UDC 342.7
DOI https://doi.org/10.32849/2663-5313/2022.2.16

Oksana Vinnyk,
Doctor of Law, Professor, Corresponding Member of the National Academy of Law Sciences of Ukraine, Chief Researcher, Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of Nationality Academy of Law Sciences of Ukraine, 23-a, Rayevsky str., Kyiv, Ukraine, postal code 01042, ndippp@adamant.net
ORCID: *orcid.org/0000-0002-9397-5127*
Scopus-Author ID: *57217737384*

Vinnyk, Oksana (2022). Digital rights and digital responsibilities amidst war and other threats to social welfare. *Entrepreneurship, Economy and Law*, 2, 101–107, doi https://doi.org/10.32849/2663-5313/2022.2.16

DIGITAL RIGHTS AND DIGITAL RESPONSIBILITIES AMIDST WAR AND OTHER THREATS TO SOCIAL WELFARE

Abstract. ***Purpose.*** The article considers the issue of digital rights and digital responsibilities, which has become especially important in the context of Russian aggression against Ukraine and, accordingly, should be solved to ensure the socially conscious use of digital opportunities.

Research methods. A set of research methods (dialectical, Aristotelian, analysis, prognostic, and others) contributes to analyzing various aspects of the issue concerned (the actual state of use of digital opportunities in war, statutory regulations, the status of theoretical development).

Results. The conclusion on the need to consolidate citizens' digital rights and digital responsibilities, particularly topical in war, in the Constitution of Ukraine relies on the complex nature of digitalization: despite the ample capacity of Internet resources in terms of communication under trying war conditions, assistance (using online payments) to the Armed Forces of Ukraine and citizens suffering from Russian aggression, informing the population about threats and evacuation, etc., the abuse of digital opportunities and irresponsible disclosure in social networks of information used by the enemy against Ukraine (about the location and movement of military equipment, the effects of rocket attacks, etc.) has become extremely dangerous. Although some of such actions (especially dangerous) were recognized as a crime in March 2022, the priority of private interests (regarding the publication of up-to-date information on social networks; a large amount of cryptocurrency mining, which threatens the energy security of the entire community of the city or region) sometimes dominates the interests of the Ukrainian people in the fight against Russian aggressors. Analysis of the current legislation indicates it has gaps concerning citizens' digital rights and digital responsibilities that often lead to the abuse of digital opportunities and protection problems in case of violation of digital rights.

Conclusions. It is proposed to solve the identified issues of legal support for socially responsible use of digital opportunities by eliminating gaps in legal regulation, i. e., supplementing the Constitution of Ukraine with provisions on digital rights and digital responsibilities of citizens. The abovementioned will contribute to the formation of digital citizenship with its inherent social responsibility for the consequences of the use of digital opportunities and, accordingly, will be the basis for determining the specifics of the digital status of participants in certain areas, including economic and environmental.

Key words: digitalization, digital rights, digital responsibilities, Russian aggression against Ukraine, digital abuse, digital citizenship.

1. Introduction

In the modern period, which is often referred to as the era of threats/risks (Beck, 1992), social relations are undergoing significant changes given the aggravation of old ones (environmental pollution, natural and anthropogenic disasters, social disintegration, and the ensuing problem of poverty), the emergence of new threats (coronavirus pandemic, global warming, digitalization risks, including the onset and growth of cybercrime, abuse of digital opportunities), and Russia's aggression against Ukraine since February 24 of this year – super-hazard due to the subsequent destruction of entire cities, the genocide of Ukrainians and humanitarian crisis on the occupied territories, the threat of nuclear pollution due to the capture of nuclear power plants by the occupants (Zaporizhzhia

and Chornobyl), the use of prohibited, incl. chemical, weapons, and the prospect of famine due to the lost opportunity of agricultural land use in the occupied and mine-infested territories by the aggressors... the list is endless.

