

Restrictions of Russian Internet Resources in Ukraine: National Security, Censorship or Both?¹

Olga Shumilo Tanel Kerikmäe **Archil Chochia**

TalTech Law School. Tallinn University of Technology Akadeemia tee 3. Tallinn 12618. Estonia E-mail: olshum@taltech.ee E-mail: tanel.kerikmae@taltech.ee E-mail: archil.chochia@taltech.ee

Abstract: In this paper, the authors analyse the ambiguous political decision to ban the major Russian web resources from access to the Ukrainian market, in spite of heavy criticisms from local and foreign experts. While the supporters of the new internet policy claimed the new strategy to be coherent with cybersecurity priorities of the country, the opponents pointed out a set of legal and political limitations. Drawing on the setting and results of taking a new approach to information policy, we describe the fragility of Euromaidan democratic heritage and drawbacks of the current political regime. The logical method of legal interpretation has been applied to analyse the controversies of the current legislation on Russian internet resources restriction. The article concludes that Ukrainian post-Euromaidan governance model needs to consolidate the efforts in order to prove the commitment to freedom of speech as a core European value and replace spontaneous actions with an evidence-based approach to political decision-making.

Keywords: censorship, cybersecurity, Euromaidan, internet freedom, policymaking, Revolution of Dignity, Russia, social networks, troll fabrics, Ukraine

This research was supported by a Marie Curie Research and Innovation Staff Exchange scheme within the H2020 Programme (grant acronym: SHADOW, no. 778118).

1. Introduction

The dexterous use of disruptive digital technologies has been exploited in the major climactic political shifts: Twitter and Facebook served as platforms for exposing political protest and critique of the 'elites' from the Middle East 'Arab Spring' to the 'Trump vote' of the United States, and protests against the kleptocratic Yanukovych regime in Ukraine in 2013 were no exception to the new millennium trend (Kerikmäe et al., 2017, pp. 27–42). The initial alarm call for protest, now carved in stone on the main square of the Ukrainian capital, was posted on the personal Facebook page of the investigative journalist and popular blogger Mustafa Navyem, leaving all the subsequent events for history. According to the survey of Euromaidan online supporters, carried out by O. Onuch (2015), both self-identified as Russians and Ukrainians named Facebook digital tool no. 1 to get in touch and coordinate their actions. The choice in favour of the western platform as the main communication channel was not random—although Russian VKontakte (international name—VK), the most popular Ukrainian social network at the time, was rarely regarded as an "online nest" for leading pro-European influencers, it still kept top positions for entertainment, political advertising and digital marketing. Even the former President of Ukraine, Petro Poroshenko, and his allies in the government, used to have "verified" pages in the *VKontakte* domain.

However, in May 2017, the Russian Facebook analogue was suddenly banned for three years by a decree signed by the President of Ukraine, along with a number of other Russian "big fish" internet companies—Yandex (search engine), Mail.ru (mail host) and others, with a total sanction list of 450 companies and 1,200 persons. This decision had been advocated by the President and explained by the urge to resolve cybersecurity challenges as well as economic reasons to cut the profits of Russian-based corporations, but still ended up in the vortex of heated debates on its legality and practicability.

The main issue is whether such a ban is in accordance with freedom of expression. Like many human rights and freedoms, freedom of expression is not an absolute right (Kerikmäe & Nyman-Metcalf, 2012, pp. 35–51). Article 10 of the European Convention on Human Rights permits different kinds of limitations, including formalities (such as licensing), conditions, restrictions or penalties, prescribed by law and necessary in a democratic society to protect valuable interests. The applicability of exceptions has been concretised by case law by the European Court on Human Rights (ECtHR).²

² The ECtHR produces regular reports on its case law related to different Articles of the ECHR, see, e.g., ECtHR, 2015.

Concerning the methodology, this article traces Ukrainian government's justifications to adapt more restrictive information and cybersecurity policy in 2017 and analyses the consecutive decision to ban Russian digital giants through the lens of logical method of legal interpretation, i.e., checks the coherence of the regulation with other binding legal acts, particularly the Constitution of Ukraine.

