Human Rights in The Context of Digitalization. International-Legal Analysis

Liydmyla Panova[1], Ernest Gramatskyy[2], Inha Kryvosheyina[3], and Volodymyr Makoda[4],

Taras Shevchenko National University of Kyiv[1,2,3,4],
Kyiv, Ukraine

Summary

The use of the Internet has become commonplace for billions of people on the planet. The rapid development of technology, in particular, mobile gadgets, has provided access to communication anywhere, anytime. At the same time, there are growing concerns about the behavior of people on the Internet, in particular, towards each other and social groups in general. This raises the issue of human rights in today's information society. In this study, we focused on human rights such as the right to privacy, confidentiality, freedom of expression, the right to be forgotten, etc. We point to some differences in this regard, in particular between the EU, etc. In addition, we describe the latest legal regulation in this aspect in European countries. Such methods as systemic, factual, formal and legal, to show the factors of formation and development of human rights in the context of digitalization were used. The authors indicate which of them deserve the most attention due to their prevalence and relevance. Thus, we concluded that the technological development of social communications has laid the groundwork for a legal settlement of privacy and opinion issues on the Internet. Simultaneously, jurisdictions address issues on every aspect of human rights on the Internet, based on previous norms, case law, and principles of law. It is concluded that human rights legislation on the Internet will continue to be actively developed to ensure a balance of private and public interests, safe online access and unimpeded access to it.

Key words:

human rights, right to be forgotten, protection of personal data, privacy, hate speech.

1. Introduction

The digital environment promotes democracy by allowing citizens to criticize and discuss social issues on the Internet, stay abreast of events, follow political leaders, communicate with others, represent themselves, etc. (Sagan & Leighton, 2010; Eakin, 2015; Kneuer, 2016). With the development of digital media and the Internet, more people have the opportunity to consume information of an educational, scientific, and cultural nature, to develop a worldview (Selwyn, Gorard, & Furlong, 2006; Szymkowiak, 2016).

At the same time, barriers and denials of access to information and communication via the Internet significantly reduce a person's ability, which can be seen as restricting his or her right to information and freedom of expression (Tăbușcă, 2010; Tully, 2014; Reglitz, 2020). In addition, the security of personal data is another problem that has arisen with the development of digital technologies (Voigt & von dem Bussche, 2017). For example, it is no longer news that search engines and sites that receive personal information, using computational algorithms and storing large amounts of data, may know more about you than you do, in addition to having accurate information about your preferences, the time you spend on viewing specific content and so on (Hasan, Morris, & Probets, 2009). Taken together, the use of modern digital technologies via the Internet is a powerful tool for influencing individuals and society, which is a matter of concern as to how these technologies will be used (Chen et al., 2015; Milan, 2015; DeVito, Gergle, & Birnholtz, 2017).

Anonymity, combined with inclusiveness, is a threat to a person's social well-being, as anyone can register on a social network and leave offensive comments to you if you do not limit other people's ability to leave comments on your page (Lapidot-Lefler & Barak, 2012; Moore, Nakano, Enomoto, & Suda, 2012; Rainie, 2013). In the case of a popular person with a large number of subscribers, the amount of offensive content that is conventionally labeled as hate speech, harsh or offensive language can reach thousands (Holmes & Redmond, 2012; Modha, Majumder, Mandl, & Mandalia, 2020). In this regard, the abolition of cancel culture is the subject of a separate debate (Ng, 2020). Freedom of expression on the Internet is also a hot topic for debate (Aswad, 2018; Jørgensen & Zuleta, 2020; York, 2021).

Other problems related to digital technologies and the Internet include cybercrime, which brings together many issues (Yar & Steinmetz, 2019).

These include, for example, the illicit circulation of personal data, fraud, hacking attacks for selfish purposes or to destabilize entire government systems, etc. (Jang-Jaccard & Nepal, 2014).

All this put before legal science the task of closely monitoring the course of events in the digital sphere and developing theoretical and practical proposals for improving the legal regulation of human rights in modern times (Coccoli, 2017; Korniienko et al., 2021). Below we analyze the facts and legal regulations regarding

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.45

fundamental rights in the digital environment on the example of EU and international legislation.

2. Methodology

In our study, we used general scientific and special methods, including systemic, factual, formal, and legal.