Therefore, there is a problem of an adequate public response to the mentioned negative phenomena, including the potential of law – legal science, rulemaking and law enforcement which often react late to threats given objective grounds (the rate of changes in social relations related to threats, the complete novelty or suddenness of their emergence, in particular, undeclared war) and subjective circumstances (the inflexibility of state policy towards some issues, the negligence of implementors, hopes for a positive course of affairs). At the same time, the war changed the attitude towards the above threats since it is about the fate of an entire nation: thus, the abuse of digital opportunities to the detriment of the country's defense capacity (disclosure in social networks of information about the transfer, movement, or location of the Armed Forces of Ukraine or other army units formed under the laws of Ukraine, if they can be identified on the ground, and if such information was not posted in the public domain by the General Staff of the Armed Forces of Ukraine, committed under martial law or state of emergency) was recognized as a crime (Verkhovna Rada of Ukraine, 2022) in addition to the warnings (Committee on Digital Transformation, 2022) covering other (not related to the crime) cases of abuse of digital opportunities (Ministry of Defence Ukraine, 2022; Interfax-Ukraine News Agency, 2021).

Certain aspects of the legal issues of society's response to the mentioned dangers have been studied before (in terms of the coronavirus pandemic (Tatsii et al., 2020), digitalization risks (Vinnyk, 2020; Razumkov Center, 2020; Lenz, 2021), including cybersecurity (Bakalinska, Bakalynskyi, 2019; Malysheva, 2021), technogenic security (Kurbanov, 2016; Varenia, 2017), climate change/global warming (Santarius, Pohl, Lange, 2020; Romanko, 2019), and the Russia's war against the Ukrainian people since March 2022 (Ukrainian Association of International Law, National University of Trade and Economics, Crimean Reintegration Association, 2022). However, they still require further research because of their complexity and the new circumstances affecting their (problems') resolution. This is highly relevant to the current threat – war, which causes other dangers: environmental pollution, the lost opportunity for agricultural land use and the resulting lack of food; the hazard of radioactive pollution and the effects of using prohibited weapons (chemical, in particular); the spread of diseases; economic collapse; people's impoverishment due to the loss of housing, work, livelihood...

All these hazards have common features (they imperil social welfare, hence requiring preventive measures towards their occurrence and/or minimization of adverse outcomes, the feasibility of establishing a special legal regime to minimize the effect/consequences of threats), and thus need a comprehensive study, which should also consider the specifics of individual types of threats. The issue of the rights and responsibilities of participants in public life (first of all, citizens) amidst threats plays an important role. This article is a further study of the mentioned problems (Vinnyk, 2021) (with an emphasis on digital rights and digital responsibilities given the changes in public life caused by the war (Ukrainian Association of International Law, National University of Trade and Economics, Crimean Reintegration Association, 2022).

The research relies on the works by Ukrainian (O. Bakalinska, Ya. Kurbanov, N. Malysheva, S. Romanko, N. Varenia, O. Vinnyk and other) and foreign researchers (U. Beck, S. Lenz, L. Pangrazio, T. Santarius and other), general scientific and special methods of scientific cognition, namely: a *dialectical method* made it possible to reveal the essence of digitalization that gave rise to digital rights and digital responsibilities; *the Aristotelian method* allowed identifying those digital opportunities, the use of which in the war can lead to abuses; *analysis* was used in studying the results of domestic and foreign scientific research and the state of legal regulation of the mentioned relations; *a prognostic method* made it possible to determine the potential consequences of abuse of digital opportunities in wartime and formulate proposals on the need to introduce legal mechanisms to prevent/minimize adverse effects of abuses of digital opportunities under any conditions, including the war.

2. The leverage of digital rights and digital responsibilities in war

During Ukraine's large-scale digitalization of all core spheres of social life, particularly in the coronavirus pandemic and the war caused by the Russian aggression (President of Ukraine, 2022), digital rights and responsibilities have been of the most immediate interest. Access to the Internet and related opportunities (online communication, online payments, as well as the provision of monetary support by citizens and organizations to the Armed Forces of Ukraine, assistance to internally displaced persons – due to the war, online consultations on medical, legal, and other issues, official notices of danger and evacuation corridors) has become highly important. Consequently,

the above opportunities should be guaranteed as the rights protected by the Constitution (Verkhovna Rada of Ukraine, 1996) and other laws of Ukraine. In addition, in wartime, the abuse of digital opportunities to the detriment of public interests is extremely dangerous, committed not only intentionally but most often carelessly (for the sake of popularity on social networks) without considering possible negative consequences (publication on social networks of sensitive information which the enemy uses to the detriment of Ukraine, including the location of critical infrastructure, military units, and equipment, etc.).