2. Internet and media freedom in Ukraine

The protests against Viktor Yanukovych, the rapidly expanding power of his clan and prioritising cooperation with Russia over the EU Association Agreement, were also instigated by the continuing pressure on free media, especially TV channels, which remained the main instrument of all political communication campaigns since the country gained independence. The almost unanimous loyalty of public broadcasting companies to the ex-President was easily explained by the deal he had concluded with their stakeholders, which left the cable TV and social networks to be the main instrument for censorship-free reflections on the situation within the country. The situation for media freedom in Ukraine as compared with other Eastern Partnership³ countries is that Ukraine is more or less in the middle. It is placed after Georgia, Moldova, Armenia but ahead of Azerbaijan and Belarus (Reporters without Borders, 2019).

As of 2013, Russian Facebook lookalike *VKontakte* used to be the most popular social media platform in the country, leaving the American original far behind and owing the success to free music and cinema hosting along with simple marketing tools for small and medium businesses. On the peak of hostilities in Donbas, in August 2014, the number of Ukrainian accounts in *VKontakte* reportedly reached 27 million, while *Odnoklassniki* (another social network, targeted at school alumni) gathered 11 million, and only 3 million of Ukrainians signed up for Facebook (Yandex, 2014). Russian search engine *Yandex* used to second Google by popularity with 8.5 million of visits versus 12.8 million in 2014 (Gemius Global, 2014). When the first protests stroke Kyiv streets, *VKontakte* and *Odnoklassniki* were utilised both by the protesters and their counterparts to mobilise the audience, instantly message friends, launch flashmobs, etc. Changing the avatar to a black square would symbolise mourning over the Heavenly Hundred and sympathy for the Euromaidan movement, while adding a St. George's ribbon would be a bold anti-Maidan statement. The

For more on Eastern Partnership, please see Kerikmäe & Chochia (2016).

communities for sharing the needs of protesters and keeping up the spirit have been organised on all platforms though—mostly on *VKontakte* and Facebook. This trend has been exemplified by Schreiber and Kosienkowski (2015), through the interviews with Russian-speaking Ukrainians from the Eastern part of the country, who formed pro-Euromaidan online communities in *VKontakte* and *Odnoklassniki*, and some deliberately opted for Russian language of communication in order to avoid isolating the liberal agenda in the Ukrainian-speaking segment of *Facebook*.

When the Revolution of Dignity leaders successfully ousted the Yanukovych government, the Kremlin immediately followed with a full-scale military occupation of Crimea, inciting "Russian Spring" protests in the Southern and Eastern regions, and massive informational campaigns on its state-owned TV channels, actively developing the narratives of "civil unrest", "voluntary referendum of Crimea" and "the coup of ultra-nationalist powers" to describe the events in Ukraine (Sayapin & Tsybulenko, 2018). The motivation to minimise the influence of propaganda has led the interim government of Ukraine to the first freedom of speech restriction—blocking the broadcasting of Russian cable TV channels throughout the country in March 2014. This decision, approved by the National Broadcasting Council, was supported by the majority of the population, but at the same time helped the opponents of the government to shape the image of the "authoritarian nationalist rule" that "oppresses" opposition forces. As a result, those unhappy with the new rule and switching back to the pro-Western agenda, became even more eager to connect with their like-minded peers through Russophone social media networks, where you could both be heard by friends and followers, but also hide your identity and remain voluntarily anonymous. The anti-Maidan community in VKontakte has managed to unite a quarter million of supporters in March 2014 (Kozachenko, 2014) and transform the wave of post-Soviet nostalgia, homophobia, anti-Semitist and "anti-fascist" narratives into an influential collective identity, a channel of mythcreation and spreading fake news for the Russophone opponents of the new Ukrainian government. According to the Head of Security Services of Ukraine, by 2017, the number of anti-Maidan analogues had reached 800, which anyhow did not raise any national-level initiatives to block the respective platforms they were operating on until then.