To conduct a full-fledged study, we operated a systematic method, which considered human rights in the context of digitalization as a separate aspect of the system of legal relations relating to human rights in general. They are interacting, the latest human rights necessary for the adequate legal regulation of current problems in the field of public Internet communication, find their origin in the principles of law in general and the basic provisions of human rights, in its general concept in particular. In this regard, it has been established that the latest human rights related to the use of the Internet are derived from and similar to their predecessors and is in line with established human rights case law, with current changes that meet today's demands for the protection of individuals, their privacy, freedom of expression, etc.

The authors used the factual presentation of information in the section on the formation of legal regulation of human rights on the Internet, in order to demonstrate how and in what direction the legislation in this area is developing. Thus, we have shown how gradually, from identifying a problem or regulatory gap, EU legislators move to address it through legal mechanisms, such as case law and the adoption of new legislation, such as the General Data Protection Regulation (GDPR) in the EU. The relatively new, such as the "right to be forgotten", is considered in the context of the GDPR. We also showed the development of legal regulation on hate speech and freedom of expression on the Internet.

Finally, we utilize the formal-legal method to consider legal norms. This is done in the part devoted to the legal regulation of the latest human rights in the digital age under the law of the European Union. In particular, this applies to the GDPR and the EU Charter of Fundamental Rights as the most relevant examples of such regulation.

3. Literature overview

It should be remarked, that Zuboff (2015), in her study, depicts the risks of new capitalism, which she defines as surveillance capitalism, to human rights. She describes the concept as a new form of information through which big capital wants to moderate people's behavior to increase their income by directing users to consume a particular type of content, purchase services, or goods based on collected information about users. Due to the narrow specialization and lack of mechanisms to counteract such rapid spread of big data technologies and incomprehensible to the average citizen in the depths of their phenomenon of collecting, and analyzing big data, legal systems are only now beginning to take measures to address privacy. Privacy is understood as a human right that has been threatened by the expansion of a new form of capital accumulation that has become big data. According to the researcher, due to the prosperity of a new form of entrepreneurship, which is engaged by technology giants such as Google and Facebook, the values of freedom and democracy, the right of citizens to choose freely without outside influence are under attack (Amnesty International, 2019).

According to Sukhorolsky (2016), European legislation had no choice but to ensure the "right to be forgotten", as it is related to other meaningful human rights such as the right to honor, dignity, and the free formation of one's identity. In his work, the author draws a line between privacy and oblivion, pointing out that the right to be forgotten does not mean the barrier behind personal life, but the impact on public representation, i.e., the "right to be forgotten" operates in the public sphere, although it is related to privacy.

Mreover, Politou, Alepis & Patsakis (2018), in their research, focused on the regulation of personal data protection in Europe. The scholars examined the legal regulation on the "right to be forgotten", according to which a person as a subject of personal data has the right to require the search engine operator to remove data about himself and his actions from search results. They conclude that (despite the problematic issues that may arise in the process of processing such requests and the actual implementation of the procedure for exercising the "right to be forgotten"), the available technical computer capabilities allow to solve them without additional regulation in this area.

Udupa & Pohjonen (2019) proposed their definition of excessive utterances on social media. They preferred the term "extreme speech".

Following the definition, this means the property of statements on the Internet, which goes beyond the permissible statements of ordinary language, is not polite and verified.

Futher, Golovko (2019) connects digital security and culture, arguing that the user in the network protects himself by possessing the knowledge and skills of cybersecurity that makes up his information (digital) culture. The researcher connects the issue of human rights in the digital age with the problems of security and protection of personal data. He derives the so-called "digital rights" from information human rights. Digital rights include the use of virtual reality, digital currency ownership, access to digital services (the Internet), and so on. Information rights, he believes, are paramount in relation to digital, as they took place before the spread of digital means of storing and transmitting the information. The main examples of information rights are the right to receive and disseminate information, the right to receive reliable information from the authorities about the

environment and social processes, the state of the economy, social sphere, etc. (the right to be informed).
Addotionally, Slavko, and Repin (2020) point out, in their work, the practical problems of implementing the "right to be forgotten". Among them, they mention spending time and resources on communication with the source or search engine operator, litigation in case of ignorance, "streisand effect".

