Svalbard because of its ideal Arctic position and an abundance of natural resources both on the land as well as in the waters and seabed surrounding the region. The Treaty of Svalbard, through which all members recognize Norwegian sovereignty, and which permits nondiscriminatory and non-preferential commercial operations and opportunities among its signatories, even for Norway and its citizens, presents a rare opportunity for Classical Realism's emphasis on power interests to directly interact with the geopolitical dynamics of the Arctic region and surrounding region of Svalbard [16, p.2].

The existence of dual-purpose infrastructure, which is civilian hardware that can be used for military and warlike applications. And given the lack of "specific binding treaties" regarding international humanitarian law [24, p.90] gives rise to apprehensions regarding military build-up, as existing infrastructure might be utilized for military objectives and purposes, potentially breaching Article 8. These accusations mostly point to Russia at the possibility of NATO interference. In Norway, observers have also focused a lot of attention on satellite stations, with some believing they have potential military uses [15, p.3]. Russia fears that electronics could be used to detect and compromise the secret nature of its nuclear facilities and submarines going to and from the Kola peninsula. There has been no proof presented that could pose a threat to Arctic military strategy [10, p.2]. In October 2021, Norway sent the frigate KNM Thor Heyerdahl to Isfjorden and Longyearbyen, this Norwegian Voyage. Nor-

way maintains that this move was not a breach of Article 9 under its interpretation of the treaty, but that did not stop loud protests from Moscow about Norway purposely increasing tensions in the area. Russia not only deceitfully claimed that Norway was violating the Svalbard Treaty, but also alleged that such a violation undermined Oslo's sovereignty over the archipelago.

According to Russian legislators' debatable interpretation, signatories of the Svalbard Treaty would only recognize Norwegian sovereignty over Svalbard on the condition that Norway adhered to the entirety of the treaty's provisions [4, p.2]. The presence of international settlers enables foreign nations to establish a *de facto* strategic foothold on the archipelago and a fresh supply of local collaborators [23, p.126]. This has led to misperceptions about Svalbard's legal status, of which the perceived dilution of Norwegian sovereignty is a vivid example that may also be leveraged by malign actors conducting gray zone activity (20, p.4). On May 9, 2023, a Victory Day parade to commemorate the Soviet victory over Nazi Germany was held in the settlement of Barentsburg [29, p.2]. The attendance of Russian helicopters on the island, sparked controversy, compounded by the parade seeming to be more militaristic than the civilian nature of previous years. These accusations have been raised, but no evidence or claims have been officially filed and can be attributed to differences in interpretation of the Treaty.

Svalbard's sovereignty, while not directly involved in the United States and NATO strategic arena due to Article 9 of the Treaty of Svalbard. Stability and security concerns in the Arctic region are becoming glaringly a weak spot in NATO's northern flank. This is particularly significant given the increasing military buildup in Russia in the Kola Peninsula and elsewhere [3, p.10]. The policy shifts focus towards ensuring freedom of navigation around the Archipelago for military vessels and identifying emerging threats before they become active, as the Arctic emerges as a new battleground for great power competition. This dynamic occasionally leads to friction with some of the activities occurring within Russia's

domain. Russia is particularly fragile regarding the interpretation of Article 9 and miscalculations by either party could lead to escalations and as stated before, causing Russia to dismiss its adherence to the treaty altogether. The United States has recently increased its EEZ territorial waters, so it has become a bigger player in Arctic affairs [4, p.3]. Considering that 7 of the 8 countries in the Arctic Council with territories above the Arctic Circle are now members of NATO, more considerations are surely on the way to ensure the security of the Arctic and increase the likelihood of a security issue and imbalance of power in the region.

The Russian Federation has a massive coastline across the Arctic and expressed its security as imperative for national security and economic development to keep the nation as a major player on the world stage. Russia feels this role on the world stage is being limited by the US and its allies especially now that it is an international pariah due to the illegal war in Ukraine [27, p.136]. The Russian Svalbardian foothold is gaining Moscow's attention and cited Norway's policy as a potential risk of war. Moscow demands more diplomatic negotiation over perceived Norwegian threats and grievances and appears to have "Unilateral revision of international agreements." However, individuals such as Russian Deputy Prime Minister Yuri Trutnev have implied that "Now is not the best time for the development of international cooperation" [20, p.2].

Warfare has changed considerably in the past 20 years, and even more so since the 2022 Russo-Ukrainian war. Drone warfare usage has reached levels reminiscent of the worst dystopian science fiction thriller, with the creativity and tactics evolution changing almost daily. Drone warfare combined with the reemergence of conventional war again with near-peer adversaries, has shown one issue needs to be addressed quite often with regards to Svalbard electronic warfare and its capabilities being used in the Arctic area with incidents being reported by Norway in 2019 of electronic warfare from the Kola peninsula impeding the function of GPS navigation in Norwegian Air space [15, p.3]. Russia's electronic warfare advan-

tage is something that has been noted by Western think tanks due to Russia heavily investing in electronic warfare (EW) long before the Russo-Ukrainian war.