At the same time, the laws of Ukraine regulating relations in emergency situations (Verkhovna Rada of Ukraine, 2000) and martial law (Verkhovna Rada of Ukraine, 2015), cybersecurity (Verkhovna Rada of Ukraine, 2017) and the Code of Civil Protection of Ukraine (Verkhovna Rada of Ukraine, 2013) guarantee the protection of *constitutional rights*. However, the absence of provisions on citizens' digital rights in the Constitution of Ukraine negatively affects their protection from various kinds of digital abuse, the need to refrain from which is also not enshrined in the Basic Law as a digital duty.

3. The need to enshrine the provisions on citizens' digital rights and digital responsibilities in the Constitution of Ukraine

Amending the Constitution of Ukraine in terms of digital rights and digital responsibilities of citizens will eliminate the above gaps and ensure a higher level of protection of citizens' digital rights and their compliance with digital responsibilities and ultimately will open the way to achieve the social focus of digitalization necessary, not only in emergency and military conditions but also in peacetime.

Therefore, it is proposed to amend the Constitution of Ukraine, supplementing it with a new article "Digital rights and digital responsibilities of citizens" with the following (or similar) content:

"Citizens of Ukraine have digital rights and digital responsibilities, which are determined by the Constitution of Ukraine (basic digital rights and digital responsibilities) and the laws of Ukraine (regarding digital rights and digital responsibilities in a specific area regulated by the relevant law).

Citizens of Ukraine are guaranteed the following digital rights:

– the right to *digital access/the right to Internet access* (everyone has the right to equal access and unowned and secure Internet);

– the right to *freedom of expression* (everyone has the right to freedom of expression and to seek, receive and impart information online);

– *the right to privacy and protection of personal data* (everyone has the right to online privacy and protection of personal data);

– the right to *freedom and personal security/cybersecurity* (the exercise of which includes protection from criminal acts, i. e., legal guarantees of protection from physical and psychological violence or harassment, hate speech, discrimination in the online environment; state promotion of the development and functioning of safe Internet technologies, mechanisms for protection against cyber abuse);

– the right to *use digital democracy tools* to exercise the rights to peaceful assembly, association, cooperation and to participate in the administration public affairs and, accordingly, to freely choose and use any services, websites or applications to create, join, mobilize and to be involved in social groups and associations; any citizen shall have access to the basic public services and shall not be discriminated against due to one's online activity or lack thereof;

– the right to *digital self-determination*, or the right to disconnect from the online world;

– the right to be *protected from unreasonable restrictions on digital rights and digital opportunities* (any restriction on digital rights shall be developed transparently, with the participation of both the state and civil society institutions).

Citizens of Ukraine, exercising their digital rights, are obliged to:

a) refrain from abusing digital rights and digital opportunities;

b) ethically use online materials;

c) report cyberbullying, threats, and other cases of inappropriate use of digital resources;

d) comply with the requirements of personal cybersecurity and restrictions on the use of digital resources in emergency and war situations;

e) adhere to the laws on intellectual property".

The above provisions will maintain so-called digital citizenship (Diana Z, 2020; Pangrazio, Sefton-Green, 2021) towards exercising digital rights and observing digital responsibilities and also stimulate the consolidation of provisions on the specifics of the exercise of digital rights and digital responsibilities in certain areas of public life (economic, environmental, health care, transport, etc.). In fact, it concerns the issue of digital citizenship and the digital status of participants in particular (including the above-mentioned) areas of public life.

4. Digital citizenship

Digital citizenship is a status that all online users should have. This kind of citizenship brings both freedoms and responsibilities that involve the accountable and full use of digital

technologies in the online environment to make it safe for users to cooperate and understand each other. There are several (often nine) elements of digital citizenship, namely:

– *digital access* (access to digital technologies);

– *digital commerce* (purchase and sale and/or order of goods/works/services using the Internet and the related need to solve problems when making online payments);

– *digital communication (communication* on the Internet, which requires empathy and appropriate – socially responsible – reactions from its users);

– *digital literacy* (awareness of online usage rules, which also includes the ability to differentiate between real and fake, useful and harmful content);