According to Vinnyk (2020), it is necessary to legislate what the digital rights of individuals are and to form mechanisms for their legal protection. In his research, the author notes that public policy in this aspect should develop in two directions:
1) concerning the positive effect of the use of digital technologies (incentives);
2) prevention of negative consequences of such use (restrictions). The second direction is characterized by the creation of mechanisms of legal influence such as the existence of algorithms of liability in case of violation of the use of digital technologies, aimed at harming others and / or society.

3. Results

Digitization is the integration of an increasing number of digital computing devices into everyday life to solve varying degrees of complexity, the most important of which is communication. That is why such gadgets, or devices, are called information and communication technologies (ICT) (Golovko, 2019). The primary way to transfer information between these tools is an Internet connection. The right to security, privacy, and confidentiality on the Internet can be seen as an example of the fourth generation of human rights, which is shaped by technological advances in computers and telecommunications. This indicates that previous generations of human rights have not been able to work with phenomena such as the Internet of Things (IoT), social networks, cryptocurrency, etc. Accordingly, there is a need to regulate these processes to ensure the concept of human rights, as there is a risk of interference in their implementation using the same digital technologies. Precisely because the development of technology is much ahead of lawmaking, we have to adapt the law to the latest technological and social phenomena ex post facto (Golovko, 2019).

From the point of view of information culture, it is very vital that users have the opportunity to take care of their rights. Thus, the formation of appropriate information culture in the individual is a factor in his protection from encroachment on his rights in the digital environment (Golovko, 2019). In this situation, the state contributes to the formation of culture through legal regulation, which aims to adapt the existing human rights framework to the realities of the digital age or consolidate new rights that best meet the principles of morality and law (Zolotar, 2016; Beak & Manuilov, 2017).
The information culture of Western democracies implies a clear demarcation of activities in the digital environment of the state and citizens. This implies the principle of non-interference of state and law enforcement agencies in the private life of citizens. However, as the story of Edward Snowden shows, in practice, everything is not so simple, and the latest technologies for data collection and processing allow to use gaps in legal regulation for special, sometimes illegal, purposes (Branum & Charteris-Black, 2015). Lyon (2014) points out that Snowden's revelations show how strong the belief in technological solutions and the synergy of government and corporate structures to implement these solutions. The researcher's conclusions are disappointing, as Snowden's case presents us with a moral dilemma as to which society we want to live in in the future, and with such a "belief in technology" democratic values are in jeopardy.

It is worth noting the features that have made possible the state of affairs with the Internet, through which we discuss digital rights and freedoms. In this regard, we can identify the following features of communication through digital technology and the Internet:

1) inclusiveness;
2) relative anonymity;
3) speed of information dissemination;
4) globality;
5) convenience;
6) the use of support programs to perform specific tasks;
7) the ability to communicate with many people at once (Mansell, 2012; Chan-Olmsted, Cho, & Lee, 2013; Siegel, 2013; Bazarova & Choi, 2014).

By inclusive, we mean the ability to access the network for a wide range of people regardless of their characteristics (Montgomery, 2018). Relative anonymity means that if you follow security measures regarding the confidentiality of your information, such as your stay, geodata using VPN protocols or proxy servers, etc., personal information (name, surname, date of birth, place of work, etc.), a person secures impersonal status online (Ma, Hancock, & Naaman, 2016). The global nature of Internet communication means that the exchange of information can take place between people in different parts of the world, different, even hostile, states (Shklovski, Lindtner, Vertesi, & Dourish, 2010). The observer does not learn from the dialogue of two people in one language that the interlocutors are citizens of different countries who may be on different continents. The convenience of online communication is to reduce the time and effort to perform specific tasks, such as sending a letter, responding to a vacancy, receiving or withdrawing cash, concluding contracts, performing work, receiving services, etc. (Coetzee & Eksteen, 2011). The use of utilities is that access to the Internet and tasks in the digital space requires appropriate tools, including special programs and applications (Godwin-Jones, 2007). For example, web browsers (Google Chrome, Mozilla Firefox, etc.), messengers (Facebook Messenger, Telegram, WhatsApp, etc.), Internet banking applications, media viewers, music players, videos, and entertainment applications. Thus, each program has its purpose and corresponding functionality. The Zoom program, which became popular in the wake of the COVID-19 pandemic, demonstrates the ability to share information with many people at once (Serhan, 2020). Another example is posting on a social network, such as Facebook, Twitter, and Instagram. If you have a large number of subscribers, your post will be seen in a short time by a large number of people who can interact with it (Leban, Thomsen, von Wallpach, & Voyer, 2021).