The sovereign state of Norway shall administer the Svalbard archipelago as a low-tension area per the white paper, for the objectives of protecting the environment and implementing the legal obligations pursuant to the Svalbard Treaty (14, p.4). Norway, in return, has indicated its commitment to sustainable development and the peaceful use of the Arctic by leading in resources and regulations, notably in environmental protection [9, p.4]. Norway has decided to flex its political muscle with moves such as fishing disputes and expressing its desire to keep the demographics of Svalbard Norwegian through its legally unconventional removal of the rights of residents to vote on the archipelago which could be seen as a wise step to take to make sure that foreign arctic powers don't wrest control over the archipelago through demographics [13, p.3].

The aim of this paper was to investigate if and how the involved parties of the Treaty of Svalbard potentially violated this treaty and, amidst the rising geopolitical tensions in the Arctic area of Svalbard, what mechanisms exist or could be invoked to settle the dispute.

The author was fully anticipating finding numerous cases of Russia blatantly defying treaties, especially after the February 2022 invasion of Ukraine. Following the imposition of the broadest spectrum of sanctions in history, the world expected that Russia would forgo some treaty obligations and agreements, just as it had violated international law with the invasion of Ukraine [26, p. 320] However, in this paper, the author discovered that Russia was *mostly* adhering to the Treaty of Svalbard. Instead, the author found instances where Norway had skirted the line of what is and is not a violation of the treaty, specifically:

- Article 3 of the treaty when it temporarily halted shipments to and from the Russian settlement of Barentsburg which was solved through diplomatic channels. The halting of resources to Barentsburg shows that, in the fog of war, Norway very quickly will take

actions that violate the treaty of Svalbard, and this could easily lead to a security dilemma and escalation.

- Article 8, brought to light the issue of non-Norwegian residents of Svalbard losing the right to vote in local elections. Article 8 specifically states that Norway is liable to create regulations for mining that do not unfairly levy taxes, privileges, monopolies, or favors of any kind for the benefit of any state including Norway with Oslo's concern for keeping the demographic balance tipped in their favor. This is understandable through the lens of realism; Norway will use this opportunity to assert power and solidify its position. The possibility is too great to have foreign governments send citizens to live and then slowly leverage them for more power in the Arctic. But the inability to have representation, especially if you own a business and have ventured there, means your economic freedom is at the mercy of the changing winds of Norwegian policy.
- Article 9 Norway had a big problem with the May 9th parade being militaristic in aesthetics, but it also brought a military Frigate to port in Longyearbyen. Warships have been long used to project power and intimidate. Norway did not violate Article 9, but the move could be taken as an upset in the balance of power.

This paper aimed to investigate *"How have the involved parties in the Treaty of Svalbard potentially violated the treaty amidst rising geopolitical tensions in the Arctic area of Svalbard? And if so, what mechanisms could be invoked to settle the dispute?"*

It seems to come down to the letter of the law vs the spirit of the law. There is no legal basis to suggest any party is directly violating the Treaty of Svalbard. Disputes on interpretations of the law exist, and certainly, the letter of the law is being violated with voting rights and fishing disputes. The Treaty of Svalbard perfectly fits into the zeitgeist of its time in its attempt to facilitate the peaceful exploitation of the Arctic's resources while piggybacking off the League of Nations attempts to keep an international order and balance of power, which is why the focus of the Treaty was on equality of opportunity [22, p.4.] Since there are no clear violations of the

letter of the law, disputes must be settled through diplomacy and negotiation as they have been in the past and more is needed to ensure that the wall of liberal democracy is preserved from malign actors by examining treaties such as this one to ensure no gaps exist that could be exploited to drive a wedge in the community of nations.

References:

1. Arlov, T. B. (2005). The Discovery and Early Exploitation of Svalbard. Some Historiographical Notes. Acta Borealia, 22(1), 3–19. https://doi.org/10.1080/08003830510020343
2. Atle, S. (2024). Deputy Prime Minister sends warning to Oslo: Russian rights at Svalbard must not be challenged. https://thebarentsobserver.com/en/2024/02/deputy-prime-minister-sends-warning-oslo-russian-rights-svalbard-must-not-be-challenged. (accessed 05/04/2024).
3. Bal, A., Dalaklis, D., Bartuseviciene, I., & Başar, E. (2024). Discussing the Influence of the Russian-Ukrainian Conflict in the High North. American Yearbook of International Law, 2(1), 117–167. https://doi.org/10.5281/zenodo.10679960
4. Baudu, P. (2023). Minding the Archipelago: What Svalbard Means to NATO. Arctic Review on Law and Politics, 14, 76–82. https://arcticreview.no/index.php/arctic/article/view/5197/8234
5. Collective Defence and Article 5, 1 (2023). https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Article%205%20provides%20that%20if,to%20assist%20the%20Ally%20attacked (accessed 05/04/2024).
6. Dawadi, S. (2020). Thematic Analysis Approach: A Step by Step Guide for ELT Research Practitioners. In Journal of NELTA (Vol. 25, Issue 2).
7. ENCyclopedia.com. (2020). Willem Barents Searches For The Northeast Passage And Finds Svalbard Instead. In Encyclopedia.com (pp. 3–8). ENCyclopedia.com. https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/willem-barents-searches-northeast-passage-and-finds-svalbard-instead. (accessed 05/04/2024).
8. ESA. (2011, August 25). Arctic shipping routes open. European Space Agency. https://www.esa.int/Applications/Observing_the_Earth/Space_for_our_climate/Arctic_shipping_routes_open#:~:text=As%20

sea%20ice%20melts%20during,now%20it%20has%20happened%20again. (accessed 05/04/2024).