3. Saying no to Russian web resources: cybersecurity or voluntarism?

The disruptive influence of Russian "troll factories" on global politics has turned into a major theme of public discourse after the astonishing result of the 2016 presidential elections in the United States, which has been strongly associated, yet not proved, with the external assistance of fake political communities and anti-liberal propaganda, organised from overseas. Since its beginning, the conflict in Ukraine has been on the frontline of informational campaigns from both parties, and the importance of social network activism could not be overestimated in the case, at the time when traditional media started losing their mainstream status, especially among youngsters. Russia has engaged in information warfare in Ukraine in more or less open ways. Television has been used but with the increasing importance of the social media, as a lot of the campaign takes place there. It has been shown that internet trolls (Lange-Ionatamishvili & Svetoka, 2015, p. 110) have been used to spread propaganda. The New York Times, Novaya Gazeta and other magazines have collected credible proofs of state-sponsored "troll bots" in Olgino and other alternatives through which Russian government would create fake stories about such public figures as Putin, Trump and Poroshenko (see, e.g., MacFarquhar, 2018). Despite being divided, the civil society of Ukraine has been very consistent in counteracting online disinformation campaigns and multiplied the efforts to prevent the manipulations of public opinion on the annexation of Crimea and military aggression in Donbas area on all major social media platforms.

Since 2014, Ukraine has introduced wide economic sanctions against Russia, later supported by the EU and the US, aimed to posit a pressure on the state budget of the country, and to stop the collaboration in the arms industry. Meanwhile, the idea to ban Russophone online platforms came out of the blue for most experts, as three years into the conflict, digital media were widely used by different parties, influencers and other people for private purposes. However, on May 15, the President of Ukraine, while acting as the head of National Security and Defense Council of Ukraine, signed a decree blaming the Russian-owned resources to be a threat to national interests in political and economic sense and ordered national IT providers to stop supporting internet connection to the listed websites. This act has also been supported by the Secretary of National Security and Defense Council, Oleksandr Turchynov, who earlier expressed hope to defend the principal frontline of hybrid war—the (dis)informational battlefield (Turchynov, 2016).

Immediate reaction from national and global opinion leaders was mostly harsh and only few experts named the decree adequate and proportionate, especially given the framework where Ukraine postulates itself as an opposite to Russia, a censorship-free country. Although the desire to take action against propaganda is well understood and legitimate, the adoption of bans on media is nevertheless problematic. Thorbjørn Jagland, the Secretary-General of the Council of Europe, has expressed his concerns about the ban as disproportional and informed Ukrainian counterparts about the inconsistency of this decision with the common understanding of shared European values—freedom of speech and free press (*The Economist*, 2017). Human Rights Watch Ukraine urged the incumbent President to cancel the Russian online media block and abstain from the attempts to pervasively influence the public discourse in Ukraine (*Human Rights Watch*, 2017).

The public perception of banning Russian web resources has immediately divided the society into supporters and opponents with a considerable regional bias. According to the survey conducted by the Democratic Initiatives Fund, in total, only 28% of Ukrainians supported the President, while 53% were unhappy with the digital blockade; anyhow, in Western Ukraine the initiative to defend national cybersecurity was supported by the majority of respondents (40%), although over one third (35%) would still like to enjoy free access to Russian websites despite the threats (DIF, 2017). Later, numerous monitoring surveys and research showed that in spite of a large migration to Facebook, Google and Gmail services, millions of Ukrainian users easily skip the ban through VPN tools. In 2019, the new President of Ukraine Volodymyr Zelensky expressed his doubts on the reasonability of the ban on Russian web resources, and an interest to collect experts' feedback on the results and further perspectives of the blockade.

4. Legal implications

Striking the balance between national security and freedom of speech has been one of the most debated areas for practitioners and researchers, and Ukraine has demonstrated different approaches to solving the challenge. Anyhow, the decree of National Security and Defense Council has been clearly formulated outside the Ukrainian legal framework, and even perceived to be illegitimate according to Viktoriya Siumar, head of Parliamentary Committee on the Freedom of Speech and Informational Policy (Interfax, 2017). What are the arguments the experts and politicians refer to?