– *digital etiquette* (compliance with the rules for using the Internet to avoid conflicts, to exercise not only personal digital freedom but also to respect the rights and legitimate interests of other users);

– *digital* law governing relations in the online environment and which digital citizens need to know (the need for such law is due to the presence in the online environment of both positive and negative interactions. Thus, this implies the need to establish the rules of conduct enshrined in laws and requirements for users of particular social networks);

– *digital rights and responsibilities* (the rules of the online world provide not only rights but also obligations that should be observed to not be held accountable for actions and misconducts in the virtual environment. The Internet can also be used for harmful purposes and anyone needs protection against cyberbullying and cybercrimes, for instance);

– *digital health and wellness* (making use of online resources is a plus, but everyone should be aware of the dangers as well. Users should be taught to protect themselves and others from potential harm);

– *digital security* – a necessary skill in today's digital world, the importance of which is undeniable: viruses and worms can move from system to system and affect the electronic devices used; therefore, users should be aware of potential consequences and malware attacks and, most importantly, learn to prevent them and protect their devices.

5. Conclusions

The introduction of the proposed amendments to the Constitution of Ukraine (although somewhat different from the mentioned theoretical definitions of digital citizenship) should contribute to the protection of digital rights and a responsible attitude to their exercise. It is an essential step towards balanced regulation of digital relations with the prevailing participation of the state, not only self-regulatory entities, as it was declared at the outset of the digital age (Barlow, 1996) and led to the emergence and rapid growth of cyber violations and cybercrime. The state should guarantee balanced consideration of public and private interests in the digital environment (Vinnyk et al., 2021) with the involvement of self-regulatory organizations of digital business and other stakeholders. Ukraine is in urgent need of the modernization of the regulatory framework for enjoying digital rights, both in general terms and given the particularities caused by the military aggression of the Russian Federation (Human rights platform, 2019). Supplementing the Constitution of Ukraine with provisions on digital rights and digital responsibilities will contribute to the formation of digital citizenship with its inherent social responsibility for the consequences of using digital opportunities and, accordingly, will be the basis for determining the specifics of the legal status of participants in certain areas, including economic and environmental.

References:

Bakalinska, O., Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal support of cybersecurity in Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo – Enterprise, Economy and Law*, no. 9, pp. 100–108. Retrieved from: https://doi.org/10.32849/2663-5313/2019.9.17 [in Ukrainian].

Barlow, J. (1996). A Declaration of the Independence of Cyberspace. Retrieved from: https://www.eff.org/cyberspace-independence [in English].

Beck, U. (1992). *Risk society: towards a new modernity*. London; Newbury Park; New Delhi: SAGE Publications, 260 p. Retrieved from: http://www.riversimulator.org/Resources/Anthropology/RiskSociety/RiskSocietyTowardsAnewModernity1992Beck.pdf [in English].

Committee on Digital Transformation (2022). Komitet z pytan tsyfrovoi transformatsii zaklykaie: Ne dopomahaite vorohu. Shcho mozhna y ne mozhna publikuvaty v merezhi Internet? [The Committee on Digital Transformation urges: Do not help the enemy. What can and cannot be published on the Internet?]. *Ofitsiinyi vebportal parlamentu Ukrainy – Official web portal of the Parliament of Ukraine*. Retrieved from: https://www.rada.gov.ua/news/razom/220741.html?search=%D0%86%D0%9D%D0%A2%D0%95%D0%A0%D0%9D%D0%95%D0%A2: [in Ukrainian].

Diana Z (2020). The 9 elements of Digital Citizens our students need to know. Retrieved from: https://blog.neolms.com/the-9-elements-of-digital-citizenship-your-students-need-to-know/ [in English].

Human rights platform (2019). *Svoboda slova v interneti: praktychnyi posibnyk [Freedom of speech on the Internet: practical manual]*. Retrieved from: https://www.ppl.org.ua/bibliotech/3-2 [in Ukrainian].

Interfax-Ukraine News Agency (2021). Na Chernihivshchyni vykryly maininh-fermu, cherez yaku bez vody i svitla mohla zalyshytysia chastyna oblasti [In the Chernihiv region, a mining farm was exposed, through which part of the region could be left without water and light]. Retrieved from: https://ua.interfax.com.ua/news/general/753184.html [in Ukrainian].