9. Government.no. (2016). Svalbard – Meld. St. 32 (2015–2016) Report to the Storting (white paper). https://www.regjeringen.no/en/dokumenter/meld.-st.-32-20152016/id2499962/?ch=3. (accessed 05/04/2024).

10. Governor of Svalbard. (2019). Environmental protection. https://www.sysselmesteren.no/en/the-governor-of-svalbard/environmental-protection/ (accessed 05/04/2024).

11. Jensen, Ø. (2020). The svalbard treaty and norwegian sovereignty. Arctic Review on Law and Politics, 11, 82–107. https://doi.org/10.23865/arctic.v11.2348

12. Kate, L. (2022, June 23). Svalbard: The Land of the Cold Coast View fullsize. Byron Magazine. https://www.byronmagazine.com/news/svalbard-the-land-of-the-cold-coast. (accessed 05/04/2024).

13. Newsinenglish.no. (2022). Svalbard's foreign residents lose their voting rights. https://www.newsinenglish.no/2022/06/20/foreigners-in-svalbard-lose-voting-rights/ (accessed 05/04/2024).

14. Nilsen, T. (2017, October 4). Kommersant: Russia lists Norway's Svalbard policy as potential risk of war. The Barents Observer, 2–5. https://thebarentsobserver.com/en/security/2017/10/kommersant-russia-lists-norways-svalbard-policy-potential-risk-war. (accessed 05/04/2024).

15. Nilsen, T. (2019, December 20). Russia's electronic warfare test causes radio- and radar disturbances in Norway. The Barents Observer, 1–4. https://thebarentsobserver.com/en/security/2019/12/testing-russias-newest-frigate-causes-radio-and-radar-disturbances-northernmost. (accessed 05/04/2024).

16. Og beredskapsdepartementet, J.-. (2017). Public institutions may order additional copies from: Norwegian Government Security and Service Organisation Svalbard. www.publikasjoner.dep.no. (accessed 05/04/2024).

17. Parfitt, T. (2007). Russia plants flag on North Pole seabed. https://www.theguardian.com/world/2007/aug/02/russia.arctic. (accessed 05/04/2024).

18. Reynolds, P. (2007, August 1). Russia ahead in Arctic "gold rush." World Affairs Correspondent, BBC News Article, 1–3.

19. Schneider, P. (2022, March 14). Spitsbergen, the ground zero of climate change. Energy Observer, 1–3. https://www.energy-observ-

er.org/resources/spitsbergen-ground-zero-climate-change. (accessed 05/04/2024).

20. Staalesen. Atle. (2024, February 13). Deputy Prime Minister sends warning to Oslo: Russian rights at Svalbard must not be challenged. The Barents Observer, 1–6. https://thebarentsobserver.com/en/2024/02/deputy-prime-minister-sends-warning-oslo-russian-rights-svalbard-must-not-be-challenged. (accessed 05/04/2024).

21. Svalbardmuseum. (2010, March 17). POMOR TRAPPERS TAKE CENTRE STAGE. Svalbardmuseum. https://svalbardmuseum.no/en/the-pomors

22. The Svalbard Treaty, 1 (1920). https://www.jus.uio.no/english/services/library/treaties/01/1-11/svalbard-treaty.html (accessed 05/04/2024).

23. Tsybulenko, E., & Francis, J. A. (2018). Separatists or Russian Troops and Local Collaborators? Russian Aggression in Ukraine: The Problem of Definitions. In S. Sayapin & E. Tsybulenko (Eds.), The Use of Force against Ukraine and International Law (pp. 123-144). T.M.C. Asser Press/Springer.

24. Tsybulenko, E., & Kajander, A. (2022). Customary International Humanitarian Law and Article 36 of Additional Protocol I to the Geneva Conventions: A Stopgap Regulator of Autonomous Weapons Systems? TalTech Journal of European Studies, 12(2), 87-112.

25. Tsybulenko, E., & Kelichavyi, B. (2018). International Legal Dimensions of the Russian Occupation of Crimea. In S. Sayapin & E. Tsybulenko (Eds.), The Use of Force against Ukraine and International Law (pp. 277-296). T.M.C. Asser Press/Springer.

26. Tsybulenko, E., & Rinta-Pollari, H. (2023). Legal Challenges in Prosecuting the Crime of Aggression in the Russo-Ukrainian War. Review of Central and East European Law, 48(3-4), 319-350.

27. Tsybulenko, E., & Platonova, A. (2019). Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea. Baltic Journal of European Studies, 9(3 (28)), 134−147.