Firstly, the text of the Decree could be summarised to a direct unequivocal order to all the internet providers of Ukraine to block a list of websites which imposed a threat to national cybersecurity, aiming to extend the list of entities under "personal" sanctions, as foreseen by the Law of Ukraine 'On sanctions' (2014), which does not require any additional approval from the Parliament. This position clearly fails to comply with the procedure, as according to the aforementioned Law on sanctions, "personal sanctions" are those applied to "foreign legal entities, legal entities controlled by a foreign legal entity or a non-resident individual, foreigners, stateless persons, as well as subjects engaged in terrorist activities", while sectoral sanctions are targeted at "a foreign state or an uncertain circle of persons of a certain type of activity". The latter, according to Article 5, can be introduced by the President of Ukraine, but later have to be approved by the Parliament in 48 hours upon issuing the decree, which did not take place.

Secondly, the role of the National Security and Defense Council in the Constitution of Ukraine is defined as "coordination and control over the executive authorities", and the respective law prescribes that the acts issued by this authority are mandatory only for *public authorities*. Since internet providers can hardly be classified as public authorities, the issue of their obedience to the ban also remains unclear.

Thirdly and most importantly, pursuant to Art. 92 of the Constitution of Ukraine, fundamental human rights and freedoms and their guarantees can be regulated exclusively by the laws of Ukraine. Access to social networks, search engines and mail services are forms to enjoy the freedom of speech, the right to entrepreneurial activity, to maintain private correspondence, etc. Hence, limiting access to a considerable share of most popular websites could only be put into effect by the Parliament, and thus should be regarded as illegitimate even if it was strongly supported by the society.

These and other arguments have been listed in the unsuccessful lawsuit of a Kyiv student to the Supreme Administrative Court of Ukraine (2017), and the online petition to the President to lift the ban on *VKontakte*, which gathered over 25,000 votes. In response to the request, the President replied with describing the social network as a refuge for Russian-sponsored disinformation campaigns, pirate content and communities inciting teen suicides ("Blue Whales"), which sounds unpersuasive especially considering the fact that the latter are no more than a fresh urban legend, hyped on a wave of moral panic (Mukhra *et al.*, 2017; Napiorkowski, 2017). Another reason given was cutting the economic benefit that Russian companies receive through online advertising in Ukraine,

but even the approximate numbers of the profits lost both by the Moscowbased websites and Ukrainians who used to advertise their goods and services on these platforms have not been revealed. Finally, while regulating online communication, one should always remember that the existing social networks and communities are not fully operating institutions of social life, but rather less controlled replications from the real life, hence they can be easily transformed in an "eligible" online place, e.g., Facebook.

Fourthly, the Ukrainian legal system also recognises the practice of the European Court of Human Rights (hereinafter ECtHR) as a secondary source of legislation, which also contradicts with the strategy undertaken towards internet policy in 2017. The ECtHR practice highlights the importance of careful consideration for each incident of suspected national security threat in the case of *Christian* Democratic People's Party v. Moldova [2010]. In the latter, the representatives of the opposition were supported by the Court in the claim that the Government of Moldova had breached Article 10 of the Convention when limiting their activities for sharing slogans "Down with Putin's occupation regime", defined as "calls to a violent overthrow of the constitutional regime and to hatred towards the Russian people". The ECtHR explained that even if these mottos would be coupled with burning flags or portraits of Russian leaders, they still "should be understood as an expression of dissatisfaction and protest" and refused to consider these actions a "call to violence". This logic seems to be somewhat applicable to the case of Russian online resources as well—if some malicious communities or single users clearly aim to manipulate public opinion with fake news, while others simply express negative feedback or support for the government, each case of cybersecurity threat should be considered individually by a respective agency (security service or a special cyber security police department). Yet, the supreme executives seemed to consider cutting out the whole segment of the internet a simpler approach, although its results (especially losing scores in foreign relations) remind either of a failure to follow the proverb "don't throw the baby out with the bathwater", or of a disguise to cover another political goal.