Kurbanov, Ya. (2016). Zabezpechennia pryrodno-tekhnohennoi bezpeky v Ukraini i problema vyznachennia poniattia "krytychna infrastruktura" [Ensuring natural and man-made security in Ukraine and the problem of defining the concept of "critical infrastructure"]. *Pivdennoukrainskyi pravnychyi chasopys – South Ukrainian Law Journal*, no. 2, pp. 150–154. Retrieved from: http://dspace.oduvs.edu.ua/bitstream/123456789/1046/1/%D0%9A%D1%83%D1%80%D0%B1%D0%B0%D0%BD%D0%BE%D0%B2%202-2016.pdf [in Ukrainian].

Lenz, S. (2021). Is digitalization a problem solver or a fire accelerator? Situating digital technologies in sustainability discourses. *Social Science Information*, vol. 60, iss. 2, pp. 188–208 [in English].

Malysheva, N. (2021). Kiberbezpeka kosmichnoi diialnosti ta mozhlyvosti yii zabezpechennia zasobamy mizhnarodnoho prava [Cybersecurity of space activities and the possibility of its provision by means of international law]. *Pravova derzhava – Constitutional state*. Kyiv: V.M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine, iss. 32, pp. 245–257 [in Ukrainian].

Ministry of Defence Ukraine (2022). Cherez opryliudnenu informatsiiu bloherom u zvilnenomu seli na Kharkivshchyni pochalosia zahostrennia [Due to the information published by a blogger in the liberated village in Kharkiv region, the aggravation began]. *Ukrainski natsionalni novyny – Ukrainian national news*. Retrieved from: https://www.unn.com.ua/uk/news/1974770-cherez-informatsiyu-blogera-u-zvilnenomu-seli-na-kharkivschini-pochalosya-zagostrennya-minoboroni [in Ukrainian].

Pangrazio, L., Sefton-Green J. (2021). Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference? *Journal of New Approaches in Educational Research*, vol. 9, iss. 2, pp. 15–27. DOI: 10.7821/naer.2021.1.616 [in English].

President of Ukraine (2022). Pro vvedennia voiennoho stanu v Ukraini: Ukaz Prezydenta Ukrainy vid 24 liutoho 2022 r. № 64/2022 [On the imposition of martial law in Ukraine: Decree of the President of Ukraine of February 24, 2022 № 64/2022]. Retrieved from: https://www.president.gov.ua/documents/642022-41397 [in Ukrainian].

Razumkov Center (2020). Tsyfrova ekonomika: trendy, ryzyky ta sotsialni determinanty: dopovid [Digital economy: trends, risks and social determinants: report]. Retrieved from: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf [in Ukrainian].

Romanko, S. (2019). Ekoloho-pravova polityka Ukrainy u sferi zminy klimatu [Environmental and legal policy of Ukraine in the field of climate change]. *Pidpryiemnytstvo, hospodarstvo i pravo – Enterprise, Economy and Law*, no. 9, pp. 88–94. Retrieved from: https://doi.org/10.32849/2663-5313/2019.9.15 [in Ukrainian].

Santarius, T., Pohl, J., Lange, S. (2020). Digitalization and the Decoupling Debate: Can ICT Help to Reduce Environmental Impacts While the Economy Keeps Growing? *Sustainability*, vol. 12, iss. 18, pp. 1–20. DOI: 10.3390/su12187496. Retrieved from: https://d-nb.info/1221184547/34 [in English].

Tatsii, V., Hetman, A., Barabash, Yu., Holovkin, B. (eds.) (2020). Zabezpechennia pravoporiadku v umovakh koronakryzy: materialy panelnoi dyskusii IV Kharkivskoho mizhnarodnoho yurydychnoho forumu [Ensuring law and order in the context of the corona crisis: materials of the panel discussion of the IV Kharkiv international legal forum] (Kharkiv, September 23–24, 2020). Kharkiv: Pravo, 250 p. Retrieved from: http://criminology.nlu.edu.ua/wp-content/uploads/2020/11/4j-forum-2020-zabezpechennya-pravoporyadku-v-umovah-koronakrizi.pdf [in Ukrainian].