3. Discussion

In our opinion, the obtained results testify to the active attempts of state institutions to influence the situation around legal issues on the Internet, which in itself is not a negative phenomenon. However, it is difficult to predict how far such regulation may go. However, it should be noted that the need to regulate human rights in the digital context is indeed an urgent problem. In this regard, we believe that the priority of research and legislative initiatives in this direction should be to create a safe, "environmentally friendly" digital environment on the Internet based on the principles of freedom, equality, legality, and the rule of law.

It should be emphasized, Vinnyk (2020) notes that to implement such a project, it is necessary to introduce state registration of public figures and businesses that use digital technologies and the Internet, as prevention of violations of public rights and interests. This view cannot be accepted, because the existing legal mechanisms are sufficient to apply responsibility to public figures, and due to the nature of their activities, their activity in the network is under close public scrutiny, so if they disseminate false information, violate the rights of others, etc., likely, the scandal will immediately go public, accountability measures will be taken by the social media administration, and public authorities will consider the case through existing legal mechanisms. An example is the case of former US President Donald Trump, who was banned for life from the social network Twitter (Twitter Inc., 2021).

At the same time, the case sparked a debate on the role of social networks in democratic processes, such as whether the social network administration has the right to restrict the activities of a legitimately elected president, and whether this is an attack on the presidency and a restriction on democracy (Alizadeh, 2021). However, this is only one aspect of the problem. In fact, the regulation of human rights on the Internet will mainly depend on an integrated approach and the creation of a framework that covers these issues such as personal data protection, hate speech, privacy, online freedom of speech, etc., defining general rules and responsibilities for activity on the Internet. In light of the active development of technology, such wording can help in the direction of further research, because with the advent of new forms of Internet use, such as virtual and augmented reality, we will have to solve new problems based on human rights results in digital conditions, which we just begin to formulate now (Lui, 2021; Needleman & Horwitz, 2021).

3. Conclusions

The need for the legal regulation of human rights on the Internet is an urgent problem today. The peculiarities of the use of social networks have led to the fact that large amounts of information partly harm the interests of individuals and entire social groups, in particular when it comes to hate speech, violation of the individual's right to privacy, etc. As a result, European jurisdictions are adopting legislation aimed at curbing abuses related to access to the network by both individuals and legal entities, in particular concerning the manipulation of users' personal data by large technology companies. These initiatives are aimed at creating a safe "ecosystem" of Internet use and maintaining a balance of private and public interests, which was reflected in the creation of regulation on the "right to be forgotten". The doctrinal factors of its formation are different for European countries and the United States, which has led to a polarization of views on the feasibility of introducing the "right to be forgotten".

We see prospects in further research into the problems of human rights in the network and monitoring the rule of law in the formulation of relevant legislation to prevent excessive state control over the use of the Internet. Due to the significant relevance and debatability of issues such as the relationship between freedom of speech, press, opinion and the right to privacy, protection of personal data, we note that in the near future legislative regulation and theoretical study of these issues in academia will expand.

References

[1] Amnesty International. (2019). Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights.

[2] Aswad, E.M. (2018). The future of freedom of expression online. *Duke L. & Tech. Rev.*, *17*, 26.

[3] Bazarova, N.N., & Choi, Y.H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, *64*(4), 635-657.

[4] Branum, J., & Charteris-Black, J. (2015). The Edward Snowden affair: A corpus study of the British press. *Discourse & Communication*, *9*(2), 199-220.

[5] Chan-Olmsted, S.M., Cho, M., & Lee, S. (2013). User perceptions of social media: A comparative study of perceived characteristics and user profiles by social media. *Online Journal of Communication and Media Technologies*, *3*(4), 149-178.

[6] Coccoli, J. (2017). The challenges of new technologies in the implementation of human rights: An analysis of some critical issues in the digital era. *Peace Human Rights Governance*, *1*(2).

[7] Eakin, P.J. (2015). Self and self-representation online and off. *FRAME, Journal of Literary Studies*, *28*(1), 11-29.

[8] Godwin-Jones, R. (2007). E-texts, mobile browsing, and rich Internet applications. *Language Learning & Technology*, *11*(3), 8-13.

[9] Holmes, S., & Redmond, S. (2012). *Framing celebrity: New directions in celebrity culture*. Routledge.