From the viewpoint of the best international practice, as supported by the ECtHR, any limits on media freedoms need to be based on law, proportional and necessary in a democratic society as interpreted in the specific case. Even in situations of challenges to security, like for example disputed territories, freedom of expression should be protected unless some specific limitation is necessary for a concrete, identified reason—and normally for a limited time. This was shown in the case of *Cyprus v. Turkey* [2001], where—although all alleged restrictions were not fully proven—the court did condemn limits on freedom of expression, even if the content was against the government in power

and seen by them as a security risk. The case of (Grand Chamber) *Catan and others v. Moldova and Russia* [2012] concerned the occupation of Transnistria from a perspective of culture, primarily education, and implicitly showed that media (including minority media) must be allowed to operate freely even in occupied territories. The internet is seen by some commentators not only as another media channel, but as an essential engine of development (Kelychavyi & Nyman Metcalf, 2019). Use of internet can promote a positive change in all sectors of the economy (Kerikmäe *et al.*, 2018, pp. 91–112). Together with different forms of communication, the internet contributes to the economic viability of states (Schwartz, Satola & Bustani, 2001, especially at pp. 488–490). Also, according to a latest study, free access to social media enhances democracy in the developing states (Jha & Kodila-Tedika, 2019).

This leads us to the following question: Why and how was it possible for the former President and his allies to adopt this decision without wide public consultations and in breach of Ukrainian legislation, which has later not been altered neither in parliament nor in court? In our view, the underlying motivation for the blockade could be the start of presidential elections campaign of 2019. A year later, the then President kicked off the race to keep the chair under the motto "The army, the language, the faith", appealing to his personal achievements in a conservative discourse. Thus, the blocking of Russian networks and resources would be fitting the security-prone national strategy, where building a liberal multicultural society would come second to protecting the country from external challenges to its physical and online borders. Due to the slow pace and low-score achievements of the judicial reform, the court system of the time is considered to be a weak, President-dependent player, functioning in a 'republic of clans', a term coined with regard to Ukraine by a prominent philosopher M. Minakov (2019).

According to Peter Drucker, culture eats strategy for breakfast (Cave, 2017), and it could not be truer for policymaking in many developing and post-Soviet states. Unfortunately, as we can see in the case of introducing restrictions on Russian websites, the decision makers have skipped the main steps of evidence-based policy and introduced a decree rather aimed at future individual political benefits than a holistic systematic approach to solving external cybersecurity challenges. Despite the parliamentary-presidential form of governance, the role of the President in Ukrainian politics is far-reaching and in the examined case neither the other branches of power and mass media nor the negative feedback from strategic Western partners prevented the head of state from adopting a controversial decision as a preparation step for building his re-election campaign. Thus, the sustainability of the current internet policy can be considered as vague and probably subject to review in case of changing the elites.

Many have said that truth is the first casualty of war. The worse the crisis that a state faces, the more tempting it is to keep information space restricted and controlled. Creating or maintaining trust in information is very challenging in a crisis (Nyman Metcalf, 2018). Propaganda and various other actions to creating confusion, shaping opinion and inflicting damage are important weapons of conflict (Lewis, 2015, pp. 39–40). This is becoming more and more important as so much of our lives happen on social media channels (Levin Jaintner, 2015, p. 88).

5. Conclusions

Open communication is the heart of democracy. The rise of primitive political propaganda and disinformation campaigns has imposed a challenge for democracies all over the world, and each country has presented its own solution on how to strike a sensitive balance between securing national sovereignty and guaranteeing the freedom of speech. While the EU upholds liberties and the Russian government has used the trend to limit the internet freedom even more, Ukrainian government had claimed to follow a liberal agenda but still adopted a controversial decision on banning Russian social media.