Ukrainian Association of International Law, National University of Trade and Economics, Crimean Reintegration Association (2022). Mizhnarodnyi ekspertnyi kruhlyi stil "Deokupatsiia. Yurydychnyi front" [International expert round table "Deoccupation. Legal Front"]. Retrieved from: https://www.youtube.com/watch?v=ALHUgxwVvu4 [in Ukrainian and in English].

Varenia, N. (2017). Pravovi aspekty zabezpechennia tekhnohennoi bezpeky v umovakh zrostaiuchykh zahroz terorystychnoho kharakteru [Legal aspects of technogenic security in the face of growing terrorist threats]. *Materialy V Mizhnarodnoinaukovo-praktychnoi konferentsii "Aktualni pytannia suchasnoi nauky" – Proceedings of the V International Scientific and Practical Conference "Current Issues of Modern Science"* (Ivano-Frankivsk, July 7–8, 2017), in 2 vols. Kherson: Helvetyka, vol. 1, pp. 76–79. Retrieved from: http://molodyvcheny.in.ua/files/conf/other/17july2017/25.pdf [in Ukrainian].

Verkhovna Rada of Ukraine (1996). Konstytutsiia Ukrainy: Zakon Ukrainy vid 28 chervnia 1996 r. № 254к/96-ВР [Constitution of Ukraine: Law of Ukraine of June 28, 1996 № 254к/96-ВР]. *Vidomosti Verkhovnoi Rady Ukrainy – Information of the Verkhovna Rada of Ukraine*, no. 30, art. 141 [in Ukrainian].

Verkhovna Rada of Ukraine (2000). Pro pravovyi rezhym nadzvychainoho stanu: Zakon Ukrainy vid 16 bereznia 2000 r. № 1550-III [About the legal regime of the state of emergency: Law of Ukraine of March 16, 2000 № 1550-III]. *Vidomosti Verkhovnoi Rady Ukrainy – Information of the Verkhovna Rada of Ukraine*, no. 23, art. 176 [in Ukrainian].

Verkhovna Rada of Ukraine (2013). Kodeks tsyvilnoho zakhystu Ukrainy: Zakon Ukrainy vid 2 zhovtnia 2012 r. № 5403-VI [Code of Civil Protection of Ukraine: Law of Ukraine of October 2, 2012 № 5403-

VI]. *Vidomosti Verkhovnoi Rady Ukrainy – Information of the Verkhovna Rada of Ukraine*, no. 34–35, art. 458 [in Ukrainian].

Verkhovna Rada of Ukraine (2015). Pro pravovyi rezhym voiennoho stanu: Zakon Ukrainy vid 12 travnia 2015 r. № 389-VIII [On the legal regime of martial law: Law of Ukraine of May 12, 2015 № 389-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy – Information of the Verkhovna Rada of Ukraine*, no. 28, art. 250 [in Ukrainian].

Verkhovna Rada of Ukraine (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII [On the basic principles of cyber security of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy – Information of the Verkhovna Rada of Ukraine*, no. 45, art. 403 [in Ukrainian].

Verkhovna Rada of Ukraine (2022). Pro vnesennia zmin do Kryminalnoho ta Kryminalnoho protsesualnoho kodeksiv Ukrainy shchodo zabezpechennia protydii nesanktsionovanomu poshyrenniu informatsii pro napravlennia, peremishchennia zbroi, ozbroiennia ta boiovykh prypasiv v Ukrainu, rukh, peremishchennia abo rozmishchennia Zbroinykh Syl Ukrainy chy inshykh utvorenykh vidpovidno do zakoniv Ukrainy viiskovykh formuvan, vchynenomu v umovakh voiennoho abo nadzvychainoho stanu: Zakon Ukrainy vid 24 bereznia 2022 r. № 2160-IX [On Amendments to the Criminal and Criminal Procedure Codes of Ukraine to counteract the unauthorized dissemination of information on the sending, movement of weapons, arms and ammunition to Ukraine, movement, movement or deployment of the Armed Forces of Ukraine or other military formations committed in the conditions of Ukraine martial law or state of emergency: Law of Ukraine of March 24, 2022 № 2160-IX]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2160-20#Text [in Ukrainian].