[10] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[11] Jansen, S., & Martin, B. (2015). The Streisand effect and censorship backfire. *International Journal of Communication, 9,* 656-671.

[12] Jørgensen, R.F., & Zuleta, L. (2020). Private Governance of Freedom of Expression on Social Media Platforms. *Nordicom Review*, *41*(1), 51-67.

[13] Kneuer, M. (2016). E-democracy: A new challenge for measuring democracy. *International Political Science Review*, *37*(5), 666-678.

[14] Korniienko, P.S. et al. (2021). Contemporary Challenges & the Rule of Law in the Digital Age. *Studies of Applied Economics*, *39*(9).

[15] Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, *28*(2), 434-443.

[16] Leban, M., Thomsen, T. U., von Wallpach, S., & Voyer, B. G. (2021). Constructing personas: How high-net-worth social media influencers reconcile ethicality and living a luxury lifestyle. *Journal of Business Ethics*, *169*(2), 225-239.

[17] Lui, T.W. (2021). Augmented reality and virtual reality: Changing realities in a dynamic world. *Information Technology & Tourism, 23,* 637-639.

[18] Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, *1*(2), 2053951714541861.

[19] Mansell, R. (2012). *Imagining the Internet: Communication, innovation, and governance*. Oxford University Press.

[20] Milan, S. (2015). When algorithms shape collective action: Social media and the dynamics of cloud protesting. *Social Media + Society*, *1*(2), 2056305115622481.

[21] Modha, S., Majumder, P., Mandl, T., & Mandalia, C. (2020). Detecting and visualizing hate speech in social media: A cyber watchdog for surveillance. *Expert Systems with Applications*, *161*, 113725.

[22] Montgomery, B.L. (2018). Building and sustaining diverse functioning networks using social media and digital platforms to improve diversity and inclusivity. *Frontiers in Digital Humanities*, *5*, 22.

[23] Moore, M.J., Nakano, T., Enomoto, A., & Suda, T. (2012). Anonymity and roles associated with aggressive posts in an online forum. *Computers in Human Behavior*, *28*(3), 861-867.

[24] Ng, E. (2020). No grand pronouncements here...: Reflections on cancel culture and digital media participation. *Television & New Media*, *21*(6), 621-627. In https://doi.org/10.1177%2F1527476420918828 (access date: 21.01.2022)

[25] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001. doi:10.1093/cybsec/tyy001

[26] Rainie, L. et al. (2013). Anonymity, Privacy, and Security Online. *Pew Research Center*, *5*. In http://pewinternet.org/Reports/2013/Anonymity-online.aspx (access date: 21.01.2022)

[27] Reglitz, M. (2020). The human right to free internet access. *Journal of Applied Philosophy*, *37*(2), 314-331.

[28] Sagan, P., & Leighton, T. (2010). The Internet & the future of news. *Daedalus*, *139*(2), 119-125.

[29] Selwyn, N., Gorard, S., & Furlong, J. (2006). Adults' use of computers and the Internet for self-education. *Studies in the Education of Adults*, *38*(2), 141-159.

[30] Serhan, D. (2020). Transitioning from face-to-face to remote learning: Students’ attitudes and perceptions of using Zoom during COVID-19 pandemic. *International Journal of Technology in Education and Science*, *4*(4), 335-342.

[31] Shklovski, I., Lindtner, S., Vertesi, J., & Dourish, P. (2010, September). Transnational times: locality, globality and mobility in technology design and use. In *Proceedings of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing-Adjunct* (pp. 515-518).

[32] Siegel, D.A. (2013). Social networks and the mass media. *American Political Science Review*, *107*(4), 786-805.

[33] Szymkowiak, A. et al. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. *Technology in Society*, *65*, 101565.

[34] Tăbușcă, S. (2010). The internet access as a fundamental right. *Journal of Information Systems and Operations Management*, *4*(2), 206-212.

[35] Tully, S. (2014). A human right to access the Internet? Problems & Prospects. *Human Rights Law Review*, *14*(2), 175-195.

[36] Udupa, S., & Pohjonen, M. (2019). Extreme Speech and Global Digital Cultures. Introduction. *International Journal of Communication, 13,* 3049-67.

[37] Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*, 3152676.

[38] Yar, M., & Steinmetz, K.F. (2019). *Cybercrime and society*. Sage.