Based on the findings about the legitimacy of the lack of decision and flaws in policy-making procedure, we can conclude that the current strategy did not achieve the expected primary result of reducing the amount of disinformation on the web, as "troll factories" remain active on other digital platforms, which was proved during the presidential and parliamentary elections in 2019. Maintaining the presence of Russian web resources, in our view, could not only demonstrate the country's respect towards the freedom of speech, but also facilitates the engagement of more people in democratic pro-Ukrainian agenda. Also, in order to counter disinformation campaigns, the government could consider the proportionate regulatory approaches of Finland and the UK, namely, to ensure that accurate legal information is publicly available, to promote digital media literacy skills, and to enforce penal legislation on prohibiting hate speech and incitement to violence.

Dr. **Olga Shumilo** is a doctoral student at the TalTech Law School of Tallinn University of Technology, writing her thesis on the issues of legal framework for smart cities. At TalTech Law School, she is teaching courses on penal and administrative law, and has contributed

to several publications in the field of European Union law. Olga has obtained her master's degree (cum laude) and first doctoral degree at Yaroslav Mudryi National Law University (Kharkiv, Ukraine) in criminal law and criminology.

Prof. Dr. **Tanel Kerikmäe** is a full professor of law who is currently head of the TalTech Law School and a foreign member of the National Academy of Legal Sciences of Ukraine. He has recently been a project leader for the government office project on the legal strategy of artificial intelligence. He established a European Union legal and policy research group of that received significant funding from the EU Commission (H2020, Jean Monnet Centre of Excellence), NATO, Folke Bernadotte Academy, USAID, etc. Many of these grants are focused on developing legal digital skills as a tool for European integration. Prof. Kerikmäe has edited several books (published by Springer, Ashgate, Kluwer, Oxford and Cambridge publishers) such as *Brexit: History, Reasoning and Perspectives* (2018); *The Law of the Baltic States* (2017); *Political and Legal Perspectives of the EU Eastern Partnership Policy* (2016); *Regulating eTechnologies in the European Union* (2016) and *The Future of Law and eTechnologies* (2016). His recent research areas relate to the artificial intelligence and law and other law & tech issues.

Dr. **Archil Chochia** is a researcher at the TalTech Law School of Tallinn University of Technology. Dr. Chochia obtained his doctoral degree from Tallinn University of Technology in 2013, and has previously studied at the University of Scranton, the Tbilisi State Medical University, the University of California, the Pepperdine University and the Harvard University. He has more than 70 academic publications as articles in peerreviewed academic journals, chapters in books, doctoral dissertation and conference papers. He is a co-editor of the books *Political and Legal Perspectives of the EU Eastern Partnership Policy* (Springer, 2016) and *Brexit: History, Reasoning and Perspectives* (Springer, 2018). Archil Chochia is a Senior Fellow of Weinstein International Foundation.

References

Catan and others v. Moldova and Russia [2012], ECtHR, nos. 43370/04, 8252/05 and 18454/06.

Cave, A. (2017), 'Culture eats strategy for breakfast. So what's for lunch?' *Forbes*, 9 November. Retrieved from https://www.forbes.com/sites/andrewcave/2017/11/09/culture-eats-strategy-for-breakfast-so-whats-for-lunch/#2d578d707e0f [accessed 29 Apr 2019]

Christian Democratic People's Party v. Moldova (no. 2) [2010], ECtHR, no. 25196/04. Cyprus v. Turkey [2001], ECtHR, no. 25781/94, especially para. 248 onwards.

DIF (2017), Vizy ta obmezhennia rosiiskoho vplyvu v Ukraini – hromadska dumka [Visas and restrictions on Russian influence in Ukraine – a survey], The Ilko Kucheriv