28. Ulfstein, G. (2008). Spitsbergen/Svalbard. http://opil.ouplaw.com

29. Vereykina, E. (2024, February 7). Russian company fined for a helicopter flight on Svalbard. The Barents Observer. Retrieved from https://thebarentsobserver.com/en/2024/02/we-are-not-disputing-decision-penalty-will-be-paid-russian-company-fined-helicopter-flight#:~:text=Rus-

sian%20company%20Convers%20Avia%20Airlines,media%20Svalbard-posten%20reported%20on%20Wednesday. (accessed 05/04/2024).

ELECTRONIC EVIDENCE IN LABOR RELATIONS

Tykhoniuk O.

Lecturer at the Department of Information, Economic and Administrative Law, Faculty of Sociology and Law, National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute".

The current labor legislation of Ukraine stipulates that employees may familiarize themselves with orders (instructions), notifications, and other documents of the employer regarding their rights and obligations using the electronic communication means specified in the employment agreement (employment contract); the fact of exchange of relevant electronic documents between the parties to the employment agreement is considered to be a confirmation of familiarization [1, part 3, Article 29], and for the period of martial law, the parties to an employment agreement may agree on alternative ways of creating, sending and storing the employer's orders (instructions), notifications and other documents on labor relations and any other available method of electronic communication chosen by agreement between the employer and the employee [2, part 2 of Article 7].

The author of an electronic document or an intermediary sends or transmits it in electronic form by means of information, electronic communication, information, and communication systems or sends electronic media on which the document was recorded [3, part 1, Article 10].

Unless the author and the addressee have previously agreed otherwise in writing, the date and time of sending an electronic document shall be the date and time when the sending of an electronic document

cannot be canceled by the person who sent it [3, part 2, Article 10]. Thus, an electronic document is deemed to have been received by the addressee from the moment the author receives an electronic notification from the addressee that he or she has received the electronic document, unless otherwise provided by law or a prior agreement between the subjects of electronic document circulation [3, part 1, article 11]. At the same time, it should be noted that according to the decision of the Supreme Court of Ukraine (the "SC") dated 08.02.2023 in case No. 199/1861/20, sending an email to an email address that is not an official email address cannot be considered as a proper sending and does not create any legal consequences for the parties.

But it turns out that "not everything is so clear," as one famous classic said, because the court may consider e-mail correspondence between persons in a messenger (as well as any other correspondence) as evidence only if it makes it possible to identify the authors of this correspondence and its content [4]. For example, the "SC", considering case No. 299/2706/20 on the employee's claim against the LLC for reinstatement and recovery of average earnings in its decision of 21.12.2022, made the following conclusions: An employee submitted an application for an annual vacation of 14 calendar days with subsequent dismissal. Later, the employee sent an application to the employer's email address signed with a personal electronic digital signature (hereinafter – EDS) to withdraw her earlier resignation and informed that she would resume her employment duties after the end of the leave. She additionally sent a similar statement to the email addresses of the company's director, head of the HR department, and head of the finance department. However, the employer dismissed the employee at his own request. The employee appealed the dismissal to the court, providing copies of screenshots of her electronic application sent to the email addresses of the LLC (limited liability company) director, head of the HR department, head of the finance department, and system administrator, with an electronic signature. The Supreme Court overturned the decisions of the previous instances and dismissed the employee's claim as she failed to pro-

vide evidence that the recipients of the sender's electronic messages had received them, which is a violation of Article 11 of the Law of Ukraine "On Electronic Documents and Electronic Document Management". Instead, if it is proved that a letter or message was sent to a certain person, the message that is a response will be considered authentic without additional evidence, since it is unlikely that anyone other than this person can receive and respond to the message, taking into account its content and the details discussed (Supreme Court ruling of 03.08.2022 in case No. 910/5408/21 At the same time, considering case No. 757/35570/21-ts (resolution of 26.10.2023), the "SC" notes that the law does not limit the method of submitting a resignation letter. Thus, a resignation letter can be submitted in person to the employer, sent by mail or telegram. At the same time, sending a letter of resignation by post to the employer, although it is a possible option for the employee to notify the employer of his or her intentions, without establishing that the employer has received such a letter, does not indicate termination of the employment relationship between the parties from the date of sending such a letter within the time period specified in it.

What else should you pay attention to?

Considering case No. 916/3027/21 in its ruling of 21.06.2023, the "SC" emphasizes that messages (with attachments) sent by e-mail or through messenger applications are electronic evidence, which is considered and evaluated by the court according to its internal conviction in conjunction with other evidence available in the case file [5], namely: if, taking into account the specific circumstances of the case, the court concludes that the relevant correspondence allows to identify its participants and can confirm certain arguments of the parties, for example, regarding the existence of relevant relations between them, conduct of certain negotiations, etc., the court may accept such correspondence as evidence and in this case evaluate it together with other evidence in the case.

The position of the "SC" is almost similar in case No. 509/7127/21 (decision of 26.07.2023): it should be borne in mind

that the court may consider e-mail correspondence between persons in the messenger (as well as any other correspondence) as evidence in the case only if it allows the court to identify the authors of this correspondence and its content.