[39] York, J.C. (2021). *Silicon Values: The Future of Free Speech Under Surveillance Capitalism*. Verso Books

[40] Vinnyk, O.M. (2020). Legal problems of digitalization in the perspective of new threats to public welfare. *Current issues of law: theory and practice, 1*(39), 11-18.

[41] Golovko, OM (2019). Digital culture and information culture: human rights in the age of digital transformations. *Information and law, 4*(31), 37-44.

[42] Beak, O.P., & Manuilov, E.M. (2017). Information security in the context of information culture. *Information and law*, *1*(20), 74-81.

[43] Zolotar, O.O. (2016). Human rights and freedoms: information dimension. *IT law: problems and prospects of development in Ukraine,* 59-68.

[44] Slavko, A.S., & Repin, D.A. (2020). Mechanism for realization and protection of the right to forget. *Legal scientific electronic journal, 8,* 522-525.

[45] Sukhorolsky, P. (2016). The right to be forgotten in the legal system of the European Union: realities, problems and prospects. *The science of international law at the turn of the century. Trends in development and transformation,* 90-101.

[46] Chadwick, A. (2008). Web 2.0: New challenges for the study of e-democracy in an era of informational exuberance. *I/S: A Journal of Law and Policy for the Information Society*, *5*, 9-41.

[47] Hasan, L., Morris, A., & Probets, S. (2009, July). Using Google Analytics to evaluate the usability of e-commerce sites. In *International Conference on Human Centered Design* (pp. 697-706). Springer, Berlin, Heidelberg.

[48] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things – promise for the future? An introduction. In *2011 IST-Africa Conference Proceedings* (pp. 1-9). IEEE.

[49] Greenwald, G. (June 6, 2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*.

[50] BBC News UA. (May 13, 2014). Користувачі Google отримали "право на забуття".

[51] Chen, J. et al. (2015, April). Making use of derived personality: The case of social media ad targeting. In *Ninth International AAAI Conference on Web and Social Media*.

[52] Ma, X., Hancock, J., & Naaman, M. (2016, May). Anonymity, intimacy and self-disclosure in social media. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3857-3869).

[53] DeVito, M.A., Gergle, D., & Birnholtz, J. (2017, May). "Algorithms ruin everything". #RIPTwitter, Folk Theories, and Resistance to Algorithmic Change in Social Media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3163-3174).

[54] The Guardian. (March 13, 2018). Myanmar: UN blames Facebook for spreading hatred of Rohingya.

[55] Twitter Inc. (January 8, 2021). Permanent suspension of @realDonaldTrump.

[56] Needleman, S.E., Horwitz, J. (April 6, 2021). Computerized glasses arrive – Facebook, Apple and Niantic bet people are ready to embrace the face-borne devices. *The Wall Street Journal*.

[57] O'Dea, B. (August 20, 2021). Facebook reports increased removal of hate speech across its platforms.

[58] Giansiracusa, N. (October 15, 2021). Facebook Uses Deceptive Math to Hide Its Hate Speech Problem.

[59] Smith, B. (December 5, 2021). How TikTok Reads Your Mind.)

[60] Alizadeh, M. et al. (December 16, 2021). Content moderation as a political issue: The Twitter discourse around Trump's ban.

[61] Bertuzzi, L. (January 20, 2022). MEPs adopt Digital Services Act with significant last-minute changes.

[62] Roth, E. (January 23, 2022). European Parliament approves initial proposal to ban some targeted ads.

[63] MediaSapiens. (January 24, 2022). The European Parliament wants to limit the opportunities for targeted advertising for Google, Amazon and Facebook.

Liydmyla Panova Ph. D., Associate Professor of Civil Law Department, Taras Shevchenko National University of Kyiv (Kyiv, Ukraine). https://orcid.org/0000-0002-1393-8626.

Ernest Gramatskyy Ph. D., Associate Professor of Civil Law Department, Taras Shevchenko National University of Kyiv (Kyiv, Ukraine). https://orcid.org/0000-0003-1260-2888

Inha Kryvosheyina Ph. D., Associate Professor of Intellectual Property Department, Taras Shevchenko National University of Kyiv, Ukraine. https://orcid.org/0000-0003-3630-2257

Volodymyr Makoda Ph. D., Associate Professor of Civil Law Department, Taras Shevchenko National University of Kyiv, Ukraine. https://orcid.org/0000-0003-4408-1925