Vinnyk, O. (2020). Pravovi problemy tsyfrovizatsii v rakursi novykh zahroz dlia suspilnoho blahopoluchchia [Legal problems of digitalization in the perspective of new threats to public welfare]. *Aktualni problemy prava: teoriia i praktyka – Current issues of law: theory and practice*, no. 1(39), pp. 11–18. Retrieved from: https://doi.org/10.33216/2218-5461-2020-39-1-11-18 [in Ukrainian].

Vinnyk, O. (2021). Zahrozy suspilnomu blahopoluchchiu: zavdannia prava [Threats to public welfare: the task of law]. *Pidpryiemnytstvo, hospodarstvo i pravo – Enterprise, Economy and Law*, no. 5, pp. 176–182. Retrieved from: https://doi.org/10.32849/2663-5313/2021.5.30 [in Ukrainian].

Vinnyk, O., Zadykhaylo, D., Honcharenko, O., Shapovalova, O., Patsuriia N. (2021). Economic and Legal Policy of the State in the Field of Digital Economy. *International Journal of Criminology and Sociology*, no. 10, pp. 383–392 [in English].

Оксана Вінник,
доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, головний науковий співробітник відділу міжнародного приватного права та правових проблем євроінтеграції, Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України, вул. Раєвського, 23-а, Київ, Україна, індекс 01042, ndippp@adamant.net
ORCID: *orcid.org/0000-0002-9397-5127*
Scopus-Author ID: *57217737384*

ЦИФРОВІ ПРАВА ТА ЦИФРОВІ ОБОВ'ЯЗКИ В УМОВАХ ВІЙНИ ТА ІНШИХ ЗАГРОЗ СУСПІЛЬНОМУ БЛАГОПОЛУЧЧЮ

Анотація. ***Мета.*** У статті порушується проблема цифрових прав і цифрових обов'язків, що набула особливої ваги в умовах російської агресії проти України та, відповідно, має бути вирішена з метою забезпечення соціально відповідального використання цифрових можливостей.

Методи дослідження. З використанням низки наукових методів дослідження (діалектичного, формально-логічного, аналізу, прогностичного та інших) розглядаються різні аспекти зазначеної проблеми, а саме: фактичний стан використання цифрових можливостей в умовах війни, нормативно-правове регулювання, стан теоретичного розроблення питання.

Результати. Висновок про необхідність закріплення на рівні Конституції України цифрових прав і цифрових обов'язків громадян, що особливо актуально в умовах війни, ґрунтується на складній природі цифровізації. Так, попри значні можливості інтернет-ресурсів щодо спілкування у складних умовах війни, допомоги (завдяки онлайн-платежам) Збройним Силам України та громадянам, що потерпають від російської агресії, інформування населення про загрози та можливість евакуації тощо, особливої небезпеки набули зловживання цифровими можливостями та безвідповідальне оприлюднення в соціальних мережах інформації, що використовується ворогом проти України (про розташування й пересування військової техніки, наслідки ракетних обстрілів тощо). І хоча частину таких дій (особливо небезпечних) у березні 2022 р. було визнано злочином, проте пріоритет приватних інтересів (щодо розміщення актуальної інформації в соціальних мережах, великого за обсягом майнингу криптовалюти, що загрожує енергетичній безпеці цілої громади міста чи області) часом домінує над інтересами українського народу в боротьбі з російськими агресорами. Аналіз

стану чинного законодавства свідчить про наявність у ньому прогалин щодо цифрових прав і цифрових обов'язків громадян, що нерідко призводить до зловживань цифровими можливостями та до проблем із захистом у разі порушення цифрових прав.

Висновки. Виявлені проблеми правового забезпечення соціально відповідального використання цифрових можливостей пропонується вирішити шляхом усунення прогалин у правовому регулюванні, зокрема шляхом доповнення Конституції України положеннями щодо цифрових прав та цифрових обов'язків громадян. Це сприятиме становленню цифрового громадянства з притаманною йому соціальної відповідальністю за наслідки використання цифрових можливостей, а отже, стане основою для визначення специфіки цифрового статусу учасників відносин у певних сферах, включно з економічною та екологічною.

Ключові слова: цифровізація, цифрові права, цифрові обов'язки, російська агресія проти України, цифрове зловживання, цифрове громадянство.

The article was submitted 11.03.2022
The article was revised 01.04.2022
The article was accepted 22.04.2022