In its ruling of 07.07.2021 in case No. 587/2051/18, the Supreme Court notes that printouts of Internet pages that are a paper reflection of an electronic document cannot be evidence in the case by themselves. They are recognized as evidence if they are made, issued and certified by the owner of the relevant Internet resource or provider, i.e., they acquire the status of written evidence. In other words, according to the court's logic, a printout of e-mail correspondence cannot be considered an electronic document (a copy of an electronic document) because it does not contain an electronic signature, which is a mandatory requisite of an electronic document, since in this case it is impossible to identify the sender of the message, and the content of such a document is not protected from editing and distortion.

A similar position can be traced in the decision of 13.12.2022 in case No. 296/3763/22, which was considered by the Zhytomyr Court of Appeal on a claim for reinstatement of an employee. The court was provided with printouts of e-mail correspondence with the employee on Viber, namely, a copy of the order warning employees of impending dismissal due to position reductions. According to the court, a printout from the Viber application is not a proper copy of an electronic document, as it does not contain an electronic signature. But the employee was still fired.

At the same time, in its ruling of 28.04.2021 in case No. 234/7160/20, the Supreme Court notes that it is not a violation of the rules not to examine the original electronic evidence if there are paper copies of this evidence in the case file and there are no reasonable doubts about their compliance with the original.

In our opinion, the following conclusion in the Supreme Court's ruling of 25.08.2020 in case No. 917/1061/19 is rather ambiguous, namely: an extract from the defendant's internal electronic document management system cannot be considered proper evidence

that the defendant may submit to confirm that it sent a notification letter to the plaintiff, given that such an extract does not confirm for the defendant the fact of sending correspondence, in particular, the transfer of the letter to the postal operator on a certain date, does not contain a barcode of the letter.

As we can see, when determining what is (or is not) considered electronic evidence and making a decision in favor of the plaintiff or defendant, the Court tries to comply with the provisions of the Commercial Procedure Code [6, Article 86]. At the same time, the decisions made are quite controversial, as courts do not always properly examine and evaluate electronic evidence, resulting in decisions based on unreliable and inadequate evidence.

References:

1. Code of Labor Ukraine dated December 10, 1971. Vidomosti Verkhovnoi Rady Ukraine. 1971. (Add. No. 50). Past 375. URL: https://zakon.rada.gov.ua/laws/show/322-08#n204. (accessed 05/10/2024).
2. On the organization of labor relations under martial law : The Law of Ukraine, March 15, 2022 (Pro orhanizatsiyu trudovykh vidnosyn v umovakh voyennoho stanu : Zakon Ukrayiny vid 15.03.2022). URL: https://zakon.rada.gov.ua/laws/show/2136-20#top (accessed 05/10/2024).
3. About Electronic Documents and Electronic Document Management : The Law of Ukraine, May 22, 2003 (Pro elektronni dokumenty ta elektronnyy dokumentoobih : Zakon Ukrayiny vid 22.05.2003). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (accessed 05/10/2024).
4. When correspondence in messengers can be evidence, determined by the Grand Chamber of the Supreme Court (Koly lystuvannya u mesendzherakh mozhe buty dokazamy, vyznachyla VP VS). URL: Коли листування у месенджерах може бути доказами, визначила ВП ВС (zib.com.ua) (accessed 05/10/2024).
5. Unified State Register of Court Decisions (Yedynyy derzhavnyy reyestr sudovykh rishen′) Єдиний державний реєстр судових рішень (court.gov.ua) (accessed 05/10/2024).
6. Commercial Procedure Code of Ukraine dated November 6, 1991 (as amended as of April 27, 2024). Vidomosti Verkhovnoi Rady Ukraine.

1992. No. 6. Past. 56. URL : Господарський процесуальний... | від 06.11.1991 № 1798-XII (rada.gov.ua) (accessed 05/10/2024).

CASE FOR DATA TRANSPARENCY ON THE WHOLESALE ENERGY PRODUCTS DURING THE MARTIAL LAW

Zahnitko O.

Doctorate Student at State Institution "Valentyn Mamutov Economy and Legal Research Institute of the National Academy of Sciences of Ukraine
ORCID ID https://orcid.org/0009-0002-3095-2590

The war greatly complicates establishment creation of transparent commodity markets. A robust and sustainable regulatory strategy for the martial law period must be developed with implementation of each step in the strategy announced in advance to the participants so that they have sufficient time to adapt. The basic scenario for wholesale energy products is to accept the martial law regime as a new normal. In fact, the market has actually been under the pressure of various extraordinary circumstances since early 2014 – annexation, occupation, gray zone, shelling, cyberattacks, economic coersion and other diversions have been happening, even if on the smaller scale. Back in 2014 as well as in 2024, the wholesale energy infrastructure requires monitoring, every second of the network`s load and frequency, of the natural gas' pressure in a pipeline transport and/or the gas storages. The wholesale energy market, thus, is not a place for 'wait and see' approach, the regulations of the market for the wholesale energy products in Ukraine must depart from the *ad hoc* controls to arrive at the rules and principles for the energy system and the market to function under the following scenarios:

(a) occupation (threat thereof) of the key assets in the production or trading infrastructure, where operators of transmission and distribution systems, producers, storage operators, suppliers and large consumers may be deprived of possessing the assets or access of the assets to the grid. In other circumstances, market participants operational control and be willing, to the extent possible comply with Ukrainian laws despite the responsibility of the aggressor state for the humanitarian situation on the territory under effective occupation, (b) de-occupation of assets, and (c) terrorist and military attacks on energy assets in one or more nodes of the system.