- Democratic Initiatives Foundation, 30 June. Retrieved from https://dif.org.ua/article/vizi-ta-obmezhennya-rosiyskogo-vplivu-v-ukraini-gromadska-dumka [accessed 29 Apr 2019]
- ECtHR (2015), 'Internet: case-law of the European Court of Human Rights,' June 2015 update, Council of Europe, European Court of Human Rights. Retrieved from http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf [accessed 29 Apr 2019]
- Gemius Global (2014), 'Ukrainian users prefer Google to Yandex,' 2 December. Retrieved from https://www.gemius.com/agencies-news/ukrainian-internet-users-prefer-google-to-yandex.html [accessed 29 Apr 2019]
- Human Rights Watch (2017), 'Ukraine: revoke ban on dozens of Russian web companies,' 16 May. Retrieved from https://www.hrw.org/news/2017/05/16/ukraine-revoke-ban-dozens-russian-web-companies [accessed 29 Apr 2019]
- Interfax (2017), 'Siumar: Blokuvannia Internet-resursiv ne robyt chesti Ukraini, ale v informviini tsei krok mozhna zrozumity' [Siumar: Blocking internet resources does not honour Ukraine, but in the infowar, this step can be understood], 16 May. Retrieved from: https://ua.interfax.com.ua/news/political/421874.html [accessed on 28 Apr 2019]
- Jha, C. K. & Kodila-Tedika, O. (2019, in press), 'Does social media promote democracy? Some empirical evidence,' *Journal of Policy Modeling*. https://doi.org/10.1016/j.jpolmod.2019.05.010
- **Kelychavyi, B. & Nyman Metcalf, K.** (2019), 'Is internet access a matter of freedom of expression? Some examples from Ukraine,' *Baltic Journal of European Studies*, vol. 9, no. 3(28), pp. 63–81. https://doi.org/10.1515/bjes-2019-022
- **Kerikmäe, T. & Chochia, A.**, eds. (2016), *Political and Legal Perspectives of the EU Eastern Partnership Policy*, Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-27383-9
- **Kerikmäe, T.; Hoffmann, T. & Chochia, A.** (2018), 'Legal technology for law firms: determining roadmaps for innovation,' *Croatian International Relations Review*, no. 24(81), pp. 91–112. https://doi.org/10.2478/cirr-2018-0005
- Kerikmäe, T.; Müürsepp, P.; Särav, S. & Chochia, A. (2017), 'Ethical lawyer or moral computer historical and contemporary discourse on incredulity between the human and a machine,' Вісник Національної академії правових наук України/Journal of the National Academy of Legal Sciences of Ukraine, no. 2(89), pp. 27–42.
- **Kerikmäe, T. & Nyman Metcalf, K.** (2012), 'Less is more or more is more? Revisiting universality of human rights,' *International and Comparative Law Review*, vol. 12, no. 1, pp. 35–51. https://doi.org/10.1515/iclr-2016-0077
- **Kozachenko, I.** (2014), 'How social media transformed pro-Russian nostalgia into violence in Ukraine,' *The Conversation*, 16 October. Retrieved from: https://

- theconversation.com/how-social-media-transformed-pro-russian-nostalgia-into-violence-in-ukraine-33046 [accessed 29 Apr 2019]
- **Lange-Ionatamishvili, E. & Svetoka, S.** (2015), 'Strategic communications and social media in the Russia–Ukraine conflict,' in K. Geers (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, Tallinn pp. 103–111.
- Law of Ukraine 'On sanctions' (2014), "*Pro sanktsii*", *Zakon Ukrainy*, 14.08.2014. Retrieved from https://zakon.rada.gov.ua/laws/show/1644-18 [accessed 28 Apr 2019]
- **Levin Jaintner, M.** (2015), 'Russian information warfare: lessons from Ukraine,' in K. Geers (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 87–94.
- **Lewis, J. A.** (2015), 'Compelling opponents to our will: the role of cyber warfare in Ukraine,' in K. Geers (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 39–47.
- **MacFarquhar, N.** (2018), 'Inside the Russian troll factory: zombies and a breakneck pace,' *The New York Times*, 18 February. Retrieved from https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html [accessed 29 Apr 2019]
- **Minakov, M.** (2019), 'Republic of clans: the evolution of the Ukrainian political system,' in B. Magyar (ed). *Stubborn Structures: Reconceptualizing Post-Communist Regimes*, Budapest: CEU Press, pp. 217–245.
- Mukhra, R.; Baryah, N.; Krishan, K. & Kanchan, T. (2017), "Blue Whale challenge': a game or crime?" *Science and Engineering Ethics*, vol. 25, no. 1, pp. 285–291. https://doi.org/10.1007/s11948-017-0004-2
- Napiórkowski, M. (2017), 'Niebieski wieloryb. List z Ministerstwa Edukacji Narodowej' [Blue Whale. Letter of the Ministry of National Education], *Mitologia Współczesna*, 21 March. Retrieved from http://mitologiawspołczesna.pl/niebieski-wieloryb-listministerstwa-edukacji-narodowej/ [accessed 29 Apr 2019]
- Nyman Metcalf, K. (2018), 'Post-conflict reconstruction of trust in media,' in S. Sayapin & E. Tsybuluneko (eds.) *The Use of Force against Ukraine and International Law*, The Hague: Springer, pp. 425–445. https://doi.org/10.1007/978-94-6265-222-4_20
- **Onuch, O.** (2015), 'EuroMaidan protests in Ukraine: social media versus social networks,' *Problems of Post-Communism*, vol. 62, no. 4, pp. 217–235. https://doi.org/10.1080/10758216.2015.1037676
- Reporters without Borders (2019), *Index Details: Data of Press Freedom Ranking 2019*. Retrieved from: https://rsf.org/en/ranking_table [accessed 12 Apr 2019]
- **Sayapin, S. & Tsybulenko, E.**, eds. (2018), *The Use of Force against Ukraine and International Law*, The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-222-4