One aspect of such 'new normal' would be amendment to the wholesale energy market legal model in reporting that ensures integrity and transparency for the market participants. For a start, general public must be informed, through the platforms of insider information, the breadth of the occupied assetsy The public should be able to see the composition (taxonomy) of data and analyze the reliability of the sources of such information for themselves.

To prevent price manipulation and insider trading, Ukrainian legislation [3] [5; Art. 20-1], following the EU *acquis* [1] [2] [4] and the legal systems of other parties to the Energy Community [6], imposed on the market participants an obligation to publish data on planned production of electricity and natural gas, availability of raw materials etc. Among other aspects of the "war regime" that await their regulation, are settlements, suspension/resumption of participation in the market, technical defaults, permanent insolvency, and collateral loss absorption/distribution.

The special (emergency, martial) situation of the Ukrainian energy industry as a target for the war crimes by the Russian Federation with the complicity of the Republic of Belarus precipitates delay in publishing insider information, in particular, scheduled and unscheduled capacity unavailability for the production and consumption of wholesale energy products. The sensitivity of this information is clear – the enemy can use it to coordinate strikes. Currently, this information is collected by operators of market

segments every hour, the dispatcher and the transmission system operator react to changes in real time, the Ministry of Energy of Ukraine and the industry regulator (NEURC) also have access to it. Given the importance of natural gas and electricity in the real sector and consumer economics, the critical state of the energy market ecosystem becomes the subject of attention of the bodies responsible for national security – the General Staff, the Armed Forces of Ukraine and the Security Service of Ukraine (for the purpose of active protection measures), law enforcement agencies (collection of evidence and investigation), the National Security and Defense Council of Ukraine and the NSDC members' offices – the President of Ukraine and his office, the Prime Minister of Ukraine and the Secretariat of the Cabinet of Ministers of Ukraine, the Chairman of the Verkhovna Rada of Ukraine etc. Decisions adopted at the meetings of the NSDC and executive authorities regarding the restoration, protection and protection of energy facilities are subject to budgeting through other state authorities, in particular, the Ministry of Finance and the Verkhovna Rada of Ukraine for budgeting expenditures and through the Ministry of Foreign Affairs, the Ministry of Defense, the Ministry of Economy, the Ministry of Strategic Industries, yet again the Ministry of Energy to coordinate international technical assistance. That is, the information is collected anyway, the sources and processors are known, but the access (distribution), despite the sensitivity, is not sufficiently controlled. Access to information processed is granted to a wider number of users, often without special security clearance due to time constraints, without adequate protection or even records of the access as a fact. This situation created paradox for the market ramification, where the risk of insider trading increases despite the efforts to keep information concealed. At the same time, uncontrolled access to information decreases chances of tracing the user to the source, which bars potential investigations and penalties for misuse or, at the very least, for insufficient protection of sensitive data. The spread of the market free riders is harder to contain with every week. Similar cir-

cumstances would surround publication of prices and volumes for the conclusion of transactions – postponing their reporting enables price manipulation and eliminates grounds for justice.

Norms for managing this insider trading risk during the martial law (after the military or terrorist assaults) should provide for additional data protection measures, such as restricted printing and copying of databases. The categories of people that have access to data can be expanded, provided that each access to the database has multifactor identification. Authorization to access database can be carried by the administrator, who will check the compliance with onboarding conditions to be stipulated in the regulation: the prohibition of copying, enhanced e-signature, IP registration, certified device etc. At the same time, the draft regulation on the data protection and the wholesale energy products data administration should be consulted and vetted by the government agency responsible for access to state secrets and the state service for protection of data in the telecommunications. The regulation should be delivered, with appropriate trainings, to the operatives and analysts in the law enforcement agencies that do surveillance and intelligence of the telecommunications systems as well as the authority that investigate cyber crimes.

Besides the sensitivity of the substance, the architecture of the system for the data processing needs to be enhanced in response to the Russian attacks and their threat in a future. Currently, information is dispersed through several processing entities, use of several processing formats and various communication channels, which was a call for the optimization and unification to enhance the quality of data. The databases of the wholesale energy products market and spot energy markets must be uniform and receive a centralized architecture that does not, hovewer, prevent a competition on the data processing. Competition determines a use of an open code software with secure communications channels, while Excel files with an open data format in a table or text in an e-mail message must be a thing of the past. It is time to force transition to the EXtensible Markup Language (XML) standard and meet the requirements

of the Standard for the Automatic Exchange of Information on Financial Accounts for Tax Purposes, commonly known as Common Reporting Standard (CRS) of the Organization for Economic Cooperation and Development, approved by the OECD Council on July 15, 2014 [7]. As of this date, the laws of Ukraine make CRS mandatory for the financial institutions, including investment firms, securities' depositories, credit institutions, deposit institutions and insurance companies. It is notable that information collected by the financial instruments is not materially different from the wholesale energy products data that is subject to processing and disclosure by law, in fact, it overlaps with the wholesale energy products to the extent their sellers and buyers trade on the regulated market or enter into risk-hedging arrangements, such as financial lookalikes.

Subject to the above-mentioned safeguards, dissemination of the wholesale energy products data among the wholesale energy market players and their agents will immediately increase the efficiency of this market. Unfortunately, very little public discussion took place since the first Russian attacks on Ukraine's energy facilities in October 2022, and very little substance to reopen data was provided against dominating discourse that such insider data is a hermetic 'matter of national security'. The cause of informed decision-making by all actors in the market is not helped by the fact that, as of 2022, a single decision-making center had been operating the market, taking into account both the *de facto* singly party majority in the executive and legislative branches of a central government as well as their symbiotic unity according to the constitutional model of semi-parliamentary republic in Ukraine. This lack of checks and balances among the Cabinet of Ministers, the Verkhovna Rada and the President has implications beyond simple distortion of the market, the market is brought much closer to a hierarchy with a central plan: people in possession of insider information become the front and center of the trades (a voter with dictatorial powers in Gibbard's theorem [8]), and the remaining market participants turn into dependent, reactive targets for influence and manipulation, thus reduced to

spectators rather than actors. Therefore, a competitive environment needs to be restored for analysis, formation of trading strategies, investment decisions (regarding renovation of old capacities and construction of new ones, for example) and for responding to abuses that have occurred.

Getting back the competition of ideas and solutions to the market – giving the traders back the power to make their own decisions will allow to change the situation by using the collective power as opposed to the centralized flow of information 'planning' by the government, with inertia as well as significant bureaucratic and financial constraints. An analogy could be brought with the paradigm shift in military technology since 2022, where private sector growth was times more than public sector. Similarly, the wholesale energy market players with multiple strategies will be able to produce innovation waves that will spread the common wisdom on appropriate methods to diversify the martial law risks in the wholesale energy products trading, building and operating power generation and natural gas mining facilities, safeguarding and repairing transmission, distribution and storage infrastructure facilities. Systematization of the strengths and weaknesses of energy project management at a emergency time or under the martial law will allow the wholesale energy sector to move into a new paradigm. The adoption of defense sector solutions and technologies in the operation and management of the energy industry deserves separate consideration, beyond the scope of this material: the use of drones, of anti-missile and anti-aircraft defense, of electronic warfare, implementation of cyber security, continuity protocols etc.

Taking into account the situation in the energy sector of Ukraine, it is appropriate for the legislature and the regulators in Ukraine provide legal terms and conditions for publishing information on transparency and integrity of the wholesale energy products provided by the market participants (a) with a delay of 10, 20, 30 days or a quarter; (b) in the regime of professional secrecy or confidentiality; (c) anonymized for journalists and other general public without clearance, authorization and/or access.

References:

1. Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency / An official website of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2011.326.01.0001.01.ENG&toc=OJ%3AL%3A2011%3A326%3ATOC(accessed 04/17/2024).

2. Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 / An official website of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0600-20240109 (accessed 04/17/2024).

3. Про ринки капіталу та організовані товарні ринки: Закон України від 23 лютого 2006 р. № 3480-IV, в редакції Закону від 19 червня 2020 р. № 738-IX / Верховна Рада України. | On capital markets and organized commodity markets: Law of Ukraine dated 23 February 2006 No. 3480-IV, recast by Law dated 19 June 2020 No. 738-IX / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/3480-15#n2602 (accessed 04/17/2024).

4. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) / An official website of the European Union. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0065-20240109 (accessed 04/17/2024).

5. Про Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг: Закон України від 22 вересня 2016 р. № 1540-VIII / Верховна Рада України. | On the National Commission for State Regulation in the Energy and Utilities Sectors: Law of Ukraine dated 22 September 2016 No. 1540-VIII / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/1540-19#Text (accessed 04/17/2024).

6. Implementing Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency: Decision of the Ministerial Council of the Energy Community D/2018/10/MC-EnC dated 18 November 2018 / An official website of the Energy Community. URL:https://www.energy-community.org/dam/

jcr:011d891f-6cef-4555-9e9a-53d88e54d4b1/Regulation_1227_2011_REMIT.pdf (accessed 04/17/2024).

7. CRS (Загальний стандарт звітності) / Міністерство фінансів України. | CRS (Common Reporting Standard) / Ministry of Finance of Ukraine. URL: https://mof.gov.ua/uk/crs-578 (accessed 04/17/2024).

8. Dezső Bednay, Anna Moskalenko, Attila Tasnádi, Dictatorship versus manipulability, Mathematical Social Sciences, Volume 101, 2019, Pages 72-76, ISSN 0165-4896, https://doi.org/10.1016/j.mathsocsci.2019.07.001.