- Schwarz, T.; Satola, D. & Bustani, C. (2001), 'Telecommunications reform in emerging markets,' in I. Walden & J. Angel (eds.) *Telecommunications Law*, London: Blackstone Press, pp. 488–529.
- Supreme Administrative Court of Ukraine (2017), Rishennia Vyshchoho Administratyvnoho Sudu Ukrainy u spravi za pozovom do Prezydenta Ukrainy pro vyznannia protypravnymy i nechynnymy pp. 11 p. 422, pp. 11 p. 423, pp. 11 p. 424, pp. 11 p. 425 dodatka do rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2017 roku "Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii)", vvedenoho v diiu Ukazom Prezydenta Ukrainy vid 15 travnia 2017 roku no. 133/2017, [Judgement of the Supreme Administrative Court of Ukraine on a lawsuit to the President of Ukraine on the recognition of clause 11 Section 422, clause 11 Section 423, clause 11 Section 424, clause 11 Section 425 of the Annex to the decision of the National Security and Defense Council of Ukraine dated April 28, 2017 'On the application of personal special economic and other restrictive measures (sanctions)', enacted by the Decree of the President of Ukraine dated May 15, 2017 no. 133/2017 unlawful and ineffective]. Retrieved from http://www.vasu. gov.ua/archive/123793/ [accessed 12 Apr 2019]
- **Surzhko-Harned, L. & Zahuranec, A. J.** (2017), 'Framing the revolution: the role of social media in Ukraine's Euromaidan movement,' *Nationalities Papers*, vol. 45, no. 5, pp. 758–779. https://doi.org/10.1080/00905992.2017.1289162
- *The Economist* (2017), 'Ukraine bans its top social networks because they are Russian,' 19 May. Retrieved from https://www.economist.com/europe/2017/05/19/ukraine-bans-its-top-social-networks-because-they-are-russian [accessed 29 Apr 2019]
- The Guardian (2011), 'Who coined the phrase, 'The first casualty of war is truth'?' Retrieved from https://www.theguardian.com/notesandqueries/query/0,5753,-21510,00.html [accessed 29 Apr 2019]
- **Turchynov, O.** (2016), Natsionalna bezpeka Ukrayiny: vyklyky ta priorytety [National security of Ukraine: challenges and priorities], *Holos Ukrayiny*, 17 August. Retrieved from http://www.golos.com.ua/article/274453 [accessed 29 Apr 2019]
- Yandex (2014), 'Ogljad sotsialnykh merezh i Tvittera v Ukrayiny' [Review of social media and Twitter use in Ukraine]. Retrieved from http://cache-mskm908.cdn.yandex.net/download.yandex.ru/company/Yandex_on_UkrainianSMM_Summer_2014.pdf [accessed 12 Apr 2019]