ANNOTATIONS FOR SCIENTIFIC WORKS:

Dr. Jarosław Greser,
Associate Professor, Faculty of Administration and Social Sciences, WARSAW UNIVERSITY OF TECHNOLOGY

GRASPING THE ELUSIVE: IS DIGITAL SERVICES ACT AN EFFECYIVE TOOL FOR ASSESSING ALGORITM PERFORMANCE?

Today's digital services are almost entirely automated and rely increasingly on artificial intelligence (Lund, Wang: p. 26). The literature suggests that the use of these solutions has negative impacts on society, such as cyberbullying, trolling, privacy invasions, and fake news (Baccarella, et al. 2018: p. 431). The potential negative impact on the mental health of both children and adults is a serious concern (Gao et al., 2020), particularly as some effects may manifest in the distant future (Chancellor & De Choudhury, 2020). Additionally, it should be noted that certain algorithms are intentionally designed to result in negative social outcomes, such as addiction (Zakon 2019).

To prevent and remedy negative effects caused by algorithms, it is important that they are controlled by independent bodies such as public bodies, researchers, and civil society organizations. Effective control requires access to information beyond just the algorithm's effects. This includes the design, logic, operation and testing of algorithmic systems and, in the case of AI systems, additional information on the data used to train, validate and test them. It is important to note that this information is often not publicly available due to intellectual property, trade secrets, or data protection laws (Foss-Solbrekk 2021, p. 256). Moreover, it is usually not subject to

public data re-use regulations (Park 2021). This makes independent control of the algorithms difficult, and in many cases impossible.

The European Union has recognized this problem (European Commission 2020), and the provisions have been included in the Digital Services Act to address it. The purpose of this presentation is to analyse these provisions and answer the question of whether they will be effective in assessing the performance of algorithms. The presentation is divided into three parts. In first two subject and object constraints to data access will be analysed. This will be follow by a summary of key findings and recommendations.

The European Union has acknowledged the issue (European Commission 2020) and incorporated relevant provisions into the Digital Services Act with the intention of addressing it. The objective of this presentation is to analyse these provisions and answer the question of whether they will be effective in assessing the performance of AI algorithms. The presentation is divided into three sections. In the first two sections, the subject and object constraints to access data necessary to assess algorithms will be analysed. This will be followed by a summary of the key findings and recommendations.

References:

1. Ch. V. Baccarella, T. F. Wagner, J. H. Kietzmann, I. P. McCarthy, Social media? It's serious! Understanding the dark side of social media, "European Management Journal" ,vol. 36, issue 4, 2018.
2. S. Chancellor, M. De Choudhury, Methods in predictive techniques for mental health status on social media: a critical review. "npj Digital Medcine", 2020, issue 3 https://doi.org/10.1038/s41746-020-0233-7
3. J. Gao,P. Zheng, Y. Jia, H. Chen, Y. Mao, S. Chen, Y. Wang, H.Fu, J.Dai, Mental health problems and social media exposure during COVID-19 outbreak, "PLOS one", 2020, https://doi.org/10.1371/journal.pone.0231924
4. European Commission, Communication from The Commission A European strategy for data, COM(2020) 66 final Brussels, 2020.

5. Brady L., Ting W., Chatting about ChatGPT: how may AI and GPT impact academia and libraries?, "Library Hi Tech News Volume", 2023, vol. 40 Issue 3.

6. K. Park, Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech, "Irvine Journal of International, Transnational, and Comparative Law". 2021, vol. 77, https://scholarship.law.uci.edu/ucijil/vol6/iss1/5

7. K. Foss-Solbrekk, Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly, "Journal of Intellectual Property Law & Practice", 2021, vo. 16, issue 3.

8. A. Zakon, Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act, Wisconsin Law Review, 2020, issue 5, http://dx.doi.org/10.2139/ssrn.3682048

Krystyna Nizioł

University of Szczecin
Faculty of Law and Administration

Automatic calculation of the probability of an individual's creditworthiness and RODO – conclusions from the analysis of the judgment of the Court of Justice of December 7, 2023, ref. C-634/21

"Article 22(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that the automated establishment, by a credit informa-

tion agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person."

References:

1. Judgment of the Court of Justice of December 7, 2023, ref. C-634/2, https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=91113

Наукове видання

ВИКЛИКИ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

(англійською мовою)

Керівник видавничого проєкту *Віталій Зарицький*
Комп'ютерний дизайн *Олена Щербина*

Підписано до друку 04.07.2024. Формат 60х84 1/16.
Папір офсетний. Друк офсетний. Гарнітура Times New Roman.
Умовн. друк. аркушів – 7,44. Обл.-вид. аркушів – 6,2.
Тираж 300

Видавець і виготовлювач: ТОВ «Видавництво Ліра-К»
Свідоцтво № 3981, серія ДК.
03142, м. Київ, вул. В. Стуса, 22/1
тел.: (050) 462-95-48; (067) 820-84-77
Сайт: lira-k.com.ua, редакція: zv_lira@ukr.net